Güvenlik Stratejileri Dergisi

ATATÜRK STRATEJİK ARAŞTIRMALAR
VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

ATATÜRK STRATEGIC STUDIES
AND GRADUATE INSTITUTE

Cilt / Volume: 21
Sayı / Issue: 52
Aralık / December 2025

BASKI / PRINTED BY
MSÜ Basım ve Yayınevi Müdürlüğü / TNDU Printing and Publishing Office

YAZIŞMA VE HABERLEŞME ADRESİ /
CORRESPONDENCE AND COMMUNICATION

Millî Savunma Üniversitesi
Atatürk Stratejik Araştırmalar
ve Lisansüstü Eğitim Enstitüsü
Yenilevent / İSTANBUL
TÜRKİYE

Web : gsd.msu.edu.tr/
dergipark.org.tr/tr/pub/guvenlikstrtj
E-posta: makale@msu.edu.tr

MİLLÎ SAVUNMA ÜNİVERSİTESİ
ATATÜRK STRATEJİK ARAŞTIRMALAR
VE LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
GÜVENLİK STRATEJİLERİ DERGİSİ

TURKISH NATIONAL DEFENCE UNIVERSITY
ATATÜRK STRATEGIC STUDIES
AND GRADUATE INSTITUTE
GÜVENLİK STRATEJİLERİ DERGİSİ

Cilt/Volume: 21 • Sayı/Issue: 52 • ISSN 1305-4740 • E-ISSN 2822-6984
Uluslararası Hakemli Dergi / International Peer-Reviewed Journal

TARANDIĞIMIZ VERİTABANLARI / DATABASES INDEXING OUR JOURNAL

EBSCO Publishing - Academic Complete Search
DOAJ
Central and Eastern European Online Library (CEEOL)
ULAKBİM-CABİM TR Dizin

DANIŞMA KURULU / ADVISORY BOARD

İÇİNDEKİLER / TABLE OF CONTENTS

*Güvenlik Stratejileri Dergisi'*nin 20 Yılı: Bibliyometrik ve İstatistiksel Bir Analiz
Sibel DİNÇ - Dilek KARABACAK 329

Turkish-American and NATO Relations After the Embargo:Türkiye's Strategic Position in Light of NSSM 227, CIA and NATO Defense Planning Documents (1974-1980)
Macide BAŞLAMIŞLI 355

Çözümü Zor Bir Çatışma Olarak Boko Haram Sorunu
Melike EKİZ KILIÇ - Zekeriyya AKDAĞ 373

Bilgi Ortamında Harekât: Bilgiye Yönelik ve Bilişsel Harp Üzerine Kavramsal Çerçeve Önerisi
Osman Gazi KANDEMİR 395

Çağrı Cihazı Saldırıları Sonrası Siber Tehdit İstihbaratı için Yeni Bir Perspektif ve Model Önerisi
Tuncay DOĞANTUNA - Onur CERAN 415

Siber Güvenlik Kanunu'nun İletişim ve Yeni Medya Faaliyetleri Bağlamında Değerlendirmesi
Mevlüt ALTINTOP 449

Uluslararası Hukuk Bakımından Uzay Faaliyetlerinde Nükleer Enerji Kaynaklarının Kullanımı
Egemen DEMİRER 479

Askerî Etik Eğitimi: West Point ve Kara Harp Okulu
Gizem Nur DEMİREL 497

Yazım Kuralları 529
Submission Guidelines 533

GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 329-354
DOI: 10.17752/guvenlikstrtj.1749299

Araştırma Makalesi
Research Article

Güvenlik Stratejileri Dergisi'nin 20 Yılı: Bibliyometrik ve İstatistiksel Bir Analiz

20 Years of the *Güvenlik Stratejileri Dergisi*: A Bibliometric and Statistical Analysis

Sibel DİNÇ*
Dilek KARABACAK**

Öz

Bu çalışma, *Güvenlik Stratejileri Dergisi*'nin (*GSD*) 2005 ile 2024 yılları arasındaki yayın profilini incelemektedir. Çalışmada öncelikle Güvenlik Çalışmaları alanında Türkiye'de yayımlanan dergilerle ilgili bir durum tespiti yapılmış, ardından *GSD*'nin tarihçesi, editoryal süreçleri ve bu süreçlerde yaşanan değişimlerin dergiye yansıması değerlendirilmiştir. Dergide yayımlanan toplam 387 makalenin 328'i araştırma makalesi olarak değerlendirilmiş ve bibliyometrik yöntemler kullanılarak analiz edilmiştir. Verilerin işlenmesi ve analizinde Python programlama dili ve Excel paket programı kullanılmış, istatistiksel yöntemlerle derginin içerik yapısı, yazar profili ve yayın eğilimleri ortaya konmuştur. Bulgular, *GSD*'nin yıllar içerisinde editoryal süreçlerinde yaşanan değişimlerin ve yayın politikalarındaki dönüşümlerin derginin uluslararasılaşma çabalarına yansıdığını göstermektedir. Ancak yabancı yazar oranının ve İngilizce yayın sayısının istenen seviyede olmadığı görülmektedir. Kadın yazar sayısının son iki yıla kadar görece düşük olması ve anahtar kelimelerin realist güvenlik perspektifiyle ilişkilendirilen konulara ve kavramlara yoğunlaşmış halde kalması, derginin daha kapsayıcı bir perspektif geliştirmesi gereğini ortaya koymaktadır.

Anahtar Kelimeler: *Güvenlik Stratejileri Dergisi*, güvenlik çalışmaları, yazar profili, uluslararasılık, bibliyometrik analiz.

Abstract

This study explores the publication profile of the *Güvenlik Stratejileri Dergisi* (*GSD*) from 2005 to 2024. It begins by assessing the current landscape of journals in Türkiye within the field of security studies, followed by an evaluation of *GSD*'s history and editorial processes, and how changes in these processes have influenced the journal's content. Out of the total 387 articles published, 328 were classified as research articles and analyzed using bibliometric methods. Data processing and analysis were conducted using the Python programming language and Excel software, while statistical methods were applied to elucidate the journal's content structure, author profiles, and publication trends. The findings indicate that changes in *GSD*'s editorial processes and evolving publication policies over the years have significantly contributed to its internationalization efforts. However, the representation of foreign authors and the quantity of publications in English remain below desired levels. Additionally, the relatively low number of female authors, particularly until the last two years, along with keywords predominantly reflecting topics and concepts tied to the realist security perspective, underscore the need for the journal to adopt a more inclusive approach.

Keywords: *Güvenlik Stratejileri Dergisi*, security studies, author's profile, internationality, bibliometric analysis.

* Arş. Gör., Millî Savunma Üniversitesi, Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, İstanbul, Türkiye, e-posta: sibel.dinc@msu.edu.tr, ORCID: 0000-0002-7456-8833b.

** Öğr. Gör. Dr., Millî Savunma Üniversitesi, Fatih Harp Tarihi Araştırmaları Enstitüsü, İstanbul, Türkiye, e-posta: dilek.karabacak@msu.edu.tr, ORCID: 0000-0002-5223-6774.

*** Bu makalenin editoryal süreçleri çift-dış-kör hakemlik usulü ile yürütülmüştür.

Geliş Tarihi / Submitted: 23.07.2025

Kabul Tarihi / Accepted: 03.12.2025

Extended Summary

The *Güvenlik Stratejileri Dergisi (Journal of Security Strategies-GSD)*,[1] published since 2005, has emerged as one of the pioneering academic journals in the field of security studies in Türkiye. This study provides a comprehensive bibliometric analysis of *GSD*'s publication history over a 20-year period (2005–2024) with the aim of assessing the journal's development, current status, and potential areas for improvement.

The study starts with an introduction to the field of Security Studies in Türkiye and to the academic journals published in this field. It then continues to provide information on the history and editorial processes of the *GSD*, along with an examination of how the changes in these processes are reflected in the journal. The selection of the *GSD* for the study is extremely valuable, as it is the first and longest-running academic journal in the field of Security Studies in Türkiye. This study is the first one analyzing the *GSD* bibliometric data, using Python-based data processing and visualization techniques. This analysis on the *GSD* aims to contribute to literature in three dimensions: First, it is the first one providing a data set for all the articles published in the *GSD*'s 20 years of history. Second, it does not only analyze the bibliometric data of the articles and their authors, but it also examines the changes and shifts in the editorial board and their reflections on the journal. Third, it demonstrates the *GSD*'s strengths and weaknesses by pointing out areas of potential improvement and provides some suggestions on possible strategies for the journal.

In total, 387 articles published in *GSD* were examined, of which 328 were identified as research articles and included in the analysis. The study utilized bibliometric methods, supported by data processing and visualization through the Python programming language and the Excel package program. Statistical analyses were employed to evaluate trends in publication frequency, author demographics, and thematic diversity across the years.

Key findings of the analysis indicate that *GSD* has undergone significant editorial and structural transformations. Particularly noteworthy is the increase in the number of research articles published annually since 2019 and the diversification of its author base, with a growing number of submissions from external contributors. However, several limitations remain. The proportion of foreign authors in the journal is only 3%, and articles published in languages other than Turkish (primarily English) constitute just 18% of the total. Gender-based analysis reveals that female authors account for only 18% of all contributors, albeit there occurs a high spike in the percentage of female authors among the first authors: Women academics have presented 32% of the first authors in 2023 and 25% of the first authors in 2024, which is worth mentioning. Moreover, the concentration of certain keywords and the limited thematic diversity suggest that a broader and more inclusive approach is required to position the *GSD* as a leading academic platform in its field. The analysis reveals that the articles published in the journal mostly fall in the category of classical security studies with a realist perspective. However, the journal does not exclude the works of critical security studies or the works written with the new perspectives on security, as the data shows that there are several articles regarding critical security studies or new perspectives published in the journal.

This study concludes that while *GSD*'s institutional heritage and editorial experience provide a strong foundation, strategic steps are necessary to enhance its academic impact and global reach. Recommendations include increasing the percentage of articles written in English, encouraging contributions from international authors and female authors, expanding

1 The journal was titled *Journal of Security Strategies* in English until 2024 to avoid confusion with similarly named journals. Since 2024, it has used the Turkish title *Güvenlik Stratejileri Dergisi* exclusively.

the range of thematic areas, and presenting itself online by taking its place in social media and social networks. As a last note, conducting this bibliometric analysis on the *GSD* on a regular basis will be a valuable contribution both to the journal and to the security studies discipline in Türkiye. This kind of future research may also include comparative analysis across the other journals in the field, as well as the other publications such as dissertations, books, and book chapters, in order to fully understand the development of the security studies discipline in Türkiye.

Giriş

Güvenlik Stratejileri Dergisi (GSD), 2005 yılından bu yana yayın hayatını kesintisiz sürdürmesi nedeniyle, Türkiye akademik yayın dünyasında güvenlik çalışmaları alanına odaklanan ilk ve en uzun soluklu dergi olma özelliğini taşımaktadır. Derginin 20. yayın yılına ulaştığı 2025 yılında *GSD*'de yayımlanan makalelere yönelik kapsamlı bir bibliyometrik analizinin yapılarak böylece derginin kat ettiği mesafenin ve Türkiye'deki güvenlik çalışmaları alanında derginin yerinin tespit edilmesi amaçlanmaktadır.

Türkiye'de son yıllarda uluslararası ilişkiler ve güvenlik çalışmaları alanında Türkiye merkezli dergilerin bir kısmına yönelik bibliyometrik analiz çalışmalar literatürde yerini almaya başlamıştır. Çokişler, Türkiye'deki Uluslararası İlişkiler disiplininde önemli bir yere sahip olan *Uluslararası İlişkiler Dergisi*'nin bibliyometrik analizini yaptığı çalışmasında makaleleri (dil, araştırma, türü, anabilim dalı, anahtar kelimeler, konu, teori, coğrafi bölge ve ülke ölçütleriyle) ve yazarları (ülke, unvan, cinsiyet, kurum, kurumsal ve kişisel üretkenlik ölçütleriyle) değerlendirmiş ve yorumlamıştır.[2] Mehmetcik ve Hakses, Türkiye'deki Uluslararası İlişkiler disiplininin üç anaakım dergisi olarak nitelendirdikleri *Uluslararası İlişkiler*, *All Azimuth* ile *Insight Turkey* dergilerini karşılaştırmalı olarak bibliyometrik analize tabii tutmuş ve aralarındaki benzerlikleri ve farklılıkları ortaya koymaya çalışmıştır.[3] Karataş ise *Güvenlik Bilimleri Dergisi*'ne yönelik bibliyometrik çalışmasında dergide yayımlanmış makaleleri konularına, araştırma yöntemlerine ve teorik çerçevelerine göre incelemiştir.[4] Bu çalışmalardan ilk ikisi ele aldıkları yayınları yayımlanmış makaleler ve bu makalelerin yazarlarına dair verileri değerlendirip yorumlamış ve buradan hareketle Türkiye'deki Uluslararası İlişkiler disiplinine dair birer kesit sunmuşken, üçüncü çalışma ele aldığı dergide yalnızca makalelere dair verileri incelemiş ve değerlendirmelerini dergiyle sınırlı tutmuştur. Ancak Türkiye'de güvenlik çalışmaları alanında önemli bir yere sahip olduğu değerlendirilen *GSD* üzerine bugüne kadar böyle bir analizin henüz yapılmamış olması bir eksiklik olarak görülmektedir ve çalışmada bu eksikliğin giderilmesi hedeflenmektedir.

Bu çalışmanın özgünlüğü, *GSD*'nin 20 yıllık yayın hayatını kapsamlı bir bibliyometrik ve istatistiksel analiz çerçevesinde ele alan *ilk çalışma* olmasından kaynaklanmaktadır. Literatürde *GSD*'nin 2005–2024 yılları arasındaki tüm yayınlarını niceliksel yöntemlerle inceleyen ve bunu yaparken Python tabanlı veri işleme ve görselleştirme tekniklerini kullanan sistematik bir araştırma mevcut değildir. Çalışmanın literatüre katkısının üç boyutlu olacağı değerlendirilmektedir: *1) Literatürdeki Boşluğun Doldurulması:* Yukarıda da belirtildiği gibi, alandaki Türkiye merkezli dergilerin bir kısmına yönelik analizler mevcut iken *GSD* üzerine böyle bir analiz henüz yapılmamıştır. Bu çalışma, güvenlik çalışmaları disiplini içinde önemli bir yayın mecrası olduğu değerlendirilen *GSD*'nin 387 makalesini ve 422 yazarı veri seti

2 Elvan Çokişler, "Uluslararası İlişkiler Dergisinin Bibliyometrik Analizi (2004-2017)", *Uluslararası İlişkiler*, 16:64, 2019, s. 29-56.

3 Hakan Mehmetcik ve Hasan Hakses, "Turkish IR Journals through a Bibliometric Lens", *All Azimuth: A Journal of Foreign Policy and Peace,* 12:1, 2023, s. 61-84.

4 Adnan Karataş, "Determining the Dominant Understandings in Security Science Literature in Turkey: A Bibliometric Analysis on the Journal of Security Science", *Heliyon,* 19:9, 2023, e19278.

haline getirerek alandaki bu boşluğu doldurmaktadır. *2) Literatürdeki Diğer Çalışmalardan Farkı:* Çalışma yalnızca *GSD*'de yayınlanmış çalışmaların bibliyometrik verilerini derleyerek yazar profillerini (cinsiyet, unvan, sivil-asker dağılımı, bağlı olunan kurum dağılımı), anahtar kelime yoğunluklarını ve bunların dönemsel değişimini incelemekle kalmamakta; ayrıca derginin geçirdiği editoryal değişimlere ve bu değişimlerin sonuçlarına da değinmektedir. Çalışma ayrıca derginin atıf trendlerini de farklı kaynaklardan inceleyerek *GSD*'nin güvenlik çalışmaları literatüründeki yerini ortaya koymaktadır. *3) Literatüre Özgün Katkı:* Çalışma, derginin güçlü yönleri kadar eksik kaldığı alanları (örneğin yabancı yazar oranı, kadın yazar temsili, İngilizce makale sayısı) sayısal verilerle göstermekte ve bu bulgular üzerinden öneriler geliştirmektedir. Dolayısıyla çalışma yalnızca dergiye yönelik tarihsel bir döküm değil, aynı zamanda geleceğe yönelik politika önerileriyle literatürü ileriye taşıyan analitik bir çerçeve sunmaktadır. Ayrıca *GSD* özelindeki bu çalışmanın belirli aralıklarla (beş yıllık periyodlarla) tekrarlanarak disiplinin ve derginin dönüşümü ve kat ettiği yol hakkında daha fazla bilgi sunulması planlanmaktadır ki bunun da alana özgün bir katkı olacağı düşünülmektedir.

Yayın hayatında 20 yılı ve 50 sayıyı geride bırakan *GSD*'yle ilgili *ilk özgün analizi* sunan bu çalışmanın hem Türkiye'deki güvenlik çalışmalarının ve *GSD*'nin gelişimini ortaya koyarak alana katkı sağlaması hem de elde edilen bulguların değerlendirilmesiyle derginin ulusal ve uluslararası alanda daha ileriye taşınması için önerilerle dergiye katkıda bulunması amaçlanmaktadır.

Çalışma hazırlanırken birincil kaynak olarak *GSD*'nin arşivinden ve ikincil kaynaklar olarak güvenlik çalışmaları alanındaki akademik çalışmalardan ve raporlardan yararlanılmıştır. Ayrıca çalışmanın ikinci yazarı, *GSD*'nin yayım hayatına başladığı 2005 yılından bu yana dergide yayın ve yazı kurulları üyeliği, yayın koordinatörlüğü, editör yardımcılığı ve dil editörlüğü gibi aktif görevlerde bulunmuştur ve hâlen derginin yayın süreçlerinde sorumluluk üstlenmeye devam etmektedir. Çalışmanın ikinci yazarının bu 20 yıllık süreç içindeki gözlemleri derginin tarihini, geçirdiği dönüşümleri ve bu dönüşümlerin dergiye yansımalarını değerlendirmede kullanılmıştır. Bu bağlamda, ilk olarak Türkiye'deki güvenlik çalışmalar alanıyla ve alandaki dergilerle ilgili kısa bir durum tespiti yapıldıktan sonra *GSD*'nin tarihçesi, editoryal süreçleri ve bu süreçler içinde yaşanan değişimler ele alınacak ve bu değişimlerin dergiye yansıması değerlendirilecektir. Ardından çalışmanın metodolojisi açıklanarak dergideki makalelerin niceliksel incelemesi sonucu elde edilen bulgular ortaya konulacaktır. Son olarak Değerlendirme ve Sonuç bölümünde bu bulgular yorumlanarak derginin gelecekte atabileceği adımlara ve benimseyebileceği stratejilere yönelik öneriler sunulacaktır.

1. Türkiye'de Güvenlik Çalışmalarının Tarihçesi

Güvenlik kavramı, siyaset bilimi teorisyenleri veya askerî stratejistler tarafından "savaş çalışmaları", "askerî çalışmalar" ve "strateji" başlıkları altında çalışılsa da Uluslararası İlişkiler disiplininde bir alt disiplin olarak ortaya çıkması 1940'lı yıllara rastlamaktadır.[5] Soğuk Savaş ortamında Stratejik Çalışmalar veya Ulusal Güvenlik Çalışmaları terimleri birbiri yerine geçer şekilde neredeyse eş anlamlı olarak kullanılmaktayken günümüzde daha kapsayıcı olarak Güvenlik Çalışmaları terimi kullanılmaktadır.[6]

5 Başar Baysal, "Güvenlik Kavramı ve Güvenliğin Dönüşümü", Başar Baysal (der.) *Uluslararası İlişkilerde Güvenlik*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2022, s. 7-8; Barry Buzan ve Lene Hansen, "Strategic Studies, Deterrence and the Cold War", *The Evolution of International Security Studies*, Cambridge University Press, Cambridge, 2009, s. 66-100.

6 Sinem Akgül-Açıkmeşe, "Algı mı, Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri", *Uluslararası İlişkiler*, 8:30, 2011, s. 45-47; Ole Wæver ve Barry Buzan, "Teoriye Dönüş Sonrası: Güvenlik Çalışmalarının Geçmişi, Bugünü ve Geleceği", Alan Collins (ed.), *Çağdaş Güvenlik Çalışmaları* (Üçüncü Basım, Çev. Nasuh Uslu), Uluslararası İlişkiler Kütüphanesi, İstanbul, 2017, s. 394.

Güvenlik Çalışmalarının devlet-merkezli geliştiği Soğuk Savaş döneminde, Türkiye'de akademik alanda uzun yıllar yeterli ilgiyi görmemiştir. Bunun en önemli nedeni olarak Türkiye'de güvenlik alanının uzun yıllar sadece askerî kurumların kontrolünde olması ve güvenlik çalışmalarının "devlet"in işi olduğunun düşünülmesi gösterilmektedir.[7] Güvenlik kavramının çok boyutlu olarak ele alınmaya başladığı ve yeni güvenlik kuramlarının ortaya çıktığı 1990'larda uluslararası literatürde yaşanan tartışmalar Türkiye'ye daha geç yansımıştır. Türkiye'deki literatüre bakıldığında, güvenliğin geniş gündeminin ve güvenliğe yönelik eleştirel bakış açılarının ancak 2000'lerde akademik çalışmalara "sınırlı" bir şekilde yansıdığı görülmektedir.[8] Ancak bu "sınırlı" ilgi hızla büyümüş ve 2010'ların başından itibaren güvenlik kavramıyla ilgili yeni aktörler, yeni tehdit türleri ve yeni kuramlar üzerine tartışmalar Türkiye literatüründe kendini göstermeye başlamıştır. Böylece Türkiye'de de Güvenlik Çalışmaları alanına sadece askerî kurumlar değil, diğer kamu kuruluşları, üniversiteler ve araştırma merkezleri de katkı sağlamaya başlamıştır.[9] Bu artan ilginin bir göstergesi de güvenlik alanında çalışan akademisyenlerin sayısıdır.

Türkiye'de Uluslararası İlişkiler disiplini içinde temel çalışma alanı olarak (uluslararası) güvenlik alanını seçen akademisyenlerin sayısı dikkat çekicidir. YÖK Akademik üzerinden bakıldığında Uluslararası İlişkiler disiplini altındaki "Uluslararası Güvenlik" alt disiplininde 436 akademisyen bulunduğu görülmektedir ki bu rakam disiplinde %30,8'lik bir dilime karşılık gelmektedir.[10] Uluslararası İlişkiler disiplinine kıyasla hayli yeni bir alan olan Güvenlik Çalışmalarında ise 56 akademisyen yer almaktadır.[11] Güvenlik Çalışmaları disiplini, Üniversitelerarası Kurul (ÜAK) tarafından 2023 yılı Ekim ayından itibaren "Sosyal, Beşerî ve İdari Bilimler Temel Alanı" altında tanımlanmıştır ve bu açıdan bakıldığında kurumsallaşma ve bilim alanı olarak kabul edilme açısından önemli bir aşamaya geçilmiştir.[12] Güvenlik Çalışmalarına yönelik lisansüstü programlarının çoğalmasıyla birlikte, önümüzdeki dönemde bu alanda çalışan akademisyenlerin sayısı da artacaktır.

2. Türkiye'de Güvenlik Çalışmaları Alanındaki Dergilerin Tarihçesi

Güvenlik Çalışmaları alanında Türkiye merkezli dergiler arasında *GSD*'nin konumunu görmek için, DergiPark'ta "güvenlik", "güvenlik çalışmaları", "güvenlik stratejileri" ve "güvenlik araştırmaları" anahtar kelimeleriyle bir tarama yapılmıştır. Tarama sonucu ulaşılan dergiler değerlendirildiğinde, *GSD*'nin bu alana odaklanan en uzun soluklu dergilerden biri

7 Mustafa Aydın, Hans Günter Brauch, Necati Polat, Mitat Çelikpala, Ursula Oswald Spring (der.), *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2012, s. xvii.

8 Sinem Akgül Açıkmeşe ve Erman Ermihan, "Türkiye'de Güvenlik Çalışmaları", Ayça Ergun, Çiğdem Üstün ve Sinem Akgül Açıkmeşe (der.), *Türkiye'de Uluslararası İlişkiler Çalışmaları. Alt Alanlar ve Bölgesel Odaklar*, İmge Kitapevi, İstanbul, 2023, s. 278.

9 Bu alandaki bir Türkçe yayınlar kaynakçası için bkz.; *Güvenlik Çalışmaları Türkçe Yayınlar Bibliyografyası (1990-2021)*, Millî Savunma Üniversitesi, Kara Harp Okulu, Ankara, 2021, https://kutuphane.msu.edu.tr/?p=5&id=H7C5D4IZ6M&dil=tr&q=bibliyografya, erişim 20.07.2025.

10 YÖK Akademik, "Yükseköğretim Akademik Arama Sayfası", https://akademik.yok.gov.tr/AkademikArama/, erişim 21.09.2025. Burada dikkat çekici husus, son yedi yılda bu oranda %10'luk artış yaşanmış olmasıdır. 2018 yılında Türkiye'de Uluslararası İlişkiler disiplini akademisyenlerine yönelik gerçekleştirilen ankette ana araştırma alanını "ulusal/küresel güvenlik" olarak belirten akademisyenlerin oranı %19,4 olarak tespit edilmiştir. Bkz. Mustafa Aydın ve Cihan Dizdaroğlu, "Türkiye'de Uluslararası İlişkiler: TRIP 2018 Sonuçları Üzerine Bir Değerlendirme", *Uluslararası İlişkiler*, 16:64, 2019, s. 6-7.

11 YÖK Akademik, "Yükseköğretim Akademik Arama Sayfası", https://akademik.yok.gov.tr/AkademikArama/, erişim 21.09.2025.

12 Erdem Özgür ve Murat Yılmaz, "Güvenlik Çalışmaları Alanının Mevcut Durumu ve Geleceği Üzerine Bir Değerlendirme", *Güvenlik Stratejileri Dergisi*, 20:49, 2024, s. 288-289. Bu disiplin Savaş Araştırmaları, Güvenlik Stratejileri ve Uluslararası Güvenlik alt disiplinlerinin yanı sıra çevre güvenliği, deniz güvenliği, su güvenliği, terörizm, trafik güvenliği, siber güvenlik, hudut güvenliği ve kamu güvenliği alt disiplinlerini de içermektedir. Dolayısıyla bu alan için belirlenen çalışma alanları hem Kamu Yönetimi hem Uluslararası İlişkiler disiplinleri altında da yer almaktadır.

olduğunu söylemek mümkündür. *GSD*'nin yayınlanmaya başladığı 2005 yılından önce bu alanda sadece *Savunma Bilimleri Dergisi*'nin (ilk sayısı 2002 yılında) ve *Uluslararası İlişkiler Dergisi*'nin (ilk sayısı 2004 yılında) yayımlanmakta olduğu görülmektedir. Bununla birlikte, *Savunma Bilimleri Dergisi*, öncelikli amacını "savunma bilimleri alanındaki bilimsel gelişmeleri takip etmek ve gelişmesine hizmet etmek" olarak belirlemiştir ve yayıncısı olan enstitüdeki lisansüstü programlara paralel şekilde mühendislik bilimleri ağırlıklı makaleler yayımlamaktadır.[13] *Uluslararası İlişkiler Dergisi*'nde ise daha kapsamlı bir dergi olarak güvenlik çalışmalarının yanı sıra uluslararası ilişkiler, politik tarih, uluslararası hukuk, diplomasi ve uluslararası politik ekonomi dahil olmak çok geniş bir konu yelpazesinde makaleler yer almaktadır.[14] Dolayısıyla bu iki dergi yalnızca güvenlik ve güvenlik çalışmaları alanına odaklanan dergiler olmamıştır.

Güvenlik Stratejileri Dergisi'ni 2006'da *Kara Harp Okulu Bilim Dergisi*; 2012'de *Güvenlik Bilimleri Dergisi* ve 2014'te *Güvenlik Çalışmaları Dergisi* izlemiştir. Bu dergiler de güvenlik odaklı kamu yükseköğretim kurumlarınca yayımlanmalarına rağmen, odaklandıkları alanlar *GSD*'den farklı olmuştur. Kara Harp Okulu Dekanlığı'nca yayımlanan *Kara Harp Okulu Bilim Dergisi*,[15] daha çok savunma bilimleri odaklı disiplinler arası bir dergidir. Jandarma ve Sahil Güvenlik Akademisi, Güvenlik Bilimleri Enstitüsü'nün yayımladığı *Güvenlik Bilimleri Dergisi*[16] ile Polis Akademisi, Güvenlik Bilimleri Enstitüsü'nün yayımladığı *Güvenlik Çalışmaları Dergisi*[17] ise yayıncı enstitülerinin çalışma alanlarına ve misyonlarına uygun olarak daha çok iç güvenlikle ilgili alanlara dönük yayın yapmaktadır.

DergiPark üzerinden yapılan taramada dikkat çekici bir husus ise, 2017 yılından itibaren güvenlik ve güvenlik araştırmaları/çalışmaları alanlarını konu kapsamları arasına alan ve kamu kurumları veya üniversiteler dışında özel kişilerce veya derneklerce yayımlanan yeni dergilerin ortaya çıkmasıdır. Ancak bu dergiler güvenlik araştırmalarını/çalışmalarını öncelikli alan olarak belirlememekte, güvenlik çalışmaları alanını uluslararası ilişkiler, uluslararası politika, diplomasi, strateji ve bölge çalışmaları ve bunların alt dallarını da içeren geniş bir konu yelpazesi içine dâhil etmektedir. Bu dergilere örnek olarak *International Journal of Politics and Security* (2019),[18] *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi* (2017),[19] *Diplomasi ve Strateji Dergisi* (2020),[20] *SDE Akademi Dergisi* (2021),[21] *Uluslararası İlişkiler ve Politika Dergisi* (2021)[22] sayılabilir. Son yıllarda ise terörizm, terörizmle mücadele ve istihbarat çalışmaları da dikkat çekmiş; bu alanda yayın hayatlarına başlayan *Terörizm ve Radikalleşme Araştırmaları Dergisi* (2022)[23] ve *Güvenlik ve İstihbarat Çalışmaları Dergisi* (2023)[24] konu yelpazelerine güvenlik araştırmalarını/çalışmalarını da dâhil etmiştir. *Savunma*

13 Dergi, 2023 yılında aldığı kararla, 2024 yılından itibaren sadece Mühendislik ve Fen Bilimleri alanlarından yayın kabul edeceği duyurusunu yapmış ve böylece temel alan değişikliğine gitmiştir. *Savunma Bilimleri Dergisi*, https://kho.msu.edu.tr/akademik/enstitu/enstitu_Alp_SAVBEN_dergi_anasayfa.html ve https://dergipark.org.tr/tr/pub/khosbd, erişim 20.07.2025.

14 *Uluslararası İlişkiler Dergisi*, https://www.ir-journal.com/tr, erişim 20.07.2025.

15 Derginin adı 2020 yılında *SAVSAD Savunma ve Savaş Araştırmaları Dergisi* olarak değiştirilmiştir. *SAVSAD Savunma ve Savaş Araştırmaları Dergisi*, http://savsad.kho.msu.edu.tr/, erişim 20.07.2025.

16 *Güvenlik Bilimleri Dergisi*, https://dergipark.org.tr/tr/pub/gbd, erişim 20.07.2025.

17 *Güvenlik Çalışmaları Dergisi*, https://guvenlikcalismalari.pa.edu.tr/, erişim 20.07.2025.

18 *International Journal of Politics and Security*, https://dergipark.org.tr/tr/pub/ijps, erişim 20.07.2025.

19 *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, http://uksad.com/, erişim 20.07.2025.

20 *Diplomasi ve Strateji Dergisi*, https://www.dsjournal.org/, erişim 20.07.2025.

21 *SDE Akademi Dergisi*, https://dergipark.org.tr/tr/pub/sde, erişim 20.07.2025.

22 *Uluslararası İlişkiler ve Politika Dergisi*, https://dergipark.org.tr/tr/pub/ulipod, erişim 20.07.2025.

23 *Terörizm ve Radikalleşme Araştırmaları Dergisi*, https://www.tradergisi.com/, erişim 20.07.2025.

24 *Güvenlik ve İstihbarat Çalışmaları Dergisi*, https://jsis.org.tr/, erişim 20.07.2025.

ve Güvenlik Araştırmaları Dergisi (2024)[25] ise bu alanda yayın hayatına başlayan en yeni dergi olmuştur.[26]

Bu bölümde ele alındığı gibi, *GSD*'nin Türkiye merkezli olarak güvenlik çalışmaları alanına odaklanan ilk ve en uzun soluklu dergi olduğu görülmektedir. Derginin bu uzun soluklu geçmişine ve geçirdiği değişimlere bakıldığında, derginin kat ettiği mesafe ve ulaştığı nokta daha iyi anlaşılabilir.

3. *Güvenlik Stratejileri Dergisi* Tarihi ve Kapsamı[27]

Dergi, Harp Akademileri Komutanlığı (HAK) bünyesinde 2003 yılında öncelikli olarak güvenlik ve strateji alanlarında lisansüstü eğitim verme amacıyla kurulan Stratejik Araştırmalar Enstitüsü (SAREN) tarafından Haziran 2005'te yayımlanmaya başlamıştır. Bu ilk sayıda dönemin Harp Akademileri Komutanı imzasıyla yayımlanan sunuş yazısında, öğretim kurumlarının saygınlığının, öğretim faaliyetlerinin yanı sıra yayın faaliyetleriyle olan bağlantısı vurgulanmış ve derginin sadece SAREN'e değil aynı zamanda HAK'a bilimsel açıdan katkı sağlayacağı vurgulanmıştır.[28] Ulusal hakemli dergi olarak yayım hayatına başlayan *GSD*, Aralık 2011'deki 14. sayısından itibaren gerek yayın ve danışma kurullarına gerekse hakem havuzuna uluslararası düzeydeki akademisyenleri dâhil etmiş, aynı zamanda farklı ülkelerden akademisyenlerin/araştırmacıların makalelerini yayımlamaya başlamış ve böylece uluslararası hakemli dergi haline gelmiştir. Millî Savunma Üniversitesi'nin (MSÜ) ve üniversite bünyesinde Atatürk Stratejik Araştırmalar Enstitüsü'nün (ATASAREN) Kasım 2016'da kurulmasının ardından,[29] *Güvenlik Stratejileri Dergisi*, MSÜ Rektörü'nün Aralık 2016 tarihli yazısıyla ATASAREN'e devredilmiştir. Dergi, böylece, yayın periyodunu aksatmadan yayın hayatına devam edebilmiştir.

Dergi yayın hayatına başlarken editörlüğünü SAREN Müdürü üstlenmiş ve bu uygulama uzun süre devam etmiştir. Ancak zamanla SAREN'deki öğrenci sayısıyla birlikte öğretim faaliyetlerinin yoğunlaşması, bilimsel etkinliklerin hem türlerinin hem sayısının artmasıyla birlikte 2011 ile 2014 yılları arasında dergi editörlüğünü SAREN Anabilim Dalı başkanlarından biri üstlenmiştir. 2014 ile 2017 yılları arasında atamalar nedeniyle değişiklikler yaşansa da dergi sayı aksatmadan yayın hayatına devam edebilmiştir.

Tablo 1'de, 2005'ten günümüze kadar olan dergi editörleri, kurum, rütbe, akademik unvan ve disiplin bilgileri yer almaktadır.

25 *Savunma ve Güvenlik Araştırmaları Dergisi*, https://kho.msu.edu.tr/akademik/enstitu/hakkimizda_guvenlik_dergi.html ve https://dergipark.org.tr/tr/pub/saga, erişim 20.07.2025.

26 Burada parantez içinde verilen yıllar, dergilerin ilk sayılarının yayımlandığı yıllardır.

27 Çalışmanın giriş bölümünde de belirtildiği gibi, çalışmanın ikinci yazarı, *GSD*'nin yayım hayatına başladığı 2005 yılından bu yana dergide aktif olarak görev almaktadır ve bu bölümdeki bilgiler ikinci yazarın gözlemlerine dayanmaktadır.

28 "Sunuş", *Güvenlik Stratejileri Dergisi*, 1:1, 2005, 5.

29 Atatürk Stratejik Araştırmalar Enstitüsü, 17 Mart 2022 tarihinde, MSÜ bünyesinde faaliyetlerine devam eden Barbaros Deniz Bilimleri ve Mühendisliği Enstitüsü (Barbaros DEBİM), Hezarfen Havacılık ve Uzay Teknolojileri Enstitüsü (Hezarfen HUTEN) ile birleşmiş ve bu birleşmenin ardından Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü adını almıştır. Enstitünün kısaltması ATASAREN olarak kullanılmaya devam edilmektedir. Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü, "Enstitümüz Hakkında", https://atasaren.msu.edu.tr/misyonvizyon, erişim 20.07.2025.

Tablo 1. *Güvenlik Stratejileri Dergisi* Editörleri[30]

Tarih Aralığı	Sayılar	Başeditör / Editör(ler)	Kurum	Rütbe	Akademik Unvan	Disiplin
Haz 2005– Ara 2005	1 ve 2	Şinasi SEDAR	SAREN (Müdürü)	Alb.	–	–
Haz 2006– Haz 2010	3 ile 11 arası	Ahmet KÜÇÜKŞAHİN	SAREN (Müdürü)	Alb.	Dr.	Uluslararası İlişkiler
Ara 2010– Haz 2011	12 ve 13	Hasip SAYGILI	SAREN (Müdürü)	Alb.	Dr.	Yakın Çağ Tarihi
Ara 2011– Eki 2014	14 ile 20 arası	R. Kutay KARACA	SAREN (ABD Bşk)	Alb.	Dr.	Uluslararası İlişkiler
Nis 2015	21	Zekeriya TÜRKMEN	SAREN (Müdürü)	Alb.	Dr.	Yakın Çağ Tarihi
Eki 2015– Nis 2016	22 ve 23	Hasan HOŞOĞLU ve Engin AVCI	SAREN (Müdürü) ve SAREN (ABD Bşk)	Alb. Alb.	Dr. Dr.	Uluslararası İlişkiler ve Güvenlik Çalışmaları
Ara 2016	24	Orhan SEZGİN ve Engin AVCI	SAREN (Müdürü) ve JSGA	Alb. Alb.	Dr. Dr.	Yönetim ve Organizasyon ve Güvenlik Çalışmaları
Nis 2017	25	Orhan SEZGİN ve Gültekin YILDIZ	ATASAREN (Müdürü) ve İstanbul Üniversitesi	Alb. –	Dr. Doç. Dr.	Yönetim ve Organizasyon ve Yakın Çağ Tarihi
Eki 2017– Mar 2021	26 ile 37 arası	Gültekin YILDIZ	ATASAREN (Müdürü)	–	Doç. Dr.	Yakın Çağ Tarihi
Haz 2021– Ara 2021	38 ile 40 arası	Cemalettin ŞAHİN	ATASAREN (Müdürü)	–	Prof. Dr.	Beşerî ve İktisadi Coğrafya
Nis 2022– Ara 2024	41 ile 49 arası	Gültekin YILDIZ	MSÜ KHO Dekanı / MSÜ Rektör Danışmanı	–	Prof. Dr.	Yakın Çağ Tarihi
Nis 2025– …	50 – …	Gültekin YILDIZ ve Barış ATEŞ	MSÜ Rektör Danışmanı ve ATASAREN (ABD Başkanı)	– Alb.	Prof. Dr. Doç. Dr.	Yakın Çağ Tarihi ve Askerî Sosyoloji

Dergi başeditörlüğü/editörlüğü 2017 yılı sonrasında yine enstitü müdürü tarafından üstlenilmiştir; ancak ATASAREN bünyesinde akademik faaliyetlerin artması (yeni lisansüstü programların açılması, öğrenci sayısının hızlı artışı ve bilimsel toplantı/çalıştayların düzenlenmesi vb.) nedeniyle derginin editör kurulunda ve sürecinde yeniden yapılanmaya gidilmiştir. Bu doğrultuda, Başeditörün/Editörün görevlerinin bir bölümü Yayın Koordinatörü, Editör Yardımcıları, Teknik Editör ve Dil Editörü tarafından üstlenilmiştir. Buna ek olarak artan miktardaki makalenin ve dergi sürecindeki değişimin analiz edilebilmesi için 2024 yılı itibariyle İstatistik Editörü dergiye atanmıştır. Dergiye gönderilen aday makalelerin sayısındaki artışı da bu yönde bir iş bölümüne gidilmesini gerektiren bir başka etken olmuştur.

30 Güvenlik Stratejileri Dergisi, "Sayılar", https://gsd.msu.edu.tr/TR/Sayilar, erişim 15.07.2025.

Derginin editoryal işleri, halihazırda editör yardımcıları tarafından etkin ve hızlı bir şekilde yürütülmektedir. Tüm süreçleri DergiPark üzerinden ilerleyen derginin süre istatistiklerine bakıldığında, makale gönderimi ile ilk editör ataması arasında geçen sürenin 2022 yılında ortalama 10 gün olduğu ve 2023 ve 2024 yıllarında ise bu sürenin ortalama üç güne indiği görülmektedir. Makale gönderimi ile makalenin iade edilmesi arasında geçen süre ise 2023 ve 2024 yıllarında ortalama 22-23 gün olarak gerçekleşmiştir.[31] Akademik dergi yayıncılığı açısından bakıldığında sürecin hızlandığı tespit edilmektedir.

4. Yöntem

Bibliyometrik analiz, literatürdeki bilimsel üretkenliği ve araştırma eğilimlerini incelemek için kullanılan nicel bir yöntemdir. Bu yöntem; yayın sayıları, atıf oranları, yazarlar, kurumlar, anahtar kelimeler ve ülkesel dağılımlar gibi değişkenler üzerinden bir alandaki bilgi üretimini sistematik olarak değerlendirmeyi amaçlar. Bibliyometrik yöntemler; literatürdeki trendleri ve araştırma boşluklarını tespit etmek için güçlü bir araç olarak kabul edilmektedir.[32]

Çalışma kapsamında *Güvenlik Stratejileri Dergisi*'nin niceliksel analizi için veriler DergiPark ve Editör erişim sayfalarından toplanmıştır. Elde edilen veriler Excel ortamına aktarılmış ve veri analizi için ön işleme (düzenleme ve verinin analize hazır hale getirilmesi) aşamalarının ardından tanımlayıcı istatistikler ile desteklenmiştir. Bu süreçte hem bibliyometrik analiz hem de betimsel istatistikler kullanılmış; verilerin işlenmesi ve analiz edilmesi için Python programlama dili ve Excel paket programından yararlanılmıştır.

Bu kapsamda, yayımlanan 387 makalenin verisi toplanmış; araştırma makalesi olan ve 2005-2024 yılları arasında yayımlanan 328 makale çalışma kapsamında analiz edilmiştir. 2025 yılı verileri yılın tamamlanmaması sebebiyle analiz sürecine dahil edilmemiştir.

Bu çalışmanın yalnızca araştırma makaleleri ile sınırlandırılmasının iki temel nedeni bulunmaktadır. İlk olarak, bibliyometrik analizlerde standart uygulama, bilimsel üretkenliği ölçmek için özgün araştırma makalelerini temel birim olarak almaktır; çünkü bu tür yayınlar atıf alma potansiyeli, metodolojik özgünlükleri ve literatüre katkı düzeyleri açısından en sağlıklı karşılaştırmayı sağlamaktadır. Derleme makaleleri, kitap incelemeleri veya editöryal yazılar daha farklı bir işlev görmekte, çoğunlukla literatürün mevcut durumunu özetlemekte veya değerlendirme amaçlı kaleme alınmaktadır. İkinci olarak, yalnızca araştırma makalelerinin analize dâhil edilmesi, yıllar içerisinde derginin üretkenlik, konu çeşitliliği ve yazar profili açısından gösterdiği eğilimlerin daha tutarlı biçimde karşılaştırılmasına olanak vermektedir. Bu nedenle, araştırma makaleleri dışındaki içerikler çalışma kapsamı dışında bırakılmıştır.

Veri seti toplanırken yaşanan en büyük problem eksik gözlem sorunudur. Dergiye başvuran yazarlar talep edilen bilgileri yanıtlamakta bilinçli ya da bilinçsiz bir şekilde geri kalmışlardır. Asker geçmişi olan ancak bu bilgileri makale gönderim sürecinde paylaşmayan yazarların olduğu çalışma kapsamındaki araştırma sırasında tespit edilmiştir. Bu da eksik ve hatalı bilgilerin mevcut olduğunu gösterir ancak araştırma kapsamında yazarların kendi paylaştıkları bilgilere ek olarak çalışma için geniş çaplı araştırma yapılıp elde edilen bilgiler ile gönderilen bilgiler karşılaştırılıp gerekli veri düzenlemeleri yapılmıştır. Buna ek olarak çalışma için seçilen değişkenler ile gözlemler (makaleler) arasında en az on katı bir oran bulunması çalışma verilerinin istatistiki analiz için uygun olduğunu göstermesi bakımında önemlidir. İlgili çalışma için oluşturulan değişkenler sırasıyla "Makale ID, Yıl, Cilt, Sayı,

31 *Güvenlik Stratejileri Dergisi*, "Süre İstatistikleri", https://dergipark.org.tr/tr/pub/guvenlikstrtj/time-statistics, erişim 08.06.2025.

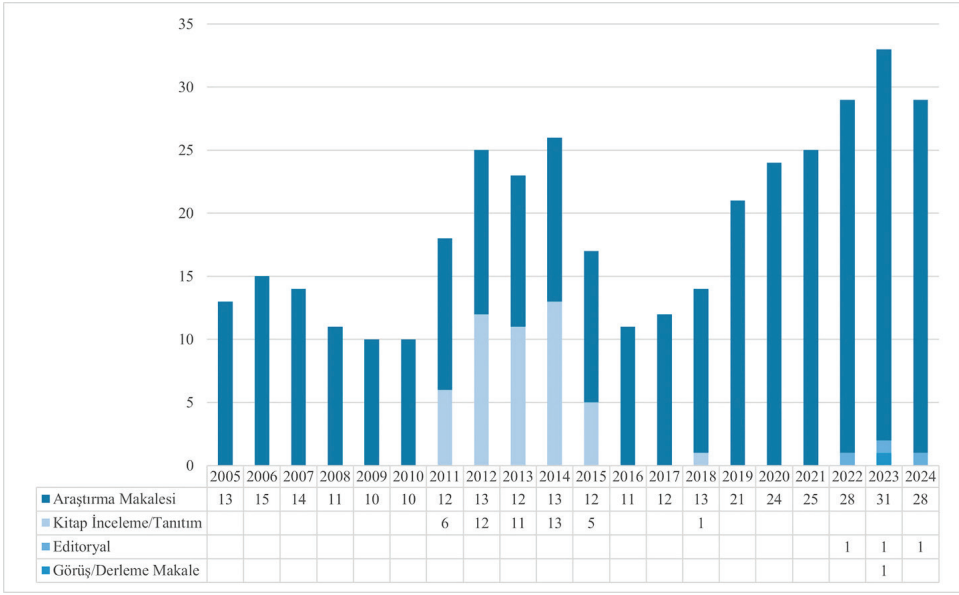
32 Naveen Donthu, Satish Kumar, Debmalya Mukherjee, Nitesh Pandey ve W. M. Lim, "How to Conduct a Bibliometric Analysis: An Overview and Guidelines", *Journal of Business Research* 133, 2021, s. 285-296.

Makale Türü, Dil, Yazar Sayısı, Yazar Cinsiyeti, Anahtar Kelimeler, Yazar Uyruğu, Yazar Özgeçmişi (Asker/Sivil), Yazar Akademik Unvanı, Yazar Kurumu, Yazar Uzmanlık Alanları, Yazar Öncelikli Uzmanlık Alanı" şeklindedir.

5. Bulgular[33]

Güvenlik Stratejileri Dergisi, 2005-2018 yılları arasında yılda iki sayı, 2019-2021 yılları arasında yılda dört sayı, 2022 ve devam eden yıllarda üç sayı ve ek bir özel sayı ile toplamda yılda yine dört sayı[34] ile yayın hayatına devam etmektedir. Dergide araştırma makalelerinin yanı sıra, görüş ve derleme makaleler, kitap incelemeleri/tanıtımları da yayımlanmaktadır. Şekil 1'deki grafikte çalışma türlerinin yıllara göre dağılımı verilmektedir. 2011-2015 yılları arasında dergideki kitap incelemesi ve kitap tanıtımı türlerindeki çalışmalar diğer yıllara göre belirgin bir artış göstermiştir. Ancak 2016'dan sonraki sayılarda bu türdeki yayınların devam etmediği görülmektedir.

Şekil 1. Yıllara Göre Yayımlanan Çalışma Türlerinin Dağılımı



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Araştırma Makalesi	13	15	14	11	10	10	12	13	12	13	12	11	12	13	21	24	25	28	31	28
Kitap İnceleme/Tanıtım							6	12	11	13	5			1						
Editoryal																		1	1	1
Görüş/Derleme Makale																			1	

Yöntem bölümünde açıklandığı gibi çalışma yalnızca araştırma makaleleriyle sınırlandırılmıştır ve Tablo 2'de derginin ciltlere göre ortalama araştırma makalesi (bundan sonra "makale") sayıları verilmiştir. Şu ana kadar toplam 20 cildi yayınlanan derginin ciltleri beşer yıllık periyotlara ayrılmıştır. Her bir periyod aralığında yer alan makale sayısının cilt sayısına bölünmesi ile her bir ciltte ortalama kaç makalenin yayımlandığı bulunmuştur. Bu dağılım içinde araştırma makalelerinde 2019 yılından itibaren yıllık bazda düzenli ve belirgin bir artış görülmektedir: Beş yıllık periyodlar bazında bakıldığında, araştırma makalelerinin ortalamaları 2005-2009 yılları arasında 12,6; 2010-2014 yılları arasında 12 ve 2015-2019 yılları arasında 13,8 iken, bu ortalama 2019-2024 yılları arasında 22,4'e yükselerek bir önceki beş yıllık periyodun iki katına yaklaşmıştır.

33 Bu bölümde sunulan şekil, grafik ve tablolar, çalışma için hazırlanan veri setinden yazarlar tarafından özgün olarak oluşturulmuştur.

34 "Türk Dünyası'nda Yeni Dönem: Türk Devletleri Teşkilatı" Özel Sayısı 2022'de, "'Yeni' Savaşlar ve 'Yeni' Ordular" Özel Sayısı 2023'te ve "War and International System" Özel Sayısı 2024'te yayımlanmış olup, bu özel sayılardaki araştırma makaleleri de analize dâhil edilmiştir.

Tablo 2. Ciltlere Göre Ortalama Makale Sayıları

Cilt	Yıl	Cilt Sayısı	Makale Sayısı	Ortalama Makale
1–5	2005–2009	5	63	12,6
6–10	2010–2014	5	60	12,0
11–15	2015–2019	5	69	13,8
16-20	2020–2024	5	112	22,4

Tablo 3'te derginin ciltlere göre makalelerdeki yazar sayısı ve oranı yer almaktadır. Tüm ciltler bazında bakıldığında makalelerinin %76'sının tek yazarlı, %21,4'ünün iki yazarlı, %1,6'sının üç yazarlı ve %1'inin de dört veya daha fazla yazarlı makalelerden oluştuğu görülmektedir. Genel çerçevede Cilt 1-5'ten Cilt 16-20'ye doğru bakıldığında tek yazarlı makale oranının %88,9'dan %58,9'a ve dört ve üzeri yazarlı makale oranının ise %3,2'den %0,9'a gerilediği görülmekte iken; iki yazarlı makale oranı %6,3'ten %36,6'ya ve üç yazarlı makale oranının %1,6'dan %3,6'ya çıktığı tespit edilmektedir.

Tablo 3. Ciltlere Göre Yazar Sayıları ve Oranları

Yazar Sayısı	Ciltler 1–5	Ciltler 6–10	Ciltler 11–15	Ciltler 16–20	Toplam
1	56 (%88,9)	55 (%91,7)	54 (%78,3)	66 (%58,9)	231 (%76,0)
2	4 (%6,3)	5 (%8,3)	15 (%21,7)	41 (%36,6)	65 (%21,4)
3	1 (%1,6)	0 (%0,0)	0 (%0,0)	4 (%3,6)	5 (%1,6)
≥4	2 (%3,2)	0 (%0,0)	0 (%0,0)	1 (%0,9)	3 (%1,0)
Toplam	**63 (%100,0)**	**60 (%100,0)**	**69 (%100,0)**	**112 (%100,0)**	**304 (%100,0)**

Tablo 4'te cilt aralıklarına göre yazarların sivil-asker olarak dağılımı yer almaktadır.[35] Genel olarak bakıldığında, yazarlar arasında en büyük çoğunluğu %58,2 ile sivil yazarlar ve ardından %39,1 ile asker yazarlar oluşturmaktadır. Emekli asker oranı %1 ve hakkında bilgi bulunmayan yazarlar %1,6'dır.

Tablo 4. Ciltlere Göre Yazarların Sivil-Asker Dağılımı

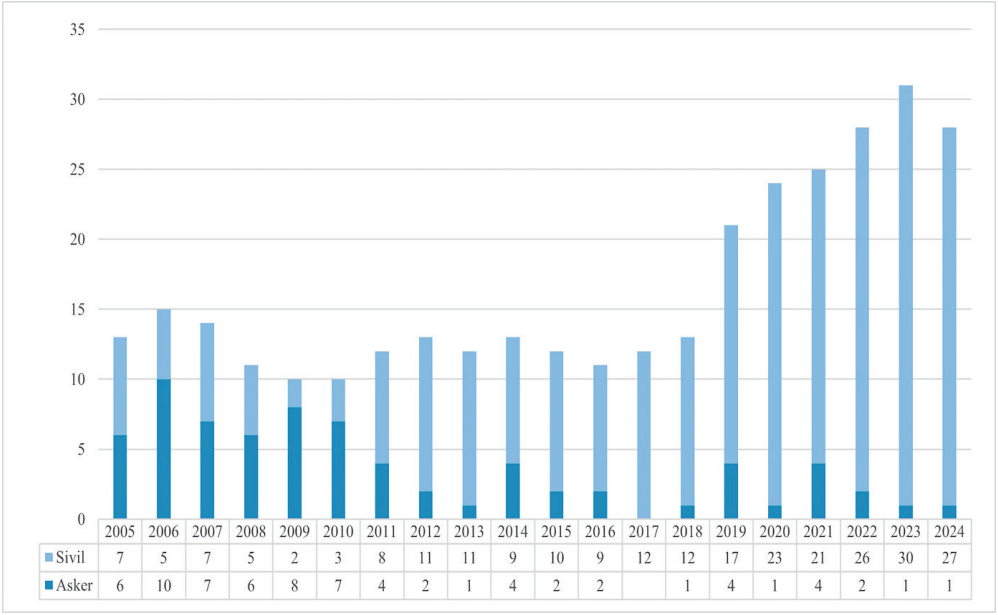
Yazar Grubu	Ciltler 1–5	Ciltler 6–10	Ciltler 11–15	Ciltler 16–20	Toplam
Asker	35 (%55,6)	25 (%41,7)	25 (%36,2)	34 (%30,4)	119 (%39,1)
Emekli Asker	1 (%1,6)	1 (%1,7)	1 (%1,4)	0 (%0,0)	3 (%1,0)
Sivil	25 (%39,7)	34 (%56,7)	43 (%62,3)	75 (%67,0)	177 (%58,2)
Bulunmuyor	2 (%3,2)	0 (%0,0)	0 (%0,0)	3 (%2,7)	5 (%1,6)
Toplam	**63 (%100,0)**	**60 (%100,0)**	**69 (%100,0)**	**112 (%100,0)**	**304 (%100,0)**

35 Yazarlar arasındaki sivil-asker dağılımına dair veriler, yayımlanan makalelerde yazarların kendi gönderdikleri özgeçmişler/makale künyeleri temel alınarak oluşturulmuştur.

Bu tabloda beş yıllık periyotlara bakıldığında ise, Cilt 1-5'ten Cilt 16-20 doğru geçen süreçte sivil yazar oranı %39,7'den %67'ye çıkmıştır. Özellikle Cilt 1-5 ve Cilt 6-10 sürecinde asker kökenli yazarların sayısı tüm yazar sayısının yaklaşık olarak yarısını oluşturmuştur. Cilt 11-15 ile Cilt 16-20 sürecinde ise bu oranda %30'lara kadar düşmüştür.

Birinci yazarlar açısından bakıldığında, 328 yazarın 73'ü (%22) asker unvanına sahiptir. Birinci yazarlar arasındaki sivil – asker dağılımına ait tablo Şekil 2'de gösterilmektedir. Grafikte, yıllara göre asker yazarların sayısında azalan bir eğim görülürken; 2011 yılında başlayan sivil yazar sayısının artışı 2019 yılı itibariyle hızlanmıştır.

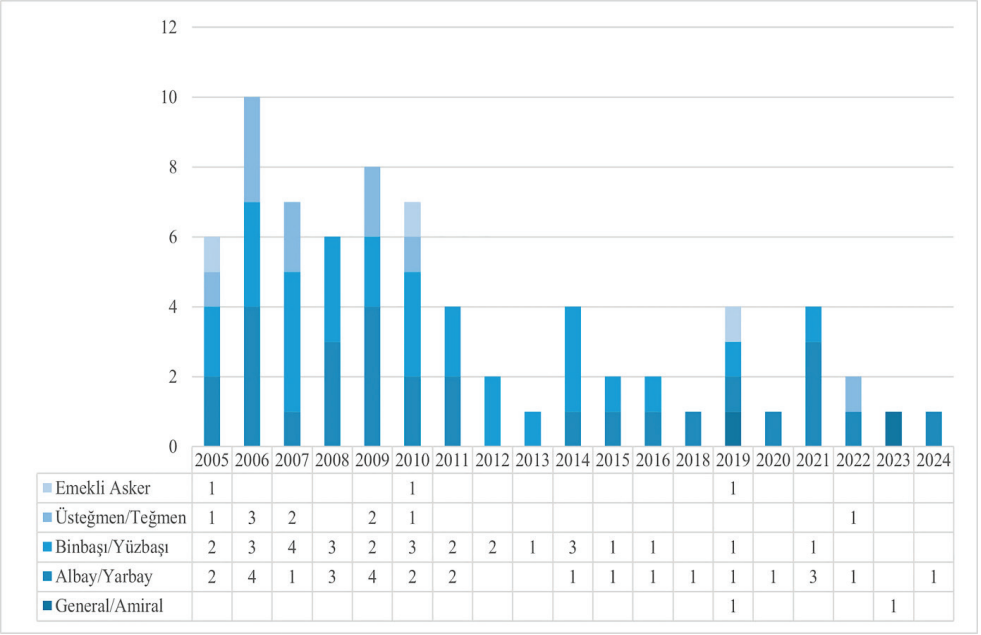
Şekil 2. Yıllara Göre Birinci Yazarlar Arasında Sivil – Asker Dağılımı



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
Sivil	7	5	7	5	2	3	8	11	11	9	10	9	12	12	17	23	21	26	30	27
Asker	6	10	7	6	8	7	4	2	1	4	2	2		1	4	1	4	2	1	1

Asker olan birinci yazarların rütbe dağılımına bakıldığında ise; General/Amiral rütbesindeki askerlerin oranının %3, Albay/Yarbay rütbesindeki askerlerin oranının %40, Binbaşı/Yüzbaşı rütbesindeki askerlerin oranının %40, Üsteğmen/Teğmen rütbesindeki askerlerin oranının %13 ve emekli askerlerin oranının %4 olduğu görülmektedir. Asker olan birinci yazarların rütbelerinin yıllara göre dağılımının Şekil 3'te gösterilmiştir. Yukarıdaki açıklamalara ve Şekil 2'deki grafiğe paralel olarak asker unvanlı yazarların sayısı yıllar içinde azalmaktadır.

Şekil 3. Yıllara Göre Asker Olan Birinci Yazarlar Arasında Rütbe Dağılımı

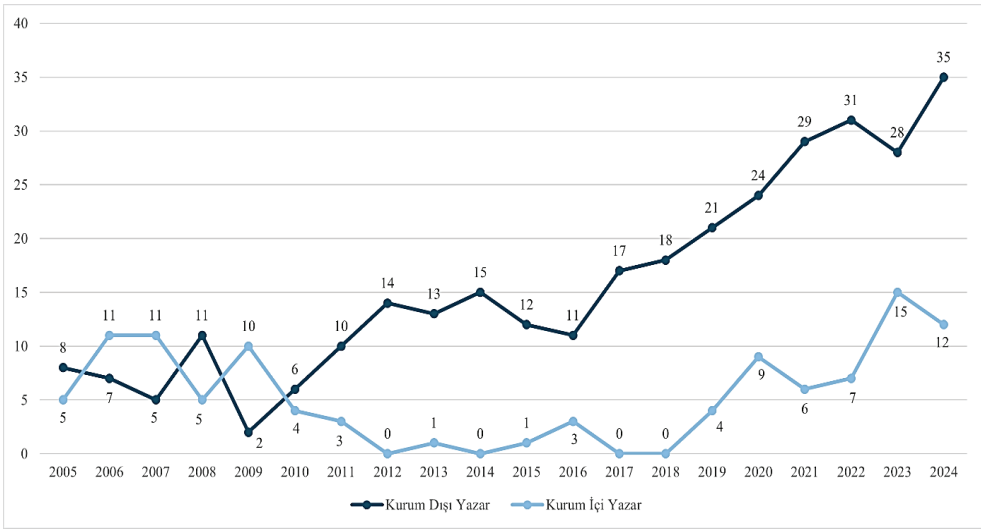


	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2018	2019	2020	2021	2022	2023	2024
Emekli Asker	1					1								1					
Üsteğmen/Teğmen	1	3	2		2	1											1		
Binbaşı/Yüzbaşı	2	3	4	3	2	3	2	2	1	3	1	1		1		1			
Albay/Yarbay	2	4	1	3	4	2	2			1	1	1	1	1	1	3	1		1
General/Amiral														1				1	

Şekil 4'te tüm yazarlar arasında kurum içi[36] ve kurum dışı yazarların sayılarının karşılaştırması yer almaktadır. Özellikle 2006 ve 2007'de kurum içi yazarların oranı tüm yazarlar arasında sırasıyla %61 ve %69 olmuş, 2009 yılında ise %83 ile zirveye ulaşmıştır. Ancak bu tarihten sonra kurum dışından makalesi yayınlanan yazarların oranında hızlı bir artış görülmektedir ki özellikle 2012, 2014, 2017 ve 2018 yıllarında dergideki makalelerin tamamı kurum dışı yazarların makaleleri olmuştur. Son beş yıllık periyoda bakıldığında ise kurum içi yazarların tüm yazarlara oranı yaklaşık olarak %23 düzeyinde kalırken, kurum içi yazar oranının 2023 yılında %35 gibi nispeten yüksek bir orana çıktığı görülmüştür. 2023 yılında bu oranın yüksek çıkmasının nedeni, söz konusu yıldaki özel sayının MSÜ ATASAREN akademisyenlerince hazırlanan "'Yeni' Savaşlar ve 'Yeni' Ordular" başlıklı özel sayı olmasıdır.

36 Kurum içi olarak kodlanan kurumlar şunlardır: HAK SAREN, HAK ve bağlısı Kara, Deniz, Hava ve Müşterek Harp Akademileri, MSÜ ATASAREN, MSÜ Rektörlüğü ve bağlısı MSÜ Kara, Deniz, Hava ve Müşterek Harp Akademileri, Kara, Deniz ve Hava Harp Okulları, Kara, Deniz ve Hava Meslek Yüksekokulları.

Şekil 4. Yıllara Göre Kurum İçi ve Kurum Dışı Tüm Yazarların Dağılımı



Yıllara göre yayımlanan araştırma makalelerinin sayısı Şekil 5'te trend eğilimi olarak yer almaktadır.

Şekil 5. Yıllara Göre Yayımlanan Makale Sayılarının Dağılımı

Dergiye gönderilen makaleler Türkçenin yanı sıra İngilizce, Almanca ve Fransızca olarak da kabul edilmektedir. Dergide 2005-2024 yılları arasında toplamda 328 araştırma makalesi yayım dili dağılımı açısından incelendiğinde, Türkçe makalelerin sayısının 268 (%82) ve diğer dillerdeki makalelerin sayısının 60 (%18) (1 Almanca + 59 İngilizce) olduğu görülmektedir. Dergide 2011'de başlayan uluslararasılaşma sürecinde Türkçe dışındaki dillerden de makale yayımlanmaya başlanmış; bu dönemden sonra özellikle 2014 yılına

dek İngilizce yazılmış araştırma makalelerinin sayısında hızlı bir artış görülmüştür. Ancak yine de diğer dillerde ve özellikle de İngilizce yazılmış araştırma makalelerinin nispeten az olduğu söylenebilir.

Dergide yayımlanan 328 makaleye katkıda bulunan 422 yazarın sadece %3'ünün yabancı uyruklu yazarlardan oluştuğu görülmektedir:[37] Çin Halk Cumhuriyeti'nden dört yazarın yanı sıra, ABD, Almanya, Gürcistan, İran, İtalya, Mısır, Nijerya, Pakistan, Sudan ve Suudi Arabistan'dan birer yazarın çalışmaları dergide yayımlanmıştır. Yabancı uyruklu yazarların yıllara göre dağılımına bakıldığında, 2011-2013 yılları arasında belirgin bir artış ve çeşitlilik görünmektedir. Buradaki artışın ilgili dönemde derginin aldığı yayın politikası ve uluslararasılaşma sürecine uyum sağlama çabalarından kaynaklandığı düşünülmektedir. Dergi Kuruluna uluslararası alanda yetkin akademisyenlerin dahil olması bu sebeple önem taşımaktadır. Ancak 2014 yılı ve sonrasında yabancı uyruklu yazarların sayısında bir azalma meydana gelmiştir. 2017'de iki, 2019'da bir, 2023'te bir ve 2024'te bir yabancı uyruklu yazarın makalesi yayımlanmıştır.

Dergide yazarların makale yayımlama sıklığına bakıldığında, Tablo 5'teki veriler elde edilmektedir. Tüm yazarlardan (422 yazardan) 301'inin (%86'sının) birer makaleyle ve 35'inin (%10'unun) iki makaleyle dergiye katkıda bulunduğu görülmektedir. Birinci yazar olarak dergide makalesi yayınlananlar (328 yazar) arasında da benzer bir dağılım ortaya çıkmaktadır. Birinci yazarlar arasında 238 yazarın (%87) birer makalesi ve 27 yazarın (%10) ikişer makalesi dergide yayımlanmıştır. Bununla birlikte, tüm yazarlar arasında dergide üç makalesi yayınlanan yazarların oranı %3'ü, dört veya daha fazla makalesi yayımlanan yazarların oranı ise %1'i geçmemektedir.

Tablo 5. Yazarların Makale Yayımlama Sıklığı

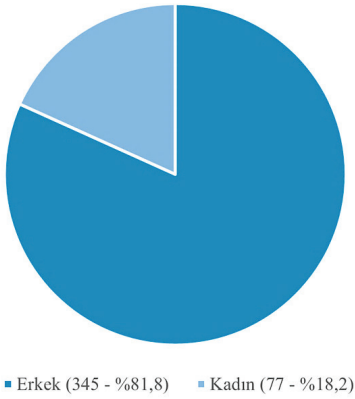
TÜM YAZARLAR		BİRİNCİ YAZARLAR	
Yazar Sayısı	**Makale Sayısı**	**Yazar Sayısı**	**Makale Sayısı**
1	6	1	6
2	5	1	5
2	4	1	4
9	3	7	3
35	1	27	2
301	1	238	1

Şekil 6'da dergide araştırma makaleleri yayımlanan toplam 422 yazarın cinsiyet dağılımı verilmiştir.[38] Tüm yazarlar arasında 345 erkek yazar ve 77 kadın yazar bulunmaktadır.

37 Yazarların uyruk bilgisi, makale gönderim sürecinde dergiye iletilen özgeçmiş/makale künyesi bilgilerinden hareketle doğrulanmış; eksik veya belirsiz durumlarda ise YÖK Akademik, ORCID ve araştırmacıların çalıştığı kurumların web sayfaları gibi açık erişim kaynaklarda yapılan taramalarla tamamlanmıştır. Dolayısıyla, veriler yazarların kendileri tarafından sağlanan bilgiler ile çevrimiçi açık kaynaklardan elde edilen kayıtların karşılaştırılması sonucunda oluşturulmuştur.

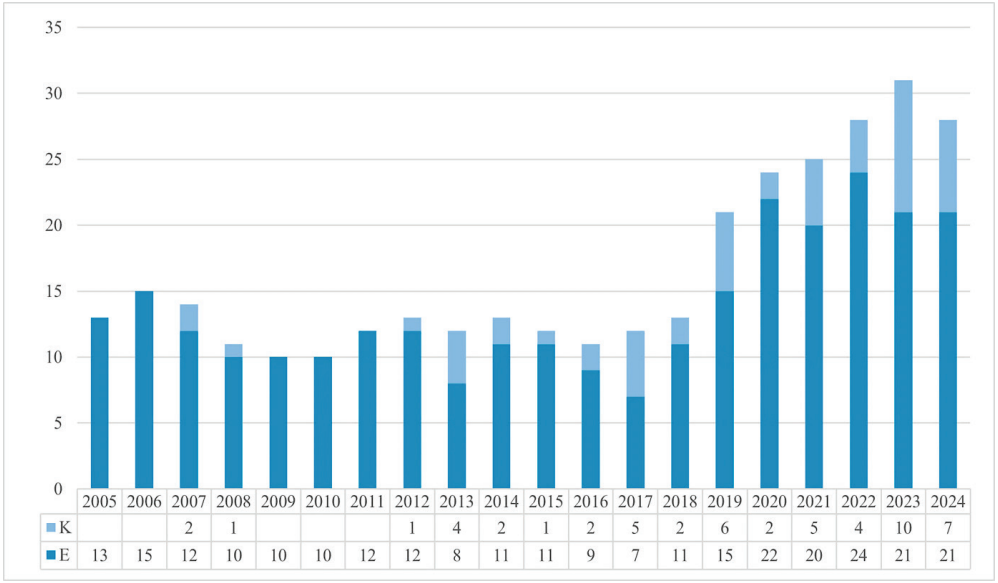
38 Yazarların cinsiyet bilgilerinin belirlenmesi için yukarıda yazarların uyruk bilgilerinin belirlenmesinde kullanılan yönteme başvurulmuş; makale künyesinde verilen bilgilerden doğrulanmış, bunların eksik olması durumunda ise yine yukarıda belirtilen çevrimiçi açık kaynaklara başvurulmuştur.

Şekil 6. Tüm Yazarların Cinsiyet Dağılımı



Yazarların birinci yazar olduğu durumda cinsiyet dağılımını gösteren Şekil 7'deki grafikte, birinci yazarı kadın olan makalelerin %16 (toplamda 328 makalede 54 kadın yazar) olduğu görülmektedir. Dergi istatistiklerine bakıldığında ilk sekiz yılda toplam 98 birinci yazar arasından sadece dördünün kadın olduğu tespit edilmiştir. Bu dağılımın 2013 sonrasında değişim gösterdiğini söylemek mümkündür ve kadın yazar sayısında bir artış görülmektedir. Özellikle son iki yılda birinci yazarlar arasında kadın yazar oranının sırasıyla %32'ye (2023) ve %25'e (2024) ulaşmış olması dikkat çekmektedir.

Şekil 7. Yıllara Göre Birinci Yazarların Cinsiyet Dağılımı



	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2022	2023	2024
K			2	1				1	4	2	1	2	5	2	6	2	5	4	10	7
E	13	15	12	10	10	10	12	12	8	11	11	9	7	11	15	22	20	24	21	21

Tablo 6'da derginin cinsiyetlere göre akademik unvan sayıları ve oranları yer almaktadır. Makalesi yayınlanan yazarların unvanına bakıldığında Dr. Öğr. Üyesi unvanı erkek yazarlarda %25,7 oranıyla, kadın yazarlarda %31,5 oranıyla ilk sırada almaktadır. En az makalesi yayımlanmış olan unvanlara bakıldığında, erkek yazarlarda %0,4 ile Arş. Gör Dr. unvanı, kadın yazarlarda ise %0,8 ile Öğr. Gör Dr. unvanı son sırada yer almaktadır. Makalesi yayınlanan yazarların cinsiyet bazında sayısına bakıldığında ise, (makale künyelerinde

unvanlarına dair bilgi bulunmayanlar hariç) 456 erkek ve 122 kadın yazar bulunmaktadır. Bununla birlikte, toplam içindeki oranlarına bakıldığında Öğr. Gör. Dr. unvanında kadın erkek oranları eşit iken, (Dr. ve Lisansüstü Öğrenci olarak makalesi yayınlanan yazarlar dışında) diğer tüm unvanlarda kadınların temsiliyetinin erkeklere göre daha yüksek olduğu tespit edilmiştir. Buna ek olarak, Öğretim Üyesi sınıfında (Prof., Doç., Dr. Öğr. Üyesi) bulunan akademisyenler arasında da kadın yazarların oranının erkek yazarlara oranla daha yüksek olduğu görülmektedir. Kadın yazarların sayısı erkeklere göre daha düşük olmakla birlikte, kadınların akademik unvan dağılımı görece daha yüksektir. Nitekim kadın yazarların %54,9'u öğretim üyesi (Prof. Dr., Doç. Dr., Dr. Öğr. Üyesi) iken, bu oran erkek yazarlarda %42,9'dur. Dolayısıyla kadın yazarların sayısı toplamda daha az olsa bile makalesi yayımlanan kadınların önemli bir kısmı daha yüksek akademik unvana sahiptir.

Tablo 6. Yazarların Akademik Unvan Dağılımı

Unvan	Erkek	Kadın	Erkek Dağılımı (%)	Kadın Dağılımı (%)
Prof. Dr.	35	9	6,9	7,3
Doç. Dr.	52	20	10,3	16,1
Dr. Öğr. Üyesi	130	39	25,7	31,5
Arş. Gör. Dr.	2	5	0,4	4,0
Öğr. Gör. Dr.	4	1	0,8	0,8
Dr.	104	8	20,6	6,5
Arş. Gör.	17	10	3,4	8,1
Öğr. Gör.	4	3	0,8	2,4
Lisansüstü Öğrencisi	97	23	19,2	18,5
Bağımsız Araştırmacı	11	4	2,2	3,2
Bilgi Bulunmuyor	50	2	9,9	1,6
Toplam	**506**	**124**	**100,0**	**100,0**

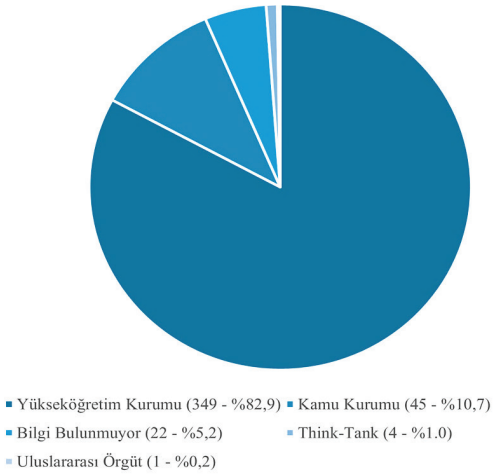
GSD'de makale yayımlayan yazarların bağlı oldukları kurumların dağılımı Şekil 8'deki grafikte verilmiştir. Grafikte de görüldüğü gibi, %82,9 ile en fazla makale yayımı Yükseköğretim Kurumlarında çalışan araştırmacılardan gelmektedir. Yükseköğretim Kurumları başlığı altında devlet üniversiteleri, vakıf üniversiteleri ve güvenlik odaklı kamu yükseköğretim kurumları[39] dâhil edilmiştir. Ardından %10,7 ile Kamu Kurumları (Bakanlıklar, Başkanlıklar vb.),[40] %1 ile Think-Tank (Araştırma Merkezleri ve Bağımsız Düşünce Kuruluşları), %0,2 ile Uluslararası Örgütler (NATO, BM vb.) gelmektedir. Temsil ettiği kurum bilgisi bulunmayan yazar[41] oranı ise %5,2 şeklindedir.

39 Güvenlik odaklı kamu yükseköğretim kurumları şunlardır: HAK SAREN, MSÜ ATASAREN ve MSÜ bağlısı okullar (Harp Enstitüleri, Harp Okulları ve Astsubay Meslek Yüksekokulları), Jandarma ve Sahil Güvenlik Akademisi ve Polis Akademisi.

40 Kamu kurumlarına, Emniyet Genel Müdürlüğü, Genelkurmay Başkanlığı, Millî Savunma Bakanlığı ve bağlısı kuvvet komutanlıkları da dâhil edilmiştir.

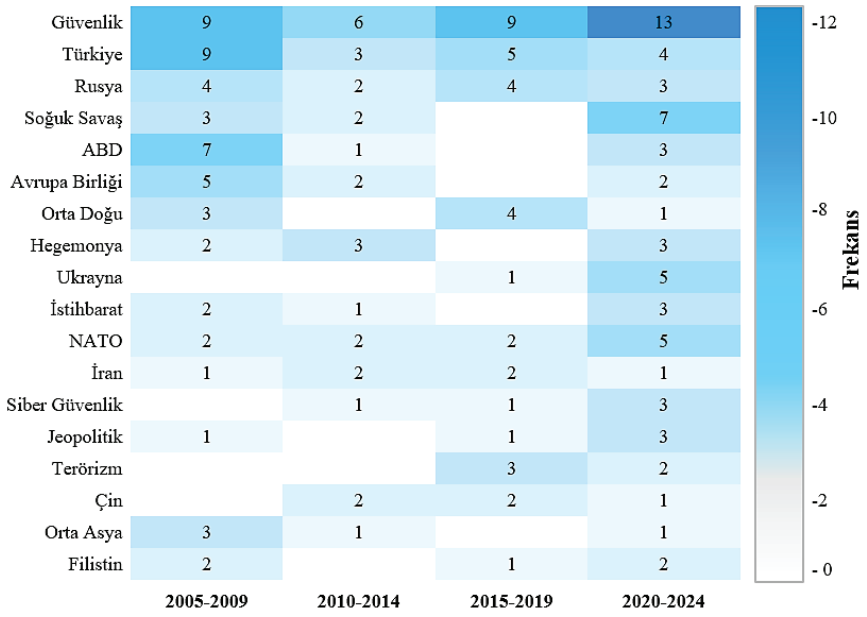
41 Kurum bilgisi gönderilen makalede yer almayan ve çevrimiçi açık kaynaklardan yapılan araştırmalar sonucu kurum bilgisine ulaşılamayan yazarlar "Bilgi Bulunmuyor" şeklinde kodlanmıştır.

Şekil 8. Yazarların Kurum Dağılımı



Şekil 9'da yer alan ısı/yoğunluk haritasında, dergide beş yıllık periyotlara göre en sık karşılaşılan yirmi anahtar kelime yer almaktadır. Sağ tarafta yer alan çubuk en sık yer alan 18 kelimenin sıklığına göre 0'dan 12' ye kadar renklerle temsil edilmektedir. Açık renk az kullanılan anahtar kelimeleri gösterirken; koyu renk daha sık kullanılan anahtar kelimeleri göstermektedir. Beşer yıllık periyotlara ayrılan veri setinde 2005-2009 yılları arasında sırasıyla Güvenlik, Türkiye, ABD, ve Avrupa Birliği anahtar kelimeleri yer alırken; 2010-2014 yılları arasında sırasıyla Güvenlik, Türkiye, Hegemonya anahtar kelimeleri; 2015-2019 yılları arasında sırasıyla Güvenlik, Türkiye, Rusya ve Orta Doğu anahtar kelimeleri ve 2020-2024 yılları arasında sırasıyla Güvenlik, Soğuk Savaş, Ukrayna ve NATO anahtar kelimeleri yer almaktadır.

Şekil 9. Beş Yıllık Periyotlara Göre En Sık Kullanılan Yirmi Anahtar Kelime



Son olarak Güvenlik Stratejileri Dergisi'ne yayımlanmış makalelere yapılan atıflara, TRDizin, SOBİAD Atıf Dizini ve Google Akademik üzerinden yapılan aramalarla ulaşılmıştır. Ulaşılan sonuçlar Tablo 7'de sunulmuştur. Kapsamını ilgili konu alanlarındaki uzmanların oluşturduğu komiteler tarafından seçilen ulusal bilimsel dergilerin oluşturduğu TRDizin'de *GSD*'de yayımlanan makalelerden 183'üne atıf yapıldığı ve derginin aldığı toplam atıf sayısının 575 olduğu görülmektedir.[42] Daha geniş kapsama sahip olan SOBİAD Atıf Dizininde atıf dizininde ise *GSD*'de yayımlanmış makalelerden 222'sine toplam 1831 atıf aldığı görünmektedir.[43] Atıf taramasında kapsamı genişletmek amacıyla Harzing's Publish or Perish[44] uygulaması aracılığıyla Google Akademik üzerinden bir tarama gerçekleştirilmiştir ve bu taramaya göre *GSD*'nin 282 makalesi toplam 3521 atıf almıştır. Bu atıf tarama kaynaklarının her birinde en çok atıf aldığı tespit edilen makaleler aşağıdaki tabloda bir arada verilmiştir.

Tablo 7. En Çok Atıf Alan Makaleler

Makale Başlığı	TRDizin'de Atıf Sayısı	SOBİAD Atıf Dizini'nde Atıf Sayısı	Google Akademik'te Atıf Sayısı
Kopenhag Okulu ve Güvenlikleştirme Teorisi	35	127	171
Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı	16	52	108
Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler	13	57	79
Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye'de DAEŞ ve YPG Örneği	13	36	70
Kimlik ve Güvenlik İlişkisine Konstruktivist Bir Yaklaşım: "Kimliğin Güvenliği" ve "Güvenliğin Kimliği"	13	44	71
Terör-Medya İlişkisi ve Medyada Terör Haberciliği	18	–	58
Türkiye'nin Suriye'nin Kuzeyindeki Askerî Harekâtının Amaçları ve Sonuçları	–	45	61
Soğuk Savaş Sonrası Uluslararası Sistem: Yeni Sürecin Adı "Koalisyonlar Dönemi mi?"	–	50	95
Modern Öncesi Devletin Yönetim Anlayışı	–	46	72
Doğu Akdeniz'de Değişen Enerji Jeopolitiği ve Türkiye	–	43	54
Doğu Akdeniz'de Deniz Yetki Alanlarının Sınırlandırılmasında Libya'nın Rolü ve Etkisi	10	–	–
Sömürge Devletlerinin Kullandığı Sömürgecilik Araç ve Metotları Vaka Analizi: Belçika Krallığı'nın Kongo'daki Sömürge Dönemi	10	–	–
Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım: Galler Ekolü	9	–	–
Dağlık Karabağ Sorununda Azerbaycan Tarafından Kuvvet Kullanım Olasılığının Analizi	9	–	–
Truman Doktrini Üzerine Bir Analiz	–	43	–

42 TRDizin, https://search.trdizin.gov.tr/tr/dergi/detay/532/guvenlik-stratejileri-dergisi, erişim 15.07.2025.
43 SOBIAD Atıf Dizini, https://atif.sobiad.com/index.jsp?modul=journals-detail&ID=wlSbVIMBYqxAIGX2zNeO, erişim 15.07.2025.
44 Harzing, A.W. (2007) *Publish or Perish*, https://harzing.com/resources/publish-or-perish üzerinden indirilen uygulama ile 15 Temmuz 2025 tarihinde yapılan tarama.

Değerlendirme ve Sonuç

Güvenlik Stratejileri Dergisi (*GSD*), 2005 yılında yayın hayatına başlamasından bu yana Türkiye'de güvenlik çalışmaları alanında önemli bir akademik platform haline gelmiştir. Yirmi yıllık süreçte derginin hem editörlük yapısı hem de yazar profili dikkate değer bir dönüşüm geçirmiştir. Bu çalışmada, *GSD*'de 2005 ile 2024 yılları arasındaki 20 yıllık dönemde yayımlanmış araştırma makalelerinin bibliyometrik ve istatistiksel analizi gerçekleştirilerek derginin mevcut durumu incelenmiştir ve bu başlık altında elde edilen bulgular yorumlanarak derginin gelecek perspektifine yönelik öneriler geliştirilmeye çalışılacaktır.

Yayımlanan çalışma türlerinin dağılımında dikkat çeken husus, kitap incelemelerinin/tanıtımlarının 2011-2015 yılları arasında yoğunlaşması olmuştur. Söz konusu dönemin dergi editörleri, enstitünün lisansüstü programlarındaki öğrencilerin çalışmalarını teşvik etmek ve alandaki önemli kitaplara dikkat çekmek amacıyla kitap incelemelerine ve tanıtımlarına özel bir önem verdiklerini belirtmişlerdir.[45] Ancak 2016'dan sonraki sayılarda bu türden yayınların devam etmediği görülmektedir ki, bunun nedeninin dergi editörlüklerinde yaşanan değişime bağlı olabileceği değerlendirilmektedir.

Ciltlere göre yayımlanan ortalama makale sayılarına bakıldığında, beşer yıllık periyotların ilk üçünde cilt başına makale sayısı 12,6 ile 13,8 arasında iken, son beş yıllık periyot olan 2019-2024 yılları arasında cilt başına makale sayısının 26,16 yükseldiği yani iki katına çıktığı görülmektedir. Daha önce de işaret edildiği gibi, 2005-2018 yılları arasında yılda iki sayı yayımlanan dergi, 2019 yılından itibaren yılda toplam dörder sayı olarak yayımlanmaktadır. Cilt içi dergi sayılarındaki artışla birlikte, cilt ve sayı başına düşen ortalama makale sayısının yükselmesi, dergiye makale arzının artığının bir göstergesi olarak görülebilir.

Dergide ciltlere göre makale yazarlarının sayılarına ve oranlarına bakıldığında, genel eğilimin şu şekilde olduğu tespit edilmektedir: Süreç içinde tek yazarlı makaleler ile dört ve üzeri yazarlı makalelerin sayısında bir düşüş; iki ve üç yazarlı makalelerde ise bir artış yaşanmıştır. Ancak tüm ciltler bazında genel ortalamaya bakıldığında yayımlanan makalelerin %76'sının tek yazarlı ve %21'inin iki yazarlı olduğu görülmektedir. Bu veri, Çokişler'in *Uluslararası İlişkiler* Dergisi'ne yönelik bibliyometrik analizindeki[46] ve Mehmetçik ve Hakses'in[47] Türkiye'deki anaakım Uluslararası İlişkiler disiplini dergileri üzerine yaptıkları bibliyometrik çalışmalarındaki yazar oranlarıyla paralellik göstermektedir.

Çalışmada ayrıca tüm yazarlar arasında ve birinci yazarlar arasında sivil-asker dağılımı ve asker olan birinci yazarlar arasında rütbe dağılımı incelenmiştir. Beş yıllık periyodlarda toplam yazarlar arasında asker kökenli yazar sayısının düşüşte olduğu ve sivil kökenli yazar sayısının katlanarak arttığı tespit edilmiştir. Özellikle 2011 yılından itibaren sivil yazar sayısının arttığı ve 2019 yılından sonra da bu artışın hızlandığı görülmektedir. İlk beş yıllık periyod olan 2005-2009 yılları arasında yazarların genellikle kurumda asker akademisyenler ile (çoğunluğu yine asker olan) lisansüstü öğrencileri olduğu tespit edilmiştir. Literatürde de akademik dergilerin ilk yıllarında tanınırlıklarının çoğunlukla yayımlandıkları kurum

45 Dönemin editörleriyle yapılan görüşmeler.

46 Çokişler, *Uluslararası İlişkiler* Dergisi'ndeki tek yazarlı makalelerin oranını %77,9 ve iki yazarlı makalelerin oranını %17,4 olarak tespit etmiştir. Elvan Çokişler, "Uluslararası İlişkiler Dergisinin Bibliyometrik Analizi (2004-2017)", *Uluslararası İlişkiler*, 16:64, 2019, 46.

47 Mehmetçik ve Hakses karşılaştırmalı olarak inceledikleri *Uluslararası İlişkiler*, *All Azimuth* ve *Insight Turkey* dergilerinde tek yazarlı makalelerin oranını %81,6 ve iki yazarlı makalelerin oranını %13 olarak bulmuşlardır. Hakan Mehmetcik ve Hasan Hakses, "Turkish IR Journals through a Bibliometric Lens", *All Azimuth: A Journal of Foreign Policy and Peace*, 12:1, 2023, 67.

ile sınırlı kalmasının doğal olduğuna işaret eden çalışmalar mevcuttur.[48] Ancak bu eğilimin 2011 yılından sonra değiştiği ve sivil kökenli yazarların sayısının hızla arttığı görülmektedir. Bu artışta zaman içinde üç farklı unsurun etkili olduğu değerlendirilmektedir: Birincisi, dergi 2011 yılında uluslararasılaşmaya giderek yazar havuzunu çeşitlendirmeyi başarmıştır. İkincisi, 2016'dan sonra bütün güvenlik odaklı kamu yükseköğretim kurumlarında olduğu gibi, yeni kurulan Millî Savunma Üniversitesi bünyesinde de (HAK ve HAK SAREN'den farklı olarak) asker kökenli akademisyenlerin yanı sıra sivil akademisyenler de çalışmaya başlamıştır. Üçüncüsü ise, giriş bölümünde de belirtildiği gibi güvenlik çalışmaları alanında 2010'ların başından itibaren güvenlik çalışmaları alanına sadece askerî kurumlar değil, diğer kamu kuruluşları, üniversiteler ve araştırma merkezleri de katkı sağlamaya başlamıştır ki bu artan ilgi zaman içinde, bulguların da gösterdiği gibi, dergideki sivil yazar sayısında da artışı beraberinde getirmiştir.

Çalışma, *GSD*'nin yayın politikalarında ve editoryal süreçlerinde zaman içinde yaşanan değişimlerin derginin uluslararasılaşma çabalarına yansıdığını göstermektedir. Özellikle 2011-2013 döneminde yabancı yazar oranında ve İngilizce yayın sayısında belirgin bir artış sağlanmış, ancak sonraki yıllarda bu artış sürekli kılınamamıştır. Dergideki makalelerin yalnızca %18'inin Türkçe dışındaki dillerde yayımlanmış olması, derginin SSCI ve Scopus gibi uluslararası dizinlerde yer alabilmesi için dil çeşitliliğinin artırılmasının önemini ortaya koymaktadır. Her ne kadar dil çeşitliliği, uluslararası dizinlerde kabul edilmek için tek başına zorunlu bir kriter olmasa da özellikle sosyal bilimlerde uluslararası görünürlüğü ve atıf alabilirliği artıran temel faktörlerden biridir. Türkiye çıkışlı dergilerden Türkçe yayın yaptığı dönemde bu dizinlere girmiş dergi örneği de literatürde mevcuttur.[49] Bununla birlikte, İngilizce dilinde yazılmış makale sayısındaki artışın tamamlayıcı bir strateji olabileceği ve derginin hâlen taranmakta olduğu (Directory of Open Access Journals -DOAJ- ve Central and Eastern European Online Library -CEEOL- gibi) diğer alan indeksleri üzerinden görünürlüğünü, yazar havuzunu ve atıf potansiyelini artırabileceği değerlendirilmektedir. Tabii ki uluslararası dizinlere girebilmek için çeşitli kalite kriterlerinin yanı sıra, karşılaştırmalı atıf analizi, yazar atıf analizi, editör kurulu atıf analizi ve içerik önemi gibi dört önemli etki kriterinde de karşılanması gerekmektedir. Derginin söz konusu atıf analizlerinde gerekli etki kriterine ulaşması için de yeni yayın stratejileri geliştirmesi gerektiği açıktır.

Dergide kadın yazar oranının tüm yazarlar arasında %18 ve birinci yazarlar arasında %16 gibi düşük bir seviyede kaldığı görülmektedir. Ancak kadın yazarların yıllara göre dağılımına bakıldığında, ilk sekiz yıldaki toplam 98 birinci yazar arasında sadece dördünün kadın yazar olduğunu tespit edilmiştir ki, bu da 20 yıllık oranlara bakıldığında kadın yazar oranının düşük çıkmasında etkili olmuştur. Kadın yazarların sayısı 2013 yılından sonra artış gösterirken, özellikle son iki yılla ilgili dikkat çekici veri elde edilmiştir: *GSD*'de makalesi yayınlanan birinci yazarlar arasında kadın akademisyenlerin oranı 2023 yılında %32'ye ve 2024 yılında %25'e ulaşmıştır. Alan geneliyle karşılaştırma yapmak amacıyla YÖK Akademik üzerinden akademisyenlerin cinsiyet dağılımına bakılmış; Uluslararası Güvenlik alt disiplininde 436 akademisyen arasındaki kadın akademisyen sayısı 137 (%31) olarak ve

48 Aileen Fyfe, Kelly Coate, Stephen Curry, Stuart Lawson, Noah Moxham ve Camilla Mørk Røstvik, *Untangling Academic Publishing: A History of the Relationship between Commercial Interests, Academic Prestige and the Circulation of Research*, University of St Andrews, St. Andrews, 2017.

49 Türkçe yayın yaptığı dönemde SSCI'a kabul edilen *Uluslararası İlişkiler* Dergisi örneği, dil faktörünün tek başına belirleyici olmadığını göstermektedir. Ancak söz konusu derginin uzun yıllar boyunca alanda yüksek atıf alan öncü bir yayın olmasının, güçlü uluslararası editörlerce desteklenmesinin ve Türkiye'deki Uluslararası İlişkiler camiasında referans dergi konumunda bulunmasının da derginin SSCI'a kabul edilmesinde belirleyici bir etken olduğu da bir gerçektir.

çok daha yeni bir alan olan Güvenlik Çalışmaları alt disiplinindeki 56 akademisyen arasında kadın sayısı altı (%11) olarak tespit edilmiştir.[50] Bu rakamlar, bizzat güvenlik alanında da halihazırda cinsiyetler arası eşit bir dağılımının uzağında olduğumuzu göstermektedir. Yine de *GSD*'de son iki yılda ulaşılan kadın yazar oranının uluslararası güvenlik alt disiplinindeki %31'lik kadın akademisyen oranına yaklaştığını vurgulamak gerekmektedir. Bu oranın önümüzdeki yıllarda da korunması ve cinsiyetler arası dengeli bir dağılımın sağlanması için çeşitli adımlar atılması yerinde olacaktır. Bu bağlamda uluslararası ve ulusal düzeyde güvenlik çalışmalarıyla ilgilenen kadın akademisyen girişimleriyle bağlantıya geçilmesi, bu girişimlerden destek alınması ve ortaklaşa özel sayılar hazırlanması, kadın yazar sayısının artırılması için yeni bir strateji olarak düşünülebilir.

Anahtar kelime analizinde, anahtar kelime çeşitliliğinin sınırlı kaldığı tespit edilmiştir. Kemikleşmiş bazı anahtar kelimeler çerçevesinde yoğunlaşan makalelerin dergide düzenli olarak yer alsa da dönemsel/konjektürel gelişmelerin etkisinin de makalelere yansıyabildiği görülmektedir. Özellikle son beş yıllık periyotta Ukrayna, NATO ve Soğuk Savaş anahtar kelimelerindeki belirgin artış, güncel gelişmelerin dergide yayımlanan makaleleri etkilemekte olduğunun işaretidir. Tüm beş yıllık periyotlarda derginin hem adına hem de yayın ilkelerine uygun olarak Güvenlik ve Türkiye anahtar kelimeleri en çok tercih edilen anahtar kelimelerdir. Yine tüm beş yıllık periyotlarda kendini gösteren bir başka ortak nokta, anahtar kelimelerin ağırlıklı ülke/bölge (Türkiye, Rusya, ABD, Orta Doğu, Ukrayna, İran vb.) odaklı olması, bununla birlikte tematik (siber güvenlik, istihbarat, terörizm vb) anahtar kelimelerin nispeten daha az kalmasıdır. Anahtar kelime yoğunluklarına bakıldığında özellikle son beş yıllık periyotta çeşitliliğin arttığı görünmesine rağmen, dergide yayımlanan makalelerin hâlâ büyük oranda klasik güvenlik anlayışı odaklı olarak realist güvenlik perspektifi içinde kaldığı görülmektedir. Bununla birlikte, derginin yeni ve eleştirel güvenlik bakış açılarını tamamen dışladığını söylemek mümkün değildir, çünkü dergide eleştirel güvenliğe dair makaleler de farklı yıllarda ve farklı sayılarda kendilerine yer bulmaktadır.[51]

---

50 YÖK Akademik, Yükseköğretim Akademik Arama sayfası, https://akademik.yok.gov.tr/AkademikArama/, erişim 21.09.2025. Uluslararası Güvenlik ve Güvenlik Çalışmaları alt disiplininde cinsiyetler arası dağılımının eşit olmamasına karşın, yükseköğretim kurumlarında akademisyenlerin cinsiyet dağılımına bakıldığında dengeli dağılımına yaklaşıldığı görülmektedir. Yükseköğretim Kurumu (YÖK) istatistiki verilerine göre, 2024-2025 öğretim yılında kadın akademisyen sayısı 86.607 (%46,8)' dir. Bu da 2013-2014 öğretim yılındaki 60.903 (%42,8) olan kadın akademisyen sayısıyla karşılaştırıldığında son on yılda %42,15'lik bir artış yaşandığını göstermektedir. Yüksek Öğretim Bilgi Yönetimi Sistemi, https://istatistik.yok.gov.tr/, erişim 24.09.2025. YÖK istatistiki verilerinde akademisyenlerin akademik görevlerine ve görevli bulundukları programlara dair bilgiler ve YÖK Akademik'te geçerli arama tarihinde bir yükseköğretim kurumunda aktif olarak çalışan akademisyenlerin temel çalışma alanlarına dair bilgiler yer almaktadır. Dolayısıyla güvenlik çalışmaları alanındaki akademisyenlerde yıllara göre cinsiyet oranı değişiminin nasıl bir değişiklik gösterdiği tespit edilememiştir. Bu değişimin yükseköğretim kurumlarındaki genel değişim çizgisini takip etmiş olabileceği düşünülse de ileride yapılacak çalışmalarda Türkiye'deki güvenlik çalışmaları alanıyla ilgili bu veri boşluğu doldurulabilir.

51 Söz konusu makalelerden bazıları için bkz: Helin Sarı Ertem, "Kimlik ve Güvenlik İlişkisine Konstrüktivist Bir Yaklaşım: 'Kimliğin Güvenliği' ve 'Güvenliğin Kimliği'", *Güvenlik Stratejileri Dergisi*, 8:16, 2012, s. 177-236; Fikret Birdişli, "Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım: Galler Ekolü", *Güvenlik Stratejileri Dergisi*, 10:20, 2014, s. 229-256; Bülent Sarper Ağır, "Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı", *Güvenlik Stratejileri Dergisi*, 11:22, 2015, s. 97-130; Özlem Özdemir ve Emrah Özdemir, "Suriyeli Mülteci Kadınlar ve İnsani Güvenlik", *Güvenlik Stratejileri Dergisi*, 14:27, 2018, s. 113-145; Helin Sarı Ertem ve Aslı Nur Düzgün, "Uluslararası İlişkiler Disiplininde Ontolojik Güvenlik Teorisi: Kavram ve Literatür Odaklı Bir İnceleme", *Güvenlik Stratejileri Dergisi*, 17:37, 2021, s. 39-83; Hatice Demirci ve Güngör Şahin, "Uluslararası Güvenlik Literatüründe Eleştirel Bir Yaklaşım: Ontolojik Güvenlik Teorisi", *Güvenlik Stratejileri Dergisi*, 19:44, 2023, s. 1-33; Muhammed Onur Çöpoğlu, "Eleştirel Güvenlik Çalışmaları'nın Tıkanıklığında Yeni Açılımlar: Görsel ve Yerel Güvenlik Çalışmaları'nın Vaatleri", *Güvenlik Stratejileri Dergisi*, 20:47, 2024, s. 43-61.

Dergide yayımlanan makalelere yapılan atıflar üç farklı kaynak (TRDizin, SOBİAD Atıf Dizini ve Google Akademik) üzerinden veri toplanarak değerlendirilmiştir. Bu veriler, kaynaklar arasında atıf sayılarındaki farklılıkları ortaya koymuştur: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu'na (TÜBİTAK) bağlı Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) tarafından geliştirilen ve Ulusal Atıf Dizini olan TRDizin'de *GSD*'de yayımlanmış makalelere yapılan atıfların görece az olmasının nedeni, TRDizin'in yalnızca kendi platformuna kabul ettiği dergilerde yapılan atıfları ölçmesidir.[52] Öte yandan, özel bir şirket tarafından geliştirilen ve uluslararası bir indeks olarak kendini konumlandıran SOBIAD Atıf Dizini'nde *GSD*'de yayımlanmış makalelere yapılan atıfların görece daha fazla olduğu görülmektedir. Bunun nedeni ise, SOBIAD'ın uluslararası düzeyde süreli olarak en az dört yıl düzenli yayın yapmış ve kendisine başvurmuş dergileri indeksine kabul etmesi ve dolayısıyla TRDizin'e oranla daha fazla dergiyi platformunu barındırması ve atıf taramasını da bu dergiler üzerinden yapmasıdır. Ancak SOBIAD da ağırlıklı olarak Türkiye merkezli dergileri taradığı için yapılan atıf taraması yine de sınırlı düzeyde kalmaktadır.[53] Google Akademik ise akademik dergilerin yanı sıra diğer akademik yayınları da (kitaplar, konferans bildirgeleri, lisansüstü tezler, özet bildiriler, raporlar, vb.) tam metin düzeyinde veya üst veri düzeyinde taramaktadır ve bu nedenle *GSD*'de yayımlanan makalelere yapılan atıflara dair gerçek anlamda uluslararası düzeyde ve kapsamlı olarak ulaşılmasına imkân tanımaktadır. Bununla birlikte, bir dizinde çok sayıda atıf alan bir çalışmanın diğer dizinde atıf almamasının nedenini tespit etmek için bundan sonraki çalışmalarda dizinlerde taranan dergilere yönelik çapraz inceleme ve makalelere yönelik çapraz atıf taraması yapılması faydalı olacaktır.

Dergideki makalelere yapılan atıflarla ilgili dikkat çekilmek istenen bir başka husus, en çok atıf aldığı tespit edilen bu makaleler içinde dört makalenin, güvenlikle ilgili kuramsal tartışmaları ele alan makaleler olmasıdır. Bu da *GSD* kabul ettiği makalelerin güvenlik alanında kuramsal tartışmalara katkıda bulunduğunu göstermesi adına önemli bir konumda bulunduğunu göstermektedir. Özellikle en çok atıf alan "Kopenhag Okulu ve Güvenlikleştirme Teorisi" başlıklı makale, söz konusu teorinin Türkçe alanyazında tartışılmaya başladığı dönemin başında *GSD*'de yayımlanmış ve güvenlik çalışmaları alanında bu teorinin tartışılması sırasında Türkçe yazılmış temel makalelerden biri haline gelmiştir.

Bu çalışmanın yazarları tarafından dergiyle ilgili tespit edilen eksikliklerden biri, derginin gerek ulusal gerekse uluslararası düzeyde etkili bir tanıtım stratejisinin bulunmamasıdır. *GSD*, 2011 yılında uluslararasılaşma çabasına girse de uzun bir süre boyunca (2014 yılına kadar) işlevsel bir web sitesine sahip olamamıştır ve derginin adının duyurulmasına yönelik faaliyetler genellikle editörlerin çabalarıyla sınırlı kalmıştır. Dergi, işlevsel sayılabilecek kendi adına web sitesini ancak 2018 yılında oluşturmuştur. Ayrıca *GSD*'nin sosyal medyada veya sosyal ağlar üzerinde bulunmaması da bir diğer önemli eksiklik olarak görülmektedir. Hâlihazırda derginin sosyal medya veya sosyal ağlar üzerindeki varlığı, MSÜ Twitter (yeni adıyla X) hesabından yeni sayının yayınlandığına dair gönderilerle ve dergide makalesi yayımlanmış olan yazarların kendi hesapları üzerinden kendi

52 TRDizin'de halihazırda taranan dergi sayısı 1770 ve Sosyal ana alanındaki dergi sayısı 841 iken, Uluslararası İlişkiler disiplininde taranan dergi sayısı 158'dir. Sosyal Bilimler altında Güvenlik Çalışmaları alanı bulunmamaktadır. "Dergi Listesi", TRDizin, https://search.trdizin.gov.tr/tr/dergi/ara?q=, erişim 21.09.2025.

53 SOBIAD, Türkiye'den 1761 dergiyi ve dokuz farklı ülkeden 332 dergi indeks listesine (toplam 2093 dergi) almıştır. SOBIAD'da Türkiye merkezli dergiler arasında Sosyal, Beşerî ve İdari Bilimler alanında 721 derginin tarandığı görünmektedir; ancak atıf dizini bu ana alan altında Uluslararası İlişkiler, Uluslararası Güvenlik veya Güvenlik Çalışmaları alt disiplinlerine yönelik bir ayrıma gitmemiştir. "Taranan Dergiler" SOBIAD, https://atif.sobiad.com/index.jsp?modul=journals, erişim 21.09.2029.

ağlarına yaptığı paylaşımlarla sınırlıdır. *GSD* adına Twitter gibi sosyal medya mecralarında veya ResearchGate, Academia ve LinkedIn gibi akademisyenlere ve araştırmacılara yönelik sosyal ağlarda hesaplar açılarak buralardan düzenli paylaşımların yapılması, dergi tarafından bir başka tanıtım stratejisi olarak uygulanabilir. Söz konusu düzenli paylaşımlarla dergiyle ilgili güncel bilgilerin, makale ile özel sayı çağrılarının alanda daha geniş çevrelere ulaşması sağlanabilir. Ayrıca derginin güncel sayısındaki makalelerin kısa tanıtımları yapılarak dergiye ilgi çekilebileceği gibi, uluslararası ilişkiler ve güvenlik konularında yaşanan güncel konularla bağlantılı olarak dergide daha önce yayımlanmış olan makalelerin hatırlatıldığı dönemsel paylaşımlar da yapılabilir. Sosyal medyada ve sosyal ağlarda bu şekilde varlık göstermesinin, derginin zaman içinde görünürlüğünü artıracağı, böylece daha geniş kitlelere ulaşırken yazar havuzunu da genişletmesine katkı sağlayacağı düşünülmektedir.

Sonuç olarak, *GSD*, güçlü kurumsal geçmişi ve editoryal tecrübesiyle alanda önemli bir konuma sahiptir. Ancak uluslararası görünürlüğünü artırmak, konu çeşitliliğini zenginleştirmek ve daha dengeli bir yazar profili oluşturmak için stratejik adımlar atılması gerekmektedir. İngilizce yayın oranının yükseltilmesi, yabancı akademisyenlerin ve kadın akademisyenlerin katkılarının teşvik edilmesi ve çevrimiçi alanda varlık gösterilmesi, derginin uluslararası dizinlerde yer almasına ve alandaki etkisini artırmasına katkı sağlayacaktır.

Son olarak, güvenlik çalışmaları alanında önemli bir yere sahip olan *GSD* üzerine sunulan literatürdeki bu ilk bibliyometrik analizin belirli periyotlarla tekrarlanması planlanmaktadır ki bu da hem disiplin hem de dergi için önemli ve özgün bir katkı sağlayacaktır. Ancak güvenlik çalışmaları disiplinin geneli hakkında daha kapsamlı bilgilerin ortaya konulabilmesi için bibliyometrik analizlerin yukarıda bahsedilen alanın yeni dergilerini kapsayacak şekilde genişletilmesi faydalı olacaktır. Disiplindeki tüm dergiler arasında geniş kapsamlı bir çalışma yapılabileceği gibi, farklı dergilerde farklı konulara veya farklı bağlamlara yoğunlaşılıp yoğunlaşılmadığını görmek için de içerik analizlerinin yapılması yeni çalışmalar için önemli bir yol açacaktır. Gelecekte bu yöndeki çalışmaların sadece dergilerle sınırlı tutulmaması, disipline dair lisansüstü tezlerinin, kitap bölümlerinin ve kitapların da bu tür bibliyometrik ve/veya içerik analizlerine dâhil edilmesi güvenlik çalışmaları disiplinin Türkiye'deki gelişimini ve ilerleyişini anlamak adına faydalı olacaktır.

Yazarların Katkı Oranı

Araştırma Tasarısı S.D., Literatür Taraması D.K., Veri Toplama S.D., Veri Seti Oluşturma S.D. ve D.K., Analiz S.D. ve D.K., Metin Oluşturma S.D. ve D.K.

Çıkar Çatışması Beyanı

Araştırmanın yazarları olarak herhangi bir çıkar çatışma beyanımız bulunmamaktadır.

Not

Çalışma kapsamında Excel paket programında hazırlanmış olan veri seti, komut dosyaları/betikler (script) ve Python programlama dilinden alınan orijinal sonuç materyalleri GSD editörlüğüyle paylaşılmıştır.

Editörlük Beyanı

Bu makalenin editoryal süreçleri çift-dış-kör hakemlik usulü ile yürütülmüştür.

Yapay Zeka Kullanımı Bildirimi

Çalışmada herhangi bir şekilde yapay zeka uygulamalarından yararlanılmamıştır.

KAYNAKÇA

Basılı Eserler

AKGÜL-AÇIKMEŞE Sinem (2011). "Algı mı, Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri", *Uluslararası İlişkiler*, 8:30, 43-73.

AKGÜL-AÇIKMEŞE Sinem ve ERMİHAN Erman (2023). "Türkiye'de Güvenlik Çalışmaları", Ayça Ergun, Çiğdem Üstün ve Sinem Akgül Açıkmeşe (der.), *Türkiye'de Uluslararası İlişkiler Çalışmaları: Alt Alanlar ve Bölgesel Odaklar*, İmge Kitapevi, İstanbul, 259-301.

AĞIR Bülent Sarper (2015). "Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı", *Güvenlik Stratejileri Dergisi*, 11:22, 97-130.

AYDIN Mustafa GÜNTER BRAUCH Hans POLAT Necati ÇELİKPALA Mitat ve SPRING Ursula Oswald (der.) (2012). *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

AYDIN Mustafa ve DİZDAROĞLU Cihan (2019). "Türkiye'de Uluslararası İlişkiler: TRIP 2018 Sonuçları Üzerine Bir Değerlendirme", *Uluslararası İlişkiler* 16:64, 3-28.

BAYSAL Başar (2022). "Güvenlik Kavramı ve Güvenliğin Dönüşümü", Başar Baysal (der.) *Uluslararası İlişkilerde Güvenlik*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 3-10.

BİRDİŞLİ Fikret (2014). "Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım: Galler Ekolü", *Güvenlik Stratejileri Dergisi*, 10:20, 229-256.

BUZAN Barry ve HANSEN Lene (2009). "Strategic Studies, Deterrence and the Cold War", *The Evolution of International Security Studies*, Cambridge University Press, Cambridge, 66-100.

ÇOKİŞLER Elvan (2019). "Uluslararası İlişkiler Dergisinin Bibliyometrik Analizi (2004-2017)", *Uluslararası İlişkiler*, 16:64, 29-56.

ÇÖPOĞLU Muhammed Onur (2024). "Eleştirel Güvenlik Çalışmaları'nın Tıkanıklığında Yeni Açılımlar: Görsel ve Yerel Güvenlik Çalışmaları'nın Vaatleri", *Güvenlik Stratejileri Dergisi*, 20:47, 43-61.

DEMİRCİ Hatice ve ŞAHİN Güngör (2023). "Uluslararası Güvenlik Literatüründe Eleştirel Bir Yaklaşım: Ontolojik Güvenlik Teorisi", *Güvenlik Stratejileri Dergisi*, 19:44, 1-33.

DONTHU Naveen KUMAR Satish MUKHERJEE Debmalya PANDEY Nitesh ve LIM W. M. (2021). "How to Conduct a Bibliometric Analysis: An Overview and Guidelines", *Journal of Business Research*, 133, 285-296.

FYFE Aileen, COATE Kelly, CURRY Stephen, LAWSON Stuart, MOCHAM Noah ve MØRK RØSTVIK Camilla (2017). *Untangling Academic Publishing: A History of the Relationship between Commercial Interests, Academic Prestige and the Circulation of Research*, University of St Andrews, St Andrews.

KARATAŞ Adnan (2023). "Determining the Dominant Understandings in Security Science Literature in Turkey: A Bibliometric Analysis on the Journal of Security Science", *Heliyon*, 19:9, e19278.

MEHMETÇİK Hakan ve HAKSES Hasan (2023). "Turkish IR Journals through a Bibliometric Lens", *All Azimuth: A Journal of Foreign Policy and Peace*, 12:1, 61-84.

ÖZDEMİR Özlem ve ÖZDEMİR Emrah (2018). "Suriyeli Mülteci Kadınlar ve İnsani Güvenlik", *Güvenlik Stratejileri Dergisi*, 14:27, 113-145.

ÖZGÜR Erdem ve YILMAZ Murat (2024). "Güvenlik Çalışmaları Alanının Mevcut Durumu ve Geleceği Üzerine Bir Değerlendirme", *Güvenlik Stratejileri Dergisi*, 20:49, 288-289.

SARI ERTEM Helin (2012). "Kimlik ve Güvenlik İlişkisine Konstrüktivist Bir Yaklaşım: 'Kimliğin Güvenliği' ve 'Güvenliğin Kimliği'", *Güvenlik Stratejileri Dergisi*, 8:16, 177-236.

SARI ERTEM Helin ve DÜZGÜN Aslı Nur (2021). "Uluslararası İlişkiler Disiplininde Ontolojik Güvenlik Teorisi: Kavram ve Literatür Odaklı Bir İnceleme", *Güvenlik Stratejileri Dergisi*, 17:37, 39-83.

"Sunuş", *Güvenlik Stratejileri Dergisi*, 1:1, 2005, 5.

WÆVER Ole ve BUZAN Barry (2017). "Teoriye Dönüş Sonrası: Güvenlik Çalışmalarının Geçmişi, Bugünü ve Geleceği", Alan Collins (ed.), *Çağdaş Güvenlik Çalışmaları* (Üçüncü Basım), (Çev. Nasuh Uslu), Uluslararası İlişkiler Kütüphanesi, İstanbul, 393–410.

İnternet Kaynakları

Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü (2025). "Enstitümüz Hakkında", https://atasaren.msu.edu.tr/misyonvizyon, erişim 20.07.2025

Diplomasi ve Strateji Dergisi (2025). https://www.dsjournal.org/, erişim 20.07.2025.

Güvenlik Bilimleri Dergisi (2025). https://dergipark.org.tr/tr/pub/gbd, erişim 20.07.2025.

Güvenlik Çalışmaları Dergisi. (2025). https://guvenlikcalismalari.pa.edu.tr/, erişim 20.07.2025.

Güvenlik Çalışmaları Türkçe Yayınlar Bibliyografyası (1990–2021) (2025). Millî Savunma Üniversitesi, Kara Harp Okulu, Ankara, https://kutuphane.msu.edu.tr/?p=5&id=H7C5D4IZ6M&dil=tr&q=bibliyografya, erişim 20.07.2025.

Güvenlik Stratejileri Dergisi (2025). "Sayılar", https://gsd.msu.edu.tr/TR/Sayilar, erişim 15.07.2025.

Güvenlik Stratejileri Dergisi (2025). "Süre İstatistikleri", https://dergipark.org.tr/tr/pub/guvenlikstrtj/time-statistics, erişim 20.07.2025.

Güvenlik ve İstihbarat Çalışmaları Dergisi (2025). https://jsis.org.tr/, erişim 20.07.2025.

Harzing A. W. *Publish or Perish* (2025). https://harzing.com/resources/publish-or-perish, erişim 15.07.2025.

International Journal of Politics and Security (2025). https://dergipark.org.tr/tr/pub/ijps, erişim 20.07.2025.

SAVSAD Savunma ve Savaş Araştırmaları Dergisi (2025). http://savsad.kho.msu.edu.tr/, erişim 20.07.2025.

Savunma Bilimleri Dergisi (2025). https://kho.msu.edu.tr/akademik/enstitu/enstitu_Alp_SAVBEN_dergi_anasayfa.html ve https://dergipark.org.tr/tr/pub/khosbd, erişim 20.07.2025.

Savunma ve Güvenlik Araştırmaları Dergisi (2025). https://kho.msu.edu.tr/akademik/enstitu/hakkimizda_guvenlik_dergi.html ve https://dergipark.org.tr/tr/pub/saga, erişim 20.07.2025.

SDE Akademi Dergisi (2025). https://dergipark.org.tr/tr/pub/sde, erişim 20.07.2025.

SOBIAD Atıf Dizini (2025). https://atif.sobiad.com/index.jsp?modul=journals-detail&ID=wlSbVIMBYqx-AIGX2zNeO, erişim 15.07.2025.

SOBIAD (2025). "Taranan Dergiler", https://atif.sobiad.com/index.jsp?modul=journals, erişim 21.09.2025.

Terörizm ve Radikalleşme Araştırmaları Dergisi (2025). https://www.tradergisi.com/, erişim 20.07.2025.

TRDizin (2025). https://search.trdizin.gov.tr/tr/dergi/detay/532/guvenlik-stratejileri-dergisi, erişim 15.07.2025.

TRDizin (2025). "Dergi Listesi", https://search.trdizin.gov.tr/tr/dergi/ara?q=, erişim 21.09.2025.

Uluslararası İlişkiler Dergisi (2025). https://www.ir-journal.com/tr, erişim 20.07.2025.

Uluslararası İlişkiler ve Politika Dergisi (2025). https://dergipark.org.tr/tr/pub/ulipod, erişim 20.07.2025.

Uluslararası Kriz ve Siyaset Araştırmaları Dergisi (2025). http://uksad.com/, erişim 20.07.2025.

YÖK Akademik (2015). "Yükseköğretim Akademik Arama Sayfası", https://akademik.yok.gov.tr/AkademikArama/, erişim 21.09.2025.

Yüksek Öğretim Bilgi Yönetimi Sistemi (2025). https://istatistik.yok.gov.tr/, erişim 24.09.2025.

GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 355-372
DOI: 10.17752/guvenlikstrtj.1786004

Araştırma Makalesi
Research Article

Turkish-American and NATO Relations After the Embargo: Türkiye's Strategic Position in Light of NSSM 227, CIA, and NATO Defense Planning Documents (1974-1980)

Ambargo Sonrası Türk-Amerikan ve NATO İlişkileri: NSSM 227, CIA ve NATO Savunma Planlama Belgeleri Işığında Türkiye'nin Stratejik Konumu (1974-1980)

Macide BAŞLAMIŞLI*

* Dr. Öğr. Üyesi, Kahramanmaraş İstiklal Üniversitesi, İnsan ve Toplum Bilimleri Fakültesi, Tarih Bölümü, Kahramanmaraş, Türkiye, e-posta: macidebaslamisli80@gmail.com
ORCID: 0000-0003-0381-4651

Geliş Tarihi / Submitted: 17.09.2025

Kabul Tarihi / Accepted: 10.12.2025

Abstract

This study examines the effects of the American arms embargo imposed after the 1974 Cyprus Peace Operation on Turkish-American relations and Türkiye's strategic position within NATO. The objective is to reassess the widely cited "crisis of confidence" thesis—often built on secondary interpretations—through primary documents, namely the U.S.'s National Security Council's National Security Study Memorandum 227 (NSSM 227) report (1975), the CIA's Interagency Memorandum (1975), and NATO Defense Planning documents (1973–1982). The research is based on systematic archival work conducted in 2023–2024, using U.S. presidential archives, CIA Freedom of Information Act (FOIA) releases, and NATO archives. The findings demonstrate that while Washington depicted Türkiye as an "unreliable but indispensable" ally, Brussels focused on military and economic deficiencies, framing Türkiye as a dependent yet critical partner. Ultimately, the study argues that Türkiye's position shifted from a "special ally" to a "compulsory partner" and that the embargo significantly amplified concerns about NATO's southern flank deterrence.

Keywords: Turkish-American Relations, NATO, Arms Embargo, NSSM 227, CIA, Türkiye's Strategic Position

Öz

Bu çalışma, 1974 Kıbrıs Barış Harekâtı sonrasında uygulanan Amerikan silah ambargosunun, Türk-Amerikan ilişkileri ve Türkiye'nin NATO içindeki stratejik konumu üzerindeki etkilerini incelemektedir. Çalışmanın amacı, literatürde çoğunlukla ikincil yorumlara dayanan güven krizi tezini, ABD Ulusal Güvenlik Konseyi'nin NSSM 227 raporu (1975), CIA'nın Kuruluşlararası Bilgi Notu (1975) ve NATO Savunma Planlama belgeleri (1973–1982) ışığında birincil belgelerle yeniden değerlendirmektir. Çalışma, ABD ulusal arşivleri, Bilgiye Erişim Özgürlüğü Yasası kapsamında erişime açılan CIA belgeleri ve NATO arşivi üzerinden yapılan sistematik taramalara dayanmaktadır. Bulgular, ABD kurumsal raporlarının Türkiye'yi "güvenilmez ama vazgeçilmez" bir ortak olarak tanımlarken, NATO'nun ise ekonomik ve askeri kapasite eksikliklerine odaklandığını göstermektedir. Sonuç olarak çalışma, Türkiye'nin söz konusu dönemde "özel müttefik" konumundan "zorunlu ortak" kimliğine evrildiğini ve ambargonun NATO'nun güney kanadındaki caydırıcılığa yönelik riskleri artırdığını ortaya koymaktadır.

Anahtar Kelimeler: Türk-Amerikan İlişkileri, NATO, Ambargo, NSSM 227, CIA, Türkiye'nin Stratejik Konumu

Introduction

The United States (U.S.) arms embargo imposed following the 1974 Cyprus Peace Operation is widely recognized in the literature as a turning point in Turkish-American relations. According to the prevailing view, the embargo led to a lasting crisis of trust between the two countries and played a decisive role in shaping the trajectory of bilateral relations in the long term.[1] However, this prevailing approach has largely been constructed based on political discourse in Türkiye, public reactions, and secondary sources. In this context, George Harris, in his 1976 article, emphasized the crisis of trust caused by the embargo and the shift in Ankara's perception of Washington.[2] Dankwart Rustow's work *Turkey: America's Forgotten Ally* emphasized Türkiye's strategic indispensability for the U.S.; however, it also demonstrated that this indispensability did not eliminate political tensions between the two countries.[3] Prominent scholars such as William Hale and Feroz Ahmad have examined the orientations of Turkish foreign policy in the 1970s in detail, with particular attention to the rise of anti-American sentiment in Turkish public opinion as a result of the embargo.[4] Although Frank Schimmelfennig's works have focused on the context of North Atlantic Treaty Organization (NATO) enlargement and the broader security order, they have not addressed Türkiye's military capacity issues during the 1970s.[5]

This study re-evaluates the prevailing approach through an analysis of primary documents. Its originality lies in the comparative examination of sources from three distinct institutional levels. These include the U.S. National Security Council's (NSC's) National Security Study Memorandum 227 (NSSM 227) documents in 1975, the Central Intelligence Agency's (CIA's) Interagency Memorandum prepared in the same year, and NATO's defense planning reports. These documents reveal that the embargo had effects on more than just bilateral relations; it also had effects on NATO's planning for collective security.

Indeed, NSSM 227 describes Türkiye as an ally whose "*reliability is in question",* while simultaneously noting the *"indispensability"* of its bases and geographical location.[6] The CIA's Interagency Memorandum, on the other hand, documented the direct military consequences of the embargo, emphasizing that the deterrent capacity of the Turkish Armed Forces was rapidly deteriorating due to a lack of modern equipment, insufficient stockpiles, and inflation.[7] The NATO documents, while detailing deficiencies in the land, air, and naval forces, explicitly stated that "substantial external assistance" was necessary to maintain deterrence.[8]

Undoubtedly, other international political developments of the period also influenced this approach. In particular, within the context of Greece's withdrawal from the military flank of NATO and the Warsaw Pact's increased presence in the Mediterranean in 1975, NATO

1 Oral Sander, *Türk-Amerikan İlişkileri*, İmge Kitabevi, Ankara, 1998, p. 245-247.
2 George S. Harris, "The Arms Embargo and Turkey", *Middle East Journal* 30:2, 1976, 129-143.
3 Dankwart Alexander Rustow, *Turkey: America's Forgotten Ally*, Council on Foreign Relations, New York, 1987.
4 William Hale, *Turkish Foreign Policy since 1774* Routledge, London, 2000; Feroz Ahmad, *The Turkish Experiment in Democracy, 1950–1975*, Westview Press, Boulder, 1977.
5 Frank Schimmelfennig, *NATO and the European Security Order: History, Theory, and Practice*, Routledge, London, 2018.
6 NSSM 227: U.S. Security Policy Toward Turkey, 1975, National Security Council, Box 37, Gerald R. Ford Presidential Library, accessed 20.03.2024.
7 CIA, Turkey After the US Arms Cutoff, Interagency Memorandum, 1975, CIA Records (CREST), https://www.cia.gov/readingroom/document/cia, accessed 20.03.2024.
8 NATO Archives, "Defence Review Committee Working Paper" (DRC/WP/74/2), 1974, "Defence Planning Committee Report" (DPC/D/76/2), 1976, s. 12; "Force Planning Country Study: Turkey", 1973–1982, NATO Archives Online, accessed 12.03.2025.

documents identified Türkiye as the keystone of the southeastern flank and emphasized that this role could not be sustained without external assistance. As a result, this study reveals not only the crisis of trust in bilateral relations with the U.S. but also NATO's reflex and effort to support Türkiye within the framework of collective security, based on primary sources.

Therefore, while the frequently asserted thesis in Türkiye that "the embargo created a rupture in Turkish-American relations" is confirmed in this study, it is also documented in a multi-layered manner through U.S. institutional documents and NATO documents. In this context, the article re-examines the period between 1974 and 1980 as a transformative process in which Türkiye's position within the Western alliance shifted from a "special relationship" to a "compelled ally".

The concepts of "special relationship" and "compelled ally" employed in this study are analytical interpretations derived from contemporary documents rather than terms explicitly stated within them. The term "special relationship" describes the special treatment the U.S. gave Türkiye during the Cold War, which included military aid, base privileges, and political coordination. However, post-1974 documents indicate a deterioration of this status, revealing Türkiye's transition into a new position that can be described as a "compelled partner". This concept is derived from statements arguing that even though there were issues with reliability and capacity, Türkiye's geographic location and its critical role on the southeastern flank made it impossible for the country to leave the alliance.

Aiming to examine Türkiye's position within the Western alliance during the period 1974–1980, this study primarily relies on archival documents and declassified official reports. The U.S. NSC's National Security Study Memorandum 227 (NSSM 227—"U.S. Security Policy Toward Turkey" [Box:37], 1975) and the Central Intelligence Agency's report titled "Interagency Memorandum: Turkey After the US Arms Cutoff (1975)" were obtained through the CIA Reading Room and the National Archives. Documents belonging to NATO's Defence Planning Committee, such as the Defence Review Committee Working Paper (DRC/WP/74/2, 1974), Defence Planning Committee Document (DPC/D/76/2, 1976), and the Force Planning Document on Turkey (1973–1982), were accessed via the NATO Archives online catalog and related declassified sources.

The documents utilized in this study were obtained through systematic digital archival searches conducted between 2023 and 2024. The U.S. presidential archives, CIA reports released under the Freedom of Information Act (FOIA), and defense planning documents made available online by the NATO archives were thoroughly reviewed, with assessments regarding Türkiye's strategic position directly extracted from relevant sections of these records. Additionally, American presidential documents from the period—such as the Johnson Letter, Ford's veto message, and statements by the Carter administration to Congress—were examined via the U.S. National Archives and Presidential Libraries collections. In addition to primary sources, the contributions of renowned scholars such as George Harris, Dankwart Rustow, William Hale, Feroz Ahmad, and Frank Schimmelfennig in the secondary literature have also been taken into account. This approach ensures that the study offers an original contribution grounded not only in secondary interpretations but directly based on archival documents.

1. Historical Roots of the Alliance

The 1947 Truman Doctrine began the shaping and institutionalization of Turkish-American relations within the context of the Cold War. By committing to provide a total of 400 million dollars in military and economic aid to Türkiye and Greece, the U.S. aimed to prevent these

two countries from falling under Soviet influence.[9] These aid programs brought about a profound transformation in Türkiye's security system, serving as a critical resource for the modernization of the military and the reconstruction of the economy. Türkiye's accession to NATO in 1952 further consolidated this process. Türkiye's geostrategic position within NATO's southern flank was considered indispensable for establishing deterrence against the Soviet Union.[10] Within this framework, the U.S. established over twenty military facilities in Türkiye, with Incirlik Air Base becoming one of Washington's most critical bases throughout the Cold War.[11] By the late 1950s, Turkish-American relations had reached a level of close cooperation that can be described as a "special relationship". Some sources note that Türkiye possessed the second-largest military force within NATO after the U.S. and was an integral part of the Alliance's collective defense posture—an arrangement that represented a significant contribution to the collective security efforts, including those led by the U.S.[12]

The 1960s had profound effects within the context of Türkiye's domestic political developments. Specifically, the military coup of May 27, 1960, significantly impacted not only Türkiye's internal politics but also its foreign policy. In the post-coup period, the rise of left-leaning, nationalist discourses brought greater visibility to the presence of American military forces in Türkiye.[13] During this period, although dependency on U.S. aid continued, skepticism toward the idea of "unconditional commitment" to the West began to grow among both the Turkish public and political elites. The first major rupture in relations occurred with the 1964 Johnson Letter. In response to escalating tensions in Cyprus and Ankara's potential intervention plans, U.S. President Lyndon B. Johnson sent a letter asserting that Türkiye could not use American weapons without permission and emphasizing the uncertainty of NATO's response in the event of a Soviet attack.[14] These statements deeply undermined the trust of Turkish decision-makers in the U.S., solidifying the perception that "the U.S. may abandon Türkiye when most needed." In the aftermath of the Johnson Letter, while Türkiye maintained its NATO membership, it began to seek diversification in its foreign policy options. Within this framework, economic and technical cooperation projects with the Soviet Union came to the forefront, marking the first signs of Ankara's search for alternatives to its alignment with the West.[15]

In the early 1970s, the Cyprus issue and the ban on poppy cultivation became central points of contention in Turkish-American relations. The relationship experienced its most severe rupture after Türkiye conducted the Cyprus Peace Operation in response to the Greek-backed coup on July 15, 1974. Simultaneously, the U.S. identified poppy cultivation in Türkiye as a primary source of its domestic drug problem and pressured Ankara to prohibit the production of this strategically important crop. The Cyprus intervention and the poppy cultivation issue formed the core of bilateral tensions. The U.S. regarded Türkiye's use of American-supplied weapons during the Cyprus operation as a violation of existing agreements. Moreover, Türkiye's firm stance on the poppy cultivation issue prompted the

9 Melvyn P. Leffler, *For the Soul of Mankind: The United States, the Soviet Union, and the Cold War*, Hill and Wang, New York, 2007, p. 132.
10 Dankwart A. Rustow, *Turkey: America's Forgotten Ally*, Council on Foreign Relations, New York, 1987, 45.
11 George S. Harris, *Troubled Alliance: Turkish-American Problems in Historical Perspective, 1945–1971* American Enterprise Institute, Washington, D.C., 1972, p. 88, 89.
12 Birol Akduman, "NATO's Southern Flank: The Evolution of Türkiye's Strategic Role and Its Implications for Regional Security", *İnsan ve Toplum Bilimleri Araştırmaları Dergisi,* 12:5, p. 2951.
13 Feroz Ahmad, *The Turkish Experiment in Democracy, 1950–1975*, Westview Press, Boulder, 1977, p. 241, 242.
14 William Hale, *Turkish Foreign Policy since 1774*, Routledge, London, 2000, 168.
15 Ibid.

U.S. Congress to impose a comprehensive arms embargo on Türkiye on February 5, 1975.[16] Undoubtedly, domestic public opinion in the U.S. also played a significant role in the adoption of this decision.[17] In particular, the convergence of Greek, Greek Cypriot, and Armenian lobbies around an anti-Turkish stance, and the pressure they exerted on the Ford administration, played a significant role in influencing the U.S. Congress's decision. President Ford repeatedly warned the Congress about the "extremely serious consequences" of such measures and pushed for the restoration of military sales and credits to Türkiye, stressing the importance of supporting a key NATO ally.[18] Indeed, despite President Ford's two veto attempts, the Congress overrode the vetoes and enacted the arms embargo on Türkiye into law.[19] President Ford, for his part, described the embargo as "*the single most irresponsible and shortsighted foreign policy action taken by the Congress during all the years I have been in Washington*".[20] The arms embargo imposed on Türkiye sparked significant disagreement within U.S. domestic politics and public opinion. Both the Ford and Carter administrations increasingly argued that the embargo was detrimental to the vital interests of the U.S. and NATO and even Israel's security. In this context, particularly under the influence of evolving regional developments and dynamics, President Carter quickly shifted away from his initially pro-embargo stance. A telling example of this shift was provided by Carter's advisor, Clark Clifford, who—after meeting with members of the Congress—noted that they were "shockingly indifferent" to the long-term implications for U.S.–Greece or U.S.–Türkiye relations, or to the potential loss of Turkish bases.[21]

In summary, while the embargo and the Cyprus issue may have benefited certain candidates in U.S. domestic politics—particularly during presidential elections—they severely strained Washington's relations with its NATO allies, namely Türkiye and Greece. These developments created uncertainty over the future of U.S. bases in Türkiye and jeopardized American security interests in the Eastern Mediterranean. In retaliation for the embargo, Türkiye refused the return of U.S. nuclear delivery systems, declared the Turkish Federated State of Cyprus, lifted the poppy cultivation ban, froze the status of U.S. military bases, and ultimately annulled the 1969 Defense Cooperation Agreement.[22]

Throughout 1977 and 1978, the Carter administration engaged in an intense struggle with the Congress to resolve the issue of the arms embargo on Türkiye. While the administration sought to advance a Defense Cooperation Agreement with Ankara, a group of influential members of the Congress staunchly opposed lifting the embargo unless Türkiye made tangible progress on the Cyprus issue. The fact that Türkiye had exploited a loophole to procure arms through NATO's supply agency further intensified this opposition. Over

16 U.S. Congress, Congressional Record, 94th Congress, House of Representatives, 1975, p. 1 https://www.congress.gov/bill/94th-congress/house, accessed 20.03.2024.; Macide Başlamışlı "ABD'nin Türkiye'ye Yönelik Ambargo Kararına İlişkin Haşhaş Sorunu Yerine 1974 Kıbrıs Krizini Ön Plana Çıkarma Girişimi", *Asia Minor Studies,* 9:1, 2021, p. 695.

17 James F. Goode, *The Turkish Arms Embargo: Drugs, Ethnic Lobbies, and US Domestic Politics (Studies in Conflict, Diplomacy, and Peace*, University Press of Kentucky, 2020, p. 19.

18 NARA, Turkey (1), Box:125, July 25, 1975, The Ron Nessen Papers at the Gerald R. Ford Presidential Library, accessed 20.03.2024.

19 Ibid.

20 Ibid.

21 NARA, "Turkey" (1), Box:125, July 25, 1975, The Ron Nessen Papers at the Gerald R. Ford Presidential Library, accessed 20.03.2024.

22 Serhat Güvenç, Soli Özel, "NATO and Turkey in the post-Cold War world: between abandonment and entrapment", *Southeast European and Black Sea Studies* Vol. 12, No. 4, December 2012, 535,536; Ayşe Ömür Atmaca, "The Alliance in the Storm: Geopolitical Representation of the United States in the Turkish Parliament during Détente", *All Azimuth,* V14, N1, 2025), 116.

time, President Carter, who had come to support the Defense Cooperation Agreement, recognized both the difficulty of securing congressional approval and the urgency of restoring U.S.–Türkiye relations. As a result, he strategically decided to pursue the unconditional lifting of the embargo. This shift in approach was informed by lessons learned during the administration's experience with the Panama Canal treaties and led to the planning of a broad lobbying campaign. However, the Greek-American lobby's influence and ongoing concerns about human rights in Cyprus continued to fuel the opposition.[23] The aforementioned reports and analyses undoubtedly influenced the shift in strategy.

The embargo had a more tangible impact on Türkiye. Specifically, it directly disrupted the modernization of the Turkish military. Since 1950, American aid to Türkiye had exceeded a total value of three billion dollars, resulting in over 90% of the Turkish Armed Forces becoming dependent on weapons systems originating from the U.S.[24] Certainly, with the implementation of the embargo, Türkiye entered a severe military bottleneck. In response, Türkiye suspended the 1969 Defense Cooperation Agreement, reclassifying U.S. military facilities on its soil to a "temporary status", thereby compelling Washington to engage in new negotiations.[25] The embargo not only strained Turkish-American relations but also prompted a reexamination of Türkiye's role within NATO. While Turkish decision-makers reaffirmed their commitment to the alliance, the bilateral crisis with the U.S. necessitated a reassessment of Türkiye's position within NATO. During this period, NATO documents increasingly emphasized Türkiye's military capacity shortfalls and its dependence on external assistance. In this context, the 1975 National Security Study Memorandum 227 (NSSM 227) and NATO defense planning documents from 1974 to 1976 emerged as critical texts that redefined Türkiye's standing within the Western alliance.

2. Türkiye in the U.S. Institutional Documents: NSSM 227 and the CIA Interagency Memorandum (1975)

The U.S. arms embargo prompted both countries to reassess their existing bilateral relations. Following the embargo decision, American policymakers received a significant strategic warning from the effective suspension of the 1969 Defense Cooperation Agreement (DCA) and the reclassification of U.S. military facilities in Türkiye to a "temporary status".[26] In this context, the U.S. NSC prepared the National Security Study Memorandum 227 (NSSM 227—U.S. Security Policy Toward Turkey) in 1975 to examine Türkiye's future position, alliance commitments, and potential foreign policy orientations.[27]

As a result, the NSSM 227 report acknowledged Türkiye's continued strategic importance on the southern flank of the Cold War while identifying the emerging trust crisis in bilateral relations as a lasting problem. The report emphasized the following key points:

23 James F. Goode, *The Turkish Arms Embargo: Drugs, Ethnic Lobbies, and US Domestic Politics Studies in Conflict, Diplomacy, and Peace*, University Press of Kentucky, Kentucky, 2020, 121.

24 NATO Defence Review Committee, DRC/WP/74/2: Defence Review Committee Working Paper on Turkey Brussels: NATO Archives, 1974), https://archives.nato.int/1975-1980-force-proposals-turkey, 5, accessed 12.03.2025.

25 James F. Goode, *The Turkish Arms Embargo: Drugs, Ethnic Lobbies, and US Domestic Politics Studies in Conflict, Diplomacy, and Peace,* University Press of Kentucky, 2020, 121.

26 James F. Goode, The Turkish Arms Embargo: Drugs, Ethnic Lobbies, and US Domestic Politics Studies in Conflict, Diplomacy, and Peace, University Press of Kentucky, 2020, 121.

27 U.S. National Security Council, NSSM 227: U.S. Security Policy Toward Turkey, 1975, Box 37, The Gerald R. Ford Presidential Library, accessed 20.03.2024.

- Loss of Trust in the U.S.: The report states that the embargo "irreversibly undermined" Ankara's confidence in Washington.[28] Turkish decision-makers were expected to maintain their commitment to NATO; however, the report indicated that efforts to reduce dependency on the West and explore alternative options would likely intensify in the future.[29]
- Priority of Military Facilities: The U.S. bases and installations in Türkiye were classified according to their strategic value. İncirlik Air Base was designated as a "critical priority" facility, while the NATO air headquarters in İzmir, logistical centers in Ankara, and fuel depots in İskenderun were listed as secondary in importance. Smaller radar and communication sites were noted as potentially subject to closure if necessary.[30]
- Dependency of the Turkish Armed Forces: It was emphasized that American aid provided between 1950 and 1974 exceeded three billion dollars and that over 90% of the Turkish military's inventory was dependent on U.S.-origin systems.[31] This situation was considered a factor preventing Türkiye from severing ties with the U.S. in the short term.
- The scenario in which Türkiye might seek security cooperation with Iran, Pakistan, and the Muslim world in the event of losing trust in the West was discussed. This is one of the rare instances in which U.S. documents explicitly acknowledge Türkiye's potential shift toward "non-Western options".[32]
- In this context, the NSSM 227 report identified four possible policy options that Washington might pursue as follows:
- to sign a new Defense Cooperation Agreement that meets Türkiye's demands.
- to prepare a package that prioritizes U.S. interests but includes partial concessions.
- to employ a delaying strategy to buy time.
- to reduce the American presence in Türkiye and retain only critical facilities.[33]

These options demonstrate that the U.S. employed a flexible and multifaceted bargaining strategy in its relations with Türkiye. The most striking conclusion of the report is that Türkiye was redefined in U.S. documents, no longer as a "special ally", but rather as an "unreliable yet indispensable" partner. Washington acknowledged that trust in Türkiye had been irreparably damaged; however, due to its geographical position and military installations, Ankara was emphasized as a strategically critical actor that could not be lost.[34]

The consequences of the American embargo manifested not only at the political level but also became markedly evident in the military sphere. One of the clearest documents illustrating this situation is the 1975 CIA report titled Interagency Memorandum: Turkey

28 Ibid.
29 Ibid.
30 Ibid.
31 NATO Defence Review Committee, DRC/WP/74/2: "Defence Review Committee Working Paper on Turkey Brussels: NATO Archives, 1974", https://archives.nato.int/1975-1980-force-proposals-turkey, accessed 12.03.2025.
32 U.S. National Security Council, NSSM 227, Box 37, The Gerald R. Ford Presidential Library, accessed 20.03.2024.
33 Ibid.
34 Dankwart A. Rustow, *Turkey: America's Forgotten Ally*, Council on Foreign Relations, New York, 1987, 112.

After the US Arms Cutoff.[35] This report provides a detailed examination of Türkiye's dependence on U.S. military equipment and the impact of the U.S. aid cutoff on Türkiye's military capabilities. Unlike NSSM 227, this report does not focus on Türkiye's political reliability but rather directly addresses the effects of the embargo on its military capacities. Nonetheless, the report analyzes Türkiye's reliance on American military hardware, the potential consequences of the embargo, and possible Turkish responses. In particular, it emphasizes that the embargo could undermine Türkiye's role within NATO and potentially lead the country toward inwardness and isolation.[36] The report also considers the possibility that Türkiye may seek alternative external sources to meet its military needs, which could, in turn, affect its relations with Western European countries. While Turkish policymakers were reportedly angered and surprised by the embargo, an immediate reaction was not anticipated. However, the report suggests that should the embargo persist, Türkiye would likely undertake gradual retaliatory measures against the U.S.[37] Here lies a critical warning:

> *"If European allies fail to meet Turkey's fundamental military needs, the Turks may interpret this as a form of 'de facto isolation from NATO,' potentially resulting in 'internal withdrawal' and a 'turn towards local conservatism,' which could pose significant challenges for Turkey's economic future and its role in Southern Europe."*[38]

Another notable point concerns the factors Türkiye would consider while seeking ways to mitigate the effects of the embargo, such as "the inevitable impact of the U.S. aid cutoff, the pursuit of alternative sources for military equipment, and the durability of its current orientation towards the West".[39] Understandably, as an intelligence report, this document also anticipated that the embargo would have major consequences regarding intelligence-gathering capabilities.[40] As a result, the report warned that if the embargo persisted, it could severely undermine the operational capabilities of U.S. forces in the region and jeopardize critical intelligence-gathering programs. The most crucial emphasis of the report was the risk of weakening deterrence on NATO's southern flank. Indeed, intelligence circles emphasized that the embargo posed a threat not only to bilateral relations but to the entire foundation of the alliance's collective defense.[41]

In conclusion, a comparison between NSSM 227 and the CIA's Interagency Memorandum reveals clear differences in institutional priorities within the U.S. administration. While NSSM 227, prepared by the NSC, primarily assesses Türkiye through the lens of political reliability—noting a decline in Ankara's dependence on Washington following the Cyprus intervention and the arms embargo, and thus suggesting a reassessment of Türkiye's role within the alliance—the CIA report adopts a different perspective by focusing directly on military capacity. The latter document provides a detailed account of deficiencies in modern equipment, structural obsolescence within the armed forces, and the deterrent effects of economic constraints, emphasizing that Türkiye cannot meet NATO standards without external assistance. When read together, these documents demonstrate that U.S. decision-making bodies define the same ally from different vantage points: for the NSC, Türkiye's main issue is reliability, whereas for the CIA, it is a matter of insufficient capacity. This

35 CIA Interagency Memorandum "Turkey After the US Arms Cutoff", CIA Records (CREST), CIA-RDP80M01066A001100020011-8, https://www.cia.gov/readingroom/document/cia. accessed, 20.03.2024.
36 Ibid.
37 Ibid.
38 Ibid.
39 Ibid.
40 Ibid.
41 Ibid.

divergence underscores the multifaceted nature of Türkiye's role within the alliance, which cannot be reduced to a single approach.

3. NATO Defense Documents and Türkiye's Concerns (1974–1976)

While U.S. institutional documents emphasize the trust deficit concerning Türkiye, the political costs of the arms embargo, and intelligence vulnerabilities, NATO reports focus more on military capacity and economic constraints. Although these two perspectives employ different terminologies, they converge on the same historical conclusion: Türkiye remains a problematic yet indispensable ally. Consequently, institutional assessments in Washington have confirmed, both politically and militarily, that Türkiye has become a contentious actor within the Western alliance. When the U.S. arms embargo came into effect, NATO documents increasingly emphasized Türkiye's military capacity challenges and dependence on external assistance. The Alliance deemed Türkiye's role in securing the alliance's southeastern flank indispensable, but it explicitly acknowledged that Ankara could not finance this role alone.[42] In this context, a prominent theme in NATO's defense planning documents was the alliance's assessment of Türkiye not merely as an ally but as a "critical infrastructural element" essential for deterrence along the southeastern flank. These documents provide detailed accounts of the degradation observed across all branches of the Turkish Armed Forces due to the embargo and economic constraints. Notable issues included an imbalance between armor and anti-armor capabilities, insufficient maneuverability, and personnel shortages in the Army; limited numbers of modern aircraft and a lack of electronic warfare capabilities in the Air Force; and the designation of over half of the fleet's destroyers as "obsolescent," i.e., functionally outdated, in the Navy.[43]

What distinguishes NATO's approach is that these assessments were not merely presented as a situational analysis. The documents clearly stated that Türkiye would be unable to close these gaps using its own economic resources; the solution was concretized through the concept of "substantial external assistance." Furthermore, it was emphasized that this assistance should not be one-time but rather "continuous, coordinated, and multidimensional." It was also noted that the alliance's other members, international financial institutions, and the U.S. needed to act collectively to support Türkiye.[44] NATO positioned itself not only as a military command structure but also as a "catalyst" responsible for coordinating external assistance.[45]

3.1. DRC/WP/74/2 (1974 Defence Committee Working Paper)

The 1974 study report by NATO's Defence Review Committee (DRC/WP/74/2) provided a comprehensive assessment of Türkiye's force structure and requirements for the period 1975–1980:[46]

- The report emphasized imbalances between armored units and air defense capabilities. The absence of electronic warfare (EW) equipment was noted as a significant factor limiting the effectiveness of the land forces.

42 NATO Defence Planning Committee, DPC/D/76/2: Defence Planning 1976-1980, https://archives.nato.int/nato-defence-planning-1976-1980-turkey, accesed 12.03.2025.
43 NATO Force Planning Document on Turkey, 1973-1982, NATO Archives Online, accessed 12.03.2025.
44 NATO Archives, Defence Planning Committee Report (DPC/D/76/2), https://archives.nato.int/nato-defence-planning-1976-1980-turkey, accessed 12.03.2025.
45 NATO Defence Review Committee, DRC/WP/74/2: Defence Review Committee Working Paper on Turkey (Brussels: NATO Archives, https://archives.nato.int/1975-1980-force-proposals-turkey, accessed 12.03.2025.
46 NATO Defence Review Committee, DRC/WP/74/2: "Defence Review Committee Working Paper on Turkey" https://archives.nato.int/1975-1980-force-proposals-turkey, accessed 12.03.2025, 1974.

- The introduction of F-4 and F-104S aircraft was regarded as a positive development; however, insufficient stocks of ammunition and spare parts were identified as key issues undermining operational effectiveness.
- It was stressed that more than half of the Turkish Navy's fleet consisted of outdated destroyers, and the acquisition of three submarines and six missile boats would only provide a limited increase in deterrence.
- The personnel strength of Category A units within the land forces corresponded to 60–65% of NATO Allied Command Europe (ACE) standards, which was recorded as a serious shortfall in terms of deterrence capability.[47]

The report's most critical emphasis is that it is "impossible" for Türkiye to achieve its force objectives solely with national resources. The document explicitly states that without "substantial external military and economic assistance," the deterrence capability of NATO's southern flank would collapse.[48]

3.2. DPC/D/76/2 (1976 Defence Planning Committee Document)

The Defence Planning Committee Document (DPC/D/76/2), prepared in 1976—while the embargo was still in effect—reassessed Türkiye's position within NATO at a strategic level:[49]

- Türkiye's Strategic Role: Türkiye is described as the "cornerstone of the southern flank against the Soviet Union."
- Economic Insufficiencies: It is emphasized that Türkiye's economic resources are insufficient to meet NATO's force targets.
- Expectations of Allies: The report notes that not only the U.S., but also other allies must also assume responsibility in order for Türkiye to fulfill its obligations.
- Impact of the Embargo: The embargo is said to have weakened not only bilateral relations but also the alliance's overall deterrent capability—this point is explicitly stated in the report.[50]

3.3. Force Planning Documents (1973–1982)

NATO's force planning reports from the 1973–1982 period provided a quantitative assessment of Türkiye's modernization efforts and existing deficiencies:[51]

- Capability Gains: The integration of F-4 Phantom II aircraft into the Turkish Air Force's inventory, coupled with the acquisition of three submarines and six missile boats by the Turkish Navy, represented a marginal but noteworthy enhancement in Türkiye's overall deterrence posture.
- Persistent Deficiencies: More than half of the Turkish Navy's fleet remained composed of obsolete platforms, with continued shortfalls in munitions stockpiles and spare parts availability. Additionally, the absence of robust EW systems

47 Ibid.
48 Ibid.
49 NATO Defence Planning Committee, DPC/D/76/2, https://archives.nato.int/nato-defence-planning-1976-1980-turkey, accessed 12.03.2025.
50 NATO Defence Planning Committee, DPC/D/76/2, https://archives.nato.int/nato-defence-planning-1976-1980-turkey, accessed 12.03.2025.
51 NATO, Force Planning Review, 1973–1982: Country Chapter on Turkey (Brussels: NATO Archives), NATO Archives Online, accessed 12.03.2025.

constituted a critical operational gap, undermining the effectiveness of combined arms operations.

- Force Structure Constraints: The manpower levels within Türkiye's Category A land force units remained substantially below NATO force generation benchmarks, significantly limiting their capacity to contribute to the Alliance's deterrence and defense objectives on the southeastern flank.[52]
- When considered together, these documents and reports reveal a fundamental duality in NATO's approach to Türkiye:
- Türkiye is a "high-cost" ally, requiring continuous external military and economic support.
- Nonetheless, its geographic location renders it indispensable.

Therefore, NATO deemed assistance and support mechanisms essential to prevent Türkiye from drifting away from the alliance and to maintain the deterrence capability of the southeastern flank.

In conclusion, while U.S. documents emphasize the trust deficit regarding Türkiye and the political costs imposed by the embargo, NATO reports focus more technically on military capacity issues and economic constraints. This difference reveals that Washington assesses Türkiye primarily through the lens of a "political reliability problem," whereas Brussels views it as a "military capability gap." Nevertheless, despite the differing terminology, both perspectives point to the same historical conclusion: Türkiye is a problematic yet indispensable ally.

The distinctive contribution of NATO reports lies in their concretization of Türkiye's position within the alliance on a cost–benefit basis. Reports prepared during the period when the U.S. embargo came into effect explicitly noted that the Turkish Armed Forces' modernization needs could not be met through national resources alone and that achieving NATO standards without external assistance was impossible. Thus, institutional assessments within NATO acknowledged Ankara's indispensability in the alliance's southeastern flank while simultaneously affirming that sustaining this role necessitated external support mechanisms.

4. Security Concerns Regarding Türkiye's NATO Commitment and Potential Shift Away from the West in U.S. Institutional Documents

Another notable concern emphasized in these documents pertains to the potential countermeasures Türkiye might undertake following the embargo. Within this framework, Türkiye's possible rapprochement with actors and alliances outside NATO and the Western bloc emerges as a key worry in both the NSSM 227 and CIA reports. Specifically, Iran, Japan, Pakistan, and India were identified as prominent alternative centers of power during that period, and the prospect of Türkiye developing defense procurement relationships with one or more of these countries was viewed as a security risk by the U.S. Consequently, the potential weakening of NATO ties, frustrations over Türkiye's position within the Western alliance, the pursuit of alternative security and defense arrangements, the risk of political isolation, and the turn toward non-Western sources of military supply were all categorized as major security concerns from the U.S. perspective.

52 Ibid.

4.1. The Potential Weakening of Türkiye's NATO Ties

In the NSSM report, it is emphasized that, in the event of a prolonged U.S. arms embargo, Türkiye would conduct a fundamental reassessment of whether it can rely on other Allies as its primary suppliers. The report states as follows:

> *"The Turkish military appears to be pessimistic about its ability to fill its short-term needs from non-US sources. In the future, if the US cut-off is prolonged, Turkey will probably make a basic assessment of whether it can rely on other Allies as its major suppliers. Such an assessment will have major implications for Turkey's future role in NATO—either formally (in terms of steps to loosen its NATO ties) or de facto, by becoming dependent in some significant part on Eastern or other non-NATO sources, such as Iran, Pakistan, or Japan."*[53]

The report further indicates that Türkiye's evaluation in this regard would have "significant consequences" for its future role within NATO. This could manifest either officially, through steps that weaken its NATO ties, or de facto, by becoming substantially dependent on non-NATO sources such as the Eastern Bloc, Iran, Pakistan, or Japan.[54]

This concern essentially reflects the strategic dilemma Türkiye faced during the embargo period. On one hand, Türkiye aimed to remain within NATO and maintain its dependence on the West; on the other hand, it sought alternative sources to meet its immediate needs. After 1975, Türkiye made limited procurement attempts from European allies such as the United Kingdom and Germany; however, these efforts proved insufficient to match the volume and diversity of supplies previously provided by the U.S.[55] Therefore, the possibility of "dependence on non-NATO sources" articulated in NSSM 227 remained a strategic warning within the context of the period, but it also served as a significant indication of how Türkiye's pursuit of alternatives could exacerbate tensions within the Western alliance.

4.2. Türkiye's Disillusionment and the Pursuit of Alternative Security Arrangements

In the long term, Türkiye's disappointment with the U.S. is likely to impact the country's security arrangements, as the NSSM 227 points out:

> *"In the longer term, Turkish disillusionment with the U.S. could intensify a process of basic reappraisal by Turkey of its security arrangements, including a search for new arrangements beyond NATO, possibly including Iran and the Muslim world."*[56]

The statement reflects a deep-seated potential change encompassing both Türkiye's defense supply strategies and its broader security posture. In fact, during the latter half of the 1970s, Türkiye increased its participation in the Organization of Islamic Cooperation (OIC) meetings and sought to revitalize bilateral relations with Iran and Pakistan; however, these initiatives did not evolve into an alternative security architecture to NATO. Consequently, this forecast in NSSM 227 reflects Washington's concerns regarding Türkiye's possible pursuit of options outside the Western alliance. From the U.S. perspective, such a shift was

53 U.S. National Security Council, NSSM 227: U.S. Security Policy Toward Turkey, Box 37, U.S. "Security Policy toward Turkey", The Gerald R. Ford Presidential Library, accessed 20.03.2024.
54 Ibid.
55 George Harris, "Turkey and the U.S. Arms Embargo of 1975–1978," *International Journal of Middle East Studies* 8, no. 4, 1976, s. 413-433; Dankwart A. Rustow, *Turkey: America's Forgotten Ally*, Council on Foreign Relations, New York, 1987, 87-95.
56 U.S. National Security Council, NSSM 227: U.S. Security Policy Toward Turkey, Box 37, U.S. "Security Policy toward Turkey", The Gerald R. Ford Presidential Library, accessed 20.03.2024.

perceived as a strategic threat not only to Türkiye's military procurement preferences but also to the integrity of NATO's southern flank.[57] Undoubtedly, this shift also constitutes a legitimate source of concern for the U.S.

4.3. The Risk of Türkiye's Isolation

Another relevant U.S. institutional document, the CIA report, states that if European allies fail to meet Türkiye's essential military needs, the Turks may interpret this situation as a form of "de facto isolation from NATO," potentially resulting in "inward isolation" and a reversion to "local conservatism".[58] This statement reflects the concern that, in the absence of external assistance, Türkiye may feel isolated, potentially weakening its ties with the West. This assessment indicates a direct correlation between the rising nationalist-conservative discourse in Turkish politics during the mid-1970s and the country's foreign policy orientation.[59] Such a scenario raised concerns not only about Türkiye's potential isolation within NATO but also about the erosion of a Western-aligned identity in the alliance's southern flank. From the U.S. perspective, this possibility signified a risk of weakening in terms of both arms procurement and Türkiye's ideological commitment to the Western alliance.[60]

4.4. Pursuit of Alternative Supply Sources.

In the event that Türkiye fails to compensate for the loss of U.S. supplies through procurement from other NATO allies, it is noted that the country may seek alternative sources of external support—such as from Arab states—although such efforts may ultimately prove insufficient to meet its needs.[61] Although the report does not explicitly mention any country by name, it is evident that Libya was the primary concern. Subsequent developments would reveal that Libya provided a certain level of support to Türkiye during this challenging period.[62]

This situation illustrates, on the one hand, Türkiye's capacity to pursue alternative, non-NATO sources while maintaining its obligatory alliance commitments; on the other hand, it signals a development that could undermine the strategic coherence of the alliance from the U.S.'s perspective.

5. The Contradiction between Bilateral Tensions and Collective Security Commitments (1974–1976)

There are certain contradictions between these documents analyzed in the previous sections. These contradictions are evident in the tensions in bilateral relations between the U.S. and Türkiye and in the Alliance's collective security commitments. The institutional documents produced in the aftermath of the embargo show that Washington and NATO approached their assessments of Türkiye within the same crisis context but through distinctly different conceptual lenses. United States documents foreground the erosion of trust evident in bilateral relations and the strategic implications of this shift, whereas NATO reports focus on how weaknesses in Türkiye's military capacity affected the integrity of the Alliance's southeastern defense.

57 George Harris, "Turkey and the U.S. Arms Embargo of 1975–1978," *International Journal of Middle East Studies* 8, no. 4 1976, 425–426; Dankwart A. Rustow, Turkey: America's Forgotten Ally (New York: Council on Foreign Relations, 1987), 92.

58 CIA Interagency Memorandum: "Turkey After the US Arms Cutoff", accessed 20.03.2024.

59 Feroz Ahmad, *The Turkish Experiment in Democracy, 1950–1975*, London: C. Hurst, 1977, 311-329; Erik J. Zürcher, *Turkey: A Modern History* I.B. Tauris, London, 2004), 243–252.

60 CIA Interagency Memorandum: "Turkey After the US Arms Cutoff", 1975, accessed 20.03.2024.

61 Ibid.

62 Türkiye Gazetesi, "Kıbrıs'ta da Libya ile omuz omuzaydık!", 25.07 2025.

5.1. Contrasting Approaches of the U.S. and NATO

During the Cold War, the U.S. approach to the Cyprus issue was often described as "constructive ambiguity".[63] NATO's southeastern flank occupied a strategically critical position, directly affecting Soviet access to sea and air routes and thus constituting a vulnerable part of U.S. security.[64] This led the U.S. to avoid taking a clear-cut position between its key allies, Türkiye and Greece. Following the 1974 intervention, rising anti-American sentiment in Greece and its withdrawal from NATO's military command temporarily prompted the U.S. to tilt its balance in favor of Türkiye.[65] However, this adjustment reflected not an explicit support for Türkiye, but a pragmatic effort to maintain control over the Alliance's fragile southern flank.[66] When the 1975 NSSM 227, CIA assessments, and NATO's DRC/WP/74/2 (1974) and DPC/D/76/2 (1976) documents are analyzed together, the divergences between U.S. bilateral priorities and NATO's collective security perspectives become clearly evident. The NSSM 227 and the CIA memorandum evaluate Türkiye through a narrower set of institutional priorities, whereas NATO documents operate on a different analytical framework. While Washington conceptualizes Türkiye primarily through the lens of military facility networks (as in the NSC) or capacity shortfalls (as emphasized by the CIA), the DPC/D/76/2 and Force Planning reports prepared in Brussels characterize Türkiye as the keystone of the alliance's southeastern flank.[67] At first glance, this approach may seem paradoxical or contradictory: The U.S. documents predominantly highlight concerns related to trust and capability deficits, while NATO's position reflects a more comprehensive and collective commitment to alliance responsibilities. In this context, the aforementioned divergence gained particular significance in light of the international political developments of 1975. Following the Cyprus crisis, Greece withdrew from NATO's military structure, leaving the southeastern flank vulnerable. Additionally, the increasing naval presence of the Warsaw Pact in the Mediterranean further heightened Türkiye's strategic importance. Consequently, NATO's institutional response framed Türkiye not as a source of problems but rather as an "indispensable partner" whose support was essential for the survival of the southern flank.[68] Therefore, NATO reports have assessed Türkiye within the framework of preserving the integrity of the alliance, moving beyond the debates on reliability and capacity found in the U.S. documents. This enables us to distinguish the priorities of the U.S. and NATO as follows:

- The U.S. Priority: The focus of U.S. documents centers on the erosion of political trust in Türkiye. NSSM 227 characterizes Türkiye as an "unreliable yet indispensable" ally and acknowledges the loss of the "special relationship" nature of bilateral ties.[69]

63 James Key Lindsay, *The Cyprus Problem: What Everyone Needs to Know*, Oxford University Press, 2011, 72-75.
64 William Hale, *Turkish Foreign Policy 1774-2000*, Frank Cass, London, 2000, 140-146, *Theodore A. Couloumbis, The United States, Greece, and Turkey: The Troubled Triangle,* Praeger, New York: 1983, 78-82.
65 George Harris, "Turkey and the United States: The Arms Embargo, 1974-1978", *International Journal of Middle East Studies,* no.4, 1976, 417-420, Tozun Bahcheli, *Greek-Turkish Relations Since 1955*, Westview Press, Boulder, 1990, 122-130.
66 Foreign Relations of the U.S. (FRUS), 1969-1976, Vol. XXX, Greece; Cyprus; Turkey, Document 68, August 14, 1974, 223-228, William Mallinson, *Kissinger and Invasion of Cyprus,* Cambridge Scholars Publishing, Newcastle, 2016, 59-61; Süha Bölükbaşı, *The Superpowers and the Third World: Turkish-American Relations and the Cyprus Issue,* University Press of America, Lanham, 1988, 112-115.
67 NATO Defence Review Committee, DRC/WP/74/2: Defence Review Committee Working Paper on Turkey Brussels: NATO Archives, 1974, https://archives.nato.int/1975-1980-force-proposals-turkey, accessed 12.03.2025.
68 NATO Defence Review Committee, DRC/WP/74/2: Defence Review Committee Working Paper on Turkey Brussels: NATO Archives, 1974, https://archives.nato.int/1975-1980-force-proposals-turkey, accessed 12.03.2025.
69 U.S. National Security Council, Box 125, Folder "Turkey (1)" of the Ron Nessen Papers at the Gerald R. Ford Presidential Library, 20.03.2024.

- NATO's Priority: NATO documents focus on Türkiye's military capability gaps and economic dependency. The reports emphasize that the modernization requirements exceed Türkiye's economic capacity and that deterrence would collapse without external assistance.[70]

When examined together, the U.S. and NATO documents reveal that differing institutional priorities ultimately point to the same strategic conclusion. While Washington characterized Türkiye as a politically unreliable ally, Brussels emphasized Türkiye's capability deficits and dependence on external assistance. Nevertheless, both the U.S. and NATO, despite employing distinct terminology and conceptual frameworks, acknowledged that Türkiye's departure from the alliance was inconceivable. Consequently, in the post-embargo period, Türkiye was no longer regarded as a "special ally" by the West but rather as a "compelled partner" despite its challenges.

5.2. Base Facilities Issue

NSSM 227 systematically prioritized the U.S. military bases in Türkiye according to their strategic importance, characterizing Ankara primarily as a "network of facilities." Within this framework, İncirlik Air Base was designated as "of critical priority," while the installations in İzmir and Ankara were classified as "of secondary importance." Smaller radar and communication sites were noted as "capable of being closed if necessary".[71] This assessment demonstrates that, beyond the political reliability debates in Washington's perspective on Türkiye, the fundamental determining factor was the bases and logistical lines. In other words, Türkiye's strategic value was measured by its critical geographical location that enabled the operational infrastructure of the alliance.

NATO documents adopt a distinct analytical framework by positioning Türkiye within the cohesive structure of the alliance's southern flank. The DPC/D/76/2 report specifically names Türkiye as a pivotal component in the southeastern defense posture vis-à-vis the Soviet Union. It also points out that Türkiye's military capacity deficiencies and economic limitations necessitate collective support from the alliance to effectively fulfill this function. Consequently, whereas the U.S. perspective predominantly evaluates Türkiye in terms of its bases and facilities, the institutional discourse within Brussels centers on Türkiye's integral role within the comprehensive deterrence architecture of NATO.[72]

5.3. Impact of the Embargo: Efforts to Alleviate Bilateral Strains within the NATO Framework

While the embargo triggered a severe crisis of confidence in U.S.-Türkiye relations, NATO's collective documents addressed the situation in a more conciliatory tone. The U.S. employed the embargo as a tool to exert pressure on Türkiye, whereas NATO acknowledged that the embargo weakened the alliance's deterrence and emphasized the necessity of compensation mechanisms.[73]

In this context, while the embargo reflected a severe crisis of confidence in U.S.–Türkiye relations, NATO's collective documents addressed the situation in a more conciliatory tone. Undoubtedly, the U.S. employed the embargo as an instrument of political pressure

70 NATO Defence Review Committee, DRC/WP/74/2: Defence Review Committee Working Paper on Turkey Brussels: NATO Archives, 1974, https://archives.nato.int/1975-1980-force-proposals-turkey, accessed 20.03.2025.
71 Ibid.
72 NATO Defence Review Committee, DRC/WP/74/2: Defence Review Committee Working Paper on Turkey Brussels: NATO Archives, https://archives.nato.int/1975-1980-force-proposals-turkey, accessed 12.03.2025.
73 Ibid.

against Türkiye; however, NATO acknowledged the detrimental impact of the embargo on the alliance's deterrence capability and consequently advocated for compensatory support mechanisms. This divergence in approach was largely shaped by the withdrawal of Greece from NATO's military flank in 1975 and the increasing Soviet naval presence in the Mediterranean. While the U.S. pursued political negotiation strategies with Türkiye, NATO prioritized burden-sharing and appeals for assistance to prevent Türkiye's estrangement from the alliance. Based on the reviewed documents, Türkiye's position within the Western alliance has been characterized as follows:

- From the U.S. perspective: Unreliable yet indispensable.
- From NATO's perspective: Dependent on external assistance yet critical.

Although these two definitions stem from distinct institutional frameworks, their convergence reveals Türkiye's repositioning within the framework of a "compelled partnership". Ultimately, starting in 1975, the understanding of a "compelled partnership" supplanted the "special relationship" that prevailed between 1947 and 1974. The U.S. policies aimed at managing the security crisis, together with NATO's collective support mechanisms, operated in tandem to prevent Türkiye's disengagement from the alliance, yet they simultaneously entrenched the persistence of the trust deficit.[74]

The reports examined reveal that the embargo not only harmed Türkiye but also directly undermined U.S. interests. From Washington's perspective, the issue had transcended mere pressure on Ankara; the weakening of deterrence in NATO's southeastern flank and the possibility of Türkiye drawing closer to Moscow rendered the embargo unsustainable. Consequently, lifting the embargo was not a concession granted to Türkiye but rather a measure to safeguard U.S. national interests. Indeed, American documents from the period contained warnings that should the embargo persist, the question, "Who lost Türkiye?" would inevitably arise in the future.[75] This statement clearly demonstrates that Washington was, in fact, unwilling to risk losing Türkiye from the alliance.

Conclusion

The 1974 Cyprus Operation and the subsequent U.S. arms embargo caused a profound rupture in Turkish-American relations, a fracture that was also reflected in NATO's defense planning documents. The examined documents demonstrate how this period redefined Türkiye's position within the Western alliance.

The first of these documents, NSSM 227, characterizes Türkiye as an actor whose reliability has become questionable, while simultaneously emphasizing the indispensability of its bases and geographical position. The CIA's 1975 Interagency Memorandum documents the direct military consequences of the embargo: a shortage of modern equipment, imbalances in stock levels, and inflation eroding the defense budget. The report explicitly states that without external assistance, Türkiye's deterrence capability would rapidly deteriorate. NATO documents provide detailed records of deficiencies in the land, air, and naval forces. In particular, it is noted that more than half of the naval vessels were "obsolescent", the ground forces fell significantly below ACE standards, and economic constraints hindered the achievement of set objectives.

74 Dankwart A. Rustow, *Turkey: America's Forgotten Ally,* Council on Foreign Relations, New York: 1987, 112.
75 James F. Goode, *The Turkish Arms Embargo: Drugs, Ethnic Lobbies, and US Domestic Politics Studies in Conflict, Diplomacy, and Peace,* University Press of Kentucky, 2020, 106-110.

Despite differing institutional priorities, the documents collectively portray a consistent picture. Internal U.S. institutional reports record Türkiye as a strategically indispensable yet reliability-challenged ally, while NATO reports emphasize military capacity deficiencies and dependence on external assistance. The CIA report bridges these two narratives by revealing both the short-term military impacts and the long-term strategic consequences of the embargo. Another implicit insight gleaned from these documents is how the embargo, initially used as a tool to exert pressure on Türkiye, quickly produced counterproductive effects. From Washington's perspective, the issue shifted from imposing costs on Ankara to avoiding the risk of losing Türkiye altogether. As confirmed by NATO reports, the weakening of the southeastern flank eroded deterrence against the Soviet Union, demonstrating that continued embargo enforcement would ultimately harm U.S. interests themselves. These concerns emerged in American documents of the period not merely as a possibility but as a historic warning delineating the limits of embargo policy.

In this context, the documents from the period 1974–1980 reveal a profound redefinition of Türkiye's position within the Western alliance. Reports from Washington's institutions characterized Ankara as a politically unreliable actor, while NATO documents portrayed Türkiye as an ally that needed external support due to its capacity deficiencies and economic constraints. Although originating from different institutional priorities, these assessments ultimately converge on the same conclusion: despite its challenges, Türkiye remains indispensable. This finding elevates the period beyond a mere diplomatic crisis or issue, marking it as a critical juncture in the Cold War during which Türkiye's role within the alliance was fundamentally reassessed through official documentation.

Conflict of Interest Statement:

The author declares that there is no conflict of interest.

AI Usage Statement

No artificial intelligence applications were used in this study.

References

Published Works

AHMAD Feroz (1977). *The Turkish Experiment in Democracy,* 1950–1975, Westview Press, Boulder.

AKDUMAN Birol (2021). "NATO's Southern Flank: The Evolution of Türkiye's Strategic Role and Its Implications for Regional Security", *İnsan ve Toplum Bilimleri Araştırmaları Dergisi,* 12:5, 2951-2968.

ATMACA Ayşe Ömür (2025). "The Alliance in the Storm: Geopolitical Representation of the United States in the Turkish Parliament during Détente", *All Azimuth,* 14:1, 107-119.

BAHCHELI Tozun (1990). *Greek-Turkish Relations Since 1955,* Westview Press, Boulder.

BAŞLAMIŞLI Macide (2021). "ABD'nin Türkiye'ye Yönelik Ambargo Kararına İlişkin Haşhaş Sorunu Yerine 1974 Kıbrıs Krizini Ön Plana Çıkarma Girişimi," *Asia Minor Studies,* 9:1, 695-712.

BÖLÜKBAŞI Süha (1988). *The Superpowers and the Third World: Turkish-American Relations and the Cyprus Issue*, University Press of America, Lanham.

COULOUMBIS Theodore A. (1983). *The United States, Greece, and Turkey: The Troubled Triangle*, Praeger, New York.

GOODE James F. (2020). *The Turkish Arms Embargo: Drugs, Ethnic Lobbies, and US Domestic Politics. Studies in Conflict, Diplomacy, and Peace*, University Press of Kentucky, Kentucky.

GÜVENÇ Serhat and ÖZEL Soli (2012). "NATO and Turkey in the post-Cold War World: Between Abandonment and Entrapment", *Southeast European and Black Sea Studies*, 12:4, 533-553.

HALE William (2000). *Turkish Foreign Policy since 1774*, Routledge, London.

HARRIS, George S. (1972). *Troubled Alliance: Turkish-American Problems in Historical Perspective, 1945–1971*, American Enterprise Institute, Washington, D.C.

HARRIS George S. (1976). "The Arms Embargo and Turkey," *Middle East Journal,* 30:2, 129-143.

KER-LINDSAY James (2011). *The Cyprus Problem: What Everyone Needs to Know*, Oxford University Press, Oxford.

LEFFLER Melvyn P. (2007). *For the Soul of Mankind: The United States, the Soviet Union, and the Cold War*, Hill and Wang, New York.

MALLINSON William (2016). *Kissinger and the Invasion of Cyprus: Diplomacy in the Eastern Mediterranean*, Newcastle upon Tyne: Cambridge Scholars Publishing, Newcastle.

RUSTOW Dankwart A. (1987). *Turkey: America's Forgotten Ally. Council on Foreign Relations,* New York.

SANDER Oral (1998). Türk-Amerikan İlişkileri. İmge Kitabevi Yayınları, Ankara.

SCHIMMELFENNIG Frank (2018). *NATO and the European Security Order: History, Theory, and Practice,* Routledge, London.

Internet Sources

Central Intelligence Agency (CIA) (1975). "Turkey After the US Arms Cutoff" Interagency Memorandum, CIA Records (CREST), https://www.cia.gov/readingroom/document/cia, accessed 20.03.2024.

NARA (1975). "Turkey (1)," Box 125, July 25, The Ron Nessen Papers, Gerald R. Ford Presidential Library National Archives | Home, www.fordlibrarymuseum.gov/digital-research-room, accessed 20.03.2024.

National Security Council (1975). NSSM 227: U.S. Security Policy Toward Turkey, Box 37, Gerald R. Ford Presidential Library National Archives,www.fordlibrarymuseum.gov/sites/default/files/pdf_documents/library/document accessed 20.03.2024.

NATO Defence Planning Committee (1976). DPC/D/76/2: "Defence Planning 1976–1980", https://archives.nato.int/nato-defence-planning-1976-1980-turkey, accessed 12.03.2025.

NATO Defence Review Committee (1974). DRC/WP/74/2: "Defence Review Committee Working Paper on Turkey". Brussels: NATO Archives, https://archives.nato.int/1975-1980-force-proposals-turkey, accessed 12.03.2025.

NATO Defence Review Committee (1973). Force Planning Country Study: Turkey, 1973–1982, s. 15, NATO Archives Online, accessed 12.03.2025.

U.S. Congress (1975). Congressional Record, 94th Congress, House of Representatives, 142. https://www.congress.gov/bill/94th-congress/house, accessed 20.03.2024.

U.S. Department of State (2007). "Minutes of the Washington Special Actions Group Meeting," 14 Aug. 1974, Foreign Relations of the United States, 1969–1976, Vol. XXX, Greece; Cyprus; Turkey. Washington, D.C.: Government Printing Office, accessed 18.11.2025.

GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 373-394
DOI: 10.17752/guvenlikstrtj.1746003

Araştırma Makalesi
Research Article

Çözümü Zor Bir Çatışma Olarak Boko Haram Sorunu

The Boko Haram Issue as an Intractable Conflict

Melike EKİZ KILIÇ*

Zekeriyya AKDAĞ**

Öz

Radikal İslamcı bir hareket olarak ortaya çıkan Boko Haram örgütü, sadece Nijerya'nın değil, aynı zamanda diğer bölge ülkelerinin de karşılaştığı ciddi bir güvenlik tehdidini oluşturmaktadır. Örgütün dinin radikal bir yorumuna dayanan ideolojisi, sivillere yönelik şiddet eylemleri ve bölgesel yayılma kapasitesi hem ulusal hem de uluslararası düzeyde kaygı yaratmaktadır. Boko Haram yerel veya uluslararası basında yüzeysel bir şekilde değerlendirilerek İslami terörizmin bir diğer örneği olarak yansıtılmaktadır. Bu çalışma, Boko Haram sorununun neden çözümü zor çatışmalar arasında değerlendirilmesi gerektiğini ortaya koymayı amaçlamaktadır. Bu çalışmada, Boko Haram'ın ortaya çıkışı ve yükselişinde sadece dini radikalizmin değil siyasal, ekonomik ve toplumsal faktörlerin bir araya gelmesiyle oluşan çok boyutlu bir kimliksel krizin etkili olduğu iddia edilmektedir. Toplumsal entegrasyonun tam olarak sağlanamadığı Nijerya'da Boko Haram'ın yol açtığı çatışma, köklü toplumsal eşitsizlikler, kimlik temelli gerilimler ve karşılıklı güvensizlik gibi nedenler dolayısıyla çözümü zor çatışma haline gelmiş bulunmaktadır.

Anahtar Kelimeler: Boko Haram, Nijerya, Çatışma, Çözümü Zor Çatışma, Batı Afrika

Abstract

Boko Haram, which emerged as a radical Islamist movement, poses a serious security threat not only to Nigeria but also to other countries in the region. Its ideology based on a radical interpretation of religion, its acts of violence against civilians, and its regional expansion capacity raise concerns at both national and international levels. The local and international press assess Boko Haram superficially, portraying it as another example of Islamic terrorism. This study aims to reveal why the Boko Haram issue should be considered as one of the intractable conflicts. It also argues that the emergence and rise of Boko Haram is not only driven by religious radicalism but also by a multidimensional identity crisis formed as a combination of political, economic, and social factors. In Nigeria, where full social integration has not been achieved, the conflict caused by Boko Haram has become an intractable one due to deep-rooted social inequalities, identity-based tensions, and mutual distrust.

Keywords: Boko Haram, Nigeria, Conflict, Intractable Conflict, West Africa

* Doktora Öğrencisi, İnönü Üniversitesi, Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Uluslararası İlişkiler Ana Bilim Dalı, Malatya, Türkiye, e-posta: melikeekiz8@gmail.com ORCID: 0009-0008-7179-131X

** Dr. Öğr. Üyesi, İnönü Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, Malatya, Türkiye, e-posta: zekeriyya.akdag@inonu.edu.tr ORCID: 0000-0002-0866-603X

Geliş Tarihi / Submitted: 18.07.2025

Kabul Tarihi / Accepted: 13.11.2025

Extended Abstract

This study aims to move beyond a narrow focus on religious radicalism to evaluate the rise of Boko Haram as a multidimensional crisis rooted in a confluence of political, economic, and social factors. Within this framework, the study analyzes the underlying dynamics of Boko Haram's opposition to Nigeria's existing state structure and social order, evaluates counter-strategies employed by the Nigerian government, regional states, and the international community, and explores why it should be classified as intractable.

Founded in the 2000s, Boko Haram is a group that employs violence against the Federal Republic of Nigeria and its civilians, predicated on a radical theological interpretation. The failure of Nigeria's post-colonial adoption of Western political and institutional structures to deliver widespread prosperity generated profound distrust of state authority, particularly in the Muslim-majority northern regions. The economic, social, and cultural disparities between the relatively more prosperous south and the marginalized north facilitated the establishment of Boko Haram's social base. The group successfully exploited the resulting social discontent by channeling opposition to Western-style education, institutions, and culture into an ideological discourse, thereby expanding its base.

Intractable conflicts generally arise in underdeveloped countries and places where the state structure is weak. Similarly, Boko Haram emerged in Nigeria, where nation-building has not been fully achieved as a result of social tensions chronicled by its colonial past. In a country with deep social divisions and incomplete institutionalization, Boko Haram had no difficulty finding a base, and the organization's violent actions led to a further weakening of the state structure. Boko Haram's excessive acts of violence have created deep divisions by generating feelings of anger, victimization, and desire for revenge among social groups with significant ethnic and religious differences. Its harsh acts of violence have eliminated the basis for social reconciliation, turning competition between different social groups, particularly Muslims and Christians, into hostility, rendering existing problems unsolvable.

Since 2009, Boko Haram has carried out large-scale terrorist attacks within Nigeria's borders and then expanded its activities to neighboring countries. Over time, it transformed from a local threat into a regional security problem. The fact that Boko Haram has found a base in other countries of the region and has been able to form networks and carry out actions has caused the problem to become more complex and difficult to solve. The spread of the conflict beyond Nigeria's borders to neighboring countries such as Cameroon, Niger, and Chad has turned the problem into a regional one. The group has significantly complicated the security landscape by establishing bases, forming transnational networks, and executing cross-border operations within the region. This regional spread is a classic example of how protracted conflicts evolve, reproduce their structural complexities, and become increasingly difficult to resolve.

Although there have been many peace talks attempted between the Nigerian government and Boko Haram at various times, these initiatives have failed without addressing the underlying structural and social problems. Peaceful resolution of conflicts requires mutual trust. When parties distrust each other, they become unwilling to take any steps toward a solution. In the Boko Haram case, there is a deep mistrust between the parties. In situations of mutual distrust, the role of third parties as mediators can be a facilitating factor. In the crisis of the Chibok schoolgirls kidnapping, the intervention of third parties has led to some successes, albeit partial. However, there is no power that can exert pressure on both sides of the conflict to resolve the issue. The government forces largely view the issue

as a security problem and therefore do not implement comprehensive reforms, which, in turn, makes resolving it more difficult.

The Boko Haram issue contains fundamental elements such as structural inequality, denial of identity, and political exclusion, as defined by Edward Azar in relation to "Protracted Social Conflict (PSC)". In northern Nigeria, where sectarian and ethnic divisions are asserted and income inequality is deepening, essential human needs such as security, recognition, and acceptance of identity have not been met. These conditions have facilitated the organization's establishment of a social base, while the government's approach to conflict management, which relies on power-based and temporary measures without addressing the underlying issues, has contributed to the prolongation of the conflict.

Furthermore, in line with Louis Kriesberg's definition of intractable conflict, Boko Haram possesses a destructive, long-standing structure that resists resolution. Boko Haram adopts a strong identity-centered stance, viewing itself as the representative of "true" Islamic values and defining the Western-oriented state and other religious communities as heretical or hostile. This claim of ideological superiority legitimizes exclusionary and violent actions, which, in turn, deepens the conflict's intractability.

Giriş

Dinin radikal bir yorumunu referans alan Boko Haram, Nijerya Hükümetini ve sivilleri hedef alan eylemler gerçekleştirmektedir. Eylem kapasitesi giderek artıran Boko Haram sadece Nijerya için değil Batı Afrika bölgesi için ciddi bir güvenlik tehdidi oluşturmaktadır. Boko Haram örgütünün ayrım gözetmeksizin sivilleri öldürmesi, kız çocukları dahil sivilleri rehin alması ve ibadethanelere zarar vermesi gibi eylemleri derin bir endişe yaratmaktadır. Boko Haram'ın Nijerya ve Batı Afrika bölgesindeki yıkıcı faaliyetleri, bölgenin karşılaştığı güvenlik tehditlerinden birini oluşturduğundan konunun detaylı ele alınması önem arz etmektedir.

Boko Haram genel olarak basitçe İslami terörizmin bir diğer örneği olarak değerlendirilmektedir. Bu çalışma Boko Haram'ın sadece dini kullanan bir terör örgütü olarak değerlendirilmesinin eksik olduğunu ortaya koymayı amaçlamaktadır. Çalışmanın amacı, Boko Haram'ın yükselişini yalnızca dini radikalizm bağlamında değil, siyasal, ekonomik ve toplumsal faktörlerin bir araya gelmesiyle oluşan çok boyutlu bir kriz olarak değerlendirmektir. Çalışmada esas olarak, Boko Haram'ın yol açtığı çatışmaların neden çözümü zor çatışmalar arasında değerlendirilmesi gerektiği sorusuna cevap aranmaktadır.

Bu çalışma, Boko Haram'ın yükselişinin yalnızca dini nedenlerle açıklanamayacağını iddia etmektedir. Örgütün oluşumu ve sürekliliği, kuzey Nijerya'da sömürge döneminden miras kalan toplumsal eşitsizlikler, siyasi dışlanmışlık, yoksulluk ve merkezi otoritenin yetersizliği gibi etkenlerin birleşimiyle mümkün olmuştur. Bölgesel ölçekte varlığını sürdüren Boko Haram sorunu sahip olduğu özellikler bakımından çözümü zor çatışmalar arasında değerlendirilebilir.

Çalışmanın ilk kısmında çözümü zor çatışmalar ile ilgili teorik tartışmalara yer verilmektedir. Sonrasında Boko Haram'ın kuruluş süreci ve ideolojik yapısı ele alınmaktadır. Ardından Boko Haram örgütünün Nijerya ve bölge ülkelerde gerçekleştirdiği faaliyetler ve şiddet eylemleri incelenmektedir. Sonrasında Nijerya hükümeti, komşu ülkeler ve uluslararası aktörlerin örgüt ile mücadelesi ele alınmaktadır. Son olarak da Boko Haram örgütü ile gerçekleştirilmeye çalışılan barış görüşmelerine değinilmektedir.

Bu çalışmada analiz yöntemi olarak nitel araştırma yöntemi benimsenmiştir. Bu çerçevede, Boko Haram'ın yol açtığı güvensizlik, düşmanlık ve bölgesel yayılma gibi faktörlerin çatışmanın uzamasına olan katkısı, çözümü zor çatışmalara dair teorik çerçeveler ışığında açıklanmaya çalışılmıştır. Kaynak toplama süreci sistematik literatür taraması yöntemiyle yürütülmüştür. Veri analizi sürecinde nitel içerik analizi temel yöntem olarak kullanılmıştır. Kaynaklarda yer alan olay anlatımları, aktörlerin tutumları ve söylemleri kimlik, güvenlik ve meşruiyet kavramları çerçevesinde analiz edilmiştir. Özellikle Boko Haram'ın önde gelen liderlerinin çeşitli medya kuruluşlarında yer alan söylemleri, çalışmanın teorik çerçevesiyle irtibatlandırılarak analiz edilmiştir.

Çalışmada akademik veri tabanları, uluslararası düşünce kuruluşlarının raporları ve Birleşmiş Milletler'e bağlı kuruluşlar gibi uluslararası kuruluşlar tarafından hazırlanan raporlardan yararlanılmıştır. Medya kaynaklarından yararlanılırken tek taraflılığı önlemek ve çeşitliliği sağlamaya özen göstererek yalnızca Batılı değil, aynı zamanda Batı dışı ve Afrika merkezli medya kaynaklarından da yararlanılmıştır. Kaynak türleri açısından, doğrulanabilirlik ve analitik derinlik sağlamaları nedeniyle uluslararası kuruluş raporları ve resmî açıklamalar birincil, akademik makaleler ve kitaplar ise ikincil kaynaklar olarak değerlendirilmiştir.

1. Çözümü Zor Çatışma Nedir?

Çatışma, rekabetçi bir ortamda iki veya daha fazla taraf arasındaki amaçlı etkileşimden kaynaklanır.[1] Çatışmalar doğası gereği şiddetlidir. İnsani krizlere dönüşebilir, insan kayıpları yaşanır ve maddi-manevi hasara neden olabilir.[2] Birçok çatışma teorisyeni, şiddet gibi ağır çekişmeli davranışların diğer tarafın ahlaki olarak dışlanmasıyla teşvik edildiğine inanmaktadır.[3]

Uzun süreli sosyal çatışmalar (*Protracted Social Conflicts*, PSC) literatüründe büyük bir öneme sahip olan Edward Azar, 1970'li yılların sonlarına doğru şiddetli ve sürekli çatışmayı ortaya çıkaran dinamiklere ilişkin anlayışını sistematik olarak geliştirmiştir. 1990'ların başındaki yazılarında bu *"yeni tür çatışmanın"* altmıştan fazla örneğini tanımlamıştır. Belki de on beş yıllık çalışmanın en özlü özeti olan *The Management of Protracted Social Conflicts: Theory and Cases* isimli eseri, bu literatürün kurucu metni niteliğindedir.[4] Uzun süreli sosyal çatışmalar çoğunlukla ekonomik olarak az gelişmiş ve geri kalmış toplumlarda ortaya çıkmakta ve gelişmektedir. Terörizm, bu anlaşmazlıkların çoğunda bulunan bir özelliktir. Bu tür çatışmalar kolaylıkla komşu ülkelere yayılmaktadır. Büyük bölgesel ve uluslararası güçler de soruna bir şekilde dahil olmaktadırlar. Günümüz dünyasında yaşanan silahlı çatışmaların birçoğu, kültürel olarak farklı toplumsal gruplara karşı ayrımcılığın yaşandığı ve ekonomik kalkınmanın çarpık olduğu toplumlarda yaşanır. Zayıf devletler ve son derece farklılaşmış toplumsal grupları barındıran devletler çatışmaya davetiye çıkarmaktadır. Az gelişmişlik genel olarak çatışmanın daha da derinleşmesine yol açmaktadır.[5] Çatışmalı ortam ise toplumsal gelişmeyi daha da sekteye uğratarak kısır bir döngü yaratmaktadır.

1 Anthony Oberschall, "Theories of Social Conflict", *Annual Review of Sociology*, 4, 1978, s. 291.
2 Rastislav Kazansky, "The Conflict Theory as a Pillar of Security Science", *Security Science Journal*, 1:2, 2020, s. 33-36.
3 Dean G. Pruitt, "Some Research Frontiers in the Study of Conflict and its Resolution", Morton Deutsch ve Peter T. Coleman (ed.), *The Handbook of Conflict Resolution: Theory and Practice*, Jossey-Bass Publishers, San Francisco, 2014, s. 853.
4 Hugh Miall, Oliver Ramsbotham ve Tom Woodhouse, *Contemporary Conflict Resolution: The Prevention, Management and Transformation of Deadly Conflicts*, Polity Press, Malden, 1999, s. 72.
5 Edward E. Azar, "The Analysis and Management of Protracted Conflict", Vamık D. Volkan, Joseph V. Montville ve Demetrios A. Julius (ed.), *The Psychodynamics of International Relationships, Volume II: Unofficial Diplomacy at Work*, Lexington Books, Massachusetts/Toronto, 1991, s. 93-94.

Kültürel, psikolojik, ekonomik veya politik kaygılar nedeniyle ortaya çıkan uzun süreli sosyal çatışmalar, uzun yıllar boyunca devam eden düşmanca etkileşimlerdir. Bu tür çatışmaların belirli bir sonlanma noktaları yoktur ve açık bir karar ile sona ermeleri beklenemez. Sosyo- etnik çatışmalar, dahil olan aktörlerin sayısı, çatışma ortamını sürdüren hedefler ve amaçlar açısından güçlü bir büyüme kapasitesi göstererek uzun süreli çatışmalar olma eğilimdedir. Uzun süren çatışma durumunda çatışma, sorunları çözmenin bir aracı olmaktan ziyade yeniden tanımlama alanı haline gelir; bu nedenle nihai bir çözüm yolu bulmak zordur.[6] Bu tür çatışmalar toplumsal grupların güvenlik, kabul görme, tanınma, siyasi kurumlara adil erişim ve ekonomik katılım gibi temel ihtiyaçların karşılanması için verilen şiddetli mücadelelerdir. Genellikle toplumsal gruplar ve devlet arasındaymış gibi kabul edilir ancak durum her zaman böyle değildir. Uzun süreli sosyal çatışmalardan muztarip toplumlarda devlet mekanizması genellikle tek bir etnik ya da dini grup tarafından kontrol edilir.[7]

Zayıf devletler ve birbirinden son derece farklılaşmış toplumlar çatışmaya davetiye çıkarır ve az gelişmişlik çatışmaların süreklilik arz etmesine zemin hazırlar. Ulusal bütünleşmenin sağlanamadığı, kurumsal inşanın gerçekleşemediği ve dolayısıyla toplumsal farklılaşmanın büyük oranda devam ettiği ülkelerde devlet *"dürüst bir arabulucu"* olarak hareket etmede başarısız olur.[8] Sömürge sonrası toplumsal farklılıkların büyük oranda derinleşerek devam ettiği toplumlarda devlet mekanizması, toplumun genelinin ihtiyaçlarına yanıt veremeyen dar bir kesim tarafından yönetilir. Bu da toplumsal yapıyı zorlayarak sonunda parçalanmaya ve uzun süreli sosyal çatışmaya yol açar.[9] Azar'a göre uzun süren toplumsal çatışmaların tipik özellikleri vardır. Bu çatışmalar ekonomik ve teknolojik bakımdan geri kalmışlık ve bütünleşememiş sosyal ve politik sistemler gibi özelliklere sahiptirler. Azar'a göre şu özellikler bu tür çatışmaların alt yapısı oluşturur: Çok etnikli mezhepsel ayrışmalar ve parçalanmalar, az gelişmişlik ve dağıtım adaletsizliği. Aynı zamanda Azar'a göre uzun süren toplumsal çatışmaların kaynağı tüm insanların gelişiminde zorunlu ihtiyaç olan unsurların reddedilmesidir. Bunlar güvenlik, ayırt edici kimlik, kimliğin toplumsal olarak tanınması, güvenlik ve kimlik koşullarını belirleyen süreçlere etkin katılım ile diğer bu tür gelişimsel gerekliliklerdir. Uzun süreli sosyal çatışmalar siyasi sürece dahil olan tarafların ayrı kimliklerinin reddedilmesi, kültürel ve değerli ilişkiler güvenliğinin olmaması ve mağduriyetin giderileceği etkili siyasal katılımın olmaması gibi algılanan mağduriyet koşullarıyla mücadele girişimlerinden kaynaklanan durumlardır.[10]

Çatışmalara çözüm bulmada çatışmanın ardında yatan esas meselelerin belirlenmesi ve ele alınması büyük önem arz etmektedir. Müzakerelerde çatışmanın temelindeki konulara değinmeyen antlaşmalar kalıcı olmamaktadır. İş birliğine dair yüzeysel çabalar, uzun süren toplumsal çatışmaları azaltmak için yeterli olmamaktadır. Gerilimi azaltmak için alınan önlemler çatışmayı kısa vadede daha katlanılabilir hale getirebilir fakat çatışma çözümü, çatışma yönetiminden daha karmaşık bir sürece sahiptir.[11]

Louis Kriesberg'e göre çözümsüz çatışmalar üç temel özelliğe sahiptir. İlk olarak çözümsüz çatışmalar uzun süre devam eder. İkincisi rakiplerin yıkıcı olarak gördüğü

6 Edward E. Azar, Paul Jureidini ve Ronald McLaurin, "Protracted Social Conflict; Theory and Practice in the Middle East", *Journal of Palestine Studies*, 8:1, 1978, s. 50-51.
7 Azar, "The Analysis and Management of Protracted Conflict", s. 93-94.
8 Age, s. 94.
9 Miall, Ramsbotham ve Woodhouse*, Contemporary Conflict Resolution*, s. 73.
10 Edward E. Azar, "Protracted International Conflicts: Ten Propositions", Edward E. Azar ve John W. Burton (ed.), *International Conflict Resolution: Theory and Practice,* Wheatsheaf Books*;* Sussex, 1986, s. 28-30.
11 Age, s. 31.

şekillerde gerçekleşir. Üçüncüsü ise taraflar veya arabulucular çatışmayı sonlandırmaya veya dönüştürmeye çalışsalar da başarısız olur. Ancak çatışma çözümsüzlüğü sabit bir özellik değildir. Çatışmalar uzun ve yıkıcıysa, onları sona erdirme veya dönüştürme çabaları muhtemeldir ve bu çabaların başarısızlığı, çatışmaların *"çözümsüz"* olarak nitelendirilmesine katkıda bulunur. Bu tür çatışmalarda bir grubun üyeleri kendi gruplarını, diğerlerinden birçok yönde daha iyi görme eğilimdedir. Bunun sonucunda etnosentrizm oluşur. Bu eğilimler diğer grupların *"aşağı"* olarak görülmesine ve bu doğrultuda muamele edilmesine sebep olur. Dolayısıyla taraflar arasında bu şekilde var olan ilişki süreci çözümsüz çatışmalara yol açar.[12] Bir çatışma çözülemez hale geldiğinde tarafların çatışmayı algılama biçiminde temel bir değişiklik gereklidir. Aynı zamanda temel ihtiyaçlar karşılandığında çözüme doğru hareket mümkün olabilir.[13] Temel insani ihtiyaçlar olan kimlik, güvenlik, hayatta kalma gibi ihtiyaçların reddedilmesi çözümsüz çatışmalara yol açar, ancak bu ihtiyaçların karşılanması ile çatışmalar sona erebilir.[14] Çözümü zor çatışmaların uzamasının sebebi, altta yatan sorunları ele almadan geçici çözümlere yönelmektir. Eş zamanlı analitik ve kolaylaştırılmış bir çatışma, çözüm süreci olmadığında geleneksel barışı koruma uygulamaları çatışmayı kurumsallaştırma eğilimdedir. Güç aracılığıyla barış, yaşam biçiminin bir parçası haline gelir ve herhangi bir çözümü daha da zorlaştırır.[15]

Uzun yıllar boyunca devam eden çözümü zor çatışmalar yapıcı bir şekilde çözmeye yönelik her girişime direnir. Bireyler, gruplar veya uluslar arasında ortaya çıkabilir. Zamanla birçok tarafın katılımını kendine çekme, daha karmaşık bir hal alma ve diğer insanlara karşı bir tehdit oluşturma eğilimdedirler. İlgili taraflar birbirlerini hor görerek karşılıklı olarak yabancılaşırlar. Çözümü zor çatışmalar, yirmi yıl ve daha fazla süren çatışmalar için kullanılır.[16]

Çözümü zor çatışmalar şiddetlidirler, çözümsüz olarak algılanırlar ve toplum üyelerinin her birini ilgilendirir. Bu tür çatışmaların varlığının ve varlığını sürdürebilmesinin temel nedenlerinden biri, toplumsal hafıza ve çatışma ahlakına dair toplumsal inançların ve kolektif duygusal yönelimlerin hakim olduğu gelişmiş bir çatışma kültürüdür. Bu kültür herhangi bir barış sürecinin önünde büyük bir engel teşkil eder. Çatışmanın kolektif hafızası, toplum üyeleri tarafından hatırlanan çatışmanın *"tarihini"* temsil eder.[17] Konu bakımından çözümsüz çatışmalar kimlik, egemenlik, değerler ve inançlar gibi konulardan oluşur. Çözümsüz çatışmalar kutuplaşmış düşmanlık ve şiddet içeren davranışları içerir.[18] Bu tarz çatışmaların resmi olarak sonlandırılması, tarafların temsilcileri tarafından müzakere aracılığıyla başlar. Ancak bu süreç karşılıklı güven ve kabul gerektirir.[19]

Toplum üyelerini derinden etkileyen çözümsüz çatışmalar, yıllarca süren şiddet, öfke, keder, mağduriyet ve intikam isteği gibi derin izler bırakır. Bu izlere rağmen uzlaşma

12 Louis Kriesberg, "Intractable Conflicts", Nigel J. Young (ed.), *The Oxford International Encyclopedia of Peace*, Oxford University Press, 2, 2010, s. 486-487.

13 Louis Kriesberg, Terrell A. Northrup ve Stuart J. Thorson, *Intractable Conflicts and their Transformation*, Syracuse University Press, New York, 1989, s. 217.

14 Miall, Ramsbotham ve Woodhouse, *Contemporary Conflict Resolution*, s. 9.

15 John Burton, "The Theory of Conflict Resolution", *Current Research on Peace and Violence*, 9:3, 1986, s. 129.

16 Peter T. Coleman, "Intractable Conflict", Morton Deutsch ve Peter T. Coleman (ed.), *The Handbook of Conflict Resolution: Theory and Practice*, Jossey-Bass Publishers, San Francisco, 2014, s. 708.

17 Daniel Bar-Tal ve Yigal Rosen, "Peace Education in Societies Involved in Intractable Conflicts: Direct and Indirect Models", *Review of Educational Research*, 79:2, 2009, s. 557.

18 Jacob Bercovitch, "Characteristics of Intractable Conflicts", *Beyond Intractability,* Ekim 2003, https://www.beyondintractability.org/essay/characteristics_ic, erişim 25.01.2025.

19 Daniel Bar-Tal, "From Intractable Conflict through Conflict Resolution to Reconciliation: Psychological Analysis", *Political Psychology*, 21:2, 2000, s. 351-352.

süreci, karşılıklı tanıma ve kabullenmeden, barışçıl ilişkilerin, karşılıklı güvenin ve olumlu tutumların geliştirilmesine yatırım yapmaktan ve diğer tarafın ihtiyaçlarına karşı duyarlılığı dikkate almayı teşvik etmekten oluşur.[20]

Uzun süreli sosyal çatışmalar ve çözümü zor çatışmalar, büyük ölçüde kesişen kuramsal özelliklere sahiptir. Her ikisi de bu tür çatışmaların kimlik, güvenlik, tanınma ve adalet gibi temel insani ihtiyaçların karşılanmamasından kaynaklandığını ve bu nedenle yüzeysel müzakerelerle sona ermeyeceğini ileri sürerler. İki yaklaşım birlikte okunduğunda şu ortak noktalar öne çıkmaktadır: Her iki çatışma türü onlarca yıl sürebilir; kolektif hafıza ve travmalar, çatışmaları sürekli yeniden üretir. Çatışmalar maddi çıkarlarla sınırlı değildir; tarafların kimlik, tanınma ve güvenlik algıları merkezde yer alır. Zayıf devletler, adaletsiz kaynak dağılımı ve dış müdahaleler çatışmayı kalıcı hale getirir.

Boko Haram çatışması çözümü zor çatışmaların birçok özelliğini taşımaktadır. 2009'dan günümüze kadar on altı yıldır devam eden şiddet eylemleri çatışmanın sürekliliğini ve yoğunluğunu göstermektedir. Ayrıca Boko Haram'ın ideolojisi dini kimlik temelli ayrışmaları güçlendirerek çözümü zorlaştırmakta ve gerçekleştirdiği saldırılar ile düşmanlığı pekiştirmektedir.

2. Boko Haram Örgütü: Ortaya Çıkışı ve İdeolojisi

Batı Afrika'da bulunan Nijerya, 350'den fazla etnik topluluğun bir arada yaşadığı 36 eyaletli federal bir cumhuriyettir. Başlıca etnik gruplar, *Hausa, Fulani, Yoruba* ve *Igbo*lar şeklindedir.[21] Oldukça karmaşık bir etnik yapıya sahip olan Nijerya'nın %55'i Müslüman, %45'i ise Hristiyan ve yerel inançlara sahiptir.[22] Toplumsal farklılıkları çok derin, etnik ve dini çeşitliliklerin belirgin olduğu bir ülke olması Nijerya'yı kırılgan kılmaktadır. Toplumsal kesimler arasındaki tarihsel etnik ve dini rekabet toplumsal bütünleşmeyi oldukça zorlaştırmakta ve çatışmalara zemin hazırlamaktadır.

1914 yılında İngiliz sömürgesi olan Nijerya, 1960 yılında İngiltere'den bağımsızlığını kazanmıştır. 1963 yılında cumhuriyet ilan edilen ülkede bir dizi darbe yaşanmış ve istikrar sağlanamamıştır.[23] 1914'te kuzey ve güney himayeleri tek bir Nijerya biriminde birleştirilen ve önemli dilsel, dinsel, kültürel farklılığa sahip olan ülkedeki kuzey ve güney kesiminin paylaştıkları tek şey ülkenin adı olmuştur.[24] Sömürge döneminde uygulanan aşağılanma, asimilasyon ve toplumsal dışlanma politikaları, Nijerya'da kimlik temelli gerilimlerin derinleşmesine yol açmıştır. Misyonerler aracılığıyla başlayan ve sonrasında zor kullanılarak sürdürülen bu politikalar, Müslüman kuzeyin kendini ötekileştirilmiş ve dışlanmış hissetmesine neden olmuştur. Bağımsızlık sonrasında da benzer zihniyetin yerel yönetimlerce devam ettirilmesi, bu tarihsel dışlanmışlık duygusunu kalıcı hale getirmiştir.[25] Boko Haram, tam da bu tarihsel ötekileştirme ve kimlik erozyonu deneyimini kullanarak destek bulmuştur ve çatışma dinamiklerini beslemiştir.

Sömürgecilik yıllarının ardından istikrarsız bir yapıya sahip olan Nijerya'da milli bir kimlik oluşturmadan bir arada yaşamaya çalışan etnik gruplar arasında gerilim ve çatışmalar baş göstermiştir. Etnik gruplar arasında yaşanan çatışmalara ek olarak Müslüman

20 Bar-Tal ve Rosen, "Peace Education in Societies Involved in Intractable Conflicts: Direct and Indirect Models", s. 558.
21 "Ülke Künyesi", *Türkiye Cumhuriyeti Dışişleri Bakanlığı*, https://www.mfa.gov.tr/nijerya-kunyesi.tr.mfa, erişim 29.03.2025.
22 "Nijerya", *İnsani ve Sosyal Araştırmalar Merkezi (İNSAMER)*, https://www.insamer.com/tr/ulke-profili-nijerya/, erişim 01.04.2025.
23 Age.
24 Özüm Sezin Uzun ve Yusuf Saheed Adegboyege, "Political Violence and Terrorism: Insight into Niger Delta Militancy and Boko Haram", *Florya Chronicles of Political Economy*, 2:2, 2016, s. 125.
25 Cihan Daban, *Nijerya'da Boko Haram Çatışması: Taraflar, Talepler ve Çözüm önerileri*, Lvre de Lyon, Lyon, 2022, s. 9-10.

ve Hristiyan gruplar arasında yaşanan dini çekişmeler, ülkenin başlıca problemleri arasında günümüze kadar gelmiştir. Ülkedeki siyasi ve ekonomik istikrarsızlık, etnik gruplar arasında yaşanan çatışmalar silahlı grupların ve terör örgütlerinin ortaya çıkmasına sebep olmuştur. Böyle bir ortamda Müslüman kesimin ekonomik, siyasi ve sosyal haklarını savunmayı ve Batılı geleneklerden uzak bir Müslüman devleti kurmayı amaçlayan Boko Haram örgütü ortaya çıkmıştır.[26] Örgütün üssü Kuzeydoğuda bulunan *Yobe* ve *Borno* eyaletlerindedir.[27] Nijerya'da ulusal bütünleşmenin ve kurumsallaşmanın tam olarak sağlanamamış olması devletin bir hakem olarak görülmesini engelleyerek bazı toplumsal kesimlerin dışlanmasına ve yabancılaşmasına yol açmıştır. Sömürge sonrası yönetimin toplumun tüm kesimlerini içine alabilecek politikalar üretememiş olması toplumsal çatışmalara zemin hazırlamıştır.

Boko Haram, Batı medeniyetine ve demokrasisine karşı olan radikal selefi aktivist Muhammed Yusuf tarafından 2002 yılında kurulan bir örgüttür. Başlangıçta örgütün adı, gayriresmî bir şekilde "Boko Haram" olarak adlandırılana kadar, *"Peygamberin öğretilerine bağlı, tebliğ ve cihad için hareket eden insanlar"* anlamına gelen (*Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihād)* olarak biliniyordu.[28] 'Boko' *Hausa* dilinde Batı ve yabancı anlamına gelirken, 'Haram' kelimesi ise yasaklama anlamında Arapça bir kelimedir. Dolayısıyla 'Boko Haram'ın kelime anlamı Batı eğitimi ve Batılı olan her şeyin haram, yasak olmasıdır.[29] Muhammed Yusuf'un Nijerya'daki okullarda verilen Batılı tarzda eğitimi lanetleyerek özellikle ülkenin kuzey bölgelerindeki eğitimi İslam dinine göre uygunsuz ve günah olarak görmesi sebebiyle örgüte Boko Haram ismi verilmiştir.[30] Bu isimlendirme ile Örgüt ülkenin sömürge geçmişinin yarattığı toplumsal dışlanmışlığı kullanarak zemin bulmaya çalışmıştır.

Muhammed Yusuf, Batı eğitiminin bölgeye yoksulluk ve acıdan başka bir şey getirmediğini bu nedenle İslam dinine uygun olmadığı, haram ve yasak olduğu kanısındadır. Yusuf'un bu söylemleri özellikle Nijerya'nın kuzeydoğusundaki mevcut durumdan memnun olmayan bazı gençler arasında hızla takipçi kitlesi kazanmasını sağlamıştır.[31] Örgüt ülkedeki Müslümanlar arasında yaygın Batı karşıtlığını kullanmış ve radikal dini söylemler, toplumsal hoşnutsuzluk içindeki gençler arasında taraftar bulmayı amaçlamıştır.

19. yüzyıldan itibaren İngiliz sömürgesi olan Nijerya'nın kuzey ve güney kesiminde izlediği politikalar, iki toplum arasındaki farklılıkları derinleştirmiştir. Kuzeyde bulunan halk, güneyde bulunan kesime kıyasla İngiliz yönetimine mesafeli durmuş ve Batı tarzı eğitime olumsuz yaklaşmıştır. 1960 yılında İngiltere'den bağımsızlığını kazanan Nijerya, kısa sivil dönemler dışında 1999 yılına kadar çoğunlukla askerî diktatörlük ile yönetilmiştir. 1999 sonrasında yönetimin kuzeydeki Müslümanlar ve güneydeki Hristiyanlar arasında dönüşümlü bir şekilde idare edilmesi noktasında mutabakata varılsa da ülkede Batı örnek alınarak yapılandırılmış kurumlar ve siyasi düzen hâkim olmuştur. Ancak bu düzenin refah ve özgürlük anlamında istenilen etkiyi vermemesi, kuzeyde bulunan Müslümanların Batı tarzı yönetim şekline tavır almasına sebep olmuştur. Dolayısıyla halk, Batılı siyasi düzenden

26 Elif Tektaş, "Nijerya'nın Ulusal Güvenliği Kapsamında Bir Terör Örgütünün Anatomisi", *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi,* 7:1, 2023, s. 213-214.

27 Stuart Elden, "The Geopolitics of Boko Haram and Nigeria's 'War on Terror'", *The Geographical Journal*, 180:4, 2014, s. 414.

28 Ali Fahd, "The Distorted Ideology of Boko Haram: Jihad or Terrorism?", *Journal of Analytic Divinity*, 8:1, 2024, s. 3.

29 Nathaniel Dominic Danjibo, "İslami Fundamentalizm ve Mezhep Şiddeti: Kuzey Nijerya'daki "Maitatsine" ve "Boko Haram" Krizleri" (çev. Zeynep Alimoğlu Sürmeli), *Mezhep Araştırmaları Dergisi*, 10:1, 2017, s. 215.

30 Tektaş, "Nijerya'nın Ulusal Güvenliği Kapsamında bir Terör Örgütünün Anatomisi", s. 215-216.

31 Adagba Okpaga, Ugwu Sam Chijioke ve Okechukwu Innocent, "Activities of Boko Haram and Insecurity Question in Nigeria", *Oman Chapter of Arabian Journal of Business and Management Review*, 1:9, 2012, s. 82.

uzaklaşarak İslami yönetimi herkesin eşit olacağı ve hükümetin denetlenebileceği bir düzen olarak görmeye başlamıştır.[32]

Kuzeydeki Müslümanların güneydeki Hristiyanlara kıyasla ekonomik olarak daha geri durumda olması, adil paylaşımdan yoksun olmaları ve eşit sosyal hakların eksikliği gibi nedenler örgütün kendine kolay bir yayılma alanı oluşturma fırsatı sunmuştur.[33] Ülkenin önemli gelir kaynağı olan petrolün büyük ölçüde güneyde bulunması sebebiyle uluslararası ticaret fırsatları güneyde yoğunlaşmaktadır. Kuzey bölgesinde ise sık sık kuraklık ve kıtlıklar yaşanmaktadır.[34] Bölgesel ekonomik eşitsizlik ve gelir dağılımındaki adaletsizlik, özellikle kuzeyde Boko Haram'ın taban bulmasını kolaylaştıran bir etken olmuştur. Ekonomik geri kalmışlık ve gelir dağılımındaki adaletsizlik bu sorunun çözümü zor çatışmalar içinde değerlendirilmesine yol açan önemli bir unsur olarak karşımıza çıkmaktadır.

Muhammed Yusuf tarafından verilen vaazlar, kuzey Nijerya'nın her yerine dağıtılmıştır. Laikliğin, demokrasinin, Batılı tarzda eğitimin ve Batılılaşmanın reddi vurgulanmıştır.[35] Örgütün temel dini ve siyasi anlatısı, selefiliğin *"şeriat"* ve *"cihat"* merkezinde inşa edilmiştir.[36] Yusuf'un anlatılarının ana hatlarından anlaşılacağı üzere örgütün ideolojisi şöyle sıralanabilir:

a. Laiklik, demokrasi ve partilerin din dışı sayıldığı tağut (putperestlik) kavramı;

b. Batı eğitimi ve Batılılaşmanın reddi;

c. İslami olmayan ülkeler ile çalışmanın kabul edilmemesi;

d. Kendilerine yöneltilen Haricilik suçlamalarının reddedilmesi.[37]

Batı eğitimine ve medeniyetine karşı olan Yusuf, Yahudilerin ve Hristiyanların Allah'ın düşmanları olduğuna inanmıştır. Dolayısıyla Batılı devletlerin benimsedikleri demokrasi, Yusuf için kabul edilemez bir yönetim biçimidir.[38] Örgütün ideolojisi ve söylemleri bir yandan sömürgeci geçmişin yarattığı tarihsel travmaları yansıtmakta iken diğer yandan sömürgecilik sonrası yönetimin Müslümanları yeteri kadar sisteme entegre edememesinin yarattığı dışlanmışlığı ortaya koymaktadır. Örgütün radikal dini söylemleri ülkedeki dinsel rekabeti de yansıtmaktadır. Dolayısıyla tarihsel dışlanmışlıklar ve toplumsal bölünmüşlükler bu sorunun ne kadar derin olduğunu ve aynı zamanda çözümü zor bir sorun olduğunu göstermektedir.

Ortaya çıkışından bu yana birçok aşamadan geçen Boko Haram, çeşitli biçimlerde ve versiyonlarda varlığını sürdürmüştür. En belirgin değişim ise 2009 yılında görülmektedir. Muhammed Yusuf ve bazı örgüt üyeleri bir saldırı sırasında öldürülmüştür. Yusuf'tan sonra örgüt, hükümete ve Batı kültürüne karşı çıkan dini bir ayaklanmadan tam teşekküllü bir örgüte dönüşmüştür. Yusuf'tan sonra liderliğe geçen Ebubekir Şekau, intikam arayışında

32 Emrah Kekilli, Hayri Ömer ve İbrahim Bahcir Abdoulaye, "Bir Örgütün Anatomisi: Boko Haram", *Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı* (*SETA)*, Sayı 214, 2017, s. 9-11.

33 İzzettin Artokça, "Boko Haram ve Eş Şebab Örgütlerinin Yapısal Bakımdan Karşılaştırılması", *Türk Asya Stratejik Araştırmalar Merkezi (TASAM)*, 2012, s. 13.

34 Elden, "The Geopolitics of Boko Haram and Nigeria's 'War on Terror'", s. 419.

35 Kyari Mohammed, "The Message and Methods of Boko Haram", Marc-Antoine Pérouse de Montclos (ed.), *Boko Haram: Islamism, Politics, Security and the State in Nigeria,* IFRA-Nigeria African Studies Centre, Leiden, 2014, s. 14.

36 Kekilli, Ömer ve Abdoulaye, "Bir Örgütün Anatomisi: Boko Haram", s. 13.

37 Mohammed, "The Message and Methods of Boko Haram: Boko Haram: Islamism, Politics, Security and the State in Nigeria", s. 15.

38 Fahd, "The Distorted Ideology of Boko Haram: Jihad or Terrorism", s. 7.

olan yeni radikal bir ideoloji ile ortaya çıkmıştır. Bu yeni ideoloji, polis güçlerine, hükümet yetkililerine ve sivillere karşı şiddetli saldırılara yol açmıştır.[39] Şiddetin derinleşmesi sorunun daha geniş bir şekilde yeniden üretilmesine yol açmaktadır. Çözümün giderek zor hale gelmesine neden olmaktadır. Verilen kayıplar toplumsal kin ve nefreti daha da büyüterek sorunu kronik hale getirmektedir.

Boko Haramın bölgedeki diğer örgütler ile karşılaştırıldığında bazı farklılıklara sahip olduğu görülmektedir. El-Şebab ve AQIM'in amacı İslam düşmanlarına karşı cihad ederek Boko Haram gibi şeriat devleti kurmaktır.[40] Fakat Boko Haram *"Batılı olan her şey yasaktır"* diyerek toplumsal yaşamın her alanına yasak koyan benzersiz bir radikallik geliştirmiştir. El- kaide'ye bağlı olan El- Şebab gibi AQIM de El Kaide'nin bir kolu olarak hareket etmiş[41] fakat Boko Haram, El kaide'ye biat etmemiştir. Zaman zaman IŞİD benzeri örgütlerle irtibat kursa da Boko Haram'ın diğer örgütlere göre daha bölgesel düzeyde faaliyet yürüten bir örgüt olduğu görülmektedir.

Boko Haram, Nijerya'daki tarihsel sömürge mirası, kuzey-güney eşitsizliği ve devletin zayıflığı zemininde ortaya çıkmıştır. Toplumsal bütünlüğün ve kurumsallaşmanın gerçekleşmemesi sorunun derinleşmesine yol açmıştır. Etnik bölünmüşlük ve farklı dini inanışlar arası tarihsel düşmanlıklar radikalizmi beslemiştir. Batı sömürgeciliğinin yerli kimliklerde yarattığı dışlanma ve yabancılaşma sorunu basit bir dini radikalizm meselesi olmaktan çıkararak çözümü zor sorunlar arasında değerlendirilmesine yol açmaktadır.

2.1. Boko Haram Örgütünün Faaliyetleri

Boko Haram, başlangıçta çoğunlukla Nijerya'daki mezhepsel çatışmaları körüklemekle ilgilenmiştir. Örgüt başlangıçta Hristiyanlara karşı küçük silahlar, palalar ve sopalar kullanarak basit saldırılar gerçekleştirmiştir. Ancak örgüt, 2008-2009 yılları arasında gerçekleştirdiği saldırılar sonucunda uluslararası kamuoyunun dikkatini çekmiştir. Boko Haram, kullandığı silahlar arasına molotof kokteylleri ve el yapımı patlayıcı cihazlar da eklemiştir. 2010 yılına gelindiğinde Nijerya'nın Plateau eyaletinde Hristiyan hedeflerine karşı konuşlandırılan bir dizi küçük el yapımı patlayıcı kullanılmıştır.[42]

Nijerya hükümeti, Örgütü 2009 yılına kadar ciddi bir tehdit olarak görmemiştir. Bu nedenle hükümetin örgüte karşı ilk müdahalesi stratejik bir eylem planı içermekten ziyade aşırı güç kullanımı şeklinde kendini göstermiştir.[43] Eylül 2010'da Bauchi eyaletindeki federal bir hapishaneye giren Boko Haram üyeleri, bir önceki yılda gerçekleşen ayaklanmadan beri yargılanmayı bekleyen 100'den fazla üyeyi serbest bırakmıştır. Bombalar ve otomatik silahlar içeren saldırı sırasında örgüt üyeleri, daha fazla şiddet gerçekleştirme konusunda uyarı niteliğinde bildiriler dağıtmışlardır. Aynı yıl içerisinde Plateau Eyaletinde yedi patlayıcı patlatmıştır. Kasabanın Hristiyan topluluklarını hedef alan bombalamalar 80 kişinin ölümüne neden olmuştur.[44] Farklı dini inanca sahip insanlara yönelik bu ölçüsüz şiddet eylemleri toplumsal bölünmüşlüğü daha da derinleştirerek sorunu daha içinden çıkılmaz hale getirmiştir.

2011 yılında Kuzey Nijerya'da Boko Haram'ın gerçekleştirdiği bir dizi hedefli cinayet, 425'ten fazla kişinin ölümüne yol açmıştır. Örgüt üyeleri saldırılar sırasında düzinelerce

39 Age, s. 7.

40 Rogue, P.C., "Somalia: Understanding Al-Shabaab. Situation Report", Pretoria: Institute for Security Studies, 2009, s. 3

41 "Al-Qa'ida in the Lands of the Islamic Maghreb", *Australian National Security,* Eylül 2024, https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/al-qaida-islamic-maghreb-aqim, erişim 02.04.2025.

42 Okpaga, Chijioke ve Innocent, "Activities of Boko Haram and Insecurity Question in Nigeria", s. 83.

43 Kekilli, Ömer ve Abdoulaye, "Bir Örgütün Anatomisi: Boko Haram", s. 21.

44 J. Peter Pham, "Boko Haram's Evolving Threat", *Africa Center for Strategic Studies*, Sayı 20, 2012, s. 4.

polis memurunu, politikacıları ve muhalif din adamlarını öldürmüştür. Aynı yıl Ağustos ayında ise BM binasına düzenlenen saldırı sırasında 24 kişinin ölümüne sebep olan intihar bombası saldırısını da Boko Haram üstlenmiştir.[45] Boko Haram 2010 ile 2012 yılları arasında yaklaşık on sekiz kiliseye saldırmış ve 127 Hristiyan'ı öldürmüştür. Örgütün Hristiyanları öldürmesinin başlıca sebebi Müslümanlar ve Hristiyanlar arasında tam ölçekli bir savaş başlatmaktır. Nijerya Hristiyan Derneği'nin Boko Haram'ın eylemlerinden Müslümanları sorumlu tutması Boko Haram'ın amacının gerçekleştiğini göstermektedir.[46] Örgütün ölçüsüz şiddet eylemleri farklı dini inanca sahip toplumsal kesimler arasındaki tarihsel güvensizliği ve rekabeti arttırmıştır. Bu açıdan şiddet eylemleri mevcut sorunların daha da derinleşerek çözümü zor meseleler haline gelmesine yol açmaktadır.

Boko Haram, Ocak 2012'de Kano'da sekiz farklı noktada güvenlik güçlerini hedef alarak oldukça karmaşık bir saldırı gerçekleştirerek polis ve orduyla saatlerce süren çatışmalara girmiştir. Toplamda 186 kişi hayatını kaybetmiştir. Saldırının ardından Başkan Goodluck Jonathan, kuzeydeki dört eyaletteki 15 Yerel Yönetim Bölgesi'nde olağanüstü hâl ilan etmiştir.[47] Çözümü zor çatışmalar genel olarak güçsüz devlet yapılarının olduğu bölgelerde ortaya çıkmakta ve çatışma hali mevcut yapıların daha da zayıflamasına yol açmaktadır. Bu açıdan Boko Haram örgütünün eylemleri ülkede genel bir güvenlik krizi yaratarak devlete olan güveni daha da sarsmıştır.

Kano saldırısından iki gün sonra, Bauchi eyaletinde ikinci bir saldırı dalgası gerçekleştiren Boko Haram, iki boş kiliseyi bombalamış ve bir polis karakoluna saldırmıştır.[48] Nijerya'da kanlı saldırılar gerçekleştiren Boko Haram'ın uluslararası kamuoyunun gündemine gelmesine sebep olan en büyük olay, 2014 yılında okullarda eğitim gören kız çocuklarının kaçırılmasıdır. Okullarda Batı geleneklerine göre verilen eğitim tarzına karşı olan örgüt, aynı zamanda kız çocuklarının eğitim görmesine de karşıdır.[49] Boko Haram, 14 Nisan 2014 tarihinde Borno eyaletinin Chibok kentinde bulunan bir okula baskın düzenleyerek 200'den fazla kız öğrenciyi kaçırmıştır. Dönemin ABD Başkanı Barack Obama'nın eşi Michelle Obama, "*Bring back our girls*" (*"kızlarımızı geri getirin"*) adı altında başlatılan kampanyaya katılarak örgütün faaliyetleri karşısında öfkelendiğini belirtmiştir.[50] Boko Haram'ın kız çocuklarını kaçırmasına tepki olarak dünyanın dört bir yanından insanlar kız öğrencilerin kurtarılması için yürüyüşlere katılmıştır. Londra'daki, Los Angeles'taki ve New York'taki insanlar Nijerya büyükelçiliğinde protesto gösterisi düzenlemişlerdir.[51] Boko Haram'ın kız öğrencileri kaçırması üzerine ABD ve İngiltere, Nijerya hükümetinin kız öğrencileri kurtarma çabalarını desteklemek için danışmanlar teklif etmiştir.[52] Bu eylem Boko Haram meselesinin etkilerinin sadece bölgeyle sınırlı olmadığını ve sorunun küresel bir mesele olarak görülmesine yol açmıştır. Diğer ülkelerin müdahaleleri Nijerya hükümeti açısından bir destek olarak değerlendirilse de sorunu daha da karmaşık hale getirmektedir.

45 "World Report 2012 Events of 2011", *Human Right Watch*, https://www.hrw.org/sites/default/files/reports/wr2012.pdf, erişim 02.04.2025.
46 Mohammed, "The Message and Methods of Boko Haram", s. 20.
47 "Government of Nigeria - JAS", *Uppsala Conflict Data Program (UCDP)*, https://ucdp.uu.se/statebased/640, erişim 25.09.2025.
48 Okpaga, Chijioke ve Innocent, "Activities of Boko Haram and Insecurity Question in Nigeria", s. 82.
49 Duman ve Çelik, "Afrika'nın Bölgesel Terör Sorunu: Boko Haram Üzerine bir İnceleme", s. 89.
50 "Michelle Obama İlk Kez Halka Seslendi", *BBC*, Mayıs 2014, https://www.bbc.com/turkce/haberler/2014/05/140510_obama, erişim 04.04.2025.
51 Emma Howard, "Bring back our girls: Global protests over abduction of Nigerian schoolgirls", *The Guardian*, Mayıs 2014, https://www.theguardian.com/world/2014/may/07/bring-back-our-girls-global-protests-abduction-nigerian-schoolgirls, erişim 06.04.2025.
52 Erin Miller, Amy Pate ve Michael Jensen, "Boko Haram Recent Attacks", *START Background Report*, Mayıs 2014, https://www.start.umd.edu/pubs/STARTBackgroundReport_BokoHaramRecentAttacks_May2014_0.pdf, erişim 21.03.2025.

Nijerya Devlet Başkanlığından 2016 yılında yapılan açıklamaya göre, örgüt tarafından kaçırılan kızların 21'i serbest bırakılmıştır. Nijerya'nın Cumhurbaşkanlığı sözcüsü yaptığı açıklamada, serbest bırakmanın Nijerya hükümeti ile Boko Haram arasında Uluslararası Kızılhaç Örgütü ve İsviçre hükümet yetkililerinin arabuluculuğunda yapılan müzakerelerin ardından gerçekleştiğini söylemiştir.[53] Bu kapsamda üçüncü tarafların müdahalesiyle sorunun belli bir ölçüde çözüldüğü görülmektedir. Bu da üçüncü tarafların çözümü zor sorunların çözümünde bazen kritik bir rol oynayabildiklerini göstermektedir.

Boko Haram, bazı bireyleri ve sivil kategorilerini kasıtlı olarak hedef almıştır. Bunlar arasında genellikle Hristiyanlar, kadınlar, laik otorite ile ilişkili olan politika yapıcılar, kamu görevlileri ve öğretmenler vardır. Mezhep liderlerinden yerel imamlara kadar İslami figürler de Boko Haram'a karşı oldukları veya öğretilerini takip etmedikleri için bu kategoriye dahil edilmiştir. Boko Haram ile mücadele etmek için birçok kasaba ve şehir Sivil Ortak Görev Güçleri (*JTF*) kurmuştur. Bunlar devlet destekli milislerden oluşmaktadır.[54] Bu gelişmeler çözümü zor sorunların çatışmaya evrilmesiyle sorunun kendini sürekli bir şekilde yeniden yaratmasına yol açtığını göstermektedir. Zayıf devlet yapıları çatışmalara uygun zemin hazırlarken çatışmalı ortamlar da mevcut devlet yapılarının daha da zayıflamasına yol açmaktadır.

2015 yılının Mart ayında Boko Haram örgütü internette yayınladığı bir videoda IŞİD'e bağlılığını duyurmuştur. Ebubekir Şekau videoda "*Halife'ye bağlılığımızı duyuruyoruz... Zorluk ve refah zamanlarında dinleyip itaat edeceğiz*" demiştir.[55] Mart 2015'te IŞİD'e bağlılık yemini ederek ISWAP (*Islamic State West Africa Province*) adını alan Boko Haram, ISWAP'ın liderliği konusunda yaşanan anlaşmazlıklar sebebiyle ikiye ayrılmıştır. Bir taraf ISWAP olarak faaliyet göstermeye devam ederken diğer taraf Boko Haram olarak faaliyetlerini sürdürmüştür.[56] IŞİD'e yapılan bağlılık bildirisi yerel veya bölgesel örgütlerin zamanla küresel ölçekte faaliyet yürüten örgütlerle bağlantı kurarak ağlarını genişletmelerine bir örnek teşkil etmektedir. Bu tür dış bağlantılar ve destekler ise sorunun çözümünü daha zorlaştırmaktadır.

2015-2016 yılları arasında Boko Haram saldırılarının sayısını artırmış ancak bunu takiben Nijerya hükümeti ve bölge ülkeler de örgüte karşı operasyon sayısını artırmıştır.[57] Örgüt giderek daha fazla sayıda saldırıyı Nijerya dışındaki bölgelere de taşıyarak faaliyet göstermeye çalışmıştır. Boko Haram Kamerun'da İslami bir yönetim uygulamak amacıyla hükümet ile doğrudan savaşmaya ilk olarak 2015 yılında başlamıştır. Örgüt zamanla Kamerun topraklarında baskın isyancı grup haline gelmiştir. En ölümcül saldırı, Nisan 2024'te Çad Gölü bölgesindeki bir balıkçı topluluğuna örgüt üyeleri tarafından saldırıldığında gerçekleşmiş ve 27 sivil hayatını kaybetmiştir.[58] Temmuz 2015'te Çad'da gerçekleşen intihar bombalamaları sırasında Çad hükümeti Boko Haram'a, örgüt üyesi olduğu iddia edilen on kişiyi idam ederek karşılık vermiştir.[59] Sınır komşusu olan Çad'a Mart 2020'de tekrar

53 "Nigeria: Boko Haram 'Releases 21 Chibok girls", *ALJAZEERA*, Ekim 2016 https://www.aljazeera.com/news/2016/10/13/nigeria-boko-haram-releases-21-chibok-girls, erişim 07.04.2025.
54 "Our Job is to Shoot Slaughter and Kill: Boko Haram Reigns of Terror in North East Nigeria", *Amnesty International*, Nisan 2015, https://www.amnesty.org/en/documents/afr44/1360/2015/en/, erişim 10.04.2025.
55 "Nigeria's Boko Haram pledges allegiance to Islamic State group", *France 24*, Mart 2015, https://www.france24.com/en/20150307-nigeria-boko-haram-islamic-state-syria-iraq-isis-isil-video, erişim 12.04.2025.
56 "Islamic State West Africa Province", Australian National Security, Eylül 2024, https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/islamic-state-west-africa-province, erişim 12.04.2025.
57 Kekilli, Ömer ve Abdoulaye, "Bir Örgütün Anatomisi: Boko Haram", s. 18.
58 "Cameroon", *UCDP*, https://ucdp.uu.se/country/471, erişim 25.09.2025.
59 "Chad sentences 10 Boko Haram members to death", *BBC News,* Ağustos 2015*,* https://www.bbc.com/news/world-africa-34091579, erişim 14.04.2025.

saldırı düzenleyen Boko Haram militanları, Çad askerî istasyonuna saldırmıştır ve 98 Çad askerini öldürmüştür.[60] Örgütün diğer bölge ülkelerinde yayılması, taban bulması ve eylem kapasitesine erişmesi yerel bir sorunun bölgesel bir sorun haline dönüşmesine yol açmıştır. Aynı zamanda farklı ülkelerden taban ve destek görmesi sorunun daha da genişlemesine ve dolayısıyla çözümünün de daha da zor hale gelmesine yol açmaktadır.

Kasım 2014'te örgütün Nijerya'nın Borno eyaletine saldırılar düzenlemesi sebebiyle binlerce kişi komşu ülke Nijer'in Diffa bölgesine kaçmak zorunda kalmıştır. Nijerya Hükümeti'nin Boko Haram'ın artan saldırılarının ardından kuzeydoğu eyaletlerinde olağanüstü hâl ilan ettiği Mayıs 2013'ten bu yana 100.000'den fazla kişi Nijer'e kaçmıştır. Nijeryalı mülteciler az gelişmiş bir bölge olan Diffa üzerinde ağır bir yük oluşturmuştur.[61]

Örgütün en aktif ve ölümcül dönemi ise 2015 yılıdır. 2015 seçimleri öncesinde merkezi otoriteyi zayıf göstermek isteyen Boko Haram, sadece Şubat 2015'te grup ile bağlantılı 110 şiddet olayına sebep olmuştur. Tüm yıl boyunca 2015'te grup tarafından bildirilen ölüm sayısı 11.500'den fazla olmuştur.[62] Boko Haram'ın eylemleri son yıllarda bir miktar azalma gösterse de tamamen etkisiz hale geldiğini söylemek mümkün değildir. Örneğin, Şubat 2021'de Nijerya'nın Maiduguri kentinde düzenlediği roket saldırısında on kişiyi öldürmüş, Mayıs 2022'de Nijerya'nın Rann köyünde bir saldırı düzenleyerek elliden fazla kişiyi öldürmüş, Aralık 2022'de Fougoh köyüne düzenlediği saldırılarda yedi sivili öldürmüştür. Örgüt, Ocak 2023'te Makilwe köyünde sekiz çiftçiyi kaçırmış ve bir kişiyi öldürmüştür.[63] Örgütün gerçekleştirdiği en son saldırı ise 25 Mart 2025 tarihinde Wulgo kasabası yakınlarındaki Çad Gölü bölgesinde iki Kamerunlu askerin öldürülmesidir.[64]

Nijerya hükümeti ve bölgesel güçler Boko Haram örgütünü etkisiz hale getirmek için çabalarını sürdürmektedir. Fakat Örgütün varlığı ve faaliyetleri günümüzde önemli bir tehdit olarak varlığını devam ettirmektedir. Nijerya uzmanı ve PRIO Küresel Üyesi Marc-Antoine Pérouse de Montclos, Nijerya hükümetinin örgüt ile mücadelesinin neden yetersiz kaldığını analiz etmiştir. Pérouse de Montclos'a göre, Nijerya hükümetinin görünmez bir düşmana karşı asimetrik bir savaşı kazanamamalarının sebebi, yerel halktan gelen destek eksikliğidir. Aynı zamanda Pérouse de Montclos, Nijerya ordusunun Boko Haram saldırısı altında olup yardım isteyen köylüleri koruyamaması ve sahada daha fazla asker bulundurmanın çözüm olacağına inanmasını çatışmanın çözülememe nedenlerinden biri olarak görmektedir.[65]

Boko Haram'ın faaliyetleri, örgütün yerel düzeyde ortaya çıkmış olsa da zamanla hem ulusal hem de bölgesel güvenliği tehdit eden, devlet otoritesini zayıflatan kalıcı bir aktöre dönüştüğünü göstermektedir. Örgüt zamanla yöntemlerini çeşitlendirmiş ve bu süreçte uluslararası kamuoyunun dikkatini üzerine çekmiştir.

60 Alaaddin Doğru, "Çad'da Boko Haram'dan askeri birliğe saldırı: 92 ölü, 47 yaralı*", Anadolu Ajansı (AA),* https://www.aa.com.tr/tr/dunya/cadda-boko-haramdan-askeri-birlige-saldiri-92-olu-47-yarali/1778302, erişim 14.04.2025.
61 "Nigeria: New Boko Haram attacks force thousands to flee to Niger", *United Nations High Commissioner for Refugees (UNHCR)*, Kasım 2014, https://www.unhcr.org/news/briefing-notes/nigeria-new-boko-haram-attacks-force-thousands-flee-niger**,** erişim 26.09.2025.
62 Hilary Matfess, "The New Normal: Continuity and Boko Haram's Violence in North East Nigeria", *Armed Conflict Location & Event Data (ACLED)*, Şubat 2019, https://acleddata.com/report/new-normal-continuity-and-boko-harams-violence-north-east-nigeria, erişim 26.09.2025.
63 "Boko Haram", *Australian National Security*, Eylül 2024, https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/boko-haram, erişim 20.01.2025.
64 Nalova Akua ve Wilson Mcmakin, "Islamic militants kill 12 Cameroonian soldiers in an attack near Lake Chad", *AP NEWS,* Mart 2025, https://apnews.com/article/cameroon-boko-haram-attack-lake-chad-wulgo-2e7710d764c72a7e53fcc9477f48354e, erişim 15.04.2025.
65 Marc-Antoine Pérouse de Montclos, "Boko Haram does not have the Fire Power of the Islamic State", Pe*ace Research Institute Oslo* (*PRIO)*, Ocak 2015, https://www.prio.org/comments/406, erişim 25.06.2025.

3. Boko Haram Örgütü ile Mücadele

Nijerya hükümeti, Boko Haram'ın yoğun faaliyet gösterdiği Borno eyaletinde örgütle mücadelesinde halkın yardımını almak amacıyla "*Auto Defence*" gruplarının kurulmasını teşvik etmiştir.[66] Boko Haram'ın gerçekleştirdiği eylemlerde ekonomik desteğin tam olarak nereden geldiği belli olmamakla birlikte[67] fidye, soygun, gasp, bağış ve diğer terör örgütleri ile kurduğu ittifak ağı aracılığıyla finansman gibi çeşitli yollarla fon aldığını söylemek mümkündür.[68] ABD Hazine Bakanlığı Yabancı Varlıklar Kontrol Ofisi (OFAC), Mart 2022'de Boko Haram ile bağlantılı altı kişiden oluşan bir ağı belirlemiştir. Altısı da Nijerya'daki Boko Haram isyancıları için fon toplamak ve maddi yardım sağlamak amacıyla BAE'de bir Boko Haram hücresi kurmaktan ve Dubai'den Boko Haram'a 782.000 dolar transfer etmekten suçlu bulunmuştur. Suçlulardan bazıları müebbet hapse mahkûm edilirken bazıları sınır dışı edilmiştir.[69] Nijerya hükümeti de terörizmin finansmanına yönelik Batı Afrika Para Aklamaya Karşı Hükümetler Arası Eylem Grubu (GIABA) ve Finansal Hareket Görev Gücü (FATF) tarzı bölgesel kuruluşlarda yer almış ve örgütün finansmanını engellemek istemiştir.

Nijerya hükümeti örgüt ile mücadelesinde zayıf kalmaktadır. Bunun başlıca sebepleri, ülkenin güvenlik kurumları arasındaki koordinasyon ve iş birliği eksikliği, yolsuzluk problemi, ülkenin kaynaklarını verimli bir şekilde kullanamaması, yargı sisteminin yavaş ilerlemesi, hükümet ile halk arasındaki iletişim kopukluğu ve teknoloji konusunda biyometrik bilgi toplama sistemleri ve gerekli veri tabanları eksikliğidir.[70] Nijerya hükümeti, örgüt ile başa çıkabilmek için sert ve aşırı kinetik bir yaklaşım benimsemiş ve çatışmanın altında yatan bağlamsal gerçekliklere ve temel nedenlere pek dikkat etmemiştir. Hükümetin doğru bir stratejisi bulunmadığı için operasyonlar genellikle isyancıların ve sivillerin ayrım gözetmeksizin öldürülmesiyle sonuçlanmıştır.[71] Aynı zamanda Nijerya'da var olan yoksulluk, işsizlik, gerçek dinsel öğretinin eksikliği gençlerin şiddet içeren aşırılığa kurban gitme konusundaki savunmasızlığını desteklemiştir. Boko Haram özellikle Kuzey Nijerya'da bu savunmasızlığı kendine taraftar toplarken ve radikalleştirme süreçlerini derinleştirmek için kullanmıştır.[72]

Boko Haram, İngiltere tarafından Temmuz 2013'te, ABD tarafından Kasım 2013'te, Kanada tarafından Aralık 2013'te ve Yeni Zelanda tarafından Mart 2014'te terör örgütü olarak tanınmıştır.[73] Mayıs 2014'te BM Güvenlik Konseyi El Kaide Yaptırımlar Komitesi Boko Haram'ı Yaptırımlar Listesine Eklemiştir. Buna göre, Boko Haram'a silah veya eleman temini de dahil olmak üzere finansal veya maddi destek sağlayan herhangi bir kişi veya kuruluş, El Kaide Yaptırım Listesi'ne eklenmeye ve yaptırım tedbirlerine tabi tutulacaktır.[74]

Çad gölü havzasında sınır ötesi silahlı haydutluğu engellemek için 1994 yılında Nijerya hükümeti tarafından kurulan Çok Uluslu Ortak Görev Gücü'ne (MNJTF), 1998 yılında Çad

66 Kekilli, Ömer ve Abdoulaye, "Bir Örgütün Anatomisi: Boko Haram", s. 21.

67 Duman ve Çelik, "Afrika'nın Bölgesel Terör Sorunu: Boko Haram Üzerine bir İnceleme", s. 90.

68 Miller, Pate ve Jensen, "Boko Haram Recent Attacks", s. 3.

69 "Treasury Sanctions Six Individuals for Raising funds in the United Arab Emirates to Support Nigeria's Boko Haram Terrorist Group", *US Deparment of the Treasury,* 25 Mart 2022, https://home.treasury.gov/news/press-releases/jy0678, erişim 15.04.2025.

70 Kekilli, Ömer ve Abdoulaye, "Bir Örgütün Anatomisi: Boko Haram", s. 21.

71 Patricio Asfura-Heim ve Julia McQuaid, "Diagnosing the Boko Haram Conflict: Grievances, Motivations, and Institutional Resilience in Northeast Nigeria", *CNA*, 2015, s. 5.

72 Freedom C. Onuoha, "Why do Youth Join Boko Haram?", UNIP Special Report 348, 2014, s. 9.

73 Australian Government, "Boko Haram", https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/boko-haram, erişim 20.01.2025.

74 "Security Council Al-Qaida Sanctions Committee Adds Boko Haram to its Sanctions List", *United Nations,* SC/11410, 22 Mayıs 2014, https://press.un.org/en/2014/sc11410.doc.htm, erişim 21.03.2025.

ve Nijer katılmıştır. Boko Haram tehdidinin artmasıyla birlikte MNJTF'nin yapısı yeniden düzenlenmiştir. 29 Ocak 2015 tarihinde MNJTF'nin mevcut hali, LCBC üye ülkeleri (Nijerya, Kamerun, Nijer, Çad) ile Benin Devlet ve Hükümet Başkanları Olağanüstü zirvesinde oluşturulmuştur.[75]Afrika Birliği Barış ve Güvenlik Konseyi, MNJTF'nin kuruluşuna tam destek vermiştir. MNJTF, grubun faaliyetlerinin genişlemesini önlemek için askerî operasyonlar yürütmeyi, gruba destek ve silah transferini engellemeyi, örgütün faaliyetlerinden etkilenen alanlarda emniyetli bir ortam yaratmayı amaçlamıştır. Böylece devletler ortak bir tehdit karşısında bir araya gelmişlerdir.[76] MNJTF, 23 Nisan 2024 tarihinde 'Lake Sanity 2' operasyonunu başlatmış ve bölgeyi yıllardır terörize eden şiddet yanlısı örgütlere karşı ilerlemeye başlamıştır.[77] Boko Haram, Nijerya hükümeti ve ortakları tarafından 2015'ten beri sürdürülen terörle mücadele çabalarının ardından önemli aksiliklerle karşılaşmasına rağmen Çad Gölü Havzası adalarındaki toprakları kontrol etmeye devam etmektedir.[78]

Örgütün saldırılarına maruz kalan Kamerun'un örgüt ile başa çıkmak için uyguladığı yöntem, Boko Haram'ın faaliyet gösterdiği bölgelere asker göndermek ve Nijerya ile olan kara ve su sınırını sıkı sıkıya kontrol etmektir. Ancak Kamerun hükümeti imkan yetersizliğinden dolayı ABD ve Fransa'dan terörle mücadele eğitimi, lojistik ve maddi destek almaktadır. Boko Haram'ın saldırılarına maruz kalan bir diğer devlet olan Çad ise, Boko Haramla mücadele etmek amacıyla kurulan MNJTF'nin harekatlarında önemli bir rol üstlenmiştir. Boko Haram ile mücadele eden bir diğer ülke olan Nijer, aktif bir şekilde MNJTF operasyonlarına katılmıştır. ABD ve Fransa ise Nijer'in terör ile mücadelesine destek vermek amacıyla ülkede askerî üsler kurmuştur.[79]

Boko Haram ile mücadelede örgüt yalnızca ulusal değil bölgesel ve uluslararası düzeyde de bir tehdit olarak algılanmıştır. Nijerya hükümetinin kurumsal eksiklikleri ve yanlış stratejileri, örgütle mücadelede kalıcı başarın elde edilmesini zorlaştırmıştır. Buna karşılık, MNJTF gibi çok taraflı iş birlikleri ve uluslararası destek, Boko Haram'ın hareket alanını daraltmaya yönelik önemli adımlar olmuştur.

3.1. Boko Haram ile Barış Görüşmeleri

Barış süreçlerinin en önemli aşaması müzakerelerdir. Barış süreçleri uzun süren bir çatışmadaki ana düşmanları içeren kalıcı barış girişimleri anlamına gelir. Barış girişimleri resmi veya gayriresmî, özel veya kamusal olabilir. Ayrıca BM veya dış taraflarca desteklenebilir. John Darby ve Roger Mac Ginty, başarılı bir barış antlaşması için şu ölçütlerin olması gerektiğini öne sürer: Tarafların iyi niyetle müzakere etmeye istekli olması, kilit aktörlerin sürece dahil edilmesi, temel konuların ele alınması, güç kullanılmaması ve müzakerecilerin sürdürülebilir bir sürece dahil olması.[80] Ancak Boko Haram örneğinde görülüyor ki örgüt, karşı tarafı *"kafir"*, *"güvenilmez"* ve *"günahkar"* olarak tanımlayarak isteklerinden taviz vermemiş ve herhangi bir iyi niyet belirtisi göstermemiştir.

75 "About the Force", *The Multinational Joint Task Force (MNJTF)*, https://mnjtffmm.org/about/#, erişim 20.03.2025.
76 William Assanvo, Jeannine Ella A. Abatan ve Wendyam Aristide Sawadogo, "La Force Multinationale de Lutte Contre Boko Haram: Quel Bilan?", *Institut d'Etudes de Sécurité*, No: 19, 2016, s. 2-3.
77 "MNJTF Operation Aims to Restore 'Sanity' to Lake Chad Basin", *Africa Defense Forum*, 01 Ekim 2024, https://adf-magazine.com/2024/10/mnjtf-operation-aims-to-restore-sanity-to-lake-chad-basin/, erişim 18.04.2025.
78 Olajumoke (Jumo) Ayandele ve Chika Charles Aniekwe, "A Decade After Chibok: Assessing Nigeria's Regional Response to Boko Haram", *ACLED*, Nisan 2024, https://acleddata.com/2024/04/16/a-decade-after-chibok-assessing-nigerias-regional-response-to-boko-haram/, erişim 18.04.2025.
79 Kekilli, Ömer ve Abdoulaye, "Bir Örgütün Anatomisi: Boko Haram", s. 22-23.
80 John Darby ve Roger Mac Ginty, *Contemporary Peacemaking Conflict, Violence and Peace Processes*, Palgrave Macmillian, NewYork, 2003, s. 2.

William Zartman'a göre, taraflar kendilerini rahatsız edici ve maliyetli bir iklimde hissettiklerinde genellikle uzun süredir havada olan ancak daha sonra cazip görünen önerilere sarılırlar. Taraflar kendilerini zaferle sonuçlanamayacak bir çatışmanın içinde bulduklarında ve bu çıkmaz her iki taraf için de acı verici olduğunda alternatif bir çıkış yolu arayışı içine girerler. Zartman bu durumu *"katlanılmaz maliyet"* olarak tanımlamıştır.[81] Boko Haram ve Nijerya hükümeti arasındaki çatışma, hem insani hem de ekonomik açıdan katlanılmaz denilebilecek düzeyde ağır maliyetler yaratmıştır. 2007-2016 yılları arasında Nijerya hükümeti için terörizmin ekonomik etkisi 97 milyar ABD Doları olmuştur. Nijerya'nın Borno eyaletinde yürütülen saha araştırmasında Boko Haram ekonomiyi çökertmek ve ticaret yollarını bozmak için pazarları ve ticaret yollarını kasten hedef almıştır. Boko Haram'ın saldırılarından dolayı işletmeler ve çiftlikler kapandığı için üretim düzensizleşmiştir. Aynı zamanda yollar ve binalar gibi sermayenin fiziksel yıkımı ekonomiyi kötü etkilerken insanların yerinden edilmesi veya öldürülmesi hem insani hem de toplumsal sorunlara yol açmıştır.[82] Katlanılmaz maliyet sadece Nijerya hükümeti için değil aynı zamanda Boko Haram için de mevcuttur. Örgüt kontrol ettiği bölgeleri kaybettikçe gelir kaynağı azalmıştır. Ayrıca Nijerya'nın Finansal İstihbarat Birimi, Boko Haram gibi aşırılıkçı grupları destekleyen karmaşık finansman ağlarını ortadan kaldırmak için küresel ortaklarla iş birliği yapmak için çalışmaktadır. Bu durum örgütün finansmanı açısından zorluklara sebep olmaktadır.[83]

Nijerya hükümeti ve sivil halk için çatışmanın maliyeti çok daha ağır ve katlanılmaz düzeydedir. Bu nedenle 2012 yılında Boko Haram'ın faaliyetlerini sonlandırması için örgüt ile bir araya gelmek isteyen Nijerya hükümeti, henüz başlangıç aşamasında olan görüşmelerde amacına ulaşamadan görüşmeler sonlanmıştır. Nijerya hükümeti ile Boko Haram arasındaki barış görüşmelerine arabuluculuk eden bir Müslüman din adamı, hükümet ve Boko Haram arasındaki görüşmelerin ayrıntıları Nijerya medyasında yer aldıktan sonra hükümetin samimiyetinden şüphe ettiğini belirterek süreçten çekilmeye karar vermiştir.[84] Nijerya hükümetinden bahsederken *"inançsızlar hükümetine"* güven olmayacağını belirten örgüt, müzakereleri bir tuzak olarak gördüğü için yetkililerle tüm görüşmeleri sonlandırmıştır. Aynı zamanda müzakereler devam ederken Nijerya güvenlik güçlerinin kendilerine yönelik operasyonlarını sürdürmesi ihanet olarak değerlendirilmiştir.[85]

Nijerya hükümeti ile Boko Haram arasında çeşitli yıllarda tek taraflı ateşkes ilanları veya görüşmeleri yaşansa da sürdürülebilir bir barış ortamı sağlanmamıştır. Örneğin, 2013 yılında grubun lideri Ebubekir Şekau'nun ikinci komutanı olan Şeyh Ebu Muhammed Ibn Abdulaziz, Nijerya'nın kuzeyindeki Maiduguri'de tek taraflı ateşkes ilan etmiştir. Ancak bu kişinin gerçekten örgütü temsil edip etmediği konusundaki şüpheler ve ateşkesin sahada uygulanıp uygulanmadığı konusundaki belirsizlikler nedeniyle bir sonuca varılamamıştır.[86]

Çatışma çözümü, çatışmanın köklü kaynaklarının ele alınıp çözüme kavuşturulması anlamına gelen bir terimdir. Çatışma çözümü davranışların şiddet içermeyen, tutumların

81 William Zartman, "The Timing of Peace Initiatives: Hurting Stalemates and Ripe Moments", *The Global Review of Ethnopolitics*, 1:1, 2001, s. 8.

82 "Measuring the Economic Impact of Violent Extremism Leading to Terrorism in Africa", *United Nations Development Programme* (*UNDP),* 2019, https://files.acquia.undp.org/public/migration/africa/undp-rh-addis_Measuring_the_Economic_Impact_of_Violent_Extremism_Leading_to_Terrorism_in_Africa.pdf, erişim 20.04.2025.

83 Hasan L. Jibiya, "Disrupting Terrorist Financing Networks in Nigeria: The Importance of Financial Intelligence in Addressing Non-traditional Threats", *Wilson Center*, Mart 2025, https://www.wilsoncenter.org/blog-post/disrupting-terrorist-financing-networks-nigeria-importance-financial-intelligence, erişim 20.04.2025.

84 ve Afolabi Sotunde, "Boko Haram talks in doubt as mediator quits", *Reuters,* 18 Mart 2012, https://www.reuters.com/article/world/boko-haram-talks-in-doubt-as-mediator-quits-idUSBRE82H09M/, erişim 20.04.2025.

85 "Boko Haram Ends Talks with Nigeria Government", *Al Jazeera,* 12 Mayıs 2012, https://www.aljazeera.com/news/2012/5/12/boko-haram-ends-talks-with-nigeria-government, erişim 22.04.2025.

86 Heather Murdock, "Nigeria's Boko Haram Militants Announce Cease-Fire", *Voa News*, 29 Ocak 2013, https://www.voanews.com/a/nigeria-boko-haram-militants-announce-ceasefire/1592925.html, erişim 22.04.2025.

düşmanca olmadığı ve çatışmanın yapısının değiştirilmesi sürecidir.[87] Çatışma çözümünde sürdürülebilir dönüşümü ve değişimi sağlayabilmek için sert politikalardan daha fazlası yapılmalıdır.[88] Çoğu başarısız barış süreci çatışma çözümü sürecinin iyi yönetilememesi, karşılıklı güven eksikliği, kök nedenlerin ihmal edilmesi, kapsayıcılıktan yoksun pazarlıklar ve zayıf uygulama kapasitesi bir araya geldiğinde süreç kırılganlaşır. Dolayısıyla çatışma çözümü, sürdürülebilir barış, kısa vadeli askerî çözümlerle değil; köklü yapısal reformlar, kapsayıcı süreçler, güven inşası ve uzun süreli toplumsal dönüşüm programları ile sağlanır.

Boko Haram meselesinde taraflar arasında derin bir güvensizlik mevcuttur. Nijerya hükümeti, Boko Haram'ın amacının barış değil, din savaşı çıkarmak olduğunu ve samimi davranmadığını düşünmektedir. Buna karşılık Boko Haram, kendilerine karşı yürütülen şiddet eylemleri devam ettiği müddetçe barışın mümkün olmayacağını dile getirirken Nijeryalı siyasetçilerin barış yanlısı söylemlerine rağmen örgüt ile mücadelede asker sayısının artırılmasını çelişkili bulmaktadır.[89] Nijerya hükümeti, Boko Haram'ın teslim olarak saldırı faaliyetlerine son vermesini isterken Boko Haram, cezaevindeki üyelerinin serbest kalmasını ve Batı geleneklerinden uzak bir eğitim ve yaşam tarzını talep etmektedir. Dolayısıyla her iki tarafın talepleri uyuşmadığı için müzakere süreçleri başarısız olmaktadır.[90] Mart 2021'de ise suçlularla müzakere yapılmasının hükümetin zayıflığı ve yetersizliği anlamına geldiğini belirten Ulusal Güvenlik Danışmanı Babagana Monguno, silahlı çete ve Boko Haram üyeleriyle müzakere yapmayacağını açıklayarak[91] müzakere seçeneğini ortadan kaldırmıştır.

Bu bağlamda barış süreçlerinin başarısız olmasının temel nedenleri; tarafların birbirine güven duymaması, taleplerin uyuşmaması, Nijerya hükümetinin orantısız güç kullanarak sivillerin desteğini kaybetmesi ve stratejik bir plandan ziyade askerî yöntemleri önceliklendirmesidir. Ayrıca, hükümetin barış söylemleri ile sahadaki uygulamaları arasındaki çelişkiler müzakere sürecini zayıflatmış, resmi yetkililerin müzakereyi reddeden tutumu ise diyaloğun tamamen tıkanmasına yol açmıştır.

Sonuç

Boko Haram örgütü sadece Nijerya için değil, tüm Batı Afrika bölgesi için ciddi bir güvenlik tehdidi oluşturmaktadır. Örgütün yükselişi, yalnızca radikal dini söylemlerle açıklanamayacak kadar çok boyutlu bir sürecin sonucudur. Her ne kadar Boko Haram sorunu yaygın olarak bir dini radikalizm örneği olarak görülse de sorun çok daha derin ve karmaşıktır. Boko Haram sorunu siyasi, ekonomik ve toplumsal eşitsizliklerden beslenen ve tarihsel travmalara dayanan bir kimliksel sorundur. Sömürgeci geçmişin bıraktığı miras, sorunun çok daha karmaşık hale gelmesine yol açmaktadır. Derin tarihsel toplumsal çatışmaların bir sonucu olan bu sorun, çözümü zor çatışmalara örnek teşkil etmektedir.

Sömürge döneminde uygulanan aşağılanma, asimilasyon ve toplumsal dışlanma ülkede kimlik temelli gerilimleri kronik hale getirmiştir. Zaman zaman zor kullanılarak sürdürülen bu politikalar, ülkenin kuzeyinde yoğun olarak yaşayan Müslüman kesimin kendini ötekileştirilmiş ve dışlanmış hissetmesine neden olmuştur. Sömürge sonrası yönetimlerin de Müslüman nüfusu sisteme entegre etmede başarılı olamaması, ülkenin çok etnikli ve dinsel yapısı ve ulus inşasının başarılamaması toplumsal çatışmalara zemin hazırlamıştır. Farklı

87 Miall, Ramsbotham ve Woodhouse, *Contemporary Conflict Resolution*, s. 21.
88 John Paul Lederach, *Building Peace: Sustainable Reconciliation in Divided Societies*, United States Institute of Peace Press, Washington, 1997, s. 25.
89 Şen ve Çiçek, "Boko Haram Terör Örgütünün Bölgedeki Etkisi ve Örgütle Müzakere Olanakları", s. 2122.
90 Daban, "Nijerya'da Boko Haram Çatışması: Taraflar, Talepler ve Çözüm Önerileri", s. 130-132.
91 "Nijerya hükümeti teröristlerle müzakere yapmayacağını açıkladı", *TRT Haber,* Mart 2021, https://www.trthaber.com/haber/dunya/nijerya-hukumeti-teroristlerle-muzakere-yapmayacagini-acikladi-563805.html, erişim 23.07.2025.

etnik ve dini grupların tarihsel düşmanlık hisleri çatışmanın şiddetlenmesine yol açarak sorunun çözümünü zorlaştırmıştır.

Çözümü zor çatışmalar genel olarak geri kalmış ülkelerde ve devlet yapısının güçlü olmadığı yerlerde ortaya çıkmaktadırlar. Boko Haram sorunu da benzer şekilde sömürge geçmişinin kronikleştirdiği toplumsal gerilimler sonucunda ulus inşasının tam olarak başarılamadığı Nijerya'da ortaya çıkmıştır. Toplumsal bölünmüşlüğün derin olduğu ve kurumsallaşmanın tam olarak sağlanamadığı ülkede Boko Haram taban bulmada pek zorlanmamış ve örgütün şiddet eylemleri devlet yapısının daha da zayıflamasına yol açmıştır.

Aynı zamanda ekonomik geri kalmışlık, bölgeler arasındaki ekonomik dengesizlik ve gelir dağılımındaki adaletsizlikler hem Boko Haram'ın taban bulmasına hem de çatışmaların şiddetlenmesine yol açmıştır. Devletin siyasi ve ekonomik kaynaklara adil erişim sağlamaması, kuzeydeki Müslüman toplulukların dışlanmışlık hissini arttırmıştır; bu da tanınma ve ekonomik katılım gibi temel ihtiyaçların şiddet yoluyla talep edildiği bir zemine dönüşmüştür.

Boko Haram'ın ölçüsüz şiddet eylemleri etnik ve dini olarak büyük farklılıklara sahip toplumsal kesimler arasında öfke, mağduriyet ve intikam isteği gibi hisler oluşturarak derin kırılmalar yaratmaktadır. Örgütün sert şiddet eylemleri toplumsal uzlaşı zeminini ortadan kaldırarak Müslümanlar ve Hristiyanlar başta olmak üzere farklı toplumsal kesimler arasındaki rekabeti düşmanlığa dönüştürerek mevcut sorunları çözümsüz hale getirmektedir.

Boko Haram örgütünün diğer bölge ülkelerinde taban bulması, ağ oluşturabilmesi ve eylem yapabilmesi sorunu daha çetrefilli hale getirerek çözümünü zorlaştırmıştır. Çatışmaların Nijerya'nın sınırlarının ötesinde Kamerun, Nijer ve Çad gibi komşu ülkelere yayılması, sorunu bölgesel bir sorun haline getirmiştir. Çatışmaların bölgeye yayılması uzun süreli çatışmaların zamanla kendilerini yeniden üretmelerine ve daha karmaşık hale gelmelerine örneklik teşkil etmektedir.

Nijerya'daki güvenlik kurumları arasındaki koordinasyon eksikliği, yaygın yolsuzluk, etkin bir yargı sisteminin bulunmaması ve dijital güvenlik altyapılarındaki eksiklikler, ulusal düzeydeki mücadelenin etkisini azaltmıştır. Aynı zamanda Nijerya hükümeti ve bölge ülkelerinin kaynak ve kapasite eksikliği nedeniyle uzun vadeli ve derinlemesine müdahalelerde bulunulamaması sebebiyle gerçekleştirilen operasyonlar sınırlı kalmıştır. Buna paralel olarak örgüt ile mücadelede uluslararası toplumun faaliyetleri de yetersiz kalmıştır.

Nijerya hükümeti ile Boko Haram arasında çeşitli dönemlerde barış görüşmeleri denenmiş olsa da, altta yatan yapısal ve toplumsal sorunlar ele alınmadan sürdürülen bu girişimler başarısız olmuştur. Çatışmaların barışçıl bir şekilde çözülebilmesi için karşılıklı güven kritik önem arz etmektedir. Taraflar birbirlerine karşı güvensiz olduklarında çözüm için herhangi bir adıma yanaşmamaktadırlar. Boko Haram meselesinde de taraflar arasında derin bir güvensizlik hali mevcuttur. Karşılıklı güvensizlik hallerinde üçüncü tarafların arabulucu rolü kolaylaştırıcı bir etken olmaktadır. Boko Haram'ın kız çocuklarını kaçırma krizinde üçünce tarafların müdahalesi kısmi de olsa bazı başarıların elde edilmesine yol açmıştır.

Boko Haram sorunu, Edward Azar'ın uzun süreli sosyal çatışmalara dair tanımladığı yapısal eşitsizlik, kimlik reddi ve siyasal dışlanma gibi temel unsurları barındırmaktadır Mezhepsel ve etnik ayrışmaların belirgin olduğu, gelir adaletsizliğinin derinleştiği Nijerya'nın kuzeyinde, güvenlik, tanınma ve kimliğin kabulü gibi zorunlu insani ihtiyaçlar karşılanamamıştır. Bu koşullar, örgütün toplumsal taban bulmasını kolaylaştırırken; hükümetin, altta yatan bu sorunları ele almadan güç temelli ve geçici önlemlerle yürüttüğü

çatışma yönetimi anlayışı, çatışmanın uzamasına neden olmuştur. Ayrıca Boko Haram, Louis Kriesberg'in çözümsüz çatışma tanımına uygun olarak uzun süreli, yıkıcı ve çözüm girişimlerine rağmen sonuçsuz kalan bir yapıya sahiptir. Örgüt, kendisini "gerçek" İslami değerlerin temsilcisi olarak görüp, Batı yanlısı devlet yapısını ve farklı inanç gruplarını sapkın ya da düşman olarak tanımlayarak kimlik merkezli güçlü bir tutum sergilemektedir. Bu üstünlük anlayışı, karşıt gruplara yönelik dışlayıcı ve şiddet içerikli eylemleri meşrulaştırmakta; böylece çatışmanın derinleşmesine ve çözümsüz bir hal almasına neden olmaktadır.

Yazarların Katkı Oranı

Yazarlar araştırmaya eşit oranda katkıda bulunmuştur.

Çıkar Çatışması

Araştırmanın yazarlarının herhangi bir çıkar çatışması beyanı bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Çalışmada herhangi bir şekilde yapay zeka uygulamalarından yararlanılmamıştır.

KAYNAKÇA

Basılı Kaynaklar

ARTOKÇA İzzettin (2012). "Boko Haram ve Eş Şebab Örgütlerinin Yapısal Bakımdan Karşılaştırılması", *Türk Asya Stratejik Araştırmalar Merkezi* (*TASAM)*, 1-15.

ASSANVO William, ABATAN Jeannine Ella A. ve SAWADOGO Wendyam Aristide (2016). "La Force Multinationale de Lutte Contre Boko Haram: Quel Bilan?", *Institut d'Etudes de Sécurité*, 19, 1-16.

AZAR E. Edward (1986). "Protracted International Conflicts: Ten Propositions", Edward E. Azar ve John W. Burton (ed.), *International Conflict Resolution: Theory and Practice,* Wheatsheaf Books*,* Sussex, 28-39.

AZAR E. Edward (1991). "The Analysis and Management of Protracted Conflict", Vamık D. Volkan, Joseph V. Montville ve Demetrios A. Julius (ed.), *The Psychodynamics of International Relationships, Volume II: Unofficial Diplomacy at Work*, Lexington Books, Massachusetts/Toronto, 93-120.

AZAR E. Edward, JUREIDINI Paul ve MCLAURIN Ronald (1978). "Protracted Social Conflict; Theory and Practice in the Middle East", *Journal of Palestine Studies*, 8:1, 41-60.

BAR-TAL Daniel (2000). "From Intractable Conflict through Conflict Resolution to Reconciliation: Psychological Analysis", *Political Psychology*, 21:2, 351-365.

BAR-TAL Daniel ve ROSEN Yigal (2009). "Peace Education in Societies Involved in Intractable Conflicts: Direct and Indirect Models", *Review of Educational Research*, 79:2, 557-575.

BURTON John (1986). "The Theory of Conflict Resolution", *Current Research on Peace and Violence*, 9:3, 125-130.

COLEMAN Peter T. (2014). "Intractable Conflict", Morton Deutsch ve Peter T. Coleman (ed.), *The Handbook of Conflict Resolution: Theory and Practice*, Jossey-Bass Publishers, San Francisco 533-560.

DABAN Cihan (2022). *Nijerya'da Boko Haram Çatışması: Taraflar, Talepler ve Çözüm Önerileri*, Lvre de Lyon, Lyon.

DANJIBO Nathaniel Dominic (2017). "İslami Fundamentalizm ve Mezhep Şiddeti: Kuzey Nijerya'daki "Maitatsine" ve "Boko Haram" Krizleri" (çev. Zeynep Alimoğlu Sürmeli), *Mezhep Araştırmaları Dergisi*, 10:1, 207-235.

DARBY John ve MAC GINTY Roger (2003). *Contemporary Peacemaking Conflict, Violence and Peace Processes*, Palgrave Macmillian, New York.

DUMAN Gökhan ve ÇELİK İsmet Mert (2021). "Afrika'nın Bölgesel Terör Sorunu: Boko Haram Üzerine bir İnceleme", *Barış Araştırmaları ve Çatışma Çözümleri Dergisi,* 9:1, 78-96.

ELDEN Stuart (2014). "The Geopolitics of Boko Haram and Nigeria's 'War on Terror'", *The Geographical Journal*, 180:4, 414-425.

FAHD Ali (2024). "The Distorted Ideology of Boko Haram: Jihad or Terrorism?", *Journal of Analytic Divinity,* 8:1, 1-23.

HEIM Patricio Asfura ve MCQUAID Julia (2015). "Diagnosing the Boko Haram Conflict: Grievances, Motivations, and Institutional Resilience in Northeast Nigeria", *CNA*.

KAZANSKY Rastislav (2020). "The Conflict Theory as a Pillarof Security Science", *Security Science Journal*, 1:2, 32-48.

KEKİLLİ Emrah, ÖMER Hayri ve ABDOULAYE İbrahim Bahcir (2017). "Bir Örgütün Anatomisi: Boko Haram", *Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA)*, 214, 1-24.

KRIESBERG Louis (2010). "Intractable Conflicts", Nigel J. Young (ed.), *The Oxford International Encyclopedia of Peace*, Oxford University Press, 2, s. 486-490.

KRIESBERG Louis, NORTHRUP Terrell A. ve THORSON Stuart J. (1989). Intr*actable Conflicts and their Transformation*, Syracuse University Press, New York.

LEDERACH John Paul (1997). *Building Peace: Sustainable Reconciliation in Divided Societies*, United States Institute of Peace Press, Washington.

MIALL Hugh, RAMSBOTHAM Oliver ve WOODHOUSE Tom (1999). *Contemporary Conflict Resolution: The Prevention, Management and Transformation of Deadly Conflicts*, Polity Press, Malden.

MOHAMMED Kyari (2014). "The Message and Methods of Boko Haram", Marc-Antoine Pérouse de Montclos (ed.), *Boko Haram: Islamism, Politics, Security and the State in Nigeria*, IFRA-Nigeria African Studies Centre, Leiden, 9-32.

OBERSCHALL Anthony (1978). "Theories of Social Conflict", *Annual Review of Sociology*, 4, 291-315.

OKPAGA Adagba, CHIJIOKE Ugwu Sam ve INNOCENT Okechukwu (2012). "Activities of Boko Haram and Insecurity Question in Nigeria", *Oman Chapter of Arabian Journal of Business and Management Review*, 1:9, 77-99.

ONUOHA Freedom C. (2014). "Why do Youth Join Boko Haram?", *UNIP,* Special Report 348.

PHAM J. Peter. (2012). "Boko Haram's Evolving Threat", *Africa Center for Strategic Studies*, No 20.

PRUITT Dean G. (2014). "Some Research Frontiers in the Study of Conflict and its Resolution", Morton Deutsch ve Peter T. Coleman (ed.), *The Handbook of Conflict Resolution: Theory and Practice*, Jossey-Bass Publishers, San Francisco, 849-868.

ŞEN Yusuf Furkan ve ÇİÇEK Hasan (2018). "Boko Haram Terör Örgütünün Bölgedeki Etkisi ve Örgütle Müzakere Olanakları", *Uluslararası Toplum Araştırmaları Dergisi*, 8:15, 2093-2145.

TEKTAŞ Elif (2023). "Nijerya'nın Ulusal Güvenliği Kapsamında Bir Terör Örgütünün Anatomisi", *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, 7:1, 206-235.

UZUN Özüm Sezin ve ADEGBOYEGE Yusuf Saheed (2016). "Political Violence and Terrorism: Insight Into Niger Delta Militancy and Boko Haram", *Florya Chronicles of Political Economy*, 2:2, 123-145.

ZARTMAN William (2001). "The Timing of Peace Initiatives: Hurting Stalemates and Ripe Moments", *The Global Review of Ethnopolitic*s, 1:1, 8-18.

İnternet Kaynakları

ABUBAKAR Aminu ve BERLINGER Joshua (2015). "Boko Haram attack on bus in Cameroon kills at least 11", *CNN World*, https://edition.cnn.com/2015/01/02/world/africa/cameroon-boko-haram-attack/index.html, erişim 12.04.2025.

ABUBAKAR Aminu ve LEVS Josh (2014). "'I will sell them,' Boko Haram leader says of kidnapped Nigerian girls", *CNN World,* https://edition.cnn.com/2014/05/05/world/africa/nigeria-abducted-girls/index.html, erişim 06.04.2025.

Africa Defense Forum (2024). "MNJTF Operation Aims to Restore 'Sanity' to Lake Chad Basin", https://adf-magazine.com/2024/10/mnjtf-operation-aims-to-restore-sanity-to-lake-chad-basin/, erişim 18.04.2025.

AKUA Nalova ve MCMAKIN Wilson (2025). "Islamic militants kill 12 Cameroonian soldiers in an attack near Lake Chad", *AP NEWS*, https://apnews.com/article/cameroon-boko-haram-attack-lake-chad-wulgo-2e7710d764c72a7e53fcc9477f48354e, erişim 15.04.2025.

Al Jazeera (2012). "Boko Haram ends talks with Nigeria government", https://www.aljazeera.com/news/2012/5/12/boko-haram-ends-talks-with-nigeria-government, erişim 22.04.2025.

Al Jazeera (2016). Nigeria: Boko Haram 'releases 21 Chibok girls'", https://www.aljazeera.com/news/2016/10/13/nigeria-boko-haram-releases-21-chibok-girls, erişim 21.03.2025.

Amnesty International (2015). "Our Job is to Shoot Slaughter and Kill: Boko Haram Reigns of Terror in North East Nigeria", https://www.amnesty.org/en/documents/afr44/1360/2015/en/, erişim 10.04.2025.

Australian National Security (2024). "Al-Qa'ida in the Lands of the Islamic Maghreb", https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/al-qaida-islamic-maghreb-aqim, erişim 02.04.2025.

Australian National Security (2024). "Boko Haram", https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/boko-haram, erişim 20.01.2025.

Australian National Security (2024). "Islamic State West Africa Province", https://www.nationalsecurity.gov.au/what-australia-is-doing/terrorist-organisations/listed-terrorist-organisations/islamic-state-west-africa-province, erişim 12.04.2025.

AYANDELE ve ANIEKWE Chika Charles (2024). "A Decade After Chibok: Assessing Nigeria's Regional Response to Boko Haram", *ACLED,* https://acleddata.com/2024/04/16/a-decade-after-chibok-assessing-nigerias-regional-response-to-boko-haram/, erişim 18.04.2025.

BBC (2009). "Nijerya'da Militanlar Orduya Direniyor", https://www.bbc.com/turkce/haberler/2009/07/090729_nigeria_police, erişim 27.03.2025.

BBC (2014). "Michael Obama İlk Kez Halka Seslendi", https://www.bbc.com/turkce/haberler/2014/05/140510_obama, erişim 04.04.2025.

BBC News (2015). "Chad sentences 10 Boko Haram members to death", https://www.bbc.com/news/world-africa-34091579 , erişim 14.04.2025.

BERCOVITCH Jacob (2003). "Characteristics of Intractable Conflicts", *Beyond Intractability,* https://www.beyondintractability.org/essay/characteristics_ic, erişim 25.01.2025.

BROCK Joe ve SOTUNDE Afolabi (2012). "Boko Haram talks in doubt as mediator quits", *Reuters,* https://www.reuters.com/article/world/boko-haram-talks-in-doubt-as-mediator-quits-idUSBRE82H09M/, erişim 20.04.2025.

DOĞRU Alaaddin (2020). "Çad'da Boko Haram'dan askeri birliğe saldırı: 92 ölü, 47 yaralı", *Anadolu Ajansı (AA)*, https://www.aa.com.tr/tr/dunya/cadda-boko-haramdan-askeri-birlige-saldiri-92-olu-47-yarali/1778302, erişim 14.04.2025.

France 24 (2015). "Nigeria's Boko Haram pledges allegiance to Islamic State group", https://www.france24.com/en/20150307-nigeria-boko-haram-islamic-state-syria-iraq-isis-isil-video, erişim 12.04.2025.

HOWARD Emma (2014). "Bring back our girls: Global protests over abduction of Nigerian schoolgirls", *The Guardian,* https://www.theguardian.com/world/2014/may/07/bring-back-our-girls-global-protests-abduction-nigerian-schoolgirls, erişim 06.04.2025.

Human Right Watch (2012). "World Report 2012: Events of 2011" https://www.hrw.org/sites/default/files/reports/wr2012.pdf, erişim 02.04.2025.

İNSAMER, "Nijerya", https://www.insamer.com/tr/ulke-profili-nijerya/, erişim 01.04.2025.

JIBIYA Hasan L. (2025) "Disrupting Terrorist Financing Networks in Nigeria: The Importance of Financial Intelligence in Addressing Non-Traditional Threats", *Wilson Center,* https://www.wilsoncenter.org/blog-post/disrupting-terrorist-financing-networks-nigeria-importance-financial-intelligence, erişim 20.04.2025.

MATFESS Hilary (2019). "The New Normal: Continuity and Boko Haram's Violence in North East Nigeria", *ACLED*, https://acleddata.com/report/new-normal-continuity-and-boko-harams-violence-north-east-nigeria, erişim 26.09.2025.

MILLER Erin, PATE Amy ve JENSEN Michael (2014). "Boko Haram Recent Attacks", *START Background Report,* https://www.start.umd.edu/pubs/STARTBackgroundReport_BokoHaramRecentAttacks_May2014_0.pdf, erişim 21.03.2025.

MNJTF, "About the Force", https://mnjtffmm.org/about/#, erişim 20.03.2025.

MURDOCK Heather (2013). "Nigeria's Boko Haram Militants Announce Cease-Fire", *Voa News,* https://www.voanews.com/a/nigeria-boko-haram-militants-announce-ceasefire/1592925.html, erişim 22.04.2025.

PEROUSE de MONTCLOS Marc-Antoine (2015). "Boko Haram does not have the Fire Power of the Islamic State", *PRIO*, https://www.prio.org/comments/406, erişim 25.06.2025.

TRT Haber (2021). "Nijerya hükümeti teröristlerle müzakere yapmayacağını açıkladı", https://www.trthaber.com/haber/dunya/nijerya-hukumeti-teroristlerle-muzakere-yapmayacagini-acikladi-563805.html, erişim 23.07.2025.

Türkiye Cumhuriyeti Dışişleri Bakanlığı, "Ülke Künyesi", https://www.mfa.gov.tr/nijerya-kunyesi.tr.mfa, erişim 29.03.2025.
UCDP, "Cameroon", https://ucdp.uu.se/country/471, erişim 25.09.2025.
UCDP, "Government of Nigeria - JAS", https://ucdp.uu.se/statebased/640, erişim 25.09.2025.
UN (2014). "Security Council Al-Qaida Sanctions Committee Adds Boko Haram to its Sanctions List", https://press.un.org/en/2014/sc11410.doc.htm, erişim 21.03.2025.
UNDP (2019). "Measuring the Economic Impact of Violent Extremism Leading to Terrorism in Africa", https://files.acquia.undp.org/public/migration/africa/undp-rh-addis_Measuring_the_Economic_Impact_of_Violent_Extremism_Leading_to_Terrorism_in_Africa.pdf, erişim 20.04.2025.
UNHCR (2014). "Nigeria: New Boko Haram attacks force thousands to flee to Niger", https://www.unhcr.org/news/briefing-notes/nigeria-new-boko-haram-attacks-force-thousands-flee-niger, erişim 26.09.2025.
US Department of the Treasury (2022). "Treasury Sanctions Six Individuals for Raising funds in the United Arab Emirates to Support Nigeria's Boko Haram Terrorist Group", https://home.treasury.gov/news/press-releases/jy0678, erişim 15.04.2025.
WALKER Andrew (2012). "What is Boko Haram?", *USIP,* https://www.usip.org/sites/default/files/SR308.pdf, erişim 25.01.2025.

GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 395-414
DOI: 10.17752/guvenlikstrtj.1646888

Araştırma Makalesi
Research Article

Bilgi Ortamında Harekât: Bilgiye Yönelik ve Bilişsel Harp Üzerine Kavramsal Çerçeve Önerisi

Information Environment Operations: A Conceptual Framework Proposal on Knowledge-Focused Warfare and Cognitive Warfare

Osman Gazi KANDEMİR*

* Dr. Tuğg. (E), Milli Savunma Üniversitesi, Kara Harp Enstitüsü Misafir Öğretim Üyesi, İstanbul, Türkiye.
e-posta: ogkandemir@gmail.com
ORCID: 0000-0002-6283-6861

Geliş Tarihi / Submitted: 25.02.2025

Kabul Tarihi / Accepted: 10.11.2025

Öz

Bu çalışma, bilgi ortamında yürütülen harekâtın kavramsal çerçevesini yeniden yapılandırmayı ve Türkçe literatürdeki terminolojik karmaşayı gidermeyi amaçlamaktadır. Çalışmanın amacı iki yönlüdür: İlk olarak, literatürdeki hâkim adlandırma olan "bilgi harbi" teriminin epistemolojik ve operasyonel yetersizliklerini ortaya koyarak yerine daha kapsayıcı bir kavram önermek; ikinci olarak, bilgi ortamındaki faaliyetleri sistematik biçimde sınıflandırmaktır. Çalışma, "information warfare" teriminin Türkçeye "bilgi harbi" olarak çevrilmesinin anlam kaymasına neden olduğunu vurgulayarak, NATO doktrinleriyle uyumlu "Bilgi Ortamında Harekât" kavramını çatı terim olarak önermektedir. Bu ortam, fiziksel, sanal ve bilişsel boyutlarıyla bütünleşik biçimde ele alınmaktadır. Çalışmanın temel katkısı, bilgi ortamındaki harekâtları iki ana kategoriye ayırmasıdır: Bilgiye Yönelik Harp (BYH) ve Bilişsel Harp (BH). BYH, siber ve elektronik harp gibi teknik araçlarla düşmanın bilgi sistemlerini hedeflerken; BH, etki harbi, dezenformasyon ve psikolojik operasyonlarla doğrudan insan zihnini hedefler. Modern hibrit çatışmalarda bu iki alan giderek iç içe geçmektedir. Sonuç olarak, çalışma Türk Silahlı Kuvvetleri ve ulusal güvenlik kurumları için bilgi ortamında açık ve tutarlı bir kavramsal çerçeve geliştirmenin stratejik zorunluluğunu ortaya koymakta; güvenlik çalışmaları ve stratejik iletişim alanlarında uygulayıcılara ve akademisyenlere rehberlik sağlamayı hedeflemektedir.

Anahtar Kelimeler: Bilgi Ortamında Harekât, Bilgiye Yönelik Harp, Bilişsel Harp, Etki Harbi, Stratejik İletişim

Abstract

This study aims to reconstruct the conceptual framework for operations conducted within the information environment while addressing terminological confusion in Turkish literature. It has two primary objectives: first, to expose the epistemological and operational shortcomings of the term "bilgi harbi" (information warfare) and to propose a more comprehensive alternative; second, to systematically categorize activities within the information environment. The study highlights that the Turkish translation of "information warfare" as "bilgi harbi" leads to semantic and doctrinal distortions, advocating for "Information Environment Operations" as a more fitting umbrella term compatible with NATO doctrines. This environment is examined holistically, encompassing its physical, virtual, and cognitive dimensions. The primary contribution of this study is the systematic classification of operations in the information environment into two main categories: Knowledge-Focused Warfare (KFW) and Cognitive Warfare (CW). KFW targets the enemy's information systems using technical tools such as cyber and electronic warfare, while CW directly influences the human mind through techniques like influence warfare, disinformation, and psychological operations. In the context of modern hybrid conflicts, these two areas get increasingly intertwined. In conclusion, the study underscores the strategic necessity of developing a clear and consistent conceptual framework for information environment operations tailored to the Turkish Armed Forces and national security institutions. It also provides essential conceptual guidance for both practitioners and academics in the fields of security studies and strategic communication.

Keywords: Information Environment Operations, Knowledge-Focused Warfare, Cognitive Warfare, Influence Warfare, Strategic Communication

Extended Summary

This study critically examines the terminological and conceptual problems arising from the long-standing use of the term "*bilgi harbi*" (information warfare) in Turkish literature and proposes a doctrinally coherent and epistemologically consistent framework for operations in the information environment. The study's fundamental argument is that the translation of "information warfare" into Turkish as "*bilgi harbi*" is based on both epistemological and operational flaws.

In Turkish, the concept "*bilgi*" refers to a final mental product that has been interpreted and internalized, while the English term "information" corresponds to organized data or a transmission process. This fundamental difference has made the concept of "bilgi harbi" inadequate for reflecting the true scope of the field. To overcome this problem, the study proposes "Information Environment Operations" as an umbrella term, which is also compatible with North Atlantic Treaty Organization (NATO) doctrines. This approach enables us to address the information environment holistically, encompassing its physical, virtual, and cognitive dimensions.

The study's second major contribution is its division of activities conducted in the information environment into two main categories based on the ultimate nature of their objectives: Knowledge-Focused Warfare (KFW) and Cognitive Warfare (CW). This distinction is explained through the "envelope and letter" metaphor: KFW targets the envelope and postal process of the letter, while CW targets how its content is read and interpreted.

KFW is a system-oriented approach that targets the enemy's capacity to collect, process, and transmit information. It is conducted through technical tools such as cyber warfare, electronic warfare, reflexive control, and command-and-control warfare. Its primary objective is to paralyze the adversary's decision-making capability and establish information dominance. KFW's strategic objectives include establishing information access superiority, directing information flow, influencing decision-making processes, protecting information sources, and maintaining information monopoly. Tools such as cyber network operations, electronic warfare, directed energy weapons, and space systems are used to achieve these objectives.

On the other hand, CW is a form of struggle that directly targets the human mind, perceptions, attitudes, and behaviors. Unlike traditional psychological warfare, this field represents a sophisticated approach that utilizes modern neuroscience and cognitive sciences, aiming to manipulate how individuals think and consequently how they behave. CW is conducted through two fundamental methods: overt activities (influence operations) and covert activities.

The Influence Warfare dimension seeks to shape the perceptions of societies, cultures, and public opinion through visible tools such as strategic communication, public diplomacy, cultural diplomacy, soft power, and digital diplomacy. Perception management, narrative construction, and reinterpretation of history are fundamental elements of this strategy. Covert activities include more complex methods such as disinformation, social engineering, reflexive control, truth decay, post-truth strategies, and neurotechnological interventions.

The study also emphasizes the interaction between KFW and CW. These two areas increasingly intertwine in the modern conflict environment, introducing a new dimension known as "hybrid information operations." A cyberattack can not only disable technical infrastructure but also create lasting effects at the cognitive level by generating distrust and

panic in society. Russia's annexation of Crimea in 2014 and invasion of Ukraine in 2022 are examples of this hybrid approach. These cases demonstrate how technical disruptions in communication networks were synchronized with large-scale cognitive influence campaigns.

The study concludes that the center of gravity of modern warfare has shifted from the physical realm to the information and consciousness domains. Clausewitz's principle of "forcing the enemy to accept our will" is now being realized in the 21st century through algorithms, narratives, and perceptions. In this context, there emerges a strategic necessity for the Turkish Armed Forces and national security institutions to develop a clear, consistent, and hierarchical conceptual framework for operations conducted in the information environment. The terminological distinction and systematic structure proposed by the study have the potential to constitute a solid foundation for future doctrinal studies, training programs, and strategic planning.

Giriş

Savaş, tarih boyunca yalnızca fiziksel çatışmalarla değil, zihin, algı ve irade üzerinde yürütülen mücadelelerle de tanımlanmıştır. "Clausewitz'in *"Savaş, politik bir amaca ulaşmak için düşmanı irademizi kabul etmeye zorlayan bir şiddet eylemidir"*[1] tanımı, savaşın özünde iradeler arasındaki mücadele olduğunu gösterir. Sun Tzu'nun *"Kendini ve düşmanını tanıyorsan, yüz savaşın sonucundan korkmazsın"* [2] sözü ise bilgi üstünlüğünün zaferdeki belirleyici rolünü vurgular.

Savaşın değişmeyen doğası, onu fiziksel, bilgi ve insan boyutlarında süreklilik arz eden bir mücadeleye dönüştürmüştür. Bu boyutlar arasında köprü görevi gören bilgi boyutu, muhasımın bilgi dünyasını hedef alan propaganda, hile, aldatma ve manipülasyon gibi tekniklerle daima stratejik bir alan olmuştur. 20. yüzyılda sanayi ve teknolojideki gelişmeler, savaşın kapsamını genişletmiş ve yıkıcılığını artırmıştır.[3] Artık savaş, sadece orduların değil, toplumların, ekonomilerin ve kültürlerin de hedef alındığı çok katmanlı bir mücadeleye evrilmiştir.

Modern savaşların en belirgin özelliklerinden biri, savaş ve barış arasındaki sınırların giderek bulanıklaşmasıdır.[4] Devletler, klasik savaş alanlarında verdikleri mücadele kadar, toplumların zihinlerine ve algılarına yönelen stratejilere de ağırlık vermektedir. Bu durum, Miller'in "sıcak barış-sıcak savaş"[5] tayfı yaklaşımını destekler nitelikte olup, üstünlük mücadelesinin uzaydan dijital dünyaya kadar genişleyen yeni bir harp sahasında sürdüğünü göstermektedir. Bilginin konvansiyonel mecralardan dijital platformlara aktarılması, toplumları birey bazında hedef alan asimetrik stratejilerin önünü açmıştır. Artık bilgisayarlar ve dijital sistemler kontrolünde olmayan bilgi istisna haline gelmiş, karar mekanizmaları da dijital sistemler üzerindeki eylemlere karşı hassas duruma gelmiştir.

Devletler, muharebe sahasına ihtiyaç duymadan bilgi ortamını kullanarak düşmanı zayıflatma, tarafsızları kendi yanına çekme ve kamuoylarını stratejik hedeflerine uygun şekilde yönlendirme çabasındadır. Günümüzde savaşlar yalnızca ordular arasında değil; sosyal medya platformlarında, ekonomik pazarlarda, diplomatik masalarda ve en önemlisi toplumların zihinlerinde verilmektedir. Üçüncü küreselleşme ve dijital teknolojilerin

1 Carl von Clausewitz, *On War* (çev. Michael Howard ve Peter Paret), Princeton University Press, Princeton, 1984, s. 83.
2 Sun Tzu, *The Art of War* (çev. Samuel B. Griffith), Oxford University Press, Oxford, 1963, s. 84.
3 Christopher Bellamy, The Evolution of Modern Land Warfare Theory and Practice, Routledge, New York, 1984, s. 62.
4 Valery Gerasimov, "The Value of Science in Prediction", *Military-Industrial Kurier*, February 27, 2013, s. 2.
5 Benjamin Miller, *States, Nations, and the Great Powers: The Sources of Regional War and Peace*, Cambridge University Press, Cambridge, 2007, s. 47-50.

gelişmesiyle birlikte, bilgi ortamında yürütülen savaşlar daha sofistike hale gelmiş, sınırlar kalkmış ve bilginin nüfuz gücü hiç olmadığı kadar artmıştır. Siber uzaydaki dezenformasyon kampanyaları, sosyal medya manipülasyonları ve yapay zekâ destekli bilgi savaşları, modern etki harbinin temel unsurları haline gelmiştir.[6]

Bilgi ortamında yürütülen harekâtların, yeni küreselleşme ve teknolojideki gelişmeler sebebiyle kendine yeni alanlar bulması, güvenlik ve savaş çalışmaları alanında literatürün zenginleşmesine vesile olmuştur. Ateş ve Evren'in söylediği gibi, savaşın doğası değişmemiştir, bugün yeni gibi adlandırılan birçok mücadele biçimi tarihin ilk dönemlerinden beri vardır ama savaşın kapsadığı alan ve aktörleri değişmiştir.[7] Bu durumda yeni kavramların ortaya çıkması bir gerekliliktir.[8] Bu bağlamda bilgi ortamında yürütülen harekâtları tanımlamak için de çok sayıda savaş çeşidi kavramı (bilişsel, etki, psikolojik, siber, elektronik, anlatı harbi vb.) üretilmiştir. Ancak, üretilen bu kavramların sınırlarının belirlenmesi, bir alan hiyerarşisi içinde bulunmaları da bir gerekliliktir.

Bu çalışma, ilk olarak Türkçe literatüre girmiş bulunan "bilgi harbi" kavramını eleştirel biçimde incelemeyi ve bu kavramın daha isabetli bir çerçeveyle yeniden tanımlanmasını amaçlamaktadır. "*Information warfare*" ifadesinin Türkçeye "bilgi harbi" olarak çevrilmesi, alanın kapsamı ve içeriği açısından çeşitli kavramsal sorunlar yaratmıştır. Bu çeviri zamanla, kavramın, insan beynini hedef alan birçok harp çeşidini içine alan şemsiye bir kavrama dönüşmesine yol açmıştır. Ancak bu kullanım hem teorik olarak muğlaktır hem de pratikte ayrıştırıcı analizlere engel teşkil etmektedir. Bu nedenle çalışmada bilgi harbi kavramı daha dar ve yerinde bir bağlama oturtulmaya çalışılacak, mevcut geniş kullanımı yerine daha kapsayıcı ve açıklayıcı bir üst kavram önerilecektir.

Çalışmanın ikinci amacı, hâlihazırda "bilgi harbi" başlığı altında birlikte anılan çok sayıda yöntem, araç ve stratejiyi daha sistematik bir yaklaşımla yeniden tasnif etmektir. Bu çerçevede bilgi ortamındaki harekâtlar, iki temel alana ayrılarak incelenecektir. Birincisi doğrudan "bilgi"nin korunması veya yok edilmesiyle ilgili harekâtlar, ikincisi ise insan beynini hedef alan harekâtlardır. Her bir alan; stratejik hedefleri, operasyonel araçları ve yöntemsel yaklaşımları bakımından ayrıştırılarak incelenecek, böylece bu alandaki kavramsal karmaşaya karşı bütüncül ama ayırt edici bir analiz çerçevesi ortaya konacaktır. Bu yaklaşım, yalnızca teorik açıklık sağlamakla kalmayacak; aynı zamanda uygulayıcılar, karar vericiler ve araştırmacılar için sağlam bir başvuru zemini oluşturacaktır.

Günümüzde savaşın boyutları yalnızca kara, deniz, hava veya siber alanlarla sınırlı değildir; bilgi, zihin ve irade üzerindeki mücadeleler de modern çatışmaların belirleyici unsuru haline gelmiştir. Bu bağlamda "bilgi boyutu", savaşın yalnızca fiziksel varlıkları değil, aynı zamanda algı, irade ve karar süreçlerini hedef alan zihinsel uzamını ifade eder. Bu makale, savaşın bilgi boyutunun tarihsel sürekliliğini inceleyerek, bilgiye ve insana yönelik harekât biçimlerinin kuramsal temelini ortaya koymayı amaçlamaktadır.

1. Aldatmadan Günümüze Kavramların Tarihsel Evrimi

Savaşlar, tarih boyunca sadece fiziksel çatışmalarla sınırlı kalmamış, aynı zamanda zihinlerde ve psikolojik alanda da mücadelelerle şekillenmiştir. Sun Tzu'nun dediği gibi,

6 P.W. Singer ve Emerson T. Brooking, *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston, 2018, s. 88-90.

7 Barış Ateş ve Evren Mercan, "Yeni Savaşlar ve Yeni Ordular", *Güvenlik Stratejileri Dergisi*, Özel Sayı, 2023, 1-11.

8 Çalışmanın başlangıcında yapılan literatür taramasında 102 farklı çeşit harp kavramına (ekine *warfare* kelimesi almış) rastlanmıştır.

"*Her savaş aldatmaca üzerine kuruludur*."[9] Düşmanın karar alma süreçlerini bozmak, yanlış yönlendirmek ve moralini bozmak için farklı taktikler kullanılmıştır. Antik çağda ordular, güçlerini abartılı göstermek için sahte mevziler kurmuş, gece boyunca ateşler yakmış ve casuslarla yanlış bilgiler yaymıştır. 14. yüzyılda Moğollar, Ceneviz kalesine vebalı cesetler fırlatarak korkuyu bir silah olarak kullanmıştır. Bu eylem, düşmanın korku ve kaos algısını hedeflemiş, bilgi üstünlüğü sağlanmıştır. Bu yöntemler, erken dönem bilgi harbi stratejileri olarak görülebilir.

Tarihsel süreçte bilgi ortamında yürütülen faaliyetleri adlandırmak için çeşitli kavramlar ve teoriler kullanılmıştır. Propaganda, bilgi harbi literatüründeki en eski kavramlardan biridir. Latince *propagare* (yaymak, çoğaltmak) kelimesinden gelir. İnsanlar, antik çağlardan beri bilinçli manipülasyon teknikleri ile birbirlerini etkilemeye çalışmıştır. Pratkanis ve Aronson'a göre propaganda, düşünce biçimlerini yönlendirmek için kullanılan sistematik bir yöntemdir ve tarih boyunca politik, ekonomik ve toplumsal alanlarda güçlü bir araç olmuştur.[10]

Modern anlamda propaganda, 1622'de Papa XV. Gregory'nin Katolik inancını yaymak için kurduğu *Sacra Congregatio de Propaganda Fide* (İnancın Yayılması için Kutsal Cemaat) ile sistematik hale gelmiştir. [11] Başlangıçta dini amaçlı kullanılan bu terim, zamanla siyasi ve ideolojik mücadelelerde de yer almıştır. Fransız Devrimi sırasında broşürler, afişler ve sloganlar, halkı etkilemek için yoğun şekilde kullanılmış, matbaanın yaygınlaşması ve okuryazarlığın artmasıyla propaganda, geniş kitlelere ulaşma imkânı bulmuştur.

20. yüzyılda bilgi ortamında harekâtın önemi artmıştır. 1928'de Edward Bernays, *Propaganda* kitabıyla modern propaganda ve kamuoyu manipülasyonunun temellerini atmış,[12] demokratik toplumlarda bile kitleleri kontrol etmek için propaganda kullanılabileceğini savunmuştur. George F. Kennan'ın politik savaş teorisi, modern bilgi harbi uygulamalarının erken ve sistematik örneklerinden biridir.[13] Kennan, Soğuk Savaş döneminde ABD'nin Sovyetler Birliği'ne karşı uygulaması gereken stratejileri belirlemiştir. Politik harp, düşmanın siyasi, ekonomik, psikolojik ve toplumsal yapısını hedef alıyordu. ABD, bu stratejiyle Sovyetler Birliği'ne karşı propaganda, gizli operasyonlar ve psikolojik harp yöntemleri kullanmıştır. *Radio Free Europe* ve *Voice of America* gibi medya araçlarıyla Sovyet halklarına ulaşmaya çalışmıştır.

1960'ta Schelling, *The Strategy of Conflict* kitabında[14] bilgi ve iletişimin çatışma stratejilerindeki rolünü incelemiş, blöf, tehdit ve güven inşası gibi kavramlara odaklanmıştır. 1964'te McLuhan, *Understanding Media*[15] eserinde, medyanın algıyı nasıl şekillendirdiğini ve bunun bilgi harbinde nasıl kullanılabileceğini anlatmıştır. 1967'de Vladimir Lefebvre, "Refleksif Kontrol" kavramını geliştirmiştir. Bu strateji, düşmanın karar alma süreçlerini manipüle ederek, onu istenen yönde hareket etmeye zorlamak amacındadır.[16]

9 Tzu, *The Art of War*, s. 66.

10 Anthony Pratkanis ve Elliot Aronson, *Age of Propaganda: The Everyday Use and Abuse of Persuasion*, W. H. Freeman, New York, 2001, s. 37-39

11 The Catholic Encyclopedia, s.v. "Congregation for the Propagation of the Faith," https://www.newadvent.org/cathen/12456a.htm, erişim 20.02.2025.

12 Edward Bernays, *Propaganda*, Horace Liveright, New York, 1928, s. 45.

13 George F. Kennan, *The Inauguration of Organized Political Warfare*, Memorandum, Policy Planning Staff, ABD Dışişleri Bakanlığı, 4 Mayıs 1948.

14 Thomas Schelling, *The Strategy of Conflict*, Harvard University Press, Cambridge, MA, 1960, s. 112.

15 Marshall McLuhan, *Understanding Media: The Extensions of Man*, McGraw-Hill, New York, 1964, s. 78.

16 Maria W. de Goeij, "Reflexive Control: Influencing Strategic Behavior," *Parameters* 53, no. 4 (2023) s. 97-108.

1980'lerde Sovyet KGB'si ve Doğu Alman Stasi'si, dezenformasyon ve psikolojik harp operasyonlarıyla düşman ülkelerin iç siyasetini ve halkın moralini bozmuş, *Operation Infection* (AIDS'in ABD tarafından geliştirildiği yalanı) gibi kampanyalar düzenlemiştir.[17] Joseph Nye, 1990'da askerî veya ekonomik güç kullanmadan kültür, değerler ve politikalarla etkilemeyi tanımlayan "yumuşak güç" kavramını ortaya atmıştır. 1994'te Albay Richard Szafranski, "*Neocortical Warfare*" (neokortikal harp) kavramını tanıtmıştır.[18] Bu strateji, düşmanın karar alma süreçlerini ve algılarını manipüle ederek savaşı insan beynine taşımayı hedeflemektedir.

1999'da Çinli Albaylar Qiao Liang ve Wang Xiangsui, "Sınırsız Savaş" teorisi ile geleneksel savaşın ötesine geçip ekonomik, siyasi, teknolojik, medya ve siber alanlarda düşmanı zayıflatmayı önermişler.[19] 2003'te Çin Halk Kurtuluş Ordusu, "Üç Savaş" stratejisini geliştirmiştir.[20] Psikolojik harp, medya harp ve hukuk harp unsurlarını içeren bu strateji, bilgi ortamını hem iç hem de dış politikada etkili şekilde kullanmayı amaçlamaktadır.

21. yüzyılda dijitalleşme ve internetin yaygınlaşmasıyla bilgi harbi yeni bir boyut kazanmıştır. Philip Taylor, modern savaşların sadece cephelerde değil, zihinlerde de kazanıldığını söylemiştir.[21] Bilgi harbi, artık sadece devletler arasında değil, toplumların algısını şekillendirme ve yönlendirme süreçlerinde de kullanılıyordu. Hibrit harple birlikte bilgi ortamında harekâtlar yoğunlaşmıştır. Devletler hem kendilerini koruma hem de gri alanda rakiplerine karşı operasyon yapma reflekslerini geliştirmişlerdir. Günümüzde ise savaşlar, fiziksel alanların ötesine geçip beyinlere ulaşmaktadır. Dr. James Giordano'nun çalışmaları,[22] beynin yeni bir harp alanı haline geldiğini göstermektedir. Bu konu, bilişsel harp başlığı altında detaylandırılacaktır.

2. Terminolojik Karmaşadan Bütüncül ve Hiyerarşik Bir Yaklaşıma

Bir eylemin "savaş" olarak tanımlanabilmesi için uluslararası hukuk ve askerî bilimler disiplinlerinin bakış açısından dört temel belirleyici özellik şart koşulmuştur: Savaş, 1) öncelikle kuvvet kullanma hâlidir; 2) düşmanca bir tutum ve/veya eylem içermelidir; 3) geleneksel hukuka göre üçüncü tarafları ilgilendiren hak ve yükümlülükler de dâhil olmak üzere hukuki bir durum yaratır ve son olarak 4) savaşın faili devlettir. Bu şartlar ışığında savaş; "Devletler veya devlet grupları tarafından, millî güç unsurlarının tamamının veya bir kısmının kullanılması suretiyle icra edilen ve taraflarca savaş niteliği kabul edilen, kuvvet kullanılmasını içeren, düşmanca niyet ve/veya eylem" olarak tanımlanmak mümkündür.[23]

Bu tanım, klasik savaş paradigmalarını açıklamak için yeterlidir; ancak bilgi ortamında gerçekleşen siber saldırılar, psikolojik harekâtlar, anlatı operasyonları veya bilişsel müdahaleler gibi faaliyetler, silahlı çatışma eşiğine ulaşmadıkları ve doğrudan kuvvet kullanımı içermedikleri için bu tanıma dâhil edilemezler. Bu faaliyetler, savaş sayılmak için

17 Douglas Selvage ve Christopher Nehring, "Operation "Denver": KGB and Stasi Disinformation regarding AIDS" https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids, erişim 20.02.2025

18 Richard Szafranski, *"Neocortical Warfare? The Acme of Skill"*, *Military Review*, 74:11, 1994, s. 41-55.

19 Qiao Liang ve Wang Xiangsui, *Unrestricted Warfare: China's Master Plan to Destroy America*, PLA Literature and Arts Publishing House, Beijing, 1999.

20 Peter Mattis, "China's 'Three Warfares' in Perspective", *War on the Rocks*, 30 Ocak 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/, erişim 15.03.2025.

21 Philip M. Taylor, *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era*, Manchester University Press, Manchester, 2003, s. 13, 217.

22 MWI Video: The Brain is the Battlefield of the Future – Dr. James Giordano https://mwi.westpoint.edu/mwi-video-brain-battlefield-future-dr-james-giordano/, erişim 10.03.2025.

23 Ali Bilgin Varlık, "Savaşı Tanımlamak: Terminolojik Bir Yaklaşım", *Avrasya Terim Dergisi*, 1:2, 2013, s. 114-129.

gereken hukuki ve askerî eşikleri karşılamamaktadır. Bu nedenle savaş hukuku da bu alanları kapsam dışında bırakmaktadır.

Bununla birlikte, 1959 basımlı Kara Harp Okulu *Harp Tarihi*[24] kitabında dikkat çekici bir açılım sunulmuş; klasik savaş anlamı içinde kuvvet kullanılarak yapılan eylemler "askerî harp" ya da "silahlı harp" olarak özel başlık altına alınmış, buna karşılık diğer mücadele biçimleri de savaş çerçevesinde değerlendirilmiştir. Bu yaklaşım, savaş kavramının yalnızca fiziki kuvvete indirgenmemesi gerektiğine işaret etmesi bakımından önemlidir.

Bu çerçevede, bilgi ortamında yürütülen çok sayıda faaliyet, klasik anlamda "savaş" sayılmasa da Clausewitz'in iradeyi zorlama amacını modern teknoloji ve bilişsel bilimler aracılığıyla gerçekleştirme çabalarıdır. Bu eylemler, sistemli, örgütlü ve düşmanca niyetle yürütüldükleri ve stratejik hedeflere ulaşmak için millî gücün tüm unsurlarını (bilgi, psikoloji, teknoloji) kullandıkları için "harp" olarak adlandırılabilirler.[25]

Alanın Türkçe literatür açısından bir başka problemi "*war*" (savaş) ve "*warfare*" (savaşma biçimi) kavramlarının Türkçede ayrı ayrı karşılığının bulunmamasıdır. Bu konunun incelenmesi makalenin konusu dışındadır. Ancak bütünlük ve anlaşılırlık açısından kolaylık olsun diye "*war*" karşılığında "savaş", "*warfare*" karşılığında "harp" kelimeleri kullanılmıştır.

2.1. Bilgi Harbi Kavramının Yeterliliği ve Çatı Kavram Önerisi

Çalışmanın ana konusu olan "*Bilgi harbi*" kavramı Türkçe literatüre, İngilizce "*information warfare*" kavramı üzerinden girmiştir. Türkçedeki "bilgi" kelimesi, eski Türkçeden bu yana kullanılan "bil-" fiilinden türetilmiştir. Bu fiil "kavramak", "öğrenmek", "farkında olmak" anlamları taşır. Fiil köküne eklenen "-gi" yapım ekiyle türetilen "bilgi", doğrudan doğruya "bilinen şey" yani zihinde anlamlandırılmış, içselleştirilmiş içerik anlamına gelir.[26] Bu yönüyle Türkçedeki "bilgi" kavramı, insan zihninde oluşmuş ve anlam kazanmış nihai bir bilişsel ürünü ifade eder.

Buna karşılık, İngilizcedeki "*information*" kelimesi Latincedeki *informare* fiilinden türemiştir. Bu fiil, "biçim vermek", "şekillendirmek" anlamlarına gelir; *informatio* ise bir zihni dışsal veriler aracılığıyla şekillendirme sürecini ifade eder.[27] Modern anlamda "*information*", genellikle verinin anlamlı biçimde düzenlenmiş hali, yani bir iletişim veya aktarım süreci olarak tanımlanır. Ancak bu içerik, bireyin zihninde anlam kazanıp özümsenmedikçe "bilgi" (*knowledge*) haline gelmiş sayılmaz.[28]

Türk Dil Kurumu, "*information*" terimini "danışma" ve "haberleşme" olarak karşılamakta; Ötüken Sözlük[29] ve Kubbealtı Lugatı[30] da benzer biçimde "bilgilendirme, haber verme, veri iletme" gibi anlamlar vermektedir. Bunun yanı sıra "*information*" kelimesinin Türkçeye, malumat[31] olarak çevrildiği de vakidir. Dolayısıyla "*information warfare*" teriminin "bilgi harbi" olarak çevrilmesi, Türkçedeki "bilgi" kavramının derinliği göz önünde bulundurulduğunda, çeviri düzeyinde önemli bir kaymaya yol açmaktadır.

24 Orhan Ergüder, *Harb Tarihi*, Kara Harp Okulu Basımevi, Ankara, 1959; akt.; Varlık a.g.m.

25 Paul A. Smith, Jr., *On Political War*, National Defense University Press, Washington D.C. 1989, s. 3.

26 Gerard Clauson, *An Etymological Dictionary of Pre-Thirteenth-Century Turkish*, Clarendon Press, Oxford, 1972, s. 330.

27 "Information", *Online Etymology Dictionary*, https://www.etymonline.com/word/information, erişim 15.10.2025.

28 Luciano Floridi, *The Philosophy of Information*, Oxford University Press, Oxford, 2011, s. 93-107.

29 Yaşar Çağbayır, *Orhun Yazıtlarından Günümüze Türkiye Türkçesinin Söz Varlığı Ötüken Türkçe Sözlük*, İstanbul, Ötüken Yayınları, 2007, s. 1448.

30 İlhan Ayverdi, *Misalli Büyük Türkçe Sözlük*, Kubbealtı Yayınları, İstanbul, 2010, s. 344.

31 Türkçe'deki enformasyon harbine bilgi harbi denmesinin yarattığı bulanıklığı gidermek için Dağhan Yet, *"malumat harbi"* kavramını önermiştir. Dağhan Yet, "Malumat Savaşında Hızlı-Etki Yaklaşımı: Türkiye Deneyimi", Barış Ateş (ed.), *Türkiye'de Askerî Yenilik*, Vakıfbank Kültür Yayınları, İstanbul, 2023, s. 315-341.

İngilizcedeki *information* kelimesinin karşılığı olarak Türkçeleşmiş bir kelime olan "enformasyon", ham verinin düzenlenmesi ve anlam kazanmasını sağlayan soyut bir yapıya sahiptir, ancak tek başına bilgi değildir. Bilgi, ancak enformasyonun işlenmesi, anlamlandırılması ve bireyler veya sistemler tarafından yorumlanmasıyla ortaya çıkar.[32] Bu bağlamda, enformasyon, bilgiye giden yolda kritik bir ara aşamadır ve onu kontrol eden aktörler, bilgi üretme ve karar alma süreçlerinde üstünlük sağlayabilirler. İletişim Başkanlığı tarafından yayınlanan sözlükte de "Bilgi Harbi" kavramı bulunmazken "Enformasyon Savaşları" kavramına yer verilmiştir.[33]

Türk Silahlı Kuvvetlerine ait askerî terimler sözlüklerinde "bilgi harbi" terimi bulunmamaktadır. Yayımlanmış taktik ya da doktriner belgelerde de bu kavrama rastlanmaz. Ancak Dışişleri Bakanlığının çevrim içi "Askerî Terimler Sözlüğü"nde "*information warfare*" terimi doğrudan "bilgi harbi" olarak çevrilmiştir. Bu çeviri eğilimi, çevrim içi sözlüklerde de yaygındır. Ancak bu uygulama, kavramın yalnızca sözcük düzeyinde karşılığını vermekte; içerik ve kapsam bakımından önemli belirsizlikleri beraberinde getirmektedir.

ABD ordusunun yeni uygulamaya başladığı "Çok Alanlı Muharebe Doktrininde" harekâtın icra edildiği çevre (*operational environment*), üç temel boyutta ele alınmaktadır: fiziksel çevre, insan boyutu ve enformasyon boyutu. Bu modelde temel unsur "bilgi" (*knowledge*) değil, "enformasyon" (*information*) olarak tanımlanır.[34] Çünkü askerî harekât ortamında aktarılan, yönlendirilen ve hedeflenen içerik, genellikle anlam kazanmamış ham veri ya da düzenlenmiş enformasyondur. Karar destek sistemleri, komuta-kontrol yapıları ve bilişsel etki süreçlerinin çoğu, henüz bireysel anlamlandırma süzgecinden geçmemiş bu enformasyon türü üzerine inşa edilir.

Bilgi kuramlarında bu ayrım daha da netleştirilmiştir:

- Veri (*data*), işlenmemiş ham ölçümlerdir.
- Enformasyon (*information*), düzenlenmiş ve bağlama yerleştirilmiş veridir.
- Bilgi (*knowledge*) ise enformasyonun anlamlandırılarak zihinde kavranmış, içselleştirilmiş hâlidir.[35]

Bu ayrım doğrultusunda her bilgi, zamanında bir enformasyondu; ancak her enformasyon, bilgiye dönüşmeyebilir. Dolayısıyla "*information warfare*" teriminin "bilgi harbi" şeklinde çevrilmesi, bilgi ile enformasyonun hem epistemolojik hem de operasyonel düzeyde farklı şeyler olduğu gerçeğini göz ardı etmektedir.

Yukarıda ifade edilen anlam kaymasına ilave olarak, "bilgi harbi" terimi çoğu zaman çatı kavram gibi kullanılmakta; siber harp, bilişsel harp, psikolojik harp, etki operasyonları ve anlatı harbi gibi çok sayıda kavram bu başlık altında toplanmaktadır. Ancak yukarıda açıklanan nedenlerle "bilgi harbi" kavramı hem epistemolojik açıdan hem de terminolojik bakımdan bu alanı kuşatmak için yetersizdir.

Bu çalışma, bu noktada bilgiye yönelik faaliyetlerin bütününü içerecek şekilde "Bilgi Ortamında Harekât" (*Information Environment Operations*) kavramını kavramsal çatı olarak önermektedir. Bu yaklaşım, enformasyonun üretimi, dağıtımı, yönlendirilmesi ve kontrolü yoluyla yürütülen tüm operasyonları birleştiren daha kapsayıcı bir çerçeve sunar.

32 Malik Yılmaz, "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi", *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi* 49, no. 1 (2009): 95-118.
33 İletişim Başkanlığı, *Stratejik İletişim Terimleri Sözlüğü*, Ankara, 2025, s. 56.
34 FM 3-0: *Operations*, Headquarters, Department of the Army, Washington, D.C., 2022, s.1-16,1-18.
35 Malik Yılmaz, a.g.m.

"Bilgi ortamı" kavramı Kuzey Atlantik Antlaşması Örgütü (*North Atlantic Treaty Organization* - NATO) doktrinlerine girmiştir. Dokümanlar, Bilgi Ortamı (BO) değerlendirmesinde BO'yu birbirleriyle etkileşim halinde olan üç temel boyutta ele almaktadır. Bu boyutlar, BO'daki eylemlerin basamaklı ve çok katmanlı etkilerini analiz etmek için temel bir çerçeve sunmaktadır:

- Fiziksel Boyut: Bilginin işlendiği ve iletildiği altyapıyı, donanımı ve insanları içerir. Komuta-kontrol merkezleri, iletişim ağları, sunucular, personel ve silah sistemleri bu boyutun temel unsurlarıdır.
- Sanal Boyut: Bilginin yaratıldığı, işlendiği ve paylaşıldığı ağlar, siber sistemler ve elektromanyetik spektrumu kapsar. Bu boyut, verinin kendisinin bulunduğu alandır.
- Bilişsel Boyut: İnsanların bilgiyi algıladığı, yorumladığı, inanç ve tutumlarını oluşturduğu ve nihayetinde karar verip davranışa dönüştürdüğü zihinsel alandır. Harekâtın nihai hedefi bu boyutta etki yaratmaktır.

Bu boyutlar sıralı değil, iç içe geçmiştir. Örneğin bir fiber optik kabloya yönelik fiziksel bir saldırı (fiziksel boyut), bağlantıyı kesintiye uğratarak (sanal boyut) hasım bir aktörün bu bilgi boşluğunu dezenformasyonla doldurup hedef kitlede panik veya güvensizlik yaratmasına (bilişsel boyut) olanak tanıyabilir. Bu nedenle etkili planlama, etkilerin bu boyutlar arasında nasıl basamaklandığını anlamayı gerektirir.

Türk Silahlı Kuvvetleri'nin doktrin geliştirme yaklaşımı açısından da bu yapı önemlidir. Nitekim Türk Silahlı Kuvvetleri (TSK), "hibrit harp" yerine "hibrit ortamda harekât" terimini kullanmakta; bu tercih, çatışmanın farklı boyutlarının eşzamanlı ve bütünleşik karakterine vurgu yapmaktadır. Benzer biçimde, NATO doktrinleriyle uyumlu olarak "Bilgi Ortamında Harekât" kavramının da TSK literatürüne dâhil edilmesi, bilgi ortamında yürütülen faaliyetlerin stratejik ve doktriner bütünlük içinde ele alınmasına katkı sağlayacaktır.

Ortam, bilginin basit bir veri akışından ibaret olmadığını, aksine onu yorumlayanların önyargıları, gündemleri ve kişisel yorumlama süreçleri gibi sosyal, kültürel ve psikolojik faktörlerle şekillendiğini gösterir. Konunun stratejik önemi de tam olarak bu noktada yatmaktadır: Bilgi Ortamı, en nihayetinde stratejik karar verme süreçlerinin gerçekleştiği temel ortamdır. NATO doktrini, bu karmaşık ortamı anlamlandırmak için "Bilgi Ortamı Değerlendirmesi (*Information Environment Assessment* – IEA)" olarak bilinen analitik bir süreç öngörmektedir.[36] Bu ortamda üstünlük kuran bir aktör, rakibinin kararlarını ve dolayısıyla eylemlerini şekillendirme yeteneği kazanır. Bilgi Ortamı'nın bu çok katmanlı yapısını anlamak, içinde yürütülen farklı harekât türlerini doğru sınıflandırmanın ve stratejik hedeflere uygun araçları seçmenin temelini oluşturur.

2.2. Bilgi Ortamında Harekâtın İki Ana Boyutu

Bu çalışmanın ikinci adımı, bilgi ortamında yürütülen harekâtları, hedefin nihai doğasına göre iki temel kategoriye ayırmaktır. Bu ayrım, harekâtın "bilginin kendisine veya iletimini sağlayan teknik sistemleri mi", yoksa "bilginin yorumlandığı insan bilişimini mi" hedef aldığına dayanmaktadır. Bu sınıflandırma, kullanılan araçlar ile ulaşılmak istenen stratejik etki arasındaki farkı netleştirmektedir.

36 NATO, *Allied Joint Doctrine for Information Operations (AJP-10),* NATO, Brussels, 2021, s. 40.

2.1.1. Bilgiye Yönelik Harp (Knowledge-Focused Warfare):

Bu kategori, doğrudan bilgi sistemlerinin, veri zincirlerinin ve karar destek altyapılarının hedef alındığı faaliyetleri içerir. Amaç, karşı tarafın bilgi edinmesini engellemek, bilgi süreçlerini bozmak ya da bilgi üretimini yönlendirmektir. Bu alanın içerisine Siber harp, elektronik harp, bilgi güvenliği operasyonları, veri akışını manipüle etme, bilgi tekelini koruma gibi hususlar girer.

Bu tür operasyonlar genellikle teknik ve sistem düzeyinde yürütülür. Hedef, insan bilinci değil; veri akışları, komuta-kontrol sistemleri ve askerî karar döngüleridir.

2.1.2. Bilişsel Harp (Cognitive Warfare):

Bilgi ortamındaki ikinci ana faaliyet alanı, doğrudan insan zihnini, algılarını, tutumlarını ve davranışlarını hedef alan harekâtlardır. Bu tür operasyonlarda fiziksel değil bilişsel etki hedeflenir. Bilgiye yönelik harp, bilginin kendisine ve akışına odaklanırken, Bilişsel Harp bilginin ötesine geçerek beynin o bilgiyle ne yapacağını hedefler. Bu nedenle bu mücadele, "bilginin kendisi üzerine değil, bilginin anlamı üzerine bir savaştır".

2.1.3. Zarf ve Mektup Metaforu: Bilgi Akışı mı, Biliş mi?

BYH ile BH arasındaki farkı açıklamak için "zarf ve mektup" metaforu öğretici bir çerçeve sunmaktadır. Bu metaforda, iletişim süreci bir mektubun gönderilmesi ve okunması üzerinden düşünülmüştür.

BYH, mektubun zarfını ve posta sürecini hedef alır. Yani mesajın alıcıya doğru, zamanında ve bütünlük içinde ulaşmasını sağlayan sistemlere müdahale eder. Amaç, bilgi akışını engellemek, zayıflatmak veya bozarak iletişim zincirini kırmaktır. Siber harekât bu alanın en somut örneğidir; mesajın fiziksel veya sanal taşıyıcılarını —ağları, sunucuları, kabloları— hedef alır. Bu, "mektubun yolda kaybolması, gecikmesi veya zarfının hasar görmesi" durumuna benzetilebilir.

Bilişsel Harp (BH) ise mektubun kendisine, yani içeriğin nasıl okunduğu ve anlamlandırıldığına odaklanır. Mektup alıcıya ulaşmıştır; fakat amaç, alıcının onu gönderenin istediği biçimde yorumlamasını sağlamaktır. Burada hedef bilgi akışı değil, bilginin anlamıdır. Bilişsel harp, insanların ne düşündüğünü değil, nasıl düşündüğünü ve davrandığını şekillendirmeyi hedefler. Bu nedenle bilişsel düzeyde yürütülen operasyonlar, mesajın gerçekliğini değil, algısını dönüştürmeyi amaçlar. Bu metafor, bilgi ortamında yürütülen harekâtların iki temel yönünü sade biçimde ayırır:

BYH bilginin taşınma sürecini, BH ise bilginin anlamlandırılma sürecini hedef alır.

Modern savaş ortamında bu iki süreç çoğu zaman iç içe geçer; bir zarfın yırtılması, mektubun içeriğine dair güvensizlik yaratabileceği gibi, yanlış yazılmış bir mektup da göndericinin güvenilirliğini zedeleyebilir. Dolayısıyla bilgi akışına yönelik teknik müdahaleler ile bilişsel algıyı hedefleyen psikolojik operasyonlar, çağdaş çatışmalarda birbirini tamamlayan araçlar hâline gelmiştir.

Çalışmanın bundan sonraki bölümlerinde Bilgi Ortamında Harp'in alt kolları analiz edilecektir.

3. Bilgiye Yönelik Harp: Modern Çatışmada Sistem-Odaklı Strateji

Modern savaşta çatışmanın ağırlık merkezi, fiziksel alanlardan bilgi alanına kaymaktadır. "Bilgiye Yönelik Harp" (BYH), hasmın karar verme döngülerini, komuta-kontrol mekanizmalarını ve bilgi altyapısını doğrudan hedef alan sistem odaklı bir stratejik

yaklaşımdır. Geleneksel psikolojik harbin aksine, insan bilincini değil, bilginin kendisini işleyen sistemleri merkezine alır.[37]

3.1. BYH'nin Temel Nitelikleri

Hedef: Bilgi sistemleri, veri zincirleri ve komuta-kontrol altyapılarıdır. Düşmanın bilgisayar ağlarından sensörlerine, iletişim uydularından radar sistemlerine kadar geniş bir yelpazedeki teknik varlıkları hedefler.

Amaç: Karşı tarafın bilgi edinmesini engellemek, bilgi süreçlerini bozmak ve bilgi üretimini yönlendirmek. Temel gaye, düşmanın durumsal farkındalığını ortadan kaldırmaktır.

Odak Noktası: İnsan bilinci yerine veri akışları, sensörler, ağlar ve askerî karar döngüleri (OODA döngüsü). BYH, bir komutanın moralini bozmak yerine, o komutanın emir almasını sağlayan iletişim ağını çökertmeye odaklanır.[38]

3.2. Stratejik Hedefler

Bilgiye Erişim Üstünlüğü: Bilgi üstünlüğü, bir tarafın kendi bilgi faaliyetlerini serbestçe yürütürken, hasmının aynı faaliyetleri yürütmesini engelleme yeteneğidir.[39] Nihai amaç, "karar üstünlüğü" elde etmektir. Karar üstünlüğü, bir komutanın rakibinden daha etkili kararlar alarak operasyonel inisiyatifi ele geçirmesi anlamına gelir.[40]

Bilgi Akışını Yönlendirmek: Bu hedef, düşmanı aktif olarak yanlış yönlendirmeyi amaçlar. Rus askerî düşüncesindeki "Refleksif Kontrol" teorisi, düşmana sahte dayanaklar sunarak onu kendi iradesiyle bizim istediğimiz yönde kararlar almaya itmeyi hedefler.[41] Düşmanın sensör ağlarını karıştırma gibi eylemler, karar vericinin önüne yanlış bir operasyonel resim koyar.[42]

Karar Alma Süreçlerini Etkilemek: BYH, OODA döngüsünün özellikle "Gözlemle" ve "Yönel" aşamalarına müdahale eder. Amaç, düşmanın karar kalitesini düşürmek ya da karar verme süresini kritik eşiğin üzerine çıkarmaktır.[43]

Bilgi Kaynaklarını Korumak: Dost bilgi altyapısını düşmanın faaliyetlerinden korumak, en az saldırmak kadar önemlidir. Bu hedef, Operasyon Güvenliği (OPSEC) ile doğrudan ilişkilidir ve BYH'nin defansif ayağının temelini oluşturur. [44]

Bilgi Tekelini Elde Bulundurmak: Çatışma bölgesindeki bilgi akışını kontrol etmek, bir gücün kendi anlatısını hem askerî hem de sivil alanda tek geçerli referans noktası haline getirmesini sağlar. Çin'in "Üç Savaş" doktrininin bir parçası olan "kamuoyu savaşı", tam olarak bu hedefe hizmet eder.[45]

---

37 John Arquilla ve David Ronfeldt, "The Advent of Netwar: Analytic Background", *Studies in Conflict & Terrorism* 22:3, 1999, s. 193-206.

38 Edward Waltz, *Information Warfare Principles and Operations*, Artech House, Boston, 1998, s. 16.

39 Martin C. Libicki, "What is Information Warfare?" *ACIS Paper 3*, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, Washington, DC, 1995, s. 94.

40 Headquarters, Department of the Army, *FM 3.0, Operations*, Washington, D.C.: Department of the Army, 2022, s. 3-72.

41 Timothy L. Thomas, "Russia's Reflexive Control Theory and the Military", *Journal of Slavic Military Studies* 17:2, 2004, s. 237-256.

42 Libicki, "What is Information Warfare?", s. 29.

43 North Atlantic Treaty Organization, *Comprehensive Operations Planning Directive COPD V3.1*, NATO, Brussels, 2023, s. 4-71.

44 NATO, AJP-10, s. 2-19.

45 Peter Mattis, "China's 'Three Warfares' in Perspective".

3.3. Temel Araçlar ve Yöntemler

Siber Ağ Harekâtları: Siber savaş, BYH'nin en bilinen aracıdır ve düşmanın bilgisayar sistemlerini hedef alır.[46] NATO doktrininde siber uzay, kara, deniz ve hava gibi ayrı bir harekât alanı olarak tanımlanmıştır.[47] Siber saldırıların faili tespit etmek zordur. Fransız TV5 Monde'a yapılan ve başlangıçta IŞİD tarafından üstlenilen saldırı, daha sonra Rusya bağlantılı APT28 hacker grubunun "sahte bayrak" operasyonu olduğu ortaya çıkmıştır.[48]

Elektronik Harp: Elektromanyetik spektrumu kullanarak düşman radar, iletişim ve seyrüsefer sistemlerini hedef alır. Uygulamaları arasında düşman sinyallerini bastırarak (*jamming*) veya sahte hedefler yaratarak (*deception*) durumsal farkındalığını yok etmek bulunur.[49]

Yönlendirilmiş Enerji Silahları: Elektromanyetik darbe (EMP) kullanarak elektronik devreleri fiziksel olarak tahrip edebilirler. Rus askerî yazarları, Batı'nın ağ merkezli savaş üstünlüğüne karşı asimetrik bir yanıt olarak bu silahların potansiyelini sıkça dile getirmektedir.[50]

Uzay Sistemleri: Modern orduların komuta-kontrol, iletişim ve istihbarat yetenekleri büyük ölçüde uydulara bağımlıdır.[51] Düşman uydularını hedef almak, bir ülkenin tüm askerî ve sivil iletişim altyapısını felç etme potansiyeline sahiptir.[52]

3.4. Değerlendirme

FM 3-0 doktrini, siber alanı eylemin gerçekleştirildiği mekân; bilgi boyutunu ise etkinin odaklandığı alan olarak tanımlar. BYH bu köprüyü operasyonel düzeye indirger: siber, elektromanyetik ve uzay araçlarıyla karar üstünlüğü elde etmeyi hedefler.[53]

BYH, karşı tarafın fizikî gücü yerine bir devletin sinir sistemi —bilgi işleme ve karar verme yeteneğini— hedef alır. Geleneksel psikolojik harbin odağı insan zihni iken BYH odağını makinelere ve komuta-kontrol sistemlerine çevirir. Yapay zekâ, kuantum bilişim ve otonom sistemlerin yaygınlaşması BYH'yi daha merkezi bir alana taşımaktadır; bu yüzden doktrin geliştirmek ve teknolojik yetenek kazanmak artık ulusal güvenliğin temel gerekliliğidir.[54]

4. Bilişsel Harp (*Cognitive Warfare*)

Bilişsel Harp, bilgi ortamındaki harekâtın ikinci ana boyutunu oluşturur. Fiziksel bir etki yerine bilişsel bir etki yaratmayı amaçlayan, insan zihnini, algılarını, tutumlarını ve davranışlarını hedef alan bir mücadele biçimidir.[55] Bu yaklaşım, "bilginin kendisi üzerine değil, bilginin

46 Varlık, Savaşı Tanımlamak: Terminolojik Bir Yaklaşım".
47 NATO, *COPD V3.1*, a.g.e., s.3-39.
48 Pascal Brangetto, Matthijs A. Veenendaal, "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations" ed.Kenneth Geers, *Cyber War in Perspective: Russian Aggression against Ukraine* Tallinn: NATO CCDCOE Publications, Talinn, 2015, 98.
49 David Adamy, *EW 101: A First Course in Electronic Warfare*, Artech House, Boston, 2001, s. 3.
50 Age, s. 4.
51 Timothy Thomas, "Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?" *The Journal of Slavic Military Studies,* 27:1, 2014, 101-130.
52 Yaakov Katz ve Amir Bohbot, *The Weapon Wizards*, St. Martin's Press, New York, 2017.
53 *FM 3.0, Operations*, s.1-17/1-23.
54 Dean S. Hartley III ve Kenneth O. Jobson, *Cognitive Superiority: Information to Power*, Springer International, Cham, 2021, s. 25-133.
55 NATO, *Cognitive Warfare*, NATO, Brussels, 2023, 1–3.

anlamı üzerine bir savaştır."[56] Nihai hedef, hedef kitlenin düşünce yapısını ve ardından eylemlerini etkilemektir. Başka bir deyişle, BH, bir hedef kitlenin nasıl düşündüğünü ve dolayısıyla nasıl davrandığını manipüle etme sanatıdır.[57]

Bu yaklaşım, bilgi ortamındaki diğer operasyonlardan temel bir farkla ayrılır. Bilgiye yönelik geleneksel operasyonlar teknik sistemlere odaklanırken, BH doğrudan insanın karar alma süreçlerini hedef alır.

4.1. Stratejik Hedefler ve Değişen Paradigma

Geleneksel askerî ve hükümet yapıları hedef olmaya devam etse de birincil savaş alanı artık rakip veya tarafsız bir ulusun kamu bilincini de kapsayacak şekilde genişlemiştir. Bu paradigma değişimi, çatışmayı sürekli hale getirmekte ve barış ile savaş arasındaki çizgileri bulanıklaştırmaktadır.

Bir ulusun kamuoyunu etkilemek artık belirleyici bir faktör olarak görülmektedir. Hükümetlerin başarısı, Edward Bernays'in belirttiği gibi, "rıza gösteren bir kamuoyuna" bağlıdır.[58] Bir aktör, kamu algısını şekillendirerek bir hükümetin meşruiyetini sarsabilir, ulusal iradeyi aşındırabilir ve geleneksel askerî eylemlerden çok daha düşük maliyetlerle stratejik hedeflerine ulaşabilir. Bu yaklaşım, ABD Stratejik Hizmetler Ofisi'nin (OSS) 1943 tarihli dokümanında belirtilen "askerî eylem dışındaki yollarla irademizi düşmana dayatmak" hedefiyle uyumludur.[59] Bu, hasmın karar alma süreçlerini felç etmek ve toplumsal uyumu bozmak suretiyle, fiziksel bir çatışmaya gerek kalmadan zafer elde etmek anlamına gelir.

4.2. Bilişsel Harp Yöntemleri

BH yöntemleri, bilişsel çevreyi şekillendirmek üzere tasarlanmış, açık ve ikna edici angajmandan gizli ve manipülatif eylemlere kadar geniş bir yelpazede faaliyet gösterir.

4.2.1. Açık faaliyetler:

Bilişsel harbin açık biçimleri genellikle etki operasyonları olarak tanımlanır. Bu faaliyetler, toplumların, kültürlerin ve karar vericilerin algılarını yönlendirmeye yönelik, doğrudan görünür stratejilerdir. Etki harbi; stratejik iletişim, kamu diplomasisi, kültürel diplomasi, yumuşak güç ve dijital diplomasi gibi araçlarla yürütülür. Yöntemlerinden bazıları aşağıda sunulmuştur.

Algı Yönetimi, devlet, lider veya olay hakkındaki algının sistematik biçimde şekillendirilmesini ifade eder. Medya manipülasyonu, kamuoyu araştırmaları, devlet destekli ajanslar ve propaganda mekanizmalarıyla desteklenir.[60] Özellikle kriz dönemlerinde algı yönetimi, rakip aktörlerin itibarsızlaştırılması ve kendi eylemlerinin meşrulaştırılması amacıyla yoğun biçimde kullanılır.

Stratejik İletişim, müttefikleri kazanmak, tarafsızları yönlendirmek ve düşmanları caydırmak için bütünleşik söylemler üretmeyi amaçlar. Lider konuşmaları, semboller ve medya içerikleri üzerinden ulusal irade yaratılır.[61]

---

56 Steve A. Tatham, *Strategic Communication: A Primer*, Defence Academy of the United Kingdom, Shrivenham, 2008, s. 2.

57 Oliver Backes ve Andrew Swab, "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States", Harvard Kennedy School, Belfer Center for Science and International Affairs, November 2019. https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states, erişim: 15 Ekim 2025

58 Edward Bernays, *Propaganda*, H. Liveright, New York, 1928, s.10.

59 Jr., *On Political War*, s. 226.

60 Walter Lippmann, *Public Opinion*, Harcourt, Brace and Company, New York, 1922, s. 33-35.

61 Richard Halloran, "Strategic Communication", *Parameters*, 38:3, 2007.

Kamu Diplomasisi, doğrudan halklar arasındaki iletişim üzerinden etki kurmayı hedefler. Edmund Gullion'un 1965'te kavramsallaştırdığı kamu diplomasisi, devletlerin güvenlik ve çıkarlarını korumak için yürüttükleri iletişim faaliyetlerini içerir.[62] Günümüzde yumuşak gücün önemli bir unsuruna dönüşmüştür.[63]

Kültürel Diplomasi, ulusal çıkarların kültürel anlatılar yoluyla desteklenmesidir. Güney Kore'nin K-Pop ve K-Drama endüstrileri veya Çin'in Konfüçyüs Enstitüleri, başarılı örnekler arasındadır.

Yumuşak Güç Araçları (insani yardım, eğitim, barış gücü programları), zorlayıcı olmayan yollarla etki yaratır. ABD'nin Peace Corps programı veya Türkiye'nin Afrika'daki insani yardım faaliyetleri bu kapsamda değerlendirilebilir.

Dijital Diplomasi, liderlerin ve hükümetlerin sosyal medya üzerinden yürüttüğü diplomatik etki faaliyetlerini kapsar.[64] Donald Trump'ın dış politika mesajlarını Twitter aracılığıyla doğrudan vermesi veya Zelenskiy'nin küresel kamuoyuna video mesajlarıyla seslenmesi çarpıcı örneklerdir.

Etki harbi yalnızca söylem düzeyinde yürütülmez; aynı zamanda bilgi ve coğrafya üzerinden de şekillenir. *Tarihin Yeniden Yazımı*, ulusal kimlikleri ve kolektif hafızayı değiştirme amacı taşır.[65] *Jeo-uzamsal Manipülasyon*, haritalar, uydu görüntüleri ve coğrafi verilerin politik amaçlarla çarpıtılmasıdır.[66]

Etki harbinin son aşaması küresel kamuoyu yönetimidir. Bu düzeyde, devletler politikalarını meşrulaştırmak için uluslararası medya, BM kararları ve hukuk söylemlerini seferber eder.[67] Rusya'nın Ukrayna'daki eylemlerini "savunma hakkı" çerçevesinde sunması, Batı'nın ise "insan hakları" vurgusuyla karşı anlatı geliştirmesi, bu stratejinin iki yönünü oluşturur.[68]

4.2.2. Örtülü faaliyetler:

Bilişsel harbin örtülü biçimleri, bireylerin bilinç düzeyini hedef alır ve manipülasyonu doğrudan zihin düzeyinde gerçekleştirir. Bu kapsamda dezenformasyon, sosyal mühendislik, refleksif kontrol, gerçekliğin çürümesi, gerçek sonrası stratejileri ve nöroteknolojik müdahaleler öne çıkar.

Bilgi Manipülasyonu, doğru bilginin çarpıtılması veya yanlış bilgiyle yer değiştirmesi yoluyla hedefin algısının yönlendirilmesidir. Yanlış bilgi (*misinformation*) bilinçsizce; dezenformasyon (*disinformation*) ise kasıtlı biçimde yayılır. Malenformasyon ise doğru bilginin bağlamından koparılarak zarar verme amacıyla kullanılmasıdır.

62 İletişim Başkanlığı, *Stratejik İletişim ve Stratejik Yönetim*, İletişim Başkanlığı Yayınları, Ankara, 2023, s. 26.
63 Abdullah Özkan, *21. Yüzyılın Stratejik Vizyonu: Kamu Diplomasisi ve Türkiye'nin Kamu Diplomasisi İmkânları*, TASAM Kamu Diplomasisi Enstitüsü, 2021, s. 18.
64 İletişim Başkanlığı, Stratejik İletişim ve Stratejik Yönetim, s. 99-101.
65 Margaret MacMillan, *Dangerous Games: The Uses and Abuses of History*, Modern Library, New York, 2009, s. 14-15.
66 Bakınız: Dr. Michael Izady, "Infographs, Maps and Statistics Collection", https://gulf2000.columbia.edu/maps.shtml, erişim:15 Ekim 2025; Avusturya İç İşleri Bakanlığı, "Ortadoğu ve Kuzey Afrika Atlası", https://www.ecoi.net/en/file/local/1408000/90_1487770786_2017-02-bfa-mena-atlas.pdf, erişim: 15 Ekim 2025; "Cartorient", https://cartorient.cnrs.fr/accueil, erişim: 15 Ekim 2025; Michael Izady'nin haritaları, Kürt nüfusunu olduğundan fazla gösterdiği için Kürdologlar tarafından bile eleştirilmiştir. Kürdolog ve İranolog Garnik Asatrian, Kürdoloji'deki sözde-tarihcilik hakkında bilgi verirken İzedi'nin "*1992 tarihli Kürtler: Bir El Kitabı"*ndan "fantazmagorik" olarak bahseder. Garnik Asatrian, "Prolegomena to the Study of the Kurds," *Iran and the Caucasus*, 13:1, 2009, s. 1-57.
67 Philip M. Taylor, "Public Diplomacy and Strategic Communications," *The Hague Journal of Diplomacy*, 3:3, 2008, s. 1-11.
68 Lawrence Freedman, *Ukraine and the Art of Strategy*, Oxford University Press, Oxford, 2019, s. 99-102.

Psikolojik Operasyonlar, düşmanın moralini bozmak ve davranışlarını yönlendirmek için propaganda tekniklerinden yararlanır.[69] Günümüzde sosyal medya trol ağları, sahte video içerikleri ve yapay etiket (*hashtag*) kampanyaları bu süreci dijital boyuta taşımıştır. İkinci Karabağ savaşında Azerbaycan'ın drone görüntülerini kısa videolarla göstermesi etkili bir psikolojik operasyon örneğidir.

Sosyal Mühendislik, bireyleri manipüle ederek bilgi sızdırma ve gizli verilere erişim amacı taşır. "İnsan korsanlığı" olarak da bilinen bu yöntem, *phishing* ve kimlik avı teknikleriyle uygulanır.[70]

Gerçekliğin Çürümesi (*Truth Decay*), nesnel bilginin değerinin azaldığı, görüş ve deneyimlerin gerçeğin yerini aldığı bir süreci ifade eder.[71] Deepfake videolar, sahte haber siteleri ve sosyal medya botları, gerçek ile yalan arasındaki sınırı silikleştirir.

Gerçek Sonrası (*Post-Truth*) stratejiler, duyguların ve kişisel inançların nesnel gerçeklerin önüne geçtiği bir ortam yaratır.[72] 2016'daki Brexit referandumu ve ABD başkanlık seçimleri, bu stratejinin tipik örnekleridir. Sosyal medya algoritmaları, yankı odaları ve filtre balonları aracılığıyla bireyler yalnızca kendi inançlarına uygun bilgileri görür.

Kutuplaştırma, bilişsel harbin hem sonucu hem aracıdır.[73] Toplumları ideolojik, etnik veya dini çizgiler boyunca bölerek iç istikrarsızlık üretir.

Refleksif Kontrol, düşmanın kendi iradesiyle hatalı kararlar almasını sağlamak için geliştirilen bir Rus stratejisidir.[74] Yanıltıcı istihbarat, sahte veriler ve çarpıtılmış bilgiyle, hedefin karar döngüsü manipüle edilir.

Neokortikal Harp, karar vericilerin bilişsel süreçlerine doğrudan müdahale ederek, OODA döngüsünü kırmayı hedefler.[75] Bilgi blokajı, aşırı veri yüklemesi ve psikolojik baskı yöntemleriyle düşmanın stratejik düşünme kapasitesi zayıflatılır.

Anlatı Harbi, olayların nasıl yorumlandığını değiştirerek kolektif hafızayı dönüştürür.[76] Sinema, medya ve dijital platformlarda kurgulanan hikâyeler, toplumların geçmiş algısını yeniden şekillendirir.

Nöroteknolojik Müdahaleler, bilişsel harbin en ileri aşamasıdır. Dr. James Giordano'ya göre, beyin modern çatışmaların "yeni savaş alanıdır."[77] Elektromanyetik dalgalar, kimyasal ajanlar veya yapay zekâ destekli psikolojik analizlerle askerî personelin moral düzeyleri etkilenebilir.

---

69 Psikolojik Operasyonlar (*Psychological Operations* (PSYOP)) – Geleneksel olarak kullanılan terimdir, ancak ABD Savunma Bakanlığı bu terimi *Military Information Support Operations* (MISO) olarak değiştirmiştir. Joint Chiefs of Staff, *JP 3-13.2, Military Information Support Operations (MISO)*, Joint Chiefs of Staff, Washington, DC, 2014.

70 "Sosyal Mühendislik Nedir?", https://www.kaspersky.com.tr/resource-center/definitions/what-is-social-engineering erişim 20.02.2025.; M. Zekeriya Gündüz ve Resul Daş, "Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri ", https://www.bingol.edu.tr/documents/Sosyal%20M%C3%BChendislik-yayg%C4%B1n%20Ataklar%20ve%20G%C3%BCvenlik%20%C3%96nlemleri.pdf, erişim 20.02.2025.

71 "About Truth Decay", RAND Corporation, https://www.rand.org/research/projects/truth-decay/about-truth-decay.html erişim 23.02.2025.

72 Lee McIntyre, *Post-Truth*, The MIT Press, Cambridge, MA, 2018, s. 5-7.; Matthew d'Ancona, *Post-Truth: The New War on Truth and How to Fight Back*, Ebury Press, London, 2017, s. 12-15.

73 Shanto Iyengar ve Sean J. Westwood, "Fear and Loathing Across Party Lines: New Evidence on Group Polarization", *American Journal of Political Science*, 59:3, 2015, s. 690-707.

74 Timothy L. Thomas, "Russia's Reflexive Control Theory".

75 Richard Szafranski, "Neocortical Warfare", John Arquilla ve David Ronfeldt (ed.), *Athena's Camp: Preparing for Conflict in the Information Age*, RAND Corporation, Santa Monica, CA, 1997.

76 Ajit Maan, "Narrative Warfare", *RealClearDefense,* https://www.realcleardefense.com/articles/2018/02/27/narrative_warfare_113118.html, erişim 21.02.2025.

77 James Giordano, "Brain as the Battlefield of the Future", YouTube video, 1:02:30, uploaded by Modern War Institute, September 25, 2018, https://www.youtube.com/watch?v=N02SK9yd60s, erişim 21.02.2025.

4.3. Değerlendirme

BH, çağdaş çatışma doktrinlerinde fiziksel güç kullanımının yerini alan stratejik bir paradigma değişimini temsil eder. Açık faaliyetler, toplumların algısını ve uluslararası meşruiyeti hedeflerken, örtülü faaliyetler bireylerin bilinç süreçlerini kontrol altına alır.

Bu iki boyut birbirini tamamlar: Etki operasyonları kamuoyu düzeyinde "görünür alanı", BH ise "zihin alanını" yönetir. Dijital çağda bu sınır tamamen silinmiş, savaşın nihai hedefi insan bilinci olmuştur.

Devletlerin, örgütlerin ve teknolojik platformların bilgi üzerindeki hakimiyeti, aynı zamanda zihin üzerindeki hakimiyet anlamına gelmektedir. Bu nedenle "bilişsel güvenlik" artık ulusal güvenliğin yeni cephesidir. Bu cephede üstünlük, tanklar veya füzelerle değil; anlatılar, algoritmalar ve algılarla sağlanmaktadır.

BH, klasik savaşın sınırlarını aşarak, insanın düşünme biçimini stratejik bir hedefe dönüştürmüştür. Bu nedenle geleceğin çatışmaları, toprak kazanmak için değil, zihinleri yönetmek için yürütülecektir.

5. Hibrit Etkileşim

Bilgiye Yönelik Harp ile Bilişsel Harp kavramsal olarak farklı hedeflere odaklanmakla birlikte, modern çatışma ortamında birbirini besleyen ve tamamlayan iki bütünleşik alan haline gelmiştir. BYH teknik sistemleri, veri zincirlerini, haberleşme ağlarını ve komuta-kontrol altyapılarını hedef alarak düşmanın bilgi üretim ve aktarım kapasitesini zayıflatırken; BH bu teknik etkinin sonuçlarını insan zihnine, algısına ve karar süreçlerine yönlendirir. Böylece bilgi ortamında yürütülen harekâtlar, hem fiziksel-dijital hem de bilişsel-psikolojik düzeyde etki üretir.

Bu iki alan arasındaki etkileşim, modern savaşlarda "hibrit bilgi harekâtı" olarak adlandırılabilecek yeni bir boyut doğurmuştur. Hibrit bilgi harekâtı, teknik müdahaleyle algısal manipülasyonun senkronize biçimde kullanılması anlamına gelir. Örneğin bir siber saldırı yalnızca bir altyapıyı devre dışı bırakmak için değil, aynı zamanda toplumda güvensizlik, panik veya moral çöküntüsü yaratmak için planlanabilir. Böylece teknik bir operasyon, bilişsel düzeyde kalıcı sonuçlar doğurur. Tersine, geniş kapsamlı dezenformasyon kampanyaları da teknik sistemleri aşırı yükleyerek veya iletişim hatlarını manipüle ederek operasyonel sonuçlar üretebilir.

NATO doktrinleri açısından bakıldığında, bu hibrit yapı "bilgi ortamının çok-alanlı entegrasyonu" (*information environment's cross-domain integration*) olarak tanımlanır. AJP-10 ve AJP-3 serisi doktrinlerde bilgi ortamı; fiziksel, sanal ve bilişsel katmanların karşılıklı bağımlılık içinde olduğu bir ekosistem olarak ele alınır. Dolayısıyla bir katmanda yaratılan etki diğerine zincirleme biçimde yansır. Bu yaklaşım, bilgi ortamındaki harekâtların artık belirli bir alana hapsedilemeyeceğini, bunun yerine çok katmanlı ve senkronize biçimde icra edilmesi gerektiğini göstermektedir.

Rusya'nın 2014 Kırım ilhakı ve 2022 Ukrayna işgali, bu hibrit etkileşimin en somut örneklerindendir. 2014'te iletişim hatlarının kesilmesi, paralel biçimde yürütülen medya operasyonları ve sahte haber kampanyalarıyla desteklenmiş; siber saldırılar, bilgiye erişimi kısıtlarken, eşzamanlı dezenformasyon, Ukrayna kamuoyunun moralini zayıflatmayı hedeflemiştir. Bu süreçte BYH ve BH faaliyetleri arasında keskin bir sınır kalmamış, bilişsel sonuç doğuran teknik eylem kalıbı kurumsallaşmıştır. Aynı stratejik yaklaşım 2022'de de yinelenmiş; dronelar, GPS bozucular ve elektronik harp sistemleriyle desteklenen bilgi saldırıları, kamuoyunun algısal yönlendirilmesiyle birleştirilmiştir.

Sonuç olarak hibrit bilgi ortamı harekâtı, savaşın hem "görünür" hem "görünmez" alanlarını eş zamanlı kullanan, teknik yıkımı algısal manipülasyonla bütünleştiren yeni bir harekât biçimidir. Bu durum, bilgi ortamında üstünlük sağlamanın yalnızca teknik kapasiteyle değil, bilişsel direnç ve toplumsal farkındalık unsurlarıyla da doğrudan ilişkili olduğunu ortaya koymaktadır.

Sonuç

Bu çalışma, bilgi ortamında yürütülen harekâtların kavramsal çerçevesini yeniden yapılandırmak ve Türkçe literatürde uzun süredir devam eden terminolojik karmaşayı gidermek amacıyla hazırlanmıştır. Çalışmanın ilk bulgusu, "bilgi harbi" teriminin hem epistemolojik hem de operasyonel açıdan yetersiz kaldığıdır. Türkçede "bilgi" kavramı, anlamlandırılmış ve içselleştirilmiş bir zihinsel ürünü ifade ederken, İngilizce "*information*" terimi düzenlenmiş veri veya aktarım sürecine karşılık gelir. Bu fark, doğrudan çeviriyle oluşturulan "bilgi harbi" kavramının hem anlam hem de kapsam bakımından hatalı bir temele oturduğunu göstermektedir.

Bu nedenle çalışma, "bilgi harbi" teriminin yerine, bilgiye, insan zihnine ve karar süreçlerine yönelik tüm faaliyetleri kapsayan daha bütüncül bir kavram olarak "Bilgi Ortamında Harekât" veya "Bilgi Ortamında Harp" terimini önermektedir. Bu kavram, NATO'nun AJP-10 ve AJP-10.1 doktrinlerinde tanımlanan *"Information Environment"* anlayışıyla uyumludur. Böylece bilgi ortamı; fiziksel, sanal ve bilişsel boyutlarıyla birlikte ele alınmış; bu üç alanın karşılıklı etkileşimi, modern savaşın temel dinamiği olarak konumlandırılmıştır.

Çalışmanın ikinci temel amacı, bilgi ortamında yürütülen faaliyetleri sistematik biçimde sınıflandırmaktır. Bu hedef, bilgi ortamındaki harekâtların nihai hedeflerine göre iki ana kategoriye ayrılmasıyla karşılanmıştır: Bilgiye Yönelik Harp ve Bilişsel Harp.

BYH, sistem-odaklıdır. Düşmanın bilgi toplama, işleme ve iletim kapasitesini hedef alır; siber harp, elektronik harp, refleksif kontrol ve komuta-kontrol savaşı gibi teknik araçlarla yürütülür. Amaç, hasmın karar verme yeteneğini felç etmek ve bilgi üstünlüğü sağlamaktır. BH ise insan zihnini, algılarını ve tutumlarını hedef alır. Etki harbi, psikolojik operasyonlar, dezenformasyon kampanyaları, anlatı inşası ve nöroteknolojik müdahaleler gibi araçlarla toplumların düşünme biçimlerini dönüştürmeyi amaçlar.

Bu iki alan arasındaki fark, hedefin mahiyetindedir: BYH bilginin kendisine, BH ise bilginin anlamına yöneliktir. Ancak günümüz hibrit çatışma ortamında bu iki alan giderek iç içe geçmekte, bir siber saldırı bilişsel bir etki üretebilmekte, bir dezenformasyon kampanyası da stratejik karar mekanizmalarını doğrudan etkileyebilmektedir. Bu durum, bilgi ortamındaki operasyonların çok katmanlı doğasını ve disiplinler arası niteliğini açıkça göstermektedir.

Modern savaşın ağırlık merkezi artık fiziksel alandan bilgi ve bilinç alanına kaymıştır. Clausewitz'in "düşmanı irademizi kabul etmeye zorlama" ilkesi, 21. yüzyılda tanklar ve tüfeklerle değil, algoritmalar, anlatılar ve algılarla gerçekleştirilmektedir. Dijitalleşme, yapay zekâ, kuantum bilişim ve nöroteknolojideki ilerlemeler, bilgi ortamında harekâtın hem kapsamını genişletmiş hem de etkisini derinleştirmiştir. Bu nedenle, savaşın geleceği artık "toprak kazanmak"tan çok, "zihinleri yönetmek"le ilgilidir.

Bu bağlamda, Türk Silahlı Kuvvetleri ve ulusal güvenlik kurumlarının bilgi ortamında yürütülen harekâtlara ilişkin açık, tutarlı ve hiyerarşik bir kavramsal çerçeve geliştirmesi stratejik bir zorunluluktur. Mevcut doktrinlerdeki kavramsal belirsizlik hem akademik düzeyde anlaşılırlığı hem de operasyonel düzeyde etkinliği sınırlamaktadır. Bu

çerçevede, Türk Silahlı Kuvvetleri'nin "hibrit ortamda harekât" yaklaşımında olduğu gibi, "Bilgi Ortamında Harekât" kavramının da doktrin ve eğitim sistemine dâhil edilmesi, bilgi ortamında üstünlük arayışını kurumsal düzeyde güçlendirecektir. Böyle bir kavramsal uyum, Türkiye'nin hem NATO doktrinleriyle eşgüdümünü artıracak hem de bilgi boyutunda bağımsız harekât planlama kapasitesine teorik bir temel sağlayacaktır. Bu çalışmanın önerdiği terminolojik ayrım ve sistematik yapı, gelecekteki doktrin çalışmaları, eğitim programları ve stratejik planlamalar için sağlam bir temel teşkil etme potansiyeline sahiptir.

Sonuç olarak, çalışma iki temel amacına ulaşmıştır:

- Türkçe literatürde "bilgi harbi" kavramının yarattığı terminolojik ve doktriner sorunları eleştirel biçimde analiz etmiş, yerini alabilecek bütünleştirici bir üst kavram önermiştir.
- Bilgi ortamındaki faaliyetleri hedefin doğasına göre ikili bir yapıda sistemleştirerek, kavramsal hiyerarşi ve teorik açıklık sağlamıştır.

Bu çerçeve, komuta-kontrol doktrinlerinin bilgi ortamına uyarlanması, bilişsel dayanıklılık eğitimleri ve sivil-asker bilgi iş birliği modelleriyle somutlaştırılabilir.

Bilgiye hükmeden, anlamı yöneten ve bilişsel çevreyi şekillendiren aktörlerin, modern savaşın ve barışın gerçek belirleyicileri olduğu açıktır. Geleceğin çatışmaları artık fiziksel alanlarda değil, insan zihninin sınırlarında yaşanacaktır. Bilgi ortamında üstünlük kuramayan hiçbir devlet, konvansiyonel gücü ne olursa olsun, stratejik rekabette kalıcı bir üstünlük elde edemeyecektir.

Çıkar Çatışması

Bu çalışmada çıkar çatışması teşkil edebilecek durum ve/veya ilişki bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Çalışmada herhangi bir şekilde yapay zeka uygulamalarından yararlanılmamıştır.

KAYNAKÇA

Basılı Eserler

ADAMY David (2001). *EW 101: A First Course in Electronic Warfare*, Artech House, Boston.

ARQUILLA John ve RONFELDT David (1999). "The Advent of Netwar: Analytic Background", *Studies in Conflict & Terrorism*, 22:3, 193-206.

ASATRIAN Garnik (2009). "Prolegomena to the Study of the Kurds", *Iran and the Caucasus*, 13:1, 1-57.

ATEŞ Barış ve MERCAN Evren (2023). "Yeni Savaşlar ve Yeni Ordular", *Güvenlik Stratejileri Dergisi*, Özel Sayı, 1-11.

AYVERDİ İlhan (2010). *Misalli Büyük Türkçe Sözlük*, Kubbealtı Yayınları, İstanbul.

BELLAMY Christopher (1984). *The Evolution of Modern Land Warfare Theory and Practice*, Routledge, New York.

BERNAYS Edward (1928). *Propaganda*, Horace Liveright, New York.

BRANGETTO Pascal ve VEENENDAAL Matthijs A. (2015). "Influence Cyber Operations: The Use of Cyberattacks in Support of Influence Operations", *Cyber War in Perspective: Russian Aggression against Ukraine*, ed. Kenneth Geers, NATO CCDCOE Publications, Tallinn.

ÇAĞBAYIR Yaşar (2007). *Orhun Yazıtlarından Günümüze Türkiye Türkçesinin Söz Varlığı – Ötüken Türkçe Sözlük*, Ötüken Yayınları, İstanbul.
CLAUSEWITZ Carl von (1984). *On War* (çev. Michael Howard ve Peter Paret), Princeton University Press, Princeton.
CLAUSON Gerard (1972). *An Etymological Dictionary of Pre-Thirteenth-Century Turkish*, Clarendon Press, Oxford.
D'ANCONA Matthew (2017). *Post-Truth: The New War on Truth and How to Fight Back,* Ebury Press, London.
DE GOEIJ Maria W. (2023). "Reflexive Control: Influencing Strategic Behavior", *Parameters*, 53:4, 97-108.
ERGÜDER Orhan (1959). *Harb Tarihi*, Kara Harp Okulu Basımevi, Ankara.
FLORIDI Luciano (2011). *The Philosophy of Information*, Oxford University Press, Oxford.
FREEDMAN Lawrence (2019). *Ukraine and the Art of Strategy*, Oxford University Press, Oxford.
HALLORAN Richard (2008). "Strategic Communication", *Parameters*, 38:3. 4-14
HARTLEY Dean S. III ve JOBSON Kenneth O. (2021). *Cognitive Superiority: Information to Power*, Springer International, Cham, 25-133.
HEADQUARTERS DEPARTMENT OF THE ARMY (2022). *FM 3-0: Operations*, Washington, D.C.
İLETİŞİM BAŞKANLIĞI (2023). *Stratejik İletişim ve Stratejik Yönetim*, İletişim Başkanlığı Yayınları, Ankara,
İLETİŞİM BAŞKANLIĞI (2025). *Stratejik İletişim Terimleri Sözlüğü*, İletişim Başkanlığı Yayınları, Ankara.
IYENGAR Shanto ve WESTWOOD Sean J. (2015). "Fear and Loathing Across Party Lines: New Evidence on Group Polarization", *American Journal of Political Science*, 59:3, 690-707.
JOINT CHIEFS OF STAFF (2014). *JP 3-13.2, Military Information Support Operations (MISO),* Joint Chiefs of Staff, Washington, D.C.
KATZ Yaakov ve BOHBOT Amir (2017). *The Weapon Wizards*, St. Martin's Press, New York.
KENNAN George F. (1948). *The Inauguration of Organized Political Warfare*, Memorandum, Policy Planning Staff, ABD Dışişleri Bakanlığı, 4 Mayıs 1948.
LIBICKI Martin C. (1995). "What is Information Warfare?", ACIS Paper 3, Center for Advanced Concepts and Technology, Institute for National Strategic Studies, National Defense University, Washington, D.C.
LIPPMANN Walter (1922). *Public Opinion*, Harcourt, Brace and Company, New York.
MACMILLAN Margaret (2009). *Dangerous Games: The Uses and Abuses of History*, Modern Library, New York.
McINTYRE Lee (2018). *Post-Truth*, The MIT Press, Cambridge, MA.
McLUHAN Marshall (1964). *Understanding Media: The Extensions of Man*, McGraw-Hill, New York.
MILLER Benjamin (2007). *States, Nations, and the Great Powers: The Sources of Regional War and Peace,* Cambridge University Press, Cambridge.
NATO (2021). *Allied Joint Doctrine for Information Operations (AJP-10),* NATO, Brussels.
NATO (2023). *Cognitive Warfare*, NATO, Brussels.
NORTH ATLANTIC TREATY ORGANIZATION (2023). *Comprehensive Operations Planning Directive (COPD)* V3.1, NATO, Brussels.
ÖZKAN Abdullah (2021). *21. Yüzyılın Stratejik Vizyonu: Kamu Diplomasisi ve Türkiye'nin Kamu Diplomasisi İmkânları*, TASAM Kamu Diplomasisi Enstitüsü.
PRATKANIS Anthony ve ARONSON Elliot (2001). *Age of Propaganda: The Everyday Use and Abuse of Persuasion,* W. H. Freeman, New York.
QIAO Liang ve WANG Xiangsui (1999). *Unrestricted Warfare: China's Master Plan to Destroy America*, PLA Literature and Arts Publishing House, Beijing.
SCHELLING Thomas (1960). *The Strategy of Conflict*, Harvard University Press, Cambridge, MA.
SINGER P.W. ve BROOKING Emerson T. (2018). *LikeWar: The Weaponization of Social Media*, Houghton Mifflin Harcourt, Boston.
SMITH Paul A. Jr. (1989). *On Political War*, National Defense University Press, Washington D.C.
SUN Tzu (1963). *The Art of War* (çev. Samuel B. Griffith), Oxford University Press, Oxford.
SZAFRANSKI Richard (1994). "Neocortical Warfare? The Acme of Skill", *Military Review* 74:11, 41-55.
SZAFRANSKI Richard (1997). "Neocortical Warfare", *Athena's Camp: Preparing for Conflict in the Information Age*, ed. John Arquilla ve David Ronfeldt, RAND Corporation, Santa Monica, CA, Bölüm 17.
TATHAM Steve A. (2008*). Strategic Communication*: A Primer, Defence Academy of the United Kingdom, Shrivenham.

TAYLOR Philip M. (2003). *Munitions of the Mind: A History of Propaganda from the Ancient World to the Present Era*, Manchester University Press, Manchester.

TAYLOR Philip M. (2008). "Public Diplomacy and Strategic Communications", *The Hague Journal of Diplomacy*, 3:3, 1-11.

THOMAS Timothy (2014) Russia's Information Warfare Strategy: Can the Nation Cope in Future Conflicts?, *The Journal of Slavic Military Studies*, 27:1, 101-130.

THOMAS Timothy L. (2004). "Russia's Reflexive Control Theory and the Military", Journal of Slavic Military Studies, 17:2, 237-256.

VARLIK Ali Bilgin (2013). "Savaşı Tanımlamak: Terminolojik Bir Yaklaşım", *Avrasya Terim Dergisi*, 1:2, 114-129.

WALTZ Edward (1998). *Information Warfare: Principles and Operations*, Artech House, Boston.

YET Dağhan (2023). "Malumat Savaşında Hızlı-Etki Yaklaşımı: Türkiye Deneyimi", Barış Ateş (ed.), *Türkiye'de Askerî Yenilik*, Vakıfbank Kültür Yayınları, İstanbul, 315-341.

YILMAZ Malik (2009). "Enformasyon ve Bilgi Kavramları Bağlamında Enformasyon Yönetimi ve Bilgi Yönetimi", *Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Dergisi*, 49:1, 95-118.

İnternet Kaynakları

About Truth Decay, RAND Corporation, https://www.rand.org/research/projects/truth-decay/about-truth-decay.html, erişim 23.02.2025.

AVUSTURYA İÇ İŞLERİ BAKANLIĞI, "Ortadoğu ve Kuzey Afrika Atlası", https://www.ecoi.net/en/file/local/1408000/90_1487770786_2017-02-bfa-mena-atlas.pdf, erişim 15.10.2025.

BACKES Oliver ve SWAB Andrew (2019). "Cognitive Warfare: The Russian Threat to Election Integrity in the Baltic States", Harvard Kennedy School, Belfer Center for Science and International Affairs, https://www.belfercenter.org/publication/cognitive-warfare-russian-threat-election-integrity-baltic-states, erişim 15.10.2025.

Cartorient, https://cartorient.cnrs.fr/accueil, erişim 15.10.2025.

GERASIMOV Valery (2013). "The Value of Science in Prediction", Military-Industrial Kurier https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf, erişim 21.02.2025.

GIORDANO James (2018). "Brain as the Battlefield of the Future", YouTube video, Modern War Institute, https://www.youtube.com/watch?v=N02SK9yd60s, erişim 21.02.2025.

GÜNDÜZ M. Zekeriya ve DAŞ Resul, Sosyal Mühendislik: Yaygın Ataklar ve Güvenlik Önlemleri, https://www.bingol.edu.tr/documents/Sosyal%20M%C3%BChendislik-yayg%C4%B1n%20Ataklar%20ve%20G%C3%BCvenlik%20%C3%96nlemleri.pdf, erişim 20.02.2025.

Information. Online Etymology Dictionary, https://www.etymonline.com/word/information, erişim 15.10.2025.

IZADY Michael, "Infographs, Maps and Statistics Collection", https://gulf2000.columbia.edu/maps.shtml, erişim 15.10.2025.

MAAN Ajit (2018). "Narrative Warfare", RealClearDefense, https://www.realcleardefense.com/articles/2018/02/27/narrative_warfare_113118.html, erişim 21.022025.

MATTIS Peter (2018). "China's 'Three Warfares' in Perspective", War on the Rocks, 30 Ocak 2018, https://warontherocks.com/2018/01/chinas-three-warfares-perspective/, erişim 15.03.2025.

MWI, "MWI Video: The Brain is the Battlefield of the Future – Dr. James Giordano", https://mwi.westpoint.edu/mwi-video-brain-battlefield-future-dr-james-giordano/, erişim 10.03.2025.

SELVAGE Douglas ve NEHRING Christopher, Operation "Denver": KGB and Stasi Disinformation regarding AIDS, https://www.wilsoncenter.org/blog-post/operation-denver-kgb-and-stasi-disinformation-regarding-aids, erişim 20.02.2025.

Sosyal Mühendislik Nedir?, https://www.kaspersky.com.tr/resource-center/definitions/what-is-social-engineering, erişim 20.02.2025.

The Catholic Encyclopedia, s.v. "Congregation for the Propagation of the Faith," https://www.newadvent.org/cathen/12456a.htm, erişim 20.02.2025.

GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 415-447
DOI: 10.17752/guvenlikstrtj.1695757

Araştırma Makalesi
Research Article

Çağrı Cihazı Saldırıları Sonrası Siber Tehdit İstihbaratı için Yeni Bir Perspektif ve Model Önerisi

A New Perspective and Model Proposal for Cyber Threat Intelligence after Pager Attacks

Tuncay DOĞANTUNA*

Onur CERAN**

* Doktora Öğrencisi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Ana Bilim Dalı (Disiplinlerarası), Ankara, Türkiye, e-posta: tidituna@gmail.com
ORCID: 0000-0003-4135-7690

** Dr. Öğr. Üyesi, Gazi Üniversitesi, Uygulamalı Bilimler Fakültesi, Yönetim Bilişim Sistemleri Bölümü, Ankara, Türkiye, e-posta: onur.ceran@gazi.edu.tr
ORCID: 0000-0003-2147-0506

Geliş Tarihi / Submitted: 09.05.2025

Kabul Tarihi / Accepted: 13.11.2025

Öz

Bu çalışma, hibrit savaş çerçevesinde Siber Tehdit İstihbaratı (CTI) için genişletilmiş bir model önermek amacıyla, Eylül 2024'te Hizbullah'a yapılan çağrı cihazı saldırılarını bir vaka çalışması olarak incelemektedir. Son derece koordineli bir İsrail operasyonuna atfedilen saldırı, yalnızca siber unsurları değil, aynı zamanda Elektronik Harp (EH), Sinyal İstihbaratı (SIGINT) ve manipüle edilmiş tedarik zincirlerini de içermektedir. Binlerce çağrı cihazı ve telsizin senkronize bir şekilde patlatılmasıyla göze çarpan olay, kinetik ve siber yeteneklerin entegrasyonuna örnek teşkil ederek geleneksel tehdit istihbaratı modellerine meydan okumaktadır. Araştırma, MITRE ATT&CK (Rakip Taktikler, Teknikler ve Genel Bilgi) çerçevesinin mevcut sınırlamalarını, özellikle Radyo Frekansı (RF) tabanlı ve analog hedefli saldırıları yeterli şekilde yakalayamamasını eleştirmektedir. Buna karşılık, EH ve SIGINT kaynaklı tehditleri daha iyi temsil etmeyi amaçlayan iki yeni teknik önermektedir: "Spektrum Tabanlı Sinyal Enjeksiyonu" ve "RF Mesaj Enjeksiyonu ve Manipülasyonu". İyileştirme stratejileri, RF anomali tespiti, güvenli haberleşme protokolleri ve entegre SIGINT olay müdahalesini içerir. Çalışma, modern çatışmalarda düşük teknolojili cihazların güvenlik açıklarının ve tedarik zinciri zafiyetlerinin stratejik kullanımını vurgulayarak fiziksel ve dijital savaş arasındaki bulanık sınırları inceler. RF değişkenli vektörleri CTI çerçevelerine entegre eden önerilen model, hibrit tehditleri tespit ve önlemek için daha kapsamlı bir yaklaşım sunabilir, dijital çağda tehdit istihbaratını ve savunma politikasını yeniden şekillendirir.

Anahtar Kelimeler: Elektronik Harp, RF, Siber Tehdit İstihbaratı, Sinyal İstihbaratı, Tedarik Zinciri

Abstract

This study explores the September 2024 pager attacks on Hezbollah as a case study to propose an expanded model for Cyber Threat Intelligence (CTI) within the framework of hybrid warfare. Attributed to a highly coordinated Israeli operation, the attack involved not only cyber elements but also Electronic Warfare (EW), Signals Intelligence (SIGINT), and manipulated supply chains. The incident marked by the synchronized detonation of thousands of pagers and radios exemplifies the integration of kinetic and cyber capabilities, challenging conventional threat intelligence models. The research critiques the current limitations of the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, especially its inability to adequately capture Radio Frequency (RF)-based and analog-targeted attacks. In response, it proposes two new techniques: "Spectrum-Based Signal Injection" and "RF Message Injection & Manipulation", aiming to better represent EW and SIGINT-driven threats. Mitigation strategies include RF anomaly detection, secure communication protocols, and integrated SIGINT incident response. The study investigates the strategic use of low-tech device vulnerabilities and supply chain compromises in modern conflicts, highlighting the blurred boundaries between physical and digital warfare. Integrating RF variable vectors into CTI frameworks, the proposed model may offer a more comprehensive approach to detect and prevent hybrid threats, reshaping threat intelligence and defense policy in the digital age.

Keywords: Cyber Threat Intelligence, Electronic Warfare, RF, Signal Intelligence, Supply Chain

Extended Summary

This study examines the sophisticated pager attacks as a case study to propose a new perspective and model for cyber threat intelligence within the context of hybrid warfare. It analyzes how Electronic Warfare (EW), including Signals Intelligence (SIGINT) and Radio Frequency (RF) capabilities, can be integrated with cyber threats. The research investigates the exploitation of supply chain security and the complexity of these attacks, proposing a model based on the MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework to better detect RF and EW-based attack traces. The aim is to bridge digital and physical security, expanding threat intelligence and enabling more proactive defense strategies. The proposed methodology, using an expanded MITRE ATT&CK matrix, seeks to enhance attack analysis and prevention for hybrid threats. This approach aims to reshape threat intelligence and security policies in cyber and electronic warfare, promoting proactive threat hunting.

The impetus for the study is the simultaneous detonation of thousands of pagers and radios used by Hezbollah in Lebanon and Syria in September 2024, attributed to an Israeli operation. While initially speculated as purely cyber, expert analysis suggests a broader involvement of electronic warfare, signal intelligence, supply chain security, and intelligence operations. The experts also compare the incident to the Stuxnet attack, which demonstrated the vulnerability of critical infrastructure even in the presence of air gaps. A key research question is whether Cyber Threat Intelligence (CTI) or MITRE ATT&CK could have detected such an attack beforehand. Investigative reports indicate a sophisticated Mossad operation involving explosives placed in pager batteries and introduced via manipulated supply chains. This highlights the strategic use of intelligence and technology, leveraging Hezbollah's shift to pagers. The pager attack underscores the instrumentalization of intelligence in asymmetrical warfare and the need for interdisciplinary approaches combining EW, SIGINT, and cyber-attack vectors. The study addresses how these elements can be integrated into threat intelligence frameworks and how physical operation preparations related to EW and supply chains can be incorporated into the MITRE ATT&CK framework.

The study defines key terms: Cyber Threat Intelligence (CTI) for predicting and neutralizing digital threats, Cyber Intelligence for strategic and operational information gathering in the digital realm, MITRE ATT&CK as a knowledge base for adversary tactics and techniques, Supply Chain Security for protecting against risks within the supply chain, Signal Intelligence (SIGINT) for intelligence from electronic communications, Electronic Warfare (EW) for military activities using the electromagnetic spectrum, Intelligence for information gathering and analysis for national security, and Covert Operations as clandestine state activities.

The literature review examines the pager attack as a case study, emphasizing the need to understand adversary TTPs (Tactics, Techniques & Procedures) and adapt security practices beyond standard frameworks. It highlights the supply chain as a key vulnerability and the need for better security in connected and even low-tech devices. It also discusses the importance of threat-informed defense, social engineering, insider threats, and integrating creativity with threat intelligence. The attack is considered a paradigm shift in cyber-physical warfare, blurring the lines between cyber and kinetic domains and demonstrating the weaponization of everyday objects.

The study analyzes the existing MITRE ATT&CK framework, noting that although it includes supply chain compromise techniques, these are primarily oriented towards

traditional IT platforms. The ICS matrix offers a more relevant, though less detailed, technique. The study argues that the current framework is insufficient to fully capture the nuances of attacks featuring significant RF and EW components targeted at analog or hybrid systems. To address this gap, the study proposes new techniques within the MITRE ATT&CK framework. The first, "T1569.xx – Spectrum-Based Signal Injection" under the "Execution" tactic, describes injecting fake messages into pager networks. Mitigation techniques include encryption, digital signatures, RF anomaly detection, and multi-factor authentication. The second proposed technique, "T1602.xx – RF Message Injection & Manipulation" under the "Impact" tactic, focuses on targeting RF-based analog or hybrid communication systems using EW and SIGINT capabilities to inject or manipulate messages or disrupt communication. Mitigation strategies involve secure communication protocols, RF signal filtering, FHSS/LFM (Frequency Hopping Spread Spectrum / Linear Frequency Modulation) usage, multi-layered authentication, and integrated SIGINT/incident response teams.

The discussion emphasizes how the pager operation demonstrates the strategic integration of EW, SIGINT, and supply chain attacks. It highlights the multi-layered planning and the blurring boundaries between digital and traditional military operations. It also underscores the vulnerability of low-tech devices and the weaponization of supply chains. The study concludes that the MITRE ATT&CK framework needs to evolve to include techniques for manipulating and tampering with both digital and analog devices. The synchronized pager explosions likely involved complex engineering with RF signals and firmware manipulation due to the devices' lack of modern security features. The security analysis recognizes that hybrid threats blur the lines between EW and cyber, highlighting the necessity of integrating RF and EW-based threats into threat intelligence. However, directly mapping these to existing MITRE ATT&CK tactics might be challenging. The proposed models aim to integrate these aspects without disrupting the framework's functionality. A limitation acknowledged is the potential ineffectiveness against sophisticated state-sponsored intelligence operations.

In conclusion, this study provides a strategic perspective on hybrid warfare in cybersecurity, analyzing the integration of electronic warfare and cyber threats. It proposes a model based on MITRE ATT&CK to better detect supply chain attacks involving RF and EW techniques. The suggested model promotes new methodologies for predicting and preventing future hybrid threats. Integrating RF and EW-based attack categories offers a more comprehensive threat analysis, bridging digital and physical security. This approach can reshape security policies and enhance proactive threat hunting. The Pager attack serves as a clear example of the blurred lines between cyber and kinetic operations in a hybrid threat environment.

Giriş

17 ve 18 Eylül 2024 tarihlerinde, Hizbullah tarafından kullanımda olan binlerce çağrı cihazı ve yüzlerce telsiz, İsrail'in saldırısı sonucu Lübnan ve Suriye'de eş zamanlı olarak patlatılmış ve akabinde kamuoyunun gündeminde günlerce yer almıştır. Bu saldırıların bazı kaynaklar tarafından siber saldırı teknikleri aracılığıyla gerçekleştirilmiş olduğu iddia edilmiştir.[1] Ancak saldırıların arka planı çeşitli teknik forum ve profesyonel sosyal ağlarda ele alındığında, birçok farklı uzmanın baskın görüşü "sadece siber saldırı teknikleriyle patlamanın

1 Twitter (X), https://x.com/hashtag/pagerexplosions?src=hashtag_click, erişim 19.09.2024.; LinkedIn, https://www.linkedin.com/search/results/all/?keywords=%23pagerexplosion&origin=HASH_TAG_FROM_FEED&sid=Q3u, erişim 20.09.2024.

gerçekleştirildiği*"* argümanı, çok zayıf bir ihtimale indirgenmiştir.[2] Vakanın ilk ortaya çıktığı andan, en son belirgin hale geldiği kritik noktaya kadar geçen süreçte sadece siber güvenlik veya siber istihbarat değil, aynı zamanda "Elektronik Harp", "Sinyal İstihbaratı", "Tedarik Zinciri Güvenliği" ve "İstihbarat Operasyonu" gibi çeşitli benzer disiplinlerin vaka özelinde dahli olduğu değerlendirilmektedir. Dolayısıyla bu saldırılar, devletlerin ve devlet dışı aktörlerin konvansiyonel ve gayrinizami yöntemleri nasıl entegre edebileceğini, teknolojiyi nasıl bir güç çarpanı olarak kullandığını ve bu tür eylemlerin bölgesel güvenlik dinamikleri ile uluslararası normlar üzerindeki potansiyel etkilerini gözler önüne sermektedir.

Lübnan'da Hizbullah'a karşı gerçekleştirilen çağrı cihazları saldırısı gibi spesifik ve planlı bir saldırı operasyonu, 2010 yılında İran'ın nükleer programını sekteye uğratmak amacıyla İsrail tarafından StuxNet zararlı yazılımı aracılığıyla gerçekleştirilen başka bir operasyonu hatırlatmaktadır.[3] O dönemki StuxNet zararlı yazılımıyla gerçekleşen siber saldırı, siber uzaydaki güvenliğin dönüşümü için bir dönüm noktası sayılmaktaydı.[4] Çünkü Stuxnet, kritik altyapıyı yöneten bilgisayar sistemlerine yönelik saldırıların en gelişmiş ve önemli ilk örneklerinden birisi konumundadır. SCADA (Supervisory Control and Data Acquisition – Denetleyici Kontrol ve Veri Toplama) sistemlerinin doğrudan internete bağlı olmamaları, yani bir hava boşluğu (*air gap*) ile izole edilmeleri, uzun süre siber saldırılara karşı koruma sağladığı düşünülen bir önlem olarak kabul edilmiştir. Ancak Stuxnet, bu inanışı kökten sarsarak, fiziksel altyapının internet bağlantısından ayrılmasının tek başına yeterli bir güvenlik tedbiri olmadığını ortaya koymuştur. Özellikle kritik altyapıların siber güvenliği, Stuxnet saldırısının ardından, nükleer emniyetin sürekliliğini sağlamak açısından kritik bir önem arz eder hale gelmiştir.[5]

Lübnan'daki çağrı cihazları saldırısının hangi aşamasında siber saldırı tekniklerinin yer aldığı veya yer almış olup olmadığı bu çalışmanın devam ettiği tarih itibarıyla kesin bir netlik kazanmamış durumdadır. Bu açıdan saldırının herhangi bir aşamasında siber saldırı tekniklerinin yer aldığını varsaydığımızda, ilgili teknik ya da taktiklere veyahut saldırı hazırlığına ilişkin emarelere siber uzayda rast gelip gelmeyeceği, bu çalışmanın araştırma sorusunu temellendirmektedir. Siber uzayda saldırıları tasnifleyerek hangi saldırının hangi APT (*Advanced Persistent Threat* – Gelişmiş Kalıcı Tehdit) grubuyla ilişkili olduğunu etiketleyen MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge* – Rakip Taktikler, Teknikler ve Genel Bilgi) Çerçevesi, siber güvenlik profesyonelleri tarafından çokça başvurulan bir başucu kaynağına dönüşmüştür. Özellikle de Rus, Çin, İran ve Kuzey Kore devlet destekli APT grupları, bu çerçeve ve Siber Tehdit İstihbaratı (CTI) kapsamında tasnif edilmekte ve incelenmektedir.[6] Benzer durumu İsrail'in Mossad veya Unit 8200 örgütleri tarafından gerçekleştirildiği iddia edilen çağrı cihazı saldırılarına uyarlarsak, CTI teknikleri veya MITRE ATT&CK Çerçevesi ile bu saldırıları, öncesinde tespit etmenin mümkün olup olmayacağı hususunun altını çizmek gerekecektir.

Saldırıların ardından yaklaşık bir ay geçtikten sonra, dikkat çekici bir araştırma gazeteciliği yayını Reuters tarafından 16 Ekim 2024 tarihinde yayınlanmıştır.[7] Araştırma

2 Reddit, https://www.reddit.com/r/geopolitics/comments/1fjnx3y/israel_planted_explosives_in_5000_hezbollah/, erişim 19.09.2024.; Medium, https://medium.com/search?q=%23pagerexplosion, erişim 20.09.2024.

3 Ekonomi ve Dış Politika Araştırmalar Merkezi, "Nükleer Tesislerin Siber Güvenliğine Giriş", *Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM)*, 20 Nisan 2016, https://edam.org.tr/siber-politikalar-ve-dijital-demokrasi/nukleer-tesislerin-siber-guvenligine-giris, erişim 01.02.2025.

4 IEEE Spectrum, "The Real Story of Stuxnet", *IEEE Spectrum*, 2024, https://spectrum.ieee.org/the-real-story-of-stuxnet, erişim 01.02.2025.

5 Ekonomi ve Dış Politika Araştırmalar Merkezi, "Nükleer Tesislerin Siber Güvenliğine Giriş", s. 104.

6 MITRE, "MITRE ATT&CK Groups", https://attack.mitre.org/groups/, erişim 05.01.2025.

7 Maya Gebeily, James Pearson ve David Gauthier-Villars, "How Israel's bulky pager fooled Hezbollah", *Reuters Graphics*, 16 Ekim 2024, https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/, erişim 17.10.2024.

haberi, saldırıya ilişkin olarak birçok uzmanın argümanını destekler nitelikte bulgular ortaya koymaktadır. Haberde Lübnan'ın güneyindeki Beyrut ve diğer Hizbullah kalelerinde, binlerce çağrı cihazının eşzamanlı olarak patlaması, İsrail istihbarat servisi Mossad'ın Hizbullah'a yönelik sofistike bir operasyonunun sonucu olduğu belirtilmiştir. Ayrıca çağrı cihazlarının pillerine, X-ray cihazları tarafından tespit edilemeyen plastik patlayıcılar ve yenilikçi ateşleyicilerin yerleştirildiği ve bu cihazların sahte çevrimiçi mağazalar ve uydurma geçmişlerle desteklenerek Hizbullah'ın güvenlik kontrolleri atlatıldığı ifade edilmiştir. Bu olayın İsrail'in Hizbullah'a karşı istihbarat ve teknoloji kullanarak gerçekleştirdiği karmaşık operasyonların bir örneği olduğuna dikkat çekilmektedir. Hizbullah'ın cep telefonu iletişiminin İsrail tarafından dinlenildiğini fark ederek çağrı cihazlarına geçmesi, bu operasyonun planlama aşaması için etkili olduğu değerlendirilmektedir.[8]

Lübnan'da Hizbullah üyelerine yönelik gerçekleştirilen çağrı cihazları ve telsizlerin patlatılmasıyla sonuçlanan saldırılar özelinde basına yansıyan diğer bir kritik haber ise CBS televizyonuna konuşan iki eski Mossad ajanının açıklamaları üzerinden ortaya çıkmıştır.[9] Bu saldırıların operasyonel boyutunu ve planlama süreçlerini gözler önüne seren haberde, ajanların ifadelerine göre, saldırılar on yıllık bir stratejik planlama sürecinin ürünü olduğu ve cihazlara yerleştirilen patlayıcıların İsrail'de üretildiği belirtilmiştir.[10] İlgili operasyonda, Mossad'ın sahte şirketler aracılığıyla Hizbullah üyelerine cihaz tedarik ettiği ve bu cihazlara yalnızca kullanıcıya zarar verecek miktarda patlayıcı yerleştirdiği bildirilmiştir.[11] Özellikle göğse yakın taşınan telsizler ve çağrı cihazları seçilerek, patlamaların etkinliğinin arttırıldığı, operasyonun Tayvan merkezli Gold Apollo gibi gerçek şirketler kullanılarak maskelendiği ve reklam stratejileri ile hedef grupların bu cihazları tercih etmesinin sağlandığı aktarılmıştır. Ajanların açıklamaları, söz konusu operasyonun, İsrail istihbaratının karmaşık paravan ağlar oluşturmadaki yetkinliğini sergilediğini ortaya koymaktadır.[12]

Saldırılar, asimetrik savaş bağlamında istihbaratın araçsallaştırılmasını ve bunun uluslararası hukuktaki sonuçlarını ele alan literatür için önemli bir vaka çalışma ortamı sunmaktadır. Asimetrik bir savaşta hibrit saldırı teknik ve taktiklerinin uygulanabilmesi için "Elektronik Harp", "Sinyal İstihbaratı" ve "Siber Atak Vektörleri" gibi unsurların ve kabiliyetlerin nasıl uyumlu bir biçimde kullanıldığı araştırmacılar için ilgi ve merak uyandırıcı olmaya devam etmektedir. Bu açıdan, klasik elektronik harp ve sinyal istihbaratı taktiklerinin, modern siber saldırı teknikleriyle bir arada kullanılması, stratejik kazanımlar açısından karar vericilerin dikkatini bu alana çekmektedir. Ancak ortaya çıkan bilgilere ve kanıtlara göre, bu vakayı sadece tek başına elektronik, sinyal veya siber tekniklerle ilişkilendirmek hatalı bir yaklaşım olacaktır. Bu noktada süreci daha iyi anlamak adına bu çalışmada, aşağıda geçen araştırma sorularına cevap aranmaktadır:

1. Tehdit İstihbaratının hibrit savaşlarda kullanımı açısından Elektronik Harp (EH), Sinyal İstihbaratı (SIGINT) ve fiziksel müdahaleler, bir bütün olarak siber tehditlerle birlikte nasıl değerlendirilebilir?

8 Age.
9 Lesley Stahl, "Israel's spy agency, Mossad, spent years orchestrating Hezbollah walkie-talkie, pager plots", *CBS News*, 22 Aralık 2024, https://www.cbsnews.com/news/israeli-mossad-pager-walkie-talkie-hezbollah-plot-60-minutes/, erişim 06.01.2025.
10 Age.
11 Lesley Stahl, "Former Mossad Agents Detail Explosive Pagers, Hezbollah Terrorists Plot - 60 Minutes Transcript", *CBS News*, 8 Haziran 2025, https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript/, erişim 09.06.2025.
12 İkbal Muhammet Arslan, "BM: Lübnan ve Suriye'de Eş Zamanlı Çağrı Cihazı Patlamaları Şok Edici", *Anadolu Ajansı (AA)*, 18 Eylül 2024, https://www.aa.com.tr/tr/dunya/bm-lubnan-ve-suriyede-es-zamanli-cagri-cihazi-patlamalari-sok-edici/3333807, erişim 07.01.2025.

2. MITRE ATT&CK çerçevesi, elektromanyetik spektrum ve tedarik zinciri güvenliği boyutları eklenerek nasıl genişletilebilir?
3. Bu genişletme ulusal güvenlik politikaları için ne tür stratejik/politik çıkarımlar üretir?

Bu çalışmanın katkısı iki düzeydedir. Birinci olarak "Çağrı Cihazı" saldırılarındaki vakadan yola çıkarak siber güvenlikte hibrit savaş konseptine yönelik stratejik bir bakış açısı sunmayı ve elektronik harp (SIGINT ve RF dahil) ile siber tehditlerin birlikte değerlendirilmesinin sağlanmasını hedeflemektedir. Bu kapsamda, MITRE ATT&CK çerçevesine tedarik zincirinin güvenliğine yönelik istismarı incelenerek, benzer saldırıların izlerinin tespit edilmesine yönelik bir modeli ortaya koyulacaktır. Bu bağlamda çalışma, MITRE ATT&CK çerçevesi içerisinde mevcutta yer alan tedarik zinciri güvenliğinin yanında ilave teknik tedbirlere dair bir model sunmayı hedeflemektedir. Tehdit istihbaratının geleneksel sınırlarını genişleterek, Elektronik Harp (SIGINT ve RF) tekniklerini de kapsayacak bir perspektif ortaya koyacaktır. İkinci olarak bu teknikleri ulusal güç, kurumsal dayanıklılık ve psikolojik etki katmanlarında politik/stratejik önerilerle ilişkilendirerek hibrit tehditlere disiplinler arası bir yanıt sunmaktadır.

1. Kavramsal Çerçeve

Bu bölümde konunun anlaşılması için gerekli kavramsal çerçeve sunulacaktır.

1.1. Hibrit Savaş

Hibrit savaş, savaşın ve savaş yöntemlerinin farklı seviyelerde, farklı alanlarda ve etki sahalarında, özellikle bilişsel ve moral etki sahalarında, çeşitli aktörlerin bir araya gelerek belirli bir zaman ve mekân düzenlemesiyle, savaşın tüm seviyelerinde hedeflere ulaşmayı amaçlayan, çeşitli yöntem ve teorilerin birleşimidir.[13] Bir devletin veya devlet dışı aktörün, stratejik hedeflerine ulaşmak amacıyla askerî ve gayriaskerî araçları (örneğin, konvansiyonel askerî operasyonlar, düzensiz harp taktikleri, siber saldırılar, dezenformasyon kampanyaları, ekonomik baskı, diplomatik manevralar ve örtülü operasyonlar) eş zamanlı ve senkronize bir şekilde kullandığı karmaşık çatışma türüdür.[14] Hibrit savaşın temel özelliği, belirsizliği arttırarak, sorumluluğu gizleyerek ve hasmın karar alma süreçlerini felç ederek avantaj sağlamaktır. Lübnan'daki çağrı cihazı saldırıları gibi olaylar, konvansiyonel olmayan yöntemlerin, istihbarat operasyonlarının ve teknolojik zafiyetlerin hibrit savaş konsepti içinde nasıl etkin bir şekilde kullanılabileceğine dair önemli bir örnek teşkil etmektedir.

1.2. Siber Güvenlik

Siber güvenlik, ulusal güvenliğin sağlanmasında kritik bir kuvvet çarpanı olarak kabul edilmektedir. Siber güvenlik sadece teknik bir disiplin olmanın ötesinde, bir ülkenin kritik altyapılarının (enerji, iletişim, finans ve sağlık gibi) korunması, devlet kurumlarının işleyişinin devamlılığı, ekonomik istikrarın sürdürülmesi ve toplumsal düzenin muhafazası için hayati öneme sahiptir. Siber uzaydaki tehditlerin artması ve çeşitlenmesi, devletleri siber savunma kapasitelerini geliştirmeye, ulusal siber güvenlik stratejileri oluşturmaya ve siber olaylara müdahale yeteneklerini arttırmaya yöneltmektedir.[15] Güçlü bir siber güvenlik

13 Daniel T. Lasica, *Strategic Implications of Hybrid War: A Theory of Victory*, School of Advanced Military Studies, United States Army Command and General Staff College, 2009, s. 8-10.

14 Erik Reichborn-Kjennerud ve Patrick Cullen, *What is Hybrid Warfare?*, Norwegian Institute for International Affairs (NUPI), 2022, s. 1-4.

15 Solange Ghernouti-Hélie, "A National Strategy for an Effective Cybersecurity Approach and Culture", *2010 International Conference on Availability, Reliability and Security*, IEEE, Şubat 2010, s. 370-373.

altyapısı, bir ülkenin caydırıcılığını arttırır, operasyonel üstünlük sağlar ve hibrit tehditlere karşı direncini yükseltir.[16] İnsanların psikolojik zafiyetlerinden, güven eğilimlerinden veya dikkatsizliklerinden faydalanarak gizli bilgilere erişmek, belirli eylemleri gerçekleştirmelerini sağlamak veya güvenlik sistemlerini atlatmak amacıyla gerçekleştirilen manipülasyon tekniklerinin bütünü olarak tanımlanabilen sosyal mühendislik saldırıları da hibrit savaşta ön alınması gereken unsurlar arasında yer almaktadır.[17]

1.3. Siber Tehdit İstihbaratı (CTI)

Siber Tehdit İstihbaratı (*Cyber Threat Intelligence*, CTI), dijital tehditlerin öngörülmesi, tanımlanması ve etkisiz hale getirilmesi amacıyla toplanan, analiz edilen ve yorumlanan stratejik, operasyonel ve taktiksel bilgileri kapsayan bir disiplindir.[18] CTI, siber saldırganların motivasyonlarını, tekniklerini, prosedürlerini ve potansiyel hedeflerini anlamaya yönelik verilerden oluşur ve güvenlik ekiplerine risk bazlı savunma stratejileri geliştirme imkânı sunar. Bu kavram, yalnızca mevcut tehditleri izlemekle kalmayıp gelecekteki saldırıları önleme ve güvenlik mimarisini proaktif şekilde iyileştirme amacını taşır. CTI'nin etkili kullanımı, tehdit aktörleri hakkında derinlemesine bilgi sağlamanın yanı sıra güvenlik olaylarının analizinde daha hızlı ve doğru müdahaleler için de kritik önem taşır.[19]

1.4. Siber İstihbarat

Siber İstihbarat (*Cyber Intelligence*), dijital ortamda gerçekleşen tehditler, saldırılar ve güvenlik açıkları hakkında stratejik ve operasyonel düzeyde bilgi toplamayı, analiz etmeyi ve bu bilgileri kullanarak proaktif güvenlik önlemleri geliştirmeyi hedefleyen bir bilgi toplama sürecidir.[20] Geleneksel istihbarat disiplinlerinden türeyen siber istihbarat, teknik ve insan kaynaklı verilerin bir araya getirilmesiyle oluşturulan, aktörlerin motivasyonları, kapasiteleri, taktikleri ve hedefleri hakkında kapsamlı bilgi sağlar. Bu süreçte elde edilen bilgiler, risk yönetimi, siber savunma stratejileri ve karar alma mekanizmalarının güçlendirilmesinde kullanılır.[21]

1.5. MITRE ATT&CK

MITRE ATT&CK (*Adversarial Tactics, Techniques, and Common Knowledge* – Rakip Taktikler, Teknikler ve Genel Bilgi), siber tehdit aktörlerinin saldırılarını nasıl gerçekleştirdiğine dair detaylı bir bilgi tabanı ve çerçeve sunan, tehdit odaklı bir modeldir. Bu çerçeve, siber güvenlik topluluğu için saldırıların tanımlanması, analiz edilmesi ve önlenmesine yönelik standartlaştırılmış bir referans sağlar.[22]

MITRE ATT&CK, saldırganların kullandığı taktikler (hedefler), teknikler (hedeflere ulaşmak için kullanılan yöntemler) ve prosedürler (belirli bir tekniği uygulamak için izlenen

16 Artem Bratko, Denys Zaharchuk ve Valentyn Zolka, "Hybrid Warfare-A Threat to the National Security of the State", *Revista de Estudios en Seguridad Internacional*, 7:1, 2021, s. 147-160.

17 Sanda Svetoka, *Social Media as a Tool of Hybrid Warfare*, NATO Strategic Communications Centre of Excellence, 2016, s. 9-11.

18 Ignacio M. G. Urbini, Paula Venosa, Patricia Bazán ve Nicolás Del Río, "Distributed Cybersecurity Strategy, Applying the Intelligence Operations Theory", *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, Haziran 2022, s. 1-6.

19 Nan Sun, Ming Ding, Jiaojiao Jiang, Weikang Xu, Xiaoxing Mo, Yonghang Tai ve Jun Zhang, "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives", *IEEE Communications Surveys & Tutorials*, 25:3, 2023, s. 1748-1774.

20 Randy Borum, John Felker, Sean Kern, Kristen Dennesen ve Tonya Feyes, "Strategic Cyber Intelligence", *Information & Computer Security*, 23:3, 2015, s. 317-332.

21 Ross W. Bellaby, "Justifying Cyber-Intelligence?", *Journal of Military Ethics,* 15:4, 2016, s. 299-319.

22 Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington ve Cody B. Thomas, "MITRE ATT&CK: Design and Philosophy", *Technical Report*, McLean, VA: The MITRE Corporation, 2018, s. 1-6.

süreçler) gibi unsurları ayrıntılı biçimde sınıflandırır. Savunma stratejilerinin geliştirilmesinde önemli bir kaynak olan bu model, siber tehdit istihbaratında tehditlerin analiz edilmesi, güvenlik açıklarının tespit edilmesi ve olay müdahale süreçlerinin geliştirilmesi için rehberlik eder.[23] Özellikle tehdit avcılığı, güvenlik kontrollerinin değerlendirilmesi ve tehdit modelleme süreçlerinde yaygın olarak kullanılmaktadır. Mitre çerçevesinde yer alan TTP (*Tactics, Techniques & Procedures*); teknik, taktik ve prosedür kelimelerinin kısaltmasıdır.[24] APT (*Advanced Persistent Threat*) ise, gelişmiş kalıcı tehditler anlamına gelen İngilizce ifadenin kısaltılmış halidir.[25] Ayrıca APT kavramı, ilgili tehditleri kendilerine has saldırı yöntemleri ve motivasyonlarıyla bir araya gelen saldırgan grupları tanımlamak için de kullanılır. Genellikle APT grupları olarak isimlendirilir. Hem TTP hem APT kavramları bölüm 4.1 içerisinde pratik örneklerle ele alınacaktır.

1.6. Tedarik Zinciri Güvenliği

Tedarik zinciri güvenliği, bir organizasyonun tedarik zincirinde yer alan tüm bileşenlerin, süreçlerin ve üçüncü tarafların siber saldırı ve bilgi güvenliği risklerine karşı korunmasını sağlama sürecidir.[26] Bu kavram, donanım, yazılım ve hizmetlerin geliştirilmesinden teslimatına kadar olan tüm aşamalarda güvenlik açıklarını ve potansiyel tehditleri ele alır. Tedarik zinciri güvenliği, özellikle dış kaynak kullanımı ve üçüncü taraflarla yapılan iş birlikleri nedeniyle karmaşık bir yapıya sahiptir. Saldırganlar, doğrudan hedefe yönelik saldırılar yerine zayıf halkalar üzerinden sisteme erişim sağlamayı tercih edebilir. Bu bağlamda, tedarik zinciri güvenliği; güvenilir tedarikçi seçimi, bileşenlerin doğrulanması, şeffaflık sağlanması ve güvenlik kontrollerinin düzenli olarak uygulanması gibi proaktif önlemleri içerir. Kritik altyapıların ve hassas verilerin korunması açısından, tedarik zinciri güvenliği modern siber güvenlik stratejilerinin temel unsurlarından biridir.[27]

1.7. Sinyal İstihbaratı (SIGINT)

Sinyal İstihbaratı (*Signals Intelligence*, SIGINT), elektronik haberleşme sistemlerinden elde edilen verilerin toplanması, analiz edilmesi ve yorumlanması yoluyla elde edilen istihbarat türüdür.[28] SIGINT, genellikle askerî ve ulusal güvenlik bağlamında kullanılmakla birlikte, modern siber güvenlik stratejilerinde de önemli bir rol oynar. Bu istihbarat türü, iletişim istihbaratı (COMINT) ve elektronik istihbarat (ELINT) gibi alt kategorilere ayrılır; birincisi haberleşme trafiğini, ikincisi ise radar ve diğer elektronik sinyalleri hedef alır.[29]

---

23 Nitin Naik, Paul Jenkins, Paul Grace ve Jingping Song, "Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model", *2022 IEEE International Symposium on Systems Engineering (ISSE)*, IEEE, Ekim 2022, s. 1-7.

24 Bir tehdit aktörünün davranışını temsil eder. Taktik, davranışın en üst düzey açıklamasıdır; teknikler, taktik bağlamda davranışın daha ayrıntılı bir açıklamasını sunar; prosedürler ise teknik bağlamda davranışın daha düşük düzeyli, oldukça ayrıntılı bir açıklamasını sunar. Bknz.: National Institute of Standards and Technology, "Tactics, Techniques, and Procedures", *National Institute of Standards and Technology (NIST)*, https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures, erişim 22.04.2025.

25 APT (*Advanced Persistent Threat*): Gelişmiş kalıcı tehdit, hedef ağ veya sistem içerisinde fark edilmeden ve kalıcı bir varlık sürdürmek için gizli saldırı tekniklerini kullanan, böylece uzun süre boyunca tespit edilmeden hedeflerine ulaşmalarını sağlayan gelişmiş bir saldırgandır. Bknz.: PICUS Security, "What is Advanced Persistent Threat (APT)?", *Picus Security*, 2025, https://www.picussecurity.com/resource/glossary/what-is-advanced-persistent-threat-apt, erişim 05.05. 2025.

26 Heinrihs K. Skrodelis ve Andrejs Romanovs, "Cyber-Physical Risk Security Framework Development in Digital Supply Chains", *2021 62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, IEEE, Ekim 2021, s. 1-5.

27 Badis Hammi, Sherali Zeadally ve Jamel Nebhen, "Security Threats, Countermeasures, and Challenges of Digital Supply Chains", *ACM Computing Surveys*, 55:14s, 2023, s. 1-40.

28 David L. Christianson, "Signals Intelligence", Gerald W. Hopple ve Bruce W. Watson (ed.), *The Military Intelligence Community*, New York, Routledge, 2019, s. 39-54.

29 D. Curtis Schleher, *Electronic Warfare in the Information Age*, Norwood MA, Artech House Inc., 1999, s. 27-35.

1.8. Elektronik Harp (EH)

Elektronik Harp (EH), elektromanyetik spektrumu kullanarak düşman iletişim, algılama ve yönlendirme sistemlerini engellemek, yanıltmak veya bozmak ve aynı zamanda kendi sistemlerinin bu tür tehditlerden korunmasını sağlamak amacıyla yürütülen askerî faaliyetlerdir.[30] Elektronik Harp, elektronik taarruz (*Electronic Attack*, EA), elektronik destek (*Electronic Support*, ES) ve elektronik koruma (*Electronic Protection*, EP) olmak üzere üç temel bileşene ayrılır. Elektronik taarruz, düşman sinyallerini hedef alan saldırı faaliyetlerini içerirken, elektronik destek, tehditlerin tespit edilmesi ve izlenmesi için sinyal toplama ve analiz süreçlerini kapsar. Elektronik koruma ise dost sistemlerin elektromanyetik spektrum tehditlerine karşı savunulmasını sağlar. Modern savaş ortamında giderek daha stratejik bir rol üstlenen elektronik harp, özellikle siber güvenlik ve sinyal istihbaratı ile iç içe geçmiş bir yapıdadır ve askerî operasyonların başarısı için kritik bir avantaj sunar.[31]

1.9. İstihbarat ve Örtülü Operasyonlar

İstihbarat, devletlerin ulusal güvenlik, dış politika ve stratejik çıkarlarını koruma amacıyla bilgi toplama, analiz etme ve yayma süreçlerini kapsayan disiplinler arası bir faaliyettir.[32] İstihbarat, karar alıcıların bilinçli ve etkili politikalar geliştirmesine yardımcı olacak bilgileri sağlamak için kullanılır. Bu süreç; insan kaynaklı istihbarat (HUMINT), sinyal istihbaratı (SIGINT), görüntü istihbaratı (IMINT) ve ölçüm ile imza istihbaratı (MASINT) gibi farklı disiplinlerden gelen verilerin toplanmasını ve bu verilerin anlamlı bir şekilde işlenmesini içerir.[33] Etkin bir istihbarat süreci, yalnızca tehditlerin tespit edilmesini değil, aynı zamanda fırsatların belirlenmesini ve risk yönetiminin güçlendirilmesini mümkün kılar.[34] İstihbarat faaliyetleri, devletlerin güvenlik stratejilerinin temel unsurlarından biri olup askerî, ekonomik ve siyasi alanlarda avantaj sağlamak amacıyla kullanılır.

Örtülü operasyonlar ise bir devletin resmi olarak üstlenmediği veya kamuya açıklamadığı faaliyetlerdir. Genellikle gizlilik gerektiren stratejik hedeflere ulaşmak için uygulanır.[35] Bu tür operasyonlar, rejim değişikliği sağlamak, rakip devletlerin etkisini zayıflatmak veya terörist faaliyetleri engellemek gibi amaçlarla gerçekleştirilebilir.[36] Örtülü operasyonların en belirgin özelliklerinden biri, operasyonun sponsoru olan devletin kimliğinin gizlenmesidir.[37] Örtülü operasyonların başarısı, planlama, gizlilik ve bilgi güvenliği unsurlarının etkili bir şekilde yönetilmesine bağlıdır.[38]

2. Literatür

Çağrı cihazları patlatılması olaylarının hemen akabinde, olayın sıcaklığıyla ilgili çeşitli teknik yorumlar, sosyal mecralarda günlerce yayılmıştı. Ancak çalışmanın araştırma probleminde vurgulanan konuya değinen sınırlı sayıda kaynak, bazı internet makalelerinde ele alınmış

30 Age, s. 37.
31 Ali Al-Khawaja ve Sattar B. Sadkhan, "Intelligence and Electronic Warfare: Challenges and Future Trends", *2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, IEEE, Ağustos 2021, s. 118-123.
32 Len Scott, "Secret Intelligence, Covert Action and Clandestine Diplomacy", Christopher Andrew, Richard J. Aldrich ve Wesley K. Wark (ed.), *Secret Intelligence*, London, Routledge, 2019, s. 526-544.
33 Age, s. 527.
34 Age, s. 528.
35 Michael Warner, "A Matter of Trust: Covert Action Reconsidered", *Studies in Intelligence*, 63:4, 2019, s. 33-39.
36 Age, s. 57.
37 Peter Gill, "Intelligence, Threat, Risk and the Challenge of Oversight", *Intelligence and National Security*, 27:2, 2012, s. 206-222.
38 Age, s. 209.

görünmektedir. Literatür incelemesinde özellikle şu analizin dikkat çekici olduğunu değerlendirmekteyiz.[39]

> *"Çağrı cihazlarıyla yapılan bu saldırı, siber güvenlik için doğrudan bir paralellik sunuyor: tıpkı askerî alanda olduğu gibi, düşman hakkında derin bilgi sahibi olmak çok önemlidir. Siber güvenlikte, kötü niyetli grupların Taktiklerini, Tekniklerini ve Prosedürlerini (TTP) sürekli olarak gözlemlememiz ve bunları güvenlik uygulamalarımıza dahil etmemiz gerekir. Bu, yalnızca NIST, CIS Kontrolleri ve ISO 27001 gibi yerleşik çerçeveleri benimsemek anlamına gelmez, aynı zamanda bunları karşı karşıya olduğumuz gerçek tehditlere göre ayarlamak anlamına da gelir".*

Araştırmamız kapsamında ele alınan diğer bir makale, Hizbullah'a yönelik 2024 yılında gerçekleşen ve grubun üyelerince kullanılan çağrı cihazlarının aynı anda infilak ettiği saldırıyı incelemektedir.[40] Olay, yüzlerce cihazın içerisine patlayıcı yerleştirilip uzaktan tetiklenmesi ile gerçekleşmiştir. İsrail'in operasyonun ardındaki güç olduğu öne sürülmüş, patlamalar ciddi can kaybına ve yaralanmalara yol açmıştır. Patlamalarda kullanılan cihazların Tayvan merkezli Gold Apollo tarafından üretilmiş olması, dikkatleri tedarik zinciri güvenliğine yöneltmiştir. Tedarik zincirine sızılarak, söz konusu çağrı cihazlarının hedef gruplara toplu olarak ulaştırıldığı anlaşılmaktadır. Uzmanlar, patlamaların pillerden kaynaklanmadığını, ancak uzaktan tetikleme kabiliyetlerinin kamuya açık dijital ağlar üzerinden gerçekleştirilebileceğini belirtmiştir.[41] Saldırı, bağlı cihazların güvenliği ve üreticilerin bu tür tehditlere karşı sağlam testler yapmasının gerekliliği konusunda ciddi bir uyarı olarak ele alınmaktadır.

Diğer bir çalışmada ise İsrail'in Hizbullah'a yönelik çağrı cihazlarını kullanarak düzenlediği saldırının, siber güvenlik stratejileri için sunduğu dersleri analiz etmektedir.[42] Yazar, istihbarat operasyonlarının sürpriz, yenilik ve düşman bilgisine dayandığını vurgularken, çağrı cihazları ve daha önce Yahya Ayyaş'a yönelik suikast gibi olaylardan örnekler vermektedir. Siber güvenlik bağlamında, saldırı taktiklerini anlamanın ve tehdit bilincine dayalı savunma mekanizmaları geliştirmenin önemine dikkat çekilmektedir. Makalede ayrıca, sosyal mühendislik saldırılarına ve içeriden gelen tehditlere karşı güvenlik programlarının önemi, tedarik zinciri güvenliğine yönelik riskler ve kullanıcı farkındalığını arttırma stratejileri ele alınmaktadır. Savaşta ve siber güvenlikte yaratıcılık ile tehdit istihbaratının entegre bir güvenlik yaklaşımındaki kritik rolü vurgulanmaktadır.[43]

Bu ilk değerlendirmeler, olayın hemen ardından yapılan ve daha çok teknik boyutlara odaklanan yorumları yansıtmaktadır. Ancak bu saldırının sadece bir cihaz güvenliği veya tedarik zinciri zafiyeti meselesi olmadığı, aynı zamanda karmaşık bir istihbarat operasyonunun ve hibrit savaş taktiklerinin bir parçası olduğu göz ardı edilmemelidir. Nitekim, Lima'nın çalışmasında vurgulanan "*düşman hakkında derin bilgi sahibi olma*" gerekliliği[44] ve ilgili yazar tarafından işaret edilen "*tehdit bilincine dayalı savunma mekanizmaları geliştirme*" ihtiyacı,[45] bu tür olayların analizinde siber güvenlik disiplininin istihbarat ve stratejik

39 Marcelo Lima, "Israeli Pager Attack: Cybersecurity Lessons", *LinkedIn*, 29 Eylül 2024, https://www.linkedin.com/pulse/israeli-pager-attack-cybersecurity-lessons-security-marcelo-kcjxf, erişim 21.10.2024.
40 Information Security Buzz Staff Reporter, "Hezbollah Pager Attack: A Wake-up Call to Tech Manufacturers to Secure their Supply Chains?", *Information Security Buzz (ISB)*, 19 Eylül 2024, https://informationsecuritybuzz.com/hezbollah-pager-attack-a-wake-up-call/, erişim 20.10.2024.
41 Age.
42 Lima, "Israeli Pager Attack: Cybersecurity Lessons".
43 Age.
44 Age.
45 Age.

çalışmalar gibi sosyal bilim alanlarıyla ne kadar iç içe geçtiğini göstermektedir. Çağrı cihazlarının hedef alınması, sadece teknik bir zafiyetin istismarı değil, aynı zamanda hedef grubun iletişim alışkanlıkları, operasyonel güvenliği ve psikolojisi üzerine kurulu kapsamlı bir istihbarat çalışmasının ürünü olduğunun göstergesidir.

Singh'in internet makalesi, modern siber-fiziksel savaşın sınırlarını zorlayan ve askerî stratejide yeni bir paradigma sunan Hizbullah'a yönelik stratejik çağrı cihazı saldırısını incelemektedir.[46] Onun analizine göre, Hizbullah'ın elektronik gözetimden kaçınmak amacıyla kullandığı çağrı cihazlarına, tedarik zinciri manipülasyonu yoluyla patlayıcılar yerleştirilmiş ve bu cihazlar uzaktan senkronize şekilde patlatılarak ciddi kayıplar verilmiştir. Saldırının başarısı, PETN (*Pentaeritritol Tetranitrat*) patlayıcısı içeren cihazların fiziksel ve siber güvenlik açıklarını bir araya getiren sofistike bir istihbarat operasyonuna dayanmaktadır. Ayrıca, saldırının iletişim altyapısına zarar vermesi ve Hizbullah'ın operasyonel güvenini sarsması, tedarik zinciri güvenliği ile siber-fiziksel sistemlerin bütüncül olarak yeniden değerlendirilmesinin önemini vurgulamaktadır. Singh, bu olayın, teknolojiyle silahlandırmanın yeni bir dönemini işaret ettiğini ve savaşın geleneksel siber ve kinetik sınırlarının bulanıklaştığını savunarak, modern çatışmaların geleceğinde siber güvenliğin kritik rolüne dikkat çekmektedir.[47]

Singh, saldırıyı "*siber-fiziksel savaşın sınırlarını zorlayan ve askerî stratejide yeni bir paradigma sunan*" bir olay olarak nitelendirirken bu paradigmanın sadece teknolojik bir dönüşümü değil, aynı zamanda savaşın doğasına ilişkin geleneksel anlayışları sorguladığını da belirtmektedir. Tedarik zinciri manipülasyonu yoluyla fiziksel ve siber güvenlik açıklarının bir araya getirilmesi, devletlerin ve devlet dışı aktörlerin yıkıcı kapasitelerini nasıl arttırabileceğini göstermektedir. Bu noktada, saldırının sadece Hizbullah'ın operasyonel güvenini sarsmakla kalmayıp, aynı zamanda genel olarak teknolojiye olan güveni ve kritik altyapıların (iletişim altyapıları dahil) güvenliğine ilişkin endişeleri de arttırdığı söylenebilir.[48] Singh'in vurguladığı gibi "*savaşın geleneksel siber ve kinetik sınırlarının bulanıklaşması*", uluslararası ilişkiler ve güvenlik çalışmaları literatüründe uzun süredir tartışılan hibrit tehditler kavramıyla doğrudan örtüşmektedir. Bu tür bir saldırı, ulusal güvenlik stratejilerinin sadece askerî kapasitelere değil, aynı zamanda siber dayanıklılığa, tedarik zinciri direncine ve toplumsal farkındalığa da odaklanması gerektiğini bir kez daha teyit etmektedir.

Diğer bir analiz çalışmasında Mark Lacy, modern çatışmaların yeni boyutlarını ve teknolojik araçların silahlandırılmasını ele almaktadır.[49] Yazar, iletişim cihazlarının patlayıcı düzeneklere dönüştürülmesini, devlet dışı aktörler tarafından geliştirilen yıkıcı teknolojilerin artan erişilebilirliği bağlamında tartışmaktadır. Bu saldırılar, iletişim güvenliğinin savaşlarda her zamankinden daha kritik hale geldiği bir dönemde yaşanmış ve sıradan nesnelerin dahi savaş aracı olarak kullanılabileceğine işaret etmiştir. Lacy, Mark Galeotti ve Audrey Kurth Cronin gibi güvenlik uzmanlarının görüşlerine atıfta bulunarak, "*her şeyin silahlandırılması*" konseptinin tehditkâr gerçekliğe dönüştüğünü vurgulamaktadır.[50] Makale, gelecekteki çatışmaların daha yaratıcı ve uzaktan gerçekleştirilen saldırılarla şekilleneceği bir dünyada,

46 Inder Singh, "New Paradigm in Cyber Warfare: Strategic Pager Attack on Hezbollah", *Medium*, 18 Eylül 2024, https://inderbarara.medium.com/new-paradigm-in-cyber-warfare-strategic-pager-attack-on-hezbollah-d100247bd9ec, erişim 22.10.2024.

47 Singh, "New Paradigm in Cyber Warfare: Strategic Pager Attack on Hezbollah".

48 Tobias B. Back, "Weaponising 'Apparently Harmless Portable Objects': Emerging Categorisations of Trust and Risk in Post 'Pager Attacks' Lebanon", *Small Wars & Insurgencies*, 36:6, 2025, s. 1025-1048.

49 Mark Lacy, "Lebanon Pager Attacks: The Weaponisation of Everything has Begun", *The Conversation*, 19 Eylül 2024, https://theconversation.com/lebanon-pager-attacks-the-weaponisation-of-everything-has-begun-239423, erişim 23.10.2024.

50 Age.

devletlerin ve güvenlik kurumlarının yeni zorluklara karşı savunmasız kalabileceğini belirtir. Özellikle devlet dışı aktörlerin geleneksel caydırıcılık stratejilerine karşı daha az duyarlı olmaları, bu tehdidi daha karmaşık hale getirmektedir. Lacy, hızla değişen teknolojik ortamda jeopolitik dengelerin de yeniden tanımlanabileceğini öne sürerek belirsizliğin, çağdaş güvenlik anlayışının temel bir özelliği olarak kaldığını savunmaktadır.

Lacy, "*her şeyin silahlandırılması*" konseptinin tehditkâr bir gerçekliğe dönüştüğünü vurgularken, bu durumun uluslararası güvenlik ortamında öngörülebilirliği azalttığını ve devletlerin yanı sıra devlet dışı aktörlerin de asimetrik avantajlar elde etmesine olanak tanıdığını belirtmek önemlidir. İletişim cihazlarının patlayıcı düzeneklere dönüştürülmesi, sadece teknolojik bir yenilik değil, aynı zamanda psikolojik bir etki yaratma ve korku yayma amacı da taşıyabilir. Bu tür saldırılar geleneksel caydırıcılık stratejilerinin etkinliğini sorgulatmakta ve devletleri yeni savunma mekanizmaları geliştirmeye zorlamaktadır. Sivil teknolojiler kullanılarak gerçekleştirilen bu saldırıların savaşçı olmayanları da hedef alabileceğinden yola çıkarak insan hakları yasalarına aykırılık teşkil edeceğinin tartışıldığı bir ortamda[51], özellikle devlet dışı aktörlerin bu tür yıkıcı teknolojilere erişiminin artması, uluslararası normların ve çatışma hukukunun bu yeni gerçekliğe nasıl uyum sağlayacağı sorusunu da beraberinde getirmektedir.

Pytlak, Siebens ve Lad'ın Lübnan'daki çağrı cihazı saldırılarını incelediği çalışması, modern çatışmaların karmaşıklığını ve hibrit savaşın dinamiklerini aydınlatmaya çalışmaktadır.[52] Özellikle eski teknolojilere yapılan saldırıların, siber operasyonların ve kinetik sabotajların kesişim noktalarını nasıl temsil ettiğine odaklanmaktadır. Çağrı cihazlarının hedef alınması, çift kullanımlı teknolojilerin silahlandırılmasının ve tedarik zincirlerine yönelik müdahalelerin güvenlik üzerindeki etkilerini çarpıcı biçimde göstermektedir. Yazarlar, geleneksel siber tehditlerin ötesinde, sorumluluk atfetmenin zorluklarını ve kısa raf ömrüne sahip hibrit silahların operasyonel sınırlamalarını analiz ederek, siber savaşın benzersiz olmadığını ve geçmişten miras alınan güvenlik açmazlarını tekrar ettiğini vurguluyor. Bu olay, hibrit savaşın insan maliyeti ve güvenlik açıkları açısından yalnızca siber alanla sınırlı olmayan daha geniş bir tehdit çerçevesine sahip olduğunu hatırlatmaktadır.[53]

Pytlak ve arkadaşları, çağrı cihazı saldırılarının "*siber operasyonların ve kinetik sabotajların kesişim noktalarını*" temsil ettiğini belirtirken, bu kesişimin sadece teknik bir birleşme olmadığını, aynı zamanda stratejik ve operasyonel bir entegrasyonu da ifade ettiğini vurgulamak gerekir.[54] Yazarların, "*hibrit savaşın insan maliyeti ve güvenlik açıkları açısından yalnızca siber alanla sınırlı olmayan daha geniş bir tehdit çerçevesine sahip olduğu*" tespiti, bu tür olayların analizinde sadece teknolojik zafiyetlere odaklanmanın yetersiz kalacağını göstermektedir.[55] Bu analiz, çalışmamızın önerdiği MITRE ATT&CK çerçevesinin genişletilmesi gerekliliğini, sadece yeni teknikler eklemekle kalmayıp, aynı zamanda bu tür hibrit saldırıların karmaşık doğasını ve sosyopolitik bağlamlarını da içerecek şekilde yapılması gerektiğini desteklemektedir.[56]

51 Andrea Lavazza ve Mirko Farina, "The Costs and Perils of Weaponizing Consumer Technologies (the 2024 Pager and Walkie-Talkie Explosions in Lebanon and Syria)", *IEEE Technology and Society Magazine*, 2024.
52 Alexa Pytlak, Jessica Siebens, ve Sahil Lad, "Old Tactics, New Targets: Unraveling Lebanon's Pager Attacks", *Stimson Center*, 25 Eylül 2024, https://www.stimson.org/2024/old-tactics-new-targets, erişim 24.10.2024.
53 Age.
54 Age.
55 Age.
56 Chuan Sheng, Wanlun Ma, Qing-Long Han, Wei Zhou, Xiaogang Zhu ve Sheng Wen, "Pager Explosion: Cybersecurity Insights and Afterthoughts", *IEEE/CAA Journal of Automatica Sinica*, 11:12, 2024, s. 2359-2362.

Söz konusu çağrı cihazı saldırıları, hibrit savaş ve siber güvenlik literatüründe giderek daha fazla önem kazanan bazı temel temaları da ön plana çıkarmaktadır. Örneğin, Hoffman tarafından kavramsallaştırılan hibrit tehditler, devletlerin ve devlet dışı aktörlerin konvansiyonel ve düzensiz taktikleri, terörizmi ve suç faaliyetlerini senkronize bir şekilde kullanarak belirsizlik yaratma ve geleneksel askerî üstünlüğü aşındırma çabalarını ifade eder.[57] Lübnan'daki olay, Hoffman'ın teorik çerçevesinin pratik bir yansıması olarak okunabilir. Benzer şekilde Nye, siber gücün (*cyber power*) uluslararası politikadaki rolüne ilişkin analizleri, siber saldırıların sadece teknik bir sorun olmanın ötesinde, devletlerin güç projeksiyonu, caydırıcılık ve diplomatik ilişkilerinde nasıl bir araç haline geldiğini ortaya koymaktadır.[58] Çağrı cihazı saldırıları, siber yeteneklerin istihbarat operasyonları ve kinetik etkilerle birleştirilerek stratejik hedeflere ulaşmada nasıl kullanılabileceğine dair çarpıcı bir örnektir. Ayrıca Rid'in, siber savaşın büyük ölçüde casusluk, sabotaj ve yıkıcılık (*subversion*) faaliyetlerinin sofistike birer versiyonu olduğu yönündeki argümanları da bu bağlamda önemlidir.[59] Lübnan vakası, Rid'in işaret ettiği gibi, doğrudan bir "*savaş*" eylemi olmasa da sofistike bir sabotaj ve istihbarat operasyonu olarak değerlendirilebilir ve bu tür eylemlerin uluslararası güvenlik üzerindeki etkileri göz ardı edilemez.

Saldırıların etkisinin günlerce kamuoyunda tartışıldığı süreçte, sosyal medya platformlarında ve geleneksel medya kanallarında görüş bildiren siber güvenlik, elektronik/sinyal/RF ve istihbarat alanlarındaki uzmanlar arasında genel bir görüş birliği oluşmuştur. Bu değerlendirmelere göre, söz konusu saldırılar bir istihbarat operasyonu çerçevesinde planlanmış, tedarik zincirindeki zafiyetleri hedef almış ve hem siber hem de elektronik yöntemlerden yararlanılmıştır. Gerçekte ise bu saldırı, farklı uzmanlık alanlarının kesişiminde yer alan disiplinler arası bir yaklaşımla kurgulanmış olup bu yönüyle alternatif yorumlara açık bir analiz çerçevesi sunmaktadır. Bu açıdan saldırının farklı bir yoruma dönük analizi şu satırlarda ifade edilmektedir:[60]

> *"Hizbullah'ın tedarik zincirlerinin kırılganlığını hafife alırken yaptığı yaygın hata, geleneksel en iyi uygulamaların yeterli olduğuna inanmasıdır. Ancak, düşmanların TTP'leri sürekli olarak gelişiyor ve bu gelişmeye ayak uyduramazsak, geride kalma riskimiz var. Tehdit Bilgili Savunma yaklaşımı, savunmalarımızı gerçek ve ortaya çıkan tehditlere uyarlama ihtiyacını vurgulayarak buna bir yanıt olarak ortaya çıkıyor. MITRE ATT&CK gibi araçlar, kötü niyetli grupların kullandığı taktiklere ilişkin değerli içgörüler sundukları için bu süreçte önemlidir".*

3. Yöntem

Bu çalışmada, nitel araştırma yöntemleri çerçevesinde yapılandırılmış bir vaka çalışması yaklaşımı benimsenmiş ve "Tasarım Bilimsel Araştırma Yöntemi" çerçevesinde yapılandırılmıştır. Vaka çalışması, belirli bir kişi, grup, olay, kurum veya duruma derinlemesine ve detaylı bir şekilde odaklanan bir araştırma yöntemidir. Genellikle, bir olayın veya durumun "neden" ve "nasıl" meydana geldiğini anlamak için kullanılır.[61] Tasarım Bilimsel Araştırma Yöntemi, bir problemi çözmek veya mevcut bir durumu iyileştirmek için yeni bir yapı (model, yöntem, algoritma ve sistem) tasarlamayı ve gerekçelendirmeyi

57 Frank G. Hoffman, *Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington: Potomac Institute for Policy Studies*, 2007.
58 Joseph S. Nye, *Cyber Power*, Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs, 2010.
59 Thomas Rid, "Cyberwar and Peace: Hacking Can Reduce Real-World Violence", *Foreign Affairs*, 92:6, 2013, s. 77-87.
60 Lima, "Israeli Pager Attack: Cybersecurity Lessons".
61 Robert K. Yin, *Case Study Research: Design and Methods*, 5, Thousand Oaks, CA, Sage, 2009.

amaçlayan bir araştırma yaklaşımıdır.[62] Bu kapsamda Eylül 2024'te Hizbullah'a yönelik gerçekleştirilen çağrı cihazı saldırısına ilişkin kamuya açık araştırma raporları, istihbarat analizleri, medya içerikleri ve teknik forumlardaki uzman yorumları sistematik olarak incelenmiş, bu içeriklerden elde edilen veriler, saldırının yapısını ve kullanılan teknikleri ortaya koymak üzere analiz edilmiştir. Mevcut MITRE ATT&CK matrisinin teknik ve taktik boyutları incelenmiş, saldırının tespit ve analizinde yetersiz kalan alanlar tespit edilmiştir. Bu bağlamda, mevcut çerçeveye entegre edilebilecek iki yeni teknik model önerilmiştir. Bu öneriler, RF sinyallerine dayalı saldırıların da tehdit istihbaratı matrisine dahil edilmesini sağlayarak, dijital ve analog tehditleri bir arada ele alan bütüncül bir modelin temellerini oluşturmaktadır.

4. Mevcut Çerçeve ve Önerilen Model

MITRE ATT&CK, bilgileri güncel tutabilmek için topluluktan gelen ve sahada gözlemlenen olayları içeren girdilere büyük ölçüde bağımlıdır.[63] Bireyler ve kuruluşlar, MITRE ATT&CK bilgi tabanını geliştirmek amacıyla sürekli olarak çeşitli tehdit istihbaratı verileri ve bilgileri paylaşmaktadır. Bu paylaşımlar sayesinde siber güvenlik profesyonelleri, elde edilen verileri tehdit profilleri, taktikler ve teknikler gibi bileşenler halinde bilgi tabanına entegre ederek, bilgi birikiminin zenginleşmesine katkı sağlamaktadır.[64] Literatürde de bu zenginleşmeye katkı sağlayan çalışmalar yer almaktadır. Jo ve arkadaşları, gemi siber güvenliği alanında yürütülen 15 önemli çalışmayı MITRE ATT&CK çerçevesini kullanarak incelemiştir.[65] Yapılan bu analizler sonucunda, modern gemilerde dikkate alınması gereken ortak güvenlik tedbirleri tespit edilmiş ve bu bulgulara dayanarak gemi ortamına özgü yeni bir güvenlik önlemleri matrisi sunulmuştur. Kanj Bonhard ve arkadaşları, kurumsal e-posta dolandırıcılığı tehdit aktörlerinin kullandığı TTP'leri MITRE ATT&CK çerçevesi kapsamında haritalandırarak 10 taktik, 34 teknik ve 46 alt-teknik belirlemiş ve özellikle posta kutusu manipülasyonu ile savunma atlatma konularındaki eksiklikleri gidermek amacıyla 5 yeni alt-teknik önermişlerdir.[66] Ahn ve arkadaşları, bir kurumun siber saldırı veya güvenlik ihlali sonrasında hızla toparlanabilme yeteneği olan siber dayanıklılığını arttırmak amacıyla Sıfır Güven (*Zero Trust* - ZT) güvenlik modelini ile MITRE ATT&CK matrisinin birleştirilmesini önermektedir.[67] Pell ve arkadaşları, 5G ağları için MITRE ATT&CK çerçevesini genişletme konusundaki yaklaşımını sundukları çalışmalarında 5G'nin bulut tabanlı mimariye geçişinin geleneksel bulut tehditlerini de beraberinde getirdiğine inanarak tüm taktikleri korumuş, ancak 5G mimarisine özgü tehditleri bir uzantı olarak tanımlayarak standart protokolun kötüye kullanımını bir teknik olarak işlemişlerdir.[68] Söz konusu MITRE ATT&CK çerçevesindeki son yıllardaki gelişmeleri dikkate alarak gerçekleşen saldırılara karşı matris üzerinde alınabilecek mevcut tedbirler değerlendirilmiş, akabinde henüz bu saldırıya karşı

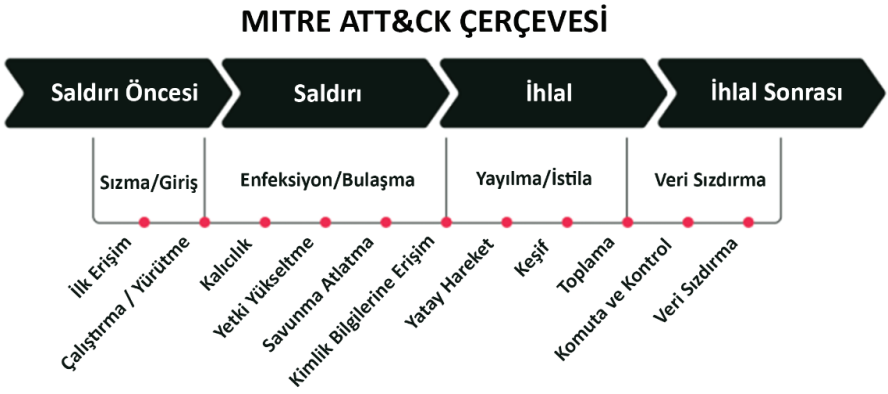
62 Ken Peffers, Tuure Tuunanen, Marcus A. Rothenberger ve Samir Chatterjee, "A Design Science Research Methodology for Information Systems Research", *Journal of Management Information Systems,* 24:3, 2007, s. 45-77.
63 Strom, Applebaum, Miller, Nickels, Pennington ve Thomas, "MITRE ATT&CK: Design and Philosophy".
64 B. Al-Sada, A. Sadighian, ve G. Oligeri, "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database*", IEEE Access,* 12, 2023, s. 1217-1234.
65 Yonghyun Jo, Oongjae Choi, Jiwoon You,Youngkyun Cha ve Dong Hoon Lee, "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework", *Sensors*, 22:5, 2022, s. 1860.
66 Sebastien Kanj Bonhard, Pau Garcia Villalta, Oriol Rosés ve Josep Pegueroles, "A Review of Tactics, Techniques, and Procedures (TTPs) of MITRE Framework for Business Email Compromise (BEC) Attacks", *IEEE Access*, 2025, s. 50761-50776.
67 Gwanghyun Ahn, Jisoo Jang, Seho Choi ve Dongkyoo Shin, "Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model with the MITRE ATT&CK Matrix", *IEEE Access*, 12, 2024, s. 89291-89309.
68 Robert Pell, Sotiris Moschoyiannis, Emmanouil Panaousis ve Ryan Heartfield, "Towards Dynamic Threat Modelling in 5G Core Networks Based on MITRE ATT&CK", arXiv preprint arXiv:2108.11206, 2021, https://arxiv.org/abs/2108.11206.

mevcut olmayan tedbir olarak eklenmesi önerilen teknik model açıklanmıştır. Genişletilmiş MITRE matrisine ait görsel çalışmanın sonunda ek olarak sunulmuştur.

4.1. Mevcut ATT&CK Çerçeve Matrisi

Mevcut durumda CTI yaklaşımını belirten ve güncelleyen çözüm olarak MITRE ATT&CK çerçevesi, siber güvenlik düzleminde genel kabul görmektedir. MITRE ATT&CK içerisinde yer alan teknik, taktik ve prosedürler (TTP) dışında atak yüzeyine göre matrisler "*Enterprise*" (Kurumsal Bilgi Teknolojileri [BT] Organizayonu), "*Mobile*" (Mobil Taşınabilir Cihazlar) ve "*ICS*" (Industrial Control Systems – Endüstriyel Kontrol Sistemleri, EKS) olarak çeşitli saldırı düzlemi ("*domain*"ler) şeklinde ayarlanmıştır. Şekil 1'de "*Enterprise*" (Kurumsal BT Organizasyonu) için ATT&CK Matrisi[69] bulunmaktadır:

Şekil 1. *Enterprise* (Kurumsal BT Organizasyonu) ATT&CK Çerçevesi[70]



APT grupları ister devlet destekli ister finansal motivasyonla bir araya gelmiş olsunlar, özel saldırı yöntemleri ve kendilerine özgü tehdit örüntülerini içeren teknik, taktik ve prosedürleri, yani TTP olarak ifade edilen saldırı davranışlarına sahiptirler. MITRE ATT&CK çerçevesi içinde TTP terimi, bir siber saldırganın kullandığı taktik, teknik ve prosedürler aşağıdaki gibi detaylandırılabilir:

- **Taktik:** Saldırganın nihai hedefi (örneğin, ayrıcalık yükseltme).
- **Teknik:** Bu hedefe ulaşmak için kullanılan yöntem (örneğin, kimlik bilgisi dökümü).
- **Prosedür:** Belirli bir saldırgan grubunun veya zararlı yazılımın, o tekniği nasıl uyguladığı (örneğin, Mimikatz aracıyla LSASS işlemini dump etmek).

Örnek olarak bir APT grubunun hedef aldığı bir kuruma sızmak için aşağıdaki MITRE ATT&CK çerçevesine göre izlediği TTP zinciri senaryo olarak aşağıdaki gibi ele alınabilir:

69 MITRE, *MITRE Enterprise Matrix*, https://attack.mitre.org/matrices/enterprise/, erişim 20.01.2025.
70 Nissim Pariente, "The Machine Identity Attack Surface - MITRE ATT&CK Framework Redefined", *Token Security*, 30 Nisan 2024, https://www.token.security/blog/the-machine-identity-attack-surface---mitre-attack-framework-redefined, erişim 20.01.2025.

Tablo 1. Bir APT Grubunun İzleyebileceği Örnek Bir TTP Zinciri Senaryosu

Taktik:	İlk Erişim (Initial Access)
Teknik:	Hedef Odaklı Oltalama Eklentisi (Spearphishing Attachment | T1566.001)
Prosedür:	Hedef çalışana özel hazırlanmış bir e-posta ve Word belgesi ile zararlı makro gönderilir.
Taktik:	Çalıştırma (Execution)
Teknik:	Kötücül Makro Yazılım (Malicious Macro | T1059.005)
Prosedür:	Kullanıcı belgeyi açınca makro, PowerShell komutu çalıştırır.
Taktik:	Kimlik Bilgisi Erişimi (Credential Access)
Teknik:	İşletim Sistemi Kimlik Bilgisi Sızdırma (OS Credential Dumping | T1003)
Prosedür:	Mimikatz aracı ile hafızadan kullanıcı şifreleri çekilir.
Taktik:	Yanal Hareket (Lateral Movement)
Teknik:	Uzak Erişim Servisleri (Remote Services – SMB/WinRM | T1021)
Prosedür:	Ele geçirilen şifre ile diğer makinelerde oturum açılır.
Taktik:	Veri Sızdırma (Exfiltration)
Teknik:	HTTPS Veri Sızdırma (Exfiltration Over HTTPS | T1041)
Prosedür:	Toplanan belgeler saldırganın kontrolündeki sunucuya HTTPS ile gönderilir.

APT saldırı gruplarının izlediği TTP örüntülerini anlamak adına, örnek bir vaka olarak APT29 saldırı grubu tarafından gerçekleştirilen "SolarWinds Saldırısı" izlerine bakılabilir. APT29, Rus istihbaratıyla bağlantılı bir tehdit aktörüdür. 2020'de SolarWinds Orion yazılımına zararlı kod yerleştirerek birçok Amerikan kurumunu etkileyen sofistike bir tedarik zinciri saldırısı gerçekleştirdi. Bu saldırı davranışına dair TTP dizilimi,[71] tehdit aktörünün yazılım tedarik zinciri zafiyetinden yararlanarak zararlı SUNBURST arka kapısını meşru bir güncelleme aracılığıyla dağıtımını içermektedir. Yasal SolarWinds imzası taşıyan bu zararlı kod, "Signed Binary Proxy Execution" tekniğiyle çalıştırılmış ve "Scheduled Task" kullanılarak sistemde kalıcılık sağlanmıştır. "Obfuscation" yöntemleriyle analizden kaçırılan zararlı yazılım, HTTPS protokolü üzerinden "Komuta ve Kontrol" (C2) iletişimi kurarak kurban sistemde keşif faaliyetleri gerçekleştirmiştir. Elde edilen kimlik bilgileriyle "Pass the Token" tekniği kullanılarak yatay hareket yapılmış; nihayetinde "Exchange" ve "O365" hesapları üzerinden hassas e-posta verileri toplanarak dışarı sızdırılmıştır. Sonuç olarak sofistike saldırı operasyonlarıyla ün kazanmış bu tür APT gruplarının davranış ve karakterini resmeden TTP diziliminde; "Taktik" ile hedef odaklı adım, "Teknik" ile kullanılan yöntem, "Prosedür" ile saldırganın bu tekniği nasıl uyguladığı tanımlanmaktadır.

18-19 Eylül'deki çağrı ve telsiz cihazları saldırılarının kamuoyuna yansıdığı şekliyle ele alındığında, en dikkat çeken husus, tedarik zinciri istismarı veya zafiyeti olacaktır. Bu

71 TTP dizilimindeki taktik ve prosedürler Türkçe olarak ifade edilse de siber ve bilişim kavramlarının çeviri karşılıkları nedeniyle TTP içerisindeki teknikleri içeren aşamalar orijinal İngilizce haliyle bırakılmıştır. Bknz. Sudhakar Ramakrishna, "New Findings from our Investigation of SUNBURST.", *SolarWinds Blog*, 11 Ocak 2021, https://www.solarwinds.com/blog/new-findings-from-our-investigation-of-sunburst, erişim 06.05.2025.

noktada, mevcut atak matrisi incelendiğinde bu yönde bir teknik bulunduğu görülmektedir. Öncelikle "İlk Erişim" (Initial Access) taktiği altında, "Tedarik Zinciri İhlali" altında yer alan "Donanım Tedarik Zinciri İhlali" alt tekniği (T1195.03) mevcut matriste yer alan bir yöntem olarak bulunmaktadır. Ancak bu teknik ve alt tekniğin saldırıları için geçerli platformların "Linux", "Windows" ve "MacOS" olduğuna dikkat edilmelidir. Bu açıdan gerçekleşen saldırılarla ilgili uygulanacak bir tedbir olarak geçerli olamayacağı değerlendirilmektedir.

Benzer isimde teknik ve alt teknik "*Mobile*" (Mobil cihaz) matrisi alanında da bulunmaktadır. Ancak aynı şekilde platformların sadece yukarıda bahsi geçen üç işletim sisteminde geçerli olduğuna dikkat edilmelidir. Bu noktada diğer bir matris olan "ICS" (EKS) alanında da "Tedarik Zinciri İhlali" tekniği (T0862) yer almaktadır. Bu teknik altında alt teknik bulunmamaktadır. Ayrıca herhangi bir platformu işaret eden gösterge de mevcut değildir. Bu nedenle, çağrı cihazı saldırısı özelinde, "ICS" (EKS) matrisi daha ilintili ve geçerli olabileceği göze çarpmaktadır. Bu yüzden ilgili kısmın atak matrisi olan "ICS" alanında ifade edilen "Tedarik Zinciri İhlali" şu şekilde açıklanmaktadır:[72]

> *"Cihazlar, yazılımlar ve teslimat mekanizmalarının son kullanıcıya ulaşmadan önce manipüle edilmesi yoluyla sistem güvenliğini tehlikeye atan bir siber saldırı türüdür. Bu tür ihlaller (zafiyetler), geliştirme araç ve ortamlarının yanı sıra yazılım dağıtım mekanizmalarını hedef alabilir ve meşru yazılım yamalarının değiştirilmesini içerebilir. Özellikle kontrol sistemleri gibi BT (bilgi teknolojileri) ve OT (operasyonel teknoloji) ağlarının bir arada bulunduğu ortamlarda, bir BT bileşenindeki zafiyet OT ortamına sızma fırsatları yaratabilir. Ayrıca, sahte cihazların küresel tedarik zincirine dahil edilmesi, güvenlik standartlarını karşılamayan ve düşük kaliteli malzemelerle üretilen ürünlerin varlık sahipleri ve operatörler için ciddi güvenlik ve operasyonel riskler oluşturmasına neden olabilir".*

Yukarıdaki açıklamaya istinaden, bu teknik ve alt tekniğin tedbir olarak yeterli gelmeyeceği, yetenekli saldırgan bir rakibin her çeşit zafiyeti tarayarak bulacağı herhangi bir açıklığı istismar edebileceği vakıadır. Bu açıdan atak matrisindeki diğer teknik ve alt tekniklere genel stratejik ve taktik operasyonel bakışla yaklaşmak faydalı olacaktır. Bu yüzden, teknikleri de kapsayan taktiklerin siber ölüm zincirindeki adımların hepsini içerdiğinden emin olacak şekilde görüntülemek gerekecektir. Aşağıda atak matrisinde her bir saldırı düzlemi (*domain*) için taktik ve kategorileri yer almaktadır:

Tablo 2. Karşılaştırmalı Taktik-Saldırı Düzlemi Atak Matrisi[73]

Taktik \ Domain	***Enterprise*** **(Kurumsal Bilgi Teknolojileri)**	***Mobile*** **(Taşınabilir Cihaz)**	***ICS*** **(Endüstriyel Kontrol Sistemleri)**
Gözetleme	Var	Yok	Yok
Kaynak Geliştirme	Var	Yok	Yok
İlk Erişim	Var	Var	Var
Çalıştırma	Var	Var	Var
Kalıcılık	Var	Var	Var
Yetki Yükseltme	Var	Var	Var

72 MITRE, "T0862: Remote Access Software", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T0862/, erişim 21.01.2025.

73 MITRE, "MITRE ATT&CK Tactics", https://attack.mitre.org/tactics/, erişim 22.01.2025.

Savunma Atlatma	Var	Var	Var
Kimlik Erişimi	Var	Var	Yok
Keşif	Var	Var	Var
Yatay Hareket	Var	Var	Var
Toplama	Var	Var	Var
Komuta ve Kontrol	Var	Var	Var
Veri Sızdırma	Var	Var	Yok
Tepki İşlevini Kısıtlamak	Yok	Yok	Var
Süreç Kontrolünü Bozmak	Yok	Yok	Var
Etki	Var	Var	Var
Ağ Etkileri	Yok	Var	Yok
Uzak Servis Etkileri	Yok	Var	Yok

Çağrı ve telsiz cihazları saldırısı özelinde, söz konusu saldırının yukarıda da belirtildiği gibi en kritik aşaması tedarik zinciri ihlali/zafiyeti olsa da planlayıcı hasım aktörün bu operasyonun başarı şansını tek başına tedarik zinciriyle denemeyeceği göz önüne alınmalıdır. Bu bağlamda atak matrisini daha detaylı ele alarak çalışmanın başında bahsi geçen diğer disiplinlerle benzerlik ve yakınlık kurgulanmalıdır. Benzer şekilde, siber güvenlik disiplini açısından atak matrisi içerisinde yer alan muhtemel ve potansiyel diğer teknik ve taktikleri ele almak araştırmanın sonuçlarını destekleyecektir. Bir önceki paragrafta "İlk Erişim" taktiği gibi "Kaynak Geliştirme" (*Resource Development*) taktiği de saldırıya ilişkin ipuçları verebilecek teknik ve alt teknikleri içermektedir. "Kaynak Geliştirme" taktiği altında yer alan "Altyapı Edinmek" (*Acquire Infrastructure*) tekniği (T1583) de yine benzer bir önlem olarak ifade edilmektedir:[74]

> *"Saldırganlar hedefleme sırasında kullanılabilecek altyapıyı satın alabilir, kiralayabilir veya elde edebilir. Muhasım operasyonları barındırmak ve düzenlemek için çok çeşitli altyapılar mevcuttur. Altyapı çözümleri arasında fiziksel veya bulut sunucuları, etki alanları ve üçüncü taraf web hizmetleri bulunur. Bazı altyapı sağlayıcıları, altyapı edinimini sınırlı veya ücretsiz olarak sağlayan ücretsiz deneme süreleri sunar. Bu altyapı çözümlerinin kullanımı, rakiplerin operasyonları sahneye koymalarına, başlatmalarına ve yürütmelerine olanak tanır. Uygulamaya bağlı olarak, rakipler fiziksel olarak kendilerine bağlanmayı zorlaştıran altyapılar kullanabilir ve ayrıca hızla sağlanabilen, değiştirilebilen ve kapatılabilen altyapıları kullanabilir".*

Saldırılar kapsamında ilintili olabilecek ve yine "İlk Erişim" taktiği altında tedarik zinciri ihlali tekniğinden sonra yer alan "Güvenilir İlişki" (*Trusted Relationship*) tekniği (T1199) de platform olarak dar kapsamlı olmasına rağmen tanım olarak benzer bir önermeyi desteklemektedir:[75]

> *"Saldırganlar, hedeflenen kurbanlara erişimi olan kuruluşları ihlal edebilir veya başka şekillerde bunlardan yararlanabilir. Güvenilir üçüncü taraf ilişkisi aracılığıyla erişim, korunmayan veya bir ağa erişim elde etmenin standart mekanizmalarından daha az incelemeye tabi tutulan mevcut bir*

74 MITRE, "T1583: Acquire Infrastructure", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T1583/, erişim 22.01.2025.

75 MITRE, "T1199: Trusted Relationship", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T1199/, erişim 23.01.2025.

bağlantıyı kötüye kullanır. Kuruluşlar genellikle dahili sistemleri ve bulut tabanlı ortamları yönetmelerine olanak sağlamak için ikinci veya üçüncü taraf harici sağlayıcılara yükseltilmiş erişim izni verir. Bu ilişkilere örnek olarak BT hizmetleri yüklenicileri, yönetilen güvenlik sağlayıcıları, altyapı yüklenicileri verilebilir. Üçüncü taraf sağlayıcının erişimi, bakımı yapılan altyapıyla sınırlı olacak şekilde tasarlanmış olabilir, ancak kuruluşun geri kalanıyla aynı ağda bulunabilir. Bu nedenle, diğer tarafın dahili ağ sistemlerine erişim için kullandığı "Geçerli Hesaplar" tehlikeye atılabilir ve kullanılabilir".

Yukarıdaki yaklaşımla devam edildiğinde; "İlk Erişim" taktiği altında "Donanım İlaveleri" (*Hardware Additions*) tekniği (T1200) de benzer şekilde tanım ve açıklama olarak vakadaki istismarın kök nedenine yakın olsa bile sadece "Linux", "Windows" ve "MacOS" platformlar için geçerli olması nedeniyle tam anlamıyla örtüşen bir tedbir olmadığı görülmektedir. Yine aynı durumda diğer benzer teknikler; "Trafik Sinyalleşmesi" (*Traffic Signaling*) tekniği (T1205), "Yapay Kodları Saklama" (*Hide Artifacts*) tekniği (T1564), "Zayıf Şifreleme" (*Weaken Encryption*) tekniği (T1600) ve "Ağ Dinleme" (*Network Sniffing*) tekniği (T1040) bu bağlamda, çağrı cihazları saldırısının arka planındaki mantığa yaklaşmakla birlikte tam anlamıyla teknik detaylar örtüşmediği için böyle sofistike bir saldırıyı önleyebilecek bir tedbir olarak uyarlanması, bu çalışma kapsamında değerlendirilmemektedir. Bu sebeple, çağrı cihazı saldırısının kendine özgü yaklaşımı göz önüne alındığında, tehdit aktörlerine karşı atak matrisinde tedbir sağlayabilecek ilintili taktik kategorisine eklenecek yeni bir teknik model önerilmektedir.

4.2. Önerilen Model (TTP & Matris Kategorisi)

Bu çalışma, çağrı cihazı saldırılarını nihai hedef olarak değil, EH, SIGINT ve siber uzay arasında gelişen hibrit tehditlerin erken bir örneği olarak değerlendirmektedir. Önerilen teknik model, bu tür saldırılarda kullanılan taktik, teknik ve prosedürlerin (TTP) yalnızca çağrı cihazlarına değil, benzer sinyal tabanlı sistemlere yönelik genişletilebilirliğini amaçlamaktadır. Bu kapsamda önerilen teknik model, yalnızca çağrı cihazı gibi tekil sistemlere değil; elektromanyetik spektrumda çalışan, düşük bant genişliğine ve yüksek parazit hassasiyetine sahip tüm sistemlere uygulanabilecek şekilde genişletilebilir. Bu yönüyle model, hibrit tehditler karşısında spektrum tabanlı tehdit tespitine yönelik CTI altyapılarına yeni bir matris katkısı sunmayı amaçlamaktadır. Bu bağlamda önerilen model, sinyal istismarı tabanlı saldırıların tespiti için mevcut MITRE ATT&CK çerçevesine SIGINT ve EH bileşenlerinin entegrasyonuna yönelik kavramsal bir açılım sağlamaktadır. Model, dar örneklemlerden yola çıkarak daha kapsayıcı CTI mimarilerine zemin hazırlamayı hedeflemektedir.

Bu hususlardan yola çıkarak saldırıların kendine özgü yapısı nedeniyle içerisinde yer alan EH, RF ve SIGINT kabiliyetleriyle atak matrisi içerisine yeni bir model olarak uygun bir teknik önerisi getirilmektedir. Diğer bir ifadeyle, mevcut CTI yaklaşımı ve MITRE ATT&CK çerçevesinde bu analizlere istinaden EH ve RF sinyalleriyle ilişkili saldırı izlerini tespit edebilecek kabiliyetlere haiz bir teknik önerilmektedir. Örneğin, RF sinyallerinin manipülasyonu, iletişim cihazlarının hedef alınması veya EH tekniklerinin uygulandığı durumlar, matris içinde kapsamlı bir teknik kategoriye dönüşmektedir. Dolayısıyla atak matris altında bilinen saldırıların tespiti ve müdahalesine yönelik mevcut teknikleri tekrar etmek yerine, dijital ve fiziksel ortamların kesişim kümesinde gerçekleşen hibrit tehditlere dair yeni bir perspektif geliştirilmektedir. Özellikle çağrı ve telsiz cihazlarına yönelik saldırılardan yola çıkarak, bu olaylar örnek olay formatında değerlendirilmiş ve siber-fiziksel alanlarda faaliyet gösteren hasım aktörlerin kullandığı taktiklerin modellenmesi hedeflenmiştir.

Bu bağlamda, klasik MITRE ATT&CK matrisinin kapsamadığı EH, RF ve SIGINT unsurları dikkate alınarak yeni bir teknik kategori önerilmektedir. Özellikle iletişim altyapılarının manipülasyonu, RF sinyallerinin yönlendirilmesi veya bozulması, EH teknikleri ile iletişimin engellenmesi gibi eylemler, geleneksel CTI araçlarının dışında kalan, ancak artan oranda karşılaşılan bir tehdit sınıfını oluşturmaktadır. Üstelik bu çalışma, çağrı cihazları gibi örnek olaylardan ilhamla, gelecekte farklı platformları da hedef alabilecek benzer tehditlere karşı genişletilebilir bir model sunmaktadır. Model önerisi, yalnızca çağrı cihazı kategorisiyle sınırlı olmayıp, benzer RF tabanlı veya radyo link sistemlerine yönelik tehditlerin de modellenmesine olanak tanıyacak biçimde geniş bir yelpazede düşünülmüştür. RF jammer cihazları, spektrum analizörleri, yazılım tanımlı radyo (SDR) sistemleri gibi hem donanım hem yazılım tabanlı unsurlar, bu tür saldırıların teknik ayak izlerini oluşturmakta ve siber-fiziksel saldırıların dijital CTI platformlarına entegrasyonu için yeni araçlara ihtiyaç duyulmaktadır.

Bu çerçevede önerilen teknik model, EH/RF izlerinin dijital tehdit istihbarat sistemlerinde yapılandırılmış biçimde izlenmesini sağlayacak yazılım araçları, teknik göstergeler ve ilişkilendirme mekanizmalarının geliştirilmesini önermektedir. Böylece tehdit istihbaratı yalnızca ağ trafiği veya zararlı yazılımlar üzerinden değil, sinyal tabanlı manipülasyon teknikleri üzerinden de zenginleşecektir. Araştırmanın odaklandığı çağrı cihazları saldırısı örneği, bu kapsayıcı modelin somut bir çıkış noktası olarak değerlendirilmelidir. Sonuç olarak bu çalışma kapsamında yürütülen araştırma, çağrı cihazları özelinde gelişse de RF spektrum temelinde yer alan tüm sistem ve altyapılar dahil edilebilir durumdadır. Bu noktada hedef alınabilecek sistemlere yönelik ilk aşamada önlem olarak yeni teknik model önerisi aşağıdaki gibidir:

Tablo 3. RF Spektrumu ve Sinyalleri için Yeni Teknik Model Önerisi

Teknik:	"T1569.xx – Spectrum-Based Signal Injection"
Taktik:	"Execution" (Çalıştırma)
Teknik Adı: "Spectrum-Based Signal Injection" (Spektrum Tabanlı Sinyal Enjeksiyonu)	
Tanım:	Saldırganlar, belirli RF spektrumlarını hedef alarak telsiz, çağrı cihazı veya diğer sinyal tabanlı haberleşme sistemlerine sahte mesajlar enjekte edebilir. Bu teknik, sinyal manipülasyonu yoluyla bilgi akışını bozmak, yanlış yönlendirme yapmak veya kriz anlarında karar destek sistemlerini yanıltmak amacıyla kullanılabilir. Özellikle acil servisler, endüstriyel kontrol sistemleri ve askerî birimlerde kritik operasyonel sonuçlar doğurabilir.

Böyle bir saldırı yüzeyinde hedefe ulaşan saldırganlar aksiyon alırken *"*sahte acil tıbbi çağrılar oluşturarak sağlık sistemlerinde kriz yaratabilir" veya "kritik altyapıyı yöneten teknisyenleri yanlış yönlendirerek operasyonları aksatabilir" veyahut da "acil durum servislerini sahte tehditlerle yanlış yönlendirerek gerçek tehditleri gizleyebilir". Bu yönde bir saldırının tedbirleri olarak birtakım iyileştirme (*mitigation*) önerileri aşağıda listelenmektedir:

- **Şifreleme Kullanımı:** Modern çağrı cihazı sistemlerinde uçtan uca şifreleme uygulanmalıdır.
- **Sayısal İmza:** Mesaj bütünlüğünü korumak için sayısal imza kullanılmalıdır.
- **RF Anomali Algılama:** Radyo trafiğini analiz eden sistemler sahte mesajları tespit etmektedir.

- **Çok Faktörlü Doğrulama:** Kritik mesajlar için ikinci bir doğrulama gerekmektedir.

Bu teknik için iyileştirme önerilerinin hayata geçirilmesi, sadece teknik bir çabanın ötesinde, kapsamlı politika ve stratejik düzenlemeler gerektirmektedir. Örneğin, "Şifreleme Kullanımı" ve "Sayısal İmza" gibi önlemlerin yaygınlaştırılması, kritik iletişim altyapılarında kullanılacak cihazlar için ulusal düzeyde asgari güvenlik standartlarının belirlenmesini ve bu standartlara uyumun denetlenmesini sağlayacak yasal ve kurumsal çerçevelerin oluşturulmasını zorunlu kılmaktadır. Telekomünikasyon düzenleme kurumları, ulusal siber güvenlik merkezleri ve ilgili bakanlıkların koordinasyonu, bu politikaların etkin bir şekilde uygulanmasında kritik rol oynamaktadır.[76] "RF Anomali Algılama" sistemlerinin geliştirilmesi ve entegrasyonu, ulusal sinyal istihbaratı ve elektronik harp kapasitelerinin sivil ve kritik altyapıların korunmasına yönelik olarak da planlanmasını gerektirmektedir. Bu tür yetenekler, bir ülkenin teknolojik bağımsızlığını ve bilgi üstünlüğünü pekiştirerek ulusal gücün bir unsuru haline gelir. Ayrıca, "Çok Faktörlü Doğrulama" gibi önlemlerin benimsenmesi, sadece teknik bir güvenlik katmanı eklemekle kalmaz, aynı zamanda kullanıcıların güvenlik bilincini arttırarak olası sosyal mühendislik saldırılarına karşı psikolojik bir direnç de oluşturur.[77] Bu tür bütüncül yaklaşımlar, devletlerin hibrit tehditlere karşı caydırıcılığını güçlendirip kriz anlarında iletişim sistemlerine olan güvenin sarsılmasını engelleyerek toplumsal paniğin de önüne geçebilir.

Teknik model önerisinin atak matrisi içinde "Çalıştırma" (*Execution*) taktiği altında eklenmesi uygun görünmektedir. Hem aktif saldırılarda (operasyon manipülasyonu) hem de kaos yaratmak için (bilgi harbi ve dezenformasyon) kullanılabilecek bir saldırı vektörü olarak ele alınmalıdır. Hizbullah'a karşı Mossad tarafından gerçekleşen saldırılar, siber atak yüzeyi dijital ortamlardan ziyade analog varsayılan çağrı ve telsiz cihazlarına yönelik olduğu için, Elektronik Harp, RF ve SIGINT gibi yetenek ve kapasitelerini öne çıkaracak teknik model önerisi kurgulanmıştır. Bu açıdan, Hizbullah hedeflerine yönelik saldırılar, aynı zamanda bir istihbarat operasyonu olarak kabul edilse de sürecin teknoloji ayağında, EH, SIGINT ve RF manipülasyonunu içeren bu tür hibrit saldırılara ilişkin aşağıdaki gibi bir teknik model önerisi önerilmektedir:

Tablo 4. RF Sinyal ve Çağrı/Telsiz Haberleşme Özelinde Teknik Model Önerisi

Teknik:	"T1602.xx – RF Message Injection & Manipulation"
Taktik:	"Impact" (Etki)
Teknik Adı: "RF Message Injection & Manipulation" (RF Mesaj Enjeksiyonu ve Manipülasyonu)	
Tanım:	Saldırganlar, eski tip çağrı cihazları, telsiz haberleşmesi (VHF/UHF), ve diğer RF tabanlı analog-dijital sistemleri hedef alarak sahte mesajlar gönderebilir, EH ve SIGINT kabiliyetleriyle mevcut mesajları değiştirebilir veya iletişimi kesintiye uğratabilir.

SIGINT ve EH yetenekleriyle desteklenerek özellikle askerî gruplar, istihbarat servisleri ve devlet destekli aktörler tarafından tetiklenebilecek bu saldırı türü, mevcut dijital altyapı yerine analog veya hibrit ortamlarda gerçekleştirir. Önerilen bu teknik modelin adımları ise şu şekilde sürdürülür:

76 Serkan Gündoğdu, "Uluslararası Politikada Bir Etki Aracı Olarak Siber Güvenlik ve Türkiye'nin Siber Güvenlik Politikası Uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM)", *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33:3, 2023, s. 1325-1337.

77 Scott D. Applegate, "Social Engineering: Hacking the Wetware!", *Information Security Journal: A Global Perspective*, 18:1, 2009, s. 40-46.

- **RF Sinyal Toplama:** Hedef telsiz/çağrı cihazı frekansları belirlenir.
- **Protokol Analizi:** Kullanılan haberleşme protokolleri incelenir.
- **Mesaj Enjeksiyonu:** Sahte mesajlar oluşturularak operasyonel yanlış yönlendirme yapılır.
- **Karıştırma ve Şifre Kırma:** Analog veya zayıf şifrelemeye sahip haberleşmeler engellenir veya deşifre edilir.
- **Psikolojik Operasyonlar ve Aldatma:** Yanlış bilgiler yayarak düşmanın karar mekanizmaları etkilenir.

Önerilen teknik modelin saldırı adımlarını inceleyerek buna yönelik çeşitli iyileştirme önerileri ihtiyaç vardır. Bu yüzden MITRE ATT&CK çerçevesi dahilinde üç farklı saldırı düzlemi olan matris içerisinde iyileştirme (*mitigation*) olarak geçen bu seçeneklere dair çalışma kapsamında aşağıdaki gibi bir tablo ilave edilmiştir:

Tablo 5. Önerilen Teknik Model için İyileştirme Seçenekleri

ID	İyileştirme Adı	Açıklama
M1030/0930 – *Network Segmentation* (Ağ Segmentasyonu)	Şifreli ve Güvenli Haberleşme Protokolleri	RF tabanlı sistemlerde AES-256 veya ECC şifreleme ve kimlik doğrulama kullanarak sahte mesajların enjekte edilmesi önlenir.
M1031 – *Network Intrusion Prevention* (Ağ Saldırısı Önleme)	RF Sinyal Filtreleme ve Anomali Algılama	SDR-tabanlı izleme sistemleri ile anormal RF sinyalleri tespit edilir ve sahte mesaj girişimleri engellenir.
M1037 – *Filter Network Traffic* (Ağ Trafiği Filtreleme)	Frekans Atlamalı Spektrum Yayılımı (FHSS) ve LFM Kullanımı	Düşman RF sinyal analizine karşı FHSS/LFM gibi tekniklerle haberleşme güvence altına alınır.
M1038/0938 – *Execution Prevention* (Çalıştırma Önleme)	Çok Katmanlı Doğrulama Mekanizmaları	Gelen RF mesajlarını ikinci bir kanal (şifreli uygulamalar, sesli doğrulama) ile kontrol ederek sahte mesaj enjeksiyonları engellenir.
M1029 – *Remote Data Storage* (Uzak Veri Depolama)	Sinyal İstihbaratı ve Olay Müdahale Ekipleri	EH ve SIGINT ekipleri entegre edilerek düşman RF operasyonları izlenir ve proaktif müdahale edilir.

Bu saldırı tekniği, RF tabanlı analog veya modern hibrit haberleşme sistemlerine yönelik ciddi bir tehdit oluşturduğundan, önerilen iyileştirme stratejileri (Tablo 5) çok katmanlı bir yaklaşımla ele alınmaktadır. Bu stratejiler, sadece teknik önlemleri ve operasyonel prosedürleri değil, aynı zamanda politika yapım süreçlerini, kurumsal yapılanmaları ve ulusal güvenlik anlayışlarını da kapsamaktadır. Böylece MITRE ATT&CK matrisi, sadece teknik bir referans olmaktan çıkarak hibrit tehditlere karşı bütüncül ve disiplinler arası bir strateji geliştirme aracı haline gelebilir.

Ağ Segmentasyonu iyileştirme adımı, teknik düzeyde şifreleme standartlarının benimsenmesini önermekle birlikte, politika düzeyinde bu standartların kritik sektörlerde zorunlu hale getirilmesi, ilgili yasal düzenlemelerin yapılması ve uyum denetim mekanizmalarının kurulmasını gerektirmektedir. Bu, ulusal bir politika kararıdır ve telekomünikasyon otoriteleri ile siber güvenlik kurumlarının eşgüdümünü zorunlu kılmaktadır.

Ağ saldırısı önleme, ağ trafiği filtreleme ve çalıştırma önleme adımları politika yapım süreçleri açısından, gerekli teknolojilerin geliştirilmesi ve yaygınlaştırılması için Ar-Ge faaliyetlerini, spektrum yönetimi politikalarının güvenlik odaklı güncellenmesini ve bu sistemlerin ulusal

erken uyarı ve müdahale merkezlerine entegrasyonunu gerektirmektedir. Bu tür yetenekler, ülkenin elektromanyetik spektrum üzerindeki egemenliğini pekiştirmekle kalmayıp hasım aktörlerin RF tabanlı saldırılarına karşı caydırıcılık oluşturarak ulusal güvenliğe doğrudan katkı sağlayacaktır. Psikolojik olarak, bu tür görünür etkin savunma sistemlerinde, kamuoyunun devletin koruma kapasitesine olan güvenini arttıracağı beklenebilir.

Uzak Veri Depolama (M1029) başlığı altında önerilen EH ve SIGINT ekiplerinin entegrasyonu, doğrudan bir ulusal güvenlik ve istihbarat politikası meselesi konumundadır. Bu tür entegre ekiplerin oluşturulması, farklı kurumlar (askerî, sivil istihbarat, siber güvenlik merkezleri ve kolluk kuvveti) arasında etkin bir iş birliği ve bilgi paylaşım mekanizmasının kurulmasını gerektirmektedir. Kurumsal olarak, bu ekiplerin yetki ve sorumluluklarının net bir şekilde tanımlanması, yasal altyapılarının güçlendirilmesi ve sürekli tatbikatlarla operasyonel yeteneklerinin geliştirilmesi elzemdir. Bu tür bir yapılanma, düşman RF operasyonlarının proaktif bir şekilde izlenmesi ve bunlara hızlı müdahale edilmesi sayesinde, potansiyel bir krizin büyümeden engellenmesine veya etkilerinin minimize edilmesine olanak tanıyacaktır.

5. Tartışma ve Güvenlik Analizi

Bu bölüm, çalışmanın konusunda ifade edilen mevcut matris ve önerilen modele ilişkin güvenlik analizi ve tartışma kısımlarını içermektedir.

5.1. Tartışma

İsrail'in bu operasyonu, MITRE ATT&CK çerçevesinde yer almayan ancak elektromanyetik spektrum temelli tehditlerin, tedarik zinciri manipülasyonu ile birleştiğinde, siber güvenlik modellerine nasıl entegre edilmesi gerektiğine dair önemli ipuçları sunmaktadır. İlk aşamada, İsrail'in Hizbullah'a yönelik yürüttüğü saldırılar, eş zamanlı patlamalarla iki dalga halinde gerçekleştirilmiş ve ilk gün "çağrı" cihazlarını, ikinci gün ise "el telsizi" cihazlarını hedef almıştır. Bu saldırılar, Hizbullah içinde operasyonel bütünlüğü bozmak ve karar alma süreçlerini sekteye uğratmak amacı taşımaktadır. İsrail'in bu saldırılarda yalnızca fiziksel hedeflere değil, aynı zamanda psikolojik ve operasyonel etkiler yaratmaya odaklandığı belirtilmektedir. Özellikle bu saldırıların zamanlaması ve hedef seçimleri, dijital harp ile geleneksel askerî operasyonların hibrit bir stratejiyle nasıl bütünleştirildiğini göstermektedir. İlk iki gün süren dijital harp sonrası Tel Aviv'in doğrudan askerî müdahaleye geçmesi, operasyonel süreçlerin çok katmanlı planlandığını ortaya koymaktadır.[78]

Söz konusu yukarıdaki ifadelere dayanarak araştırma kapsamında dijital harp sahasında EH ve SIGINT imkanlarının siber istihbarat ve CTI kabiliyetleriyle ele alınarak hibrit ve disiplinler arası yaklaşımla kurgulanabileceği potansiyelini göstermektedir. Çünkü İsrail'in bu operasyonu gerçekleştirme biçimi, insan istihbaratı ile siber, sinyal ve elektronik istihbaratın entegre edildiği, yüksek hassasiyetle yürütülen bir planlamayı işaret etmektedir. Özellikle Hizbullah'ın haberleşme cihazlarına yönelik gerçekleştirilen saldırıların, tedarik zincirine sızma yoluyla mümkün hale geldiği vurgulanmaktadır. İsrail'in, hedeflenen cihazların tedarik sürecine önceden müdahale ederek, cihazlara patlayıcı veya zararlı yazılım yerleştirdiği ve bu sayede hedefe doğrudan zarar vermeden önce haberleşme altyapısını çökerttiği belirtilmektedir. Bu durum, tedarik zinciri saldırılarının modern askerî stratejilerde nasıl kritik bir unsur haline geldiğini ve elektronik harp ile siber güvenlik arasındaki sınırların giderek bulanıklaştığını göstermektedir. Bu operasyon hem askerî hem

78 Merve Seren, "İsrail'in Yeni İstihbarat Operasyonu: Pager ve Walkie-Talkie saldırıları", *Fikir Turu*, 24 Eylül 2024, https://fikirturu.com/jeo-politika/israilin-yeni-istihbarat-operasyonu/, erişim 25.09.2024.

de istihbarat doktrinlerinde yeni bir paradigma oluşturmuştur ve tedarik zinciri güvenliğinin, ulusal güvenlik stratejilerinde öncelikli bir unsur olması gerektiğine dikkat çekmiştir.[79]

Bu çalışmanın temel araştırma sorularından birisi olan "MITRE ATT&CK çerçevesi, elektromanyetik spektrum ve tedarik zinciri güvenliği boyutları eklenerek nasıl genişletilebilir?" ifadesine yanıt ararken, ATT&CK matrisinin mevcut sınırları ile analog ve fiziksel sistemleri yeterince kapsayamayan yapısı ortaya çıkmaktadır. Özellikle elektromanyetik spektrum temelli saldırılar ve donanım tedarik zincirine yönelik tehditler, mevcut çerçevede bütünsel olarak temsil edilmemektedir. İsrail'in Lübnan'da gerçekleştirdiği sinyal tabanlı saldırı operasyonu bu boşluğa dikkat çekmekte ve yeni bir modelleme ihtiyacını gündeme getirmektedir.

MITRE ATT&CK çerçevesi, esas olarak yazılım ve ağ katmanlarında çalışan dijital saldırı tekniklerini modellemekte başarılıdır. Ancak elektromanyetik spektrum üzerinden gerçekleştirilen saldırılar, özellikle RF tabanlı iletişim cihazlarını hedef aldığında, bu çerçevede kendisine karşılık bulamamaktadır. "Spectrum-Based Signal Injection" tekniğiyle önerilen yeni modelleme, özellikle çağrı cihazları gibi analog sistemlerin güvenlik boyutunu MITRE terminolojisi içine entegre etmeyi hedeflemektedir. İsrail'in saldırısı örneğinde olduğu gibi, analog haberleşme protokollerini hedefleyen düşük frekanslı enjeksiyonlar, dijital ağ güvenliği araçlarıyla tespit edilememekte, buna karşılık taktik ve operasyonel seviyede yüksek etkiler yaratmaktadır. Bu durum, elektromanyetik spektrumun saldırı yüzeyi olarak modellenmesi gerektiğini ve bu alanın MITRE içinde ayrı bir kategori olarak ele alınmasını zorunlu kılmaktadır.

Gerçekleşen saldırıların en başından itibaren dillendirilen tedarik zinciri zafiyeti ve istismarı siber istihbarat disiplininde ve MITRE çerçevesinde halihazırda kendisine yer bulmaktadır. Ancak mevcut MITRE çerçevesinde yer alan teknikler üç farklı saldırı düzlemi (*domain*) için de dijital tabanlı cihazlar için uygulanabilir yöntemleri içermektedir. Lakin gerçekleşen çağrı cihazı saldırılarının RF sinyalleri işleyecek analog tabanlı veya analog-dijital dönüştürücü modülleri içeren cihazlara yönelik olduğu bir vakıadır. Hizbullah'ın basit tasarıma sahip çağrı cihazlarını kullanması, modern gözetim sistemlerinden kaçınma amacı taşırken, bu durum aynı zamanda cihazların güvenlik açıklarının kurcalanmasına karşı savunmasız hale gelmesine de neden olmuştur. Modern şifreleme veya kurcalamaya karşı koruma mekanizmalarından yoksun olan bu cihazlar, kolayca modifiye edilebilecek bir zafiyet yaratmıştır. İsrail'in bu güvenlik açığını istismar ettiği ve Hizbullah'ın lojistik ekipleri tarafından fark edilmeyecek şekilde çağrı cihazlarına patlayıcı maddeler yerleştirdiği değerlendirilmektedir. Bu sürecin, paravan bir şirket aracılığıyla gerçekleştirilen kontrollü bir üretim ve teslimat mekanizması üzerinden yürütüldüğü, ardından senkronize bir patlatma ile operasyonun tamamlandığı düşünülmektedir. Bu durum, düşük teknolojili cihazların basit yapılarının dahi istihbarat operasyonlarında nasıl stratejik bir avantaja dönüştürülebileceğini göstermektedir.[80]

ATT&CK matrisinde tedarik zinciri saldırılarına ilişkin belirli teknikler bulunsa da bunlar daha çok yazılım güncellemeleri ve lojistik manipülasyonlar çerçevesinde sınırlı kalmaktadır. Oysa modern siber-fiziksel saldırılar, donanım bileşenlerinin üretiminden yerleşik anten yapılarına kadar geniş bir yelpazeyi hedef almaktadır. İsrail'in saldırısında kullanılan sinyal enjeksiyonu tekniği, yalnızca mesaj içeriklerini değil, mesajların alındığı

79 Age.

80 Salih Bıçakçı, "Lübnan'da Patlayan Çağrı Cihazları: Elektronik Harp, Siber Sabotaj ve Kötülüğün Sıradanlığı", *Fikir Turu*, 23 Eylül 2024, https://fikirturu.com/jeo-politika/lubnanda-patlayan-cagri-cihazlari/, erişim 24.09.2024.

cihazın fiziksel kabiliyetlerini de manipüle etmiştir. Bu durum, ATT&CK çerçevesinin donanım güvenliğine ilişkin daha derinlemesine alt tekniklerle genişletilmesi gerektiğini göstermektedir. Zira Lübnan'daki operasyon kapsamında çağrı cihazlarının eşzamanlı patlaması, RF sinyalleri ve donanım yazılımı manipülasyonuna dayalı karmaşık bir mühendislik çalışması ile açıklanabilir. Çağrı cihazlarının basit tasarımı ve sınırlı işlem kapasitesi, modern güvenlik protokollerinden yoksun olmaları nedeniyle, RF sinyalleriyle uzaktan tetiklenmeye veya ürün yazılımına yönelik bir sabotaja açık hale gelmiştir. Olası senaryolardan biri, cihazlara güç yönetim sistemlerini etkileyen özel bir RF sinyali gönderilmesi ve elektrik akımında bir dalgalanma yaratılarak patlamaların başlatılmasıdır. Diğer olasılık ise, cihazların belirli bir RF frekansına ayarlanarak merkezi bir "patlatma" komutunu algılayacak şekilde tasarlanmış olmasıdır. Ayrıca, cihazların ürün yazılımına önceden yerleştirilen bir arka kapı sayesinde, belirli bir sinyal veya zaman gecikmeli komutla patlamaların tetiklenmesi mümkün olabilir. Bu durumda, senkronizasyonun sağlanması için cihazlara küçük zamanlayıcıların entegre edilmesi ve bu zamanlayıcıların RF sinyalleri ile tetiklenmesi muhtemeldir. Bu operasyon, istihbarat örgütlerinin düşük teknolojili cihazlara yönelik hassas mühendislik ve karmaşık siber/elektronik manipülasyon tekniklerini başarıyla birleştirdiğini gösteren bir planlama örneği olarak literatüre geçmiştir.[81]

Bu bağlamda geliştirilen "T1569.xx – *Spectrum-Based Signal Injection*" ve "T1602.xx – *RF Message Injection & Manipulation*" teknik model önerileri, teknik düzeyde hem elektromanyetik hem donanım hem de taktiksel bütünlük açısından hibrit bir saldırı modelini temsil etmektedir. Bu öneri, halihazırda "Çalıştırma" (*Execution*) taktiği altında yer alan benzer tekniklerle kavramsal bir akrabalık taşımakta ancak donanımsal sinyal manipülasyonlarını kapsayan yeni bir katman tanımlamaktadır. Böylece, ATT&CK çerçevesi genişletilerek, analog/dijital hibrit savaş alanlarına daha duyarlı hale getirilebilir. Tüm bu bulgular, araştırma sorusunun ortaya koyduğu boşluğun somut örneklerle desteklendiğini göstermektedir. MITRE ATT&CK çerçevesi, elektromanyetik spektrumun ve donanım temelli saldırıların dikkate alınmadığı sürece, hibrit savaş ve istihbarat operasyonlarının gerçekliğini modellemekte yetersiz kalmaktadır. Bu nedenle, elektromanyetik spektrum tabanlı saldırılar ve fiziksel cihaz manipülasyonları, çerçevenin genişletilmesi gereken temel alanlar olarak önerilmekte ve "Spektrum Tabanlı Sinyal Enjeksiyonu" ve "RF Mesaj Enjeksiyonu ve Manipülasyonu" bu genişlemenin bir ön modeli olarak sunulmaktadır.

5.2. Güvenlik Analizi

Bu çalışmada analiz edilen olaylar, hibrit tehditlerin operasyonel güvenliğe yönelik çok yönlü riskler barındırdığını ortaya koymaktadır. EH, SIGINT ve RF teknikleri ile siber saldırılar arasında giderek belirsizleşen çizgiler, geleneksel güvenlik önlemlerinin yeterliliğini sorgulatmaktadır. Özellikle, RF tabanlı sinyallerin ve iletişim altyapılarının manipülasyonu gibi tehditler, siber tehdit istihbaratı çerçevesinde ele alınması gereken yeni bir kategoriye veya matris içerisinde uygun taktik altında bir tekniğe işaret etmektedir. Dünya genelinde hükümetleri ve kuruluşları siber güvenlik çerçevelerini yeniden değerlendirmeye sevk eden[82] ve analiz edilen çağrı cihazı saldırıları olayı, hibrit tehditlerin sadece teknik bir zafiyetten ibaret olmayıp aynı zamanda operasyonel güvenliğe, toplumsal psikolojiye ve uluslararası ilişkilere yönelik çok yönlü riskler barındırdığını çarpıcı bir şekilde ortaya koymaktadır. Özellikle, RF tabanlı sinyal tehditleri, CTI ve genel güvenlik analizleri çerçevesinde

81 Age.

82 Pantha Protim Sarker, Upoma Das, Nitin Varshney, Shang Shi, Akshay Kulkarni, Farimah Farahmandi ve Mark Tehranipoor, "When Everyday Devices Become Weapons: A Closer Look at the Pager and Walkie-Talkie Attacks", arXiv preprint arXiv:2501.17405, 2025.

ele alınması gereken, ancak mevcut yaklaşımların tam olarak kapsayamadığı yeni risk kategorileri oluşturmaktadır. Bu durum, güvenlik analizlerinin sadece teknik zafiyetlere değil, aynı zamanda bu zafiyetlerin istismar edilme biçimlerinin ardındaki stratejik niyetlere, sosyopolitik bağlamlara ve potansiyel toplumsal etkilere de odaklanması gerektiğini göstermektedir.

MITRE ATT&CK çerçevesini görselleştiren atak matrisi üzerinde RF ve EH tabanlı saldırıları siber tehditlerle ilişkilendirmek zorlayıcı ve anlaşılmaz olabilir. Matristeki taktik ve tekniklerin kapsamıyla söz konusu alanların doğası uyuşmayabilir. Örneğin, iletişim cihazlarının bozulması veya ele geçirilmesi gibi RF manipülasyon teknikleri, "Komuta ve Kontrol" veya "İlk Erişim" aşamalarında daha önce tanımlanmamış saldırı vektörleri olarak incelenmektedir. Bu tür bir genişletme, özellikle siber tehdit istihbaratıyla ve atak matrisiyle somutlaştırılan kategorilerin yapısını kullanışsız hale getirebilir. Sonuç olarak, hibrit saldırıların karakteristiğini yansıtan RF ve EH tabanlı bileşenlerin, tehdit istihbaratı analizinde ayrı bir odak noktası haline getirilmesi hem siber hem de fiziksel güvenlik mekanizmalarının iyileştirilmesine olanak tanıyacak şekilde ele alınmıştır. Ancak sinyal istihbaratı ile EH veya RF yöntemleri, mevcut atak matrisinin işleyişini sekteye uğratmayacak şekilde kurgulanmıştır.

Önerilen teknik modelin ve iyileştirme stratejilerinin bir diğer önemli kırılganlığı, çağrı cihazı saldırılarında görüldüğü gibi, iyi kurgulanmış ve devlet destekli sofistike istihbarat operasyonlarına karşı tam bir koruma sağlayamama ihtimalidir. Bir devletin, elindeki geniş imkân ve kabiliyetler (insan istihbaratı, teknik istihbarat, diplomatik ve ekonomik araçlar) sayesinde, mevcut savunma mekanizmalarını aşabilecek özgün ve çok katmanlı bir hibrit saldırı operasyonu planlaması her zaman mümkündür. Böyle bir durumda, MITRE ATT&CK matrisine eklenecek yeni teknikler dahi yetersiz kalabilir. Bu, siber güvenliğin ve genel olarak ulusal güvenliğin sadece teknik tedbirlerle sağlanamayacağını, aynı zamanda güçlü bir karşı-istihbarat kapasitesi, stratejik öngörü, uluslararası iş birlikleri ve toplumsal direnç gibi unsurları da gerektirdiğini göstermektedir. Bu bağlamda, güvenlik analizleri, sadece bilinen tehdit vektörlerine değil, aynı zamanda potansiyel "bilinmeyen bilinmeyenlere" karşı da esneklik ve adaptasyon yeteneği geliştirmeye odaklanmalıdır.

Hizbullah'a yönelik çağrı cihazı operasyonu, istihbarat, sabotaj ve düşük yoğunluklu savaş stratejileri açısından önemli bir dönüm noktası olarak değerlendirilmektedir. Bu operasyon, siber çatışma, elektronik harp ve fiziksel savaşın giderek daha fazla iç içe geçtiğini ve modern istihbarat operasyonlarının artık dijital ve fiziksel alanların birleşimini kapsadığını ortaya koymaktadır. Yapay zekâ ve diğer gelişen teknolojilerin bu tür saldırılara açık olduğu düşünüldüğünde, gelecekte daha karmaşık ve sofistike operasyonların gerçekleşmesi olası görünmektedir.[83] Bu durum, teknolojinin yıkıcı potansiyelinin sınırlandırılması meselesini gündeme getirmektedir. Bu sınırlamanın sadece teknik önlemlerle değil, aynı zamanda uluslararası düzeyde kabul görmüş etik normlar, ortak ahlaki kabuller ve uluslararası hukuk çerçeveleri ile mümkün olabileceği düşünülmektedir.[84] Ancak savaşın değişen doğası günümüzde teknolojik yenilikler ve siyasi gelişmeler tarafından şekillenmektedir. Bu durum, hükümetlerin ve bireylerin savaş sırasındaki eylemlerini değerlendirmek için uluslararası hukuk ve haklı savaş doktrini etkisinde kullanılan geleneksel standartlara karmaşık meydan

83 Izabela Marszałek-Kotzur, "Ethical Perspective of the Development and Use of Modern Military Technologies", *Scientific Papers of Silesian University of Technology Organization & Management*, 165, 2022.
84 Luciano Floridi, *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press, 2010.

okumalar sunmaktadır.[85] Esnek yapısından dolayı bir güç dengesizliğinin varlığında hukukun güçlüden yana tavır aldığı bir dünyada,[86] normların ve hukuk kurallarının oluşturulması, benimsenmesi ve etkin bir şekilde uygulanması, devletlerin egemenlik anlayışları, ulusal güvenlik çıkarları ve teknolojik rekabet gibi faktörler nedeniyle karmaşık bir politik süreçtir. Zira bazı ağır suçlarda devletlerin kendi sınırları dışındaki olayları yargılamasına olanak tanıyan, devlet egemenliğini sınırlayan bir yetki olan evrensel yargı yetkisinde dahi, hangi suçların kapsama girdiği ve yargılama yetkisinin nasıl paylaşıldığı uzun sürelerdir tartışılagelen bir konudur.[87]

Cenevre Sözleşmesi, saldırıların yalnızca askerî unsurlara yöneltilmesini, sivil hedefleri ise hariç tutmasını zorunlu kılmaktadır. Ölümcül otonom silahların etik ilkelerle programlanarak savaşta insan müdahalesinin yerini alması ve tutarlı yetenekleri sayesinde, etik savaş yürütmede daha ileri keşifler yapılana dek insan faktörünün çatışmalardan çıkartılması gerektiği belirtilmektedir.[88] Ancak otonom olarak gerçekleştirildiği değerlendirilen çağrı cihazı operasyonu da çağrı cihazlarının savaşçı olmayan kişilere ve olaya karışmamış sivillere, hatta patlamadan hemen önce cihazları yanlışlıkla almış olabilecek çocuklara da dağıtılmış olabileceği, çağrı cihazının patladığı an itibarıyla kimin taşıdığının bilinmediği ve belki de bilinemeyeceği iddia edilerek saldırının hukukiliği yönünde eleştirilere konu olmuştur.[89]

Bu sebeple bu tür tehditlere karşı ulusal güvenlik politikaları için üretilecek stratejik ve politik çıkarımlar hem teknolojik hem de hukuki ve yönetsel değişkenleri içermelidir. Siyaset, politikayı (devletin amaç ve hedeflerini) üretir. Strateji ise bu politikayı, askerî unsurlarla ilişkilendirir ve politikanın arzu edilen hedeflerine ulaşılmasını sağlayacak askerî kuvvetleri ve görevlerini belirler. Operasyonel ve taktik seviyeler ise strateji tarafından belirlenen somut görevleri icra eder.[90] Özellikle uluslararası tehditlerin oluşmasını beklemek tehlike arz eden bir stratejidir.[91] Bu bağlamda yeni tehditler ve güvenlik açıklarının tespiti amacıyla, tehdit algılama mekanizmaları etkin bir şekilde kullanılmalı ve tahkim edilmelidir. Bu kapsamda, ihlal veya saldırı bulma ve yanıt verme ekiplerinin kapasiteleri arttırılarak, proaktif bir güvenlik duruşu sağlanmalıdır. Mevcut cihazların elektromanyetik dayanıklılığını arttıracak modifikasyonların yanı sıra bu direnci barındıran cihazların temini de uygun olmakla birlikte[92] bu tür kritik teknolojileri yerli imkanlarla geliştirmek ve üretmek bir tercih değil, mutlak bir zorunluluk haline gelmiştir.[93]

85 Scott D. Sagan, "Ethics, Technology & War", *Daedalus*, 145:4, 2016, s. 611.

86 Burak Güneş, "Egemenlik ve İnsancıl Müdahale: Çelişkili Bir Kuram Olarak Uluslararası Hukuk", *Güvenlik Bilimleri Dergisi*, 10:1, 2021, s. 31-58.

87 Merve Ş. Akdemir, "Egemenlik ve Evrensel Yargı Yetkisi İlişkisinin Uluslararası Ceza Hukuku Boyutu", *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, 8:2, 2022, s. 261275.

88 Steven Umbrello, Phil Torres ve Angelo F. De Bellis, "The Future of War: Could Lethal Autonomous Weapons Make Conflict More Ethical?", *AI & Society*, 35:1, 2020, s. 273-282.

89 Amichai Cohen ve Yuval Shany, "Well, it Depends: Explosive Pagers Attack Revisited", *Articles of War*, 11 Ekim 2024, https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited/, erişim 24.09.2024; Fabio Massacci, "Exploding Pagers and the Birth of State Cyberterrorism", *IEEE Security & Privacy*, 23:1, 2025, ss. 4-6

90 Murat Caliskan, "Hybrid Warfare and Strategic Theory", *Horizon Insights*, 6, 2019.

91 Cahit Karakuş, "Kritik Alt Yapılara Siber Saldırı", *Yüksek Lisans Tezi*, İstanbul Kültür Üniversitesi, 2013.

92 Shobendra S. Mahat, "Vulnerabilities of the Communication System to an Electromagnetic (EM) Attack, Threat Assessment and Mitigation", *The Shivapuri Journal*, 26:1, 2025, s. 134-144.

93 Halil Ibrahim Sincar ve Bestami Bodruk "Turkish Minister Underscores Need for National Technology after Pager Explosions in Lebanon", *Anadolu Ajansı (AA)*, 18 Eylül 2024, https://www.aa.com.tr/en/turkiye/turkish-minister-underscores-need-for-national-technology-after-pager-explosions-in-lebanon/3334019, erişim 29.05.2025.

Sonuç

Bu çalışma, siber güvenlikte hibrit savaş konseptine yönelik stratejik bir bakış açısı sunarak, elektronik harp ve siber tehditlerin bir arada nasıl ele alınabileceğini analiz etmiştir. Tedarik zinciri saldırılarının karmaşıklığı ve etkileri incelenmiş; MITRE ATT&CK çerçevesine dayalı olarak bu tür saldırıların izlerinin daha kapsamlı bir şekilde tespit edilmesine yönelik bir model yaklaşımı önerilmiştir. Çalışma, tehdit istihbaratının geleneksel sınırlarını genişleterek, RF ve EH tekniklerini kapsayan bir model geliştirmiştir.

Bu çalışma kapsamında önerilen teknik model, yalnızca mevcut saldırıların izlenmesi ve belgelenmesi için değil, aynı zamanda gelecekteki tehditlerin daha iyi öngörülmesi ve önlenmesi için yeni metodolojilerin benimsenmesini teşvik etmektedir. Hibrit tehditlerin doğasına uygun olarak genişletilmiş bir MITRE ATT&CK matrisi, saldırı yüzeylerinin daha detaylı analizine ve daha etkin savunma stratejilerinin oluşturulmasına olanak tanıyacaktır. Sonuç olarak, RF ve EH tabanlı saldırılarla ilgili kategorilerin entegre edilmesi, dijital ve fiziksel güvenlik arasında köprü kurarak daha kapsamlı bir tehdit analizi çerçevesi sunmaktadır. Bu tür yenilikçi yaklaşımlar, siber ve elektronik harp alanındaki güvenlik politikalarının yeniden şekillendirilmesini ve daha proaktif tehdit avcılığı yöntemlerinin geliştirilmesini sağlayacaktır. Gelecekte yapılacak çalışmalar, önerilen modelin pratik uygulamalarını ve gerçek dünya senaryolarında sağlayabileceği etkileri daha detaylı şekilde ele almalıdır.

Çağrı cihazı saldırısı, hibrit tehdit ortamında siber ve kinetik operasyonlar arasındaki sınırların bulanıklaştığını net şekilde ortaya koymuştur. Bu durum, düşük maliyetli analog cihazların bile tedarik zinciri güvenliğini tehdit edebileceğini kanıtlamıştır. Tedarik zincirinin dijital ve fiziksel bileşenlerinin bütünleşik zafiyetleri hem BT hem de OT katmanlarında saldırı yüzeyini genişletmektedir. Sahte cihazlar, donanımsal arka kapılar ve yazılım manipülasyonları, operasyonel güvenliği doğrudan etkileyecek biçimde silahlandırılabilmektedir. Sonuç olarak, hibrit tehditlere karşı güvenlik analizlerinin sadece teknik düzeyde değil, aynı zamanda düzenleyici ve sistemik düzeyde de ele alınması gereklidir. Siber savaş, geleneksel çatışma doktrinlerinin dijitalleştirilmiş bir uzantısı hâline gelmiş; bu nedenle siber tehdit analizleri, fiziksel çatışma bağlamlarıyla entegre edilmelidir.

Yazarların Katkı Oranı

Yazarlar araştırmaya eşit oranda katkıda bulunmuştur.

Çıkar Çatışması

Araştırmanın yazarları olarak herhangi bir çıkar çatışma beyanımız bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Bu çalışmanın hazırlanması sırasında yazarlar, yalnızca metnin okunabilirliğini arttırmak, dil bilgisel hataları düzeltmek ve akışı iyileştirmek amacıyla ChatGPT-4 aracından yararlanmıştır. Bu ve benzeri teknolojiler içerik üretmek, bilimsel çıkarımlar yapmak ve bilimsel önerilerde bulunmak için kullanılmamıştır. Yapay zekâ destekli araçların kullanımı yazarların denetimi ve kontrolü altında gerçekleştirilmiş ve ortaya çıkan metin yazarlar tarafından dikkatlice gözden geçirilip düzenlenmiştir. Yapay zekâ sistemlerinin zaman zaman eksik, hatalı veya ön yargılı içerik üretebileceği göz önünde bulundurularak, çalışmanın tüm içeriğine ve doğruluğuna ilişkin nihai sorumluluk yazarlara aittir.

KAYNAKÇA

Basılı Eserler

AHN Gwanghyun, JANG Jisoo, CHOI Seho ve SHIN Dongkyoo (2024). "Research on Improving Cyber Resilience by Integrating the Zero Trust Security Model with the MITRE ATT&CK Matrix", *IEEE Access*, 12, 89291–89309.

AKDEMİR Merve Ş. (2022). "Egemenlik ve Evrensel Yargı Yetkisi İlişkisinin Uluslararası Ceza Hukuku Boyutu", *Anadolu Üniversitesi Hukuk Fakültesi Dergisi*, 8:2, 261-275.

AL-KHAWAJA Ali ve SADKHAN Sattar B. (2021). "Intelligence and Electronic Warfare: Challenges and Future Trends", *2021 7th International Conference on Contemporary Information Technology and Mathematics (ICCITM)*, IEEE, 118-123.

AL-SADA, Bader, SADIGHIAN, Alireza ve OLIGERI, Gabriele (2023). "Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database", *IEEE Access*, 12, 1217–1234.

APPLEGATE Scott D. (2009). "Social engineering: Hacking the wetware!", *Information Security Journal: A Global Perspective*, 18:1, 40-46.

BACK Tobias B. (2025). "Weaponising 'apparently harmless portable objects': emerging categorisations of trust and risk in post 'pager attacks' Lebanon", *Small Wars & Insurgencies*, 36:6, 1025-1048.

BELLABY Ross W. (2016). "Justifying Cyber-Intelligence?", *Journal of Military Ethics*, 15:4, 299–319.

BORUM Randy, FELKER John, KERN Sean, DENNESEN Kristen ve FEYES Tonya (2015). "Strategic Cyber Intelligence", *Information & Computer Security*, 23:3, 317–332.

BRATKO Artem, ZAHARCHUK Denys ve ZOLKA Valentyn (2021). "Hybrid Warfare–A Threat to the National Security of the State", *Revista de Estudios en Seguridad Internacional*, 7:1, 147–160.

CALISKAN Murat (2019). "Hybrid warfare and strategic theory", *Horizon Insights*, 6.

CHRISTIANSON David L. (2019). "Signals intelligence", Geral W. Hopple ve Bruce W. Watson (ed.), *The Military Intelligence Community*, New York, Routledge, 39-54.

COHEN Amichai ve SHANY Yuval (2024). "Well, it depends: Explosive pagers attack revisited", *Articles of War*, https://lieber.westpoint.edu/well-it-depends-explosive-pagers-attack-revisited/, erişim 24.09.2024.

FLORIDI Luciano (2010). *The Cambridge Handbook of Information and Computer Ethics*, Cambridge University Press.

GHERNOUTI-HÉLIE Solange (2010). "A national strategy for an effective cybersecurity approach and culture", *2010 International Conference on Availability, Reliability and Security*, IEEE, 370-373.

GILL Peter (2012). "Intelligence, Threat, Risk and the Challenge of Oversight", *Intelligence and National Security*, 27:2, 206-222.

GÜNDOĞDU Serkan (2023). "Uluslararası Politikada Bir Etki Aracı Olarak Siber Güvenlik ve Türkiye'nin Siber Güvenlik Politikası Uygulaması: Ulusal Siber Olaylara Müdahale Merkezi (USOM)", *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 33:3, 1325-1337.

GÜNEŞ Burak (2021). "Egemenlik ve İnsancıl Müdahale: Çelişkili Bir Kuram Olarak Uluslararası Hukuk", *Güvenlik Bilimleri Dergisi*, 10:1, 31-58.

HAMMI Badis, ZEADALLY Sherali ve NEBHEN Jamel (2023). "Security threats, countermeasures, and challenges of digital supply chains", *ACM Computing Surveys*, 55:14s, 1-40.

HOFFMAN Frank G. (2007). "Conflict in the 21st century: The rise of hybrid wars", *Arlington: Potomac Institute for Policy Studies.*

JO Yonghyun, CHOI Oongjae, YOU Jiwoon, CHA Youngkyun ve LEE Dong H., (2022). "Cyberattack Models for Ship Equipment Based on the MITRE ATT&CK Framework", *Sensors*, 22:5, 1860.

KANJ BONHARD S., VILLALTA Pau G., ROSES Oriol, PEGUEROLES Josep (2025). "A Review of Tactics, Techniques, and Procedures (TTPs) of MITRE Framework for Business Email Compromise (BEC) Attacks", *IEEE Access*.

KARAKUŞ Cahit (2013). Kritik Alt Yapılara Siber Saldırı, *Yüksek Lisans Tezi*, İstanbul Kültür Üniversitesi.

LASICA Daniel T. (2009). "Strategic implications of hybrid war: A theory of victory", School of Advanced Military Studies, United States Army Command and General Staff College.

LAVAZZA Andrea ve FARINA Mirko (2024). "The Costs and Perils of Weaponizing Consumer Technologies (The 2024 Pager and Walkie-Talkie Explosions in Lebanon and Syria)", *IEEE Technology and Society Magazine*.

LIAROPOULOS Andrew (2011). "War and Ethics in Cyberspace", *Leading Issues in Information Warfare and Security Research*, 1:121.

MAHAT Shobendra S. (2025). "Vulnerabilities of the Communication System to an Electromagnetic (EM) Attack, Threat Assessment and Mitigation", *The Shivapuri Journal*, 26:1, 134-144.

MARSHALL Kimball P. (1999). "Has Technology Introduced New Ethical Problems?", J*ournal of Business Ethics*, 19, 81-90.

MARSZAŁEK-KOTZUR Izabela (2022). "Ethical Perspective of the Development and Use of Modern Military Technologies", *Scientific Papers of Silesian University of Technology, Organization & Management/Zeszyty Naukowe Politechniki Slaskiej, Seria Organizacji i Zarzadzanie*, 165.

MASSACCI Fabio (2025). "Exploding Pagers and the Birth of State Cyberterrorism", *IEEE Security & Privacy*, 23:01, 4-6.

NAIK Nitin, JENKINS Paul, GRACE Paul ve SONG Jingping (2022). "Comparing Attack Models for IT Systems: Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK Framework and Diamond Model", *2022 IEEE International Symposium on Systems Engineering (ISSE)*, IEEE, 1–7.

NYE Joseph S. (2010). *Cyber Power*, Cambridge: Harvard Kennedy School, Belfer Center for Science and International Affairs.

PEFFERS Ken, TUUNANEN Tuure, ROTHENBERGER Marcus A. ve CHATTERJEE Samir (2007). "A Design Science Research Methodology for Information Systems Research", *Journal of Management Information Systems*, 24:3, 45–77.

PELL Robert, MOSCHOYIANNIS Sotiris, PANAOUSIS Emmanouil ve HEARTFIELD Ryan (2021). "Towards Dynamic Threat Modelling in 5G Core Networks Based on MITRE ATT&CK", arXiv preprint arXiv:2108.11206, https://arxiv.org/abs/2108.11206.

REICHBORN-KJENNERUD Erik ve CULLEN Patrick (2022). "What is hybrid warfare?", *Norwegian Institute for International Affairs (NUPI).*

RID Thomas (2013). "Cyberwar and peace: Hacking can reduce real-world violence", *Foreign Affairs*, 92:6, 77-87.

SAGAN Scott D. (2016). "Ethics, technology & war", *Daedalus*, 145:4, 6-11.

SARKER Pantha Protim, DAS Upoma, VARSHNEY Nitin, SHI Shang, KULKARNI Akshay, FARAHMANDI Farimah ve TEHRANIPOOR Mark (2025). "When Everyday Devices Become Weapons: A Closer Look at the Pager and Walkie-talkie Attacks", arXiv preprint arXiv:2501.17405.

SCHLEHER D. Curtis (1999). *Electronic Warfare in the Information Age*, Norwood, MA: Artech House, Inc., 1999.

SCOTT Len (2019). "Secret Intelligence, Covert Action and Clandestine Diplomacy", Christopher Andrew, Richard J. Aldrich ve Wesley K. Wark (ed.), *Secret Intelligence*, London, Routledge, 526–544.

SHENG Chuan, MA Wanlun, HAN Qing-Long, ZHOU Wei, ZHU Xiaogang ve WEN Sheng (2024). "Pager Explosion: Cybersecurity Insights and Afterthoughts", I*EEE/CAA Journal of Automatica Sinica*, 11:12, 2359-2362.

SKRODELIS Heinrihs K. ve ROMANOVS Andrejs (2021). "Cyber-Physical Risk Security Framework Development in Digital Supply Chains", *62nd International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS)*, IEEE, 1–5.

STROM Blake E., APPLEBAUM Andy, MILLER Doug P., NICKELS Kathryn C., PENNINGTON Adam G. ve THOMAS Cody B. (2018). "MITRE ATT&CK: Design and Philosophy", *Technical Report*, McLean, VA: The MITRE Corporation.

SUN Nan, DING Ming, JIANG Jiaojiao, XU Weikang, MO Xiaxing, TAI Yonghang ve ZHANG Jun (2023). "Cyber Threat Intelligence Mining for Proactive Cybersecurity Defense: A Survey and New Perspectives", *IEEE Communications Surveys & Tutorials*, 25:3, 1748-1774.

SVETOKA Sanda (2016). "Social media as a tool of hybrid warfare", *NATO Strategic Communications Centre of Excellence.*

UMBRELLO Steven, TORRES Phil ve DE BELLIS Angelo F. (2020). "The future of war: Could lethal autonomous weapons make conflict more ethical?", *Ai & Society*, 35:1, 273-282.

URBINI Ignacio M. G., VENOSA Paula, BAZÂN Patricia ve DEL RIO Nicolâs (2022). "Distributed Cybersecurity Strategy, applying the Intelligence Operations Theory", *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, IEEE, 1-6.

WARNER Michael (2019). "A matter of trust: Covert action reconsidered", *Studies in Intelligence*, 63:4, 33–41.

İnternet Kaynakları

ARSLAN İkbal Muhammet (2024). "BM: Lübnan ve Suriye'de Eş Zamanlı Çağrı Cihazı Patlamaları Şok Edici", *Anadolu Ajansı (AA)*, https://www.aa.com.tr/tr/dunya/bm-lubnan-ve-suriyede-es-zamanli-cagri-cihazi-patlamalari-sok-edici/3333807, erişim 07.01.2025.

BIÇAKÇI Salih (2024). "Lübnan'da Patlayan Çağrı Cihazları: Elektronik Harp, Siber Sabotaj ve Kötülüğün Sıradanlığı", *Fikir Turu*, https://fikirturu.com/jeo-politika/lubnanda-patlayan-cagri-cihazlari/, erişim 24.09.2024.

Ekonomi ve Dış Politika Araştırma Merkezi (2016). "Nükleer Tesislerin Siber Güvenliğine Giriş", *EDAM*, https://edam.org.tr/siber-politikalar-ve-dijital-demokrasi/nukleer-tesislerin-siber-guvenligine-giris, erişim 01.02.2025.

GEBEILY Maya, PEARSON James ve GAUTHIER-VILLARS David (2025). "How Israel's bulky pager fooled Hezbollah", *Reuters*, https://www.reuters.com/graphics/ISRAEL-PALESTINIANS/HEZBOLLAH-PAGERS/mopawkkwjpa/, erişim 17.10.2024.

IEEE Spectrum (2024). "The Real Story of Stuxnet", https://spectrum.ieee.org/the-real-story-of-stuxnet, erişim 01.02.2025.

ISB Staff Reporter (2024). "Hezbollah Pager Attack: A Wake-up Call to Tech Manufacturers to Secure their Supply Chains?", *Information Security Buzz*, https://informationsecuritybuzz.com/hezbollah-pager-attack-a-wake-up-call/, erişim 20.10.2024.

LACY Mark (2024). "Lebanon Pager Attacks: The Weaponisation of Everything has Begun", *The Conversation*, https://theconversation.com/lebanon-pager-attacks-the-weaponisation-of-everything-has-begun-239423, erişim 23.10.2024.

LIMA Marcelo (2024). "Israeli Pager Attack: Cybersecurity Lessons", *LinkedIn*, https://www.linkedin.com/pulse/israeli-pager-attack-cybersecurity-lessons-security-marcelo-kcjxf, erişim 21.10.2024.

LINKEDIN,https://www.linkedin.com/search/results/all/?keywords=%23pagerexplosion&origin=HASH_TAG_FROM_FEED&sid=Q3u, erişim 20.09.2024.

MEDIUM, https://medium.com/search?q=%23pagerexplosion, erişim 20.09.2024.

MITRE, "MITRE ATT&CK Groups", https://attack.mitre.org/groups/, erişim 5.01.2025.

MITRE, "MITRE Enterprise Matrix", https://attack.mitre.org/matrices/enterprise/, erişim 20.01.2025.

MITRE, "T0862: Remote Access Software", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T0862/, erişim 21.01.2025.

MITRE, "MITRE ATT&CK Tactics", https://attack.mitre.org/tactics/, erişim 22.01.2025.

MITRE, "T1583: Acquire Infrastructure", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T1583/, erişim 22.01.2025.

MITRE, "T1199: Trusted Relationship", *MITRE ATT&CK*, https://attack.mitre.org/techniques/T1199/, erişim 23.01.2025.

NIST, "Tactics, Techniques, and Procedures", *National Institute of Standards and Technology*, https://csrc.nist.gov/glossary/term/tactics_techniques_and_procedures, erişim 22.04.2025.

PARIENTE Nissim (2024). "The Machine Identity Attack Surface – MITRE ATT&CK Framework Redefined", *Token Security*, https://www.token.security/blog/the-machine-identity-attack-surface---mitre-attack-framework-redefined, erişim 20.01.2025.

PICUS Security (2024). "What is Advanced Persistent Threat (APT)?", *Picus Security*, https://www.picussecurity.com/resource/glossary/what-is-advanced-persistent-threat-apt, erişim 05.05. 2025.

PYTLAK Allison, SIEBENS Siebens ve LAD Shreya (2024). "Old Tactics, New Targets: Unraveling Lebanon's Pager Attacks", *Stimson Center*, https://www.stimson.org/2024/old-tactics-new-targets, erişim 24.10.2024.

RAMAKRISHNA Sudhakar (2021). "New Findings from Our Investigation of SUNBURST", *SolarWinds Blog*, https://www.solarwinds.com/blog/new-findings-from-our-investigation-of-sunburst, erişim 06.05.2025.

REDDIT (2024). "Israel planted explosives in 5,000 Hezbollah pagers, say sources", https://www.reddit.com/r/geopolitics/comments/1fjnx3y/israel_planted_explosives_in_5000_hezbollah/, erişim 19.09.2024.

SEREN Merve (2024). "İsrail'in Yeni İstihbarat Operasyonu: Pager ve Walkie-Talkie saldırıları", *Fikir Turu*, https://fikirturu.com/jeo-politika/israilin-yeni-istihbarat-operasyonu/, erişim 25.09.2024.

SİNCAR Halil İbrahim, BODRUK Bestami (2024). "Turkish Minister Underscores Need for National Technology after Pager Explosions in Lebanon", *Anadolu Ajansı (AA)*, https://www.aa.com.tr/en/turkiye/turkish-minister-underscores-need-for-national-technology-after-pager-explosions-in-lebanon/3334019, erişim 29.05.2025.

SINGH Inder (2024). "New Paradigm in Cyber Warfare: Strategic Pager Attack on Hezbollah", *Medium*, https://inderbarara.medium.com/new-paradigm-in-cyber-warfare-strategic-pager-attack-on-hezbollah-d100247bd9ec, erişim 22.10.2024.

STAHL Lesley (2025) " Israel's spy agency, Mossad, spent years orchestrating Hezbollah walkie-talkie, pager plots", *CBS News*, https://www.cbsnews.com/news/israeli-mossad-pager-walkie-talkie-hezbollah-plot-60-minutes/, erişim 06.01.2025.

STAHL Lesley (2025). "Former Mossad Agents Detail Explosive Pagers, Hezbollah Terrorists Plot – 60 Minutes Transcript", *CBS News*, https://www.cbsnews.com/news/israel-former-mossad-agents-detail-explosive-pagers-hezbollah-terrorists-plot-60-minutes-transcript/, erişim 09.06.2025.

TWITTER (X). https://x.com/hashtag/pagerexplosions?src=hashtag_click, erişim 19.09.2024.

EKLER:

1. Genişletilmiş MITRE Matrisi:

GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 449-478
DOI: 10.17752/guvenlikstrtj.1708377

Derleme Makale
Review Article

Siber Güvenlik Kanunu'nun İletişim ve Yeni Medya Faaliyetleri Bağlamında Değerlendirmesi

Assessment of the Cybersecurity Law in the Context of Communication and New Media Activities

Mevlüt ALTINTOP*

* Doktora Öğrencisi, Erciyes Üniversitesi, Sosyal Bilimler Enstitüsü, Gazetecilik Ana Bilim Dalı, Kayseri, Türkiye, e-posta: mevlutaltintop@hotmail.com, ORCID: 0000-0002-1731-9064

Geliş Tarihi / Submitted: 28.05.2025

Kabul Tarihi / Accepted: 03.11.2025

Öz

Yirmi birinci yüzyıl itibariyle büyük bir ivme yakalayan internet ve bilişim teknolojileri hayatın her alanını domine etmektedir. Sürecin ortaya çıkardığı dijitalleşme siyasi ve ekonomik işleyiş kadar iletişim süreçleri ve medya faaliyetleri ile gündelik hayat pratiklerinde de köklü değişimlere yol açmıştır. Bu değişimler yeni suç biçimlerinin ortaya çıkmasına ve güvenlik sorunlarına neden olmuştur. Devletler yasal düzenlemeler yoluyla bir yandan dijitalleşmenin neden olduğu bu suçları engellemeye çalışırken, diğer yandan da ortaya çıkan ihlal ve güvenlik sorunlarını aşmayı amaçlamaktadır. Sürecin en önemli parçalarından birisi internet ve bilişim teknolojileriyle desteklenen iletişim süreçleri ve yeni medya faaliyetleridir. Bu bağlama odaklanan çalışma, 12.03.2025 kabul tarihli ve 7545 numarasıyla 19.03.2025 tarihinde Resmî Gazete'de yayımlanan Siber Güvenlik Kanunu'nun iletişim ve medyayla ilgili bölümlerini Habermas'ın "Kamusal Alan" kavramsallaştırması ekseninde ele almaktadır. Yapılan analizlerde, Siber Güvenlik Kanunu'nun anayasal açıdan tanımlanmış ve güvence altına alınmış olan iletişim ve haberleşme özgürlüklerini kısıtlama, medya faaliyetlerini sınırlama getirme, yeterince şeffaf ve uyumlu olmaması nedeniyle keyfi uygulamalara yol açma gibi kamusal ve özel alana yönelik riskler taşıdığı sonucuna ulaşılmıştır.

Anahtar Kelimeler: Siber Güvenlik Kanunu, İletişim, Yeni Medya, Sosyal Medya, Sanal Dünya

Abstract

By the twenty-first century, the internet and information technologies, which have gained great momentum, dominate every aspect of life. The digitalization produced by this process has brought profound changes not only to political and economic operations but also to communication processes, media activities, and everyday practices. These changes have given rise to new forms of crime and security problems. States are attempting, through legal regulations, to prevent crimes caused by digitalization and to address security issues. One of the most important components of this process is the communication and new media activities supported by the internet and information technologies. This study examines the sections of the Cybersecurity Law related to communication and media within the framework of Habermas's conceptualization of the "public sphere"; the law was adopted on 12 March 2025 (Law No. 7545) and published in the Official Gazette of the Republic of Türkiye on 19 March 2025. The assessment concludes that the Cybersecurity Law poses risks of restricting constitutionally defined freedoms of communication and correspondence, imposing limitations on media activities, and–due to insufficient transparency and lack of coherence–leading to arbitrary application.

Keywords: Cybersecurity Law, Communication, New Media, Social Media, Virtual World

Extended Summary

This study critically evaluates the implications of Türkiye's Cybersecurity Law (Law No. 7545), enacted on March 19, 2025, by focusing on its impact on communication freedoms, media activities, and constitutional rights. The analysis emphasizes the tension between national security objectives and the protection of fundamental liberties in the digital age. The research employs a multidisciplinary approach, combining legal, sociological, and communication theories to assess the law's compliance with democratic principles and international human rights standards. The rapid digitalization of the 21st century has transformed political, economic, and social dynamics and has introduced new forms of crime and security challenges. States respond through legal frameworks like Türkiye's Cybersecurity Law, which aims to counter cyber threats but risks undermining constitutional rights. This study examines the law's provisions related to communication and media and argues that its vague language and broad enforcement powers threaten transparency, press freedom, and privacy.

The literature on cybersecurity is divided into technical studies, such as infrastructure security, and social science-oriented research, which addresses societal impacts. While technical studies dominate literature, few of them address the intersection of cybersecurity with communication and media. Key findings from prior work include the emphasis of international organizations like the North Atlantic Treaty Organization (NATO) and the European Union (EU) on transparency and human rights in cybersecurity policies and Türkiye's historically lagging legal infrastructure, exemplified by the 1991 "Crimes in the Field of Informatics", and low cybersecurity literacy among citizens, as shown in studies on university students. This study identifies a gap in research linking cybersecurity laws to communication freedoms and positions itself to fill this void.

Cybersecurity is defined as practices protecting digital systems, data, and infrastructure from threats, extending to societal and international dimensions. The term "cyber" originates from "cybernetics", reflecting control systems in digital environments. Cybercrime encompasses activities like hacking, data theft, and online harassment, requiring adaptive legal responses. The study highlights how communication has evolved beyond interpersonal exchanges to include systemic data transfers, network security, and digital infrastructure. This shift makes communication a critical component of national security strategies, as seen in Türkiye's Cybersecurity Law.

The law's provisions are analyzed in light of Türkiye's Constitution and international treaties such as the European Convention on Human Rights (ECHR) and International Covenant on Civil and Political Rights (ICCPR). Key findings include restrictions on fundamental rights, such as Article 13 of the law limiting freedom of expression by prohibiting media from disclosing information obtained by the Cybersecurity Presidency, and Article 6 granting authorities unchecked access to "log records", risking mass surveillance. Article 12 imposes broad media bans, contradicting democratic norms of proportionality and necessity. Ambiguities in the law, such as data retention policies lacking independent oversight and international data sharing without clear safeguards, raise concerns about misuse. Remote intervention powers in Article 6(1c) permit authorities to access communication infrastructure, threatening systemic transparency. The law diverges from EU and NATO guidelines, which prioritize human rights and judicial oversight, as seen in the absence of the ECHR's "necessary in a democratic society" criterion in Türkiye's implementation.

The study critiques the law's failure to balance security and freedom. Surveillance overreach through log collection and data centralization echoes Baudrillard's critique of virtual worlds replicating real-world power imbalances. Broad media bans and vague definitions of "cyber threats" may stifle dissent and undermine democratic discourse. Bureaucratic inertia in updating laws exacerbates rights violations, as seen in delayed responses to cybercrimes. To mitigate risks, this study proposes strengthening proportionality by aligning restrictions with constitutional principles, enhancing transparency through independent audits, adopting international norms like EU frameworks, and promoting digital literacy through public campaigns.

While the Cybersecurity Law addresses critical gaps in Türkiye's cyber defense, its ambiguous provisions and lack of safeguards endanger constitutional rights. This study underscores the need for reforms to reconcile security imperatives with democratic freedoms, urging policymakers to prioritize transparency, accountability, and international cooperation. Future research should explore the law's societal impact through qualitative studies and assess emerging technologies like Artificial Intelligence (AI) in cybersecurity frameworks.

Giriş

Yirmi birinci yüzyılla birlikte internet ve bilişim teknolojilerinin toplumsal yaşamdaki yaygınlığı keskin bir biçimde artarak siyasal, ekonomik, sosyal ve kültürel pratiklerinin yeniden düzenlenmesine yol açmıştır. Bu teknolojik dönüşüm, bilgi üretimi ve dağıtımının ötesinde kamusal tartışmanın biçimini, iletişim süreçlerini, medya faaliyetlerini ve bireylerin gündelik yaşam pratikleri de dönüştürmüştür. Değişim ve dönüşümün hayata birçok olumlu yansıması olmuştur fakat beraberinde olumsuz durumlar ve sorunlar getirmiştir. Bu bağlamda, örneğin, dijitalleşme yeni suç tipleri ve sistemik güvenlik riskleri doğurmuştur. Bu durum ise devletleri teknik tedbirler almanın yanında geniş ve kapsamlı yasal düzenlemeler yapmaya zorlamıştır. Onlardan biri olan ve bu çalışmanın odaklandığı 7545 sayılı Siber Güvenlik Kanunu[1], 12 Mart 2025'te kabul edilmiş ve 19 Mart 2025 tarihli Resmî Gazete'de yayımlanarak yürürlüğe girmiştir.

Çalışmanın temel amacı, Siber Güvenlik Kanunu'nun iletişim süreçleri ve yeni medya faaliyetleri üzerindeki doğrudan ve dolaylı etkilerini Jurgen Habermas'ın "Kamusal Alan" kavramı çerçevesinde analiz etmektir. Habermasçı perspektif, kamusal alanı rasyonel-kritik tartışmanın mekânı ve demokratik meşruiyetin nesnesi olarak ele almaktadır. Dolayısıyla ifade serbestliği, bilgiye erişim ve medya özerkliği gibi ölçütler, bu değerlendirme için normatif bir çerçeve sunmaktadır. Derleme makalesi olarak hazırlanan çalışma, metodolojik açıdan kanun metni ve ilgili düzenleyici belgelerin doküman incelemesine dayanmaktadır. Bu bağlamda "Kanun" hükümlerinin anayasal haklar, uluslararası sözleşmelerin dikkat çektiği insan hakları standartları ve uygulama mekanizmalarıyla ilişkisinin eleştirel bir yorumunu sunmaktadır.

İki blok üzerinde yapılan analizin ilkinde, Kanun'un ifade ve haberleşme özgürlükleri bakımından taşıdığı sınırlama riskleri, şeffaflık ve hesap verebilirlik ekseninde Anayasal hak ve özgürlükler ile uluslararası sözleşmeler bağlamında ele alınmaktadır. İkincisinde ise, Kanun'un teknik hükümlerde öngördüğü veri toplama, iletişim izleme ve müdahale yetkilerinin medya kuruluşlarının haber alma, haber üretme ve yayımlama süreçleri üzerinde baskı oluşturma potansiyeli tartışılmaktadır. Bir başka ifadeyle, her iki sürecin kamusal alan açısından ne anlama geldiği çözümlenmeye çalışılmıştır.

1 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*, Kanun No. 7545, 12 Mart 2025, https://resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm, erişim 13.05.2025.

Son olarak çalışma, Habermasçı normlar ile uyumlu olacak şekilde denetim mekanizmalarının güçlendirilmesi, orantılılık ilkesi ile teknik önlemlerin sınırlandırılması ve şeffaflık yükümlülüklerinin netleştirilmesi yönünde politika önerileri üretmeyi hedeflemektedir. Bu yaklaşım, hem hukuki meşruiyeti hem de kamusal tartışmanın demokratik niteliğini korumaya dönük bir normatif çerçeve sunarak, siber güvenlik konusunda iletişim süreçleri ve medya faaliyetleri bağlamında literatüre katkı sunmayı amaçlamaktadır.

1. Çalışmanın Amacı, Önemi ve Yöntemi

Çalışmanın amacını genel ve özel olarak iki aşamada açıklamak mümkündür. Çalışmanın genel amacı, günümüz dünyasının önemli unsurlarından olan siber ve siber güvenlik kavramlarına dikkat çekerek bu kavramlarının anlaşılmasına katkı sağlamak ve bu alandaki farkındalığı artırmaktır. Özel amacı ise, siber ve siber güvenlik kavramlarından yola çıkılarak oluşturulan yasal düzenlemenin bireysel, toplumsal ve kurumsal boyutlarının iletişim ve medya açısından anlamsal karşılığını bulmaya çalışmaktır.

Çalışmanın önemi, dijitalleşmenin büyük bir hızla artışının birey, toplum, kurum ve devletler açısından ortaya çıkardığı hayati sorunlardan kaynaklanmaktadır. İnternet ve bilişim teknolojileri aracılığıyla gerçekleştirilen zararlı faaliyetler, kişisel verilerin çalınması, finansal kayıplar ve hem ulusal hem de uluslararası güvenlik tehditleri (terör, casusluk vb.) açısından ciddi sonuçlara yol açabilmektedir. Sorun ve tehditleri bertaraf etmek için oluşturulan siber güvenlik önlemlerini almak, dijital ve ekonomik varlıkların korunması açısından kritik bir zorunluluktur. Bu çerçeve çalışmanın önemini de ifade etmektedir.

Derleme makalesi türünde yapılan bu çalışmada yöntem olarak doküman incelemesi kullanılmıştır. Bu bağlamda kitap, makale, kurum raporları, kanun maddeleri ve ilgili web sitelerinden faydalanılmıştır. Elde edilen inceleme sonuçları kapsamında, 12.03.2025 tarihinde kabul edilen ve 7545 numarasıyla 19.03.2025 Resmî Gazete'de yayımlanan Siber Güvenlik Kanunu'nun iletişim ve (yeni) medya ile ilgili kısımları analiz edilerek konunun kapsamlı ve karşılaştırmalı şekilde ele alınması sağlanmıştır. Değerlendirmede konuyla ilgili birçok kuramsal yaklaşıma değinilmiştir fakat çalışmanın ana izleğini Habermas'ın "Kamusal Alan" kavramsallaştırması oluşturmaktadır.

2. Literatür Taraması ve Kavramsal Çerçeve

Literatüre bakıldığında son yıllarda siber güvenlik ile ilgili çok faza çalışma yapıldığı ve bu çalışmalarda konunun genel olarak iki kategoride ele alındığı görülmektedir. İlki, siber ve/veya siber güvenlik konusunun donanım ve yazılım boyutunun değerlendirildiği teknik/teknoloji içerikli çalışmalardır. Bilişim teknolojilerine yönelik detayların yer aldığı bu çalışmalar siber teknolojilerinin mühendislik faaliyetleriyle ilgilidir. İkincisi ise, bu çalışmanın da dâhil olduğu, siber güvenlik konusunun kamusal ve toplumsal yansımalarına ele alan sosyal bilim ağırlıklı çalışmalardır. Bu çalışmalarda, siber teknolojilerin ulusal ve uluslararası olmak üzere iki kategoride çözülmesi gereken sorunlara yol açan gelişmeler olarak değerlendirildiği görülmektedir. Başka bir deyişle, siber teknolojilerinin yol açtığı siber güvenlik meselesi hem saldırı ve savunma, hem de asayiş sorunları olarak karşımıza çıkmaktadır. Öte yandan günümüz dünyasında teknik disiplinler ve teknolojik gelişmeler ideolojik bir form verilerek "sosyal mühendislik" faaliyetlerinde kullanılmaktadır.[2] Bu bağlamda, yukarıda değinilen ilk kategorinin de dolaylı olarak sosyal bilim alanıyla ilişkilendirilmesi mümkündür. Dolayısıyla siber teknolojilerin ulusal ve uluslararası alandaki etkisi ve bu etkinin toplumsal yansımasının bu yönü ayrıca dikkate alınmalıdır.

2 Nilüfer Göle, *Mühendisler ve İdeoloji* (Çev. Eli Levi), İletişim Yayınları, İstanbul, 1986, s. 13.

Konunun saldırı ve savunma bağlamı ülkelerin istihbarat ve askeri birimleri, silah sanayisi, enerji kaynakları ve ekonomik varlıklarına yönelik siber ortamda yapılan müdahaleleri konu edinmektedir. Bu alana dair yapılan çalışmalar ise genel olarak üç başlıkta toplanmaktadır. İlki, uluslararası bir sorun olarak siber güvenlik, ikincisi ulusal bir sorun olarak siber güvenlik ve üçüncüsü siber güvenliğe yönelik faaliyetlerin kamusal ve sosyal açılardan niteliğidir. Aşağıda bu üç başlığa dair örnekler verilerek çalışmanın ana izleği olan Siber Güvenlik Kanunu'nun iletişim süreçleri ve medya faaliyetleri açısından analizi yapılmıştır. Analizin temel argümantasyonunu Jurgen Habermas'ın "Kamusal Alan" kavramlaştırması oluşturmaktadır.

Tarihsel açıdan siber güvenlikte dönüm noktalarından biri, ABD'nin 1969'da ARPANET'i kullanmaya başlamasıdır. Başlangıçta askeri amaçlı olan bu sistem, veri paylaşımı ve iş birliği sağlayan bir dijital ortam olarak gelişerek günümüz internetinin temelini oluşturmuştur. Ancak internetin yaygınlaşmasıyla veri güvenliği riski de artmıştır.[3] Bilişim teknolojilerinin temel işlevleri (bilgiyi kaydetme, depolama, erişim sağlama ve işleme vb.) ihlal edildiğinde siber güvenlik sorunu ortaya çıkmaktadır.[4]

Siber dünya da tıpkı gerçek dünyada olduğu gibi hayatın olumlu ve olumsuz yönlerini yansıtmaktadır. Gerçek dünyada suç kelimesi en basit şekliyle, yetkili otoritenin belirlediği sınırların aşılması olarak tanımlanırken[5], siber dünyada ise bu durum "siber suç" olarak kavramsallaştırılmıştır.[6] Bununla birlikte, siber suçların kapsamı teknolojinin gelişimine paralel olarak genişlemektedir.[7] Bilişim teknolojilerinin mekân ve zaman kısıtlarını ortadan kaldırması, faaliyetlerin ulusal sınırları aşarak uluslararası boyut kazanmasına yol açmaktadır. Bu çerçevede, küresel normlar ve diplomatik yöntemler geliştirme çabaları gündeme gelmiştir.[8] Birleşmiş Milletler (BM), Avrupa Birliği (AB) ve Kuzey Atlantik Antlaşması Örgütü (NATO) gibi kuruluşlar da uluslararası sözleşmelerle bu alana müdahil olmaktadır.[9] Tüm bunlar siber güvenlik konusunu ulusal ve uluslararası bir boyuta taşımaktadır.

Batı'da 1990'larla birlikte toplumda karşılık bulan internetin Türkiye'de yaygınlaşması 2000'li yıllara denk gelmiştir.[10] Gecikmeye rağmen, Türkiye'de pek alışılmamış şekilde, bu alandaki yasal düzenlemeye dair faaliyetlerin daha önce başladığı görülmektedir. Örneğin 1991 yılında "Bilişim Alanında Suçlar"[11] başlıklı ilk yasal düzenleme yapılmış,[12] ancak

3 H. Alpay Karasoy ve Pelin Babaoğlu, "Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı", *Yasama Dergisi,* 44, 2021, s. 131.

4 Enes Çınar, *"Bilişim Suçları"*, Çınar Hukuk Bürosu, 2025, s. 2, https://www.cinarhukukburosu.com/blog/bilisim-suclari, erişim 11.05.2025.

5 Türk Dil Derneği, Türkçe Sözlük, Türk Dil Derneği, Ankara, 2012, s. 1576.

6 Çınar, "Bilişim Suçları", s. 20.

7 Zeynep Ata, "Sosyal Medyada Suç Korkusunun Oluşması ve Yayılması: X Örneği", *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 37, 2024, s. 395.

8 Tuba Eldem, "Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik", *İstanbul Hukuk Mecmuası*, 79:1, 2021, s. 349.

9 Sena Nezgitli ve Recep Benzer, "Avrupa Birliği Siber Güvenlik Kanunu", *Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi,* 2:1, 2020, s. 10.; Gülşah Özdemir, "Uluslararası Güvenlikte Siber Tehditlerin Yükselişi ve Stratejik Savunma Politikaları", *Elektronik Sosyal Bilimler Dergisi*, 24:1, 2025, s. 2-3.

10 Mevlüt Altıntop, *Zygmunt Bauman Sosyolojisinde İletişim Olgusu*, Kitapyurdu Doğrudan Yayıncılık, İstanbul, 2021, s. 76.

11 "Mülga 1926 tarih 657 sayılı Türk Ceza Kanunun Yürürlükten Kaldırılmış Hükümleri": Türk Ceza Kanunun Yürürlükten Kaldırılmış Hükümleri, 767 Mülga 765 sayılı Türk Ceza Kanunu On Birinci Bab Bilişim Suçları §§ 106-122, 1991, https://mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf, erişim 15.05.2025. Onbirinci Bap'ın dipnotunda şu ifadeler yer almaktadır: "Bu bap ve başlık, 6/6/1991 tarih ve 3756 sayılı Kanunun 20'nci maddesiyle metne eklenmiştir" "Mülga" kelimesinin sözlükteki karşılığı "kaldırılmış" şeklindedir. Türk Dil Derneği, *Türkçe Sözlük*, s. 1248.

12 Salih Bıçakçı, Doruk Ergun ve Mitat Çelikpala, *Türkiye'de Siber Güvenlik*, EDAM Siber Politika Kağıtları Serisi 2015/1, Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM), 25 Aralık 2015, s. 4, https://edam.org.tr/wp-content/uploads/2015/12/EDAM_TR_Siber_Guv_1.pdf, erişim 16.05.2025.

sonraki yıllarda mevzuat yetersiz kalmakla birlikte geçerli şekilde güncellenememiştir.[13] Bu konuda son yıllarda önemli ilerlemeler sağlansa da kaynak, eğitim ve şeffaflık gibi unsurlarda eksiklikler devam etmektedir.[14] 2003'ten bu yana sekiz eylem planı hazırlanmış[15] ve alanla ilgili kamusal kurumlar oluşturulmuştur.[16] Ancak teknolojiye hızla uyum sağlayan toplum karşısında, siyasi ve bürokratik yapıların geriden gelmesi, yasal boşlukların siber suçlular tarafından istismar edilmesine yol açmaktadır.[17]

Siber güvenlik konusunun iletişim süreçleri ve medya faaliyetleri boyutu literatürde sınırlı yer bulmaktadır. Mevcut çalışmalar genellikle teknik altyapıya odaklanmakta[18] ya da siber güvenlik konusundaki toplumsal farkındalığı ölçmektedir. Örneğin bu konuda yapılan az sayıdaki çalışmanın birinde iletişim fakültesi öğrencilerinin siber güvenlik ile ilgili farkındalık düzeyinin düşük olduğu saptanmıştır.[19] Bir başka ifadeyle, siber güvenlik ile ilgili yasal düzenlemelerin iletişim süreçleri ve medya faaliyetleri açısından anayasal düzlemle ele alan araştırmalar -yasal düzenlemelerle doğru orantılı olarak- son derece azdır. Çalışma bu bağlamda literatüre önemli bir katkı sunmayı amaçlamaktadır. Aşağıda öncelikle Habermas'ın Kamusal Alan yaklaşımı açıklanmış, ardından siber ve siber güvenlik literatürüne değinilmiş ve son olarak da yasal zemin açısından öncesi ve sonrasıyla Siber Güvenlik Kanunu değerlendirilmiştir.

2.1. Habermas'ın Kamusal Alan Yaklaşımı

Jürgen Habermas'ın kamusal alan kavramsallaştırması, modern demokratik toplumların iletişimsel yapısını anlamak açısından temel bir kuramsal çerçeve sunmaktadır. Habermas, ideal kamusal alanı, bireylerin kamusal meseleleri tartışmak, fikir alışverişinde bulunmak ve politik irade oluşturmak amacıyla bir araya geldikleri, devlet ve sermaye baskılarından görece bağımsız bir sosyal alan olarak tanımlamaktadır.[20] Bu alan, özellikle on sekizinci yüzyıl Avrupa'sında kafe, salon ve basın aracılığıyla gelişerek rasyonel-eleştirel tartışmaların demokratik meşruiyetin oluşumunda merkezi rol oynamasını sağlamıştır. Habermas'a göre, kamusal alanın ideal formu, katılımcıların eşitlik temelinde bir araya geldiği ve iletişimin güç ilişkilerinden arındığı bir ortamı gerektirmektedir.[21]

Habermas yirminci yüzyılda kamusal alanın yapısal dönüşüme uğradığını ileri sürmektedir. Yüzyılın ortalarında etkisi artıran kitle iletişim araçlarının zamanla daha fazla ticarileşmesi, kamusal söylemin giderek piyasa mantığı ve devlet propagandası tarafından şekillendirilmesine neden olarak rasyonel-eleştirel tartışma kültürünü zayıflatmıştır.[22] Bu durum, kamusal alanın demokratik işlevlerini yerine getirme kapasitesini azaltmakta ve

13 Hüseyin Çakır ve Murat Taşer, "Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi", *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji,* 11:2, 2023, s. 363.
14 Arzu Yıldırım, "Türkiye'nin Siber Güvenlik Politikasının Eylem Planları üzerinden Analizi", *Organizasyon ve Yönetim Bilimleri Dergisi,* 16:1, 2024, s. 23.
15 Karasoy ve Babaoğlu, *"Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı"*, s. 138.; Yıldırım, *"Türkiye'nin Siber Güvenlik Politikasının Eylem Planları üzerinden Analizi"*, s. 42.
16 Ali Burak Darıcılı, "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler", *TESAM Akademi Dergisi*, 6:2, 2019, s. 27-29.
17 Özen Akçakanat vd., "İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi", *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi*, 5:2, 2021, s. 267.
18 Muhammed Zekeriya Gündüz ve Resul Daş, "Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik", *Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 10:2, 2020, s. 971.
19 Mustafa Aksoğan vd., "İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği", *Kesit Akademi Dergisi*, 13, 2018, s. 285.
20 Jurgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Çev. Thomas Burger ve Frederick Lawrence), MIT Press, Cambridge, 1991.
21 Age, s. 56.
22 Age, s. 142.

yurttaşların politik katılımını pasifleştirmektedir. Habermas'ın teorisi, günümüzde dijital medya ortamlarının demokratik potansiyelini ve tehditlerini analiz etmek için de önemli bir referans noktası olarak kullanılmaktadır. Zira sosyal medya platformları hem yeni kamusal alan olanakları ortaya çıkarmakta, hem de popülizm, radikalizm, dezenformasyon, manipülasyon, propaganda ve kutuplaşma gibi kamusal alanın fayda eğilimi ortadan kaldırma risklerini beraberinde getirmektedir.[23] Buradaki en önemli detay, siber uzayın teoride sahip olduğu özgürlük ve demokratik katılım özelliği, Antik Yunan'daki kamusal alan olan agoranın postmodern versiyonu olarak değerlendirilmesidir. Bir başka ifadeyle, bugünün insanının ideal şartlarda hayatını sürdürebilmesi için sanal kamusal ("kamusanal") alana ihtiyacı vardır. Bu durum da, sanal kamusal ("kamusanal") alanda ortaya çıkan sorunların giderilmesini gerektirmektedir. Siber Güvenlik Kanunu da bunlardan sadece biridir.

2.2. Kavramsal Açıdan Siber ve Siber Güvenlik

"*Cybernetic*" sözcüğünün kısaltması olan "*cyber*" Türkçeye "siber" olarak çevrilmiştir ve "internete veya bilgisayara ait" anlamında kullanılmaktadır.[24] Daha geniş anlamıyla sibernetik, yapay veya biyolojik sistemlerin kontrol ve haberleşmesini konu alan bilim dalıdır. Etimolojik olarak Eski Yunancada "dümen tutan" anlamındaki *"kybernáō"*ya dayanmaktadır.[25] Siber kavramından türeyen "siber uzay" ise bilişim teknolojileri ve sanal ortamların oluşturduğu dijital evreni (siber uzayı) ifade etmektedir.[26]

Siber uzayda işlenen suçlara ilişkin farklı terimler bulunmakla birlikte, literatürde "siber suç" kavramı yaygın olarak benimsenmiştir.[27] Bu suçlar, bilişim sistemlerine izinsiz erişim, veri silme veya değiştirme gibi eylemleri ve ekonomik, ticari ya da siyasi amaçlı zarar/fayda ilişkilerini kapsamaktadır.[28] Bu bağlamda siber güvenlik, bilgisayar sistemlerini, ağları, yazılımları, kritik altyapıları ve verileri dijital tehditlerden koruma uygulamaları bütünü olarak kabul edilmektedir.[29] Bunun yanı sıra, uluslararası ilişkiler ve toplumsal süreçlerle de ilişkili olduğundan ulusal güvenlik boyutuna sahiptir.[30]

Siber kavramı, kontrol ve iletişim teorisinin kurucularından Norbert Wiener'in (1894-1964) *Cybernetics* adlı eserinde tanımladığı "geri besleme döngüleri"nden (*feedback loops*) türemiştir.[31] Dilimize teknik sistemlerin denetim süreçlerini betimleyen bir ön ek olarak

23 Jurgen Habermas, "Political Communication in Media Society: Does Democracy Still Enjoy an Epistemic Dimension?", *Communication Theory,* 16:4, 2006, s. 420.

24 Türk Dil Kurumu, *Türkçe Sözlük*, 10. Baskı, Türk Dil Kurumu, Ankara, 2005, 2, s. 2093.

25 Sevan Nişanyan, *Nişanyan Sözlük Çağdaş Türkçenin Etimolojisi*, Liberus, İstanbul, 2022.

26 Mehmet Alperen Önal, "Siber Uzay Ve Güvenlik İlişkisi Bağlamında Siber Güvenliğin Boyutları", *Hitit Ekonomi ve Politika Dergisi*, 1:2, 2021, s. 115.

27 İsmail Ergün, *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Adalet Yayınevi, Ankara, 2008, s. 13.

28 Siber Suçlarla Mücadele Daire Başkanlığı, "Siber Suç Nedir?", Emniyet Genel Müdürlüğü (EGM), 2025, https://www.egm.gov.tr/siber/sibersucnedir? erişim 16.05.2025.

29 Soner Çelik, "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *ARHUSS,* 1: 2, 2018, s. 118.

30 Ulusal Siber Olaylara Müdahale Merkezi USOM, *Siber Güvenliğe İlişkin Temel Bilgiler*, Telekomünikasyon İletişim Başkanlığı, 2014, s. 1. https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf?, erişim 16.05.2025.

31 Norbert Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, 3. Baskı, MIT Press, Cambridge, 2019, s. 11. (İlgili kitap 1948 yılında yazılmış olup ikinci baskısı ise 1961 yılında yapılmıştır. Bu çalışmada 1961 yılında yapılan ikinci basımın 2019 yılında tıpkıbasım nüshası kullanılmıştır.) Geri besleme döngüleri (feedback loops), sibernetikte makinelerin veya organizmaların çevrelerine uyum sağlamasını ve denetimli davranış geliştirmesini açıklamak için kullanılan teknik bir terimdir. Sistem, çıktılara göre otomatik olarak kendini düzeltmek ya da geliştirmek için yeni girdi oluşturmaktadır. Bir başka ifadeyle sonuçlarına göre sistemin kendini veya eylemlerini kesme, sürdürme veya yeniden düzenleme sürecidir. Örneğin, bireyin sosyal medyadaki etkileşimin çokluğunun paylaşım yapmaya sevk etmesi veya sistemin beğenilere yönelik içerikleri kullanıcıya sunması geri besleme döngüleridir. Sibernetiğin kurucu ismi sayılan Wiener geri besleme döngülerini şöyle açıklamaktadır: *"(...) bir sistemin çıktısının, sistemin gelecekteki davranışını etkileyecek biçimde tekrar girdiye dönmesidir. Bu mekanizma, sistemin kendi davranışlarını düzenlemesini sağlar"*. Wiener, *Cybernetics or Control and Communication in the Animal and the Machine*, s. 64.

geçmiştir.[32] Yirminci yüzyılın ortalarında Claude Shannon (1916-2001) ve Warren Weaver'ın (1894-1878) oluşturduğu Matematiksel İletişim Modeli'ndeki bilgi kuramı yaklaşımı, kanaldan geçen sinyallerin niceliksel ölçümünü vurgulayarak siber uzayın yalnızca devrelerden ibaret olmadığını ileri sürmektedir. Bu yaklaşım aynı zamanda belirsizlik ve gürültünün iletişimin ontolojik temellerinin birer parçası olduğunu savunmuştur.[33] Sosyal Sistemler Teorisi bağlamında Niklas Luhmann, sosyal ve teknik alt sistemlerin kendi kendini yeniden üreten bir ağ oluşturduğunu vurgulayarak internet dünyasının (siber uzayın) karmaşık uyum ve özerklik boyutlarını ortaya koymuştur.[34] Luciano Floridi'nin "bilgi etiği" perspektifi ise, "infosfer" kavramını benimseyerek dijital varlıkların etik statüsünün yalnızca araçsal değil aynı zamanda değer çerçevesinde ele alınması gerektiğini savunmaktadır.[35]

Ross Anderson'ın *Security Engineering* (Güvenlik Mühendisliği) adlı çalışmasında siber güvenlik olgusunu mühendislik, yönetişim ve hukuki düzenlemelerin kesişim noktasında yer alan disiplinler arası bir alan olarak tanımlanmaktadır.[36] Bruce Schneier ise şifreleme, güvenlik duvarları ve izinsiz giriş tespit sistemleri gibi teknik tedbirlerin yanı sıra risk yönetimi süreçlerinin de siber güvenliğin ayrılmaz parçası olduğunu belirtmektedir.[37] Bu kapsamda *National Institute of Standards and Technology* (NIST)'nin oluşturduğu çerçeve metinde kritik altyapı koruma standartları tanımlanarak, kuruluşların varlık envanteri, zafiyet değerlendirmesi ve olay müdahalesi süreçlerini sistematik hale getirmesi gerektiğini öngörmektedir.[38] Daniel Solove'un "Gizlilik Kuramı" ise kişisel verilerin sınıflandırılması ve kullanım senaryoları üzerinden mahremiyet ihlallerinin çok boyutlu analizine odaklanarak, siber güvenlik stratejilerinin "bireyin bilgi özerkliğini" de koruması gerektiğini ortaya koymaktadır.[39]

Siber suçlar alanında Ronald Clarke ve Derek Cornish, geleneksel suç tiplerinde görülen saldırgan tipolojileri, karar verme süreçleri ve eylemlerinin modellenerek dijital ortama uyarlanması gerektiğini ileri sürmüştür. Böylelikle geleneksel suç tipleri ve müeyyidelerinden hareketle dijital suç normlarının da oluşturulması ve/veya geliştirilmesi sağlanabilecektir.[40] David Wall ise siber suçları hem teknik saldırı yöntemleri hem de örgütlenme biçimleri bağlamında ele alarak, uluslararası iş birliğinin önemini ve sınır ötesi hukuki müesseselerin güçlendirilmesi gerektiğini vurgulamaktadır.[41] Konuyu "risk yönetimi" bağlamında ele alan Douglas Thomas ve Brian Loader, siber suç mücadelesinin etkinliğinin, güvenlik ve gözetim mekanizmalarıyla birlikte sivil özgürlüklerin korunmasına da bağlı olduğunu belirtmektedir.[42]

32 Nezir Akyeşilmen, *Disiplinlerarası Bir Yaklaşımla: Siber Politika & Siber Güvenlik*, Orion Kitabevi, Ankara, 2018, s. 54.
33 Claude E. Shannon, "A Mathematical Theory of Communication", *Bell System Technical Journal*, 27: 3, 1948, s. 379.
34 Niklas Luhmann, *Social Systems*, Stanford University Press, Stanford, 1996, s. 45.
35 Luciano Floridi, "Information Ethics: On the Philosophical Foundation of Computer Ethics", *Ethics and Information Technology*, 1, 1999, s. 42.
36 Ross Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, Wiley, New York, 2020, s. 3.
37 Bruce Schneier, *Secrets and Lies: Digital Security in a Networked World*, Wiley, New York, 2004, s. 18.
38 Kevin M. Stine, Kim Quill, ve Gregory A. Witte, "Framework for Improving Critical Infrastructure Cybersecurity", *National Institute of Standards and Technology*, 2014, s. 5, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity, erişim 12.06.2025.
39 Daniel J. Solove, *Understanding Privacy*, Harvard University Press, Cambridge, 2007, s. 77.
40 Ronald V. Clarke ve Derek B. Cornish, "Modeling Offenders' Decisions: A Framework for Research and Policy", *Crime and Justice*, 6, 1985, s. 159.
41 David S. Wall, *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge, 2007, s. 57.
42 Brian D. Loader ve Douglas Thomas, *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age,* Routledge, London, 2000, s. 102.

Teknik boyutun ötesinde siber uzayın felsefi olarak ele alınması, Martin Heidegger (1889-1976)'in teknoloji eleştirisi özelindeki dünyakaynak ilişkisi analizine dayandırılabilir. Bu açıdan dijital platformlarda kullanıcı verilerinin "kaynak" hâline getirilmesi, modernitenin dayattığı araçsal bakışın bir tezahürüdür.[43] Michel Foucault (1926-1984) iktidarbilgi ilişkisine dayanan yaklaşımını oluştururken, modernitenin birey ve toplumu gözetim ve denetim altında tutma anlayışını açık olarak yansıtma özelliği nedeniyle Jeremy Bentham (1748-1832) tarafından geliştirilen bir hapishane modeli olan Panoptikon'dan faydalanmıştır.[44] Panoptikon metaforu dijital gözetim pratikleriyle (sinoptikon ve omniptikon)[45] örtüşmektedir ve siber güvenlik aktörlerinin veri toplama ve analiz faaliyetleri açısından iktidar olduğunu söylemek mümkündür. Bu bağlamda Gilles Deleuze (1925-1995) ve Félix Guattari'nin (1930-1992) "kontrol toplumları" eleştirisi ise sürekli izlenme ve veri profillemenin bireysel öznelliği otorite isteğine göre şekillendirdiğine dikkat çekmektedir.[46]

Bu bağlamda bir kontrol alanı olarak siber uzayda var olmaya çalışan bireyin kimlik ve öznellik yönlerinin etkilenme biçimleri üzerinde durulması gereken konulardandır. Tüm bu değerlendirmeler güvenlik ile teknolojinin iç içe geçen bir yapısı olduğunu göstermektedir ve böyle bir ortamda teknolojinin geldiği aşama güvenlik konusunun en önemli ayaklarından biri olan siber uzaydaki faaliyetleri oluşturmaktadır. Dolayısıyla bu ortamda güvenlik tesis edilirken herhangi bir suiistimal, ihlal, tehdit, risk ve zararlara karşı önlem almak başta devlet ve kurumları olmak üzere kamusal faydayı gözeten STK, akademi ve ekonomik kuruluşlara görevler düşmektedir.

Diğer yandan Manuel Castells'in "Ağ Toplumu" modelinde sosyal medya platformlarının demokratik katılım araçları açısından olumlu katkı sunduğunu fakat dezenformasyon ve manipülasyon bağlamında tam tersi bir etki yaptığı vurgulanmaktadır.[47] Hukuk felsefesi açısından en güncel tartışma metinlerinden biri olan Bir Adalet Teorisi (*A Theory of Justice*, 1971)'nde John Rawls'ın "adil ve eşit özgürlükler ilkesi ile adil fırsatlar ilkesi" kavramsallaştırmaları[48] bağlamında siber güvenlik düzenlemelerinin bireysel hakları koruyacak şekilde şekillendirilmesini, orantılılık ve demokratik denetim mekanizmalarının tesisini bir zorunluluk olduğunu söyleyebiliriz. Bu temel metinlere dayanan analitik çerçeve, Siber Güvenlik Kanunu'nun yeni medya ve iletişim faaliyetlerine ilişkin düzenlemelerini değerlendirirken iktidar, toplum, hukuk, güvenlik ve teknoloji ilişkisi ile bireysel haklar ve demokratik denetim mekanizmalarının birlikte ele alınmasının zorunluluğu ortaya çıkmaktadır. Yukarıdaki genel çerçeve bağlamında, çalışmanın ana izleği olarak seçilen Jurgen Habermas'ın İletişimsel Eylem Kuramı ile ilişkilendirdiği Kamusal Alan yaklaşımı, dijital kamusal alanda[49] şeffaf diyalog ve toplumsal uzlaşma için normatif bir çerçeve sunmaktadır.[50]

---

43 Martin Heidegger, *The Question Concerning Technology and Other Essays*, Harper & Row, New York 1977, s. 23.
44 Michel Foucault, *Hapishanenin Doğuşu* (Çev. Ali Yaşar Kılıçbay), İmge Kitabevi Yayınları, Ankara, 1992, s. 251.
45 Panoptikon, 360 derecelik görüş açısına sahip bir mimari yapı sayesinde tek kişinin birçok kişiyi aynı anda gözetleyebildiği "hapishane" modelidir. Sinoptikon, kitle iletişim araçları aracılığıyla çok sayıdaki kişinin az sayıdaki kişiyi gözetlediği ve/veya izlediği gündelik hayat pratiğidir. Omniptikon ise bilişim ve internet teknolojileri sayesinde çok sayıdaki kişinin gönüllü olarak çok sayıdaki kişiyi hem gözetlediği hem de onlar tarafından gözetlendiği etkileşimli bir işleyiştir. (Kaynak: Selin Bitirim Okmeydan, Postmodern Kültürde Gözetim Toplumunun Dönüşümü: 'Panoptikon'dan 'Sinoptikon' ve 'Omniptikon'a. *AJIT-e: Academic Journal of Information Technology*, 8: 30, s. 45.
46 Gilles Deleuze ve Félix Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*, University of Minnesota Press, Minneapolis, 1987, s. 162.
47 Manuel Castells, *Ağ Toplumunun Yükselişi* (Çev. Ebru Kılıç), İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2008, ss. 13-15.
48 John Rawls, *Bir Adalet Teorisi* (Çev. Vedat Ahsen Coşar), Phoenix Yayınevi, Ankara, 2017, s. 17.
49 Sanal kamusal alan olarak da tanımlanan dijital kamusal alan için ***"kamusanal alan"*** terkibi kullanılabilir.
50 Jurgen Habermas, *İletişimsel Eylem Kuramı* (Çev. Mustafa Tüzel), 1, Kabalcı Yayıncılık, İstanbul, 2001, s. 360.

Literatür taraması bağlamında temel bir kavramsal çerçeve çizildiğinde siber güvenlik literatürünün genel olarak üç ana eksende toplandığı görülmektedir. Bunlar, teknik altyapı odaklı çalışmalar, hukuki ve normatif çerçeveye odaklı çalışmalar ve yönetişim ve toplumsal etki analizleri şeklindedir. Aşağıdaki değerlendirme, buradaki üç başlıkta özetlenen sınıflandırma çerçevesinde ele alınarak Siber Güvenlik Kanunu'nun anayasal haklar ile iletişim ve medya özgürlüğü üzerindeki olası etkilerini anlamaya dönük metodolojik bir bağ kurmaktadır.

i. Teknik Yaklaşımlar

Bu grup çalışmalar, donanım ve yazılım güvenliği, ağ altyapısı, veri şifreleme, sızma testleri gibi mühendislik ve bilişim teknolojileri boyutlarını ele almaktadır.[51] Teknik araştırmalar, iletişim altyapısının korunmasında gerekli tedbirleri tanımlamaktadır. Ancak, çoğunlukla demokratik denetim, orantılılık ve ifade özgürlüğü gibi anayasal konulara değinmemektedir. Bu nedenle, hukuki analizler için yalnızca teknik çerçevenin yeterli olmadığı açıktır.

ii. Hukuki ve Normatif Çerçeve

Siber güvenliğin hukuki boyutuna odaklanan çalışmalar, ulusal mevzuatların gelişimi[52] ve uluslararası normların[53] anayasal ilkelerle uyumu konularını işlemektedir. Avrupa Birliği'nin Şebeke ve Bilgi Güvenliği Direktifi,[54] Budapeşte Konvansiyonu ve İkinci Ek Protokol[55] gibi belgeler, güvenlik önlemlerinin temel haklarla dengelenmesini öngörmektedir. Türkiye bağlamında ise 5651 sayılı Kanun,[56] Kişisel Verileri Koruma Kanunu (KVKK) ve Bilgi Teknolojileri İletişim Kurumu (BTK) düzenlemeleri,[57] Siber Güvenlik Kanunu öncesinde de dijital ortamda veri ve iletişim akışının kontrolünü mümkün kılan yetkiler sağlamaktadır. Ancak literatür, yeni kanunun önceki düzenlemeleri nasıl genişlettiği veya değiştirdiği konusunda sınırlı bilgi sunmaktadır.

iii. Yönetişim ve Toplumsal Etki

Toplumsal düzeyde yapılan araştırmalar, siber güvenlik politikalarının demokratik toplum ilkeleri, özgürlük-güvenlik dengesi ve ifade özgürlüğü üzerindeki etkilerini irdelemektedir.[58] Bu çalışmalar, siber güvenlik söyleminin gözetim teknolojilerini meşrulaştırma potansiyeline dikkat çekmektedir. Ancak literatüründe Siber Güvenlik Kanunu'nun özellikle iletişim süreçleri ve medya faaliyetlerinin dijital kamusal ("kamusanal") alan üzerindeki etkisini, anayasa hukuku perspektifinden ele alan kapsamlı bir değerlendirme bulunmamaktadır.

Mevcut literatür, teknik, hukuki ve yönetişim boyutlarında önemli birikim sunmakla birlikte, bu üç alanın iletişim süreçleri ve medya faaliyetleri bağlamında birbirine entegre

51 Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*, s. 3; Schneier, *Secrets and Lies: Digital Security in a Networked World*, s. 18.

52 Karasoy ve Babaoğlu, *"Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı"*, s. 131.

53 Eldem, *"Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik"*, s. 371.

54 The Council of Europe, "Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems", The Council of Europe Publishing, Strasbourg, 2003, https://rm.coe.int/168008160f, erişim 10.05.2025.

55 The Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, The Council of Europe Publishing, Strasbourg, 2021.

56 Türkiye Büyük Millet Meclisi, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, Kanun No. 5651, 04 Mayıs 2007, https://resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm, erişim 15.05.2025.

57 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu*, Kanun No. 6698, 24 Mart 2016, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf, erişim 16.05.2025.

58 Ulrich Beck, *Risk Toplumu: Başka Bir Modernliğe Doğru* (Çev. Kazım Özdoğan ve Bülent Doğan), İthaki Yayınları, İstanbul, 2011, s. 232.; Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York, 2018, s. 119.

edildiği az sayıda çalışma mevcuttur. Tablo 1, bu konuda hem çalışmanın genel perspektifini hem de literatürdeki tematik sınıflandırmayı analitik sentez düzeyinde özet olarak sunmaktadır:

Tablo 1. Literatürde Tematik Sınıflandırma ve Analitik Sentez

Tema	Temel Kaynaklar	Literatürün Analitik/Kritik Sentezi
Hukuki Normatif Bağlam	*A Theory of Justice*,[59] *Understanding Privacy*,[60] Avrupa Konseyi Strasburg[61] ve Budapeşte Sözleşmeleri,[62] 5651 Sayılı Kanun,[63] 6698 sayılı KVKK,[64] Siber Güvenlik Kanunu.[65]	Bu literatür kümesi, temel haklar-özgürlükler ile güvenlik önlemlerinin meşruiyet koşullarını göstermektedir. Rawls'un öncelik ilkesi ve Solove'un mahremiyet sınıflandırması, veri-toplama ve ifade kısıtlarının hukukî sınırlarını ölçmek için kullanılabilme potansiyeline sahiptir. Uluslararası sözleşmeler ve ulusal kanunlar ise uygulamada hangi araçların meşru sayıldığına ilişkin normatif çerçeveyi sağlamaktadır.
Teknolojik Mühendislik Bağlamı	*Security Engineering*,[66] *Secrets and Lies*,[67] *Modern Operating Systems*,[68] *Framework for Improving Critical Infrastructure Cybersecurity*,[69] USOM/ BTK teknik rehberleri.[70]	Teknik literatür, loglama, olay müdahalesi, sistem bütünlüğü ve veri saklama uygulamalarının nasıl çalıştığını göstermektedir. Bu kaynaklar, hukuki kısıtlamaların pratikte uygulanabilirlik düzeyini ve teknik zorunlulukları anlamak için gereklidir.
Yönetişim Kurumsal Bağlamı	*Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı*,[71] *Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli* ***için Öneriler***,[72] BTK ve USOM resmi raporları,[73] AB Siber Güvenlik Strateji Belgesi.[74]	Kurumsal çalışmalar, hangi kurumların hangi yetkiye sahip olduğunu ve hesap verebilirliğin nasıl tesis edileceğini tartışmaktadır. Türkiye özelinde siber güvenlik ile ilgili resmî kurumların faaliyetlerinde yetki alanı, şeffaflık gibi kısımlarda belirsizlikler olduğu görülmektedir.

59 John Rawls, *A Theory of Justice*, Harvard University Press, Cambridge, 1971, s. 76.
60 Solove, *Understanding Privacy*.
61 Avrupa Konseyi, *"Additional Protocol to the Convention on Cybercrime, concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems"*.
62 Council of Europe, *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*.
63 Türkiye Büyük Millet Meclisi, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun.
64 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu*.
65 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.
66 Anderson, *Security Engineering: A Guide to Building Dependable Distributed Systems*.
67 Schneier, *Secrets and Lies: Digital Security in a Networked World*.
68 Andrew S. Tanenbaum ve Herbert Bos, *Modern Operating Systems*, Pearson, New Jersey, 2015.
69 Stine, Quill ve Witte, *"Framework for Improving Critical Infrastructure Cybersecurity"*.
70 USOM, *Siber Güvenliğe İlişkin Temel Bilgiler*.
71 Karasoy ve Babaoğlu, *"Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı"*.
72 Darıcılı, *"Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli için Öneriler"*.
73 USOM, *Siber Güvenliğe İlişkin Temel Bilgiler*.
74 European Data Protection Supervisor, "Opinion of the European Data Protection Supervisor on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace", *EDPS*, 2013, https://www.edps.europa.eu/sites/default/files/publication/13-06-14_cyber_security_en.pdf, erişim 19.05.2025.

İletişim ve Medya Etkileri Bağlamı	*The Theory of Communicative Action*,[75] Ağ Toplumunun Yükselişi,[76] *Convergence Culture*,[77] *The Age of Surveillance Capitalism*[78] kaynaklarındaki medya ile ilgili değerlendirmeler.	Bu kaynaklar dijital kamusal alanın yapısını açıklarken platform-dinamizmini, sosyo-kültürel dönüşümü, gözetim kapitalizminin yükselişini ve tüm bu gelişmelerin ifade ortamına etkisini ortaya koymaktadır. Kanundaki ifadeyi/erişimi sınırlayan hükümler buradaki değerlendirmelerin ortak tespiti olan demokratik açıdan olumsuz görüntüyle örtüşmektedir.

Çalışma, yukarıdaki sınıflandırmaya dayalı olarak Siber Güvenlik Kanunu'nu iletişim ve medya bağlamında spesifik biçimde ele alarak kapsamlı bir değerlendirme sunmaktadır. Ancak bu yaklaşım, kanunun multidisipliner yapısı nedeniyle genel çerçevesini bütünüyle yansıtamama riskini de beraberinde getirmektedir. Diğer yandan literatürde, özellikle siber güvenlik mevzuatının iletişim özgürlüğü, mahremiyet hakkı, orantılılık ve şeffaflık ilkeleri ile ilişkisini doğrudan tartışan ampirik ve normatif çalışmaların eksikliği göze çarpmaktadır. Bu eksikliği kısmen gidermeyi amaçlayan çalışma, kamusal alan ve siber güvenlik ekseninde ilerleyerek Siber Güvenlik Kanunu'nun iletişim süreçleri ve yeni medya faaliyetleri üzerindeki etkilerini incelemektedir. Ele alınan kavramsal çerçeve, teknik ve toplumsal boyutları kapsayan disiplinlerarası bir zeminde inşa edilmenin yanında, ana eksenini Habermas'ın "Kamusal Alan" yaklaşımı oluşturmaktadır. Kapsamın kısıtları gereği, yapılan değerlendirme anayasal açıdan bireysel haklar ve diğer hukuki düzenlemeler çerçevesinde iletişim ve medya alanındaki etkiler ile sınırlandırılmıştır. Bununla birlikte, literatür taraması ve kavramsal çerçeve bölümünde (iletişim süreçleri ve medya faaliyetlerinin kapsam dışında kalan) diğer alanlarla ilişkisine dair hususlara da kısmen değinilmiştir.

3. Siber Güvenlik Kanunu ve Öncesi

1990'ların sonlarından başlayarak dijital altyapıların yaygınlaşmasıyla Türkiye'de siber güvenlik alanı hem teknik hem kurumsal olarak gelişmiş, fakat idari ve yasal yetkiler uzun süreli bu evrim içinde parçalı bir gelişim göstermesi sonucu yetersiz kalmıştır. Bu dönemde yapılan düzenlemelere bakıldığında sorumluluk ve yetkiler, politika, koordinasyon, teknik müdahale, istihbarat ve adli/kolluk kurumlarının sorumlulukları arasında dağılım göstermiştir. Bunun yanında kişisel verilerin korunması ayrı bir yasal çerçeve altında düzenlenmiştir. Parçalı yapı ile görev ve yetki paylaşımının net tanımlanamaması kurumların faaliyetlerinde örtüşme/boşluk ve sürtüşmeler doğurmuştur. Sağlıklı işlemeyen bu yapı koordinasyon, etkin bilgi paylaşımı ve hukuki şeffaflık gereksinimlerini ön plana çıkarmıştır.[79] Siber Güvenlik Kanunu öncesinde Türkiye'de siber güvenlik ile ilgili yetkilendirilmiş çok parçalı yapı şöyledir.

i. Bilgi Teknolojileri ve İletişim Kurumu (BTK): BTK, elektronik haberleşme düzenleyicisi olarak yıllar içinde ulusal siber güvenlik politikalarının oluşturulmasında merkezi bir rol üstlenmiştir. BTK çatısı altında çalışan ve ülke çapında koordinasyonu sağlamaya yönelik mekanizmalar ile (Siber Güvenlik Kurulu vb.) strateji, politika ve kritik altyapı belirleme gibi görevler yerine getirilmiştir. Ayrıca düzenleyici/denetleyici yetkiler kapsamında erişim, telekomünikasyon altyapısı ve bazı güvenlik standartlarına ilişkin

75 Jurgen Habermas, *The Theory of Communicative Action* (Çev. Thomas McCarty), Beacon Press, Boston, 1984.
76 Castells, *Ağ Toplumunun Yükselişi*.
77 Henry Jenkins, *Convergence Culture: Where Old and New Media Collide*, New York University Press, New York, 2006.
78 Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*.
79 Ege Çakırca, Tuna Çakırca ve Oylum Çelik, "Türkiye'de Siber Güvenliğin Yeni Yasal Çerçevesi: 7545 Sayılı Siber Güvenlik Kanunu", *Turkish Law Blog*, 16 Mayıs 2025, https://turkishlawblog.com/insights/detail/turkiyede-siber-guvenligin-yeni-yasal-cercevesi-7545-sayili-siber-guvenlik-kanunu, erişim 15.08.2025.

düzenlemeler yapma kapasitesine sahiptir. Bu yetkiler, ilgili elektronik haberleşme mevzuatı ve BTK'nin kurumsal düzenlemeleri temelinde kullanılmıştır.[80] Diğer yandan BTK'nin bilgi-belge talep etme yetkisi, sektörel düzenleme ve denetim çerçevesinde sınırlı, mevzuata bağlanmış ve idari yaptırımlara tabi bir yetki formu olarak ortaya çıkmaktadır. BTK, 5809 sayılı Elektronik Haberleşme Kanunu kapsamında bu alana ilişkin düzenleme, denetim ve denetim sonucu elde edilecek bilgi ve belgelerin talep edilmesi yetkisini kullanmakta ve mevzuata aykırılıklar halinde idari para cezası gibi yaptırımlar uygulayabilmektedir.[81]

ii. USOM / TR-CERT (Ulusal Siber Olaylara Müdahale Merkezi): Teknik müdahale, olay tespit-haberleşme ve ulusal tehdit paylaşımı fonksiyonları büyük oranda USOM (TR-CERT) çerçevesinde yürütülmüştür. USOM, 7/24 faaliyet gösteren bir ulusal CSIRT merkezi olarak kurumlar arası olay koordinasyonu, uyarı yayma, tehdit analizi ve kurumsal SOME'lerle eşgüdüm sorumluluğu üstlenmiştir. Operasyonel işleyişi BTK ile yakın ilişki içinde olan USOM'un uygulamaları, müdahale süreçleri ve kurumsal SOME (CSIRT) ağı, uygulamadaki teknik kapasitenin omurgasını teşkil etmiştir.[82]

iii. Millî İstihbarat Teşkilâtı (MİT) ile İçişleri Bakanlığı/Emniyet Genel Müdürlüğü: MİT, ulusal güvenlik boyutundaki (siber istihbarat, yabancı kaynaklı tehditler vb.) faaliyetler ve istihbarat toplama görevleriyle bu alanın güvenlik-istihbarat cephesini temsil etmektedir. İçişleri bakanlığına bağlı Emniyet Genel Müdürlüğü ise siber suç soruşturmaları, adli takip, kolluk operasyonları ve suç delillerine erişim süreçlerinde yetkili organlardır. Bu aktörlerin yetkileri, istihbarat ve kolluk hukukuna ilişkin ayrı mevzuat ile düzenlenmiş olup pratikte bilgi paylaşımı ve operasyonel koordinasyonunu BTK/USOM ile etkileşim hâlinde yürütmektedir.[83]

iv. KVKK ve Sektör Düzenleyicileri (BDDK, EPDK, SPK vb.): Kişisel verilerin korunması veri işleme süreçlerinin hukuki çerçevesini belirleyen kanun, sektör bazlı düzenleyiciler (örneğin bankacılık, enerji, sermaye piyasaları) kendi alanlarına münhasır ek düzenlemeler ve yükümlülükler koyabilme yetkisi verilmiştir.[84] Bu iki katmanlı düzenleme, veri koruma ile siber güvenlik tedbirleri arasında hem işbirliği hem de uyum gerektiren bir ilişkiyi getirmiştir fakat hem yetki alanı belirsizliği hem de çift başlılık doğurmuştur.

v. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi (CBDDO): CBDDO geleneksel olarak politik–stratejik koordinasyon, dijital dönüşüm politika ve rehberliği ile kamu kurumları arası eşgüdüm rolü üstlenen; doğrudan cezaî/idari yaptırım uygulama veya zorlayıcı belge/erişim talebi yetkisi olmayan bir yapıdır.[85] Ancak, 28 Mart 2025 tarihli Cumhurbaşkanlığı kararnamesiyle CBDDO kapatılmış[86] ve bazı görev ile yetkileri genişletilerek Siber

80 Bilgi Teknolojileri ve İletişim Kurumu, "Siber Güvenlik Kurulu", *Bilgi Teknolojileri ve İletişim Kurumu*, 2025, https://www.btk.tr/siber-guvenlik-kurulu, erişim 15.08.2025.

81 Türkiye Büyük Millet Meclisi, *Bilgi Teknolojileri ve İletişim Kurumu İdari Yaptırımlar Yönetmeliği*, Yönetmelik No 28914, 2014, https://www.resmigazete.gov.tr/eskiler/2014/02/20140215-7.htm, erişim 15.08.2025; Türkiye Büyük Millet Meclisi, *Elektronik Haberleşme Kanunu*, Kanun No 5809, 05 Kasım 2008, https://resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm, erişim 15.05.2025.

82 Ulusal Siber Olaylara Müdahale Merkezi, "Hakkımızda/about Us", *Ulusal Siber Olaylara Müdahale Merkezi*, 15 Ağustos 2025, https://www.usom.gov.tr/hakkimizda, erişim 15.05.2025.

83 Millî İstihbarat Teşkilâtı, *"Yetki ve Sorumluluklar", Millî İstihbarat Teşkilâtı (MİT)*, 2025, https://www.mit.gov.tr/yetki-ve-sorumluluklar.html, erişim 15.08.2025; Siber Suçlarla Mücadele Daire Başkanlığı, *"Siber Suç Nedir?*".

84 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu*.

85 Govinsider, "Digital Transformation Office (DTO) of the Presidency of the Republic of Türkiye", *Govinsider*, 2025, https://govinsider.asia/intl-en/digital-government/country/turkey?utm_source=chatgpt.com&type=info&agency=digital-transformation-office-dto-of-the-presidency-of-the-republic-of-turkiye-80, erişim 15.08.2025.

86 Hüseyin Cem Dağıstanlı ve Abdullah Sarıca, "Cumhurbaşkanlığına bağlı ofis ve politika kurullarına ilişkin düzenlemeler Resmi Gazete'de", *Anadolu Ajansı*, 28 Mart 2025, https://www.aa.com.tr/tr/gundem/cumhurbaskanligina-bagli-ofis-ve-politika-kurullarina-iliskin-duzenlemeler-resmi-gazetede/3522186, erişim .

Güvenlik Başkanlığı veya ilgili yeni yapılar arasında yeniden dağıtılmıştır. Bu görev devri/organizasyon değişikliği sonucunda Siber Güvenlik Kanunu bağlamında başkanlığa tanınan "kurum ve kuruluşlardan bilgi ve belge talep etme" gibi geniş erişim yetkileri, CBDDO'nun daha çok koordinatif nitelikteki fonksiyonları ile BTK'nin sektörel, yaptırıma dayalı denetim yetkileri arasında hibrit bir yetki profilinin doğmasına yol açmıştır. Diğer bir deyişle, politik koordine edici roller ile zorlayıcı erişim-yetkilerinin aynı merkezde toplanması, hem hukuki sınırların yeniden çizilmesini hem de denetim ve hesap verebilirlik mekanizmalarının güçlendirilmesini gerektirmektedir.[87]

Yukarıdaki yetki ve uygulama aşamalarındaki sorunları gidermek amacıyla Siber Güvenlik Kanunu çıkarılmıştır. Daha geniş ifadeyle, bu Kanun'a duyulan ihtiyaç, Türkiye'de siber tehditlerin artan sıklığı ve karmaşıklığı karşısında mevcut mevzuatın dağınık ve yetersiz kalması; kritik altyapıların, kamu hizmetlerinin ve özel sektör veri varlıklarının etkin korunamaması; olaylara hızlı müdahale ve koordinasyon kapasitesinin güçlendirilmesinin gerekliliğinden kaynaklanmıştır (Kanun'un amaç ve kapsamı Resmî Gazete'de açıkça belirtilmiştir).[88] Ayrıca Kanun, siber olaylara ilişkin raporlama, sorumlulukların netleştirilmesi, ulusal strateji ve merkezî bir yönetim/başkanlık yapısının kurulması yoluyla hem önleme hem de müdahale mekanizmalarını hukuki zemine oturtmayı hedeflemektedir. Böylece kurumlar arası koordinasyon eksikliğini gidermeyi ve cezaî/idarî yaptırımlarla caydırıcılığı artırmayı amaçlamaktadır.[89] Bununla birlikte kritik sektörlerin korunması, yerli siber güvenlik ekosisteminin güçlendirilmesi ve uluslararası iş birliği ile bilgi paylaşımının düzenlenmesi ihtiyacına da cevap vermek amacıyla hem operasyonel hem de stratejik zafiyetleri kapatmayı amaçlayan kapsamlı bir düzenleme ihtiyacının sonucu olarak ortaya çıkmıştır.[90]

4. İletişim Süreçleri ve Medya Faaliyetleriyle İlgili Anayasal Hak ve Özgürlükler ile Uluslararası Sözleşmeler Bağlamında Siber Güvenlik Kanunu

Siber güvenlik ve hukuk arasındaki ilişki, dijitalleşen dünyada giderek daha karmaşık ve çok katmanlı bir hâl almıştır. Siber güvenlik, sadece teknik bir mesele olmaktan çıkıp, ulusal ve uluslararası hukuk sistemlerinin düzenleme ve müdahale alanına girmiştir. Bu bağlamda, siber güvenliğin sağlanması ve korunmasında hem ulusal hem de uluslararası hukuk düzenine önemli roller düşmektedir.[91] Siber alandaki faaliyetlerin düzenlenmesinde hukuk, geleneksel devlet hukukunun ötesine geçerek, farklı normatif düzenlemeleri ve kural koyucuları içeren çok hukuklu bir yapıya dönüşmektedir.[92] Bu durum, siber güvenlik alanında hukuki düzenlemelerin, teknolojik gelişmelerle eş zamanlı olarak evrilmesini ve adaptasyonunu zorunlu kılmaktadır. Ayrıca, siber suçların artması ve çeşitlenmesi, kamu otoritelerinin sorumluluğunu artırmakta ve bu alanda etkin hukuki mekanizmaların geliştirilmesini

87 Aslıhan Deniz Bilgehan, "Siber Güvenlik Başkanlığının Düzenlenişine Dair Değerlendirme", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 12:1, 2025, ss. 63-88,

88 Siber Güvenlik Kanunu, c. 7545.

89 Mehmet Karlı, Osman Gazi Güçlütürk ve Zeynep Ekinci, "Türkiye'de Siber Güvenlik Kanunu Yürürlüğe Girdi", *Lexology*, 20 Mart 2025, https://www.lexology.com/library/detail.aspx?g=ea84ee2a-52c2-4abe-acb1-2c48021f85cf, erişim 16.08.2025.

90 Gözde Esen Sakar, Ece Nart ve Pelinsu Üstündağ, "7545 Sayılı Siber Güvenlik Kanunu", *Mondaq*, 02 Nisan 2025, https://www.mondaq.com/turkey/security/1606732/7545-say%C4%B1l%C4%B1-siber-g%C3%BCvenlik-kanunu, erişim 15.08.2025.

91 Merve Erdem ve Gürkan Özocak, "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 68:1, 2019, s. 130.

92 Fatma Hatipoğlu Aydın, *Siber Güvenlik ve Kişisel Verilerin Korunması: Hukuki Bir Değerlendirme*, Adalet Yayınevi, Ankara, 2023, s. 50.

gerektirmektedir.[93] Sonuç olarak, siber güvenlik ve hukuk arasındaki ilişki, dinamik ve sürekli gelişen bir alan olup, etkin bir siber güvenlik stratejisi için hukuki altyapının güçlendirilmesi ve güncellenmesi elzemdir.

Dijitalleşen dünyada iletişim, yalnızca bireyler arası mesaj alışverişi olmaktan çıkarak, sistemler, kurumlar ve devletlerarasındaki ilişkileri kapsayan interaktif ve stratejik bir alana dönüşmüştür. Türkiye'de 2025 yılında yürürlüğe giren Siber Güvenlik Kanunu, siber uzayda kamu güvenliğini artırmayı hedeflerken, aynı zamanda iletişim sistemleri üzerinde ciddi etkiler oluşturmaktadır. Siber uzayın gelişimi, iletişim kavramını hem teorik hem pratik anlamda dönüştürmektedir. Devletlerin dijital ortamda birey, toplum ve kurumları korumaya yönelik çabaları, yalnızca teknik düzenlemeleri değil, aynı zamanda iletişim ve medyayı kontrol altına alma stratejilerini de içermektedir. Siber Güvenlik Kanunu bu bağlamda değerlendirildiğinde iletişim sosyolojisi, kitlesel medya çalışmaları, siyasal iletişim ve kültürel yapı açısından önemli düzenlemeler içerdiği görülmektedir. Aşağıda, bu düzenlemelerin son örneği olan Siber Güvenlik Kanunu, anayasal hak ve özgürlükler bağlamında analiz edilmiştir.

4.1. Anayasal Haklar ve İletişim Özgürlüğü Bağlamında Siber Güvenlik Kanunu'nun Değerlendirmesi

İletişim hakkı, demokratik toplumların temel unsurlarından biri olarak, bireylerin bilgi alma, yayma ve ifade özgürlüğünü kapsamaktadır.[94] Bu hak, yalnızca bireyler arası ilişkiyi değil, aynı zamanda kamusal alanın işleyişini ve siyasal katılım süreçlerini doğrudan etkilemektedir. Türkiye Cumhuriyeti Anayasası başta olmak üzere, tarihsel süreç içinde yürürlüğe giren Basın Kanunu, Radyo ve Televizyonların Kuruluş ve Yayın Hizmetleri Hakkında Kanun ve İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun gibi yasal düzenlemeler bu alanı şekillendirmektedir. 2025 tarihli Siber Güvenlik Kanunu, bu yasal çerçeveye yeni bir katman ekleyerek dijital iletişim alanında ilgili resmî kurumlara güçlü müdahale yetkileri tanımlamaktadır. Tablo 2'de, Siber Güvenlik Kanunu kapsamında anayasal olarak bireyin iletişim ve medyaya ilişkin sahip olduğu haklara yer verilmiştir:

Tablo 2. Bireyin Anayasal Olarak Sahip Olduğu Haklar ve Siber Güvenlik Yasasıyla İlgili Bölümlerinin Değerlendirmesi

Madde	İçerik ve Açıklama	Değerlendirme
Anayasa'nın 26. Maddesi: İfade Özgürlüğü	Türkiye Cumhuriyeti Anayasası'nın 26. maddesi, herkesin düşünce ve kanaatlerini söz, yazı, resim veya başka yollarla açıklama ve yayma hakkına sahip olduğunu belirtmektedir.[95] Siber Güvenlik Kanunu 13. maddesiyle, Başkanlık tarafından edinilen bilgi ve belgelerin medya aracılığıyla paylaşılmasını yasaklayarak bu özgürlüğü daraltmaktadır.[96] Bu durum, ifade özgürlüğü ile kamu güvenliği arasında anayasal bir denge sorununu gündeme getirmektedir.	İfade özgürlüğü, güvenlik gerekçesiyle ciddi biçimde sınırlanmakta; anayasal hak ile yasa arasında denge bozulmaktadır.

93 Ahmet Efe, *Bilişim Suçları ve Türk Ceza Hukukundaki Yeri*, Seçkin Yayıncılık, Ankara, 2017, s. 5.
94 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*, TBMM Basımevi, Ankara, 2020.
95 Age, s. 30.
96 Türkiye Büyük Millet Meclisi, "Siber Güvenlik *Kanunu"*, Kanun No. 7545, 12 Mart 2025, https://resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm., erişim: 12.06.2025.

Anayasa'nın 22. Maddesi: Haberleşme Hürriyeti	Anayasa'nın 22. maddesi, haberleşme hürriyetini güvence altına almaktadır.[97] Bu hak, yalnızca kişisel yazışmaları değil, internet üzerinden veri alışverişini ve dijital haberleşme süreçlerini de kapsamaktadır. Siber Güvenlik Kanunu'nun 6. maddesi, Başkanlık'a "log"[98] verileri toplama, inceleme ve saklama yetkisi verirken, bu hak üzerinde istisnai bir denetim yetkisi tanımaktadır.[99] İlgili maddenin, *"gerekli olduğu sürece"* verilerin saklanmasına izin vermesi, orantılılık ve ölçülülük ilkesi çerçevesinde tartışmalıdır.	Özel hayatın gizliliği ihlal etme ve keyfi veri toplama, denetim dışı uygulamalara kapı aralama riski taşımaktadır.
5187 Sayılı Basın Kanunu ve Yayın Özgürlüğü	5187 sayılı Basın Kanunu, basının serbestçe bilgi edinme, yayma ve eleştirme hakkını güvence altına almaktadır.[100] Ancak Siber Güvenlik Kanunu'nun 12. ve 13. maddelerinde getirilen yayın yasağı ve medya açıklama kısıtlamaları, bu özgürlüğü ciddi biçimde sınırlandırmaktadır. Özellikle "her türlü medya aracıyla açıklama yasağı"nın kapsamı oldukça geniş olması basın özgürlüğü ilkesiyle örtüşmemektedir.	Medya üzerindeki baskı artırılmıştır. Bu durum medyanın kamusal fayda sağlayıcı faaliyet yapma niteliğine zarar verebilme riski taşımaktadır.
5651 Sayılı Kanun ve İnternet Yayıncılığı	İnternet Ortamında Yapılan Yayınların Düzenlenmesi Hakkında Kanun (5651) internette içerik ve yer sağlayıcıların yükümlülüklerini belirlerken, içeriklerin kaldırılması ve erişimin engellenmesini de düzenlemektedir.[101] Siber Güvenlik Kanunu bu yapıya paralel olarak, bazı maddelerde 5651'i referans almakta ve hatta 19. maddede bu kanunda değişiklik yapmaktadır. Ancak Siber Güvenlik Kanunu, içeriğe değil sisteme dair erişim, kayıt ve gözetim yetkilerini tanımladığı için daha üst düzey bir denetim mekanizması inşa etmektedir.	İçeriklerin kontrolünün bu denli genişletilmesi ifade ve bilgiye erişim özgürlüğü sınırlı hale getirmektedir.
6698 Sayılı Kişisel Verilerin Korunması Kanunu	Kişisel verilerin korunması, Anayasa'nın 20. maddesiyle[102] güvence altına alınmış ve 6698 sayılı Kişisel Verilerin Korunması Kanuni (KVKK) ile detaylandırılmıştır.[103] Siber Güvenlik Kanunu'nda kişisel verilerin en fazla iki yıl süreyle saklanacağı ve sonrasında "silineceği ya da anonim hale getirileceği" ifade edilse de, bu süreçlerin denetiminden ve şeffaflığından bahsedilmemektedir. Bu durum, bireylerin verileri üzerindeki denetimini sınırlayabilecek niteliktedir.	Bireylerin şahsi verileri üzerinde kişisel kontrollerini zayıflatma riski taşıyan bu durum veri güvenliği konusunda şeffaflık ve hesap verebilirlik ilkeleriyle çelişmektedir.

Yukarıdaki tabloda görüldüğü üzere bireylerin iletişimi de içeren temel hakları anayasal güvence altına alınmıştır. Bununla birlikte yürürlüğe giren Siber Güvenlik Kanunu

97 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*, s. 28.

98 "Log" (kayıt), bilişim sistemlerinde gerçekleşen olayların, işlemlerin veya hataların kronolojik ve düzenli bir şekilde kaydedilmesini ifade eden bir terimdir. Log'lar sistemlerin izlenmesi, hataların tespiti, güvenlik ihlallerinin analizi ve performans optimizasyonu gibi kritik süreçlerde kullanılmaktadır. Kaynak: Andrew S. Tanenbaum ve Herbert Bos, *Modern Operating Systems*, Pearson, New Jersey, 2015, s. 294.

99 Siber Güvenlik Kanunu, c. 7545.

100 Türkiye Büyük Millet Meclisi, *"Basın K*anunu", Kanun No. 5187, 09 Haziran 2004, https://www.resmigazete.gov.tr/eskiler/2004/06/20040626.htm., erişim 11.06.2025.

101 Türkiye Büyük Millet Meclisi, *"İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun"*.

102 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*.

103 Türkiye Büyük Millet Meclisi, *"Kişisel Verilerin Korunması Kanunu"*.

bireyin burada dikkat çekilen haklarını yok sayıcı birtakım ifade ve riskler içermektedir. Dolayısıyla anayasal çerçeve ihlal edilme tehlikesiyle karşı karşıya kalınmaktadır. Benzer tehlike medya içerikleri ve medyanın kamusal rolü için de geçerlidir.

4.2. *Siber Güvenlik Kanunu'nun İletişim ve Medya ile İlgili Bölümleri*

Teknolojik gelişmelerin sonucu olarak ortaya çıkan siber güvenlik meselesi multidisipliner bir alandır ve uluslararası ilişkilerden ulusal güvenliğe, siyasi uygulamalardan sosyo-kültürel yapıya, ekonomik faaliyetlerden gündelik hayat pratiklerine kadar birçok alanı birbiriyle ilişkili ve etkileşimli biçimde kapsamaktadır. Bu alanlardan en önemlilerin ikisini iletişim ve medya faaliyetleri oluşturmaktadır. İletişim ve medya faaliyetlerinin zarar verici nitelikte kullanılması güvenlik zafiyeti doğurmaktadır. Devletin ilgili kurumları bu zafiyeti ortadan kaldırmak ve adaleti tesis etmek için yasal düzenlemeler yapmaktadır. Aşağıda Siber Güvenlik Kanunu'nun[104] iletişim ve medya ile ilgili kısımları doğrudan ve dolaylı olacak şekilde sınıflandırılmıştır. Bu bağlamda Tablo 3'te yer alan sınıflandırma, Kanun'un "doğrudan" "iletişim araçları ve medya" ile tanımlanıp düzenlenen hükümlerini gösterirken, Tablo 4'teki sınıflandırma Kanun'un "veri aktarımı, altyapı kullanımı ve idari bildirim" gibi "dolaylı" iletişim boyutlarını içeren hükümlerini göstermektedir.

4.2.1. Doğrudan İletişim ve Medya ile İlgili Kısımlar

Aşağıda Siber Güvenlik Kanunu'ndaki doğrudan iletişim ve medya ile ilgili düzenlenen hükümler görülmektedir (Tablo 3).

Tablo 3. Siber Güvenlik Kanunu'ndaki Doğrudan İletişim ve Medya ile İlgili Kısımlar

Madde	İçerik	Açıklama
Madde 3(c), (i), (k)	"Bilişim sistemleri", "siber uzay" ve "varlık" tanımları	Bilgi ve iletişim teknolojileriyle sağlanan hizmetler, elektronik haberleşme ağları ve iletişim yoluyla aktarılabilen veri kavramlarıyla doğrudan iletişim kavramı ve süreci tanımlanmaktadır.
Madde 5(f)	Uluslararası bilgi alışverişi	Başkanlığın, uluslararası kuruluş ve ülkelerle "bilgi alışverişinde bulunma" yetkisi doğrudan iletişim alanıyla ilgilidir.
Madde 6(1)(c)	İletişim altyapısından yararlanma	"Elektronik bilgi işlem merkezlerinden ve iletişim altyapısından yararlanma, iletişim kanalında irtibat kurma" ifadesi doğrudan iletişim hakkına gönderme yapmaktadır.
Madde 12(2)	Medya yayın yasağı	Radyo, televizyon, internet, sosyal medya, gazete, dergi ve diğer tüm kitle iletişim araçlarıyla "yayınlama veya açıklama" yasağı doğrudan iletişim/medya alanına ve kitle iletişim araçlarına müdahaledir.

Tablo 3, iletişim ve medya faaliyetlerine yönelik Anayasal haklar açısından değerlendirildiğinde;

- **Madde 3(c), (i), (k):** Bu maddede "bilişim sistemleri", "siber uzay" ve "varlık" gibi temel kavramların tanımı yapılırken, iletişimin doğrudan bir bileşen olduğu kabul edilmektedir. Bu tanım, Anayasa'nın haberleşme hürriyetini düzenleyen 22. maddesiyle doğrudan ilişkilidir. Anayasa, haberleşmenin gizliliği ve engellenmemesi ilkesini esas almaktadır. Bu kapsamda iletişim teknolojilerinin tümü gizli olma ve engellenmeme ilkesinden faydalanmaktadır.

104 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*, c. 7545.

- **Madde 5(f):** Uluslararası bilgi alışverişine dair yetki verilmesi, hem ifade özgürlüğü[105] hem de bilgiye erişim hakkı[106] çerçevesinde değerlendirilebilir. Ancak bu yetkinin sınırsız veya denetimsiz kullanımı, hak ihlallerine yol açabilir.
- **Madde 6(1)(c):** "İletişim altyapısından yararlanma" doğrudan haberleşme özgürlüğüyle ilgilidir ve Anayasa'daki *"herkes haberleşme hürriyetine sahiptir"*[107] ilkesiyle uyumludur. Bu madde, bireyin elektronik kanallar üzerinden iletişim kurma hakkını tanıyarak anayasal güvence sağlamaktadır.
- **Madde 12(2):** Medya yayın yasağı getiren bu hüküm, Anayasa Madde 28'de güvence altına alınan basın özgürlüğüyle çelişebilme riskini içermektedir. Bu tür bir sınırlama, ancak Anayasa'nın 13. maddesinde belirtilen kriterlerle (kanunilik, ölçülülük, demokratik toplum gereği) sınırlanabilir. Aksi hâlde orantısız ve antidemokratik sansür anlamına gelmektedir.

Yukarıdaki maddeler (Tablo 3), doğrudan anayasal haberleşme özgürlüğü ve basın hakkıyla ilişkilidir. Anayasa'ya uygunluk, ancak sınırlamaların açık, orantılı ve yargı denetimine açık biçimde uygulanmasıyla mümkün olabilecektir.

4.2.2. Dolaylı Olarak İletişim ve Medya ile İlgili Kısımlar

Aşağıda Siber Güvenlik Kanunu'ndaki dolaylı olarak iletişim ve medya ile ilgili düzenlenen hükümler görülmektedir (Tablo 4).

Tablo 4. Siber Güvenlik Kanunu'ndaki Dolaylı Olarak İletişim ve Medya ile İlgili Kısımlar

Madde	İçerik	Açıklama
Madde 3(g)	Varlık tanımı	*"*İletişim yoluyla aktarılabilen *veri"*yi kapsasa da, burada iletişim altyapısından ziyade varlığının kapsamı tanımlanmaktadır. Kavramın soyut uzamına müdahale edilmektedir.
Madde 6(1)(b)	Veri ve log aktarımı	"Ürünler tarafından üretilen veya toplanan veri ve log kayıtlarının Başkanlık sistemlerine aktarılması" dolaylı iletişim (veri işleme) faaliyetidir. Denetim mekanizmasının yetkisi artırılmıştır.
Madde 6(1)(c)	Uzaktan müdahale desteği	Siber olay müdahale desteğinin "yerinde veya uzaktan" sağlanması, teknik iletişim kanalları üzerinden koordinasyon anlamına gelir. Denetim mekanizmasının yetkisi artırılmıştır.
Madde 7(1)(a-b)	Bildirim ve katkı yükümlülüğü	Kurum ve kuruluşların "talep edilen veri, bilgi, belge ve katkıyı zamanında iletme" sorumluluğu, idari iletişim süreçlerine işaret eder. Denetim mekanizmasının yetkisi artırılmıştır.
Madde 8(4)	Denetimde elektronik inceleme	Denetime konu doküman, sistem ve iletişim altyapısının incelenmesi yetkisi, esasen denetim amaçlı dolaylı iletişim (erişim) faaliyetidir. Denetim mekanizmasının yetkisi artırılmıştır.

Tablo 4'teki maddeler iletişimle dolaylı olarak bağlantılı olmakla birlikte anayasal açıdan dikkatle alınması gereken durumlar içermektedir:

- **Madde 3(g):** "Varlık" tanımı ile veri kavramı genişletilirken, bireylerin iletişim verilerinin de bu kapsama alınması mümkün hâle gelmektedir. Bu durum, kişisel verilerin korunması hakkı ve özel hayatın gizliliğiyle (Anayasa Madde 20) ilgilidir.

105 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*, Md. 26.
106 Age, Md. 74.
107 Age, Md. 22.

- **Madde 6(1)(b):** Veri ve log aktarımı, bireylerin dijital faaliyetlerine dair izleme ve kayıt tutma anlamına gelmektedir. Bu uygulama, Anayasa Madde 22'deki haberleşmenin gizliliği ilkesini ilgilidir. Log'ların izinsiz veya sürekli toplanması, ölçülülük ve orantılılık ilkesini ihlal edebilecek riski taşımaktadır.
- **Madde 6(1)(c):** Uzaktan müdahale desteği, haberleşme sistemlerine dışarıdan erişim anlamına gelmektedir. Bu durum da Anayasa Madde 22'nin koruduğu haberleşmenin gizliliğine müdahale niteliği taşımaktadır. Burada meşruiyeti sağlamak için uygulamanın yalnızca yasal ve denetimli çerçevede yapılması koşulu yerine getirilmelidir.
- **Madde 7(1)(a-b):** Bildirim ve katkı yükümlülüğü, kurumların belge sunma yükümlülüğünü düzenlerken idari süreçlerde iletişimi doğrudan etkilemektedir. Bu tür yükümlülüklerin Anayasa'nın "adil yargılanma" ve "özel hayat" hükümleriyle (Madde 36 ve Madde 20) dengelenmesi gerektiği görülmektedir.
- **Madde 8(4):** Elektronik denetim yetkisi, iletişim altyapısına müdahale imkânı sunmaktadır. Bu durum, haberleşmenin ve verilerin denetlenmesi anlamına geldiğinden, ancak mahkeme kararıyla ve sınırlı şekilde yürütüldüğünde Anayasa'ya uygun olabilecektir.

Yukarıdaki maddeler (Tablo 4) dolaylı da olsa iletişim özgürlüğü ve özel hayatın gizliliği gibi temel haklara müdahale niteliği taşımaktadır. Müdahalenin Anayasal ilkelere uygunluğu güç kullanımında ölçülülük, yasal dayanaklılık ve yargı denetimine açıklık (şeffaf) şeklinde yapılmasıyla mümkündür.

Her iki tabloya göre Siber Güvenlik Kanunu'nda yer alan düzenlemeler, anayasal haberleşme özgürlüğü (Madde 22), ifade ve basın özgürlüğü (Madde 26-28), özel hayatın gizliliği (Madde 20) ve bilgiye erişim hakkı (Madde 74) ile yakından ilişkilidir. Bu düzenlemelerin hukuk devleti ilkesine uygun olarak yürütülmesi; ölçülülük, kanunilik ve demokratik toplum ilkeleri doğrultusunda yorumlanması gerekmektedir. Özellikle iletişim ve medya üzerindeki doğrudan ve dolaylı düzenlemelerin yargı denetimine açık olması, temel hakların korunması açısından zorunludur. Tüm bunlar ilgili yasal düzenlemenin yeterli şeffaflığı sağlamadığı ve olumsuz sonuçlanabilecek uygulamalara yol açabileceğini göstermektedir.

4.3. İletişim Süreçleri ve Medya Faaliyetlerine Yönelik Uluslararası Sözleşmeler

Türkiye'de iletişim ve medya faaliyetleri hukuki açıdan uluslararası sözleşmeler, Türkiye Cumhuriyeti Anayasası ve iletişim ile güvenlik alanındaki temel yasa ve mevzuatlar ile düzenlemektedir. Uluslararası düzeyde İfade Özgürlüğü ve İletişim Hürriyeti Hakkı, Uluslararası Medeni ve Siyasi Haklar Sözleşmesi (ICCPR) ve Avrupa İnsan Hakları Sözleşmesi (ECHR) ile güvence altına alınmıştır. ICCPR, ifade ve bilgi alma-verme özgürlüğünü korumaktadır ancak diğer yandan aynı metinler, "ulusal güvenlik" ve "kamu düzeni" gerekçesiyle iktidara "meşru, orantılı ve kanunda öngörülmüş" düzeyde güç kullanma ya da bazı özgürlükleri "kısıtlama"[108] veya "sınırlama" hakkı [109] vermektedir.

108 United Nations, "International Covenant on Civil and Political Rights, ICCPR", United Nations Treaty Series, 1967, https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf?utm, erişim 18.05.2025; The Council of Europe, "European Convention on Human Rights", The Council of Europe Publishing, Rome, 4.XI.1950, 1950, https://www.eods.eu/library/CoE_European%20Convention%20for%20the%20Protection%20of%20Human%20Rights%20and%20Fundamental%20Freedoms_1950_EN.pdf?utm, erişim 12.06.2025.

109 United Nations, *"Article 19: Freedoms of Opinion and Expression"*, United Nations Human Rights Committee, July 2011, https://www.refworld.org/legal/general/hrc/2011/en/83764, erişim 12.06.2025.

Ayrıca ECHR, devletlerin "radyo, televizyon veya sinema kuruluşlarının lisanslanması" gibi teknik sınırlamalarını da meşru kabul etmektedir.[110] Yukarıdaki sınırlama veya kısıtlamalar demokratik bir toplumda "gerekli" olmakla birlikte zorunlu kıstas "ölçülü" ve "şeffaf" olmasıdır.[111]

Türkiye'de ise ifade ve haberleşme özgürlüğünün sınırları temel Anayasal haklar[112] İnternet Ortamında Yapılan Yayınlar[113], Elektronik Haberleşme[114] Kişisel Verilerin Korunması[115] ve en son 2025'te yürürlüğe giren Siber Güvenlik Kanunu[116] ile çerçevelenmiştir ve bu çerçeve iktidara güvenlik gerekçelerini öne sürerek iletişim süreçlerine müdahale yetkisi tanımaktadır. Bu bağlamda İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun içerik ve erişim sağlayıcıları alanlarını düzenleyerek, yetkili kurumlara "kamu güvenliği" ve "suç önleme" gerekçesiyle içerik kaldırma ve erişim engelleme yetkisi tanımaktadır. Yargı kararı veya Bilişim Teknolojileri Kurumu (BTK) kararıyla anlık müdahaleye imkân tanınmaktadır.[117] Elektronik Haberleşme Kanunu, telekomünikasyon işletmecilerine haberleşme verilerini "gizli" tutma yükümlülüğü getirirken, "milli güvenlik", "ulusal savunma", "suç soruşturması", "kamu düzeni" ve "kamu güvenliği" gibi gizliliği ortadan kaldıran istisnalara yer vermektedir.[118] Siber Güvenlik Kanunu ise yetkili mercilerin iletişim altyapıları üzerindeki denetimini genişleterek, "siber tehdit istihbaratı" toplama ve yayma, "Log" kayıtlarına müdahale, veri merkezlerinde arama ve kopya alma gibi olağanüstü yetkiler tanımaktadır.[119] Türk Ceza Kanunu'na göre haberleşmenin gizliliğini ihlal edenlere ve iletişim verilerine izinsiz erişim sağlayanlara, suçun niteliğine göre farklı oranlarda hapis ve/veya para cezası öngörülmektedir.[120]

Yukarıda değinilen kanuni düzenlemelerin ihlali "siber suç" kapsamına girmektedir. Siber suç, literatür bölümünde de değinildiği üzere, bilişim teknolojileri aracılığıyla hem bireysel ve toplamsal açıdan zarar verici, hem de ulusal güvenliği ve kamusal düzeni zedeleyici nitelikler taşımaktadır. Bu bağlamda iletişim ve medya faaliyetleri ile güvenlik arasındaki denge, hem uluslararası hem de ulusal hukukta Anayasa, kanun ve sözleşmelerle düzenlenmiştir. Yapılan düzenlemeler sorunu çözme noktasında önemli katkılar sunmaktadır fakat aynı zamanda hak ve özgürlükleri kısıtlayıcı nitelikler de taşımaktadır. Bir başka ifadeyle, birey ve toplumun sağlıklı bir ortamda yaşaması için oluşturulan kanun ve uygulamaların tersi yönünde de etkileri ortaya çıkarak kamusal alana zarar verme riskini gündeme getirmektedir. Literatürde bu durumu dikkat çeken birçok yaklaşım bulunmaktadır. Aşağıda bu yaklaşımlardan Habermas'ın Kamusal Alan kavramsallaştırmasından yola çıkılarak Kanun'un ortaya çıkardığı olumsuz durum ve risk potansiyeli analiz edilmiştir.

110 The Council of Europe, *"European Convention on Human Rights"*.
111 The Council of Europe, *"Guide on Article 10 of the European Convention on Human Rights", The Council of Europe* Publishing, Strasbourg, 2021. https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/11/Guide_Art_10_ENG.pdf, erişim 12.06.2025.
112 Türkiye Büyük Millet Meclisi, *Türkiye Cumhuriyeti Anayasası*.
113 Türkiye Büyük Millet Meclisi, İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun, c. 5651.
114 Türkiye Büyük Millet Meclisi, *"Elektronik Haberleşme Kanunu"*.
115 Türkiye Büyük Millet Meclisi, *Kişisel Verilerin Korunması Kanunu*.
116 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.
117 Ebru Çetin, "Kitle İletişim Aracı Olarak İnternet ve Hukuk İlişkisi: Türkiye Örneği", *Sosyoloji Dergisi,* 33, 2016, s. 5.
118 Şehriban İpek Aşıkoğlu, "Veri Sorumlularının Aydınlatma Yükümlülüğü -Avrupa Birliği ve Türk Hukukunda-", *Kişisel Verileri Koruma Dergisi*, 1:2, 2019, ss. 55-56.; Reyhan Karcı, "Ulusal Hukukta Kişisel Verilerin Korunması Hakkına İlişkin İstisnai Haller", Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy (Ed.), *Kişisel Verilerin Korunmasına Uzman Bakışı*, KVKK Yayınları, Ankara, 2023, s. 265.
119 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.
120 Pınar Kartal ve Gülfem Işıklar Alptekin, "Türk Ceza Hukukunda Bilişim Sistemine Girme Suçuna İlişkin Değerlendirmeler", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 29:1, 2023, s. 18.

5. Habermas'ın Kamusal Alan Yaklaşımı ve Siber Güvenlik Kanunu Açısından Analizi

Habermas'ın Kamusal Alan kavramı, demokratik siyasetin rasyonel-kritik tartışma zeminini, bu zeminin tarihsel koşullarını ve modernleşme ile birlikte kamusal alanın dönüşümünü açıklamaktadır. Bu yönüyle, iletişim ve medya düzenlemelerinin anayasal etkilerini değerlendirmek için güçlü bir kuramsal araç sunmaktadır.[121] Dolayısıyla siber güvenlik düzenlemesinin medya/iletişim üzerindeki etkisini değerlendirirken, metnin kamusal tartışmayı nasıl dönüştürdüğünü, hangi aktörlere yetki verdiğini ve kamusal alanın niteliğini nasıl etkilediğini Habermasçı kıstaslarla sorgulamak uygun olacaktır. Aşağıdaki tabloda (Tablo 5), Habermasçı yaklaşımın ölçütlerinin temel çerçevesi yer almaktadır:

Tablo 5. Habermas'ın Kamusal Alan Analizi

Analitik Çerçeve	Habermasçı Ölçütler
Erişilebilirlik ve Kapsayıcılık	Kamusal alanın tartışmaya açık, eşit erişime imkân veren bir alan olması gerekir.[122]
Rasyonel-Kritik Tartışma	Kamuoyunun neden temelli, gerekçeye dayanan tartışmalara elverişli olması; çıkar-odaklı propagandaya dönüşmemesi gerekir.[123]
Özerk Medya-Aracı Rolü	Medyanın kamusal denetim ve bilgi sağlama işlevini, devletin tek yanlı yönlendirmesinden korunmuş biçimde yerine getirebilmesi gerekir.[124]
Kamusallıkla Bürokratik-Kamusal İktidarın Ayrımı	Devlet/idare ile kamusal tartışma alanı arasındaki sınırları belli olmalıdır. Devletin bünyesindeki güçlerin de kamusal tartışmayı ("refeodalizasyon" riski) bağlamında bu sınırlar içinde tutması gerekir.[125]

i. Kamusal Alanın Erişilebilirliği ve Kapsayıcılık Ölçütü Analizi

Habermas'a göre kamusal alanın demokratik işlevi, farklı toplumsal aktörlerin rasyonel-kritik tartışmaya erişebilmesiyle doğru orantılıdır.[126] Siber Güvenlik Kanun'un "her türlü medya aracıyla açıklama yasağı" (m. 12–13) gibi geniş kapsamlı sınırlamalarının kamuoyunun erişim ve katılım kanallarını daraltma potansiyeli taşıması[127] kamusal alanın erişebilirliği ve kapsayıcılık ölçütüyle çakışmaktadır. Eğer devletin kurumları bilgi ve tartışma alanlarını tek taraflı biçimde kapatma yetkisine sahip ise, kamusal tartışmanın kapsayıcılığı ve dolayısıyla demokratik meşruiyeti zarar görecektir.

ii. Rasyonel-Kritik Tartışmanın Zedelenmesi Ölçütü Analizi

Habermas'ın ideal kamusal alanı, argümanların en iyi gerekçenin lehine geliştiği; manipülasyonun, pazarlama ve propaganda mekanizmalarının hâkim olmadığı bir alandır.[128] Siber Güvenlik Kanunu'nun geniş yetki tanıyan düzenlemelerinin (idarenin geniş takdir yetkisi ve gizlilik istisnaları gibi[129]) kamunun haber alma, eleştirel kamuoyu oluşturma, denetimi zayıflattığı için kamusal tartışmanın niteliğiyle çakışmaktadır. Başka bir ifadeyle, devletin bilginin dolaşımını kısıtlamaya yönelik mekanizmalarının eleştirel tartışmayı değil, yönlendirilmiş veya susturulmuş bir kamuoyu üretme riskini artırması kamusal-aklın zayıflaması anlamına gelmektedir.

121 Jurgen Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Çev. Thomas Burger), MIT Press, Cambridge, 1989, s. 40.
122 Age, s. 36.
123 Age, ss. 89-109.
124 Habermas, *The Structural Transformation of the Public Sphere*: An Inqu*iry into a Category of Bourgeois Society*, s. 165.
125 Age, s. 232.
126 Age, s. 36-40.
127 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.
128 Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, s. 89-103.
129 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.

iii. Medya Kuruluşlarının Özerkliği ve Kamu-Siyaset Ayrımı Ölçütü Analizi

Habermas'a göre ideal kamusal alanda faydaya yönelik toplumsal düşüncenin etkin olması gerekmektedir. Oysa kitlesel medya, etki alanını derinleştiren dönüşümüyle birlikte kamu otoritesi ve pazar güçlerini kamusal alan üzerinde etkili hâle getirmektedir. Bu da kamusal tartışmaları ticarileştirme ve/veya devletleştirme sonucunu doğurmaktadır.[130] Siber Güvenlik Kanunu'nda tarif edilen yetki genişlemeleri, Habermasçı risk profiliyle örtüşmekte ve dolayısıyla devletin iletişim üzerinde geniş idari müdahale hakları medyanın özerk kamusal tartışma işlevini zayıflatabilme riskini ortaya çıkarmaktadır.

iv. Yönetimsel Güç ve "Refeodalizasyon" Riski

Habermas'ın kamusal alanla ilgili tarihsel analizinde, bürokrasinin ve pazarın kamusal alanı içselleştirip onun işlevini bozduğu "refeodalizasyon" uyarısı önemli yer tutmaktadır.[131] Siber Güvenlik Kanunu'nun vurguladığı yürütme-odaklı yetki tahsisinin[132] şeffaflık ve yargısal denetim mekanizmalarını zayıflatmaya yönelik olması, kamusal alanda güçlü aktörlerin (devlet bürokrasisi ve sermayenin) kamusal gündemi belirleme potansiyelini güçlendirmektedir. Sonuç olarak, yeni bir feodal etki oluşturulduğu için kamusal alanın "entelektüel özerkliği" zedelenmektedir.

Yukarıdaki ölçütler bağlamında, karar süreçlerinin kamuya açıklanabilir derecede şeffaf bir yapı sağlanmasının yanında yargısal denetimin müdahale yetkileri açık ve yargısal denetime tabi olmalıdır. Kanuni düzenlemeler kamusal tartışma alanını kapatmamalıdır. Bağımsız denetim kurumları ve sivil toplum örgütlerinin **güçlendirilerek kam**usal alanın işlevinin korunması sağlanmalıdır.

5.1. Habermas'ın Kamusal Alan Perspektifi Bağlamında Siber Güvenlik Kanunu'nun İletişim Süreçleri ve Medya Faaliyetlerinin Değerlendirmesi

Siber güvenlik ve hukuk arasındaki ilişki, Habermas'ın kamusal alan teorisi açısından değerlendirildiğinde, modern iletişim sistemlerinin yapısal dönüşümünün dijital ortamda yeni bir evreye ulaştığı görülmektedir. Habermas'a göre kamusal alan, yurttaşların serbestçe bir araya gelerek kamusal meseleler üzerine tartışabildikleri, devlet ile toplum arasındaki aracı alanı ifade etmektedir.[133] Dijitalleşen dünyada bu alan, yalnızca fiziksel mekânlarla sınırlı olmayıp, çevrim içi platformlar ve sosyal medya aracılığıyla genişlemiştir. Ancak siber güvenlik düzenlemeleri ve özellikle de Türkiye'de 2025 yılında yürürlüğe giren Siber Güvenlik Kanunu, bu alanın sınırlarını yeniden çizmektedir.

Habermas'ın İletişimsel Eylem Kuramı, toplumsal uzlaşıya ulaşmanın temel yolunun rasyonel, şeffaf ve eşitlikçi iletişim süreçleri olduğunu vurgulamaktadır.[134] Bu perspektiften bakıldığında, siber güvenlik politikaları yalnızca teknik koruma mekanizmaları değil, aynı zamanda iletişimin yapısını ve yönünü belirleyen güç ilişkilerinin de ürünüdür. Hukuki düzenlemeler, kamusal alanın özgür tartışma kapasitesini güçlendirebilme potansiyeline sahiptir ancak hukuk yoluyla aşırı denetim, iletişimsel rasyonaliteyi zayıflatma riski taşımaktadır.

130 Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, s. 196-232.

131 Habermas, *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*, s. 232.

132 Türkiye Büyük Millet Meclisi, *Siber Güvenlik Kanunu*.

133 Habermas, *The Structural Transformation of the Public Sphere: An inquiry into a Category of Bourgeois Society*, s. 27.

134 Habermas, *The Theory of Communicative Action, Volume One: Reason and the Rationalization of Society*.

Siber güvenlik ve hukuk etkileşimi, çok hukuklu bir yapıya evrilirken, bu normatif çoğulluk iletişimsel eylem süreçlerinde yeni sorunlar doğurmaktadır. Örneğin, farklı kural koyucuların (devlet, devletin yetkilendirdiği kurumlar, uluslararası örgütler, teknoloji şirketleri vb.) siber alanda eş zamanlı etkili olması, Habermas'ın yaşam dünyasının sömürgeleştirilmesi kavramıyla açıklanabilecek bir durumu ortaya çıkarmaktadır.[135] Devletin güvenlik gerekçesiyle dijital iletişim alanını düzenlemesi, bireylerin kamusal tartışmalara katılımını sınırlayabilme ve iletişim alanını piyasa/sermaye ya da bürokrasi mantığıyla şekillendirme olasılığını artırmaktadır.

Bu bağlamda, 2025 tarihli Siber Güvenlik Kanunu'nun anayasal haklar, iletişim sosyolojisi, medya çalışmaları ve siyasal iletişim açısından iki yönlü bir etkisi olduğu görülmektedir. Bir yandan, siber tehditlere karşı kamusal güvenliği artırarak kamusal alanın güvenli işleyişini sağlamayı hedeflerken, diğer yandan, iletişim akışını düzenleme ve denetleme yetkisi, kamusal tartışma özgürlüğü üzerinde sınırlayıcı etki oluşturmaktadır. Habermas'ın demokratik meşruiyet vurgusu dikkate alındığında,[136] bu tür düzenlemelerin meşruluğu, ancak kapsayıcı, şeffaf ve yurttaşların katılımına açık karar alma süreçleriyle sağlanabilecektir.

Sonuç olarak, siber güvenlik ile hukuk arasındaki ilişki, Habermas'ın Kamusal Alan ve İletişimsel Eylem Teorisi çerçevesinde değerlendirildiğinde hem güvenlik hem de özgürlük boyutlarının dengelenmesini gerektiren dinamik bir alan olarak karşımıza çıkmaktadır. Türkiye'de yürürlüğe giren Siber Güvenlik Kanunu, dijital kamusal alanın sınırlarını ve işleyişini doğrudan etkileyen bir düzenleme olarak, kurumların şeffaf faaliyetleri ve demokratik iletişim kültürünün korunması açısından dikkatle izlenmelidir.

Sonuç ve Öneriler

Dijitalleşmenin yaygınlaşmasıyla birlikte siber güvenlik konusu hem bireysel hakların korunması, hem ulusal güvenlik, hem de uluslararası ilişkiler ve uluslararası güvenlik açısından merkezi bir politika alanı haline gelmiştir. Türkiye'de 19 Mart 2025'te yürürlüğe giren 7545 sayılı Siber Güvenlik Kanunu, teknolojik tehditlere karşı hukuki boşlukları kapatmayı ve kapsamlı bir savunma mekanizması kurmayı amaçlamaktadır. Ancak kanunun iletişim ve yeni medya faaliyetleri üzerindeki doğrudan ve dolaylı etkileri, özgürlük–güvenlik dengesi açısından ciddi tartışmalara açıktır. Örneğin, son dönem hukuk felsefesinin önemli isimlerinden Rawls'un adalet prensiplerine göre güvenlik politikalarının temel hakların korunması adaletin öncelikli koşuludur.[137] Oysa Kanun'un genel çerçevesi bu koşulu görmezden gelinmeye açık hâle getirmektedir. Gözetim kuramlarının tümünde olduğu gibi[138], Solove'un mahremiyet analizlerine göre Kanun'un yetki kapsamı toplanan verinin kullanım biçimlerinin çeşitli zararlar doğurabileceğini göstermektedir.[139]

Floridi'nin "bilgi etiği" kuramına göre geniş log toplama, uzun süreli saklama, merkezi veri aktarımı ve medya kısıtlamaları infosferin bütünlüğünü ve bireylerin bilgi özerkliğini zedeleyerek bilgi varlıklarına etik zarar riski doğurduğundan, bu müdahalelerin

135 Jurgen Habermas, *The Theory of Communicative Action, Volume Two: Lifeworld and System: A Critique of Functionalist Reason* (Çev. Thomas McCarty), Beacon Press, Boston, 1987, s. 232.

136 Jurgen Habermas, *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (Çev. William Rehg), MIT Press, Cambridge, 1996, s. 307.

137 Rawls, *Bir Adalet Teorisi*.

138 Zygmunt Bauman, *Akışkan Gözetim* (Çev. Elçin Yılmaz), Ayrıntı Yayınları, İstanbul, 2016.; Castells, *Ağ Toplumunun Yükselişi*; Deleuze & Guattari, *A Thousand Plateaus: Capitalism and Schizophrenia*; Foucault, *Hapishanenin Doğuşu*.

139 Solove, *Understanding Privacy*.

"zarar vermeme", ölçülülük, şeffaflık, denetlenebilirlik ve bilgi yöneticiliği (*stewardship*) ilkeleri[140] bağlamında Kanun'un açık şekilde sınırlandırılması gerektiğini göstermektedir. Baudrillard'ın teknolojinin/dijitalleşmenin geldiği aşamayı tartıştığı "simülasyon/simülakr" kuramında sanal olanın gerçeğin yerine geçtiğine yönelik "hipergeçeklik" kavramsallaştırmasına[141] referansla, siber uzay üzerindeki devlet müdahalelerinin gerçek dünyadaki iletişim ve toplumsal ilişkiler üzerinde derin etkileri olması, siber uzayda olan her şeyin gündelik hayatın her anını ve özellikle iletişim süreçleri ve medya faaliyetleri üzerinde de büyük bir etkiye sahip olduğunu göstermektedir. Dolayısıyla buradaki adımların daha dikkatli atılması kamusal fayda için bir zorunluluktur. Buradan da anlaşılacağı üzere, Kanun'un yetkilendirme ve icraat boyutları medya faaliyetleri de dâhil tüm iletişim süreçlerinde olduğu kadar kişisel bilgi ve mahremiyet haklarına yönelik ihmal veya kasıtlı/keyfi uygulamaları zemin hazırlama potansiyeline sahiptir. Kuramsal örnekler çoğaltılabilir çünkü Kanun literatürün (teknoloji, güvenlik, kültür, siyaset özgürlük, adalet, kişisel haklar vb.) tartıştığı birçok kuramsal yaklaşımla değerlendirilebilir niteliktedir. Kapsamı daraltan bu çalışma, Kanun'un iletişim süreçleri ve yeni medya üzerindeki etkilerini anayasal haklar perspektifiyle Habermas'ın Kamusal Alan kavramı çerçevesinde uluslararası sözleşmelere de değinerek analiz etmiştir.

Kanun'un 12. maddesi radyo, televizyon, internet ve sosyal medya dâhil tüm kitle iletişim araçlarıyla yapılan yayınlara yönelik yasaklar getirmekte; m. 12(2) gibi hükümler medyaya geniş kapsamlı kısıtlamalar öngörmektedir. Bu düzenlemeler, Türkiye Cumhuriyeti Anayasası'nda güvence altına alınmış olan basın (m. 28) ve ifade özgürlüğü (m. 26) ile Avrupa İnsan Hakları Sözleşmesi (AİHS/ECHR) Madde 10'un "demokratik toplum gerekliliği", "gerekli ve orantılı" kısıtlama kriterleri açısından sorunlu bir zemin oluşturmaktadır. Mevcut hâliyle bu kısıtlamaların ölçülülük, açıklık ve yargısal denetime yeterince tâbi olmadığı ve bunun sansür riskinin yanında keyfî uygulamalara zemin hazırladığı anlaşılmaktadır.

Madde 6(1)(c) uyarınca yetkililere tanınan iletişim altyapısına uzaktan müdahale yetkisi, haberleşmenin gizliliği ve Anayasa'nın haberleşme hürriyeti (m. 22) ile açıkça çatışma potansiyeli taşımaktadır. Bu tür doğrudan müdahaleler, kamusal tartışma ortamını zayıflatmakta ve Habermas'ın iletişimsel eylem perspektifinden bakıldığında kamusal diyaloğun özerkliği zarar görebilmektedir.

Madde 7(1)(a–b) ile kurumlara yüklenen "veri ve log aktarımı" yükümlülüğü; log kayıtlarının iki yıl saklanması ve anonimleştirme süreçlerinin denetimsizliği, kişisel verilerin korunması ilkeleri ve özel hayatın gizliliği (Anayasa m. 20; KVKK) ile uyumlu görünmemektedir. Madde 6(1)(b) kapsamında Başkanlığa aktarılan log kayıtları iletişimin gözetlenmesi anlamına gelmektedir. Solove'un çok boyutlu mahremiyet analizine göre bu tür uygulamalar bireylerin bilgi özerkliğini zayıflatmaktadır. Anonimleştirme uygulamalarının şeffaf olmaması ve denetim mekanizmalarının belirsizliği, veri suiistimaline ve sosyal mühendislik yoluyla kötüye kullanıma zemin hazırlayabilme riskini taşımaktadır.

Madde 3(c), (i) ve (k) ile tanımlanan "bilişim sistemleri" ve "siber uzay" gibi kavramlar, iletişim özgürlüğünü doğrudan etkileyen teknik düzenlemeleri içermektedir. Ancak bu tanımların ve düzenlemelerin Anayasa'nın öngördüğü hukuki güvencelerle (yasallık ilkesi) birlikte demokratik toplum bağlamında ölçülülük ve gereklilik kriterlerini sağlayıp sağlamadığı tartışmalıdır. Teorik olarak uygulama süreçlerine kanunilik yeterli olsa bile demokratik denetim kriterlerinin gözetilmememe sorunu ortaya çıkmaktadır.

140 Floridi, *"Information Ethics: On the Philosophical Foundation of Computer Ethics"*.
141 Jean Baudrillard, *Simülasyon ve Simülakr* (Çev. Oğuz Adanır), Doğu Batı Yayınları, Ankara, 2011, s. 13.

BM, AB ve NATO gibi kuruluşların siber güvenlik politikaları genellikle şeffaflık ve insan hakları odaklı standartlar içerirken, Türkiye'deki düzenlemelerde "ulusal güvenlik" vurgusunun geniş tanımlanması bu standartlardan sapma riski taşımaktadır. Özellikle Madde 5(f) ile Siber Güvenlik Başkanlığı'na verilen "uluslararası bilgi alışverişi" yetkisinin kapsam ve denetiminin belirsiz olması uluslararası normlarla uyum kaygısını artırmaktadır. Yerel mevzuata uluslararası normların yeterince entegre edilmemesi, uzun vadede iş birliğini zayıflatabilme ve politikaların meşruiyetini azaltma riski taşımaktadır.

Madde 8(4) ile yetkililere tanınan "elektronik inceleme" yetkisi ve sistemlere ilişkin denetim kapasitesinin genişletilmesi, iletişim altyapısında kalıcı gözetim mekanizmalarının kurulmasına yol açabilecek niteliktedir. Schlink'in devlet koruma sorumluluğu ile bireysel özgürlükler arasındaki gerilim vurgusu burada görünür hâle gelmektedir. Kanun ile doğrudan yasaklamanın ötesinde, gözetim ve veri işleme süreçleri üzerinden yürüyen dolaylı müdahaleler devletin otoriterliği bağlamında daha yaygın ve kalıcı etkiler doğurabilecek potansiyele sahiptir.

Yukarıdaki özet, Kanun'un genel çerçevesinin Habermas'ın ideal kamusal alan kavramındaki toplumsal faydaya yönelik açıklamalarıyla tezatlık göstermektedir. Habermas'ın Kamusal Alan Teorisi, kamusal tartışmanın serbestliği ve toplumsal uzlaşının iletişimsel yollarla sağlanmasının önemini ortaya koymaktadır. Bu bağlamda değerlendirildiğinde, Kanun'un mevcut düzenlemelerinin hem kamusal alanın işlevselliğini zayıflatma hem de adalet ve mahremiyet standartlarıyla çelişme riski taşıdığı sonucuna ulaşılmaktadır. Yine bu çerçeveye göre Siber Güvenlik Kanunu'nun getirdiği geniş kapsamlı kısıtlamalar ve denetimsizlik riski, kamusal tartışmanın sağlıklı işlemesi için gerekli olan iletişimsel koşulları zedelemektedir. Habermas'a göre kamusal alan, farklı toplumsal aktörlerin eşit koşullarda rasyonel-eleştirel tartışmaya katıldığı ve kamuoyunun özgürce oluştuğu bir mekân ve/veya ortamdır. Bu mekân ve/veya ortamın işlerliği, sansürsüz ifade, erişim serbestliği ve konuşma alanının korunmasına dayanmaktadır. Kanun'un medya üzerindeki yayın yasakları, altyapıya müdahale yetkileri ve geniş veri toplama uygulamaları, eşitlikçi ve açıklığa dayalı iletişim koşullarını bozarak kamusal aklın oluşumunu engelleyebilme potansiyelini taşımaktadır. Bu şekilde oluşan kamusal alanda ise toplumun kendini yöneten bir kamuoyuna dönüşme kapasitesinin zayıflama ihtimali yüksektir.

Bu nedenle Habermasçı perspektif, politika önerilerini normatif bir zemine oturtmak için yol göstericidir. Kamusal alanın korunması, sadece ifade özgürlüğünün teknik garantileriyle değil, aynı zamanda şeffaflık, bağımsız denetim ve yargısal denetim mekanizmalarının tesis edilmesiyle mümkündür. İleri teknoloji ve güvenlik gerekçeleriyle yapılan düzenlemeler, kamusal tartışma alanının asgari koşullarını koruyacak şekilde yeniden biçimlendirilmelidir. Aksi takdirde güvenlik politikaları, kamusal rasyonaliteyi ve demokratik meşruiyeti zayıflatma riski taşıyacaktır. Habermas'ın vurguladığı iletişimsel eylem ve kamusal rasyonalite ilkeleri, Kanun'un uygulanmasında ölçülülük, hesap verebilirlik ve katılımcılığı güçlendirecek reformların temel normatif dayanağını oluşturmaktadır.

Kanun'un iletişim ve medya üzerindeki olumsuz etkilerini azaltmak ve anayasal/uluslararası normlarla uyumu sağlamak için şu tedbirler önerilmektedir:

i. Ölçülülük ve Yargısal Denetim: Kısıtlayıcı hükümlerin Anayasa m. 13'te belirtilen "demokratik toplum gerekliliği" çerçevesinde yeniden tanımlanarak tüm istisnai tedbirler bağımsız yargı denetimine tabi kılınmalıdır.

ii. Şeffaf Veri Yönetimi ve Bağımsız Denetim: Log ve kişisel veri toplama/saklama süreçleri için şeffaf veri yönetimi, açık kurallar, denetlenebilir yapılar ve bağımsız denetim mekanizmaları oluşturulmalıdır.

iii. Uluslararası Uyum: BM, AB ve NATO gibi uluslararası kuruşların standartlarıyla uyumlu mevzuat uyarlamaları yapılarak uluslararası normlarla entegrasyon sağlanmalıdır.

iv. Siber Okuryazarlık ve Adalet Bilinci: Toplum, medya çalışanları ve sivil toplum dijital haklar, veri güvenliği ve yeni medya okuryazarlığı konularında eğitilerek hak ve sorumluluk bilinci güçlendirilmelidir.

v. Teknoloji-Politika Entegrasyonu: Siyaset kurumu ve bürokratik yapının hızla şekilde sektörle birlikte hareket etmesi sağlanmalı ve yapay zekâ, blokzincir gibi ileri teknolojilerin mevzuata entegrasyonu konusunda disiplinlerarası düzenlemeler geliştirilmelidir.

vi. Alanyazın Çalışmaları: Gelecek araştırmalar Kanun'un uygulamadaki yansımalarını izlemeye odaklanarak medya mensupları, sivil toplum ve hukukçuların deneyimleri temel alınarak niteliksel çalışmalar yoğunlaştırılmalıdır. Ayrıca ileri teknolojilerin (yapay zekâ, blokzincir vb.) iletişim süreçleri, ifade özgürlüğü ve mahremiyet ve medya faaliyetleri üzerindeki etkileri bakımından disiplinlerarası nitelikli araştırmalar yapılmalıdır.

Sonuç olarak, 7545 sayılı Siber Güvenlik Kanunu teknolojik tehditlere karşı önemli engelleyici mekanizmalar getirse de uygulama biçimi ve denetim eksiklikleri nedeniyle ifade ve iletişim özgürlükleri ile özel hayatın gizliliği açısından ciddi riskler barındırmaktadır. Kanun'un demokratik meşruiyeti ve uzun vadeli etkinliği, şeffaflık, ölçülülük, yargısal denetim ve uluslararası standartlarla uyum yoluyla güvence altına alınmalıdır. Bu çalışma, siber güvenlik ile iletişim özgürlüğü arasındaki adalete dayalı, katılımcı dengenin nasıl kurulabileceğine yönelik hem akademik hem de politika yapıcı tartışmalara katkı sunmayı amaçlamıştır.

Çıkar Çatışması

Bu çalışmada çıkar çatışması teşkil edebilecek durum ve/veya ilişki bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Bu çalışma oluşturulurken, araştırma konusuyla ilgili Türkçe dışındaki literatürün daha iyi anlaşılabilmesi amacıyla çeviri desteği almak ve metnin bazı bölümlerinde daha akıcı bir dil oluşturmak için yapay zekâdan yararlanılmıştır.

KAYNAKÇA

Basılı Kaynaklar

AKÇAKANAT Özen ÖZDEMİR Ozan ve MAZAK Mehmet (2021). "İşletmelerde Siber Güvenlik Riskleri ve Bilgi Teknolojileri Denetimi: Bankaların Siber Güvenlik Uygulamalarının İncelenmesi", *Mehmet Akif Ersoy Üniversitesi Uygulamalı Bilimler Dergisi*, 5:2, 246-270.

AKSOĞAN Mustafa BAYER Harun GÜLADA Mehmet Ozan ve ÇELİK Enes (2018). "İletişim Fakültesi Öğrencilerinin Siber Güvenlik Farkındalığı: İnönü Üniversitesi Örneği", *Kesit Akademi Dergisi,* 13, 271-288.

AKYEŞİLMEN Nezir (2018). *Disiplinlerarası Bir Yaklaşımla: Siber Politika & Siber Güvenlik*, Orion Kitabevi, Ankara.

ALTINTOP Mevlüt (2021). *Zygmunt Bauman Sosyolojisinde İletişim Olgusu*, Kitapyurdu Doğrudan Yayıncılık, İstanbul.

ANDERSON Ross (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems*, (3. Baskı), Wiley, New York.

AŞIKOĞLU Şehriban İpek (2019). "Veri Sorumlularının Aydınlatma Yükümlülüğü-Avrupa Birliği ve Türk Hukukunda-", *Kişisel Verileri Koruma Dergisi*, 1:2, 41-65.

ATA Zeynep (2024). "Sosyal Medyada Suç Korkusunun Oluşması ve Yayılması: X Örneği", *Dicle Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 37, 382-398.

AVŞAR Zakir ve ÖNGÖREN Gürsel (2010). *Bilişim Hukuku*, Türkiye Bankalar Birliği, İstanbul.

BAUDRILLARD Jean (2011). *Simülasyon ve Simülakr* (Çev. Oğuz Adanır), Doğu Batı Yayınları, Ankara.

BAUMAN Zygmunt (2016). *Akışkan Gözetim* (Çev. Elçin Yılmaz), Ayrıntı Yayınları, İstanbul.

BECK Ulrich (2011). *Risk Toplumu: Başka Bir Modernliğe Doğru* (Çev. Kazım Özdoğan ve Bülent Doğan), İthaki Yayınları, İstanbul.

BİLGEHAN A. Deniz (2025). "Siber Güvenlik Başkanlığının Düzenlenişine Dair Değerlendirme", *İstanbul Medipol Üniversitesi Hukuk Fakültesi Dergisi*, 12:1, 63-88.

BİTİRİM OKMEYDAN Selin. (2017). "Postmodern Kültürde Gözetim Toplumunun Dönüşümü: 'Panoptikon'dan 'Sinoptikon' ve 'Omniptikon'a", *AJIT-e: Academic Journal of Information Technology*, 8:30, 45-69.

CASTELLS Manuel (2008). *Ağ Toplumunun Yükselişi* (Çev. Ebru Kılıç), İstanbul Bilgi Üniversitesi Yayınları, İstanbul.

CLARKE Ronald V., ve CORNISH Derek B. (1985). "Modeling Offenders' Decisions: A Framework for Research and Policy", *Crime and Justice*, 6, ss. 147-185.

COOMBS W. Timothy (2022). *Ongoing Crisis Communication: Planning, Managing, and Responding*, 6. Baskı, Sage Publications, Florida.

CROWLEY David ve HEYER Paul (2019). *İletişim Tarihi* (Çev. Berkay Ersöz), Siyasal Kitabevi, Ankara.

ÇAKIR Hüseyin ve TAŞER Murat (2023). "Türkiye'de Yapılan Siber Güvenlik Faaliyetlerinin ve Eğitim Çalışmalarının Değerlendirilmesi", *Gazi Üniversitesi Fen Bilimleri Dergisi Part C: Tasarım ve Teknoloji*, 11:2, 347-366.

ÇELİK Soner (2018). "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *ARHUSS,* 1: 2, 110-119.

ÇETİN Ebru (2016). "Kitle İletişim Aracı Olarak İnternet ve Hukuk İlişkisi: Türkiye Örneği", *Sosyoloji Dergisi*, 33, 1-13.

DARICILI Ali Burak (2019). "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Siber Güvenlik Modeli İçin Öneriler", *TESAM Akademi Dergisi*, 6:2, 11-33.

DELEUZE Gilles ve GUATTARI Félix (1987). *A Thousand Plateaus: Capitalism and Schizophrenia*, University of Minnesota Press, Minneapolis.

EFE Ahmet (2017). *Bilişim Suçları ve Türk Ceza Hukukundaki Yeri*, Seçkin Yayıncılık, Ankara.

ELDEM Tuba, (2021). "Uluslararası Siber Güvenlik Normları ve Sorumlu Siber Egemenlik", İstanbul Hukuk Mecmuası, 79: 1, 347-378.

ERDEM Merve ve Gürkan ÖZOCAK (2019). "Siber Güvenliğin Sağlanmasında Uluslararası Hukukun ve Türk Hukukunun Rolü", *Ankara Üniversitesi Hukuk Fakültesi Dergisi,* 68:1, 127-212.

ERGÜN İsmail (2008). *Siber Suçların Cezalandırılması ve Türkiye'de Durum*, Adalet Yayınevi, Ankara.

FLORIDI Luciano (1999). "Information Ethics: On the Philosophical Foundation of Computer Ethics", *Ethics and Information Technology*, 1, 37-56.

FOUCAULT Michel (1992). *Hapishanenin Doğuşu* (Çev. Ali Yaşar Kılıçbay), İmge Kitabevi Yayınları, Ankara.

GÖLE Nilüfer (1986). *Mühendisler ve İdeoloji* (Çev. Eli Levi), İletişim Yayınları, İstanbul.
GÜNDÜZ Muhammed Zekeriya ve DAŞ Resul (2020). "Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik", *Iğdır Üniversitesi Fen Bilimleri Enstitüsü Dergisi*, 10:2, 970-984.
HABERMAS Jurgen (2001). İletişimsel Eylem Kuramı (Çev. Mustafa Tüzel), Kabalcı Yayıncılık, İstanbul.
HABERMAS Jurgen (1984). *The Theory of Communicative Action* (Çev. Thomas McCarty), Beacon Press, Boston.
HABERMAS Jurgen (1987). *The Theory of Communicative Action, Volume Two: Lifeworld and System: A Critique of Functionalist Reason* (Çev. Thomas McCarty), Beacon Press.
HABERMAS, Jurgen (1989). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Çev. Thomas Burger), MIT Press, Cambridge.
HABERMAS Jurgen (1991). *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society* (Çev. Thomas Burger ve Frederick Lawrence), MIT Press, Cambridge.
HABERMAS Jurgen (1996). *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy* (Çev. William Rehg), MIT Press, Cambridge.
HABERMAS, Jurgen (2006). "Political Communication in Media Society: Does Democracy still Enjoy an Epistemic Dimension?", *Communication Theory*, 16:4, 411-26.
HATİPOĞLU AYDIN Fatma (2023). *Siber Güvenlik ve Kişisel Verilerin Korunması: Hukuki Bir Değerlendirme*, Adalet Yayınevi, Ankara.
HEIDEGGER Martin (1977). *The Question Concerning Technology and Other Essays*, Harper & Row, New York.
JENKINS Henry (2006). *Convergence Culture: Where Old and New Media Collide*, New York University Press, New York.
KARASOY H. Alpay ve BABAOĞLU Pelin (2021). "Türkiye'de Siber Güvenlik: Yasal ve Kurumsal Altyapı", *Yasama Dergisi*, 44, 123-155.
KARCI Reyhan (2023). "Ulusal Hukukta Kişisel Verilerin Korunması Hakkına İlişkin İstisnai Haller", Pınar Çağlayan Aksoy ve Hüseyin Can Aksoy (Ed.), *Kişisel Verilerin Korunmasına Uzman Bakışı*, KVKK Yayınları, Ankara, 243-302.
KARTAL Pınar ve IŞIKLAR ALPTEKİN Gülfem (2023). "Türk Ceza Hukukunda Bilişim Sistemine Girme Suçuna İlişkin Değerlendirmeler", *Marmara Üniversitesi Hukuk Fakültesi Hukuk Araştırmaları Dergisi*, 29:1, 16-31.
LOADER Brian D. ve THOMAS Douglas (2000). *Cybercrime: Law Enforcement, Security and Surveillance in the Information Age*, Routledge, London.
LUHMANN Niklas (1996). *Social Systems*, Stanford University Press, Stanford.
NEZGİTLİ Sena ve Recep BENZER (2020). "Avrupa Birliği Siber Güvenlik Kanunu", *Bilişim Sistemleri ve Yönetim Araştırmaları Dergisi*, 2:1, 10-17.
NİŞANYAN Sevan (2022). *Nişanyan* Sözlük Çağdaş Türkçenin Etimolojisi, Liberus, İstanbul.
ÖNAL Mehmet Alperen (2021). "Siber Uzay Ve Güvenlik İlişkisi Bağlamında Siber Güvenliğin Boyutları", *Hitit Ekonomi ve Politika Dergisi*, 1:2, 114-23.
ÖZDEMİR Gülşah (2025). "Uluslararası Güvenlikte Siber Tehditlerin Yükselişi ve Stratejik Savunma Politikaları", *Elektronik Sosyal Bilimler Dergisi*, 24:1, 1-20.
POMERANTSEV Peter (2021). *Bu Propaganda Değil Gerçeğe Karşı Savaş Maceraları* (Çev. Alain Matalon), Mundi Kitap, İstanbul.
RAWLS John (2017). *Bir Adalet Teorisi* (Çev. Vedat Ahsen Coşar), Phoenix Yayınevi, Ankara.
RAWLS John (1971). *A Theory of Justice*, Harvard University Press, Cambridge.
SCHNEIER Bruce (2004). *Secrets and Lies: Digital Security in a Networked World*, New York: Wiley.
SHANNON, Claude E. (1948). "A Mathematical Theory of Communication", *Bell System Technical Journal*, 27:3, 379-423, https://archive.org/details/bstj27-3-379
SOLOVE Daniel J. (2007). *Understanding Privacy*, Harvard University Press, Cambridge.
TANENBAUM Andrew S. ve BOS Herbert (2015). *Modern Operating Systems*, Pearson, New Jersey.
TBMM (2020). *Türkiye Cumhuriyeti Anayasası*, TBMM Basımevi, Ankara.
The Council of Europe (2021). *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence*, The Council of Europe Publishing, Strasbourg.
Türk Dil Derneği (2012). *Türkçe Sözlük*, Türk Dil Derneği, Ankara.
Türk Dil Kurumu (2005). *Türkçe Sözlük*, 10. Baskı, 2., Türk Dil Kurumu, Ankara.
VOLKMAN Ernest (2004). *Casusluk* (Çev. Sevde Kubilay ve Melike Atik), Truva Yayınları, İstanbul.
WALL David S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*, Polity Press, Cambridge.

WIENER Norbert (2019). *Cybernetics or Control and Communication in the Animal and the Machine*, 3. Baskı, MIT Press, Cambridge.

YILDIRIM Arzu (2024). "Türkiye'nin Siber Güvenlik Politikasının Eylem Planları Üzerinden Analizi", *Organizasyon ve Yönetim Bilimleri Dergisi*, 16:1, 23-47.

YILMAZ Onur (2018). "Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik", *Cyberpolitik Journal*, 4, 22-43.

ZUBOFF Shoshana (2018). *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, Public Affairs, New York.

İnternet Kaynakları

BIÇAKCI Salih ERGUN Doruk ve ÇELİKPALA Mitat (2015).*"Türkiye'de Siber Güvenlik"*, Ekonomi ve Dış Politika Araştırmalar Merkezi (EDAM) Siber Politika Kâğıtları Serisi 1, İstanbul, https://edam.org.tr/wp-content/uploads/2015/12/EDAM_TR_Siber_Guv_1.pdf, erişim 16.05.2025.

Bilgi Teknolojileri ve İletişim Kurumu (2025). "Siber Güvenlik Kurulu", *Bilgi Teknolojileri ve İletişim Kurumu*, https://www.btk.tr/siber-guvenlik-kurulu, erişim 15.08.2025.

ÇINAR Enes (2025). "Bilişim Suçları", Çınar Hukuk Bürosu, https://www.cinarhukukburosu.com/blog/bilisim-suclari, erişim 11.05.2025.

ÇAKIRCA Ege ÇAKIRCA Tuna ve ÇELİK Oylum (2025). "Türkiye'de Siber Güvenliğin Yeni Yasal Çerçevesi: 7545 Sayılı Siber Güvenlik Kanunu", *Turkish Law Blog*, https://turkishlawblog.com/insights/detail/turkiyede-siber-guvenligin-yeni-yasal-cercevesi-7545-sayili-siber-guvenlik-kanunu, erişim 15.08.2025.

DAĞISTANLI Hüseyin Cem ve SARICA Abdullah (2025). "Cumhurbaşkanlığına bağlı ofis ve politika kurullarına ilişkin düzenlemeler Resmi Gazete'de", *Anadolu Ajansı (AA)*, https://www.aa.com.tr/tr/gundem/cumhurbaskanligina-bagli-ofis-ve-politika-kurullarina-iliskin-duzenlemeler-resmi-gazetede/3522186, erişim 15.08.2025.

Siber Suçlarla Mücadele Daire Başkanlığı (2025). "Siber Suç Nedir?", *Emniyet Genel Müdürlüğü (EGM)*, https://www.egm.gov.tr/siber/sibersucnedir, erişim 16.05.2025.

ESEN SAKAR Gözde NART Ece ve ÜSTÜNDAĞ Pelinsu (2025). "7545 Sayılı Siber Güvenlik Kanunu", *Mondaq*, https://www.mondaq.com/turkey/security/1606732/7545-say%C4%B1l%C4%B1-siber-g%C3%BCvenlik-kanunu, erişim 15.08.2025.

European Data Protection Supervisor (2013). *Opinion of the European Data Protection Supervisor on the Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace*, European Data Protection Supervisor (EDPS), https://www.edps.europa.eu/sites/default/files/publication/13-06-14_cyber_security_en.pdf, erişim15.08.2025

Govinsider (2025). "Digital Transformation Office (DTO) of the Presidency of the Republic of Türkiye", *Govinsider*, https://govinsider.asia/intl-en/digital-government/country/turkey?utm_source=chatgpt.com&type=info&agency=digital-transformation-office-dto-of-the-presidency-of-the-republic-of-turkiye-80, erişim 15.08.2025.

Millî İstihbarat Teşkilatı (2025). "Yetki ve Sorumluluklar", *Millî İstihbarat Teşkilatı*, https://www.mit.gov.tr/yetki-ve-sorumluluklar.html, erişim15.08.2025.

STINE Kevin M. QUILL Kim ve WITTE Gregory A. (2014). "Framework for Improving Critical Infrastructure Cybersecurity", *National Institute of Standards and Technology*, https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity, erişim 20.05.2025.

The Council of Europe (2021). *Guide on Article 10 of the European Convention on Human Rights*, The Council of Europe Publishing, Strasbourg, https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2020/11/Guide_Art_10_ENG.pdf?utm, erişim 10.05.2025.

The Council of Europe (1950). *European Convention on Human Rights*, The Council of Europe Publishing, Strasbourg, https://www.eods.eu/library/CoE_European%20Convention%20for%20the%20Protection%20of%20Human%20Rights%20and%20Fundamental%20Freedoms_1950_EN.pdf?utm, erişim 19.05.2025.

The Council of Europe (2003). *Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems*, The Council of Europe Publishing, Strasbourg, https://rm.coe.int/168008160f, erişim 15.08.2025.

Türkiye Büyük Millet Meclisi (2004). *Basın Kanunu*, Kanun No. 5187, https://www.resmigazete.gov.tr/eskiler/2004/06/20040626.htm, erişim 16.05.2025.

Türkiye Büyük Millet Meclisi (2008). *Elektronik Haberleşme Kanunu*, Kanun No. 5809, https://resmigazete.gov.tr/eskiler/2008/11/20081110M1-3.htm, erişim 15.05.2025.

Türkiye Büyük Millet Meclisi (2007). İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Ed*ilmesi Hakkında Kanun*, Kanun No. 5651, https://resmigazete.gov.tr/eskiler/2007/05/20070523-1.htm, erişim 16.05.2025.

Türkiye Büyük Millet Meclisi (2016). *Kişisel Verilerin Korunması Kanunu*, Kanun No. 6698, https://www.resmigazete.gov.tr/eskiler/2016/04/20160407-8.pdf, erişim 15.05.2025.

Türkiye Büyük Millet Meclisi (2025). *Siber Güvenlik Kanunu*, Kanun No. 7545, https://resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm, erişim 13.05.2025.

Türkiye Büyük Millet Meclisi (1991). *Türk Ceza Kanunun Yürürlükten Kaldırılmış Hükümleri, 767 Mülga 765 sayılı Türk Ceza Kanunu On Birinci Bab Bilişim Suçları*, ss. 106-122., https://mevzuat.gov.tr/MevzuatMetin/5.3.765.pdf, erişim 15.05.2025.

United Nations (2011). *"Article 19: Freedoms of Opinion and Expression"*, United Nations Human Rights Committee, https://www.refworld.org/legal/general/hrc/2011/en/83764?utm, erişim 18.05.2025.

United Nations (1967). *"International Covenant on Civil and Political Rights (ICCPR)*", United Nations Treaty Series, https://treaties.un.org/doc/treaties/1976/03/19760323%2006-17%20am/ch_iv_04.pdf?utm, erişim 18.05.2025.

Ulusal Siber Olaylara Müdahale Merkezi (2014). *"Siber Güvenliğe İlişkin Temel Bilgiler", Ulusal Siber Olaylara Müdahale Merkezi (USOM/TR-CERT)*, Bilgi Teknolojileri ve İletişim Kurumu Telekomünikasyon İletişim Başkanlığı, Ankara, https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf, erişim 15.05.2025.

Ulusal Siber Olaylara Müdahale Merkezi (2025). *"Hakkımızda/About Us"*, Ulusal Siber Olaylara Müdahale Merkezi, https://www.usom.gov.tr/hakkimizda, erişim 15.08.2025.

GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 479-496
DOI: 10.17752/guvenlikstrtj.1738715

Araştırma Makalesi
Research Article

Uluslararası Hukuk Bakımından Uzay Faaliyetlerinde Nükleer Enerji Kaynaklarının Kullanımı*

Using Nuclear Energy Sources in Outer Space Activities from the Perspective of International Law

Egemen DEMİRER**

Öz

Uzay görevlerinde kullanılan nükleer enerji sistemleri, güneş ışığının yetersiz olduğu veya uzun süreli keşif gerektiren görevlerde sağladıkları kesintisiz güç üretimi nedeniyle çağdaş uzay faaliyetlerinde kritik bir gereklilik hâline gelmiştir. Bu makalenin amacı, nükleer güç kullanımının tarihsel gelişimini inceleyerek günümüzde hangi teknik, çevresel ve operasyonel koşullar altında zorunlu bir teknolojiye dönüştüğünü açıklamak ve bu gerekliliğin devlet sorumluluğu ile risk yönetimi bakımından doğurduğu sonuçları hukuki açıdan değerlendirmektir. Çalışmanın hipotezi, nükleer enerji kullanımının tamamen sınırlandırılması yerine, uygun güvenlik tedbirleri ve şeffaf operasyon süreçleriyle yönetilebilir bir alan oluşturduğu yönündedir. Araştırma sorusu şu şekilde belirlenmiştir: "Nükleer güç kaynakları uzay görevlerinde hangi koşullarda vazgeçilmez hâle gelmekte ve bu zorunluluk devletlerin üstlenmesi gereken hangi yükümlülükleri beraberinde getirmektedir?" Çalışmada doküman analizi yöntemi kullanılarak farklı dönemlerde gerçekleştirilen nükleer destekli uzay misyonları ve ulusal–uluslararası uygulamalar karşılaştırmalı olarak incelenmiştir. Bulgular, nükleer enerji sistemlerinin belirli görevlerde teknik açıdan alternatifsiz olduğunu, ancak çevresel risklerin azaltılması ve olası zararların önlenmesi için sıkı güvenlik standartlarının zorunlu olduğunu göstermektedir. Sonuç olarak çalışma, nükleer teknolojinin uzayda barışçıl, güvenli ve sürdürülebilir kullanımının ancak çok katmanlı bir yönetim yaklaşımı ve güçlü uluslararası iş birliğiyle mümkün olabileceğini ortaya koymaktadır.

Anahtar Kelimeler: Çevresel Etkiler, Güvenlik Çerçevesi, Nükleer Enerji, Uzay Hukuku, Uluslararası İş Birliği

Abstract

Nuclear energy systems used in space missions have become a critical technological requirement, particularly in environments where solar radiation is insufficient or where long-duration exploration demands uninterrupted power generation. The purpose of this article is to examine the historical development of nuclear power use in space and identify the technical, environmental, and operational conditions under which it has become indispensable, while assessing the resulting implications for state responsibility and risk management from a legal perspective. The study is based on the hypothesis that the use of nuclear power in space cannot be entirely restricted; rather, it constitutes a manageable domain when supported by robust safety measures and transparent operational procedures. The central research question is formulated as follows: "Under what circumstances do nuclear power sources become essential in space missions, and what obligations arise for states as a consequence of this necessity?" Employing a document-analysis method, the study compares nuclear-supported space missions conducted in different periods and examines relevant national and international practices. The findings indicate that while nuclear systems are technically irreplaceable for certain missions, they also require stringent safety standards to minimize environmental risks and prevent harm. The article concludes that the peaceful, safe, and sustainable use of nuclear technology in outer space is achievable only through multilayered governance and strong international cooperation.

Keywords: Environmental Impact, International Cooperation, Nuclear Energy, Safety Framework, Space Law

* Bu çalışmanın ilk versiyonu 13th IAASS Conference: Building a Safe, Secure and Sustainable Space" konferansında sunulmuştur.v

** Yüksek Lisans Öğrencisi, Sakarya Üniversitesi, Sosyal Bilimler Enstitüsü, Kamu Hukuku Ana Bilim Dalı, Sakarya, Türkiye, e-posta: egemen.demirer@ogr.sakarya.edu.tr
ORCID: 0000-0001-6701-8692

Geliş Tarihi / Submitted: 10.07.2025

Kabul Tarihi / Accepted: 17.12.2025

Extended Summary

Equipping spacecraft with nuclear power sources has become essential for humanity's most ambitious and technically demanding space objectives. Nuclear energy systems offer continuous and high-density power capabilities that cannot be matched by solar technologies, particularly in deep-space environments where sunlight is insufficient or intermittent. Their unique ability to operate reliably for years, even decades, positions nuclear power as a foundational element for missions to the outer planets, long-duration robotic exploration, and potential human settlements beyond Earth. While the advantages of these systems are clear, the challenges they raise—ranging from environmental safety to legal responsibility—require meticulous evaluation and robust international governance.

The pickup of nuclear sources in space activities began during the early Cold War, a period characterized by intense scientific and technological competition. The first nuclear-powered spacecraft made by the USA demonstrated that radioisotope power systems could reliably operate beyond Earth's orbit and provide stable energy in extreme environments. Historic deep-space missions such as Pioneer, Voyager, Cassini, and New Horizons relied heavily on radioisotope thermoelectric generators (RTGs), proving that nuclear energy is indispensable for reaching distant celestial bodies. Other states also explored advanced compact reactor technologies, further expanding the capabilities of space systems and contributing to a diversified technological landscape. These cumulative advances underscore that many of humanity's most significant scientific breakthroughs would have been impossible without nuclear power.

However, the operational benefits of nuclear systems are accompanied by sensitive environmental and legal considerations. International law plays a decisive role in regulating how states may employ nuclear materials in outer space. While foundational treaties prohibit the arrangement of weapons in orbit, they permit the peaceful use of nuclear power sources under strict conditions. This legal distinction allows states to use nuclear systems, but only if they comply with due-diligence obligations, transparency requirements, and safety protocols designed to prevent harm.

Building upon these foundational rules, more specialized instruments articulate detailed expectations for responsible behavior. The 1992 Principles Relevant to the Use of Nuclear Power Sources in Outer Space outline procedural obligations, technical safeguards, and operational criteria that states must meet before launching a space object containing nuclear material. These include rigorous risk assessments, failure-mode analyses, contingency plans, and information-sharing mechanisms. The 2009 IAEA Safety Framework further refines these standards by emphasizing safety culture, emergency preparedness, and robust institutional cooperation. Together, these documents establish a multilayered regulatory framework that guides the safe and responsible use of nuclear systems in outer space.

A crucial component of this framework concerns the liability of states. Under the international liability regime, launching states bear absolute liability for damage caused by their space objects. This principle is particularly significant for nuclear activities, given the potential for radiological contamination, atmospheric reentry risks, or accidental dispersion. The liability regime ensures that victims can receive compensation without needing to prove fault and incentivizes states to adopt the highest safety standards. It also reinforces the importance of precise terminology and legal accuracy, as concepts such as *"launching state"* carry specific implications for attribution and responsibility.

Environmental protection represents another indispensable dimension of nuclear energy use in space. The growing density of space debris significantly increases the risk of accidental collisions in Earth orbit and beyond. A collision involving a nuclear-powered spacecraft could produce severe ecological consequences, potentially releasing radioactive particles into orbit or triggering cascading debris events. Therefore, integrating elements of international environmental law—such as prevention, due diligence, and sustainable use—into the governance of nuclear activities in space has become an urgent priority. These principles guide states to anticipate ecological risks, implement mitigation strategies, and adopt technologies that decrease potential damage to the space environment.

International cooperation is equally vital. As more nations become active space participants and new private actors emerge, multilateral governance mechanisms must evolve to accommodate diverse technological capacities and regulatory perspectives. Cooperative frameworks promote transparency, confidence-building, and shared safety standards, reducing the likelihood of accidents and misunderstandings. Moreover, ensuring impartial access to the value derived from space-based nuclear technologies aligns with the broader principles of peaceful use and collective progress embedded in international space law.

Ultimately, nuclear energy plays a reformer role in humanity's next phase of space exploration. It can enable sustained operations on distant worlds, power scientific instruments in extreme environments, and support future human activities beyond Earth. Yet this technological progress must be accompanied by rigorous legal oversight, environmental stewardship, and international solidarity. If states adopt comprehensive safeguards, uphold their international obligations, and engage in constructive cooperation, nuclear energy can function as a catalyst for a safer, more sustainable, and scientifically productive era in space exploration.

Giriş

1957'de başlayan uzay çağının ardından uzay teknolojilerinin gelişim hızına paralel olarak araştırmaların kapsamı derinleşmiştir. Özellikle gezegenler arası uçuşlar ve derin uzay misyonları için uzun süreli ve yoğun enerji güç kaynaklarına olan ihtiyaç belirgin biçimde artmıştır. Güneş enerjisinin yetersiz kaldığı uzak bölgelerde sürdürülebilir enerji elde edilmesi zorunluluğu, nükleer enerji kaynaklarının uzay araçlarında kullanılmasını giderek daha önemli bir seçenek hâline getirmiştir.

Nükleer enerji kaynakları, yüksek enerji ve uzun süre kesintisiz güç sağlayabilmeleri sayesinde derin uzay misyonlarında önemli avantajlar sunmaktadır. Bununla birlikte, bu sistemlerin kullanımı; insan sağlığı, çevresel etkiler ve atmosfere geri giriş aşamalarında ortaya çıkabilecek riskler nedeniyle uluslararası hukuk açısından ciddi yükümlülükler doğurmaktadır. Bu sebeple nükleer güç kaynaklarının kullanımı devletlerin güvenlik yükümlülükleri, çevresel koruma sorumlulukları ve uluslararası iş birliği mekanizmalarına uyum gerektiren çok boyutlu bir meseledir.

Bu çalışmanın temeli, nükleer enerji kaynaklarının uzay misyonlarında kullanılmasının tarihsel gelişimini incelemek ve bu teknolojinin ne ölçüde gerekli hâle geldiğini örnek misyonlar üzerinden ortaya koymaktır. Tarihsel süreç, hem nükleer güç sistemlerinin hangi bağlamlarda kullanıldığını hem de söz konusu teknolojinin günümüz uzay araştırmalarındaki kaçınılmaz rolünü anlamak açısından değerlidir. Bu doğrultuda makalenin araştırma sorusu: *"Nükleer enerji kaynaklarının uzay faaliyetlerinde kullanımının uluslararası hukuk bakımından doğurduğu yükümlülükler ve güvenlik gereklilikleri nelerdir?"* şeklinde

belirlenmiştir. Hipotez ise, *nükleer güç kaynaklarının derin uzay misyonları için teknik olarak zorunlu hâle geldiği ve bu nedenle uluslararası hukuk tarafından düzenlenen güvenlik ve sorumluluk çerçevesinin gelecekte önemli bir role sahip olacağıdır.*

İkinci aşamada, nükleer enerji kullanımıyla doğrudan veya dolaylı şekilde ilişkili uluslararası hukuk belgeleri incelenecektir. Bu kapsamda; 1967 tarihli Dış Uzay Antlaşması, 1972 tarihli Deniz Tabanı Silah Kontrol Anlaşması, 1986 tarihli Nükleer Kazanın Erken Bildirilmesi Sözleşmesi, 1978'den itibaren Birleşmiş Milletler Genel Kurulu (BMGK)'nda alınan kararlar, 14 Aralık 1992 tarihli A/RES/47/68 sayılı "Uzayda Nükleer Güç Kaynaklarının Kullanımına İlişkin İlkeler"[1], 19 Mayıs 2009 tarihli A/AC.105/934 sayılı Uluslararası Atom Enerjisi Ajansı (IAEA) tarafından ortaya konulan "Dış Uzayda Nükleer Güç Kaynakları için Güvenlik Çerçevesi"[2] ile Uluslararası Atom Enerjisi Ajansı'nın standart ve deklarasyonları ele alınacaktır. Bu belgeler çerçevesinde devletlerin sorumlulukları, güvenlik protokolleri, risk yönetimi mekanizmaları ve çevresel koruma yükümlülükleri değerlendirilecektir.

Son olarak sonuç bölümünde, öğretideki görüşler, devlet uygulamaları, ilgili uluslararası örgütlerin dokümanları ve Birleşmiş Milletler (BM) kararları ışığında nükleer güç kaynaklarının kullanımı konusunda geliştirilen güvenlik önlemleri, hukuksal yükümlülükler ve uluslararası iş birliği gereklilikleri tartışılacak; nükleer enerjinin uzay faaliyetlerinde giderek artan rolü, güvenlik ve sürdürülebilirlik bağlamlarıyla birlikte ele alınarak çalışma tamamlanacaktır. Bu kapsamlı değerlendirme, hem mevcut uluslararası düzenlemelerin bütüncül bir analizini sunmakta hem de gelecekte nükleer enerji kullanımının hukuki çerçevesinin nasıl şekilleneceğine dair öngörüler geliştirmeyi amaçlamaktadır.

1. Uzay Faaliyetlerinde Nükleer Enerji Kaynaklarının Kullanımının Tarihçesi

Nükleer enerji, uzun ömürlü ve yüksek yoğunluklu güç üretme kapasitesi sayesinde derin uzay misyonlarında giderek daha önemli bir rol üstlenmiştir. Özellikle Plütonyum-238 gibi radyoizotoplar, düşük gama radyasyonu yaymaları, yüksek ısı üretmeleri ve uzun yarılanma ömürleri nedeniyle uzay araçlarının enerji ihtiyaçlarını karşılamak için uygun bir seçenek hâline gelmiştir. Bu tür izotopların sağladığı düzenli ısı akışı, radyoizotop termoelektrik jeneratörler (RTG) aracılığıyla güvenilir elektrik üretimi sağlamakta; bu özellikleri onları hem derin uzay sondalarında hem de düşük güneş ışığı alan bölgelerde gerçekleştirilen görevlerde vazgeçilmez kılmaktadır. Her ne kadar bu sistemler geleneksel nükleer reaktörlerden farklı olup sürekli radyasyon yaymıyor olsa da, taşıdıkları maddeler nedeniyle bir kaza durumunda ortaya çıkabilecek çevresel ve sağlık temelli riskler uluslararası düzeyde ciddi endişelere yol açmaktadır.[3]

1 Birleşmiş Milletler Genel Kurulu, *14 Aralık 1992 Tarihli ve A/RES/47/68 Sayılı Karar*, https://docs.un.org/en/A/RES/47/68, erişim 14.04.2025.; Kararda uzayda nükleer enerji kaynağı kullanımına ilişkin temel ilkeler benimsenerek uzay çevresinin ve dünyanın kirlenmemesi uzay paydaşlarına yönelik karara bağlanmıştır. Bu ilkeler, nükleer enerji kaynaklarının uzayda kullanımı sırasında insan yaşamının ve çevrenin korunmasına yönelik sorumlulukları ve teknik güvenlik önlemlerini belirleyen en kapsamlı uluslararası belge niteliğindedir. Ayrıca, uzay faaliyetlerinde nükleer enerji kaynaklarına ilişkin sorumluluk, bildirim yükümlülüğü ve uluslararası iş birliği gibi ilkeleri içermesi bakımından devlet uygulamaları üzerinde bağlayıcı olmasa da yönlendirici etkisi büyüktür. Bu ilkeler çalışmanın devamında ise "1992 tarihli Temel İlkeler" olarak adlandırılacaktır.

2 Uluslararası Atom Enerjisi Ajansı, *Nükleer Enerjinin Uzayda Güvenli Kullanımına İlişkin Güvenlik Çerçevesi*, 2009, https://www.unoosa.org/pdf/reports/ac105/AC105_934E.pdf, erişim 13.04.2025.; Uluslararası Atom Enerjisi Ajansı (IAEA) tarafından hazırlanan ve günümüzde artan uzay faaliyetleri neticesinde gezegenler arası uçuşların gerçekleştirilebilmesi için önem arz eden nükleer enerjinin uzayda güvenli bir şekilde kullanılması açısından 2009 tarihli Güvenlik Çerçevesi kabul edilmiştir. Bahse konu güvenlik çerçevesi çalışmanın devamında ise "2009 tarihli Güvenlik Çerçevesi" olarak adlandırılacaktır.

3 U.S. Department of Energy, "The History of Nuclear Power in Space", Haziran 2015, https://www.energy.gov/articles/history-nuclear-power-space, erişim 10.06.2025.

Uzayda nükleer enerji kullanımının geçmişi 1961 yılında ABD'nin Transit 4A uydusunu RTG ile güçlendirmesiyle başlamıştır. Bu görev, uzun süreli enerji üretiminin mümkün olduğunu göstermiş ve sonraki on yıllarda gerçekleştirilecek keşif görevlerinin önünü açmıştır. 1969–1977 yılları arasında Apollo programı kapsamında Ay yüzeyine yerleştirilen bilim istasyonları SNAP-27 RTG sistemleriyle çalışmış; bu sistemler Ay yüzeyindeki deneylere yıllarca enerji sağlamıştır. Bunu takip eden dönemlerde Galileo, Ulysses, Cassini ve New Horizons gibi görevlerde radyoizotop sistemler kritik bir bileşen hâline gelmiş; Jüpiter, Satürn, Titan ve Kuiper Kuşağı hakkında bugün bilinen pek çok veri bu sistemler sayesinde elde edilmiştir.

Bu gelişmeler yalnızca ABD ile sınırlı kalmamıştır. Avrupa Uzay Ajansı (ESA) 1960'lardan itibaren nükleer füzyon teknolojileri ve radyoizotop güç sistemleri üzerine araştırmalar yürütmüş; böylece Avrupa ülkeleri uzay araştırmalarında nükleer enerji alanında daha etkin bir rol oynama hedefini benimsemiştir. Özel sektörün entegrasyonu da bu süreçte önem kazanmış; ABD merkezli Exlabs ve Antares gibi şirketler radyoizotop güç sistemlerinin geliştirilmesine yönelik çalışmalar yapmıştır. Benzer şekilde Rusya'nın Topaz nükleer reaktör programı, Soğuk Savaş döneminde dahi ABD ile bilimsel iş birliğine konu olmuş; termoiyonik enerji dönüşüm teknolojileri uzun süreli uzay görevleri için alternatif bir reaktör modeli olarak test edilmiştir. Sovyetler Birliği'nin 1987 ve 1988 yıllarında gerçekleştirdiği Topaz reaktör test uçuşları, özellikle termoiyonik teknoloji konusunda önemli ilerlemeler sağlanmasına katkı sunmuştur.

1.1. ABD'nin SNAP Programı

Amerika Birleşik Devletleri'nin uzayda nükleer enerji kullanımına yönelik çalışmaları, 1940'lı yılların sonlarında başlatılan *Systems for Nuclear Auxiliary Power* (SNAP) (Nükleer Yardımcı Güç Sistemi) programıyla[4] kurumsal bir çerçeve kazanmıştır. Program kapsamındaki çalışmalar, hem nükleer reaktörlerin uzayda kullanılabilirliğini araştırmayı hem de radyoizotoplara dayalı küçük ölçekli güç sistemleri geliştirmeyi hedeflemiştir.[5] NASA, Atom Enerjisi Komisyonu ve ABD Savunma Bakanlığı'nın ortak katkılarıyla yürütülen program hem askerî hem sivil amaçlara yönelik tasarımları içermiştir.

1961'de fırlatılan Transit IV-A ve Transit IV-B uyduları, SNAP programının uzay ortamında başarıyla uygulandığı ilk örnekler arasında yer almaktadır. Transit IV-A'nın yaklaşık on yıllık operasyon sürecinde Dünya çevresinde 55.000'den fazla tur atması ve iki milyar milin üzerinde yol katetmesi, o dönemin sınırlı teknolojik kapasitesine rağmen nükleer gücün güvenilirliğini ortaya koymuştur.[6]

1.2. Radyoizotop Termoelektrik Jeneratörler (RTG'ler) ve Cassini–Huygens Misyonu

RTG'lerin en önemli özellikleri; bakım gerektirmemeleri, uzun süre sabit güç sağlamaları ve düşük sıcaklıklarda dahi çalışabilir olmalarıdır.[7] Bu nedenle hem Dünya yörüngesindeki uzun

4 U.S. Department of Energy, "System for Nuclear Auxiliary Power (SNAP) Overview", t.y., https://www.energy.gov/etec/system-nuclear-auxiliary-power-snap-overview, erişim 14.04.2025.; SNAP programı, ABD tarafından 1940'lı yıllarından sonundan itibaren geliştirilen ve uzay görevlerinde kullanılmak üzere nükleer enerjiyle çalışan kompakt güç sistemlerini kapsamaktadır. Bu sistemler özellikle derin uzay görevlerinde uzun süreli ve güvenilir enerji kaynağı sağlaması açısından öncü bir rol oynamıştır.

5 Steven Aftergood, David W. Hafemeister, Oleg F. Prilutsky, Joel R. Primack ve Stanislav N. Rodionov, "Nuclear Power in Space", *Scientific American*, 265:6, 1991, s. 42-49.

6 U.S. Department of Energy, "The History of Nuclear Power in Space".

7 NASA, "Radioisotope Power Systems (RTGs)–Frequently Asked Questions", https://science.nasa.gov/planetary-science/programs/radioisotope-power-systems/faq/, erişim 20.08.2025.; Radyoizotop Termoelektrik Jeneratörler (RTG), Plütonyum-238'ün radyoaktif bozulmasıyla açığa çıkan ısıyı, termokupllar aracılığıyla elektriğe çeviren, hareketli parçası olmayan bir nükleer güç kaynağıdır. Uzayda uzun süreli, güvenilir ve çevresel koşullardan bağımsız enerji sağlar.

süreli görevlerde hem de derin uzay misyonlarında tercih edilmektedirler. Galileo uzay aracı, RTG'lerle güçlendirilmiş ilk büyük misyonlardan biri olarak Jüpiter'in yörüngesine giriş yapmış ve Europa'nın yüzeyi altında bir okyanus bulunduğuna dair bulgular elde etmiştir. Bu keşif, RTG destekli uzun süreli görevlerin bilimsel önemini açıkça göstermektedir.

Satürn ve Titan'ı incelemek amacıyla başlatılan Cassini–Huygens misyonu da üç adet RTG sistemi ile donatılmıştır.[8] Huygens sondasının Titan yüzeyine başarılı inişi, uzak gök cisimlerine erişimin teknik olarak mümkün olduğunu kanıtlamış; Cassini'nin Satürn sistemi boyunca yürüttüğü çok yıllı gözlemler ise nükleer güç sistemlerinin bilimsel keşiflerde oynadığı belirleyici rolü bir kez daha ortaya koymuştur.

1.3. Rusya'nın Topaz Reaktör Programı

Rusya'nın Topaz programı, termoiyonik enerji dönüşümü[9] alanında yürütülen en kapsamlı çalışmalardan biridir. Soğuk Savaş koşullarına rağmen ABD ve Sovyetler Birliği arasında sınırlı da olsa bilimsel iş birliği yapılmış; özellikle 1980'lerde ABD'nin Stratejik Savunma Girişimi kapsamındaki ilgisi termoiyonik reaktör teknolojilerinin yeniden gündeme gelmesine yol açmıştır.[10] 1987 ve 1988 yıllarında gerçekleştirilen iki test uçuşu, reaktörlerin uzay ortamında çalışabilirliğini göstermiş ve daha hafif, kompakt reaktör modelleri için önemli veriler sağlamıştır.

1.4. Avrupa Uzay Ajansı'nın Çalışmaları

ESA, uzun vadeli uzay keşif hedeflerine paralel olarak nükleer füzyon reaktörleri ve radyoizotop güç sistemleri üzerine çeşitli araştırma girişimleri başlatmıştır. 1960'lardan 1990'lara uzanan bu süreçte[11] Avrupa ülkeleri, ulusal laboratuvarlar, özel sektör ve uluslararası ortaklarla iş birliği yaparak teknolojiyi geliştirme yönünde adımlar atmıştır. Bu çalışmalar, Avrupa'nın nükleer enerji destekli derin uzay görevlerinde daha bağımsız ve yetkin bir aktör hâline gelme hedefini güçlendirmiştir.[12]

Bu tarihsel gelişim, nükleer güç sistemlerinin hem teknik bir tercih hem de insanlık tarihi açısından en uzak noktalara ulaşmasını mümkün kılan, yüksek risk–yüksek getiri

8 NASA, "Cassini Mission", *NASA Science*, https://science.nasa.gov/mission/cassini/, erişim 14.04.2025.; NASA tarafından yürütülen Cassini görevi, Satürn ve uydularını incelemek amacıyla geliştirilmiş uzun soluklu bir uzay araştırma misyonudur. 1989 yılında NASA tarafından yürütülen projenin amacı Jüpiter'i ve çevresinde yer alan uyduları keşfetmek olmuştur. Ayrıntılı bilgi için bkz.: NASA, "Galileo Mission", *NASA Science*, https://science.nasa.gov/mission/galileo/, erişim 18.08.2025.

9 ScienceDirect, "Thermionic Power Generation", *ScienceDirect Topics*, https://www.sciencedirect.com/topics/engineering/thermionic-power-generation, erişim 20.08.2025.; Termoiyonik Enerji Dönüşümü (TEC), yüksek sıcaklıktaki yüzeyden yayılan elektronların soğuk toplayıcıya geçmesiyle ısının doğrudan elektriğe çevrildiği, hareketli parçasız bir enerji üretim yöntemidir.

10 Richard Dabrowski, "U.S.–Russian Cooperation in Science and Technology: A Case Study of the TOPAZ Space-Based Nuclear Reactor International Program", *Connections: The Quarterly Journal*, 13:1, 2013, s. 72–74.; ABD ile Rusya arasında gerçekleştirilen bilimsel iş birliğinin bir örneği olan Topaz nükleer reaktör programı, uzayda nükleer güç sistemlerinin ortak kullanımı açısından önemlidir.

11 Adam M. Baker, John H. Free ve Stephen H. Priebe, *Future Power Systems for Space Exploration*, ESA Raporu No. 14565/NL/WK, QinetiQ, Şubat 2002.; Leopold Summerer ve Armin Stapelmann, "ESA's Approach to Nuclear Power Sources for Space Applications", *International Congress on Advances in Nuclear Power Plants (ICAPP 2007): The Nuclear Renaissance at Work*, Fukui–Kyoto, Japonya, 24-28 Nisan 2007.; Leopold Summerer, Trevor Wilcox, Robert Bechtel ve Stephen Harbison, "The International Safety Framework for Nuclear Power Source Applications in Outer Space – Useful and Substantial Guidance", *Acta Astronautica*, 111, 2015, s. 89-101.

12 Birleşmiş Milletler, *Multi-Year Work Plan on the Development of an International Technical Framework Based on Goals and Recommendations for the Safety of Nuclear Power Source Applications in Outer Space for the Period 2003–2006*, COPUOS Bilimsel ve Teknik Alt Komitesi, Teknik Rapor No. A/AC.105/804, Ek III, Viyana, 2003, https://documents.un.org/doc/undoc/ltd/v06/535/62/pdf/v0653562.pdf, erişim 02.04.2025.; Birleşmiş Milletler, *Report of the Working Group on the Use of Nuclear Power Sources in Outer Space: Inter-Sessional Meeting Held in Vienna, 13–15 June 2005*, COPUOS Bilimsel ve Teknik Alt Komitesi, Teknik Rapor No. A/AC.105/L.260, Viyana, 2005, https://www.unoosa.org/pdf/limited/c1/AC105_C1_L260E.pdf, erişim 02.04.2025.

dengesine sahip kritik bir teknoloji olduğunu göstermektedir. Ancak beraberinde getirdiği çevresel riskler ve uluslararası hukukun yetki alanına giren sorumluluklar,[13] bu teknolojinin sıkı bir denetim ve hukuki çerçeve içerisinde[14] kullanılmasını zorunlu kılmaktadır.

2. Uluslararası Hukuk Çerçevesinde Nükleer Enerji Kaynaklarının Uzay Faaliyetlerinde Kullanımı

Yukarıda kısaca ele alınan tarihi gelişmelerin yanında, nükleer enerji kaynaklarının kullanımına ilişkin hukuki düzenlemeler de güvenlik çalışmalarının vazgeçilmez boyutunu oluşturmaktadır. Zira geri dönüşü zor veya imkânsız çevresel ve insani sonuçlar doğurabilecek nükleer güç kaynaklarının, hukuka uygun ve denetim altında kullanılması, uluslararası hukukun temel hedefleri arasında yer almaktadır. Uluslararası toplum, çevrenin korunması ve insan sağlığını tehlikeye atabilecek faaliyetlerin önlenmesi amacıyla çeşitli ilke ve kurallar geliştirmiş; bu çerçeve, uzay faaliyetleri bakımından da giderek daha somut hâle gelmiştir.

Bu bölümde BMGK kararları ve bazı temel uluslararası hukuk enstrümanları ışığında, uzay faaliyetleri sırasında nükleer enerji kaynaklarının kullanımına getirilen sınırlamalar, öngörülen güvenlik mekanizmaları ve bunların neden önemli olduğu ele alınacaktır. Böylece nükleer enerji kaynaklarının uzay faaliyetlerinde kullanımının, uluslararası hukuk kaynakları bakımından nasıl düzenlendiği bütüncül bir bakışla ortaya konulacaktır.

2.1. 1967 Tarihli Dış Uzay Antlaşması'na Göre Nükleer Enerji Kaynaklarının Kullanımı

Uzay hukukunun temelini oluşturan 1967 tarihli Dış Uzay Antlaşması,[15] nükleer enerji kaynaklarının kullanımına dolaylı fakat son derece önemli bir çerçeve sunmaktadır. Antlaşma'nın 6. maddesi, devletlerin dış uzayda gerçekleştirdikleri tüm ulusal faaliyetler bakımından uluslararası sorumluluk taşıdığını hükme bağlamaktadır. Buna göre, devletler uzay faaliyetlerinin antlaşma hükümlerine ve genel uluslararası hukuka uygun yürütülmesinden sorumludur.[16]

Antlaşma'nın 4. maddesi ise yıkıcı etkiye sahip olan silahların yörüngeye yerleştirilmesini, gök cisimlerinde konuşlandırılmasını veya uzayın herhangi bir başka şekilde silahlandırılmasını yasaklamaktadır.[17] Bu düzenleme, doğrudan nükleer güç kaynaklarının

13 Armel Kerrest, "The Liability Convention and Liability for Space Activities", *United Nations / International Institute of Air and Space Law Workshop: Papers on Capacity Building in Space Law,* Birleşmiş Milletler Yayınları, 2003, s. 25.

14 Birleşmiş Milletler, *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies,* BM Genel Kurulu Kararı No. 2222 (XXI), 10 Ekim 1967, https://docs.un.org/en/A/RES/2222(XXI), erişim 02.04.2025.; Birleşmiş Milletler, *Convention on International Liability for Damage Caused by Space Objects,* BM Genel Kurulu Kararı No. 2777 (XXVI), 01 Eylül 1972, https://docs.un.org/en/A/RES/2777%20(XXVI), erişim 02.04.2025.; Birleşmiş Milletler, *Convention on Registration of Objects Launched into Outer Space,* BM Genel Kurulu Kararı No. 3235 (XXIX), 15 Eylül 1976, https://docs.un.org/en/A/RES/3235%20(XXIX), erişim 02.04.2025.

15 Türkiye, Ay ve Diğer Gök Cisimleri Dâhil Uzayın Keşfi ve Kullanılmasında Devletlerin Faaliyetlerini Yöneten İlkeler Hakkında Andlaşma'yı 13 Temmuz 1967 tarihinde kabul etmiştir. Andlaşma metni, 24 Temmuz 1967 tarihli ve 12655 sayılı Resmî Gazete'de yayımlanarak yürürlüğe girmiştir. Metin için bkz. Türkiye Büyük Millet Meclisi, *Ay ve Diğer Gök Cisimleri Dâhil, Uzayın Keşfi ve Kullanılmasında Devletlerin Faaliyetlerini Yöneten İlkeler Hakkında Andlaşma*, Resmî Gazete No. 12655, https://www5.tbmm.gov.tr/tutanaklar/KANUNLAR_KARARLAR/kanuntbmmc050/kanuntbmmc050/kanuntbmmc05000902.pdf, erişim 13.04.2025.; Obed. Y. Asamoah, "Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space", *The Legal Significance of the Declarations of the General Assembly of the United Nations*, Springer, Dordrecht, 1966, ss. 129-160.

16 Steven A. Mirmina ve David J. Den Herder, "Nuclear Power Sources and Future Space Exploration", *Chicago Journal of International Law*, 6:1, 2005, s. 158.

17 Erdem Denk, "Bir Kitle İmha Silahı Olarak Nükleer Silahların Yasaklanmasına Yönelik Çabalar", *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi,* 66:3, 2020, ss. 93–136.

barışçı amaçlarla kullanılmasını hedef almamakla birlikte, nükleer teknolojinin uzayda askerî amaçlarla kullanılmasına açık bir sınır getirmesi bakımından konumuzla dolaylı olarak ilişkilidir. Zira başlangıçta enerji üretimi amacıyla kullanılan nükleer teknolojilerin, ileride silahlandırma potansiyeli barındırabileceği ihtimali, uluslararası toplumun dikkatle izlediği bir alandır. Bu tür silahların gök cisimlerine yahut yörüngeye yerleştirilmesini yasaklanmasının sebeplerinden birisi de işte bu potansiyelin taşınmasıdır.[18]

Antlaşma'nın 7. maddesi, uzay faaliyetleri sonucu meydana gelen zararlardan "fırlatan devlet"in (*launching state*) sorumluluğunu düzenlemektedir. Nükleer enerji kaynağı taşıyan bir uzay aracı tarafından Dünya'da sebep olunan zararlar bakımından fırlatan devletin sorumluluğu, kusurdan bağımsız ve mutlak nitelikte yorumlanmaktadır. Böylece, nükleer enerji kaynaklarının kullanıldığı uzay faaliyetlerinde olası bir kaza veya yeniden giriş hadisesi durumunda, zarar gören taraflara tazminat sağlanması güvence altına alınmaya çalışılmaktadır.[19]

9. madde ise devletlere, uzayda yürüttükleri faaliyetlerin diğer devletler üzerinde zararlı etkiler doğurmamasını sağlama yönünde "uygun önlemleri alma" yükümlülüğünü getirmektedir. Devletlerin, özellikle yörüngeden çıkış veya Dünya atmosferine yeniden giriş aşamalarında, zararlı nesnelerin çevreye ve insan sağlığına zarar vermesini önlemek için gerekli teknik ve idari tedbirleri alması gerektiği vurgulanmaktadır. Bu ifade, nükleer enerji kaynaklarının içerdiği potansiyel riskler dikkate alındığında, insan sağlığı ve Dünya biyosferinin korunması açısından özel bir önem kazanmaktadır.

Uzay çevresinin korunması, hangi amaçla kullanılırsa kullanılsın, tüm tarafların dikkatini ve iş birliğini gerektiren hassas bir konudur.[20] Devletler, yürütülen uzay faaliyetleri bakımından zararlı müdahaleler söz konusu olduğunda uygun uluslararası danışma ve iş birliği mekanizmalarını işletmekle yükümlüdür.[21] Nükleer enerji kaynaklarının kullanımında da bu ilkenin uygulanması, olası bir kazanın küresel ölçekte sonuçlar doğurabileceği gerçeği karşısında kaçınılmazdır.

Öğretide bazı yazarlar, 9. maddede yer alan *"zararlı kontaminasyonun engellenmesi"* ve *"uygun önlemler alınması"* ibarelerinin geniş yorumlanması gerektiğini, buna göre

18 1963 tarihli Atmosferde, Dış Uzayda ve Su Altında Nükleer Silah Testlerinin Yasaklanması Andlaşması, nükleer ve kitle imha silahlarının kullanımını yasaklamıştır. Andlaşmanın konumuzla alakalı kısmı Dış Uzaya ve yörüngeye konuşlandırılması yasaklanan nükleer silahlarla ilgilidir. Fakat bu bağlantı esasında dolaylı bir bağlantılıdır çünkü anlaşmanın amacı uzay çevresinin korunması ve radyoaktif maddelerin dünyaya zarar vermesinin engellenmesidir. Andlaşma metninde aynı zamanda Ay'ın ve diğer gök cisimlerinin Andlaşmaya taraf olan tüm devletler tarafından yalnızca barışçıl amaçlarla kullanılacağı belirtilmiştir. Fakat burada tartışmalı husus barışçıl amaçların ne olduğu konusunda net bir tanımın ortaya konulmamasıdır. Bazı kaynaklarda saldırgan olmayan demek istenirken bazı kaynaklara göre de askerî olmayan anlamında değerlendirilmiştir. Dolayısıyla uzayda yürütülen faaliyetlerin barışçıl yürütülmesi kavramının aydınlatılması ve kesin bir tanımın yapılması gerekmektedir. Birleşmiş Milletler, *Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water*, 05 Ağustos 1963, https://www.archives.gov/milestone-documents/test-ban-treaty, erişim 14.04.2025.; İlgili antlaşma bu çalışmada, "Test Yasağı Sözleşmesi" olarak anılacaktır.

19 Burada dünyada gerçekleşmesi ya da dış uzayda gerçekleşmesi konusunda sorumluluk hususu ihtilaflıdır çünkü dünyada meydana gelen kazalar neticesinde kusur sorumluluğu aranırken uzayda meydana gelen kazalarda ise kusursuz sorumluluk geçerlidir.

20 Devletler, uzayın keşfi ve kullanımı sırasında iş birliği ve bilgi paylaşımı prensibini benimsemelidir. Her faaliyet, diğer tarafların çıkarlarına saygı gösterilerek yürütülmeli ve çevreyi koruma önlemleri alınmalıdır. Potansiyel zararlı etkiler öngörüldüğü takdirde uluslararası danışmalar yapılması gereklidir; H. Ph. Diederiks-Verschoor, *An Introduction to Space Law*, Kluwer Law International, 2008, ss. 29–30.

21 H. Ph. Diederiks-Verschoor, *An Introduction to Space Law*, Kluwer Law International, 2008, s. 30.; Eilene Galloway, "Consensus Decision-Making by the United Nations Committee on the Peaceful Uses of Outer Space", *Journal of Space Law*, 7:1, 1979, ss. 3–15.

kapsamın nükleer enerji kaynaklarının Dünya biyosferine ve uzay çevresine verebileceği olası zararları da kapsayacak şekilde anlaşılması gerektiğini savunmaktadır.[22] Bu yorum, nükleer güç kaynaklarının kullanımında çevresel koruma boyutunun daha belirgin hâle getirilmesine katkı sunmaktadır.

2.2. 1992 Tarihli ve A/RES/47/68 Sayılı Temel İlkeler Metnine Göre Nükleer Enerjinin Kullanımı

Nükleer enerji kaynaklarının kullanımına ilişkin en somut ve özel düzenlemelerden biri, 14 Aralık 1992 tarihli ve A/RES/47/68 sayılı "Dış Uzayda Nükleer Güç Kaynaklarının Kullanımına İlişkin İlkeler"dir. Bu Belge, Soğuk Savaş döneminde ve sonrasında uzaya fırlatılan uydularda nükleer güç kaynaklarının artan kullanımı karşısında, ortaya çıkabilecek risklerin azaltılması ve Dünya biyosferinin korunması amacıyla kabul edilmiştir.

Temel İlkeler, nükleer enerji kaynaklarının uzun ömürlü ve yüksek yoğunluklu olması nedeniyle bazı gezegenler arası misyonlarda teknik olarak vazgeçilmez hâle geldiğini kabul etmekle birlikte, bu kaynakların kullanımının ayrıntılı güvenlik değerlendirmelerine tabi tutulmasını öngörmektedir. Fırlatma öncesinde çevresel etki değerlendirmesi yapılması, olası risklerin analiz edilmesi ve bu risklerin azaltılması için gerekli önlemlerin planlanması, çevrenin, biyosferin ve insan sağlığının korunması yönünden asli bir yükümlülük olarak ortaya çıkmaktadır.

Öğretide, bu risklerin nasıl yönetilmesi gerektiğine ilişkin farklı yaklaşımlar mevcuttur. Gorbiel, nükleer güç kaynaklarına ilişkin güvenlik çalışmalarını dört temel başlıkta toplamaktadır: (a) nükleer güç kaynaklarının kullanımına dair bilgi paylaşımı, (b) yeniden giriş öncesinde bildirim yükümlülüğü, (c) acil durumlarda devletlere yardım sağlanması ve (d) radyasyona maruziyet seviyelerine ilişkin standartların belirlenmesi.[23] Haanappel ise, bu tür uyduların yörüngede bulunmasının Dünya'daki insanlar ve mülkler açısından önemli tehditler taşıdığını, çevresel risklerin yüksekliğine dikkat çekerek, nükleer kaynakların uzayda kullanımına mümkün olduğunca sınırlı yaklaşılması gerektiğini vurgulamaktadır.[24]

1992 tarihli Temel İlkeler'in 1. maddesi, bu ilkelerin yalnızca taraf devletleri değil, genel anlamda uzayda nükleer güç kaynağı kullanan tüm devletleri bağlayıcı olduğunu ifade etmektedir. 3. maddeye göre, nükleer enerji kaynaklarının kullanımı, nükleer güç olmaksızın yürütülmesi mümkün olmayan veya makul ölçüde gerçekleştirilemeyen görevlerle sınırlandırılmalıdır.[25] Böylece nükleer teknolojinin yalnızca zorunlu hâllerde devreye sokulması, çevre ve insan sağlığı bakımından ihtiyatlı bir yaklaşımın benimsendiğini göstermektedir. 4. madde ise, devletlerin nükleer güç kaynaklarının kullanımı öncesinde uluslararası hukukun öngördüğü *"özen yükümlülüğü"*ne uygun hareket etmeleri, kapsamlı güvenlik değerlendirmeleri yapmaları ve bu değerlendirmeyi fırlatan devletin sorumluluğu altında yerine getirmeleri gerektiğini belirtmektedir. Bu bağlamda, 1976 tarihli Tescil Sözleşmesi uyarınca tescil devletinin belirlenmesi aynı zamanda sorumluluğun belirlenmesinde elzemdir.

22 Steven A. Mirmina ve David J. Den Herder, "Nuclear Power Sources and Future Space Exploration", *Chicago Journal of International Law*, 6:1, 2005, s. 159.

23 Durgambini Patel, Priyanka M. Jawale, "Nuclear On-Board: Prospects and Challenges of Outer Space Exploration with Nuclear Power Sources", *Indian Journal of Law and Justice*, 12:1, 2021, s. 26.; H. Ph. Diederiks-Verschoor, *An Introduction to Space Law*, Kluwer Law International, 2008, s. 102.; A. Gorbiel, "Some Comments on the Proposal Concerning the Elaboration of New Legal Norms Governing Nuclear Power Sources Use in Outer Space", *Proceedings of the 22nd Colloquium on the Law of Outer Space*, Münih, 1979, ss. 131–139.

24 P. P. C. Haanappel, "Nuclear Power Sources in Outer Space", *Proceedings of the 27th Colloquium on the Law of Outer Space*, ss. 215–217.; Diederiks-Verschoor, *An Introduction to Space Law*, s. 102.

25 1992 tarihli Temel İlkelerinin 3. ilkesinde gezegenler arası görevlerde, yüksek yörüngede bulunan uzay araçlarında kullanılması vurgulanarak sınırlandırılması gerektiği ayrıca ifade edilmiştir.

Bunun yanında radyoaktif madde taşıyan bir uzay aracının atmosfere yeniden girişi söz konusu olduğunda BM Genel Sekreteri'nin zamanında bilgilendirilmesi yükümlülüğünü getirmektedir. Bu bildirim yükümlülüğü, olası bir kaza durumunda diğer devletlerin koruyucu önlemler almasını ve sivil nüfus ile çevrenin zarar görmesinin asgari düzeye indirilmesini amaçlamaktadır. 6. ve 7. maddeler ise devletler arasında bilgi paylaşımı, danışma ve karşılıklı yardımı öngörerek, nükleer güç kaynaklarından kaynaklanabilecek risklere karşı uluslararası iş birliği mekanizmasının güçlendirilmesini hedeflemektedir. Gorbiel'in bilgi paylaşımı ve iş birliği vurgusu da bu ilkelerle paralellik göstermektedir.

Sonuç itibarıyla, Temel İlkeler tüm devletleri bağlayan ve uygulamada teamül hukuku niteliği kazandığı kabul edilen bir çerçeve sunmaktadır. Nükleer enerji kaynaklarının yalnızca belirli ve zorunlu görevlerle sınırlandırılması, fırlatan devletin güvenlik değerlendirmesi yapma yükümlülüğü, yeniden giriş aşamasında BM'nin bilgilendirilmesi ve iş birliklerinin geliştirilmesi gerekliliğinin vurgulanması, bu çerçevenin temel sütunlarını oluşturmaktadır. Böylece uzayda nükleer enerji kullanımı, teknik bir tercih olmaktan çıkarak, uluslararası hukukun özen yükümlülüğü, çevre koruma ve insanlığın ortak çıkarlarının korunması ile doğrudan bağlantılı bir sorumluluk alanına dönüşmektedir.

2.3. 27 Ekim 1986 Tarihli Nükleer Kazanın Erken Bildirilmesi Sözleşmesi ve Uluslararası Çevre Hukuku Açısından Değerlendirilmesi

Uzayda nükleer enerji kaynağı kullanılan görevlerde ortaya çıkabilecek risklerin uluslararası boyutu dikkate alındığında, 27 Ekim 1986 tarihli Nükleer Kazanın Erken Bildirimi Hakkında Sözleşme,[26] uzay faaliyetleri bakımından da özel bir önem taşımaktadır.[27] Sözleşme, esasen nükleer tesislerde meydana gelen kazalara yönelik hazırlanmış olsa da içerdiği bildirim yükümlülüğü ve erken uyarı mekanizması, uzayda meydana gelebilecek nükleer kaynaklı kazaların yönetimi açısından da tamamlayıcı bir rol oynamaktadır.[28] Nükleer enerji kaynağı taşıyan bir uzay aracında meydana gelecek kontrol kaybı, parçalanma ya da atmosferik yeniden giriş sırasında radyoaktif yayılma ihtimali, sözleşmenin öngördüğü erken bildirim sisteminin uzay hukuku ile kesiştiği temel noktayı oluşturmaktadır.

Devletler, nükleer enerji kaynaklarının kullanıldığı bir uzay görevi sırasında ortaya çıkabilecek ve dünya biyosferine yayılma riski taşıyan her türlü olası kazayı önlemekle yükümlüdür. Olası bir kazanın ardından çevreye ve insan sağlığına verilebilecek zararların azaltılması, erken bildirim yükümlülüğü sayesinde mümkün olabilmektedir. Bu nedenle sözleşme, nükleer enerji taşıyan uzay araçlarının beklenmedik bir durumda atmosfere yeniden giriş yapması ihtimalinde, diğer devletlerin önleyici tedbir almasını sağlayacak bir hukuki araç niteliği taşımaktadır.

Uluslararası çevre hukukunun temel ilkeleri bakımından değerlendirildiğinde, devletlerin kendi yetki alanları dışında yer alan bölgelerde bile çevresel zarar doğurmaktan

26 Uluslararası Atom Enerjisi Ajansı, *Convention on Early Notification of a Nuclear Accident*, 27 Ekim 1986, https://www.iaea.org/sites/default/files/infcirc335.pdf, erişim 15.04.2025.

27 27 Ekim 1986 tarihli Nükleer Kazanın Erken Bildirilmesi Sözleşmesi, Çernobil Nükleer Felaketi'nin ardından Uluslararası Atom Enerjisi Ajansı (IAEA) nezdinde kabul edilerek, sınır ötesi etkiler doğuran nükleer kazaların meydana gelmesi durumunda derhal bilgi paylaşımını zorunlu kılan ilk bağlayıcı uluslararası belge olmuştur. Bu sözleşme, hem uluslararası hukukun devletlerin karşılıklı bildirim yükümlülüğüne ilişkin temel prensiplerini pekiştirmiş hem de çevre hukukunun önleme ve ihtiyat ilkelerine işlerlik kazandırarak, çevresel zararın azaltılması yönünde önemli bir adım atmıştır. Ayrıntılı bilgi için bkz.: https://www.iaea.org/topics/nuclear-safety-conventions/convention-early-notification-nuclear-accident, erişim 15.04.2025.

28 Steven A. Mirmina, David J. Den Herder, "Nuclear Power Sources and Future Space Exploration", *Chicago Journal of International Law,* 6:1, 2005, s. 162.

kaçınma yükümlülüğünün bulunduğu ilk kez Trail Smelter uyuşmazlığında[29] açık biçimde vurgulanmıştır. Bu yaklaşım, egemenlik sınırlarının ötesinde dahi çevre koruma sorumluluğunun bulunduğunu teyit etmektedir. Ancak nükleer enerji kaynaklarının kullanımına ilişkin çevre hukukuna dair önceden belirlenmiş, geniş kapsamlı bir kurallar bütünü bulunmamaktadır; bu nedenle diğer çevre hukuku belgelerinden tümevarım yoluyla bir hukuki çerçeve oluşturulmaktadır.

Bu noktada 1972 Stockholm Deklarasyonu, 1972 Beşerî Çevre için Eylem Planı[30] ve 1992 tarihli Çevre ve Gelişim Hakkında Rio Konferansı,[31] nükleer enerji kullanımının çevresel etkilerinin değerlendirilmesi bakımından önemli belgeler olarak görülmektedir. Stockholm Deklarasyonu'nun 21. ilkesi, devletlerin kendi yetki alanlarında çevreye zarar vermeme yükümlülüğünü düzenlerken, bunun uzay faaliyetlerini de kapsayacak şekilde geniş yorumlanabileceği açıktır. Rio Deklarasyonu'nun 15. ilkesi olan ihtiyati yaklaşım, ciddi veya geri döndürülemez zarar riski bulunan faaliyetlerde, bilimsel kesinlik aranmasa dahi önleyici tedbirlerin alınmasını emretmektedir.[32]

Bu ilkeler çerçevesinde nükleer enerji kaynaklarının uzayda kullanımında çevresel etki değerlendirmesi yapılması, risklerin belirlenmesi ve önleyici teknik/hukuki tedbirlerin alınması hem uluslararası çevre hukukunun hem de uluslararası uzay hukukunun ortak sorumluluk alanı olarak görülmelidir.[33] Bu yaklaşım, *tüm insanlığın ortak mirası* kavramı[34] ile de uyumlu olup uzay çevresi ve Dünya biyosferi birbirinden kopuk değil; bütünsel bir ekosistemin parçalarıdır ve devletlerin her iki alanı da koruma yükümlülüğü bulunmaktadır.

2.4. 1972 Deniz Tabanı Silah Kontrol Anlaşması ve Çift Kullanım (Dual-Use) Riskinin Değerlendirilmesi

Nükleer teknolojilerin çift kullanım (*dual-use*) niteliği, uzayda nükleer enerji kaynaklarının kullanımında hem teknik hem de hukuki açıdan en önemli sorun alanlarından birini oluşturmaktadır. Çift kullanım riski, aynı teknolojinin hem sivil hem askerî amaçlarla kullanılabilmesi anlamına gelir. Sivil alanlarda enerji üretimi, tıbbi izotop kullanımı ve uzay araştırmaları için geliştirilen teknolojilerin, nükleer silah programlarına aktarılabilme

29 Trail Smelter Arbitration (United States v. Canada), "ABD–Kanada Uluslararası Hakemliği", https://legal.un.org/riaa/cases/vol_iii/1905-1982.pdf, erişim 13.04.2025.; Devletlerin kontrolü ve egemenliği dışında bulunan ve insanlığın ortak mirası olarak adlandırılan bölgelerin çevresel zararlara karşı korunması gerekliliği ilk olarak ABD ve Kanada arasında gerçekleşen Trail Smelter Davası'nda yer almıştır. Bu açıdan dava uluslararası hukuk açısından oldukça önemlidir.

30 Birleşmiş Milletler, *Declaration of the United Nations Conference on the Human Environment (Stockholm Declaration)*, 5–16 Haziran 1972, https://docs.un.org/en/A/CONF.48/14/Rev.1, erişim 13.04.2025.

31 Birleşmiş Milletler, *Rio Declaration on Environment and Development*, 3–14 Haziran 1992, https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdf, erişim 13.04.2025.

32 Lotta Viikari, *The Environmental Element in Space Law: Assessing the Present and Charting the Future*, Brill Publishing, 2008, s. 128.

33 İnan Şimşek, Aybüke Atvur ve Senem Atvur, "21. Yüzyılda Uluslararası Uzay Rejiminin İnsanlığın Ortak Mirası Temelinde Yeniden İnşası"*, Alternatif Politika,* 13:3, 2021, ss. 593–628.

34 Birleşmiş Milletler, *Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space*, BM Genel Kurulu Kararı No. 1962 (XVIII), 13 Aralık 1963, https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/legal-principles.html, erişim 15.04.2025.; 1. ilkede doğrudan uzayın insanlığın ortak yararına kullanılması gerektiği ifade edilirken 1979 tarihli Devletlerin Ay ve Diğer Gök Cisimleri Üzerindeki Faaliyetlerini Düzenleyen Anlaşması'nın 11.maddesine de ışık tutmuştur. Birleşmiş Milletler, *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, BM Genel Kurulu Kararı No. 34/68, 5 Aralık 1979, https://www.unoosa.org/pdf/gares/ARES_34_68E.pdf, erişim 16.04.2025.; Bu çerçevede insanlığın ortak mirası ilkesine uygun olarak yürütülmesi gereken uzay faaliyetlerinde nükleer enerji kullanımın da bu ilkeye uygun bir şekilde yürütülmesi gerektiği kanaatindeyim.

potansiyeli, uluslararası toplum açısından istikrarlı bir güvenlik rejimi kurulmasını zorlaştırmaktadır.[35]

Bu nedenle uluslararası hukuk, nükleer teknolojinin askerî amaçlarla kullanılmasını sınırlamak için çeşitli araçlar geliştirmiştir. 1968 Nükleer Silahların Yayılmasının Önlenmesi Antlaşması (NPT),[36] devletlere barışçıl nükleer teknoloji kullanım hakkını tanımakla birlikte, nükleer silahların yayılmasını önlemeyi temel hedef olarak belirlemiştir.[37] Aynı doğrultuda 1972 tarihli Deniz Tabanı Silah Kontrol Anlaşması,[38] karasuları dışında kalan deniz yatakları ve okyanus tabanına silahların yerleştirilmesini kesin biçimde yasaklamıştır. Böylece uluslararası toplum, nükleer teknolojinin kullanılabileceği jeostratejik alanlardan birini daha denetim altına almıştır.

Nükleer teknolojinin askerî alanlara kaymasını önlemeye yönelik bu düzenlemeler, uzay faaliyetleri için de önemli bir emsal teşkil etmektedir. Zenginleştirme, yeniden işleme ve reaktör geliştirme gibi teknolojilerin barışçıl görünürken askerî kapasite yaratabilmesi, uzayda nükleer enerji kullanımına ilişkin düzenlemelerin neden sıkı bir güvenlik denetimi gerektirdiğini açıkça göstermektedir. Birleşik Krallık'ın "Civil Nuclear: Roadmap to 2050" isimli belgesinde[39] sivil ve askerî nükleer teknolojilerin karşılıklı etkileşimi açıkça vurgulanmış olması da bu ilişkinin günümüzde ne kadar belirgin olduğunu ortaya koymaktadır.

Dolayısıyla çift kullanım riski, yalnızca teknik değil; aynı zamanda hukuki, politik ve güvenlik boyutları olan bir meseledir. NPT, Deniz Tabanı Anlaşması ve IAEA denetim mekanizmaları birlikte değerlendirildiğinde; uluslararası toplumun nükleer enerjiyi hem barışçıl kullanım açısından teşvik etmeye hem de askerî amaçlarla kullanılmasını sınırlandırmaya çalışan bir denge kurmaya çalıştığı görülmektedir. Bu dengeyi korumak, uzayda nükleer enerji kullanımı bakımından da kritik önemdedir.

2.5. Birleşmiş Milletler Genel Kurulu Kararları Açısından Uzayda Nükleer Enerji Kullanımı

1967 Dış Uzay Antlaşması ve 1992 Temel İlkeler'in yanı sıra, BMGK tarafından kabul edilen çeşitli kararlar da nükleer güç kaynaklarının kullanımına ilişkin önemli hükümler içermektedir. Bu kararların ortak noktası, nükleer güç kaynaklarının kullanımında çevresel

35 James M. Acton, "Chapter 1: On the Regulation of Dual-Use Nuclear Technology", Elisa D. Harris (ed.), *Governance of Dual-Use Technologies: Theory and Practice*, Cambridge, Mass.: American Academy of Arts & Sciences, 2016, https://www.amacad.org/publication/governance-dual-use-technologies-theory-and-practice/section/4, erişim 19.08.2025.

36 Birleşmiş Milletler Silahsızlanma İşleri Ofisi, *Treaty on the Non-Proliferation of Nuclear Weapons (NPT),* UNODA, 1968, https://disarmament.unoda.org/wmd/nuclear/npt/, erişim 19.08.2025.; 1968 tarihli Nükleer Silahların Yayılmasının Önlenmesi Antlaşması için bkz.: https://disarmament.unoda.org/wmd/nuclear/npt/, erişim 19.08.2025.

37 Ministry of Foreign Affairs of Japan, "Diplomatic Bluebook 2019", Tokyo: MOFA, 2019, https://www.mofa.go.jp/policy/other/bluebook/2019/html/chapter3/c030104.html, erişim 19.08.2025.

38 Birleşmiş Milletler, *Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Seabed and the Ocean Floor and in the Subsoil Thereof*, 11 Şubat 1971, 18 Mayıs 1972, https://treaties.unoda.org/t/sea_bed, erişim 19.08.2025.; İlgili antlaşma 18 Mayıs 1972 tarihinde yürürlüğe girmiştir.

39 Department for Energy Security and Net Zero (DESNZ), *Civil Nuclear: Roadmap to 2050*, Birleşik Krallık Hükümeti, 11 Ocak 2024, https://assets.publishing.service.gov.uk/media/65c0e7cac43191000d1a457d/6.8610_DESNZ_Civil_Nuclear_Roadmap_report_Final_Web.pdf, erişim 19.08.2025.; Birleşik Krallık hükümeti tarafından yayımlanan "Civil Nuclear: Roadmap to 2050" belgesi, ülkenin uzun vadeli nükleer enerji stratejisini ortaya koyarken aynı zamanda nükleer teknolojinin dual-use niteliğine de dolaylı biçimde işaret etmektedir. Belgede, sivil nükleer altyapının geliştirilmesi ile ulusal güvenlik arasındaki yakın bağ vurgulanmakta; nükleer teknolojinin yalnızca enerji üretimi değil, aynı zamanda askerî denizaltı programları ve stratejik güvenlik kapasiteleri için de kritik rol oynadığı belirtilmektedir. Bu durum, sivil ve askerî nükleer programların birbirini destekleyen bir yapı içinde yürütüldüğünü ve teknolojik yetkinliklerin iki alanda da ortak bir temele dayandığını göstermektedir.

risklerin azaltılması, güvenlik önlemlerinin geliştirilmesi ve uluslararası iş birliğinin güçlendirilmesi gerekliliğinin sürekli vurgulanmasıdır.

1997 tarihli UNGA/A/AC.105/C.1/L.208 sayılı belge,[40] nükleer enerji kaynaklarının uzay görevlerinde kullanımına ilişkin tarihsel olayları ve karşılaşılan riskleri değerlendirmiş; özellikle Cosmos uydularının neden olduğu kazalar üzerinden güvenlik önlemlerinin geliştirilmesi gerektiğini belirtmiştir. Cosmos 954'ün Kanada topraklarına düşerek radyoaktif madde yayması ve Sovyetler Birliği'nin tazminat ödemek zorunda kalması, uluslararası sorumluluk hukukunun bu alandaki önemini net biçimde ortaya koymuştur.[41] Bu olaydan sonra nükleer güç kaynaklarının kontrolsüz şekilde atmosfere yeniden girişinin yaratabileceği küresel sonuçlar, BM tarafından özel olarak ele alınmıştır.

2019 tarihli A/AC.105/C.1/2019/CRP.10 sayılı belge,[42] Avrupa Uzay Ajansı'nın (ESA) nükleer güç kaynaklarının kullanımına ilişkin iç güvenlik politikasını tanıtarak, hukuki ve kurumsal sorumlulukların örgütsel düzeyde nasıl uygulandığını göstermektedir. ESA, BM'nin Güvenlik Çerçevesi ile paralel bir iç politika benimseyerek;[43] görev onay süreçlerini, risk değerlendirmelerini ve acil durum mekanizmalarını kurumsal yapısına entegre etmiştir. Bu politika, ESA'nın yasal ve kurumsal sorumluluk alanı içinde yürütülen program ve faaliyetlerde geçerli olup, sadece ESA personelini bağlayan bir hüküm ifade etmektedir. ESA her ne kadar bir devlet kurumu değil, uluslararası bir örgüt olsa da BM tarafından kabul edilen "Uzayda Nükleer Güç Kaynaklarının Kullanımına İlişkin Güvenlik Çerçevesi" ile Uluslararası Atom Enerjisi Ajansı'nın 2007 tarihli Terimler Sözlüğünde[44] yer alan esaslara atıf yaparak, devletlere yöneltilmiş yükümlülükleri kurumsal işleyişine uyarlama çabasındadır. Bu kapsamda ESA, özellikle devletlere yönelik olarak belirtilen uzay görevlerinde nükleer güvenlik politikasının oluşturulması, uygulama gerekçesinin doğrulanması, görev onay süreçlerinin oluşturulması ve olası acil durumlara hazırlık yapılması gibi hususları, kurum içi işleyişe adapte etmeye çalışmaktadır.

ESA'nın iç güvenlik politikasına göre, nükleer güç kaynağı kullanılacak uzay görevlerinin gerçekleştirilmesi üç aşamalı bir iç yetkilendirme sürecine tabidir. İlk aşamada ESA Üye Devletlerinin uygun görüşünün alınması, ikinci aşamada Genel Direktör tarafından misyonun uygulanmasına izin verilmesi ve son aşamada ESA'nın fırlatma ve operasyon iznini vermesi gerekmektedir. Ancak dikkat çekici biçimde, uzay aracının fırlatılacağı ülkenin hükümeti tarafından yapılacak nükleer güvenlik değerlendirmeleri ve izin süreçleri bu politikanın kapsamı dışında bırakılmıştır. Diğer bir deyişle, ESA yalnızca kendi iç yapısı içerisinde bir onay mekanizması işletmekte, ancak fırlatma devleti tarafından yürütülecek yasal ve idari işlemleri düzenlememektedir.

40 Birleşmiş Milletler Genel Kurulu (UNGA), *Use of Nuclear Power Sources in Outer Space*, Belge No. A/AC.105/C.1/L.208, 13 Şubat 1997, https://www.unoosa.org/res/oosadoc/data/documents/1997/aac_105c_1l/aac_105c_1l_208_0_html/AC105_C1_L208E.pdf, erişim 10.04.2025.; Birleşmiş Milletler, *Working Group on the Use of Nuclear Power Sources in Outer Space,* COPUOS Bilimsel ve Teknik Alt Komitesi, https://www.unoosa.org/oosa/en/ourwork/copuos/stsc/nps/index.html, erişim 19.08.2025.

41 Japan Aerospace Exploration Agency (JAXA), "Space Law and Debris", https://www.jaxa.jp/library/space_law/chapter_3/3-2-2-1_e.htm, erişim 10.04.2025.

42 Birleşmiş Milletler Genel Kurulu (UNGA), *Use of Nuclear Power Sources in Outer Space*, Belge No. A/AC.105/C.1/2019/CRP.10, 08 Şubat 2019, https://www.unoosa.org/res/oosadoc/data/documents/2019/aac_105c_12019crp/aac_105c_12019crp_10_0_html/AC105_C1_2019_CRP10E.pdf, erişim 16.04.2025.

43 K. M. Wright, "Safety for European Space Agency Space Programmes", F. Redmill ve T. Anderson (ed.), *Directions in Safety-Critical Systems*, Springer, London, 1993, ss. 17–35.; Patricia Birnie, Alan Boyle ve Catherine Redgwell, *International Law and the Environment*, 3. Baskı, Oxford University Press, Oxford, 2009, ss. 128-137.

44 Uluslararası Atom Enerjisi Ajansı (IAEA), "IAEA Glossary: Terminology Used in Nuclear Safety and Radiation Protection", 2007 Basımı, 2018 Yayımı, https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf, erişim 15.04.2025.

Politika, yalnızca izin süreçlerine değil, aynı zamanda görev boyunca nükleer güvenliğin sağlanmasına yönelik teknik gerekçelere de yer vermektedir. Bu bağlamda, radyasyon risklerinin mümkün olan en düşük seviyeye indirilmesi, görev döngüsünün tüm safhalarına nükleer güvenliğin entegre edilmesi, olası kazalara karşı zararın sınırlandırılması ve ulusal ve uluslararası düzenlemelere uyum politikada detaylandırılmıştır. Söz konusu uygulama gerekleri, politikanın eklerinde ayrıntılı biçimde yer almaktadır.

2021 tarihli A/AC.105/C.1/L.386 sayılı taslak raporda,[45] 1992 Temel İlkeler ile 2009 IAEA Güvenlik Çerçevesi arasında tutarlı bir uygulamanın sağlanması gerektiği vurgulanmıştır. Buna göre, nükleer güç kaynaklarının yalnızca teknik gereklilik hâlinde kullanılması, güvenlik değerlendirmelerinin güncel bilgiler ışığında yapılması ve uluslararası iş birliğinin güçlendirilmesi gerekmektedir.

2023 tarihli A/AC.105/C.1/L.406/Add.2 sayılı belge,[46] 1992 tarihli Temel İlkeleri'nin konsensüsle kabul edilmiş olmasının, bunların uluslararası teamül hukuku niteliği taşıdığı yönündeki görüşü güçlendirdiğini belirtmiştir. Aynı şekilde, 2009 tarihli Güvenlik Çerçevesinin düzenli olarak uygulanması ve geliştirilmesi gerektiği ifade edilmiştir. Komite ayrıca, nükleer güç kaynaklarının kullanımında barışçıl amaçların korunması, çevreye zarar verilmemesi ve insan sağlığı açısından meydana getirebileceği risklerin azaltılması gerektiğini vurgulamıştır.

Son olarak, 06 Şubat 2024 tarihli A/AC.105/C.1/L.411/Add.10 sayılı karar,[47] 2024–2028 dönemine ilişkin beş yıllık çalışma planını kabul etmiştir. Bu plan üç temel hedefe dayanmaktadır:

1. 2009 IAEA Güvenlik Çerçevesinin uygulanmasını teşvik etmek,
2. Teknik analizler ve geçmiş görevlerden elde edilen verilerle nükleer güvenliği geliştirmek,
3. Bu analizler doğrultusunda somut uygulama adımları belirlemek.

Komite ayrıca, geçmiş ve mevcut uzay görevlerine ilişkin bilgi paylaşımının artırılmasını ve nükleer güç kaynaklarının kullanımında güvenlik politikalarının geliştirilmesini gerekli görmüştür.

Tüm bu kararlar, nükleer enerji kaynaklarının uzayda kullanımının yalnızca teknik bir tercih olmadığı; aksine güvenlik, çevre koruma, insan sağlığı ve uluslararası iş birliği boyutları olan çok katmanlı bir sorumluluk alanı olduğunu kanıtlamaktadır. Bu sebeple, uzayda nükleer enerji kullanımının milletlerarası barış ve güvenlik ilkesi ile uyumlu, çevresel açıdan sürdürülebilir ve tüm devletlerin eşit erişimini gözeten bir anlayışla yürütülmesi gerekmektedir.

45 Birleşmiş Milletler Genel Kurulu, "Draft Report", Belge No. A/AC.105/C.1/L.386, 22 Nisan 2021, https://www.unoosa.org/res/oosadoc/data/documents/2021/aac_105c_1l/aac_105c_1l_386_0_html/AC105_C1_L386E.pdf, erişim 15.04.2025.
46 Birleşmiş Milletler Genel Kurulu, "Draft Decision", Belge No. A/AC.105/C.1/L.406/Add.2, 10 Şubat 2023, https://www.unoosa.org/res/oosadoc/data/documents/2023/aac_105c_1l/aac_105c_1l_406add_2_0_html/AC105_C1_L406Add02E.pdf, erişim 15.04.2025.
47 Birleşmiş Milletler Genel Kurulu, "Draft Decision", Belge No. A/AC.105/C.1/L.411/Add.10, 06 Şubat 2024, https://www.unoosa.org/res/oosadoc/data/documents/2024/aac_105c_1l/aac_105c_1l_411add_10_0_html/AC105_C1_L411Add10E.pdf, erişim 14.04.2025.

Sonuç

Bu çalışma, nükleer enerji kaynaklarının uzay faaliyetlerindeki rolünü yalnızca teknik bir unsur olarak değil, aynı zamanda kapsamlı hukuki ve yönetimsel sonuçlar doğuran çok boyutlu bir mesele olarak ele almıştır. Uygulanan doküman analizi yöntemi sayesinde hem tarihsel misyonlar hem de devlet uygulamaları ayrıntılı biçimde incelenmiş; bu inceleme çalışmanın temel hipotezini destekler nitelikte bulgular ortaya çıkarmıştır. Araştırmanın hipotezi, nükleer güç kaynaklarının uzun süreli ve derin uzay görevlerinde teknik bir zorunluluk olduğunu; ancak bu zorunluluğun devlet sorumluluğu, çevresel koruma ve şeffaflık gerekleriyle sıkı şekilde ilişkilendirildiğinde sürdürülebilir bir çerçeve oluşturabileceğini öne sürmekteydi. Elde edilen bulgular, bu varsayımın hem teknik hem hukuki düzeyde doğrulandığını göstermektedir.

Tarihsel misyonların analizinde görüldüğü üzere, nükleer güç sistemlerinin sağladığı yüksek enerji yoğunluğu, uzun ömürlülük ve çevresel koşullara karşı dayanıklılık, özellikle güneş ışığının yetersiz olduğu veya enerji ihtiyacının sürekli yüksek olduğu görevlerde vazgeçilmezdir. Güneş paneli, batarya veya kimyasal enerji sistemleri gibi alternatif teknolojilerin mevcut fiziki sınırları, nükleer gücün belirli operasyonel senaryolarda teknik olarak ikame edilemeyeceğini ortaya koymaktadır. Bu durum, nükleer enerji kullanımına karşı geliştirilen mutlak ret yaklaşımlarını zayıflatmakta; daha gerçekçi ve risk-temelli bir değerlendirmeyi zorunlu kılmaktadır.

Öte yandan, çalışma boyunca incelenen uluslararası ve ulusal uygulamalar, nükleer enerji kullanımının teknik gerekliliklerle sınırlı olmadığını, beraberinde kapsamlı hukuki yükümlülükler getirdiğini açıkça göstermiştir. Bulgular, devletlerin yalnızca nükleer sistemleri güvenli şekilde tasarlama ve işletme sorumluluğuna sahip olmadığını; aynı zamanda diğer devletleri bilgilendirme, riskleri önceden değerlendirme, çevresel etkileri azaltma, yeniden giriş senaryolarını kontrol altına alma ve şeffaflık ilkesine uygun davranma gibi çok yönlü yükümlülükler taşıdığını ortaya koymuştur. Bu yükümlülükler, nükleer enerjinin uzayda kullanımının yalnızca teknik bir konu değil, aynı zamanda uluslararası toplumun ortak güvenliğini ilgilendiren bir alan olduğunu göstermektedir.

Çalışmanın bulguları ayrıca, nükleer bir kazanın etkilerinin sınır aşan nitelik taşıması nedeniyle tek taraflı güvenlik önlemlerinin yetersiz kalacağını, dolayısıyla uluslararası iş birliği mekanizmalarının güçlendirilmesinin zorunlu olduğunu göstermektedir. Bilgi paylaşımı, erken bildirim, ortak güvenlik standartları, bilimsel veri alışverişi ve kararlı diplomatik koordinasyon, gelecekteki görevler için risklerin azaltılmasında temel araçlar olarak öne çıkmaktadır. Bu durum, nükleer enerji kullanımının yalnızca ulusal kapasiteye bırakılamayacak kadar kritik bir konu olduğunu; sürdürülebilirliğin ancak devletlerin kolektif yaklaşım benimsemeleriyle sağlanabileceğini göstermektedir.

Ayrıca uzayın insanlığın ortak mirası olarak kabul edilmesi, nükleer güç kaynaklarının doğurabileceği her türlü zararın yalnızca bir devleti değil, uluslararası toplumun tamamını ilgilendirdiği anlamına gelmektedir. Uzay çevresinin korunması, yalnızca aktif misyonlardaki güvenlik tedbirleriyle değil, aynı zamanda uzun vadeli çevresel yönetim ve bilimsel temelli yeni enerji alternatiflerinin geliştirilmesiyle mümkündür. Özellikle düşük radyoaktif etki potansiyeline sahip yeni nesil güç sistemleri ve füzyon temelli çözümler, gelecekte nükleer enerji bağımlılığını azaltacak önemli araştırma alanları olarak görülmektedir.

Sonuç olarak bu çalışma, nükleer enerji kullanımının uzay araştırmalarındaki yerinin teknik gereklilikler, hukuki sorumluluklar ve güvenlik standartları bakımından çok boyutlu bir çerçevede değerlendirilmesi gerektiğini ortaya koymuştur. Araştırmanın

hipotezi doğrulanmış; teknik zorunluluklar ile hukuki yükümlülüklerin kesiştiği bir alan olarak nükleer enerji kullanımının mutlak bir yasak ile değil, rasyonel bir yönetim modeliyle sürdürülebilir kılınabileceği sonucuna ulaşılmıştır. Nükleer enerjinin uzayda kullanımının geleceği, yalnızca mevcut teknolojinin sağladığı avantajlara değil, aynı zamanda devletlerin risk yönetim kapasitesine, uluslararası iş birliği iradesine ve şeffaflık ilkelerine bağlı olacaktır. Bu nedenle nükleer enerji, ancak bilimsel bilgiye dayalı, hukuki çerçevesi net biçimde tanımlanmış ve uluslararası koordinasyonla desteklenen bir yaklaşım benimsendiğinde hem uzay çevresinin korunması hem de insanlığın uzun vadeli güvenliği bakımından kabul edilebilir bir araç hâline gelebilecektir.

Çıkar Çatışması

Araştırmanın yazarının herhangi bir çıkar çatışması beyanı bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Çalışmada herhangi bir şekilde yapay zeka uygulamalarından yararlanılmamıştır.

KAYNAKÇA

Basılı Eserler

ACTON James M. (2016). "Chapter 1: On the Regulation of Dual-Use Nuclear Technology", Elisa D. Harris (ed.), *Governance of Dual-Use Technologies: Theory and Practice*, Cambridge, Mass.: American Academy of Arts & Sciences, 8-59.

AFTERGOOD Steven, HAFEMEISTER David W., PRILUTSKY Oleg F., PRIMACK Joel R. ve RODIONOV Stanislav N. (1991). "Nuclear Power in Space", *Scientific American*, 265:6, 42-49.

ASAMOAH Obed. Y. (1966). "Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space", *The Legal Significance of the Declarations of the General Assembly of the United Nations*, Springer, Dordrecht, 129-160.

BAKER Adam M., FREE John H. ve PRIEBE Stephen H. (2002). *Future Power Systems for Space Exploration*, ESA Report 14565/NL/WK, *QinetiQ*, Şubat.

BIRNIE Patricia, BOYLE Alan ve REDGWELL Catherine (2009). *International Law and the Environment* (3. Baskı), Oxford University Press, Oxford.

DABROWSKI Richard (2013). "U.S.–Russian Cooperation in Science and Technology: A Case Study of the TOPAZ Space-Based Nuclear Reactor International Program", *Connections: The Quarterly Journal,* 13:1, 71-87.

DENK Erdem (2020). "Bir Kitle İmha Silahı Olarak Nükleer Silahların Yasaklanmasına Yönelik Çabalar", *Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi*, 66:3, 93-136.

DIEDERIKS-VERSCHOOR H. Ph. (2008). *An Introduction to Space Law,* Kluwer Law International, Lahey.

GALLOWAY Eilene (1979). "Consensus Decision-Making by the United Nations Committee on the Peaceful Uses of Outer Space", *Journal of Space Law*, 7:1, 3-15.

GORBIEL Andrzej (1979). "Some Comments on the Proposal Concerning the Elaboration of New Legal Norms Governing Nuclear Power Sources Use in Outer Space", *Proceedings of the 22nd Colloquium on the Law of Outer Space*, Münih, 131-139.

HAANAPPEL P.P.C. (1984). "Nuclear Power Sources in Outer Space", *Proceedings of the 27th Colloquium on the Law of Outer Space*, 215-217.

KERREST Armel (2003). "The Liability Convention and Liability for Space Activities", *United Nations / International Institute of Air and Space Law Workshop: Papers on Capacity Building in Space Law*, Birleşmiş Milletler, 25-30.

MIRMINA Steven A. ve DEN HERDER David J. (2005). "Nuclear Power Sources and Future Space Exploration", *Chicago Journal of International Law*, 6:1, 149-175.

PATEL Durgambini ve JAWALE Priyanka M. (2021). "Nuclear On-Board: Prospects and Challenges of Outer Space Exploration with Nuclear Power Sources", *Indian Journal of Law and Justice*, 12:1, 11-38.

SUMMERER Leopold, STAPELMANN Armin (2007). "ESA's Approach to Nuclear Power Sources for Space Applications", *ICAPP 2007 – International Congress on Advances in Nuclear Power Plants: The Nuclear Renaissance at Work*, Fukui ve Kyoto, Japonya.

SUMMERER Leopold, WILCOX Trevor, BECHTEL Robert ve HARBISON Stephen (2015). "The International Safety Framework for Nuclear Power Source Applications in Outer Space – Useful and Substantial Guidance", *Acta Astronautica*, 111, 89-101.

ŞİMŞEK Aybüke İnan ve ATVUR Senem (2021). "21. Yüzyılda Uluslararası Uzay Rejiminin İnsanlığın Ortak Mirası Temelinde Yeniden İnşası", *Alternatif Politika*, 13:3, 593-628.

VIIKARI Lotta (2008). *The Environmental Element in Space Law: Assessing the Present and Charting the Future*, Brill, Leiden.

WRIGHT K. M. (1993). "Safety for European Space Agency Space Programmes", F. Redmill ve T. Anderson (eds.), *Directions in Safety-Critical Systems*, Springer, Londra, 17-35.

İnternet Kaynakları

Birleşmiş Milletler (1963). *Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space*, BM Genel Kurulu Kararı 1962 (XVIII), https://www.unoosa.org/oosa/en/ourwork/spacelaw/principles/legal-principles.html, erişim 15.04.2025.

Birleşmiş Milletler (1967). *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies*, UNGA Res. 2222 (XXI), https://docs.un.org/en/A/RES/2222(XXI), erişim 14.04.2025.

Birleşmiş Milletler (1972). *Convention on International Liability for Damage Caused by Space Objects*, UNGA Res. 2777 (XXVI), https://docs.un.org/en/A/RES/2777%20(XXVI), erişim 14.04.2025.

Birleşmiş Milletler (1972). *Declaration of the United Nations Conference on the Human Environment (Stockholm Declaration)*, https://docs.un.org/en/A/CONF.48/14/Rev.1, erişim 13.04.2025.

Birleşmiş Milletler (1976). *Convention on Registration of Objects Launched into Outer Space*, UNGA Res. 3235 (XXIX), https://docs.un.org/en/A/RES/3235%20(XXIX), erişim 14.04.2025.

Birleşmiş Milletler (1979). *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*, BM Genel Kurulu Kararı 34/68, https://www.unoosa.org/pdf/gares/ARES_34_68E.pdf, erişim 16.04.2025.

Birleşmiş Milletler (1991). *Protocol on Environmental Protection to the Antarctic Treaty (Madrid Protocol)*, https://ncpor.res.in/antarcticas/display/411-madrid-protocol, erişim 13.04.2025.

Birleşmiş Milletler (1992). *Principles Relevant to the Use of Nuclear Power Sources in Outer Space*, UNGA Res. 47/68, https://docs.un.org/en/A/RES/47/68, erişim 14.04.2025.

Birleşmiş Milletler (1992). *Rio Declaration on Environment and Development*, https://www.un.org/en/development/desa/population/migration/generalassembly/docs/globalcompact/A_CONF.151_26_Vol.I_Declaration.pdf, erişim 13.04.2025.

Birleşik Krallık Enerji Güvenliği ve Net Sıfır Departmanı (2024). *Civil Nuclear: Roadmap to 2025*, https://assets.publishing.service.gov.uk/media/65c0e7cac43191000d1a457d/6.8610_DESNZ_Civil_Nuclear_Roadmap_report_Final_Web.pdf, erişim 19.08.2025.

Birleşmiş Milletler Genel Kurulu (1997). *Working Paper, A/AC.105/C.1/L.208*, UNGA, https://www.unoosa.org/res/oosadoc/data/documents/1997/aac_105c_1l/aac_105c_1l_208_0_html/AC105_C1_L208E.pdf, erişim 10.04.2025.

Birleşmiş Milletler Genel Kurulu (2019). *Conference Room Paper, A/AC.105/C.1/2019/CRP.10*, UNGA, https://www.unoosa.org/res/oosadoc/data/documents/2019/aac_105c_12019crp/aac_105c_12019crp_10_0_html/AC105_C1_2019_CRP10E.pdf, erişim 16.04.2025.

Birleşmiş Milletler Genel Kurulu (2021). *Draft Report, A/AC.105/C.1/L.386*, UNGA, https://www.unoosa.org/res/oosadoc/data/documents/2021/aac_105c_1l/aac_105c_1l_386_0_html/AC105_C1_L386E.pdf, erişim 15.04.2025.

Birleşmiş Milletler Genel Kurulu (2023). *Decision, A/AC.105/C.1/L.406/Add.2*, UNGA, https://www.unoosa.org/res/oosadoc/data/documents/2023/aac_105c_1l/aac_105c_1l_406add_2_0_html/AC105_C1_L406Add02E.pdf, erişim 15.04.2025.

Birleşmiş Milletler Genel Kurulu (2024). *Decision, A/AC.105/C.1/L.411/Add.10*, UNGA, https://www.unoosa.org/res/oosadoc/data/documents/2024/aac_105c_1l/aac_105c_1l_411add_10_0_html/AC105_C1_L411Add10E.pdf, erişim 14.04.2025.

Birleşmiş Milletler Silahsızlanma İşleri Ofisi (1968). *Treaty on the Non-Proliferation of Nuclear Weapons (NPT),* UNODA, https://disarmament.unoda.org/wmd/nuclear/npt/, erişim 19.08.2025.

Birleşmiş Milletler Silahsızlanma İşleri Ofisi (1971). *Treaty on the Prohibition of the Emplacement of Nuclear Weapons and Other Weapons of Mass Destruction on the Sea-Bed and the Ocean Floor and in the Subsoil Thereof,* UNODA, https://treaties.unoda.org/t/sea_bed, erişim 19.08.2025.

Birleşmiş Milletler Uzay İşleri Ofisi (t.y.). "Nuclear Power Sources Working Group", *UNOOSA*, https://www.unoosa.org/oosa/en/ourwork/copuos/stsc/nps/index.html, erişim 19.08.2025.

Interesting Engineering. "Startups Partner for Nuclear-Powered Spacecraft", https://interestingengineering.com/space/startups-partner-for-nuclear-powered-spacecraft, erişim 19.08.2025.

Japan Aerospace Exploration Agency (JAXA) (t.y.). "Space Law and Debris", https://www.jaxa.jp/library/space_law/chapter_3/3-2-2-1_e.htm, erişim 10.04.2025.

Ministry of Foreign Affairs of Japan (2019). "Diplomatic Bluebook 2019", Tokyo, MOFA, https://www.mofa.go.jp/policy/other/bluebook/2019/html/chapter3/c030104.html, erişim 19.08.2025.

NASA (2010). "Iridium–Cosmos Collision: Post-Event Analysis", https://ntrs.nasa.gov/api/citations/20100002023/downloads/20100002023.pdf, erişim 10.04.2025.

NASA, "Cassini Mission", *NASA Science*, https://science.nasa.gov/mission/cassini/, erişim 14.04.2025.

NASA, "Galileo Mission", *NASA Science*, https://science.nasa.gov/mission/galileo/, erişim 14.04.2025.

NASA, "Radioisotope Power Systems – FAQ", *NASA Science*, https://science.nasa.gov/planetary-science/programs/radioisotope-power-systems/faq/, erişim 20.08.2025.

ScienceDirect, "Thermionic Power Generation", *ScienceDirect Topics*, https://www.sciencedirect.com/topics/engineering/thermionic-power-generation, erişim 20.08.2025.

Secure World Foundation (2012). "Iridium–Cosmos Collision Fact Sheet", https://swfound.org/media/6575/swf_iridium_cosmos_collision_fact_sheet_updated_2012.pdf, erişim 10.04.2025.

Stockholm Uluslararası Barış Araştırmaları Enstitüsü (1983). "Nuclear Power Sources on Satellites in Outer Space", *SIPRI*, SIPRI Fact Sheet No. 83/1.

Trail Smelter Arbitration (United States v. Canada) (1938–1941). "ABD–Kanada Uluslararası Hakemliği Kararı", https://legal.un.org/riaa/cases/vol_iii/1905-1982.pdf, erişim 13.04.2025.

Türkiye Büyük Millet Meclisi (1967). *Ay ve Diğer Gök Cisimleri Dâhil, Uzayın Keşfi ve Kullanılmasında Devletlerin Faaliyetlerini Yöneten İlkeler Hakkında Andlaşma*, Resmî Gazete No. 12655, https://www5.tbmm.gov.tr/tutanaklar/KANUNLAR_KARARLAR/kanuntbmmc050/kanuntbmmc050/kanuntbmmc05000902.pdf, erişim 13.04.2025.

U.S. Department Of Energy (2015). "The History of Nuclear Power in Space", https://www.energy.gov/articles/history-nuclear-power-space, erişim 10.06.2025.

U.S. Department Of Energy. "System for Nuclear Auxiliary Power (SNAP) Overview", https://www.energy.gov/etec/system-nuclear-auxiliary-power-snap-overview, erişim 14.04.2025.

Uluslararası Atom Enerjisi Ajansı (1986). *Convention on Early Notification of a Nuclear Accident*, https://www.iaea.org/sites/default/files/infcirc335.pdf, erişim 15.04.2025.

Uluslararası Atom Enerjisi Ajansı (2009). *Safety Framework for Nuclear Power Source Applications in Outer Space*, https://www.unoosa.org/pdf/reports/ac105/AC105_934E.pdf, erişim 13.04.2025.

Uluslararası Atom Enerjisi Ajansı (2018*).* "IAEA Glossary: Terminology Used in Nuclear Safety and Radiation Protection", https://www-pub.iaea.org/MTCD/Publications/PDF/PUB1830_web.pdf, erişim 15.04.2025.

Uluslararası Atom Enerjisi Ajansı (1986). *Convention on Early Notification of a Nuclear Accident – Overview,* https://www.iaea.org/topics/nuclear-safety-conventions/convention-early-notification-nuclear-accident, erişim 15.04.2025.

Unıted States National Archives (1963). *Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water*, https://www.archives.gov/milestone-documents/test-ban-treaty, erişim 14.04.2025.

GÜVENLİK STRATEJİLERİ DERGİSİ

Güv. Str. Derg. 2025, 21:52, 497-527
DOI: 10.17752/guvenlikstrtj.1708636

Araştırma Makalesi
Research Article

Askerî Etik Eğitimi: West Point ve Kara Harp Okulu

Military Ethics Education: West Point and Turkish Military Academy

Gizem Nur DEMİREL*

* Doktora Öğrencisi, Ludovika University of Public Service, Faculty of Military Sciences and Officer Training, Budapeşte, Macaristan (MSÜ ATASAREN öğrencisi, Erasmus Öğrenci Değişim Programı kapsamında Ludovika'da bulunmaktadır.)
e- posta: demirel.gizem.nur@stud.uni-nke.hu ORCID: 0000-0001-8129-9574

Geliş Tarihi / Submitted: 29.05.2025

Kabul Tarihi / Accepted: 06.11.2025

Öz

Türkiye'de etik üzerine yapılan akademik çalışmalar büyük oranda uluslararası ilişkiler, iklim ve teknolojiye odaklanmıştır. Askerî alanda etik araştırmalarının ihmal edildiği, var olan birkaç araştırmanın da genellikle savaş etiğine odaklandığı ve askerî etik eğitimi konusunun derinlemesine incelenmediği görülmektedir. Bu kapsamda çalışmada nitel bir vaka çalışması tasarımı kullanılarak, askerî etik kavramı tanımlanmakta, askerî etik eğitiminin Harp Okulu düzeyinde nasıl planlandığını West Point ve Kara Harp Okulu örneği ile; mesleki yaşam boyunca nasıl olması gerektiğini ise NATO "Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı" belgesi ile incelenmektedir. Bulgular, sistematik etik eğitiminin subayların karakter gelişimini desteklediğini ve askerlik mesleğinin misyonunu, değerlerini ve düzenlemelerini içselleştirmelerini sağlayarak ortak bir profesyonel anlayış geliştirdiğini göstermektedir.

Anahtar Kelimeler: Etik, Askerî Etik, Askerî Etik Eğitimi, Harbiye, West Point

Abstract

In Türkiye, scholarly work on ethics has tended to emphasize international relations, climate, and technology, while military ethics—distinct from the ethics of war—remains underexamined. This study defines military ethics as a professional normative framework that integrates character, judgment, and institutional values, and examines how it is taught to military officers. Using a qualitative case-study design, it analyzes the structure and delivery of ethics education at the pre-commissioning level at both the United States Military Academy at West Point and the Türkiye's Military Academy-Harbiye. It also analyzes NATO's Generic Officer Professional Military Education Reference Curricula to assess when, where, and how ethical formation is embedded across the learning continuum. Findings indicate that systematic ethics education fosters officers' character development and cultivates a shared professional understanding by enabling them to internalize the mission, values, and regulations of the military profession.

Keywords: Ethics, Military Ethics, Military Ethics Education, Turkish Military Academy, West Point

Extended Summary

The current complex and multidimensional security environment indicates that armies' tasks will extend beyond the traditional battlefield. In this context, armies operate across a wide range of areas beyond national defense. In the expanding range of duties, it is possible for military personnel to manage ambiguous and complex situations where the law is insufficient, to define what the right behavior is, and to act by prioritizing the army's values. Military ethics education supports personnel's character development and fosters a shared ethical awareness by enabling them to internalize the values, rules, and goals of the military profession. In this context, the formation of common military ethics awareness in the Armed Forces is carried out through military ethics education.

This study aims to clarify the definition of military ethics education and its implementation at the officer level. The study uses a qualitative research method. The case study examines how the military ethics education is planned at the military academy level by using West Point and the Turkish Military Academy as examples. The study also outlines the concept of professional development throughout an officer's life by examining the Generic Officer Professional Military Education Reference Curriculum document. While analyzing the documents that constitute the source of the case study, foreign sources were mostly used due to the inadequacy of resources in Türkiye regarding military ethics education. These sources include official military websites, military publications, reports, manuals, doctrines, and articles.

The literature review reveals that the definition of the concepts of military ethics and military ethics education is incomplete, that the importance of military ethics education is unaddressed, that military ethics is discussed only within the scope of war ethics, and that the military ethics education of West Point and the Turkish Military Academy has not been examined historically. In this context, this study will contribute to the literature by defining military ethics and military ethics education, distinguishing between the concepts of military ethics and war ethics, understanding the importance of military ethics education, and examining the military ethics education of West Point and the Turkish Military Academy historically.

The research has encountered certain limitations. The first of the most obvious limitations is that, although the ethics education curriculum at West Point can be examined in detail, a direct curricular comparison between the two institutions cannot be conducted due to the absence of courses with similar content at the Turkish Military Academy. The second limitation is that, since there are no existing studies examining the historical development of the military ethics curriculum at the Turkish Military Academy, the study has not been able to conduct a comparative analysis. West Point and the Turkish Military Academy were chosen to illustrate how military ethics education is provided at the officer level for several reasons: military ethics is regarded as an important value, courses on military ethics have been offered at the military academy level since the early 19th century, and both academies are internationally recognized for offering education to students from various countries. One of the reasons for choosing West Point is the easy accessibility of its curriculum documents. The Generic Officer Professional Military Education Reference Curriculum was selected because it includes information on which learning methods can be used, which issues should be considered when covering the subjects, and the creation of an education plan suitable for each officer level with the philosophy of lifelong learning.

Military ethics consists of a set of rules that require military personnel to act not only in accordance with legal regulations but also in accordance with universal moral principles, values of the military profession, and an understanding of social responsibility. Military ethics is a crucial competency that personnel at all levels must acquire, develop, and strengthen throughout their professional life. Military ethics education is essential for achieving these goals.

Military ethics education has a deep-rooted history at both West Point and the Turkish Military Academy. Since its establishment, West Point has given importance to military ethics education and has developed military ethics courses over time. Currently, West Point has a developmental, gradual, and multidimensional military ethics education. This education is reorganized in line with the needs of cadets in each class. At the Turkish Military Academy, similar to West Point, there are related courses and publications stating that military ethics education is important. However, when the curriculum of the Turkish Military Academy is examined, one can see that military ethics is not offered as a separate course and that the issue of military ethics is included in the Military Sociology course. It is noteworthy to mention that the Book of Military Sociology integrates military ethics within the ethics of war, and this creates a deficiency in understanding military ethics.

The Generic Officer Professional Military Education Reference Curriculum is an educational program that reflects the learning philosophy of the armed forces. This education program progresses in a holistic way based on previous information and experiences in line with the needs of the entire officer corpus. The Generic Officer Professional Military Education Reference Curriculum can be designed according to the basic values, rules, and legal frameworks of the countries and included in the education systems of the armed forces.

Finally, for military ethics, which is a separate discipline, it is considered that its experts should receive appropriate training. In addition to theoretical education, practical education should be given importance: Contemporary cases should be analyzed; the simulation method should be used for performance evaluation; augmented reality, virtual reality, and mixed reality applications should be used to create realistic scenarios; and the courses should be taught by experienced personnel.

Giriş

Günümüzde orduların, görev alanlarının geleneksel muharebe sahasına ek olarak düzensiz göçün engellenmesine yönelik tedbir ve mücadele, doğal afetlere müdahale, arama kurtarma ve sonrasındaki iyileştirme faaliyetleri, çok boyutlu harp ortamında siber saldırılara karşı koyma, insani yardım ve tahliye operasyonları**,** barışı destekleme ve koruma operasyonları kapsamında bir genişleme gösterdiği görülmektedir. Askerî personelin, genişleyen görev yelpazesinde kanunların yetersiz kaldığı belirsiz ve karmaşık durumları yönetebilmesi, doğru davranışın ne olduğunu tanımlayabilmesi ve kurumunun değerlerini önceleyerek hareket edebilmesi askerî etik eğitimi ile mümkündür. Askerî etiğin önemi iki temel perspektiften açıklanabilir. Bunlardan birincisi, personelin karakter gelişimini desteklemesidir. İkincisi, personelin askerlik mesleğinin değerlerini, kurallarını, amaçlarını öğrenme süreçlerini içselleştirmelerine olanak tanıyarak ortak bir etik bilinci oluşturmasıdır. Silahlı kuvvetlerde ortak askerî etik bilinci, askerî etik eğitiminin varlığı ile mümkündür.

Çalışmanın amacı, askerî etiğin ne olduğunu açıklamak ve subay sınıfında askerî etik eğitiminin nasıl verildiğini incelemektir. Bu kapsamda çalışmanın temel sorusu, "askerî etik nedir ve subay sınıfı düzeyinde askerî etik eğitimi nasıl verilmektedir?" şeklinde belirlenmiştir. Araştırmanın alt soruları ise:

1. Askerî etik ve askerî etik eğitimi nedir?
2. Askerî etik ve savaş etiği arasındaki farkın kavramsal farklılıklarının tanımı nasıldır?
3. West Point ve Kara Harp Okulu askerî etik eğitiminin tarihi ve günümüzdeki müfredatı nasıldır?
4. Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı'nın askerî etik eğitimindeki önemi nedir?
5. Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı'nın askerî etik bilincinin gelişimindeki rolü nedir?

Çalışma nitel araştırma yöntemine göre tasarlanmıştır. Çalışmanın araştırma deseni olan durum çalışması, askerî etik ve askerî etik eğitimi kavramlarının West Point ve Kara Harp Okulu askerî etik eğitimi dersleri ile Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı belgesi özelinde incelenmesine dayanmaktadır. Durum çalışması deseni, askerî etik eğitiminin iki farklı kurumda nasıl yapılandırıldığını anlamak amacıyla tercih edilmiştir. Bu kapsamda ilgili ders içerikleri ve müfredat belgeleri doküman analizi yöntemiyle sistematik biçimde incelenmiştir. Durum çalışmasının kaynağını oluşturan doküman analizi yapılırken askerî etik eğitimi ile ilgili Türkiye'deki kaynakların yetersiz olması nedeniyle çoğunlukla yabancı kaynaklardan yararlanılmıştır. Bu kaynaklar resmi askerî internet sitelerini, askerî yayınları, raporları, talimnameleri, doktrinleri ve makaleleri içermektedir.

Literatür taraması sonucunda yabancı kaynaklardaki askerî okullarda verilen askerî etik eğitiminin tarihsel süreç veya karşılaştırmalı boyutlarıyla ele alındığı çalışmaların sınırlı olduğu ve doğrudan bu konuyu inceleyen çalışmaların bulunmadığı görülmüştür. İlgili çalışmalara bakıldığında Gaitán-Monje ve De Castro García'nın 2023 yılında yayınlanan "En búsqueda de la mejor formación de oficiales: academia militar de España vs. West Point"[1] adlı makalesi İspanya ve Amerika'nın subay eğitim modelinin karşılaştırmalı olarak incelemektedir. Makale, West Point'te karakter gelişimi programının etik değerler, karakter eğitimi ve liderlik gelişimini uzun vadeli bir müfredat çerçevesinde işlediğini, Academia General Militar'de ise bu unsurların müfredatta yer almadığını yalnızca liderlik planı aracılığıyla yürütüldüğünü göstermektedir.

Peperkamp ve arkadaşlarının 2023 yılında yayınlanan "Military Ethics and Military Ethics Education in Search of a European Approach"[2] adlı makalesinin amacı, Avrupa'da ortak bir askerî etik ve askerî etik eğitimi yaklaşımının mevcut olup olmadığını incelemek ve farklı ülkelerdeki uygulamaları karşılaştırarak benzerlik ile farklılıkları tespit etmektir. Makale, Hollanda ve Avustralya örnekleri kapsamında etik eğitimin amaç, içerik, yöntem, kuramsal temeller ve ele alınan konular kapsamında önemli farklılıklar gösterdiğini vurgular. Sonuç kısmında da tek bir Avrupa askerî etik anlayışından söz etmenin zor olduğunu fakat bu çeşitliliğin Avrupa'da askerî etik eğitimin gelişimi için önemli bir zenginlik oluşturduğu ifade edilir. Stanar'ın 2023 yılında yayınlanan "Military Ethics Education Bridging the Gap or Deepening the Chasm"[3] adlı makalesi askerî etik eğitiminin uygulanma biçiminin ordu ve toplum arasındaki ilişkiyi şekillendirdiğini savunmaktadır. Makale, ordu ile

1 Enrique Gaitán-Monje ve Andrés de Castro-García, "En búsqueda de la mejor formación de oficiales Academia militar de España vs. West Point", *Revista Colombiana de Estudios Militares y Estratégicos*, 21:44, 2023.

2 Lonneke Peperkamp, Kevin van Loon, Deane-Peter Baker ve David Evered, "Military Ethics and Military Ethics Education: In Search of a 'European Approach'", *Ethics and Armed Forces: Controversies in Military Ethics and Security Policy: Core Issues of European Military Ethics*, 02, 2023.

3 Dragan Stanar, "Military Ethics Education – Bridging the Gap or Deepening the Chasm?", *Ethics and Armed Forces: Controversies in Military Ethics and Security Policy: Core Issues of European Military Ethics*, 02, 2023.

toplum arasındaki mesafeyi artıran Huntington'un "*objective contro*" (nesnel kontrol) paradigmasına dikkat çeker. Askerî etik eğitiminin personelin moral ve etik sorumluluklarını içselleştirmelerine yardımcı olacağı ancak yanlış uygulandığında ise orduyu toplumdan üstün görme duygusunu güçlendirebileceği iddia edilir. Bu nedenle askerî etik eğitimi, toplumla daha güçlü bir bağ kurmayı hedeflemelidir. Ayrıca makale, askerî etik eğitimlerinin farklı ülkelerde farklı yaklaşımlarla uygulandığını vurgular. Bazı ülkelerde işlevsel bir yaklaşım benimsenirken bazı ülkelerde karakter gelişimine odaklanan hedeflenen bir yaklaşım öne çıkar. Bu çeşitlilik askerî etik eğitiminin evrensel bir standart yerine kültürel ve toplumsal bağlamlara göre şekillendiğini göstermektedir. Gillner'in 2019 yılında yayınlanan "Ethical Education in the German Armed Forces: Embraced Values and Moral Judgement"[4] adlı makaleye göre Alman Silahlı Kuvvetleri'nde askerî etik eğitimi, personelin yalnızca yasal düzenlemelere uymalarını değil, insan onuru, özgürlük, barış, adalet, eşitlik ve demokrasi gibi temel değerlere dayalı etik bir bilinç geliştirmelerini amaçlamaktadır. Bu değerler Almanya Anayasası'ndaki ilkelerle uyumlu olup "*Innere Führung*" (iç liderlik) konseptiyle askerî uygulamalara uyumlu hale getirilir. Burada askerî etik eğitimi teorik bilgi sunmanın ötesinde, değer temelli etik bilinç oluşturmayı amaçlayan bir süreç olarak tasarlanmıştır. Askerlerin etik kararlar alabilme yeteneklerini geliştirmek için deneyimsel öğrenme, vaka analizleri, tartışma ve eleştirel düşünme yöntemleri uygulanmaktadır. Ayrıca duygusal ve bilişsel yaklaşımlar, ahlaki duyguların geliştirilmesi ve üst düzey liderlerin rol model olması da eğitimde önemli bir yer tutmaktadır. Kullanılan yöntemler personelin etik değerleri içselleştirmelerini ve pratikte uygulamalarını sağlamaktadır.

Lohmann'ın 2019 yılında yayınlanan "*Ethical Education – A Central Component of Training and Development in the German Armed Forces*"[5] adlı makalesinde Alman Silahlı Kuvvetleri'nde (Bundeswehr) askerî etik eğitiminin önemini vurgulamaktadır. Makale, etik eğitimin yalnızca bilgi aktarımı değil, aynı zamanda duygusal ve bilişsel düzeyde değerlerin içselleştirilmesi ve uygulanması süreci olduğunu belirtmektedir. Bu yaklaşım personelin "ne yapması gerektiğini" değil, "neden yapması gerektiğini" anlamasını hedefler. Askerî etik eğitimin, askerî bir zorunluluk olmaktan çok personelin kişisel gelişimi ve toplumla uyumlu bir şekilde hizmet etmesi için temel bir unsur olduğu vurgulanmaktadır. Troy tarafından 2024 yılında yayınlanan "Ethics as Moral Practice in Peacekeeping Missions: Insights on the Importance of Ethical Training"[6] başlıklı makale, barış gücü misyonlarının temelinde yatan etik boyutu incelemektedir. Makalenin amacı, barışı koruma faaliyetlerinin bir pratik etik alanı olarak tanımlanması gerektiğidir. Mevcut askerî etik eğitim yaklaşımlarındaki yetersizlikler, etik uygulamalara yönelik standart belirleme süreçlerinde problemlere yol açmakta ve bu durum askerî etik eğitimin yeniden ele alınması gerekliliğini ortaya koymaktadır. Makale hem teorik hem de pratik avantaj ve dezavantajlarını göstermek için Avusturyalı barış gücü askerlerinin etik eğitimini detaylı bir örnek olay olarak kullanmaktadır.

Türkiye'deki askerî etik ile ilgili kaynaklara bakıldığında Mert'in *Türk Savaş Çalışmaları* dergisinde 2020 yılında yayınlanan "Askerî Etik"[7] başlıklı çalışması askerî etik kavramının tanımını sınırlı olarak içerdiği ve askerî etiğin savaş etiği kapsamında ele alındığı görülmektedir. Bu çalışmada askerî etik kavramı yerine savaş etiği kavramı ön plana çıkmaktadır. Ateş'in 2022 yılında yayınlanan *Askerî Sosyoloji Ordu ve Toplum*

4 Matthias Gillner, "Ethical Education in the German Armed Forces: Embraced Values and Moral Judgement", *Ethics and Armed Forces: Controversies in Military Ethics and Security Policy: Between Personality Development and Skills Acquisition: Ethics for Soldiers, 02, 2019.*

5 Friedrich Lohmann, "Ethical Education – A Central Component of Training and Development in the German Armed Forces", *Ethics and Armed Forces: Controversies in Military Ethics and Security Policy: Between Personality Development and Skills Acquisition: Ethics for Soldiers*, 02, 2023.

6 Jadok Troy, "*Ethics as Moral Practice in Peacekeeping Missions: Insights on the Importance of Ethical Training*", *International Peacekeeping*, 31:3, 2024.

7 İbrahim Mert Sani, "Askeri Etik", *Turkish Journal of War Studies*, 1:1, 2020.

Araştırmaları[8] kitabında yer alan "Savaş Etiği" bölümünde askerî etik kavramının kısaca ne olduğunun açıklandığı, askerî etiğin öneminden bahsedildiği, savaş etiği ve askerî etiğin iki ayrı unsur olarak belirtildiği görülmektedir. Ünal'ın 2024 yılında *İstanbul Üniversitesi Şarkiyat Mecmuası'*nda yayınlanan "Megan Cassidy-Welch'in "Crusades and Violence*"* Adlı Eserinin Değerlendirilmesi"[9] kitap değerlendirmesinde adil savaş teorisinin, savaş etiği kapsamında değil askerî etik doktrini olarak ele alındığı görülmektedir. Benzer kullanımı Birdişli'nin 2023 yılında *Ankara Üniversitesi Siyasal Bilimler Fakültesi Dergisi*'nde yayınlanan "Uluslararası Kurumların Normatif Bir Unsuru Olarak Uluslararası Güvenlik"[10] adlı makalesinde de görmekteyiz. Bu iki çalışmadaki kullanım askerî etik ve savaş etiği kavramlarının anlamı noktasında bir karmaşa yaşandığını göstermektedir. Jandarma ve Sahil Güvenlik Akademisi Güvenlik Araştırmaları Merkezi Müdürlüğü tarafından 2023 yılında *30 Soruda Jandarma* kitap serisi yayınlanmıştır. Bu kitap serisinde beşinci kitap olarak Mehmet Avcı tarafından hazırlanan "Jandarma ve Etik"[11] çalışmasında kolluk etiği kavramı tanımlanmakta ve belirlenen 30 soru kapsamında da kolluk etiği incelenmektedir. Bademli'nin 2024 yılında yayınlanan "Türkiye'de Ordu ve Siyaset: Sivil-Asker İlişkilerinin Dönüşümü"[12] adlı doktora tezinde askerî etiğin ideolojiler çerçevesinde değerlendirildiği fakat askerî etik kavramının tanımı noktasında yetersiz kaldığı görülmektedir. Bu kapsamda çalışmanın; askerî etik ve askerî etik eğitiminin tanımlanması, askerî etik ve savaş etiği kavramlarının ayrımının yapılması, askerî etik eğitiminin öneminin kavranması, West Point ve Kara Harp Okulu askerî etik eğitimlerinin tarihsel olarak incelenmesiyle alanyazına katkı sağlayacağı düşünülmektedir.

Çalışmanın sınırlılıkları; askerî etik ve askerî etik eğitimi kavramlarının tanımı, incelemenin yalnızca subay sınıfı üzerinden yürütülmesi, West Point ve Kara Harp Okulu'ndaki askerî etik eğitimi tarihi ve derslerinin incelenmesi ile Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı belgesindeki etik müfredatın esas alınması çerçevesinde şekillenmektedir. Bununla birlikte en belirgin sınırlılıklardan birincisi West Point'te etik eğitiminin müfredat düzeyinde ayrıntılı olarak incelenebilmesine karşın Kara Harp Okulu'nda benzer içerikte derslerin bulunmaması nedeniyle iki kurum arasında doğrudan bir müfredat karşılaştırmasının yapılamamasıdır. İkincisi Harp Okulu'ndaki askerî etik müfredatının tarihsel gelişimini inceleyen herhangi bir çalışmanın bulunmaması nedeniyle, bu çalışmanın karşılaştırmalı bir analizinin gerçekleştirilememesidir.

Subay sınıfı düzeyinde askerî etik eğitimin nasıl verildiğini açıklamak için West Point ve Kara Harp Okulu'nun seçilme nedenleri, askerî etiğin önemli bir değer olarak görülmesi, 19. yüzyılın ilk yarısından itibaren Harp Okulu düzeyinde askerî etik ile ilgili derslerin veriliyor olması, birçok ülkeden öğrenciye eğitim imkânı sunması nedeniyle uluslararası alanda tanınırlığının fazla olmasıdır. West Point'in seçilme nedenlerinden bir diğeri eğitim müfredatına dair dokümanların kolay ulaşılabilir olmasıdır. Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı'nın seçilme nedenleri ise yaşam boyu öğrenme felsefesiyle her bir subay sınıfına uygun eğitim planının oluşturulması, konular işlenirken hangi hususların dikkate alınması gerektiğinin belirtilmesi ve hangi öğrenme yöntemlerinin kullanılabileceğine dair bilgileri içermesidir.

8 Barış Ateş, *Askerî Sosyoloji Ordu ve Toplum Araştırmaları,* Selenge Yayınları, İstanbul, 2022, s. 166.

9 Elif Ünal, "Megan Cassidy-Welch'in 'Crusades and Violence' Adlı Eserinin Değerlendirmesi", *Şarkiyat Mecmuası - Journal of Oriental Studies,* 44, 2024, s. 311.

10 Fikret Birdişli, "Uluslararası Kurumların Normatif Bir Unsur Olarak Uluslararası Güvenlik", *Ankara Üniversitesi SBF Dergisi,* 78:2, 2023, s. 400.

11 Mehmet Avcı, *30 Soruda Jandarma ve Etik,* JSGA Basımevi Müdürlüğü, Ankara, 2023.

12 Hakan Bademli, "Türkiye'de Ordu ve Siyaset: Sivil-Asker İlişkilerinin Dönüşümü", Doktora Tezi, Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı Siyaset ve Sosyal Bilimler Bilim Dalı, 2024.

Çalışmada askerî etik kavramının anlaşılabilmesi için öncelikle etik kavramı açıklanmıştır. Etik ve ahlak kavramları ile askerî etik ve savaş etiği kavramları arasındaki farka değinilerek askerî etik eğitiminin ne olduğu, neden gerek gerekli olduğu ele alınmıştır. Askerî etik eğitiminin Harp Okulu düzeyinde West Point ve Kara Harp Okulu kapsamında, mesleki yaşamda nasıl olması gerektiği ise Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı belgesi kapsamında incelenmiştir.

1. Askerî Etik

Askerî etik, ahlak ve toplum kuralları ile meslek, savaş, görev, erdem ve hukuk etiğini içerisinde barındıran çok boyutlu bir kavramdır. Alanyazın incelemesi sonucunda Silahlı Kuvvetlerde askerî etik kavramı yerine meslek etiği kavramının da kullanıldığı görülmektedir. Aynı zamanda askerî etik kavramının, meslek etiği kavramının bir alt dalı olarak değerlendirildiği çalışmalar da bulunmaktadır. Örneğin Türk Silahlı Kuvvetleri Meslek Etiği Yönergesi'ne göre meslek etik kuralları incelendiğinde askerlik yeminine sadakat göstermek, anayasa ve yasalara bağlı olmak, askerlik mesleğini yaşam tarzı olarak tatbik etmek, emir ve itaat anlayışı içinde olmak, adil olmak, insan haklarına saygı göstermek, yetki kullanımı, kurumsal itibara zarar verici davranışlardan kaçınmak, sağlam bir ahlaka sahip olmak, askerî nezaket ve terbiye kurallarına uymak, astlarını sürekli gözetmek, yükümlü askerlere en iyi imkan sağlama gayreti, takdir hakkını her koşulda objektif kullanmak, dürüst ve denetime açık olmak, tevazu sahibi olmak, ast-üst ilişkilerinde profesyonel olmak, astların fikir ve düşüncelerine saygı göstermek maddeleri askerî etiğin inceleme alanına girmektedir.[13] Bu kapsamda meslek etiği, kanunlardan farklı olarak mesleki uygulamaları yönlendiren, personelin davranışlarını değerlendiren, mesleğe özgü ahlaki ilkeler bütününü oluşturmaktadır.[14] Fakat bu kavramın askerî etik kavramı kadar çok boyutlu olmaması ve Silahlı Kuvvetlerin etik anlayışını ifade etmekte yetersiz kalması nedeniyle çalışmada askerî etik kavramının kullanılması daha doğru bulunmuştur. Bu kapsamda askerî etik kavramını açıklamadan önce etik kavramını incelemek gerekmektedir.

Etik, bireylerin davranışlarını doğru-yanlış, adil-adaletsiz, erdemli-erdemli olmayan şeklinde kategorize ederek inceleyen bir felsefe dalıdır.[15] Etik kavramının tanımlanması noktasında kurumların yaklaşımlarında karmaşık bir yapı bulunmaktadır. Bu karmaşık yapıyı üç şekilde inceleyebiliriz. Birincisi etik kavramının ahlak ile eş anlamlı olduğu yaklaşımdır. Bu yaklaşıma göre etik eğitiminin temel amacı, karakter gelişiminin sağlanmasıdır. İkinci yaklaşım ise etik kavramının ahlak kavramından farklı olduğunu belirtmektedir. Bu yaklaşıma göre etik eğitiminin amacı, karakter gelişiminin yanında icra edilen mesleğin amaçları ve yöntemleri doğrultusunda mesleği destekleyen değerler hakkında bireylere anlayış kazandırmaktadır. Üçüncüsü ise etik kelimesinin yerine "ethos" kelimesinin kullanıldığı yaklaşımdır. "Ethos", topluluk üyelerinin davranışlarına rehberlik eden ve somut olmayan bir ruhu temsil edilmektedir.[16]

Etik kelimesinin kökeni incelendiğinde Yunanca'da *ēthos* ve *ēthikē*, Latince'de *ethice*, eski Fransızca'da *éthique* sonrasında ise İngilizce'de *ethic* olarak karşımıza çıkmaktadır.[17]

13 "Türk Silahlı Kuvvetleri Meslek Etiği Yönergesi".

14 David Whetham, "What Senior Leaders in Defence Should Know about Ethics and the Role That They Play in Creating the Right Command Climate The Leadership Edge", *The International Journal of Ethical Leadership,* 8:19, 2021, s. 3.

15 Stephen Coleman, "Ethical Dilemmas and Tests of Integrity", *Key Concepts in Military Ethics*, ed. Deane-Peter Baker, NewSouth Publishing, Sydney, 2015, s. 8.

16 Paul Robinson, "Introduction: Ethics Education in the Military", Paul Robinson, Nigel De Lee, ve Don Carrick (ed.), *Ethics Education in the Military,* Ashgate Publishing Company, England, 2010, s. 1-2.

17 "ethic noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com", https://www.oxfordlearnersdictionaries.com/definition/english/ethic?q=ethics, erişim 22.11.2024.

Etik kelimesi *ēthos* kelimesinden türetilmiş olup[18] ahlaki karakter, gelenek, örf ve âdet anlamına gelmektedir. 1650'li yıllardan itibaren ise etik kelimesinin bireylerin veya grubun ahlaki ilkeleri olarak tanımlandığı görülmektedir.[19] Etik kelimesinin tanımlamaları özetle şu şekilde ifade edilebilir:

a. ahlaki ilkeler sistemi,

b. belirli bir sınıfa, gruba, kültüre bağlı olarak ifade edilen davranış kuralları,

c. bireylere yönelik ahlaki ilkeler,

d. bireylerin eylemlerinin doğruluğu veya yanlışlığı ile bu eylemlerin motivasyonları ve amaçlarının iyiliği-kötülüğü ile ilgilenen felsefe dalı.[20]

Etik ve ahlak kavramlarının birbirlerinin yerine kullanıldığı çalışmalar da oldukça fazladır. Bu kapsamda etik ve ahlak arasındaki kullanım farkına değinmekte fayda vardır. Ahlak, doğru ile yanlış arasındaki ayrım, doğru davranış ilkeleri, etik,[21] çoğu insan tarafından doğru kabul edilen davranış standartlarına uymak[22] olarak tanımlanmaktadır. Ahlak, bireylerin neyin doğru neyin yanlış olduğuna ilişkin belirli değerlerini içerir. Etik ise genel olarak ahlak tanımına atıfta bulunuyor olsa da ahlakın daha dar bir faaliyet alanı içindeki doğru davranış kalıplarının uygulanmasını içerdiği görülür. Ahlak, genellikle bireylerin öznel bir tercihini ifade ederken, etik evrensel adaletin yönlerini, bireylerin bir eylemin sonuçlarından sorumlu olup olmadığı sorununu vurgular.[23] Bu kapsamda her ne kadar belirli ahlaki ölçütler olsa da bireyler arasında farklı ahlaki kalıpların gelişebileceği değerlendirildiğinde, ahlak kavramının etik kavramına göre daha öznel olduğunu söylemek mümkündür. Dolayısıyla etik, bir grup, sınıf, kurum veya kültürde bulunan bireyler için aynı olan gelenekleri, davranış kalıplarını ve kurallarını içerir.[24] Bu kuralların tümü Silahlı Kuvvetler için askerî etiğin varlığı ile öğretilmekte, uygulanmakta ve desteklenmektedir. Askerî etik, personelin askerlik mesleğindeki rolüne uygun yükümlülüklere ve kurallara uyma sanatıdır.[25] Personelin uyacağı kurallar ve ilkeler konusunda temel referans noktasıdır.[26]

Askerî etiğin amacı, etik uzmanı olmayan personele askerlik mesleğine yönelik verilen görevleri onurlu ve doğru bir şekilde yerine getirmek için yol göstermektir. Temel işlevleri ise personelin kendisinden beklenen etik talepleri daha iyi anlamalarına yardımcı olmak, mesleklerini icra ederken en uygun şekilde hareket etmelerine olanak tanımak, yürütülen faaliyetlerin doğasında yer alan ahlaki zorluklar üzerine düşünmelerini sağlamak[27] ve bir hareket tarzını diğerine tercih edilebilir olarak desteklemek için ne tür iyi nedenlerin

18 "Plato, Laws, Book 7, section 792e" https://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.01.0166:book=7:section=792e&highlight=ethos, erişim 22.11.2024.
19 "ethics | Search Online Etymology Dictionary", https://www.etymonline.com/search?q=ethics, erişim 22.11.2024.
20 "Dictionary.Com | Meanings & Definitions of English Words", Dictionary.com, https://www.dictionary.com/browse/ethics, erişim 22.11.2024.
21 "Dictionary.Com | Meanings & Definitions of English Words", Dictionary.com, https://www.dictionary.com/browse/moral, erişim 22.11.2024.
22 "moral adjective - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com", https://www.oxfordlearnersdictionaries.com/definition/english/moral_1?q=moral, erişim 22.11.2024.
23 "Definition of ETHIC", https://www.merriam-webster.com/dictionary/ethic, erişim 22.11.2024.
24 George Lucas ve John R. Allen, *Military Ethics: What Everyone Needs to Know,* Oxford University Press, New York, 2016, s. 3.
25 Richard A. Gabriel, *The Warrior's Way: A Treatise on Military Ethics,* Canadian Defence Acad. Press, Kingston, Ontario: 2007, s. 16.
26 Joseph Sanders, Douglas Lindsay, Craig A. Foster ve James Cook "Ethics in the 21st Century Profession of Arms: A Context for Developing Leaders of Character", Jeff Stouffer and Stefan Seiler (ed.), *Military Ethics: International Perspectives*, Canadian Defence Academy Press, Kingston, Ontario: 2010, s. 110.
27 Martin L. Cook ve Henrik Syse, "What Should We Mean by 'Military Ethics'?", *Journal of Military Ethics,* 9:2, 2010, s. 119-120, https://doi.org/10.1080/15027570.2010.491320.

sunulabileceğine yönelik farkındalık geliştirmelerine yardımcı olmaktır.[28] Bu kapsamda askerî etik, bir iç disiplin unsuru olarak bireyin ahlaki ve psikolojik gücünün aynasıdır denilebilir.[29]

Askerî etik gelişimseldir, kademeli olarak ilerler ve çok boyutludur. Personel mesleki yaşamı boyunca farklı zorluklarla karşılaştığında ve gelişimsel ihtiyaçları ortaya çıktığında daha önceki gelişimin temelleri üzerine inşa edilen askerî etik bilgileri, yeni kabiliyetleri ve beklentiler kapsamında tekrar şekillendirilmektedir. Bu askerî etiğin gelişimsel olduğu ve kademeli olarak ilerlediğini gösterir. "Ol, bil, yap" çerçevesinde doğru boyutları yakalayarak personelin ne olması gerektiğini tanımlayan karakter özellikleri, hangi bilgileri bilmesi gerektiği, farklı koşullar ve durumlarda ne yapması gerektiğini içeren bilgiler de askerî etiğin çok boyutlu yapısına işaret eder.[30]

Silahlı Kuvvetlerin görev yelpazesindeki değişimle birlikte ortaya çıkan yeni görevler kapsamındaki askerî eylemler, ahlaki karar verme ile yakından bağlantılıdır. Bu kapsamda ahlaki karar verme ile askerî etik kavramı daha da önem kazanmaktadır.[31] Görev kapsamındaki askerî eylemler savaş etiği kavramı kapsamında da incelenebilir. Burada askerî etik ve savaş etiği ayrımını yapmak gerekir. Askerî etik, personelin karakter gelişiminin sağlanmasıyla birlikte askerlik mesleğinin değerleri ve kurallarını içselleştirmelerini amaçlarken; savaş etiği, savaşın başlatılması, yürütülmesi ve savaş sonrasındaki durumların ahlaki ve hukuki ilkelerinin öğretilmesini amaçlar. Askerî etik, barış ve savaş zamanlarını kapsarken; savaş etiği, savaş öncesi, esnası ve sonrasındaki zamanı kapsar. Askerî etik, eğitimde birey düzeyine odaklanırken; savaş etiği eğitimde hem birey hem de devlet düzeyine odaklanır. Askerî etik için Silahlı Kuvvetlerin misyonu, vizyonu, askerlik yemini, iç hizmet hukuku, doktrinler ve talimnameler hukuki bir çerçeveyi oluştururken; savaş etiği uluslararası hukuk ve silahlı çatışma hukuku çerçevesinde düzenlenir. Savaş etiği, askerî etiğe göre daha özel bir alanı tanımlar. Bu kapsamda savaş etiğinin, askerî etiğin bir alt dalı olarak incelenmesinin daha doğru olacağı düşünülmektedir. Tablo 1.'de ilgili kavramsal farklılıklara dair bilgiler yer almaktadır.

Tablo 1. Askerî Etik ve Savaş Etiğinin Kavramsal Farklılıkları[32]

Özellikler	Askerî Etik	Savaş Etiği
Amaç	Personelin karakter gelişiminin sağlanması ve askerlik mesleğinin değerlerinin, kurallarının içselleştirilmesi	Savaşın başlatılması, yürütülmesi ve savaş sonrasındaki durumların ahlaki ve hukuki ilkelerinin öğretilmesi
Zaman Kapsamı	Barış ve savaş zamanı	Savaş öncesi, esnası ve sonrası
Odak Kapsamı	Birey	Birey ve devlet
Hukuki Çerçevesi	Silahlı Kuvvetler misyonu ve vizyonu, askerlik yemini, iç hizmet hukuku[33], doktrinler, talimnameler	Silahlı Çatışma Hukuku, Uluslararası Hukuk

28 Bill Rhod *An Introduction to Military Ethics: A Reference Handbook (Contemporary Military, Strategic, and Security Issues,* Praeger Publishers, Canada, 2009, s. 4.

29 Feridun Akkor, "İç Disiplin", Ordu Saati Konuşmaları içinde*, E.U. Personel Başkanlığı Moral Şubesi Yayınları No:15,* E.U. Basımevi, Ankara, 1957, s. 25.

30 Martin L. Cook., *Issues in Military Ethics To Support and Defend the Constitution,* State University of New York Press, New York, 2013, s. 92.

31 Brigadier Daniel Lätsch, "Preface", Jeff Stouffer and Stefan Seiler (ed.), *Military Ethics: International Perspectives,* Canadian Defence Academy Press, Kingston, 2010, iii-v.

32 Tablo yazar tarafından oluşturulmuştur.

33 İç Hizmet Hukuku, Silahlı Kuvvetler personelinin görev ve yetkilerini tanımlamanın dışında personelin nasıl davranması, nelere dikkat etmesi gerektiğine dair değerleri de içermeyi nedeniyle askerî etiği oluşturan bir unsur olarak değerlendirilmektedir.

2. Askerî Etik Eğitimi Harp Okulu Düzeyinde Nasıl Verilmektedir?

Etik eğitimi, Silahlı Kuvvetlerde geçmişten günümüze ilgilenilen bir konu olmuştur. Askerî eğitim kurumlarında hem subay hem de astsubay sınıfında etik eğitimlerinin verildiği bilinmektedir. Askerî etkinliğin arttırılması için tüm kademedeki personelin temel eğitiminde etik konusunun yer alması gerekmektedir. Bu kapsamda askerî etik, tüm kademedeki personelin mesleki yaşamı boyunca kazanması, geliştirmesi ve güçlendirmesi gereken önemli bir yetkinliktir. Askerî etik eğitiminin temel amacı, kanunların artık kullanılamaz olduğu bir durumda personele doğruyu yanlıştan ahlaki olarak ayırt edebilme kabiliyeti kazandırmaktır.[34]

2.1. West Point Askerî Etik Eğitimi

West Point 16 Mart 1802 tarihinde asker mühendislik konusunda eğitim verebilecek bir askerî akademi olarak kurulmuştur.[35] 1818 yılında Harp Okulu'nun kurucu lideri Albay Sylvanus Thayer, daha önce Etik, Tarih ve Coğrafya alanlarında eğitim verilmesine rağmen bu alanlarda yetkin profesör atamaları yaparak yeni bir bölüm kurmuştur.[36] Bu kapsamda etik eğitiminin West Point tarihi kadar eski olduğunu söylemek mümkündür.

1850'lerde, West Point'te müfredat değişikliği yaşanmıştır. 1854'te beş yıllık bir eğitim uygulanmaya başlamıştır. Amerika Birleşik Devletleri ordusunda mühendis subay olan Josept Tonten (1788-1864), profesyonel askerî eğitim konularını içeren tarih, yabancı dil, etik konularında teknik ve bilimsel çalışmalar yapılması gerektiğini belirtir. 1850'den sonra verilmeye başlanan dersler, onun çalışmalarının bir sonucudur. Müfredat değişimde West Point'in "Etik" alanı olarak adlandırdığı alanın genişletilmesi ile beşerî bilimlerin önemine dair yapılan vurgu da Tonten'ın bu alanda temsilci olarak görülmesine neden olmuştur. Bu dönemde etik alanında benimsenen dersler bugün İngilizcenin, felsefenin, tarihin ve hukukun bir parçası olarak kabul edilmektedir.[37] Birçok etik dersi, Profesör John W. French tarafından verilmiştir. Etik ders kitaplarından bazılarını kendisi yazdığı ve diğer yazarların çalışmalarından bazı hususları kendi yorumlarına göre uyarladığı veya birleştirdiği bilinmektedir. French'in metinleri, iç savaş sırasında subay eğitiminin, savaş teorisi ve pratiğiyle birlikte yıkıcı veya yapıcı tüm insani çabaların felsefi gerekçelerine dair bir girişi nasıl kapsadığını gösterir. French'in 1858 yılında yazdığı *A Short Course of Study in the Practical Part of Ethic*[38] adlı kitabın orijinal nüshası West Point kütüphanesindedir.[39]

Subay sınıfının yetiştirildiği West Point için askerî etik eğitimi, karakter gelişimi, mesleki amaç, yöntem ve değerlerin öğrenilmesi konusunda anlayış kazandırmayı kapsar. Askerî ortamın doğası göz önüne alındığında, bir subay özellikle yüksek etik standartlara uymalı ve ahlaki bir sorumlulukla hareket etmelidir. Ahlaki sorunları ele almak, doğru ahlaki kriterleri seçmek ve vicdani hareket etmek için öncelikle askerî etiğin iyi kavranması gerekmektedir. Bu amaçla subayları birer askerî lider olarak hazırlama konusunda askerî etik eğitimi ön plana çıkmaktadır.[40]

34 Florian Emonet, "The Importance of Ethics Education in Military Training", https://www.armyupress.army.mil/Journals/NCO-Journal/Archives/2018/November/Ethics/#:~:text=Military%20ethics%2C%20like%20medical%20or,laws%20are%20no%20longer%20helpful, erişim 16.11.2024.

35 İsrafil Kurtcephe ve Mustafa Balcıoğlu, *Kara Harp Okulu Tarihi,* Kara Harp Okulu Matbaası, Ankara, 1991, s. 33.

36 "History About | United States Military Academy West Point", https://www.westpoint.edu/academics/departments/history/about, erişim 11.11.2024.

37 "Prelude to War 1860 – 1861 · West Point and The Civil War · U.S. Military Academy Library Exhibits", https://usmalibrary.omeka.net/exhibits/show/westpointcivilwar/prelude-to-war-----1860-1861, erişim 11.11.2024.

38 Etiğin Uygulamalı Kısmında Kısa Bir Çalışma Kursu.

39 J. W. (John William) French, *A Short Course of Study in the Practical Part of Ethics* (New York: J.F. Baldwin, Printer, 1858), https://usmalibrary.omeka.net/items/show/11, erişim 16.11.2024.

40 Heydar Piriyev "The Role of Military Ethics and Morals as a Subject of Pedagogy in the Leadership Training of Officers for Multinational Environment", *Journal of Defense Resources Management,* 10:2, 2019, s. 22-24.

West Point misyonu, "Harbiyelilerin "görev", "onur", "ülke" değerlerine bağlı olarak orduya ve ulusa profesyonel mükemmellikte hizmet kariyerine hazırlanmış liderler olmaları için eğitilmesi, yetiştirilmesi ve onlara ilham verilmesi" şeklinde ifade edilir.[41] Görev, onur ve ülke değerleri, Harbiyelilerin karakter gelişimini önceleyen bir sistemde eğitim gördüklerini göstermektedir. Bu kapsamda Harbiyeliler için karakter geliştirme programı bulunmaktadır. Program, West Point Lider Geliştirme Sistemini (WPLDS- *West Point Leader Development System*) desteklemektedir. Ayrıca West Point misyonunu desteklemek için William E. Simon Profesyonel Askerî Etik Merkezi (SCPME- *The William E. Simon Center for the Professional Military Ethic*), Harbiyelilerin onurlu bir şekilde yaşama ve onurlu bir şekilde liderlik etmelerinin ne anlama geldiğini çözümlemelerine yardımcı olan Karakter Programı'nın destekçisi olarak hizmet vermektedir. Karakter Programının sonrasında Harbiyeliler:[42]

- Harbiyeli Onur Kodunu[43] anlar. [44]
- Onur Kodunun etkin yönetimini yürütür.
- Onur sisteminin adil ve etkili olduğuna güvenir.
- West Point değerlerini ve Ordu değerlerini anlar.
- Devam eden karakter gelişimlerinin sorumluluğunu kabul eder.
- Diğer Harbiyelilerin karakter gelişimini olumlu yönde etkileme sorumluluğunu kabul eder.
- Karakterin, subaylığın tüm yönlerine nasıl dahil edildiğini anlar.
- Görevlendirilen subayların ahlaki liderlik sağlama sorumluluğunu anlar.
- Subayların ahlaki taleplerini yerine getirme yeteneklerine güvenir.

West Point akademik programın yedi ana hedefi bulunmaktadır.[45] Bunlar: a. iletişim, b. eleştirel c. düşünme ve yaratıcılık, d. yaşam boyu öğrenme, e. etik akıl yürütme, f. beşeri ve sosyal bilimler, g. disiplin derinliği, h. bilim, teknoloji, mühendislik ve matematik. Çalışma konusu ile ilgili olan etik akıl yürütme hedefinde eleştirel düşünür olarak mezunlar fikirlerin, bilgilerin güvenilirliğini ve kullanışlılığını analiz ederler. Aynı zamanda karmaşık konulara uygun, etkili ve yenilikçi yaklaşımlar geliştirebilirler. Yaratıcı düşünüler olarak da geleneklerin sınırlarına takılmadan mevcut bilgileri farklı şekillerde kullanabilme yeteneğine sahip olurlar. Etik akıl yürütme kısmında mezunların neler yapabileceğine dair dört öneri bulunmaktadır. Bunlardan birincisi, "etik ilkelerin entelektüel temellerini anlayın". İkincisi, "sorunların ve durumların etik bileşenlerini tanıyın". Üçüncüsü, "farklı etik bakış açıları, ilkeleri ve kavramlarını bağlamlar içinde inceleyin ve değerlendirin". Dördüncüsü, "askerî ortamlarda bulunan da dahil olmak üzere karmaşık sorunları çözme noktasında etik bakış açılarını ve kavramlarını uygulayın".[46]

41 "West Point Mission Statement | United States Military Academy West Point", https://www.westpoint.edu/about/history-of-west-point/west-point-mission-statement, erişim 11.11.2024.

42 "United States Military Academy Charcter Programı Academic Year 2020 / Simon Center for the Prefessional Military Ethic", 3, https://www.thefire.org/sites/default/files/2002/06/31174402/Goldbook-20191.pdf, erişim 12.11.2024.

43 *Honor Code*: "*A cadet will not lie, cheat, steal, or tolerate those who do.*"

44 "Simon Center for the Professional Military Ethic | United States Military Academy West Point", https://www.westpoint.edu/about/academy-leadership/commandant/simon-center-for-the-professional-military-ethic, erişim 12.11.2024.

45 "Educating Future Officers Preparing Soldier - Scholars to Win on the Modern Battlefield", 8-13, https://s3.amazonaws.com/usma-media/inline-images/about/superintendent/Educating_Future_Officers%20_AY22.pdf, erişim 11.12.2024.

46 *Educating Future Officers Preparing Soldier- Scholars to Win on the Modern Battlefield,* 10.

West Point akademik programın yedi ana hedefinden biri olan etik akıl yürütme, Harbiyelilere West Point'in akademik müfredatı kapsamında öğretilmektedir. Akademik müfredatta Etik, Askerî Etik, PME2 (*Professional Military Ethic Education*) ve MX400 (*Officership*) dersleri bulunmaktadır. Bu derslere ek olarak Etik Konuları, Etik-Askerlik Mesleği, Teknoloji Etiği, Siber Etik, Çevre Etiği, Tıp Etiği dersleri de yer almaktadır. Diğer derslerde direkt olarak etik adı geçmiyor olsa da derslerin kapsamında etik konusuna değinildiği görülmektedir.[47]

Etik dersi, standart etik doktrinlerinin sistematik bir incelemesinin ve karşılaştırmasının yanı sıra etik düşüncenin doğasına ait bazı temel kavram ve varsayımların analizini sunar. Etik doktrinler, Aristoteles (erdem teorisi), Kant (deontoloji) ve Mill (faydacılık) gibi ünlü filozoflarla ilişkili olanları içerir. Derste doktrinlerin orijinal metinleriyle birlikte çağdaş filozofların eleştiri ve savunmaları da işlenmektedir.

Askerî etik dersi ise savaşçı ahlakının temel değerlerini ve ilkelerini antik Yunan ve Roma'ya kadar inceler. Bu değerler askerlik mesleğinin ahlaki sınırlarını belirlerken mesleğin üyelerini amaçlarına ulaşmak için şiddet kullanan diğer kişi ve gruplardan ayırır. Harbiyeliler bu derste mesleğin ahlaki ilkeleri, siyasi hedeflere ulaşmak için güç kullanımına ne zaman izin verildiği, gücün nasıl kullanıldığı ve hangi sınırlarla yönetilmesi gerektiğini incelerler.[48]

Profesyonel Askerî Etik Eğitimi, değerler eğitimi, karakter gelişimi, subaylık mesleği ve liderlik üzerine odaklanarak öğrencilerin icra edecekleri mesleğe yönelik etik boyutları öğrenmelerini sağlar. PME2'nin amacı, subaylık kavramını Amerikan askerlik mesleği ahlakını ve karakter geliştirme alanları kapsamında özetlenen niteliklerin geliştirilmesine yardımcı olmak için mevcut akademik programları güçlendirmektir. PME2,[49] Harbiyelilerin ordu değerlerine göre düşünme ve hareket etme yeteneğini geliştirmek için tasarlanmış dersler, okuma ve yazma ödevlerini içerir. West Point'te PME2 birinci sınıftan dördüncü sınıfa kadar kademeli ve tamamlayıcı bir şekilde ilerler.

Program müfredatı, karakterli liderler yetiştirmek için temel öneme sahip üç alan doğrultusunda düzenlenmiştir. Bunlar:

a. Ordu Değerleri (Subaylığın ahlaki ve etik gereksinimlerinin yerine getirilmesi),

b. Subaylık (Amerikan Görevli Subayı olarak hizmet etmek için neyin gerekli olduğunun belirtilmesi),

c. Liderlik (Mezunların, komuta ortamında öğrenilen nitelikleri ve değerleri uygulaması).[50]

PME2 programının onur, saygı ve subaylık kavramları odaklı ilerleyen müfredatını tamamlayan tüm kademedeki Harbiyelilerin yapmaları beklenen davranışlar bulunmaktadır.[51] Bu davranışlar listesi aşağıda Tablo 2'de özetlenmektedir.

47 "Course Subject Search Results", https://courses.westpoint.edu/crse_sbjct_rslts.cfm, erişim 11.11.2024.

48 "United States Military Academi Academic Program Class of 2026 Circulum and Course Descriptions", 194, https://s3.amazonaws.com/usma-media/inline-images/academics/dean/strategic_documents/RedBook_GY2026_20220810_0.pdf, erişim 11.11.2024.

49 " Acronym/Term/Phrase", https://www.westpoint.edu/sites/default/files/inline-images/DMI/what%20is%20that.pdf?ref=cortis.com, erişim 23.12.2024.

50 "United States Military Academy Academic Program Class of 2024 Curriculum and Course Descriptions", 88, https://s3.amazonaws.com/usma-media/inline-images/academics/dean/PDFs/RedBook_GY2024_20210712.pdf, erişim 03.01.2025.

51 "Information Paper: Professional Military Ethic Education (PME2) Program Overview ",https://www.westpoint.org/class/usma1965/Class2015/Activities/PME2_InfoPaper-5July2010-Final.pdf, erişim 29.11.2024.

Tablo 2. West Point PME2 Müfredatını Tamamlayan Harbiyelilerden Beklenen Davranışlar[52]

Müfredat ve Sınıf	Beklenen Davranışlar
PME2 Harbiye Temel Eğitim müfredatını tamamlayan Birinci Sınıf Harbiyeliler	Ordu değerlerini bilmek ve anlamak.
	Harbiyeli onur kodlarını bilmek ve anlamak.
	Onur kodunun[53] dört yasağının asgari etik davranışının standardı olduğunu bilmek.
	Saygı programının amacını bilmek ve anlamak.
	Bir ekibin etkili bir üyesi olmayı öğrenmek.
	Karakter liderini tanımlayabilmek.
	Hem Onur hem de Saygı Programları için belirlenmiş standartlara uymak.
PME2 müfredatını tamamlayan Birinci Sınıf Harbiyeliler	Profesyonel askerî etik kavramını anlamak.
	Subaylığın temellerini öğrenmek.
	Onur Kodu ve Sistemi ile Kurallar Ruhu arasındaki ilişkiyi anlamak.
	Günlük aktiviteler boyunca onurlu ve saygılı bir yaşamın nasıl uygulanacağını bilmek.
	Bir Harbiyeli olarak saygılı bir davranış sergilemek; cinsel tacizin ve fırsat eşitliği ihlallerinin önlenmesinin önemini anlamak.
PME2 müfredatını tamamlayan İkinci Sınıf Harbiyeliler	Profesyonel askerî etik kavramını anlamak ve uygulamak.
	Subaylığın dört yönünü anlamak.[54]
	Liderlik yönlerini üstlenmede kişisel zorlukların kaynaklarını belirlemek ve kişisel gelişim planı hazırlamak.
	Harbiyeli Onur Kurallarını, kuralların ruhunu ve erdeme saygıyı bilmek; bunlara bağlı kalmak ve desteklemek.
	Ulusa olan bağlılığı ve hizmeti anlamak.
PME2 müfredatını tamamlayan Üçüncü Sınıf Harbiyeliler	Profesyonel askerî etiğe uygun hareket etmek.
	Subaylığın dört yönünü küçük birim lideri seviyesinde uygulamak.
	Öğrenci onur kurallarını ve sistemini bilmek; buna bağlı kalmak ve buna inanmak. Kurallar ruhu ile yaşamak.
	Şefkatli, cesur bir liderlik sergilemek. Tüm insanlara; geleneklerine, mülklerine saygı göstermek.
	Astları geliştirmek; standartları modellemek ve uygulamak.

Dördüncü sınıf Harbiyeliler ise diğer Harbiyeliler için PME2 eğitimini kolaylaştırarak onlara liderlik etmektedir. Aynı zamanda dördüncü sınıf Harbiyelilerden MX400[55] eğitimi aracılığıyla bireysel ve profesyonel kimliklerini geliştirmeleri beklenmektedir. MX400[56] eğitimi, subayın bitirme parkuru olarak adlandırılmaktadır. MX400, her bir subayın ahlaki liderlik yapma görevine önem vermektedir. Bu kapsamda Harbiyelilerin erdemli, onurlu,

52 Tablo yazar tarafından oluşturulmuştur.
53 "WHITE PAPER", https://www.west-point.org/users/usma1951/18250/whitepaper.htm, erişim 03.01.20*24. "A cadet will not lie, cheat, steal, or tolerate those who d*o".
54 "academic, military, physical, character".
55 OFFICERSHIP
56 "USMA Academic Program", https://courses.westpoint.edu/static/index.htm#t=Simon_Center_for_the_Professional_Military_Ethic.htm&rhsearch=MX400&ux=search, erişim 17.12.2024.

vatansever ve sivil otoriteyi dikkate alan liderler olmalarını destekleyen bir eğitim programını içermektedir. MX400'te Harbiyeliler hem geçmişe hem de geleceğe bakarak, West Point Lider Geliştirme Sistemi'nin (WPLGS) bir parçası olarak kendi karakter geliştirme deneyimlerini değerlendirir. Aynı zamanda Harbiyeliler icra edecekleri mesleğin kalıcı ve ortaya çıkan etik zorluklarını incelemektedir. MX400, Harbiyelilerin lider olarak devam eden gelişimlerini, subay olarak ortaya çıkan kimliklerini anlamaları ve benimsemeleri için yardımcı olur. MX400'ün tamamlanmasının ardından, her öğrenci mesleki kimliğini içselleştirmeli; karmaşık durumlarda eleştirel düşünmeyi uygulama ve askerî sorunlara disiplinlerarası çözümler sunma yeteneğine güvenmelidir. MX400 dersi, onurlu hizmet kavramlarını disiplinlerarası konulara da dahil etmektedir. Bu kapsamda askerî personel için askerî etik, toplam etik benliğinin yalnızca bir parçasını oluşturur. Diğer sahip olduğu roller etik davranışlara da tabii olarak değerlendirilmektedir.[57] William E. Simon Profesyonel Askerî Etik Merkezi departmanı bu dersin verilmesinden sorumludur.

Harbiyeliler bu ders kapsamında:[58]

- Karakterin, subaylığın tüm yönlerine nasıl dahil edildiğine dair ortak bir anlayış oluşturarak, çok kültürlü ekiplerinden yararlanmanın, güven üzerine inşa edilmiş sağlıklı ilişkiler kurmanın ve etik akıl yürütmeyi kullanmanın faydalarını tanımayı öğrenirler.
- Mesleklerinin ahlaki ağırlığını kabul ederek ve görev yeminin kutsal anlamının farkında olarak profesyonel kimliklerini benimserler.
- Karmaşık askerî sorunlara disiplinlerarası çözümler üretir, çok kültürlü ekip içinde nasıl güven oluşturulabileceğine dair hususları öğrenirler.

West Point'te, askerî kişiliği inşa eden askerî etik eğitiminin sistematik ve kurumsallaşmış bir yapıya sahip olduğu görülmektedir. Askerî etik eğitiminin temelini karakter inşası, liderlik gelişimi, kurumsal aidiyet, ahlaki sorumluluk, hesap verilebilirlik ve disiplin oluşturmaktadır. West Point askerî etik eğitimi teorik alt yapı ve uygulama temelli öğrenme ile sentezlenen bütüncül bir eğitim modelini benimsemektedir. Bu kapsamda eğitimin teorik temellendirilmesinin yanında hem günlük hem de mesleki yaşamda uyarlanabilmesinin desteklendiği görülmektedir. Sonuç olarak West Point askerî etik eğitimi Harbiyelilerin ahlaki değerler sistemine etki eden, davranış kalıplarını inşa eden ve sorumluluk bilincini oluşturan kademeli bir süreçtir.

2.2. Kara Harp Okulu Askerî Etik Eğitimi

Kara Harp Okulu askerî etik eğitimi incelendiğinde "askerî etik" veya "etik" adında bir eğitim verilmediği fakat ilgili konularda disiplin, ahlak, hukuk, talim, sosyoloji, liderlik, hitabet, moral, komuta ve kontrol başlıkları altında birçok dersin veya yayının bulunduğu görülmektedir. Bu kapsamda askerî etik eğitiminin West Point'te olduğu gibi Kara Harp Okulu'nda da okul tarihi kadar eski olduğunu söylemek mümkündür.

Kara Harp Okulu Maçka Kışlasında 400 kişilik bir kadro ile 1834 yılında açılmış,[59] açılış sürecinde okulun tamir ve düzenlemesi yapılmış.[60] Resmi açılış ise 1 Temmuz 1835

57 Richard A. Gabriel, *To Serve with Honor A Treatise on Military Ethics and the Way of the Soldier,* Greenwood Press, London, 1982, s. 26.
58 *United States Military Academy Academic Program Class of 2024 Curriculum and Course Descriptions*, s. 45.
59 Muharrem Giray, *Şanlı Harbiye'nin Tarihi,* Hilmi Kitabevi Ltd., İstanbul, 1961, s. 6.
60 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi,* s. 51.

yılında Sultan II.Mahmut'un katılımıyla gerçekleştirilmiştir.[61] 1836 yılında öğrenci sayısı 315'e yükselen Kara Harp Okulu ilk mezunlarını 1842 yılında vermiştir.[62] Başlangıçta Kara Harp Okulu tabur teşkilatına göre düzenlenmiş olup, Tablo 3.'de yer alan sekiz sınıfa ayrılmıştır.[63]

Tablo 3. 1835 Kara Harp Okulu Sekiz Sınıf[64]

Birinci Sınıf	Alfabe ve Rakam Öğretimi, Yazı Çalışmalarının Yapılması
İkinci ve Üçüncü Sınıf	Amme Cüzü
Dördüncü ve Beşinci Sınıf	İlm-i Hal, Akaid-i Diniyye, Şurut-i İslamiye
Altıncı Sınıf	Askerî Talimname, Askerî Kanunname
Yedinci ve Sekizinci Sınıf	Sarf ve Nahiv Okumaları, Rika Yazısı Öğretimi

Birinci ve sekizinci sınıf arasındaki devreye "ilk mektep", sekizinci sınıfı bitirip yapılan sınavda başarılı olanların girmeye hak kazandığı dokuzuncu sınıfa "ikinci mektep" denilmektedir.[65] Sekizinci sınıf sonunda başarılı olan öğrencilerden 100 kişi seçilmekte, seçilen öğrenciler bir subayın yetiştirilmesi için gerekli bilgileri içeren İlm-i Hesap, Mecmuatü'l-Mühendis-in, Hendese, Harita Tersimi, Basit İstihkam Eğitimi, Cebirin Hendeseye Uygulanması, Farsça, Arapça, Dini Bilgiler, Kılıç, Tüfek, Meç ve Top Eğitimi, Resim, Coğrafya, Bostan ve Gülistan[66] dersleriyle birlikte fotoğrafın yaygın olmaması ve harita eksikliği nedeniyle her subayın kroki ve harita çizebilecek kabiliyete sahip olacak şekilde yetiştirilmesi amacıyla harita ve topografya çalışmaları da yapmaktadır.[67]

1845 yılı nisan ayında yapılan düzenlemeler sonucunda 1846 yılına kadar Harp Okulu'nda okutulan derslere bakıldığında üçüncü sınıfta "Tabur Talimi", "Tabur Talimi Ameliyatı", "Piyade Dahiliye Kanunnamesi", dördüncü sınıfta "Fenn-i Harp" derslerinin[68] askerî etik kapsamında değerlendirilebileceği görülmektedir. 1867'de piyade ve süvari sınıfları ayrılmıştır. Bu kapsamda 1867'den 1884'e kadar piyade sınıfı öğrencilerine üçüncü sınıfta "Askerî Kitabet" ve "Dahiliye Nizamnamesi" dersleri verilmiştir. 1875 yılında Askerî Mektepler Nazırlığına Mirliva (Tuğgeneral) rütbesi ile tayin edilen tarihçi bir komutan olan Süleyman Paşa'nın okullarda disiplin ve askerî terbiyenin temellerini bilinmektedir.[69]

1892-1902 yılları arasında Kara Harp Okulu'nda eğitim süresi üç yıldır. Birinci ve üçüncü sınıfta 1892-1901 yılları arasında "Malümat ve Terbiye-i Askeriyye"; birinci, ikinci ve üçüncü sınıfta 1892-1901 yılları arasında "Talim Nazariyatı"; ikinci sınıfta 1900-1901 yılları arasında "İlm-i Ahlak"; ikinci sınıfta 1897-1901 yılları arasında "Ceza Kanunname-i Hümayunu";[70] üçüncü sınıfta 1892 yılında "Tabiye", 1900-1901 yılında ise "Tabiye Tatbikatı" derslerinin verildiği görülmektedir.[71] II. Meşrutiyet'in ilan edildiği 1908 yılında

61 Cemalettin Taşkıran, *Yüzyıllardır Harbiye Harbiye'nin 180 Yıllık Tarihi ve En Büyük Harbiyeli Atatürk,* Doğan Kitap, İstanbul, 2009, s. 176.
62 Yusuf Çam, *Atatürk'ün Okuduğu Dönemde Askeri Okullar Rüşştiye-İdadi-Harbiye (1892-1902),* Genelkurmay Basım Evi, Ankara, 1991), s. 127.
63 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi,* s. 52.
64 Tablo yazar tarafından oluşturulmuştur.
65 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi*, s. 129.
66 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi*, s. 129-130.
67 Yusuf Çam, *Atatürk'ün Okuduğu Dönemde Askeri Okullar Rüştiye-İdadi-Harbiye (1892-1902),* s. 154.
68 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi*, s. 131.
69 Yusuf Çam, *Atatürk'ün Okuduğu Dönemde Askeri Okullar Rüşştiye-İdadi-Harbiye (1892-1902),* s. 129.
70 Ceza Hukuku ve Kanunu
71 Yusuf Çam, *Atatürk'ün Okuduğu Dönemde Askeri Okullar Rüşştiye-İdadi-Harbiye (1892-1902*), s. 155-161.

Harp Okulu'nda okutulan dersler arasında yer almaya devam eden "İlm-i Ahlak", "Askerî Terbiye", "İç Hizmet", "Tabiye" derslerinin verildiği görülmektedir.[72]

1926 yılında Harp Okulunun ders programında yapılan düzenleme ile dersler; içerisinde "Ordu Bilgisi (Askerî Hukuk ve Mâlûmat) dersinin de yer aldığı Fennî Dersler, Umumî Dersler ve Amelî Talim ve Tatbikatlar olmak üzere üç kategoriye ayrılmıştır.[73] 1934 yılında yayınlanan Harbiye Mektebi Talimatı D-25 ile Harp Okulu eğitim esasları düzenlenmiştir. Bu kapsamda birinci sınıf dersleri arasında "Askerî Ceza ve Hukuk", ikinci sınıfta "Tabiye" dersinin,[74] 1946 yılından itibaren birinci sınıfta "İç Hizmet ve Askerî Söz ve Yazı Usulü", "Askerî Ceza" ve "Anayasa ve İdare Hukuku" derslerinin verildiği görülmektedir. "Tabiye" dersi birinci ve ikinci sınıfta verilmeye devam etmiştir.[75] 11 Aralık 1948 tarihli bir emirle kültür derslerine yenileri eklenmiş, birinci sınıf müfredatına "Ordu Kurumu" ve "İç Hizmet" dersleri eklenmiştir. 1948'de hazırlanan düzenleme 1960'lı yıllara kadar küçük değişikliklerle devam etmiştir.

1960-1970 yılları arasında Harp Okulu birinci sınıfa "İç Hizmet ve Askerî Yargı Usulleri" ve "Komutanlık Saati"; ikinci sınıfa ise "Önderlik" dersi eklenmiştir. Kara Kuvvetleri Komutanlığı'nın 10 Şubat 1970 tarihli emri ile Harp Okulu öğrenim süresinin üç yıla çıkarılması çalışmaları başlamış; 1462 sayılı Harp Okulları Kanunu'nun kabulü sonucunda öğrenim süresi üç yıla çıkarılmıştır. Bu kapsamda 1971-1972 eğitim yılında birinci sınıfta "Hitabet" ve "Türkçe-Kompozisyon"; üçüncü sınıfta ise "Sosyoloji" ve "Personel" dersleri eklenir.

Genelkurmay Başkanlığının emri[76] ile 1974-1975 eğitim öğretim yılından itibaren Harp Okulu lisans seviyesinde dört yıl eğitim vermeye başlamıştır. Yeni düzenlemelerle üçüncü sınıfa "Meslek Nazariyatı" dersi eklenmiş[77], 1978-1979 yıllarında dördüncü sınıfta "Meslek Nazariyatı" dersi devam ederken "Liderlik" ve "Askerî Hitabet" dersleri eklenmiştir. 1980-1981 yılında birinci sınıfta "Personel" dersi devam ederken "İç Hizmet ve Askerî Görgü Kuralları" ile "Türkçe-Askerî Yazışma-Hitabet" dersleri eklenmiştir. Üçüncü sınıfta "Komuta Kontrol" dersi verilmeye başlanmış, Dördüncü sınıfta "Meslek Nazariyatı" ve "Liderlik" dersleri verilmeye devam etmiştir. 1985-1986 tarihlerinde üçüncü sınıfta "Komuta Kontrol", dördüncü sınıfta ise "Meslek Nazariyatı" dersinin verilmeye devam ettiği görülmektedir.[78]

1990-1991 eğitim-öğretim yılında "Liderlik", "Türkçe-Askerî Yazışma-Hitabet" dersleri verilmeye devam etmiştir. 1991 yılı sonrasında da "Askerî Etik" adında bir ders verilmediği askerî etiği içeren "Taktik", "Sevk ve İdare Uygulamaları", "Silahlı Çatışma Hukuku", "Askerî Liderlik", "İdare Hukuku", "Hukuka Giriş" ve "Savunma Mevzuatı" dersleri verilmiştir.

Günümüzde Kara Harp Okulu eğitim-öğretim programına bakıldığında askerî etik konusu ayrı bir ders olarak verilmemekte "Askerî Sosyoloji" dersinin bir konusu olarak ele alınmaktadır. "Askerî Sosyoloji" ders kitabında askerî etik başlığı ve tanımı itibariyle yer almasına rağmen savaş etiği konusunun ön plana çıktığı görülmektedir. Diğer yandan Kara Harp Okulu'nda askerî eğitim ve akademik eğitim kapsamında kazandırılan temel askerî ve değer kabiliyetlerine bakıldığında askerî etik ile ilgili unsurların yer aldığı görülmektedir. Bu

72 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi,* s. 111-113.
73 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi,* s. 181.
74 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi,* s. 187.
75 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi,* s. 189.
76 7 Mart 1974 sayılı HRK: 530-1-74\Ak.Ok. (Ak.150) sayılı emir.
77 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi,* s. 190-193.
78 Kurtcephe ve Balcıoğlu, *Kara Harp Okulu Tarihi,* s. 196-198.

unsurların yer aldığı maddeler Harp Okulları Kanunu, Harp Okulları Yönetmeliği ve Kara Harp Okulu Yönergesinde yer alan amaç ve ilkelere uygun olarak asker kişilerde bulunması gereken niteliklerin Türk Silahlı Kuvvetleri (TSK) İç Hizmet Kanunu ve TSK İç Hizmet Yönetmeliğinin muhtelif maddelerinde belirtildiği ifade edilmiştir. Bu kapsamda Kara Harp Okulu'nun görevi:[79]

- "Dürüst, yurdunu seven, ahlâkî değerlere, vatanseverlik duygusuna, vatandaşlık sorumluluğuna, millî ve kültürel değerlere sahip,
- Başta disiplin olmak üzere askerlik mesleğinin temel değerlerini özümsemiş, silah arkadaşlığının anlam ve önemini kavramış,
- Yeterli fizikî yeteneği kazanmış, liderlik, komutanlık, yöneticilik özellikleri ve becerileri gelişmiş,
- Askerî sevk ve idare edebilme yeteneği kapsamında kıta sevk ve idare usulünü uygulayabilecek bilgileri edinmiş ve fiilen tatbik etmiş,
- Barış şartlarında birlik (takım ve bölük/batarya seviyesinde) sevk ve idaresi, eğitimin sevk ve idaresi alanlarında gerekli yetenekleri kazanmış,
- Yıkıcı ve bölücü faaliyetler ile istihbarata karşı koyma, kişisel güvenlik ve sır saklama konularında yetişmiş muvazzaf subaylar yetiştirmektir."

2016 yılında Kara Harp Okulu bünyesinden ayrılan Jandarma sınıfı, Jandarma ve Sahil Güvenlik Akademisi bünyesinde yetiştirilmeye başlanmıştır. Bu kapsamda Jandarma sınıfı muvazzaf subayların yetiştirildiği Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Fakültesi ders programı incelendiğinde askerî etik kapsamında değerlendirebileceğimiz "Din ve Değerler Eğitimi", "Kolluk Bilgisi ve Uygulamaları", "Ceza Hukuku Genel Hükümler", "İdare Hukuku", "Harekât Yönetimi", "Protokol ve Görgü Kuralları", "Disiplin Hukuku", "Kolluk ve Harekât Yönetimi Oyunları" ve "Kolluk Etiği" derslerinin olduğu görülmektedir. Kolluk Kuvveti olan Jandarma subay sınıfında kolluk etiği dersinin bulunmaktadır.[80]

Kara Harp Okulu gibi Güvenlik Bilimleri Fakültesi'nin teşkili ve görevleri incelendiğinde askerî etik unsurların yer aldığı görülmektedir:[81]

- "Öğrencinin düşünebilme, tasavvur, tahayyül, analiz, sentez ve diğer niteliklerini geliştirir ve bunları mümkün olduğu kadar kısa zamanda yapmaya alıştırır. Komutanlık ve liderlik nitelikleri aşılar ve bu niteliklerin kökleşmesini sağlar.
- Öğrencileri vatansever, milliyetperver, vazifeşinas, sorumluluk duygusuna, disiplin şuuruna üstün bir ahlâk ve karaktere sahip, bilgili, cesur, fedakâr, feragatli, kanun, nizam, amir ve üstlerine itaatkâr, astlarına karşı müşfik, her bakımdan yüksek ve mütekâmil manevî değerlere mücehhez bir seviyeye getirir.
- Her öğrencinin Devletimizin yasal temelini oluşturan Atatürk ilke ve inkılâplarına tam olarak intibakını sağlar. Atatürk ilke ve inkılâplarının her öğrenciye içtenlikle benimsetilmesini ve her öğrencinin, bu ilke ve inkılâplara sahip çıkacak ve onları gerektiğinde savunabilecek bir fikir düzeyine getirilmesini sağlar."

79 "Kara Harp Okulu Eğitim-Öğretiminde Kazandırılan Temel Askerî ve Değer Kabiliyetler", https://kho.msu.edu.tr/hakkinda/amac_gorevler.html, erişim 13.05.2025.

80 Jandarma ve Sahil Güvenlik Akademisi, "Güvenlik Bilimleri Fakültesi Müfredatı (2022-2026)", https://www.jsga.edu.tr/kurumlar/jsga.edu.tr/IcSite/fakulte/Dersler/Mufredat(1).pdf, erişim 09.04.2025.

81 "Güvenlik Bilimleri Fakültesi Teşkili ve Görevler", https://www.jsga.edu.tr/fakulte/amac-ve-gorevler, erişim 13.05.2025.

Askerî etik kapsamında değerlendirilebilecek yayınlar incelendiğinde Harp Okulu ve askerî lisede görev yapan kişiler tarafından yayınlanan eserler dikkat çekmektedir. Bu eserlerin başlıklarında askerî etik yer almamasına rağmen askerî etiğin unsurları içinde değerlendirilen ahlak, moral, disiplin, terbiye, vazife başlıkları görülmektedir. Bu yayınlardan birincisi Maltepe ve Kuleli Askerî Liseleri felsefe ve sosyoloji öğretmeni Ahmet Faik Türkmen[82] 1933 yılında yayınlanan *Askerliğin Psychologie'si Hakkında Bir Kalem Tecrübesi* eseridir. İkincisi 1938 yılında yine Ahmet Faik Türkmen tarafından yayınlanan *Moral* adlı eserdir. Türkmen bu eserin tanıtımında Yüksek Levazım Okulu Moral Hocası Üniversite Reisliğinde Propaganda ve Psikoloji Uzmanı olarak geçmektedir. Üçüncü eser Harp Okulu Ordu Bilgisi Öğretmeni Yarbay Hadi Atay tarafından 1941 yılında yayınlanan *Ordu Bilgisi 1941 Ders Yılı Notları II. Kısım Askeri Terbiye* adlı eserdir. Dördüncüsü Harp Okulu öğretmeni Cemal Ungan tarafından 1941 yılında yayınlanan *Saygı* adlı eserdir. Beşincisi Ahmet Faik Türkmen tarafından 1943'te yayınlanan *Milli ve Askeri Ahlak*[83] ve 1946'da yayınlanan *Vazife ve Ahlak* eserleridir. Türkmen, bu eserin tanıtımında Bursa Işıklar Askerî Lisesi Felsefe Öğretmeni olarak sunulmaktadır.

Eserlerin içerik incelemesine bakıldığında, *Askerliğin Psychologie'si Hakkında Bir Kalem Tecrübesi* adlı eser dört bölümden oluşmaktadır. Birinci bölüm başlığı "Askerî Otorite"dir. Bu bölümde disiplinin tanımı, değerlendirmesi ve komutanlığın psikolojisi açıklanmıştır. İkinci bölüm başlığı "Askerliğin Psikolojisi"dir. Bu bölümde askerliğin temelinde Volontarizm felsefesinin olduğu ileri sürülerek askerî terbiyenin mekanizmasını Volontarizmde aramak gerektiği belirtilmektedir. Üçüncü bölüm başlığı "Harp ve Medeniyet"tir. Bu bölümde askerliğin uluslararası alandaki yeri ve önemi değerlendirildikten sonra medeniyetlerin meydana gelmesinde harbin nasıl belirleyici bir etken olduğu analiz edilmiştir. Dördüncü bölüm başlığı "Toplumsal Perspektiften Askerliğimizin Yakın Tarihi"dir. Bu bölüm kendi içinde üçe ayrılmaktadır. Bölümler sırayla Askerliğin soylu sınıf devri, ücretli askerlik devri, muvazzaf askerlik devridir. Burada bölümün yazılış amacı, askerliğin yakın geçmişine dair bir değerlendirme yapmak, toplumsal sınıflar arasındaki konumunu belirlemek ve tanımlamak, asker sınıfının toplumsal rollerini bilmek ve büyük inkılap tarihimizde yapmış oldukları icraatları göstermektir.[84]

Moral adlı eser, Mustafa Kemal Atatürk'ün talimatı ile yazılmıştır. Eserin başında Atatürk tarafından kaleme alınan bir önsöz bulunmaktadır. Önsözün bağlığı "Kumandan, Subay ve Ordu Morali"dir. Bu önsözde harbin ve askerlik sanatının öğrenilmesine vasıta olan en gerçekçi unsurun ahlak olduğu belirtilir. Ayrıca askerî ahlak, tüm rütbelerdeki askerlerin taşıması gereken temel bir unsur olarak değerlendirilir. Eserde ahlakın içerik ve kapsamı, ordu ve askerlikle ahlakın ilgisi, adalet ve subay ilişkisi, askerlik ve vazifenin önemi, askerî düşünce yapısı, nizam ve disiplin, moral bozukluğu ve askerlik, askerî terbiye, subay ve merhamet, propaganda, askerî karakter, askerî otorite, askerlikte çeşitli kademelerin psikolojisi, denizcilerin psikolojisi konuları yer almaktadır. Askerî karakterin esaslarından bahsedilirken, askerî personelin birinci vazifesi kanunlar ve talimnamelere uygun hareket etmesi gerektiği belirtilir. Kanun ve talimnamelerde yer almayan durumlarda askerî personelin, vicdanını dinlemesi gerektiği belirtilir. Askerî personelin ikinci vazifesi

82 1933 yılında yayınlanan kitabın yazarı Ahmet Faik olarak geçmektedir. Bu kapsamda 1943 Soyadı Kanunu öncesinde yayınlanan bu eserde Türkmen soyadı bulunmadığı görülmektedir. Soyadı Kanunu sonrasında yayınlanan eserlerde yazar adı "Faik Türkmen, A.Faik Türkmen" olarak ifade edilmektedir. Bilginin geçerliliği Türk Tarih Kurumu Kütüphanesi arşivinde yer alan ve yazara ait olan "Mufassal Hatay (1937)" eserine bakıldığında "Türkmen, A. [Ahmet] Faik." kullanımı ile doğrulanmaktadır. Bakınız: https://kutuphane.ttk.gov.tr/details?id=430686&materialType=KT&query=ahmet+faik+.

83 Bu kitap "Askerliğin Ahlakı" olarak da geçmektedir.

84 Ahmet Faik, *Askerliğin Psychologie'si Hakkında Bir Kalem Tecrübesi,* Milli Mecmua Matbaası, İstanbul, 1933, s. 18-19.

vicdanının emrine itaat etmektir.[85] Burada vicdan emri, askerî personelin doğru olanı tercih etmesi kapsamında askerî etik ile doğrudan ilişkidir.

Ordu Bilgisi 1941 Ders Yılı Notları II. Kısım Askeri Terbiye adlı eser 11 bölümden oluşmaktadır. Birinci bölüm "subaylık şerefi, meslek ve vazife aşkı, subayın takınacağı vasıflar, mesleğe karşı vazifesi ve bağlılığı"; ikinci bölüm "iyi geçinmek ve iyi olmak, iyi ahlak sahibi olmak, az söylemek, sır saklama, intizarı severlik"; üçüncü bölüm "disiplin ve önemi, askerlikte fedakârlık ve feragat duyguları"; dördüncü bölüm "askerlik ve astlara karşı yapılacak muamele"; beşinci bölüm "psikoloji bilgisi"; altıncı bölüm "terbiye nedir, talim nedir, terbiye ilminin gerekliliği ve önemi, terbiyeyi etkileyen unsurlar, terbiyenin türleri, terbiyede ferdin etkisi, çevreye uyum sağlama"; yedinci bölüm "hislerin ve fikirlerin fertlerde nasıl oluştuğu, terbiyeyi yönlendiren unsurlar, terbiyenin etkisi"; sekizinci bölüm "terbiyede eğiticinin rolü, terbiyenin amacı ve yöntemi"; dokuzuncu bölüm "ahlak terbiyesinin gerekliliği ve önemi, ahlak terbiyesi nedir, ahlak terbiyesinin amacı, cezalandırma ve ödüllendirme sisteminin uygulanmasında genel ilkeler, teveccühün dereceleri" şeklindedir.

Saygı adlı eserde saygının hangi durumlarda kimlere karşı yapılmasına dair genel geçer kuralların olmadığı belirtilir. Bu kurallar bütünü bireylerin entelektüel birikimi, akıl yürütme kabiliyeti ve duygusal değerlendirmesi ile oluşmaktadır.[86] Saygı konusu belirli başlıklar altında incelenmiştir. Askerî etik ile alakalı olanlar başlıklar şunlardır: Kanuna Saygı, Devletin Haklarına Saygı, Başkalarının Haklarına Saygı, Vazifeye Saygı, Doğruluğa Saygı, Tertip ve Nizama Saygı.

Milli ve Askeri Ahlak, adlı eser konferans kitabı olarak tanımlanmaktadır.[87] Savaş yıllarından etkisinde kaleme alınan bu eser ordu-millet anlayışını temele alarak milli askerî değerlerin güçlendirilmesi amacıyla Türk gençlerine ithafen yazılmıştır. Yazarın daha sonra yazmış olduğu Vazife ve Ahlak kitabı dikkate alındığında Türk gençliği ithafının askerî öğrencilere yapıldığı görülmektedir.[88] Milli ve Askeri Ahlak kitabı, 23 bölümden oluşmaktadır. Bölüm başlıkları: ahlak, ahlakın tarihçesi, vicdan, vazife, havsala (ahlak ölçüsü), namus, fazilet, nizam, korku, cesaret, öfke, onur/şeref, intihar, erdem, vatan ve millet, menfaat, yardım, çağdaşlık, cesaret, saadet, hitabet, propaganda, karakter şeklindedir. Bu eserde ordu, milli ahlakın temeli olarak görülmektedir. Ayrıca askerliğin iki cephesinin olduğu, dış cephesini kurallar, kanunlar, amirlerinden aldığı emirler oluştururken, iç cephesini askerî personelin vicdanını kullanarak vazifesini yapmasının oluşturduğu belirtilir. Bu kapsamda askerliğin iç cephesinin askerî etik ile doğrudan ilgili olduğunu söylemek mümkündür. Bu eserin hazırlanmasında Mustafa Şekip Tunç'un *Hissiyat Ruhiyatı*, Mustafa Namık'ın *Ahlâk* ve Necmettin Sadak'ın *Sosyoloji* kitaplarından istifade edildiği belirtilmiştir.

Vazife ve Ahlak adlı eser dört kısımdan oluşmaktadır. Eser, askerî öğrencilere ithafen yazılmıştır. İyi asker olmak için gereken yedi şarttan bahsedilen birinci kısım silah ve bayrak sevgisinin açıklaması ile başlar. Bu şartlar sırasıyla: vatanın ve milletin şeref ve haysiyetini koruma, doğruluk, disiplin, cesaret ve yiğitlik, üste itaat, dayanıklılık, iyi ilişkiler kurarak güvenilir olmaktır. İkinci kısımda vazife, milli ve askerî vazife, vicdan, ahlak ve egoistlik unsurları ele alınmıştır. Üçüncü kısımda disiplin, merhamet ve zalimlik, yiğitlik, soğukkanlılık, öfke, korku, saygı ve itaat unsurları incelenmiştir. Dördüncü kısımda ise ahlakın temelleri, milli ve askerî ahlak unsurları ele alınmıştır.

85 Faik Türkmen, *Moral,* Medeniyet Matbaaları, Ankara, 1938, s. 261.
86 Cemal Ungan, *Saygı*, Harp Okulu Matbaası, Ankara, 1941, s. 3-4.
87 Faik Türkmen, *Milli ve Askeri Ahlak,* Askeri Liseler Neşriyatı, İstanbul, 1943, s. 7.
88 Faik Türkmen, *Vazife ve Ahlak,* Askeri Liseler Neşriyatı, İstanbul, 1946), s. 3.

Türk Silahlı Kuvvetleri bünyesinde askerî etik kapsamında değerlendirebileceğimiz yayınların olduğu da görülmektedir. Bu yayınlara ilk örnek Kurmay Yarbay Remzi tarafından 1928 yılında yazılan *Kumandanlık Ruhiyatı ve Felsefesi* eseri gösterilebilir. Eser Osmanlı Türkçesi ile yazılmıştır.[89]

Nureddin Fuad Alpkartal tarafından 1951 yılında yazılan *Silahlı Kuvvetlerde Moral* adlı eser üç bölümden oluşmaktadır. Moralin silahlı kuvvetler teşkilatındaki ve askerî edebiyattaki yerleri başlıklı ilk bölümde alt başlıklar disiplin, manevi kuvvet ve moralin askerî edebiyattaki yeridir. Fransa faciasının moral sebepleri başlıklı ikinci bölüm milli savunma şartları, menfi propagandanın rolü ve subayların maneviyatı alt başlıklarına sahiptir. Silahlı Kuvvetlerin korunması başlıklı son bölümde moral doktrini hakkında, içerden beliren zaaf, dışarıdan gelen menfi tesir ve netice alt başlıkları bulunmaktadır. Bu kitapta moral olarak bahsedilen unsur, psikolojik eğilimler/özellikler, ahlak biliminin teorik ve pratik yönleridir. Silahlı Kuvvetlerde disiplini sağlamak, disipline aykırı hareket edilmesini önlemek için askerî personeli psikolojik olarak desteklemek, zor zamanların üstesinden gelmelerini kolaylaştırmak için ahlaki değerler, vatanseverlik, feragat ve şeref duygularını güçlendirmek ve disiplini bozacak davranışlar karşısında cezalandırma sistemi oluşturmak gibi çeşitli yollara başvurulduğu belirtilmektedir.[90]

Kurmay Albay Şadi Yaprak tarafından 1956 yılında yazılan *Moral İzahları* adlı eser sekiz bölümden oluşmaktadır. Sırayla bu bölümlersosyal hayat içinde harp ve sulhun yeri, milli müdafaa hizmetinin lüzum ve ehemmiyeti, milli müdafaa hizmetinde milletin durumu, ordu ve lüzum sebebi, hazar ve sefer orduları, askerlik mesleği, asker, kurmanda ve vazifeler, milli karakter, milli terbiye ve adetler, askerî vasıfların geliştirilmesi şeklindedir. Eserin yazılma amacı, Moral ve Personel Hizmetleri Talimatı doğrultusunda moral ve moralin manevi yönüyle ilgili olan milli savunma hizmetlerini analiz ederek, ilgiyi oluşturan hususlarını açıklamaktır.[91]

Terbiye Doktoru olarak geçen Baha Arıkan tarafından 1960 yılında yayınlanan *Ordu Psikolojisi* adlı eser; otoritenin kullanılması, ast, ahlak ve adetlerin etkisi, müesseselerin rolü, şef, faaliyet ve tesir vasıfları, disipline hazırlama şeklinde yedi bölümden oluşmaktadır. Bu eserin hazırlanmasında 1911-1912 yıllarında askerî okullarda verinden "Ahlak ve Eğitim Dersleri"nden istifade edildiği belirtilmektedir.[92]

Kemal Eker tarafından 1960 yılında yayınlanan *Millet Morali ve Ordu* eseri dokuz bölümden oluşmaktadır. Sırayla bu bölümler giriş, moralin tarifi ve önemi, millet morali, moral seferberlik, fert ve kitle psikolojisi, ordunun milletle teması, moral şahsiyetleri, fert ve cemiyette moralin doğuşu, netice şeklindedir. Giriş kısmında moralin tanımı ve önemi kısmında moral kelimesinin ahlak ve maneviyat olarak iki anlamda da kullanılabileceği belirtilerek, moralin iç (ahlak, psikolojik…) ve dış unsurlar (çevre) kapsamında desteklenebileceği vurgulanmaktadır.[93] Subay ahlakının temelinde vicdanının olduğu ifade edilmektedir.[94]

Nazif Oka tarafından 1985 yılında yazılan *Komutanlık Kavramı ve Komutanlık San'atı Üzerine Düşünceler* eserinde bireyin psikolojik durumu üzerinde dini, ahlaki ve geleneksel bağların önemli bir yer tuttuğu belirtilmektedir. Ahlaki bağlar, bireylerin içinde yetiştiği

89 Kur.Yb. Remzi, *Komutanlık Ruhiyatı ve Felsefesi,* Harp Akademileri Matbaası, İstanbul, 1928.
90 Nureddin Fuad Alpkartal, *Silahlı Kuvvetlerde Moral,* Genelkurmay Basım Evi, Ankara, 1951, s. 7.
91 Şadi Yaprak, *Moral İzahları,* E.U. Basımevi, Ankara, 1956.
92 Baha Arıkan, *Ordu Psikolojisi,* Anıl Yayınevi, İstanbul, 1960, s. 15.
93 Kemal Eker, *Millet Morali ve Ordu,* Ayyıldız Matbaası, Ankara, 1960, s. 9.
94 Kemal Eker, *Millet Morali ve Ordu,* s. 34-37.

çevreye göre şekillenen dini kurallara göre daha yumuşak kurallar bütünüdür. Komutanların sevk ve idare yönetimlerinde emirleri altındaki farklı bölgelerden, kültürlerden, ailelerden gelen personelin bu farklılıklarını dikkate alması gerektiği belirtilmektedir.[95]

Hulusi Çelikpazu tarafından 1986 yılında yayınlanan *Kurmay Subayın Nitelikleri* kitabının giriş kısmında yer alan Kurmay Subayın Tanımı bölümünde "Kurmay Subay, Komutanın Vicdandır." cümlesi yer almaktadır.[96] Burada vicdan, askerî personelin içsel doğru-yanlış algına sahip olmasını, etik sorumluluk hissetmesini, muhakeme kabiliyetine sahip olmasını ifade etmektedir.

Harp Akademileri Komutanlığı tarafından 1991 yılında yayınlanan *Komutanlık* yayınında Military Review dergisinin Mayıs 1990 tarihli 5. sayısında yayınlanmış olan "*Toward a Professional Military Ethic*"[97] makalesinin çevirisi yer almaktadır. Çeviride askerî etik yerine askerî ahlak[98] kavramının kullanıldığı görülmektedir.

Veli Yılmaz'ın 1994 tarihli *Komutanlık ve Liderlik Üzerine* adlı eserinin "Atatürk'ün Ahlak Anlayışı" bölümünde milli ahlakın, milletin fertleri tarafından sorgulanmadan, vicdani ve duygusal iç muhakeme ile herhangi bir sebep aranmadan yerine getirilmesi gerektiği belirtilmektedir.[99]

Yukarıda işaret edilen çalışmalarla ilgili olarak bir özet tablo aşağıda Tablo 4.'te sunulmaktadır.

Tablo 4. Askerî Etik ve Askerî Etik Eğitimi ile İlgili Yayınlar[100]

Yıl	Yazar	Eser Adı	Askerî Etik ve Askerî Etik Eğitimi ile ilgili Anahtar Kelimeler
1928	Kurmay Yarbay Remzi	*Kumandanlık Ruhiyatı ve Felsefesi*	Komutanlık, disiplin, moral, liderlik
1933	Ahmet Faik Türkmen	*Askerliğin Psychologie'si Hakkında Bir Kalem Tecrübesi*	Askerî otorite, disiplin, asker psikolojisi, terbiye
1938	Ahmet Faik Türkmen	*Moral*	Ahlak, moral, subay ilişkisi, vicdan, disiplin, terbiye, askerlik görevleri, propaganda, askerî karakter
1941	Yarbay Hadi Atay	*Ordu Bilgisi II: Askeri Terbiye*	Subaylık şerefi, disiplin, ahlak terbiyesi, psikoloji, terbiye yöntemleri, ödül-ceza sistemi
1941	Cemal Ungan	*Saygı*	Kanuna saygı, devlet haklarına saygı, başkalarına saygı, vazifeye saygı, doğruluk, tertip ve nizam.
1943	Ahmet Faik Türkmen	*Milli ve Askeri Ahlak*	Ahlak, vicdan, vazife, erdem, vatan-millet, karakter, milli değerler, askerî etik

95 Nazif Oka, *Komutanlık Kavramı ve Komutanlık San'atı Üzerine Düşünceler,* Kara Kuvvetleri Komutanlığı, Ankara, 1985, s. 3-29.
96 Hulusi Çelikpazu, *Kurmay Subayın Nitelikleri,* Harp Akademileri Basımevi, İstanbul, 1986, s. 1.
97 Mason E. Smith, "Military Review". *Toward a Professional Military Ethic*, 5, Mayıs 1990, s. 74-82.
98 ABAM Başkanlığı, "Profesyonel Bir Askerlik Ahlakına Doğru", *Komutanlık* içinde, Harp Akademileri Basımevi, İstanbul, 1991, s. 75-85.
99 Veli Yılmaz, *Komutanlık ve Liderlik Üzerine,* Harp Akademileri Basımevi, İstanbul, 1994, s. 16.
100 Tablo yazar tarafından oluşturulmuştur.

1946	Ahmet Faik Türkmen	*Vazife ve Ahlak*	Silah ve bayrak sevgisi, doğruluk, disiplin, cesaret, itaat, vicdan, ahlak, milli ve askerî vazife
1951	Nureddin Fuad Alpkartal	*Silahlı Kuvvetlerde Moral*	Moral, disiplin, manevi kuvvet, ahlak, vatanseverlik, feragat, şeref, cezalandırma sistemi
1956	Şadi Yaprak	*Moral İzahları*	Moral, milli karakter, milli terbiye, askerlik mesleği, asker-vazife, askerî vasıfların geliştirilmesi
1960	Baha Arıkan	*Ordu Psikolojisi*	Otorite kullanımı, disiplin, ahlak ve adetler, psikoloji, terbiye, personel üzerinde kurum etkisi
1960	Kemal Eker	*Millet Morali ve Ordu*	Moral, ahlak, psikoloji, disiplin, subay ahlakı, vatanseverlik, iç ve dış moral unsurları
1985	Nazif Oka	*Komutanlık Kavramı ve Komutanlık San'atı*	Psikoloji, ahlaki bağlar, dini ve geleneksel bağlar, komutanlık, etik sorumluluk
1986	Hulusi Çelikpazu	*Kurmay Subayın Nitelikleri*	Vicdan, etik sorumluluk, doğru-yanlış muhakemesi, kurmay subay nitelikleri
1991	Harp Akademileri Komutanlığı	*Komutanlık (Çeviri Eser)*	Askerî ahlak, komutanlık, etik, liderlik
1994	Veli Yılmaz	*Komutanlık ve Liderlik Üzerine*	Atatürk'ün ahlak anlayışı, vicdani muhakeme, milli ahlak

Kara Harp Okulu askerî etik eğitiminin kurumsal ve tarihsel bir temele sahip olduğu görülmektedir. West Point gibi Kara Harp Okulu'nda da askerî kişiliği inşa eden askerî etik eğitimi ile Harbiyelilerin bireysel, kurumsal ve toplumsal sorumluluklarının farkında olan, disiplinli, vicdanlı, görev bilincine sahip birer subay olarak yetiştirilmesini amaçlanmaktadır. Bu amaç doğrultusunda askerî etik eğitiminin ahlak, disiplin, komuta kontrol, hukuk, sosyoloji konuları altında ele alındığı görülmektedir. Bu durum askerî etiğin savaş etiği çerçevesinde sınırlı bir perspektifle ele alınmasına yol açtığı ve Harbiyelilerin etik bilincinin gelişimini sınırlandırdığı düşünülmektedir. Diğer yandan West Point örneğinde görüldüğü üzere askerî etik eğitimi, birinci sınıftan itibaren kademeli bir şekilde verilmekte ve Harbiyelilerin karakter gelişimi, liderlik kabiliyetleri ve değer odaklı davranış biçimleri üzerinde doğrudan etkili olmaktadır. West Point yaklaşımı, askerî etiği disiplinler arası bir bakış açısıyla ve sürekli tekrar edilen bir müfredat çerçevesinde ele alırken, Kara Harp Okulu'nda bu alanın mevcut uygulaması sınırlı kalmaktadır. Aşağıda Tablo 5'te özeti sunulan bu karşılaştırma, askerî etik dersinin ayrı bir ders olarak sunulmasının, subay sınıfı yetiştirme sürecinde etik bilincinin oluşturulması açısından önemli bir katkı sağlayabileceğini göstermektedir.

Tablo 5. West Point ve Kara Harp Okulu Askerî Etik Eğitimi Karşılaştırması[101]

Askerî Etik Eğitimi	West Point	Kara Harp Okulu
Yapısı	Askerî Etik, Harbiyelilere birinci sınıftan itibaren kademeli ve bütüncül bir şekilde ayrı dersler ve uygulamalar ile verilir.	Askerî etik, Harbiyelilere ayrı bir ders olarak verilmez. Askerî Sosyoloji dersi kapsamında ele alınır.
Müfredatı	Karakter gelişimi, liderlik kabiliyetleri ve ulusal değerlerin benimsenmesini içerir.	Savaş etiği kapsamında değerlendirilir.
Sürekliliği	Sınıflar ilerledikçe önceli bilgi ve deneyimin üzerine inşa edilir. Kademeli ve sürekli eğitim.	Tek ders veya modülle sınırlıdır. Süreklilik yok.
Hedefleri	Askerî mesleğin etik ve ahlaki sorumluluklarını benimsetmek, karmaşık durumlarda doğru karar verebilme, liderlik ve karakter gelişimi sağlamak.	Temel olarak milli değerlere, askerî disiplin ve kurallara uyumun sağlanması.
Sivil-Asker İlişkileri	Sivil-asker ilişkilerini ve toplumsal rollerin farkındalığını vurgular.	Sınırlı; etik konusu çoğunlukla savaş ve görev bağlamında ele alınır.

Sonuç olarak Kara Harp Okulu'nda askerî etik konusunun ders içinde sınırlı biçimde yer almasının, konunun derinlemesine öğrenilmesini ve ortak bir etik bilincin gelişmesini zorlaştırdığı düşünülmektedir West Point örneği ise etik eğitiminin sürekliliğinin ve karakter gelişimine katkısının önemini göstermektedir. Bu kapsamda askerî etik eğitimi yaşam boyu devam eden bir öğrenme sürecini ifade etmektedir. Dolayısıyla askerî etik eğitiminin mesleki yaşam boyunca nasıl olması gerektiği konusuna da değinmek gerekmektedir.

3. Askerî Etik Eğitimi Meslek Yaşam Boyunca Nasıl Olmalıdır?

NATO ile Barış İçin Ortaklık Konsorsiyumu (*Partnership for Peace Consortium-PfPC*) Savunma Akademileri ve Güvenlik Çalışmaları Enstitüleri (*Partnership for Peace Consortium of Defense Academies and Security Studies Institutes*) adına Kanada Savunma Akademisi'nin öncülüğünde çok uluslu bir akademisyen ekibi tarafından geliştirilen "*Generic Officer Professional Military Education (PME) Reference Curriculum (RC)* (Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı)" başlıklı belgeyle, üye ülkelerde subay profesyonel askerî eğitimini geliştirmek amacıyla akademik dersler ile ilgili ayrıntılı öğrenme hedefleri ve müfredat desteği amaçlanmaktadır. Bu çalışma, hem NATO ve ortakları arasında askerî birlikte çalışabilirliğin geliştirilmesine önemli bir katkı sağlamakta hem de subayların profesyonel askerî eğitimini yeniden düzenlemek veya geliştirmek isteyen ortaklar için bir kaynak oluşturmaktadır.

Kapsamlı Subay Profesyonel Askerî Eğitim Referans müfredatı üç safhadan oluşmaktadır:

a. Teğmen-Üsteğmen,

b. Yüzbaşı-Binbaşı,

c. Kıdemli Binbaşı-Yarbay.

Kapsamlı Subay Profesyonel Askerî Eğitim Referans müfredatı üç safhadan oluşmaktadır. Bunlar:

a. Teğmen-Üsteğmen,

b. Yüzbaşı-Binbaşı,

101 Tablo yazar tarafından oluşturulmuştur.

c. Kıdemli Binbaşı-Yarbay.

Müfredatın içerdiği iki ana tema ise:

a. Askerlik Mesleği (*Profession of Arms*),

b. Komuta, Liderlik ve Etik (*Command, Leadership and Ethics*), Savunma ve Güvenlik Araştırmalarıdır (*Defense and Security Studies*).

"Müfredatın içerdiği iki ana tema ise

a. Askerlik Mesleği (*Profession of Arms*),

b. Komuta, Liderlik ve Etik (*Command, Leadership, and Ethics*), Savunma ve Güvenlik Araştırmaları (*Defense and Security Studies*) şeklindedir.

"Komuta, Liderlik ve Etik" teması öğrencilere profesyonel askerî etik, liderlik teorileri, silahlı çatışma hukuku, komuta kontrol konsepti aracılığıyla askerlik mesleğini tanıtmaktadır.[102] Temanın içerisinde eğitim seviyesi, görev ve rütbelere[103] göre sınıflandırılan "Profesyonel Askerî Etiğe Giriş", "Askerlik Mesleğinin Etiği" ve "Etik"[104] dersleri bulunmaktadır. Tablo 6'da ilgili bilgiler yer almaktadır.

Tablo 6. Komuta, Liderlik ve Etik Teması[105]

Rütbe	Teğmen-Üsteğmen	Yüzbaşı-Binbaşı	Kıdemli Binbaşı-Yarbay
Görev	Küçük birlik düzeyinde birliklere liderlik etme yeteneğine sahip	Bölük düzeyinde birliklere liderlik etme yeteneğine sahip	Bir tabur, tugay vb. için genel komuta kurmayında liderlik etme yeteneğine sahip
Dersler	Profesyonel Askerî Etiğe Giriş Ders	Askerlik Meslek Etiği Dersi	Etik Dersi

Profesyonel Askerî Etiğe Giriş, Askerlik Mesleğinin Etiği ve Etik dersleri, tanım, öğrenme hedefleri/çıktıları, dikkate alınması gereken konular, potansiyel modüller ve öğrenme metodolojisi/değerlendirmesi başlıklarında açıklanmıştır. Bu çalışma kapsamında dikkate alınması gereken konular ve öğrenme metodolojisi incelenecektir.

3.1. Profesyonel Askerî Etiğe Giriş Dersi[106]

- Dikkate Alınması Gereken Konular:

  a. Yasal temeller (anayasa, anlaşmalar, görev yemini, angajman kuralları)

  b. Ahlaki temeller (askerî/hizmet/branş kültürü, evrensel davranış normları, evrensel insan hakları, inançlar ve sloganlar, davranış kodları, askerin davranış kuralları)

  c. Silahlı kuvvetlerin temel değerleri (özverili bağlılık, ahlaki cesaret ve kişisel sorumluluk, disiplin, dürüstlük, çatışan bağlılıklar, güvenilirlik ve takım çalışmaları; bir savaş çarpanı olarak saygı, eşitlik ve insan hakları)

  d. Tam kapsamlı operasyonlar için gerekli olan gelecekteki lider yetkinlikleri

102 "Generic Officer Professional Military Reference Curriculum", 21, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20111202_generic-officer-pme-rc.pdf, erişim 11.11.2024.
103 *Generic Officer Professional Military Reference Curriculum*, s. 6-7.
104 *Generic Officer Professional Military Reference Curriculum*, s. 7.
105 Tablo yazar tarafından oluşturulmuştur.
106 *Generic Officer Professional Military Reference Curriculum,* s. 21.

- Öğrenme Metodolojisi

  a. Dersler

  b. Tartışmalar

  c. Vaka Çalışmaları

Birinci aşamayı oluşturan "Profesyonel Askerî Etiğe Giriş" dersi, personelin mesleki kimliğini geliştirmeyi amaçlayan öncü bir eğitim basamağı olarak değerlendirilebilir. Bu dersin temel hedefi personelde askerî etik bilincinin oluşturulması, geliştirilmesi ve kurumsal değerlerle bütünleştirilmesidir. Eğitim süreci yalnızca teorik bilgilerin aktarımıyla sınırlı kalmamakta, bu bilgilerin tartışma, vaka analizi ve uygulama çalışmalarıyla pekiştirilmesini de içerdiği görülmektedir. Eğitim süreci personele askerî etik ilkeleri öğrenmenin ötesinde bu ilkeleri mesleki yaşamında karşılaştığı karmaşık durumları doğru biçimde yorumlama ve uygulama yetkinliği de kazandırmaktadır. Dolayısıyla bu ders bireysel ahlaki yargıları kurumsal normlar ve hukuki düzenlemeler ile uyumlu hale getirilmesini hedefleyen bütüncül bir yaklaşımı benimsemektedir.

3.2. Askerlik Mesleğinin Etiği Dersi[107]

- Dikkate Alınması Gereken Konular:

  a. Etik ve ahlak anlayışı ülkeden ülkeye farklılık gösterebileceği için ilgili vakaların incelemelerinde uyarlamalar yapılması gerekebileceği göz önünde bulundurulmalıdır.

  b. Ders kapsamı ulusal ve uluslararası düzeyleri yansıtan vaka çalışmaları odaklı olmalıdır.

  c. Öğretmen veya eğitmen ders verme ve rehberlik yapma arasında geçiş yapabilme kabiliyetine sahip olmalıdır.

  d. Askerî organizasyon ve operasyon alanında eşitlik değerleri nasıl desteklenebilir?

  e. Davranış kuralları, etik davranışta nasıl bir rol oynamaktadır?

- Öğrenme Metodolojisi

  a. Öğretim sunumu, etiği tanıtmaya yönelik dersleri içerecektir.

  b. Vaka çalışmaları. Örnek olarak "Er Ryan'ı Kurtarmak" filmi.

  c. Grup tartışmaları.

İkinci aşamayı oluşturan "Askerlik Mesleğinin Etiği" dersi, personelin askerî etik bilincini uluslararası düzeyde yönetebilme ve uygulayabilme yetkinliğini kazandırmayı amaçlamaktadır. Dersin temel hedefi personelin farklı kültürel ve operasyonel ortamlarda karşılaşabileceği çok boyutlu durumlarda askerî etik ilkeleri içselleştirerek bunları karar alma süreçlerinde etkin bir şekilde uygulayabilmesidir. Bu süreç personelin askerî etik ilkelere uygun ve bilinçli karar alabilme kabiliyetlerini geliştirerek mesleki uygulamalarda disiplinlerarası bütüncül bir askerî etik farkındalığı kazanmalarını sağladığı değerlendirilmektedir. Bu aşamada yararlanılan vaka analizleri ve grup tartışmaları askerî personelin etik ikilemler karşısında hızlı ve tutarlı değerlendirmeler yapabilme kapasitesini artırdığı, eleştirel düşünme yetkinliklerini geliştirdiği ve sorumluluk bilincini derinleştirdiği düşünülmektedir.

107 *Generic Officer Professional Military Reference Curriculum,* s. 48.

3.3. Etik Dersi[108]

- Dikkate Alınması Gereken Konular:

  a. Bu düzeyde etkili bir liderlik sağlamak için gerekli değerler en iyi şekilde nasıl desteklenebilir?

  b. Adil savaş teorisi nedir?

  c. Bir lider etik değerleri ve askerî gereklilikleri nasıl uzlaştırır?

  d. Çaresiz koşullar karamsar bir öngörüyü kaçınılmaz hale mi getirir?

- Öğrenme Metodolojisi

  a. Bireysel çalışma

  b. Dersler

  c. Tartışmalar

  d. Saha gezileri

  e. Simülasyonlar

  f. Küçük grup tartışmaları ve katılımı

  g. Bilimsel makaleler

  h. Yansıtıcı günlük tutma,

Üçüncü aşamanın temel amacı, personelin bir lider olarak karmaşık ve kritik karar alma süreçlerinde askerî etik bilincini stratejik düzeyde uygulayabilme yetkinliğini kazanmasını sağlamaktır. Önceki aşamalarda edinilen temel askerî etik bilgisi ve uluslararası bağlamda etik farkındalık üçüncü aşamada üst düzey bir liderlik perspektifi ile bütünleşmektedir. Bu dersin öğrenme hedefleri personelde bireysel askerî etik farkındalık ile sınırlı kalmayıp, stratejik karar alma süreçlerinde askerî etik ve operasyonel gereklilikler arasında bilinçli bir denge kurabilme kapasitesini geliştirmeye odaklanır. Metodolojik olarak üçüncü aşama öğrenme sürecini teorikten pratiğe taşıyan çok boyutlu bir yaklaşımı benimsediği görülmektedir. Burada askerî etik eğitiminde üst düzey bir bütünsellik sunulmakta; bilgi, etik ve davranış unsurları arasındaki ilişkiyi pekiştirmektedir.

Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı, Silahlı Kuvvetler için askerî etik eğitiminin subay sınıfının her kademesinde nasıl uygulanması gerektiğine dair hem teorik hem de uygulamalı bir çerçeve sunmaktadır. Müfredat, askerî etik eğitimin yalnızca Harp Okulu düzeyinde sınır kalmaması gerektiğini, mesleki yaşam sürecinde sürekli olarak desteklenmesi gerektiğini göstermektedir. Birinci aşamada personel, yasal ve ahlaki temeller, kurumsal değerler ve davranış kuralları hakkında bilgilendirilir; tartışmalar ve vaka çalışmaları ile bu bilgiler pratiğe dönüştürülür. İkinci aşamada personel, ulusal ve uluslararası bağlamda etik uygulamaları öğrenir, farklı kültürel ve operasyonel ortamlarda etik ikilemleri analiz edebilme ve grup içinde çözüm geliştirebilme yetkinlikleri kazanır. Üçüncü aşamada ise personele, liderlik, adil savaş ilkeleri ve zor koşullarda etik karar alma becerileri kazandırılır; stratejik kararları etik ve operasyonel gereklilikler arasında dengeleyebilme, etik davranışı yönlendirebilme ve etik kararlar alma becerileri geliştirilir. Müfredatın bu yapılandırması, askerî etik eğitimini sistematik, bütüncül, stratejik ve proaktif bir şekilde sunar. Müfredat her aşamada farklı öğrenme hedefleri ve metodolojilerle ilerleyen

108 *Generic Officer Professional Military Reference Curriculum,* s. 76.

bir çerçeveye sahip olmasıyla sistematiktir. Başlangıçtan ileri düzeye kadar süregelen bir etik bilinci ve davranış geliştirmeyi kapsamasıyla bütüncüldür. Sadece bireysel davranışını değil, kurumsal kararlarını da askerî etik çerçevesinde yönlendirebilmesini hedeflemesiyle stratejiktir. Personelin, meslek yaşamı boyunca karşılaşabileceği etik sorunlara hazırlıklı olmasını sağlayarak, etik karar alma kabiliyetlerini önceden geliştirmeye yönelik olmasıyla proaktiftir. Sonuç olarak bu müfredat personelin askerî etik alanındaki bilgi ve kabiliyetini geliştirmekte böylece hem bireysel sorumluluk bilincini hem de kurumsal düzeyde askerî etik standartlarının uygulanmasını pekiştirmektedir.

Sonuç

Askerî etik, Silahlı Kuvvetlerin misyonunu, vizyonunu, temel değerlerini, kanunlarını, disiplin ve sorumluluk bilincini içeren çok boyutlu bir kavramdır. Bu bilincin askerî personelin kişisel ve mesleki yaşamına aktarımının sağlanması ise askerî etik eğitimi ile mümkündür. Askerî etik eğitimi, personelin askerlik mesleğinin etik ve ahlaki sorumluluklarını üstlenmesine, karmaşık ve belirsiz durumlar karşısında doğru kararı verebilmesine, toplumsal rollerinin farkında olarak sivil-asker ilişkileri üzerindeki etkisini kavramasına yardımcı olmaktadır. Bu çalışmada hem askerî etik kavramının hem de askerî etik eğitiminin Harp Okulu düzeyinde incelenmesi ve mesleki yaşam boyunca nasıl olması gerektiğinin anlaşılması hedeflenmiştir.

Askerî etik, West Point ve Kara Harp Okulu müfredatında yer almaktadır. Literatür taramasında Kara Harp Okulu'nda askerî etik eğiminin okulun başlangıcından bu yana önemsendiği, ilgili derslerin ve yayınların olduğu görülmektedir. Fakat günümüzde Kara Harp Okulu müfredatı incelendiğinde askerî etik dersinin ayrı bir ders olarak verilmediği, askerî etik konusunun Askerî Sosyoloji dersi içerisinde yer aldığı görülmektedir. Askerî Sosyoloji kitabında askerî etik kısmının savaş etiği kapsamında değerlendirildiği ve bunun da askerî etiği anlamak adına bir eksiklik oluşturduğu dikkat çekmektedir.

Askerî etik dersinin neden ayrı bir ders olarak verilmesi gerektiğine West Point kayda değer bir örnektir. West Point'te birinci sınıftan başlayarak kademeli bir şekilde ilerleyen askerî etik eğitimi, okulun tarihi kadar eskidir. Harbiyeliler yeni bir sınıfa geçtiğinde askerî etik konusunda önceki bilgi ve deneyimlerinden faydalanmaktadır. West Point için askerî etik eğitimi, Harbiyelilerin karakter gelişimini desteklemekte, liderlik vasıflarının getirmiş olduğu zorlukları anlamalarına yardımcı olmakta, ordunun ve ulusun değerlerini önceleyerek hareket edebilen subaylar olarak yetiştirilmesini sağlamaktadır.

Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatı ise Silahlı Kuvvetlerin yaşam boyu öğrenme felsefesini yansıtan, subayların mesleki, etik ve liderlik kabiliyetlerini bütüncül bir şekilde geliştirmeyi hedefleyen bir eğitim programı sunmaktadır. Bu eğitim programı tüm subay kademesinin ihtiyaçları doğrultusunda bir önceki bilgi ve deneyimlerini temel alarak kademeli bir ilerleme sağlamakta; başlangıç seviyeden üst düzey liderlik eğitimine kadar farklı aşamaları kapsamaktadır. Kapsamlı Subay Profesyonel Askerî Eğitim Referans Müfredatının uygulama öncesinde, ülkelerin temel değerlerine, kurum içi disiplinine, etik standartlarına, yasal çerçevelerine ve uluslararası askerî normlarına uygun olarak şekillendirilmesi ve Silahlı Kuvvetlerin eğitim sistemlerine uyumlu hale getirilmesinin önemli olduğu değerlendirilmektedir. Program, teori ve pratiği birleştiren modüller, simülasyonlar, vaka analizleri, saha tatbikatları ve liderlik atölyeleri ile desteklenmekte, subayların etik karar alma, kriz yönetimi ve liderlik becerilerini gerçekçi senaryolar üzerinden pekiştirmesine olanak sağlamaktadır. Ayrıca sürekli geri bildirim ve performans değerlendirmesi mekanizmaları ile subayların gelişimi izlenmekte ve eğitim süreçleri güncel ihtiyaçlara göre yeniden şekillendirilmektedir. Bu müfredat aynı zamanda

subayların ulusal ve uluslararası operasyonlarda karşılaşabilecekleri etik ve profesyonel zorluklara hazırlıklı olmasını sağlayacak bir yapı sunmakta ve Silahlı Kuvvetlerin misyon ve vizyonuyla uyumlu, etik değerlere bağlı, sorumluluk bilinci yüksek liderlerin yetiştirilmesini olanak sağlamaktadır.

Silahlı Kuvvetlerde verilen veya planlanan askerî etik eğitimi, personelin mesleki sorumluluklarını yerine getirebilmesi ve etik karar alma kabiliyetlerini geliştirebilmesi için hem teorik hem de pratik boyutlarıyla ele alınmalıdır. Teorik boyutta, askerî etik ilkeler, savaş hukuku, insan hakları, kurumun temel değerleri ve disiplin anlayışı detaylı bir şekilde öğretilmelidir. Teorik eğitimde amacı personelin sadece ilgili kuralları ve değerleri bilmesi değil, aynı zamanda bunları içselleştirerek kararını ve davranışlarını yönlendirmesini hedeflemelidir. Eğitim süreci sosyoloji, psikoloji ve liderlik disiplinleriyle desteklenmeli, tartışma oturumları ve geribildirim mekanizmalarıyla pekiştirilmelidir. Ayrıca personelin etik karar alma süreçlerinin ölçülebilmesi için standart bir değerlendirme kriteri de geliştirilmelidir. Pratik boyutta ise performans değerlendirmesi için simülasyon yöntemlerinden, arttırılmış gerçeklik, sanal gerçeklik ve karma gerçeklik uygulamalarından yararlanılmalıdır. Deneyimli personelden mesleki tecrübe aktarımının yapıldığı dersler ve konferanslar düzenlenmelidir. Pratik eğitim personelin baskı altında, stresli ve karmaşık ortam senaryolarında etik karar alma becerilerini uygulamalı olarak deneyimlemelerine olanak sağlar. Ayrıca saha tatbikatları, rol oyunları ve kriz yönetimi uygulamaları ile personelin teorik bilgilerini gerçek durumlarda kullanabilme kapasitesini arttıracağı düşünülmektedir. Son olarak ayrı bir disiplin olarak değerlendirilen askerî etik için, askerî etik uzmanlarının yetiştirilmesi gerektiği değerlendirilmektedir. Bu uzmanlar hem teorik bilgiye hem de saha deneyimine sahip olmalı, eğitim programlarını tasarlayabilmeli, simülasyon ve vaka analizlerini yönetebilmeli ve farklı kademelerdeki personelin askerî etik gelişimini takip edebilmelidir. Uzmanlar ayrıca uluslararası etik standartlar, operasyonel gerçeklikler ve gereklilikler konularında güncel bilgiye sahip olarak, personelin etik karar alma süreçlerini yönlendirebilecek rehberliği sağlamalıdır.

Çıkar Çatışması

Bu çalışmada çıkar çatışması teşkil edebilecek durum ve/veya ilişki bulunmamaktadır.

Yapay Zeka Kullanımı Bildirimi

Çalışmada herhangi bir şekilde yapay zeka uygulamalarından yararlanılmamıştır.

KAYNAKÇA

Basılı Eserler

GABRIEL Richard (1982). *To Serve with Honor A Treatise on Military Ethics and the Way of the Soldier,* London: Greenwood Press.

ABAM Başkanlığı (1991). *Profesyonel Bir Askerlik Ahlakına Doğru*, *Komutanlık* İçinde, Harp Akademileri Basımevi, İstanbul.

Ahmet Faik (1933). *Askerliğin Psychologie'si Hakkında Bir Kalem Tecrübesi,* Milli Mecmua Matbaası, İstanbul.

AKKOR Feridun (1957). *İç Disiplin*, *Ordu Saati Konuşmaları* İçinde, E.U. Personel Başkanlığı Moral Şubesi Yayınları No:15, E.U. Basımevi, Ankara.

ALPKARTAL Nureddin Fuad (1951). *Silahlı Kuvvetlerde Moral*, Genelkurmay Basım Evi, Ankara.

ARIKAN Baha (1960). *Ordu Psikolojisi*, Anıl Yayınevi, İstanbul.

ATEŞ Barış (2022). *Askerî Sosyoloji Ordu ve Toplum Araştırmaları*, Selenge Yayınları, İstanbul.

AVCI Mehmet (2023). *30 Soruda Jandarma ve Etik*, JSGA Basımevi Müdürlüğü, Ankara.

BADEMLİ Hakan (2024). "Türkiye'de Ordu ve Siyaset: Sivil-Asker İlişkilerinin Dönüşümü". *Yayınlanmamış Doktora Tezi*, Bursa Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı Siyaset ve Sosyal Bilimler Bilim Dalı, Bursa.

BİRDİŞLİ Fikret (2023). "Uluslararası Kurumların Normatif Bir Unsur Olarak Uluslararası Güvenlik". *Ankara Üniversitesi SBF Dergisi* 78:2, 381-405.

BRIGADIER Daniel Lätsch (2010). "Preface", Jeff Stouffer and Stefan Seiler (ed.), *Military Ethics: International Perspectives,* Canadian Defence Academy Press, Kingston, iii-v.

COLEMAN Stephen (2015). "Ethical Dilemmas and Tests of Integrity", Deane-Peter Baker (ed.), *Key Concepts in Military Ethics,* NewSouth Publishing, Sydney, 8-11.

COOK Martin L. ve SYSE Henrik (2010). "What Should We Mean by 'Military Ethics'?" *Journal of Military Ethics,* 9:2, 119-122.

COOK Martin L. (2013). *Issues in Military Ethics To Support and Defend the Constitution,* State University of New York Press, New York.

ÇAM Yusuf (1991). *Atatürk'ün Okuduğu Dönemde Askeri Okullar Rüşştiye-İdadi-Harbiye (1892-1902),* Genelkurmay Basım Evi, Ankara.

ÇELİKPAZU Hulusi (1986). *Kurmay Subayın Nitelikleri,* Harp Akademileri Basımevi, İstanbul.

EKER Kemal (1960). *Millet Morali ve Ordu,* Ayyıldız Matbaası, Ankara.

GABRIEL Richard A (2007). *The Warrior's Way: A Treatise on Military Ethics,* Canadian Defence Acad. Press, Kingston, Ontario.

GAITAN-MONJE Enrique ve DE CASTRO-GARCIA Andres (2023). "En búsqueda de la mejor formación de oficiales Academia militar de España vs. West Point". *Revista Colombiana de Estudios Militares y Estratégicos*, 21:44, 927-948.

GILLNER Matthias (2019). "Ethical Education in the German Armed Forces: Embraced Values and Moral Judgement". *Ethics and Armed Forces: Controversies in Military Ethics and Security Policy: Between Personality Development and Skills Acquisition: Ethics for Soldiers*, 02, 22-29.

GIRAY Muharrem (1961). *Şanlı Harbiye'nin Tarihi,* Hilmi Kitabevi Ltd., İstanbul.

KURTCEPHE İsrafil ve BALCIOĞLU Mustafa (1991). *Kara Harp Okulu Tarihi*, Kara Harp Okulu Matbaası, Ankara.

LUCAS George ve ALLEN John R. (2016). *Military Ethics: What Everyone Needs to Know,* NY: Oxford University Press, New York.

LOHMANN Friedrich (2023). "Ethical Education – A Central Component of Training and Development in the German Armed Forces", *Ethics and Armed Forces: Controversies in Military Ethics and Security Policy: Between Personality Development and Skills Acquisition: Ethics for Soldiers*, 02.

OKA Nazif (1985). *Komutanlık Kavramı ve Komutanlık San'atı Üzerine Düşünceler,* Kara Kuvvetleri Komutanlığı, Ankara.

PEPERKAMP Lonneke, van LOON Kevin, BAKER Deane-Peter ve EVERED David (2023). "Military Ethics and Military Ethics Education: In Search of a 'European Approach'". Ethics and Armed Forces: Controversies in Military Ethics and Security Policy: Core Issues of European Military Ethics 02, 4-11.

PIRIYEV Heydar (2019). "The Role of Military Ethics and Morals as a Subject of Pedagogy in the Leadership of Officers for Multinational Environment", J*ournal of Defense Resources Management*, 10:2, 243-249.

RHOD Bill (2009). *An Introduction to Military Ethics: A Reference Handbook - Contemporary Military, Strategic, and Security Issues*, Praeger Publishers, Canada.

ROBINSON Paul, DE LEE Nigel ve CARRICK Don (2010). *Ethics Education in the Military*.: Ashgate Pub. Co., Aldershot, England Burlington, VT.

SANDERS Joseph, LINDSAY Douglas, FOSTER Craig A. ve COOK James (2010). "Ethics in the 21st Century Profession of Arms: Context for Developing Leaders of Character", Jeff Stouffer ve Stefan Seiler (ed.), *Military Ethics: International Perspectives*, Canadian Defence Academy Press. Kingston, Ontario, 79-116.

SANİ İbrahim Mert (2020). "Askeri Etik". *Turkish Journal of War Studies,* 1:1, 24-34.

SMITH Mason E. (1990). "Military Review". *Toward a Professional Military Ethic*, 5: 74-82.

STANAR Dragan (2023). "Military Ethics Education – Bridging the Gap or Deepening the Chasm?".

TAŞKIRAN Cemalettin (2009). *Yüzyıllardır Harbiye Harbiye'nin 180 Yıllık Tarihi ve En Büyük Harbiyeli Atatürk,* Doğan Kitap, İstanbul. Milli Savunma Bakanlığı (2021), *Türk Silahlı Kuvvetleri Meslek Etiği Yönergesi*.

TROY Jadok (2024). "Ethics as Moral Practice in Peacekeeping Missions: Insights on the Importance of Ethical Training". *International Peacekeeping* 31:3, 309-331.

TURNER Michael E. DEBOS Chad W. ve LICAMELI Francis C. (2010). "Moral Development: The West Point Way". *Journal of Character and Leadership Development,* 1:2, 11-23.

TÜRKMEN Faik (1943). *Milli ve Askeri Ahlak,* Askeri Liseler Neşriyatı, İstanbul.

TÜRKMEN Faik (1938). *Moral,* Medeniyet Matbaaları, Ankara.

TÜRKMEN Faik (1946). *Vazife ve Ahlak,* Askeri Liseler Neşriyatı, İstanbul.

ÜNAL Elif (2024). "Megan Cassidy-Welch'in 'Crusades and Violence' Adlı Eserinin Değerlendirmesi". *Şarkiyat Mecmuası - Journal of Oriental Studies*, 44, 309-314.

UNGAN Cemal (1941). *Saygı,* Harp Okulu Matbaası, Ankara.

YILMAZ Veli (1994). *Komutanlık ve Liderlik Üzerine,* Harp Akademileri Basımevi, İstanbul.

WHETHAM David (2021). "What Senior Leaders in Defence Should Know about Ethics and the Role That They Play in Creating the Right Command Climate The Leadership Edge", *The International Journal of Ethical Leadership*, 8:19, 73-93.

İnternet Kaynakları

"Acronym/Term/Phrase", https://www.westpoint.edu/sites/default/files/inlineimages/DMI/what%20is%20that.pdf?ref=c ortis.com, erişim 23.12.2024.

"Course Subject Search Results". https://courses.westpoint.edu/crse_sbjct_rslts.cfm, erişim 11.11.2024.

"Definition of ETHIC", https://www.merriam-webster.com/dictionary/ethic, erişim 22.11.2024.

"Dictionary.Com | Meanings & Definitions of English Words" https://www.dictionary.com/browse/ethics, erişim 22.11.2024.

"Dictionary.Com | Meanings & Definitions of English Words", https://www.dictionary.com/browse/moral, erişim 22.11.2024.

"Educating_Future_Officers Preparing Soldier – Scholars to Win on the Modern Battlefield". https://s3.amazonaws.com/usmamedia/inlineimages/about/superintendent/Educating_Future_Officers%20_AY22.pdf, erişim 11.12.2024.

EMONET Florian. "The Importance of Ethics Education in Military Training", https://www.armyupress.army.mil/Journals/NCO Journal/Archives/2018/November/Ethics/#:~:text=Military%20ethics%2C%20like%20medical%20or,laws%20are%20no%20longer%20helpful, erişim 16.11.2024.

"ethic noun - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's

Dictionary at OxfordLearnersDictionaries.com", https://www.oxfordlearnersdictionaries.com/definition/english/ethic?q=ethics, erişim 22.11.2024.

"ethics | Search Online Etymology Dictionary", https://www.etymonline.com/search?q=ethics, erişim 22.11.2024.

FRENCH John William (1858). "A Short Course of Study in the Practical Part of Ethics" *New York: J.F. Baldwin, Printer,* https://usmalibrary.omeka.net/items/show/11, erişim 16.11.2024.

"Generic Officer Professional Military Reference Curriculum", https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_topics/20111202_generic-officer-pme-rc.pdf, erişim 11.11.2024.

"Güvenlik Bilimleri Fakültesi Teşkili ve Görevler", https://www.jsga.edu.tr/fakulte/amac-ve-gorevler, erişim 13.05.2025.

"History About | United States Military Academy West Point", https://www.westpoint.edu/academics/departments/history/about, erişim 11.11.2024.

Jandarma ve Sahil Güvenlik Akademisi, "Güvenlik Bilimleri Fakültesi Müfredatı (2022-2026)".

https://www.jsga.edu.tr/kurumlar/jsga.edu.tr/IcSite/fakulte/Dersler/Mufredat(1).pdf, erişim 09.04.2025.

"Kara Harp Okulu Eğitim-Öğretiminde Kazandırılan Temel Askerî ve Değer Kabiliyetler", https://kho.msu.edu.tr/hakkinda/amac_gorevler.html, erişim 13.05.2025.

"moral adjective - Definition, pictures, pronunciation and usage notes | Oxford Advanced Learner's Dictionary at OxfordLearnersDictionaries.com", https://www.oxfordlearnersdictionaries.com/definition/english/moral_1?q=moral, erişim 22.11.2024.

"Plato, Plato, Laws, Book 7, section 792e" https://www.perseus.tufts.edu/hopper/text?doc=Perseus:text:1999.01.0166:book=7:section=792e&highlight=ethos, erişim 22.11.2024.

"Information Paper: Professional Military Ethic Education (PME2) Program Overview",https://www.west-point.org/class/usma1965/Class2015/Activities/PME2_InfoPaper-5July2010-Final.pdf, erişim 29.11.2024.

"Prelude to War 1860 – 1861 · West Point and The Civil War · U.S. Military Academy Library Exhibits", https://usmalibrary.omeka.net/exhibits/show/westpointcivilwar/prelude-to-war-----1860-1861, erişim 11.11.2024.

"Simon Center for the Professional Military Ethic | United States Military Academy West Point", https://www.westpoint.edu/about/academy-leadership/commandant/simon-center-for-the-professional-military-ethic, erişim 12.11.2024.

"United States Military Academy Character Programı Academic Year 2020 / Simon Center for the Prefessional Military Ethic",3, https://www.thefire.org/sites/default/files/2002/06/31174402/Goldbook-20191.pdf, erişim 12.11.2024.

"United States Military Academy Academic Program Class of 2024 Curriculum and Course Descriptions", https://s3.amazonaws.com/usma- media/inlineimages/academics/dean/PDFs/RedBook_GY2024_20210712.pdf, erişim 03.01.2025.

"United States Military Academi Academic Program Class of 2026 Circulum and Course Descriptions", https://s3.amazonaws.com/usma-media/inline-images/academics/dean/strategic_documents/RedBook_GY2026_20220810_0.pdf, erişim 11.11.2024.

"USMA Academic Program", https://courses.westpoint.edu/static/index.htm#t=Simon_Center_for_the_Professional_Military_Ethic.htm&rhsearch=MX400&ux=search, erişim 17.12.2024.

"West Point Mission Statement | United States Military Academy West Point", https://www.westpoint.edu/about/history-of-west-point/west-point-mission-statement, erişim 11.11.2024.

"WHITE PAPER", https://www.west-point.org/users/usma1951/18250/whitepaper.htm, erişim 03.01.2024.

YAZIM KURALLARI

Güvenlik Stratejileri Dergisine gönderilen çalışmalar daha önce yayımlanmamış ve ilgili alana katkı sağlayacak özgün çalışmalar olmalıdır. "Yayın Etiği ve Değerlendirme Süreci"nde yer alan parametreler dışında deskriptif ya da ilgili konuda mükerrer olan çalışmalar değerlendirme safhasına alınmayacaktır. Bilimsel toplantılarda sunulmuş bildiriye dayanan çalışmalar, ilgili bildiri kitabında yayımlanmamış olması ve bu durumun Editörler Kuruluna belirtilmesi koşuluyla kabul edilebilir.

Güvenlik Stratejileri Dergisi'nin etik ilkeler ve yayın politikası Committee on Publication Ethics (COPE) tarafından yayınlanan rehberler ve politikalar dikkate alınarak hazırlanmıştır. Yayın ilkeleri, yazarlar ile ilişkiler ve hakemlerle ilişkiler konularında ayrıntılı bilgiye dergimizin internet sitesindeki ilgili başlıklar altından erişilebilir. Yayımlanmak üzere https://dergipark.org.tr/tr/pub/guvenlikstrtj üzerinden Güvenlik Stratejileri Dergisine iletilen makale metinleri, aşağıda belirtilen biçimsel özellikleri haiz ve konu/alan açısından uygun bulunmaları halinde alan uzmanı (en az) iki hakeme gönderilir. Yazarlar, Yayın Kurulu tarafından reddedilen çalışmalarını hakem raporları çerçevesinde gözden geçirerek Güvenlik Stratejileri Dergisi editörlüğüne gönderir. Bu çalışmalardan yeterli değişiklik yapılmadığı tespit edilenler yazarlarına iade edilir ve süreç sona erer. Yeterli değişiklik yapıldığı tespit edilen çalışmalar ise tekrar değerlendirme sürecine alınır. Hakem raporları tavsiye niteliğindedir ve yayın kararı Editör Kurulu tarafından alınır.

Güvenlik Stratejileri Dergisine yabancı dilde makale gönderen yazarlar, çalışmalarını makale yazım dili anadili olan ve alanında yetkinliği bulunan bir akademisyene/uzmana "son okuma" yaptırıp bunu ibraz etmekle yükümlüdür.

Güvenlik Stratejileri Dergisinde yayımlanan çalışmalarda ifade edilen görüşler yazarların şahsi bilimsel değerlendirme ve görüşleri olup, mensubu oldukları kurum ve kuruluşlar ile derginin yayımcısı olan Atatürk Stratejik Araştırmalar ve Lisansüstü Eğitim Enstitüsü'nün ve Millî Savunma Üniversitesi'nin kurumsal kimliğini bağlamaz ve bu kurumların görüşü olarak lanse edilemez.

Dergide yayın yapmış tüm yazarlar, Güvenlik Stratejileri Dergisinin doğal hakemleri sayılmaktadır. Yayın Kurulu'nun talebi üzerine yazarlar en az bir defaya mahsus hakemlik yapmakla mükelleftir.

Makale Metin Şekil Esasları

1. Güvenlik Stratejileri Dergisinin yayın dili Türkçedir. Ancak İngilizce, Almanca ve Fransızca makale ve değerlendirme yazıları da yayımlanabilir. Türkçe makalelerin imla ve noktalamasında Türk Dil Kurumu kurumsal web sayfasında yer alan güncel sözlük ve yazım kuralları esas alınır. Gönderilen makaleler dil ve anlatım açısından bilimsel kıstaslara uygun, açık ve anlaşılır olmalıdır.

2. Gönderilen makale metni (öz, abstract, kaynakça, geniş özet-summary- ve dipnotlar dâhil) asgari 6000, azami 10.000 kelime olmalıdır. Belirtilen sınırların üzerinde veya altında olan çalışmalar değerlendirilmeden yazara iade edilir.

3. Makalelere Türkçe ve İngilizce olarak hazırlanmış azami 200 kelimelik öz ve beş anahtar kelime (İngilizce abstract ve keywords) eklenmelidir. Öz, makalenin kaleme alınma amacını, yöntemini, hipotezini/araştırma sorusunu, bulguları ve sonucunu kısaca belirtmelidir. Öz yazımında "bir kısa, iki uzun cümle" prensibine riayet edilmelidir. (Almanca veya Fransızca olarak hazırlanan makalelerde Türkçe ve İngilizce öz/abstract ve anahtar kelime/keywords yanı sıra makalenin yazıldığı dilde de yukarıdaki ilkelerle öz ve anahtar kelime eklenmelidir.) Ayrıca öz ve abstract bölümünün devamında 750-1000 kelime aralığında olacak şekilde İngilizce geniş özete (extended abstract) yer verilmelidir. Geniş özet, öz kısmında yer verilen hususlara ilave olarak vurgulanması gerekli görülen noktaları, tartışmaları ve makalenin genel akışını içermelidir. Türkçe hazırlanan makalelerde söz konusu geniş özet İngilizce; İngilizce hazırlanan makalelerde geniş özet Türkçe yazılmalı; Almanca ve Fransa hazırlanan makalelerde ise geniş özet hem İngilizce hem Türkçe olarak hazırlanmalıdır.

4. Güvenlik Stratejileri Dergisine gönderilen makaleler Microsoft Word programında Times New Roman karakteri kullanılarak 11 punto yazılmalıdır. Dipnotlar ise 9 punto yazılmalıdır. Metnin paragraf özellikleri hizalama iki yana ve satır aralığı 1,5 iken dipnotlarda paragraf özellikleri iki yana hizalı ve 1 satır aralığında olmalıdır. Sayfa numaraları sayfa altında verilmelidir.

5. Yazar adı, İngilizce ve Türkçe olarak yazılan makale başlığının altına yazılmalı; yazarın unvanı, görev yeri ve elektronik posta adresi dipnotta (*) işareti ile 9 punto yazılarak belirtilmelidir. Diğer açıklamalar için yapılan dipnotlar metin içinde ve sayfa altında numaralandırılarak verilmelidir. Makalelerde ikili alt başlık sistemi kullanılmalıdır. Alt başlıklar koyu yazılmalı ve (giriş ile sonuç dışında) rakam ile numaralandırılmalıdır.

6. Metnin içindeki alıntılar çift tırnak ile gösterilmeli; üç satırı geçen alıntılar yeni bir paragraf olarak, içerden, tek aralık ve iki yana yaslı şeklinde yazılmalıdır. Alıntı içerisindeki alıntılar tek tırnak içerisinde gösterilmelidir. Metin içinde vurgulanmak istenen kelimeler koyu veya altı çizili yapılmamalı, çift tırnak içerisinde yazılmalıdır.

7. Makalelerin hazırlanmasında kullanılan kaynaklara yapılacak atıflarda aşağıdaki Yazım Kurallarına uyulmalıdır. Bu kurallara riayet etmeyen çalışmalar, doğrudan reddedilecektir.

8. Birden fazla kez aynı kaynağa atıfta bulunulduğunda; ilk atıfta künye tam olarak verilmeli, ikinci atıfta yazarın soyadı ve çalışmanın kısaltılmış başlığı kullanılmalıdır. Birbirini takip eden dipnotlarda aynı kaynağa yapılacak atıflarda ise soyadı ile birlikte "age" kullanılmalıdır. (Yabancı dildeki makalelerde "Ibid." kullanılmalıdır.)

9. Yazarlar makale başvurusu sırasında aksini belirtmedikleri sürece çalışmaya dair katkı oranları yarı yarıya kabul edilir.

9. Dipnotlarda atıflar şu şekillerde verilmelidir:

9.1. Kitaplara yapılan atıflarda yazar adı ve soyadı, eser adı, (varsa cilt numarası), (varsa çeviren), yayınevi, yayımlandığı yer, yayımlandığı tarih ve sayfa numarası aşağıdaki örneklere uygun olarak sırayla verilmelidir.

1 Morris Janowitz, *The Professional Soldier: A Social and Political Portrait*, Free Press, New York, 1964, s. 210.

2 John J. Mearsheimer ve Stephen M. Walt, *The Israel Lobby and U.S. Foreign Policy*, FSG Adult, New York, 2008, s. 92.

3 Mustafa Aydın, Mitat Çelikpala vd., *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Bilgi Üniversitesi Yayınları, İstanbul, 2015, s. 79.

4 Janowitz, *The Professional Soldier*, s. 155.

5 Age, s. 156.

9.2. Makalelere yapılan atıflarda yazar adı ve soyadı, "makale adı" (varsa çeviren), yayımlandığı süreli yayının adı, yayımlandığı yıl, sayı ve cilt numarası, alıntının yapıldığı sayfa numarası aşağıdaki örneklere uygun olarak sırayla verilecektir. Ansiklopedi maddelerine yapılan atıflarda da makalelere atıf şekli kullanılacaktır.

Adam Grissom, "The Future of Military Innovation Studies", *Journal of Strategic Studies*, 29:5, 2006, s. 910.

Özlem Durgun ve Mustafa Caner Timur, "Savunma Harcamaları ve Ekonomik Büyüme İlişkisi: Türkiye Analizi", *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, 54, 2017, s. 119.

Lütfi Sürücü, Fehiman Eminer ve Murat Sağbaş, "The Relationship of Defense Expenditures and Economic Growth Examples of Turkey and China (2000-2020)", *Güvenlik Stratejileri Dergisi*, 18:41, 2022, s. 175.

Dört ve daha fazla yazarlı makalelerde birinci yazardan sonra Gültekin Yıldız vd. şeklinde kısaltma yapılır.

9.3. Derleme kitaplar ve bildiri kitaplarında bölüm/makale:

Engin Avcı, "Ceza Adalet Sistemi Çerçevesinde Şiddet İçeren Radikalleşmeyle Mücadele: Terörist Rehabilitasyonu ve Yeniden Topluma Kazandırma", Gökhan Sarı ve Cenker Korhan Demir (ed.), *Uluslararası Güvenlik Kongresi, Kuram, Yöntem, Uygulama*, Jandarma ve Sahil Güvenlik Akademisi Yayınları, Ankara, 2019, s. 433.

9.4. İnternette Makale:

George F. Kennan, "The Sources of Soviet Conduct", *Foreign Affairs Magazine*, Temmuz 1947, https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct, erişim 21.11.2019.

Kaan Kılıç, "Türk Hava Sanayinin Gelişiminde Polonyalıların Etkisi", https://savasarastirmalari.

com/turk-hava-sanayinin-gelisiminde-polonyanin-etkisi/, erişim 21.05.2022.

"War in Ukraine", www.internetkaynak.com, erişim 10.05.2022.

9.5. Tezlere yapılan atıflarda, yayımlanmamış tezlerin başlıkları için italik kullanılmayacaktır. Yazar adı ve soyadı, tezin adı, tezin derecesi, tezin yapıldığı kurum ve enstitü, yapıldığı yer ve tarih, sayfa numarası aşağıdaki şekilde verilecektir.

Barış Ateş, Soğuk Savaş Sonrası Dönemde Askeri Değişim: NATO Orduları ve Türk Silahlı Kuvvetleri Üzerine Karşılaştırmalı Bir Analiz, *Doktora Tezi*, Gazi Üniversitesi, Ankara, 2014, s. 84.

10. Ekler yazının sonunda verilmeli ve altında belgenin içeriği ve kaynağına dair kısa bilgi yer almalıdır. Tablo, Grafik ve şekiller, Ekler kısmında verilebileceği gibi metin içerisine de yerleştirilebilir. Metin içerisinde verilmeleri durumunda tablo ve şekiller kendi içinde sıralanarak numaralandırılmalı (Tablo: 1, Şekil: 2 gibi) ve gerek bu numara gerekse tablo veya şeklin içeriğine dair tanıtıcı başlık tablo ve şeklin üst orta kısmında verilmelidir. Tablo, şekil, grafik ve resim için alıntı yapılmış ise mutlaka kaynak belirtilmelidir.

11. Aday makale metinlerinin sonlarında, alfabetik sıraya göre tasniflenmiş kaynakça yer almalıdır. İnternet kaynakları kaynakçanın sonuna eklenmelidir. Kaynakça düzenlenirken yazarın önce soyadı (BÜYÜK HARFLERLE) ve ardından adı yazıldıktan sonra, metin içindeki dipnotlarda yer alan bilgiler aynen aktarılmalıdır.

KAYNAKÇA ÖRNEĞİ

Metin dosyasında "Kaynakça" başlığı altında eserler Arşiv Kaynakları, Basılı Eserler ve İnternet Kaynakları olmak üzere 3 alt başlığa ayrılmalıdır.

KAYNAKÇA

Arşiv Kaynakları (Varsa)

İlgili arşivin kendi atıf kuralları dikkate alınmalıdır.

Kitap

YILDIZ Gültekin (2021). *Osmanlı Devleti'nde Askeri İstihbarat*, Yeditepe Yayınları, İstanbul.

SCHELLING Thomas C. (2008). *Arms and Influence*, Yale University Press, Revised edition, New Haven.

YILDIZ Gültekin (ed.) (2017). *Osmanlı Askeri Tarihi: Kara, Deniz ve Hava Kuvvetleri 1792 – 1918*, Timaş Yayınları, İstanbul.

MEARSHEIMER John J. ve WALT Stephen M. (2008). *The Israel Lobby and U.S. Foreign Policy*, FSG Adult, New York.

SCHMITT Carl (2018). *Kara ve Deniz* (Çev. Gültekin Yıldız), Vakıfbank Kültür Yayınları, İstanbul.

Kitap Bölümü

İNALCIK Halil (2002). "Barbaros'tan İnebahtı (Leponto)'ya Akdeniz", Bülent Arı (ed.), *Türk Denizcilik Tarihi*, T.C. Başbakanlık Denizcilik Müsteşarlığı Yayınları, Ankara, 141-154.

BALZACQ Thierry ve DOMBROWSKI Peter J. (2019). "Introduction Comparing Grand Strategies in the Modern World", Thierry Balzacq, Peter J Dombrowski ve Simon Reich (eds.), *Comparative Grand Strategy: A Framework and Cases*, Oxford University Press, Oxford, 2019. 1-21.

Makale

GRISSOM Adam (2006). "The Future of Military Innovation Studies", *Journal of Strategic Studies*, 29:5, 905-934.

ARQUILLA John ve FREDRICKSEN Hal (1995). "Graphing' an Optimal Grand Strategy", *Military Operations Research*, 1:3, 3-17.

KALELİOĞLU Uğur Berk (2022). "Alman Askeri Sosyolojisi: Gelişim, Kurumsallaşma ve Sınırlılıklar", *Güvenlik Stratejileri Dergisi*, 18:41, 201-224.

Tez

ATEŞ Barış (2014). Soğuk Savaş Sonrası Dönemde Askeri Değişim: NATO Orduları ve Türk Silahlı Kuvvetleri Üzerine Karşılaştırmalı Bir Analiz, *Doktora Tezi*, Gazi Üniversitesi, Ankara.

KİBAROĞLU Mustafa (1996). The Nuclear Non-Proliferation Regime at The Crossroads: Strengthening or Uncertainty, *Doktora Tezi*, Bilkent Üniversitesi, Ankara.

İnternet

KENNAN George F. (1947). "The Sources of Soviet Conduct", *Foreign Affairs Magazine*, https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct, erişim 21.10.2023.

CHARAP Samuel ve PRIEBE Miranda. "Avoiding a Long War: U.S. Policy and the Trajectory of the Russia-Ukraine Conflict", *RAND Report*, Ocak 2023, https://www.rand.org/content/dam/rand/pubs/perspectives/PEA2500/PEA2510-1/RAND_PEA2510-1.pdf, erişim 21.10.2023.

KILIÇ Kaan. "Türk Hava Sanayinin Gelişiminde Polonyalıların Etkisi", https://savasarastirmalari.com/turk-hava-sanayinin-gelisiminde-polonyanin-etkisi/, erişim 21.05.2022.

"War in Ukraine", www.internetkaynak.com, erişim 10.05.2022.

SUBMISSION GUIDELINES

Articles submitted to the *Güvenlik Stratejileri Dergisi* shall not be previously published and shall be authentic in a way that it will contribute to literature of the relevant field. Articles, which are descriptive, expect for the stated parameters in the "Publication Ethics and Evaluation Process" or which are repetitive in their field, will not be taken into evaluation. Articles based on presentations submitted in scientific meetings may be accepted for evaluation, provided that they have not been published in the proceedings of the meetings and that the authors inform the editors so.

The ethical principles and publication policy of the Güvenlik Stratejileri Dergisi have been prepared in accordance with the guidelines and policies published by the Committee on Publication Ethics (COPE). Detailed information on publication principles, relations with authors and relations with referees can be found under the relevant sections on the website of our journal.

If the articles submitted via https://dergipark.org.tr/en/pub/guvenlikstrtj comply with the formatting principles presented below and is found to eligible in terms of subject/field, they are assigned to (at least two) referees who are experts in the field for review and evaluation. The authors may re-submit their articles, which are rejected by the Publication Committee, after they revise their work in accordance with the reports of reviewers. If the article is considered to be ill-revised, it is rejected and the process is over. If the article is considered to be revised properly, it is taken as a newly submitted article into the reviewing process. The reports of the referees are of advisory nature and the decision to publish is taken by the Editorial Board.

Authors, who send articles in a foreign language to the Journal, are obliged to get their work proof-read by a native speaker academic who is considered as an expert on their field and to provide an evidence of this proof-reading.

Opinions expressed in the articles published in the Journal are the personal scientific evaluations of the authors and are not, in any way, the institutional views or opinions of their own organizations/institutes or of the Atatürk Strategic Studies and Graduate Institute or the Turkish National Defence University.

The authors whose articles have been published in the Güvenlik Stratejileri Dergisi are considered as natural peer-reviewers of the Journal and they are obliged to perform a peer-review at least once upon the request of the Editors.

Formatting Principles for Articles

1. The publication language of JGüvenlik Stratejileri Dergisi is Turkish. However, articles written in English, German, and French may also be published. The texts submitted shall be clear and understandable and be in line with scientific criteria in terms of language and expression.

2. The article submitted shall have minimum of 6000 words and maximum of 10,000 words including abstract, summary, bibliography, and footnotes. The articles which are below the minimum or above the maximum counts of words are returned to the authors without being evaluated.

3. The articles shall be submitted with the abstract no longer than 200 words and five keywords. The abstract shall include purpose, method, hypothesis/question, and findings of the article and present the conclusion reached in the article shortly. While writing the abstract, the author shall comply to the rule of "one short and two long sentences". (In the articles written in German or French, abstracts and keywords in Turkish and English shall be added, as well as the abstract and keywords in the original language of the article.) The article shall also have a summary 750-1000 words at the end of the text. The summary shall include the points and arguments, which are considered to emphasize and the general outline of the article, in addition to the points pointed out in the abstract. In the articles written in Turkish, the aforementioned extensive summary shall be in English. For articles written in English, extensive summary shall be written in Turkish. The articles written in German or France, the extensive summary shall be written in both English and Turkish.

4. Articles submitted to the JGüvenlik Stratejileri Dergisi shall be written using the program Microsoft Word in 11 font size in the text and 9 font size in the footnotes. Paragraph properties of the text shall be aligned and line spacing of 1.5 line and paragraph properties of the footnotes shall be aligned and line spacing of 1 line. The page numbers shall be at the bottom of the page.
5. Name of the author shall be placed under the title of the article; their title, place of duty and e-mail address shall be indicated in the footnote with (*) in 9 font size. Footnotes for other explanations shall be provided in numbers at the bottom of the page. The article shall have two-level subheadings and these subheadings shall written bold and numbered (except for introduction and conclusion).
6. Citations in the text shall be shown with double quotes ("...") and citations with more than three lines shall be written as a new paragraph as a inward, singled spaced and aligned paragraph. Citations within citations shall be shown with a single quote ('...'). The words to be emphasized within the text shall not be written in bold or underlined but shall be written with double quotes ("...").
7. The citations shall be made according to guidelines presented below. Articles, which do not comply with these guidelines, will be rejected directly.
8. Multiple references for the same publication shall be made by fully complying the guidelines below in the first reference and then by using the surname and the shortened name of the study. For multiple references in subsequent footnotes, the phrase "ibid" shall be used.
9. The citations in the shall be written as follows:
9.1. Books: name and surname of the author, name of the book, (volume number, if any), (translator, if any), publishing house, place of publication, date of publication, and page number shall be given in order in accordance with the following examples.

1 Morris Janowitz, *The Professional Soldier: A Social and Political Portrait*, Free Press, New York, 1964, p. 210.
2 John J. Mearsheimer and Stephen M. Walt, *The Israel Lobby and U.S. Foreign Policy*, FSG Adult, 1st edition, New York, 2008, p. 92.
3 Mustafa Aydın, Mitat Çelikpala et al., U*luslararası İlişkilerde Çatışmadan Güvenliğe*, Bilgi Üniversitesi Yayınları, İstanbul, 2015, p. 79.
4 Janowitz, *The Professional Soldier*, p. 155.
5 Ibid, p. 156.

9.2. Articles: name and surname of the author, "name of the article" (translator, if any), name of the periodical, date of publication, number and volume, page number of the reference shall be given in order in accordance with the following examples. For the reference to the encyclopedia articles, same rules apply.

Adam Grissom, "The Future of Military Innovation Studies", *Journal of Strategic Studies*, 29:5, 2006, p. 910.
Özlem Durgun and Mustafa Caner Timur, "Savunma Harcamaları ve Ekonomik Büyüme İlişkisi: Türkiye Analizi", *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, 54, 2017, p. 119.
Lütfi Sürücü, Fehiman Eminer and Murat Sağbaş, "The Relationship of Defense Expenditures and Economic Growth Examples of Turkey and China (2000-2020)", J*ournal of Security Strategies*, 18:41, 2022, p. 175.

In the articles with four or more authors, the names are abbreviated after the first author, as "Gültekin Yıldız et al.".
9.3. Chapters/articles in edited books and proceedings books:

Engin Avcı, "Ceza Adalet Sistemi Çerçevesinde Şiddet İçeren Radikalleşmeyle Mücadele: Terörist Rehabilitasyonu ve Yeniden Topluma Kazandırma", Gökhan Sarı & Cenker Korhan Demir (eds.), *Uluslararası Güvenlik Kongresi, Kuram, Yöntem, Uygulama*, Jandarma ve Sahil Güvenlik Akademisi Yayınları, Ankara, 2019, s. 433.

9.4. Online articles:

George F. Kennan, "The Sources of Soviet Conduct", *Foreign Affairs Magazine*, July 1947, https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct, accessed 21.11.2019.

Kaan Kılıç, "Türk Hava Sanayinin Gelişiminde Polonyalıların Etkisi", https://savasarastirmalari.com/turk-hava-sanayinin-gelisiminde-polonyanin-etkisi/, accessed 21.05.2022.

"War in Ukraine", www.internetkaynak.com, accessed 10.05.2022.

9.5. Theses/dissertations: no italics shall be used for the titles of the unpublished theses/dissertations. Name and surname of the author, title of the thesis/dissertation, degree of the thesis/dissertation, institution or institute to which it was submitted, place and date, page number shall be given in accordance with the following example.

Tolga Öz, Reverse Logistics and Applications in the Defense Industry, *Unpublished Master's Thesis*, Dokuz Eylül Üniversity, İzmir, Turkey, 2007, p.60.

10. Attachments shall be presented at the end of the text and brief information as to the content and source of the document shall be presented at the bottom of it. Tables and figures (including graphics) may be presented within the text of the article as well as in the attachments. If they are to be presented within the text of article, tables, figures, and graphics shall be numbered in their own order (such as Table 1, Figure 2, etc). The number of the table or figure and the introductory title regarding the content of it shall be given at the bottom of the table or figure centered. If citations are made for tables, figures, graphics and pictures, the sources of the citations shall be given with a footnote.

11. Resources shall be sorted alphabetically in a bibliography at the end of the article. Internet sources shall be added at the end of the bibliography. The entries of the bibliography shall be written by putting the surname of the author first (IN CAPITAL LETTERS) and then name of the author; then all the other information of the sources shall be included as done in the references.

REFERENCES SAMPLE:

REFERENCES

Archival Sources (If available)

The referencing rules of the relevant archive should be taken into account.

Published Works

Book

YILDIZ Gültekin (2021). *Osmanlı Devleti'nde Askeri İstihbarat*, Yeditepe Yayınları, Istanbul.

SCHELLING Thomas C. (2008). *Arms and Influence*, Yale University Press, Revised edition, New Haven.

YILDIZ Gültekin (ed.) (2017). *Osmanlı Askeri Tarihi: Kara, Deniz ve Hava Kuvvetleri 1792 – 1918*, Timaş Yayınları, Istanbul.

MEARSHEIMER John J. and WALT Stephen M. (2008). *The Israel Lobby and U.S. Foreign Policy*, FSG Adult, New York.

SCHMITT Carl (2018). *Kara ve Deniz*, (trans. Gültekin Yıldız), Vakıfbank Kültür Yayınları, İstanbul.

Book Chapter

İNALCIK Halil (2002). "Barbaros'tan İnebahtı (Leponto)'ya Akdeniz", Bülent Arı (ed.), *Türk Denizcilik Tarihi*, T.C. Başbakanlık Denizcilik Müsteşarlığı Yayınları, Ankara, 141-154.

BALZACQ Thierry and DOMBROWSKI Peter J. (2019). "Introduction Comparing Grand Strategies in the Modern World", Thierry Balzacq, Peter J Dombrowski ve Simon Reich (eds.), *Comparative Grand Strategy: A Framework and Cases*, Oxford University Press, Oxford, 2019. 1-21.

Article

GRISSOM Adam (2006). "The Future of Military Innovation Studies", *Journal of Strategic Studies*, 29:5, 905-934.

ARQUILLA John ve FREDRICKSEN Hal (1995). "Graphing' an Optimal Grand Strategy", *Military Operations Research*, 1:3, 3-17.

KALELİOĞLU Uğur Berk (2022). "Alman Askeri Sosyolojisi: Gelişim, Kurumsallaşma ve Sınırlılıklar", *Güvenlik Stratejileri Dergisi*, 18:41, 201-224.

Doctoral Dissertation/Master's Thesis

ATEŞ Barış (2014). Soğuk Savaş Sonrası Dönemde Askeri Değişim: NATO Orduları ve Türk Silahlı Kuvvetleri Üzerine Karşılaştırmalı Bir Analiz, *Doctoral Dissertation*, Gazi Üniversitesi, Ankara.

KİBAROĞLU Mustafa (1996). The Nuclear Non-Proliferation Regime at The Crossroads: Strengthening or Uncertainty, *Doctoral Dissertation*, Bilkent Üniversitesi, Ankara.

Web Page

KENNAN George F. (1947). "The Sources of Soviet Conduct", Foreign Affairs Magazine, https://www.foreignaffairs.com/articles/russian-federation/1947-07-01/sources-soviet-conduct, erişim 21.10.2023.

CHARAP Samuel ve PRIEBE Miranda. "Avoiding a Long War: U.S. Policy and the Trajectory of the Russia-Ukraine Conflict", RAND Report, Ocak 2023, https://www.rand.org/ content/dam/rand/pubs/perspectives/PEA2500/PEA2510-1/RAND_PEA2510-1.pdf, erişim 21.10.2023.

KILIÇ Kaan. "Türk Hava Sanayinin Gelişiminde Polonyalıların Etkisi", https://savasarastirmalari.com/turk-hava-sanayinin-gelisiminde-polonyanin-etkisi/, erişim 21.05.2022.

"War in Ukraine", www.internetkaynak.com, erişim 10.05.2022.