Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü

Güvenlik Bilimleri Dergisi

Gendarmerie and Coast Guard Academy
Security Sciences Institute

Journal of Security Sciences

Cilt/Volume: 12
Sayı/Issue: 1
Yıl/Year: 2023
Mayıs/May

ISSN: 2147–2912
E-ISSN: 2147–5075
www.jsga.edu.tr

Ankara 2023

Güvenlik Bilimleri Dergisi

The Journal of Security Sciences

GÜVENLİK BİLİMLERİ DERGİSİ

Cilt 12* Sayı 1* Yıl 2023* ISSN 2147-2912 / E-ISSN 2147-5075

BASKI

Jandarma Basımevi Müdürlüğü/ANKARA

YAZIŞMA VE HABERLEŞME ADRESİ

Jandarma ve Sahil Güvenlik Akademisi Beytepe / ANKARA
Telefon:0312 464 74 74 Dâhili: 7600 / 7635
Web: http://www.jsga.edu.tr/gbd
E-posta: editorgbd@jandarma.gov.tr

THE JOURNAL OF SECURITY SCIENCES

Volume 12* Issue 1* Year 2023* ISSN 2147-2912 / E-ISSN 2147-5075

PRINTED BY

Gendarmerie Printing House Directorate /ANKARA

CORRESPONDENCE AND COMMUNICATION

Gendarmerie and Coast Guard Academy Beytepe / ANKARA
Telephone: +90 312 464 74 74 ext: 7600/7635
Web: http://www.jsga.edu.tr/gbd
E-mail: editorgbd@jandarma.gov.tr

Bu Sayının Hakemleri

Prof. Dr. Mustafa ALKAN *Akdeniz Üniversitesi*	Dr. Öğr. Üyesi Yusuf DÜNDAR *Aksaray Üniversitesi*
Prof. Dr. Orhan ATAKOL *Ankara Üniversitesi*	Dr. Öğr. Üyesi İskender KARAKAYA *Yozgat Bozok Üniversitesi*
Prof. Dr. Hamza ATEŞ *İstanbul Medeniyet Üniversitesi*	Dr. Öğr. Üyesi Hüseyin NERGİZ *Hacettepe Üniversitesi*
Doç. Dr. Hasan ACAR *Jandarma Genel Komutanlığı*	Dr. Öğr. Üyesi Gülçin ORHAN *Jandarma ve Sahil Güvenlik Akademisi*
Doç. Dr. Naci AKDEMİR *Jandarma ve Sahil Güvenlik Akademisi*	Dr. Öğr. Üyesi Sadullah ÖZEL *Batman Üniversitesi*
Doç. Dr. Recep BENZER *Başkent Üniversitesi*	Dr. Öğr. Üyesi Fatih UYSAL *Kafkas Üniversitesi*
Doç. Dr. Taner BORA *Polis Akademisi*	Dr. Tarık AK *Jandarma ve Sahil Güvenlik Akademisi*
Doç. Dr. Zühal KARAKOÇ DORA *Türkiye Büyük Millet Meclisi*	Dr. Begüm ÇARDAK *Jandarma ve Sahil Güvenlik Akademisi*
Doç. Dr. Mehmet GÜMÜŞTAŞ *Ankara Üniversitesi*	Dr. Fatih DEDEMEN *Jandarma Genel Komutanlığı*
Doç.Dr. Çisel Ekiz GÖKMEN *Muğla Sıtkı Koçman Üniversitesi*	Dr. Mesut GUVEN *Jandarma ve Sahil Güvenlik Akademisi*
Doç. Dr. Serkan YENAL *Milli Savunma Üniversitesi*	Dr. Cengiz ÖZEL *Jandarma ve Sahil Güvenlik Akademisi*
Dr. Öğr. Üyesi Alev AKTAŞ *Sivas Cumhuriyet Üniversitesi*	Dr. Bülent SUNGUR *Jandarma ve Sahil Güvenlik Akademisi*
Dr. Öğr. Üyesi Hüseyin ARAS *Nevşehir Hacı Bektaş Veli Üniversitesi*	

Referees of this Issue

Prof. Mustafa ALKAN, Ph.D. *Akdeniz University*	Assist. Prof.Yusuf DÜNDAR, Ph.D. *Aksaray University*
Prof. Orhan ATAKOL, Ph.D. *Ankara University*	Assist. Prof.İskender KARAKAYA, Ph.D. *Yozgat Bozok University*
Prof. Hamza ATEŞ, Ph.D. *İstanbul Medeniyet University*	Assist. Prof.Hüseyin NERGİZ, Ph.D. *Hacettepe University*
Assoc. Prof. Hasan ACAR, Ph.D. *Gendarmerie General Command*	Assist. Prof.Gülçin ORHAN, Ph.D. *Gendarmerie and Coast Guard Academy*
Assoc. Prof. Naci AKDEMİR, Ph.D. *Gendarmerie and Coast Guard Academy*	Assist. Prof.Sadullah ÖZEL, Ph.D. *Batman University*
Assoc. Prof. Recep BENZER, Ph.D. *Baskent University*	Assist. Prof. Fatih UYSAL, Ph.D. *Kafkas University*
Assoc. Prof. Taner BORA, Ph.D. *Police Academy*	Tarık AK, Ph.D. *Gendarmerie and Coast Guard Academy*
Assoc. Prof. Zühal KARAKOÇ DORA, Ph.D. *Grand National Assembly of Turkey*	Begüm ÇARDAK, Ph.D. *Gendarmerie and Coast Guard Academy*
Assoc. Prof. Mehmet GÜMÜŞTAŞ, Ph.D. *Ankara University*	Fatih DEDEMEN, Ph.D. *Gendarmerie General Command*
Assoc. Prof. Çisel Ekiz GÖKMEN, Ph.D. *Mugla Sitki Kocman University*	Mesut GUVEN, Ph.D. *Gendarmerie and Coast Guard Academy*
Assoc. Prof. Serkan YENAL, Ph.D. *National Defense University*	Cengiz ÖZEL, Ph.D. *Gendarmerie and Coast Guard Academy*
Assist. Prof.Alev AKTAŞ, Ph.D. *Sivas Cumhuriyet University*	Bülent SUNGUR, Ph.D. *Gendarmerie and Coast Guard Academy*
Assist. Prof.Hüseyin ARAS, Ph.D. *Nevsehir Haci Bektas Veli University*	

İÇİNDEKİLER

CONTENTS

EDİTÖR'DEN

Değerli "Güvenlik Bilimleri Dergisi" okuyucularımız,

Güvenlik Bilimleri Dergimizin Mayıs sayısını asrın felaketi olarak nitelenen ve 11 ilimizi etkisi altına alan deprem felaketinin acılarını en derinden hissettiğimiz, depremzedelerimizin yaralarını sarmak için devletimizin tüm unsurları ve milletimizin her bir ferdinin büyük fedakârlıklar göstererek cansiparane çalışmaya devam ettiği bir dönemde çıkarıyoruz. Güvenlik Bilimleri Dergisi olarak deprem felaketinde hayatını kaybeden vatandaşlarımıza Allah'tan rahmet, yaralılarımıza acil şifalar diliyoruz.

Asya kıtası eski çağlardan itibaren dünyanın önemli güç merkezlerinden biri olmuştur. Hindistan jeopolitik konumu, yeraltı zenginlikleri, mimarisi, kültürü ve gelenekleri ile bu kadim kıtada güç dengelerinin sağlanmasında her zaman önemli bir aktör olmuştur. Günümüzde de teknolojisi ve hızla büyüyen ekonomisi ile Asya kıtasındaki etkin güç unsurlarından biri olmaya devam etmektedir. **ARAS** ve **KANDEMİR** makalelerinde, Hindistan'ın bağlantısızlık politikasını devam ettirdiği günümüzde uygulamaya başladığı yerlileşme hareketinin yanı sıra askerî ve stratejik iş birlikleriyle şekillenen yeni savaş doktrininin doğuracağı riskleri ve fırsatları incelemektedir. Hindistan'ın uygulamış olduğu Ortodoks saldırı doktrininin incelenmesi ile başlayan makalede 21. yüzyılda Hindistan'ın uyguladığı askerî politikaların başarısız olmasının nedenleri analiz edildikten sonra yeni dönemde uygulanacak askerî doktrinin esasları incelenmiştir.

Yapay Zekâ (YZ) araştırmalarının kökleri 1950'li yıllara dayanmakla birlikte çalışmalar günümüzde yeni bir ivme kazanmıştır. Tıp, bilimsel araştırmalar, yazılım, eğlence ve sanat gibi farklı alanlarda uygulama imkânı olan Yapay Zekâ araçlarının 2023 yılındaki gelişimi bilim insanları ve bu alanda faaliyet gösteren aktörleri Yapay Zekânın gelecekte insanlık için oluşturabileceği tehditleri ve riskleri daha yakından incelemeye davet etmesine yol açacak bir boyuta erişmiştir. Yapay Zekâ kaynaklı risklere yönelik etik tartışmalar devam ederken ticari firmaların yanı sıra devletler de Yapay Zekâ araştırmalarına yönelik AR-GE yatırımlarını arttırmaktadır. **KÜÇÜKSOLAK** ve **FIRAT** İngilizce olarak kaleme aldıkları makalelerinde Çin ve Rusya'nın yürüttüğü Yapay Zekâ

çalışmalarının iki devletin ilişkileri üzerindeki etkilerini güç siyaseti çerçevesinde incelemektedir. Yazarlar, Rusya ve Çin'in Yapay Zekâ politikalarını analiz ettikleri makalelerinde Çin'in daha sistematik ve kapsamlı bir Yapay Zekâ stratejisi uygulamasına karşın Rusya'nın daha çok Yapay Zekânın askerî uygulamaları üzerine yoğunlaştığına ve bu yarışta Çin'in gerisinde kaldığına vurgu yaparak bu strateji farklılıklarının olası politik sonuçlarını tartışmaktadır.

Avrupa Birliği (AB), Soğuk Savaş sırasında Amerika Birleşik Devletleri (ABD) ve NATO ile olan ilişkilerine odaklanmak durumunda kaldığı için uzun süredir arzu ettiği bağımsız bir güvenlik ve savunma politikası geliştirmeye ağırlık verememiştir. Ancak günümüzün değişen politik konjoktüründe AB bu alandaki faaliyetlerine ağırlık vermektedir. Bu kapsamda Avrupa Birliği tarafından Mart 2021'de duyurulan Stratejik Pusula; Avrupa Birliği'nin güvenlik ve savunmaya yönelik stratejik önceliklerini özetleyen, önümüzdeki on yılda AB'nin güvenlik ve savunma politikasına rehberlik etmesi amaçlanan bir belgedir. Belge; dayanıklılık, caydırıcılık, savunma ve ortaklıklar olmak üzere dört temel odak alanını tanımlamaktadır. Belge; AB'nin siber saldırılar, dezenformasyon kampanyaları ve hibrit savaş dâhil olmak üzere çok çeşitli tehditlere yanıt verebilmesi gerektiğini vurgulamaktadır. **AKŞEMSETTİNOĞLU** tarafında hazırlanan makale böyle bir politikanın uygulanabilirliğini araştırmayı amaçlamaktadır. Doküman ve metin analizi yöntemini kullanan çalışma, bu yeni anlayışın AB'nin transatlantik ortaklarıyla iş birliği içinde bağımsız bir güvenlik ve savunma politikası geliştirme hedefini ilerletebileceğini ancak bunun ABD ve NATO'ya karşı çıkmaktansa iş birliği yapmakla sağlanabileceği sonucuna varmaktadır.

İnsanlar alışveriş, bankacılık ve sosyalleşme gibi günlük faaliyetler için teknolojiye giderek daha fazla güvenirken artan siber saldırı tehditleri önemli bir endişe hâline gelmektedir. İşletmeler yeni teknolojilere uyum sağladıkça siber ortamda siber suç riski de dâhil olmak üzere yeni tehlikelerle karşı karşıya kalmaktadır. **EROĞLU** tarafından yapılan ampirik çalışma, Siber Güvenlik İhlalleri Anketi 2021'den elde edilen verileri kullanarak işletmeleri siber suçlara karşı savunmasız kılan faktörleri araştırmaktadır. Siber güvenlik ve siber risk konusunda Türkiye'de işletmeler ve siber suçlar üzerine çok az araştırma yapılmış olması bu araştırmayı özellikle önemli kılmaktadır. Çalışma; işletme

büyüklüğü, insan faktörleri, dijital görünürlük, siber güvenlik önlemleri, siber farkındalık ve siber suç eğitimi ile siber suç mağduriyeti arasındaki ilişkiyi incelemektedir. Sonuçlar, orta ve büyük ölçekli işletmelerin siber suçlara karşı daha savunmasız olduğunu ve oltalama saldırılarının en yaygın saldırı türü olduğunu göstermektedir. Çalışma aynı zamanda insan faktörünün oltalama suçu riskini ve siber ortamda daha fazla görünürlüğün mağduriyet olasılığını artırdığını ortaya koymaktadır.

Trafik güvenliğini artırmaya ve kazaları azaltmaya yönelik birçok çabaya rağmen, trafik olaylarının sayısı endişe verici derecede yüksek olmaya devam etmektedir. Örneğin Türkiye İstatistik Kurumuna göre 2020 yılında Türkiye'de 1.154.441 trafik kazası yaşanmıştır. Bu kazalarda 4.131 ölüm ve 268.613 yaralanma meydana gelmiştir. Kazaların en yaygın nedeni sürücü hatası veya ihmali (%87,9) olarak kayıtlara geçmiştir. COVID-19 salgını ve buna bağlı seyahat ve hareketlilik kısıtlamaları nedeniyle kaza sayısı bir önceki yıla göre %27,5 azalmasına rağmen, trafik kazaları Türkiye'de önemli bir halk sağlığı sorunu olmaya devam etmektedir. Sürücülerin riskleri nasıl algıladığını ve bunlara nasıl tepkiler verdiğini anlamak, trafik güvenliğini iyileştirmek için çok önemlidir. Risk algısı, sürücülerin değerlendirmelerini ve dolayısıyla sürüş davranışlarını etkileyen önemli bir faktördür. **ÇORAK** tarafından yürütülen çalışma, sürücülerin riskleri nasıl algıladıklarını, algılarını hangi faktörlerin etkilediğini ve risk algısına dayalı olarak davranışlarını nasıl düzenlediklerini incelemektedir. Çalışmada Risk Dengeleme Teorisi teorik çerçeve olarak kullanılmıştır. Çalışma; sürücülerin risk algılarının sürüş sırasındaki değerlendirmeleri ve davranışları üzerindeki etkilerini açıklamayı, trafik ve ulaşım psikolojisindeki alternatif çalışma alanlarına ışık tutmayı amaçlamaktadır. Risk algısı ve sürüş davranışı arasındaki karmaşık etkileşime ışık tutan bu araştırma, trafik güvenliğini iyileştirme ve kazaları azaltma çabalarına katkıda bulunacaktır.

Prof.Dr. İsmail Hakkı DEMİRCİOĞLU
Başeditör

EDITOR'S NOTE

Dear Journal of Security Sciences Readers,

We are publishing the May issue of the Journal of Security Sciences at a time when we feel the deep pain of the earthquake disaster, which is described as the disaster of the century and has affected our 11 provinces, and when all the elements of our state and every member of our nation continue to work diligently by showing great sacrifices to heal the wounds of our earthquake victims. As the Journal of Security Sciences, we wish mercy from Allah to our citizens who lost their lives in the earthquake disaster and urgent healing to those wounded.

The Asian continent has been one of the world's most important power centers since ancient times. With its geopolitical position, underground riches, architecture, culture and traditions, India has always been an important actor in maintaining the balance of power in this ancient continent. Today, with its technology and rapidly growing economy, it continues to be one of the influential power players in Asia. In their article, **ARAS and KANDEMİR** examine the risks and opportunities arising from India's new war doctrine, which is shaped by military and strategic cooperation, as well as the domestic production movement that India has initiated to implement today as it continues its non-aligned policy. Beginning with an examination of India's orthodox offensive doctrine, the article analyzes the reasons for the failure of India's military policies in the 21st century and then examines the principles of the military doctrine to be implemented in the new era.

Although the roots of Artificial Intelligence (AI) research date back to the 1950s, studies have gained a new momentum today. The development of Artificial Intelligence tools in 2023, which have application possibilities in different fields such as medicine, scientific research, software, entertainment and art, has reached a dimension that leads scientists and actors operating in this field to examine more closely the threats and risks that Artificial Intelligence may pose

to humanity in the future. While ethical debates on the risks arising from Artificial Intelligence continue, commercial companies, as well as governments, are increasing their R&D investments in Artificial Intelligence field. In their article written in English, **KÜÇÜKSOLAK and FIRAT** analyze the effects of Artificial Intelligence studies carried out by China and Russia on the relations of the two states within the framework of power politics. In their article examining the Artificial Intelligence policies of Russia and China, the authors discuss the possible political implications of these strategy differences, emphasizing that while China has implemented a more systematic and comprehensive Artificial Intelligence strategy, Russia has focused more on the military applications of Artificial Intelligence and has lagged behind China in this race.

The European Union (EU) was unable to focus on developing an independent security and defence policy, which it has long desired, as it had to focus on its relations with the United States of America (USA) and NATO during the Cold War. However, in today's changing political conjuncture, the EU focuses on its activities in this area. Within the context, the Strategic Compass announced by the European Union in March 2021 is a document outlining the European Union's strategic priorities for security and defence, intended to guide the EU's security and defence policy over the next decade. The document defines four key focus areas: resilience, deterrence, defence and partnerships. The document stresses the need for the EU’s response to threats, including cyber-attacks, disinformation campaigns and hybrid warfare. The article by **AKŞEMSETTİNOĞLU** aims to explore the feasibility of such a policy. Using document and textual analysis, the paper concludes that this new approach could advance the EU's goal of developing an independent security and defence policy in cooperation with its transatlantic partners, but only by cooperating rather than opposing the US and NATO.

As people increasingly rely on technology for everyday activities such as shopping, banking and socializing, the growing threat of cyberattacks is

becoming a major concern. As businesses adapt to new technologies, they face new threats in cyberspace, including the risk of cybercrime. The empirical study by **EROĞLU** investigates the factors that make businesses vulnerable to cybercrime using data from the Cyber Security Breaches Survey 2021. This research is particularly important as there is very little research on cybersecurity and cyber risk in Turkish literature on businesses and cybercrime. The study examines the relationship between business size, human factors, digital visibility, cybersecurity measures, cyber awareness and cybercrime education and cybercrime victimization. The results show that medium and large enterprises are more vulnerable to cybercrime, with phishing attacks being the most common type of attack. The study also reveals that the human factor increases the risk of phishing crime, and greater visibility in cyberspace increases the likelihood of victimization.

Despite numerous efforts to improve traffic safety and reduce accidents, the number of traffic incidents remains alarmingly high. For example, according to the Turkish Statistical Institute, there were 1,154,441 traffic accidents in Turkey in 2020. These accidents resulted in 4,131 deaths and 268,613 injuries. The most common cause of accidents was recorded as driver error or negligence (87.9%). Although the number of accidents decreased by 27.5% compared to the previous year due to the COVID-19 pandemic and related travel and mobility restrictions, traffic accidents continue to be a major public health problem in Turkey. Understanding how drivers perceive and react to risks is crucial for improving traffic safety. Risk perception is an important factor influencing drivers' assessments and, therefore, their driving behavior. The study conducted by **ÇORAK** examines how drivers perceive risks, which factors affect their perceptions and how they regulate their behavior based on risk perception. Risk Compensation Theory is used as the theoretical framework in the study. The study aims to explain the effects of drivers' risk perceptions on their evaluations and behaviors while driving and to shed light on alternative areas of study in traffic and transportation psychology. By shedding light on the complex

interaction between risk perception and driving behavior, this research will contribute to efforts to improve traffic safety and reduce accidents.

Prof İsmail Hakkı DEMİRCİOĞLU, Ph. D.
Editör in Chief

Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2023,Cilt:12, Sayı:1, 1-24
doi:10.28956/gbd.1196748

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2023,Volume:12, Issue:1, 1-24
doi:10.28956/gbd.1196748

Makale Türü ve Başlığı / Article Type and Title
Araştırma/ Research Article
Hindistan'ın Savaş Doktrini: Riskleri ve Fırsatları Yeniden Değerlendirmek
India's War Doctrine: Reassessing Risks and Opportunities

Yazar(lar) / Writer(s)
Ferhat Çağrı ARAS, Doktor Öğretim Görevlisi, Karadeniz Teknik Üniversitesi, İİBF, Uluslararası İlişkiler Bölümü, ferhatcagriaras@ktu.edu.tr, ORCID: https://orcid.org/0000-0003-2108-1981
Ekber KANDEMİR, Dr, Serbest Araştırmacı, ekberkndmyr@gmail.com ORCID: https://orcid.org/0000-0001-6211-2276

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :31.10.2022
Makale Kabul Tarihi / Accepted :25.05.2023

Atıf Bilgisi / Citation:
Aras F.Ç. ve Kandemir E., (2023). Hindistan'ın Savaş Doktrini: Riskleri ve Fırsatları Yeniden Değerlendirmek, *Güvenlik Bilimleri Dergisi, 12(1), ss 1-24. doi:10.28956/ gbd.1196748*

HİNDİSTAN'IN SAVAŞ DOKTRİNİ: RİSKLERİ VE FIRSATLARI YENİDEN DEĞERLENDİRMEK

Öz

Bu makalenin amacı, Hindistan'ın Ortodoks saldırı doktrinin Hindistan'ın stratejik coğrafi konumundaki köklü değişiklikler karşısında bile ordusunu daha verimsiz bir araç hâline getirdiğini ve bu bağlamda son dönemdeki Hint ordusunun inovasyon ve yenileşme hareketlerinin bu doktrin ile neden daha verimsiz olacağı değerlendirmektedir. Hindistan'ın geçmişten gelen bağlantısızlık politikasının daha küresel ölçekte yeni bir boyutunu dış politikada uyguladığı son dönemde Hindistan'ın yeni bir doktrin ile bölgesel ve küresel çıkarlarını ve gücünü daha verimli kullanılabileceğinin tartışıldığı bu makaledeki temel varsayım, Hindistan'ın mevcut askerî doktrininin son dönemdeki askerî ve stratejik iş birlikleri ve yerlileşme hareketleri ile dışa bağımlılığı azaltmayı hedeflediği dış politika izlencelerini verimli kılmayacağı ve yeni bir askerî doktrin ve vizyon geliştirilmesinin ortaya çıkaracağı riskler ve fırsatların yeni bir doktrin çerçevesinde tartışılması gerektiğidir. Bütün bu sınırlamalar ve çıkarımlar ışığında bu makale 3 bölümden oluşmaktadır. İlk bölüm, Hindistan'ın kara kuvvetlerini güvence altına almak üzerine geliştirdiği Ortodoks saldırı doktrini bağlamında Hindistan'ın askerî stratejisinin tarihini inceliyor. İkinci bölümde, 21.yy'da Hindistan'ın güvenlik paradigmalarını altüst eden gelişmeler ve sonrasındaki statik ortamda izlenen askerî politikaların başarısızlığı ve bu başarısızlığın nedenlerini ve sonuçlarını analiz etmektedir. Son bölüm ise, Hindistan'ın askerî gücünün mevcut doktrinde diretilmesi durumunda neden başarısız olacağı ve yeni atılımların verimlilikle sonuçlanabilmesi için oluşturulması gereken yeni modern bir askerî doktrin için bazı analizler ve çıkarımlar üzerine değerlendirmeler yapılmıştır.

Anahtar Kelimeler: *Hindistan, Savaş Doktrini, Saldırı Doktrini, Güvenlik Çalışmaları, Askerî Güvenlik.*

INDIA'S WAR DOCTRINE: REASSESSING RISKS AND OPPORTUNITIES

Abstract

The purpose of this article is to evaluate the fact that India's orthodox offensive doctrine has made its army a more inefficient tool even in the face of radical changes in India's strategic geographical position, and in this context, why the innovation movements of the Indian army in the recent period will be more inefficient with this doctrine. The primary assumption in this article, in which it is discussed that India can use its regional and global interests and power more efficiently with a new doctrine, is the central assumption of India's current military doctrine in the recent period when India has implemented a new dimension of its non-alignment policy on a more global scale in its foreign policy. Strategic cooperation, indigenization movements, and foreign policy programs aiming to reduce foreign dependency will not make the Indian military productive. The risks and opportunities that will arise from developing a new military doctrine and vision should be discussed within the framework of a new doctrine. Considering all these limitations and inferences, this article consists of three parts. The first chapter examines the history of India's military strategy in the context of India's orthodox doctrine of aggression to secure its ground forces. In the second part, the developments that overturned the security paradigms of India in the 21st century and the failure of the military policies followed in the static environment afterwards, and the causes and consequences of this failure are analyzed. In the last part, some analyzes and implications are made for why India's military power will fail if it insists on the current doctrine and for a new modern military doctrine that should be created so that breakthroughs can result in efficiency.

Keywords: *India, war doctrine, offensive doctrine security studies military security*

GİRİŞ

Bağımsızlığından günümüze ekonomisi ve nüfusu istikrarlı bir şekilde büyüyen Hindistan, 1,5 milyara yaklaşan nüfusu ile dünyanın en büyük demokratik ülkelerinden biri konumundadır. Bununla beraber, kalkınmanın sürekliliği ve korunması için bölgesel istikrar seviyesinin korunduğu ve geniş bir uzlaşı kültürüne sahip ülke konumunda olan Hindistan, kuruluşundan beri geleneksel olarak kapsamlı bir defansif savunma politikası izlemektedir. Ancak özellikle son 20 yıldaki askerî ilerlemeler, Pakistan ve Çin ile artan sınır çatışmaları ve kendisine karşı sergilenen muhalif tutumların artışı Hindistan'ın bu savunmacı bakış açısının yanında olası bölgesel bir çatışma ya da savaşı önleme stratejisi benimsemesini de beraberinde getirdi. Bunun yanında Hindistan'ın son dönemdeki kalkınma ve inovasyon programları sonucu ekonomisinin hızla büyümesi ve ülkenin dünyanın geri kalanındaki ekonomik, teknolojik ve politik gelişmelerden giderek daha fazla etkilenmesine ve uluslararası güvenlik ve stratejik iş birliklerindeki değişimlerin sonuçlarından ekonomisinin de olumlu ya da olumsuz anlamda etkilenmesine neden olmuştur. Hindistan'ın ulusal güvenlik stratejilerini şekillendiren bu gibi gelişmeler, küresel bağlamda komşu ülkeler ile ilişkilerinde de çeşitli farklılaşmalara yol açmıştır. Bununla birlikte nükleer silahlanmaların bölgede artması, Hindistan'ın ABD ve Rusya ile ilişkilerindeki çok yönlü ilerlemeler, Orta Asya ve Afganistan'daki istikrarsızlık, küresel terörizm, bölgede Çin ve Pakistan ile artan çatışma ortamı Hindistan'ın da askerî stratejilerinin yeni stratejik doktrinler çerçevesinde son dönemde baştan değerlendirilme gereksinimini de beraberinde getirmektedir.

Tarihsel bağlamda Hindistan'ın askerî stratejisine ülkenin kuzeyindeki tehditleri engellemeyi yöneten kara kuvvetleri hâkimdir. Hindistan'ın hava kuvvetlerindeki gücü, geleneksel olarak bağımsız bir stratejik politika izlemesinden de öte, günümüzde yalnızca ülkenin kara kuvvetlerini destekleyici bir yardımcı araç olarak kullanılmasını mümkün kılmaktadır (C. H. V. Singh, 2022). Hindistan'ın Hint-Pasifik okyanusunda kayda değer bir denizcilik ve nüfuz geçmişine sahip olmasına rağmen günümüze kadar gelinen dönemde önemli bir askerî deniz gücüne yönelik bir stratejisi bulunmamaktadır. Tarihsel bağlamda Hindistan'ın kara kuvvetlerine atfedilen önemin iki önemli nedeni bulunmaktadır. Bunlardan ilki Pakistan ve Çin ile olan sınır muhalefetleri sebebiyle bu iki ülkeye sınır bölgelerde sürekli yaşanan anlaşmazlıkların getirdiği çatışmacı ortam neticesinde yaşanan savaşlar ile ilgilidir. Bunun sonucunda da Hindistan, bağımsızlığından beri askerî kanadını modernleştirme üzerine kurgulamış ve tüm yenileşme çalışmalarını kara

kuvvetlerine ağırlık verecek şekilde gerçekleştirmiştir. Hindistan'ın bugün bile en büyük güvenlik tehditleri Jammu ve Keşmir'in kuzey bölgelerindeki sınır ötesi terörizmden ve Çin ile olan tartışmalı sınırlarındaki periyodik saldırılardan kaynaklanmaktadır. Sınırdaki bu ortamda güvenliğini sağlamak ve herhangi bir sızıntıyı engellemek için Hindistan ordusu askerî bütçeden ve kaynaklardan gün geçtikçe daha büyük oranda pay almaktadır. İkinci büyük önem atfı ise özellikle ülkenin güneydoğusunda kalan bölgelerdeki ayrılıkçı faaliyetler ve radikal grupların varlığı neticesinde artan terör faaliyetlerinin yarattığı tehditlerle alakalıdır (Yadav, 2021). Bu iki temel sebepten ötürü Hindistan'ın hibrit bir kıtasal deniz gücü potansiyeli olmasına rağmen bir zorunluluk olarak ülkenin güvenlik politikalarına kara kuvvetleri daha çok hâkimdir.

Hintli ünlü stratejist Tarapore'nin daha da spesifikleştirerek detaylandırdığı kuramlar bakımından günümüzde Hindistan'ın askerî stratejilerine Ortodoks bir saldırının hâkim olduğu aşikârdır. Düşman topraklarına direk saldırılarla sıcak bir çatışma ortamı yerine mevcut statükoda toprak bütünlüğünü korumaya yönelik caydırıcılığı artırma ve saldırılara karşı güç kullanmayı öngören bu doktrin, genellikle kara kuvvetleri haricindeki diğer askerî hizmetlerin kara kuvvetlerini destekleyici faaliyet kapsamında organize edilmesini öngörmektedir (Tarapore, 2020). Bu doktrin, mevcut askerî düzenin özerk bir şekilde faaliyet gösteren askerî kanadın ana gücünün silahlı kara kuvvetleri olması bakımından Ortodoks'tur. Her ne kadar bu doktrinin düşmana cezai bir maliyet dayatmak gibi saldırgan bir askerî hedefi olmasa da, bu hedefin genellikle savaş ya da çatışma sonrası müzakerelerde avantaj sağlamak amacıyla toprak ele geçirme hedefi göz önünde bulundurulduğunda, bölgesel savunmanın statükoyu koruyucu bir vizyonu olduğu göz önünde bulundurularak Hint ordusunun güç kullanımının çizgilerini belirleyici bir dizi ilkeyi temsil etmesi bakımından da geçerli ve önemli bir doktrindir.

Bu makale, Hindistan'ın Ortodoks saldırı doktrinin inatçı egemenliğinin Hindistan'ın stratejik coğrafi konumundaki köklü değişiklikler karşısında bile ordusunu daha verimsiz bir araç hâline getirdiğini ve bu bağlamda son dönemdeki Hint ordusunun inovasyon ve yenileşme hareketlerinin bu doktrin ile daha da verimsiz kılınacağını savunmaktadır. Hindistan'ın geçmişten gelen bağlantısızlık politikasının küresel ölçekte yeni bir boyutunu dış politikada uyguladığı son dönemde yeni bir doktrin ile bölgesel ve küresel çıkarlarını ve gücünü daha verimli kullanılabileceğinin tartışıldığı bu makalede temel varsayım; Hindistan'ın mevcut askerî doktrininin son dönemdeki askerî ve stratejik iş birliklerini ve yerlileşme hareketleri ile dışa bağımlılığı azaltmayı hedeflediği dış politika manevralarını

verimli kılmayacağı ve yeni bir askerî doktrin ve vizyon geliştirilmesinin gerekliliği üzerinedir.

Hindistan'ın Kargil bölgesindeki son savaşından günümüze ortalama 20-25 yıl gibi bir süre geçmiştir. Hint ordusu, bağımsızlığından beri herhangi bir topyekûn savaşa dâhil olmasa da irili ufaklı birçok sınır çatışmasına dâhil olmuş ve bu süreçte Hindistan'ın güvenlik paradigmalarını üç büyük stratejik eğilim belirlemiştir: bunlar nükleer caydırıcılık, askerî inovasyon ve Çin'in küresel yayılmacılığıdır. Hindistan'ın kuzey sınırlarındaki askerî güç dengesi göz önünde bulundurulduğunda, Hindistan savaş alanında başka bir dengeleyici devlet olmadan ne Pakistan'a ne de Çin'e kesin olarak üstünlük sağlaması mümkündür. Böyle bir savı kabul etmeden Hindistan'ın bu Ortodoks askerî doktrini, çatışma maliyetlerini karşılama hususunda kararlı olan bu iki devleti caydırma konusunda yeterli olamaz. Öte yandan Çin ve Pakistan'ın saldırgan askerî politikalarına sınırda devam etmesi nükleer güç kullanılması riskini de artırmaktadır. Hindistan'ın askerî doktrini, ülkenin toprak genişliği göz önünde bulundurulduğunda, büyük bir kara kuvvetleri yapılanmasının gerekliliğini de ortaya koymaktadır. Kıt kaynakların olduğu konjonktürel bir ortam da göz önünde bulundurulduğunda, askerî alanda yapılan yerlileşme hareketleri ve dışa bağımlılığı azaltıcı programlar dâhilinde, Hindistan'ın askerî doktrininin de kara kuvvetlerini koruyucu ve sadece kara sınırlarındaki güvenliği sağlamaya yönelik bir atılımdan da öte askerî kanadın yekpare bir merkezden ve tüm savunma sanayisinin efektif kullanılmasını da sağlayacak yeni bir modern doktrinin oluşturulması ihtiyacını gözler önüne sermektedir. Covid-19 Pandemisi döneminde ve sonrasındaki süreçte dünya üstündeki ekonomik krizlerin bulunduğu çatışmacı ortam, bu yeni doktrinin de geliştirilebilmesi için makul bir fırsatı da beraberinde getirmektedir. Her ne kadar bu ortamdan Hindistan ekonomisi de yüksek oranda etkilense de, bölgede bu krizlerden en az etkilenen devlet Hindistan olmuştur.

Bütün bu sınırlamalar ve çıkarımlar ışığında bu makale üç bölümden oluşmaktadır. İlk bölümde, Hindistan'ın kara kuvvetlerini güvence altına almak üzerine geliştirdiği Ortodoks saldırı doktrini bağlamında Hindistan'ın askerî stratejisi tarihi perspektiften incelenmiştir. İkinci bölümde, 21.yy'da Hindistan'ın güvenlik paradigmalarını altüst eden gelişmeler ve sonrasındaki statik ortamda izlenen askerî politikaların başarısızlığı ile bu başarısızlığın nedenleri ve sonuçları analiz edilmiştir. Son bölümde ise, Hindistan'ın askerî gücünün son dönemde mevcut doktrinde diretilmesi durumunda neden başarısız olacağı ve yeni atılımların

verimlilikle sonuçlanabilmesi için oluşturulması gereken yeni modern askerî doktrin için bazı analizler ve çıkarımlar öne sürülmüştür.

1. HİNDİSTAN'IN ORTODOKS SALDIRI DOKTRİNİ; SINIRLARDA DÜZENİ SAĞLAMA ARAYIŞLARI

Bağımsızlığından Soğuk Savaş'ın sonuna kadar olan dönemde genel bağlamda bağlantısızlık politikası izleyen Hindistan, Sovyetler Birliğinin çöküşünden sonraki dönemde dış politikasında ciddi sorunlar ile karşılaşmıştır. Birleşmiş Milletler Güvenlik Konseyinde Sovyetlerin vetosundan yoksun bir durumda kalan Hindistan, o dönemde uluslararası forumlardaki en büyük destekçisini de kaybetmiştir. Stratejik alanda yaşanan bu trajik değişim, Hindistan'ın uluslararası yönelimini de yeniden değerlendirmesi ve kendisini Doğu-Batı ayrımının dar jeopolitik sınırlarının da ötesinde ekonomik, sosyal ve askerî açıdan tekrar bir doktrin belirmesinin de önemi ortaya çıkarmaktadır (Hilali, 2001, s. 745). Yeni oluşturulacak bir strateji ile tek kutuplu bir dünya düzeninde daha az idealist ve ahlakçı bir doktrin belirlemeye yönelik bir girişim içine giren Hindistan, o dönemde değişken olan güvenlik ortamında Soğuk Savaş sonrası dünyanın karşı karşıya olduğu sorunlarda da kendi çıkarlarını koruma gayreti içine girmektedir.

1947'deki bağımsızlığından günümüze Hindistan'ın ekonomisi ve nüfusu istikrarlı bir şekilde büyümeye devam etmektedir. Birinci önceliği kuruluşundan beri sosyo-ekonomik açıdan kalkınmak olan Hindistan, bu hedefin sürdürülebilmesi için askerî açıdan güvende olabileceği bir bölgesel istikrar arayışı içerisindedir. Bu amaçla, Hindistan geleneksel olarak geniş çaplı bir savunma politikası izlemektedir. Ancak askerî gelişmelerin yanı sıra Çin ve Pakistan ile artan rekabet ve düşmanlıklar, geçmişten günümüze Hindistan'ı da sürekli savaşı önlemeye yönelik bir strateji geliştirmeye yönlendirmektedir. Hindistan'ın büyümesi ve kalkınması Asya'nın geri kalanını ekonomik, teknolojik ve politik olarak etkileyeceği görüşünden ötürü, Hindistan'ın uluslararası güvenlik doktrinlerindeki stratejik değişimleri mevcut statüko üzerinden değerlendirerek yeni bir doktrin oluşturulmaya çalışılmaktadır (Hagerty, 1991, s. 353). Fakat geçmişte oluşturulan doktrinler, teknolojinin gelişmesi ve dünya düzeninin küresel ölçekte artık daha hızlı değişmesi sonucu Hint alt kıtasında düzeni sağlayıcı bir yapı olmaktan çıkmış durumdadır.

Hindistan'ın kara kuvvetleri ülkenin kuruluşundan beri askerî doktrinlerin sürekli merkezinde yer almaktadır. Özellikle Hindistan ordusunun dâhil olduğu bütün savaşlarda güç kullanımı Ortodoks saldırı doktrini üzerinden ikame

edilmekte ve bu doktrinin temel felsefesi yüksek maliyetli bir misilleme tehdidi ile düşmanı saldırgan bir tavır almaktan caydıracağı mantığına dayanmaktadır (Clary, 2018, s. 107). Bu doktrin eski dönemlerde birkaç savaştan ve çatışmadan önce sürekli olarak uygulanmış ve örgütsel reformlar ve askerî eğitim yoluyla da düzenli olarak kurumsallaştırılmaya çalışılmıştır. Modern askerî örgütlenmelerde kara ordusu sürekli açık ara en büyük hizmet ve kaynaklara sahip olduğundan, bu doktrin Hindistan'da her savaşın ve çatışmanın en temelinde sürekli yer almaktadır (Mansingh, 1984, s. 290).

Ortodoks saldırı doktrini, ilk defa 1960'ların ortalarında Hint ordusuna İngiliz Raj'ın sınır savunma doktrininin ayrıntılarını öğreten iki deneyim ile işlevsel hâle getirilmeye çalışılmıştır (Tarapore, 2020, s. 5). Bu deneyimlerden ilki 1947'de başlayan birinci Keşmir çatışmasıdır. 1947-48'deki ilk Keşmir Savaşı, tartışmalı bölgenin kontrolünü ele geçirmek için yapılan hafif bir piyade çatışmasıdır. O dönemde Hindistan kısa bir süre içerisinde Srinagar ve Keşmir vadisinin kontrolünü eline geçirmiş, devam eden süreçte çoğu çatışma, çevredeki dağlık arazide meydana gelmiştir. Bu durumda hâliyle topyekûn bir savaş stratejisinin gerçekleşmemesi sonucunu doğurmuş ve konvansiyonel savaş bir asimetrik çatışmaya dönüşmüştür. Bununla birlikte Hindistan o dönemde Keşmir'de konuşlanabilmek için, hava kuvvetlerini bölgede kara kuvvetlerinin ilerleyebilmesi için bir savunma mekanizması olarak kullanmış ve bu durum kara kuvvetlerinin inisiyatifi ele geçirmesine ve Pakistan'da önce kara kuvvetlerine ait askerî varlıkların bölgeye konuşlanmasına yardımcı olmuştur (Mukherjee, 2022, s. 7). Hava kuvvetlerinden böyle bir destek ile yararlanılmasa belki de Hindistan'ın askerî operasyonları, o dönemde Keşmir'de başarısızlıkla sonuçlanacaktır. Fakat o dönemde hava harekâtları temelde bir saldırı gerçekleştirmek için değil kara kuvvetlerinin bölgede konuşlanmasını sağlamak için yapılmıştır (Clary, 2018, s. 106). Nitekim savaşın devamında Hindistan ilk olarak Jammu üzerinden kara iletişim hatlarını güvence altına alarak ateşkes dönemine kadar bu dağlık bölgede kontrolü ele almak için asimetrik çatışmalara devam etmiştir.

Bu doktrinin ikinci büyük deneyimi ise Çin ile yaşanan sınır çatışmalarıdır. İlk çatışmaların bir çıkmazla sonuçlanması sonrası Hindistan'ın 1962'de Çin'e karşı gerçekleştirdiği savaşta Hindistan ordusu ezici bir yenilgiyle mağlup olmuştu. Geniş bir cephede Çin saldırılarını püskürtmek için savaşan Hint ordusu, bir kez daha yüksek dağlık bölgelerde zorlu piyade savaşlarına girmek zorunda kalmıştı. İngiliz Raj'ın sınır savunma doktrininden bu savaşta da uygulayan Hint ordusu, genel anlamda sınırlarını korumak için bir saldırıya geçmeden önce düşman

hatlarının düzenini bozmak için yapılanmasını tekrar asimetrik bir çatışma düzenine göre ayarlamıştı (Mansingh, 1984). O dönemde Hintli komutanların temel hedefi sarp kayalıklardan oluşan bu bölgede kara kuvvetlerine düzenli ikmal sağlayarak savunmayı derinleştirmek üzerineydi (Maxwell, 2015, s. 110). Fakat bu ikilemde topçu desteğinin coğrafi koşullarda pek de mümkün olmayacağı düşünülerek hava kuvvetleri kara kuvvetlerinin ikmali için kullanılmıştı. Aynı dönemde Hindistan'ın hava kuvvetleri Çin ordusuna karşı saldırı operasyonları yürütmek için herhangi bir şekilde kullanılmamıştı. Bu durumda Hindistan için savaşın kara kuvvetlerinin merkezinde bir strateji geliştirmesiyle sonuçlanmıştı (Lintner, 2018, s. 62). Nitekim savaş büyük bir hezeyanla sonuçlanmış ve yıkıcı bir kayıp yaşanmıştı. Fakat o dönemde Hindistan ordusu bu Ortodoks savaş doktrinine tamamen bağlı kalmaya devam etmiş ve ilerleyen dönemlerde kara ordusu nüfusunu iki katına çıkararak ve aynı zamanda alınan bir kararla orduyu siyasi denetimden uzak tutarak tam bir özerk konuma getirmişti (Clary, 2018). Sonraki dönemlerde Hint ordusu bu Ortodoks saldırı doktrinine daha sadık bir şekilde hareket ederek sınırlarda yaşanan tüm çatışmalarda bu doktrini uygulamaya devam etmiştir. 1965'te Keşmir'de yaşanan ikinci savaşta; 1971'de Pakistan ile gerçekleşen savaşta, hatta 1980'lerde ve 1990'larda Güney Asya'da yaşanan birçok düzensiz çatışmada temelleri Raj'a dayanan bu savaş doktrininin izleri fazlasıyla görülebilmektedir.

Hindistan'ın orduda reform hareketlerinin de bu konjonktürde kara kuvvetleri temelinde bir eğilimde olduğu hâliyle kaçınılmaz bir gelişmedir. Özellikle 1960'larda Hint ordusu zırhlı personel taşıyıcılarla donatılmış, yeni mekanize piyade birimleri oluşturmuş, hızlı hareket edebilen RAPID (Reorganized Army Plains Infantry Divisions) örgütlenmelerle baştan reform edilmiştir (Romjue, 1984, s. 27). Bu dönemde ordu reform edildikten sonra hava kuvvetleri komutanlığına verilen temel görev sınır bölgelerinde saldırı gerçekleştirmek değil, sınır hattı topraklarına askerlerin hızlıca konumlanabilmesi için nüfuz merkezleri oluşturarak stratejik bilgi edinebilmekti (Smith, 1994, s. 144). Esasında Sundarji Reformları olarak da adlandırılan bu doktrin politikalarından örnek alının bu sistem, ABD'nin hava kuvvetlerinde uygulanan bir stratejik doktrindir (Ahmed, 2012, s. 12). Fakat gözden kaçırılan temel husus ABD, bu stratejiyi çift kutuplu bir dünya düzeninde istihbarat elde edebilmek istediği dönemlerde kullanmaktaydı. Özellikle yumuşama (detente) dönemine kadar gelinen süreçte ABD bu doktrin ile kendi ana karasını tehdit edebilecek unsurlara karşı önceden bilgi edinebilmek ve olası askerî tehlikeleri önleyebilmek üzerine bir strateji kurgularken, esasen keşif ve güvenliği

sağlama üzerine bir doktrin öngörmüştü. Çift kutuplu ve rekabetçi bir dünya düzeninde kendi ana karasını savunmak üzerine böyle bir doktrin benimsemek elbette bir ülkenin ileri görüşlülüğünün göstergesi olabilir. Fakat bir meydan muharebesinde böyle bir doktrinin kullanılıp nüfuz elde etme girişimi bir ülkenin sadece hava savunmasını değil, mevcut sistemde kara kuvvetlerini de tehlikeye sokabilir. Politik bağlamdan bağımsız bir düzende böyle bir saldırı doktrinine bağlı kalınarak saldırı eylemine odaklanmak Brasstacks gibi bir tatbikatta işe yarayabilir (Chari vd., 2007, s. 33); fakat geçmişin savaş muharebelerinin çoğu kaynakların kıt, askerî düzenin modern anlamda sağlanmamış olduğu bir düzende başarılı olması düşük bir olasılıktır.

Günümüzde böyle bir doktrinde ısrarcı olmak, mevcut statükoda düzen sağlayamayacağı gibi olası bir savaşta ciddi kayıpları da beraberinde getirebilir. Nitekim 2000'li yıllara girilmeden önce Kargil'deki savaş bu durumunda habercisi olmuştur. Bu savaş, Hindistan ve Pakistan'ın nükleer güç elde etmesinden ortalama bir yıl sonra gerçekleşmiştir. Hint ordusunun temel hedefi kara ordularının bölgede kontrolü sağlayabilmesi için mevcut hava kuvvetlerinin istihbarat bilgisi elde edinmesi ve kontrol hattı sağlanabilmesi için kara kuvvetlerini desteklemesi üzerineydi (Ahmed, 2012). Nitekim savaşa ABD'nin diplomatik kanallarla müdahale etmesi sonucu çatışma süreci uzun sürmemişti. Fakat bu diplomatik hamlelerde iki devletin ortak bir konuda fikir birliğine varmasını sağlanamamıştır (Ladwig III, 2007, s. 161). Mukherjee, genel olarak muharebede nükleer caydırıcılığın olmasından dolayı Ortodoks saldırı doktrininin hâlen etkinliğini koruduğunu savunmaktadır (Mukherjee, 2020, s. 13). Nitekim bu yaşanan krizlerin hepsi Hindistan'ın askerî hareketlerinin başarısı ile sonuçlanıp sonuçlanmadığından da öte, büyük kara kuvvetleri seferberliklerinin sınırlı bir fayda sağladığı ve Hindistan'ın Ortodoks saldırı doktrininin stratejik kısıtlama politikası bağlamında başarı sağlayacağını göstermektedir.

Görüldüğü üzere Hindistan ordusunda gerçekleşen her reform hareketinin merkezinde kara kuvvetlerini destekleme ve kuvvetlendirme hedefi yatmaktadır. Böyle bir hedef belirlenmesindeki temel sebep, Hindistan'ın askerî politikalarında misilleme hareketi ya da topraklarını fiilen kontrol etme isteğinden kaynaklanmaktadır. Fakat buradaki temel sorun kara kuvvetlerinin fiili sayısının artırılarak bölgede kontrolün sağlanmasının herhangi bir topyekûn muharebe esnasında kara kuvvetlerinde ciddi kayıplar doğurabileceği tezi üzerinedir. Bu durum ordunun yapısını bir savaş doktrini içerisinde oluşturulması ile değil, bölgede çatışma çıkmasının engellenmesi üzerine kurgulamaktadır. Bir çatışma

çıkması riskine yapılan daimî atıf ise rakip ülkelerin bölgedeki radikal terör gruplarını desteklemesiyle bölgede çatışmayı artırıcı bir takım eylemin oluşturulması ile alakalıdır. Peki, bu konjonktürde bahse konu doktrinde ordunun görevlerinin polisinin görevlerinden farkı nedir? Yapılan yatırımların çok daha azı ile mevcut statükoda iç güvenlik birimleri daha verimli bir şekilde kullanılarak da güvenlik sağlanabilir. 2001 yılında Srinagar'daki terör saldırılarında bu doktrin çerçevesinde yeni bir teşkilatlanmaya gidilmiştir. Aynı zamanda bu yapılanma 2017 yılına kadar Hindistan ordusunun temel savaş doktrini olmaya da devam etmişti. Fakat 21.yy'daki kaygan küresel ortam Hindistan'ın bu doktrin yerine topyekûn bir savaştan hibrit bir çatışma ortamına kadar tüm savaş katmanlarını kapsayıcı genel bir doktrin benimseyip ordunun modernizasyonunun da bu bağlamda geliştirilmesini gerekli kılmaktadır.

2. TEKNOLOJİK GELİŞMELER VE STRATEJİK HATALAR: DEĞİŞEN SİSTEMDE ESKİ DOKTRİNDE DİRETMELER

Hindistan 1999'da son konvansiyonel savaşını verdiğinden beri, küresel askerî ve stratejik ortam önemli ölçüde değişti. O dönemden günümüze Hindistan'ın krizlere verdiği kararsız tepkilerden de görüleceği üzere, Hindistan'ın askerî yapısı ve ordudaki güç dağılımı hâlen stabil olmamıştır. Hindistan'ın savunma sanayisi üzerinde yapılan inovasyon ve modernizasyon çalışmaları, askerî stratejilerin topyekûn, planlı ve ortak bir şekilde efektif olarak çalışabilmesini engellemektedir. Bir devletin yeni bir askerî doktrin geliştirmesi kendisine tehlike olarak gördüğü unsurlardaki askerî doktrinleri inceleyerek kendi askerî doktrinini geliştirmesini (Connable vd., 2016, s. 7); eğer mevcut doktrini geliştiremiyorsa da yeni stratejik saldırı ve savunma doktrini geliştirmesini gerekli kılar. Özellikle devletler; yerleşik daimî bir düşmana sahipse, akut bir güvenlik krizine karşı kendi doktrinini beklenmedik bir çatışma ya da muharebe zamanında düşmanın stratejilerini, çatışmaya girilecek coğrafyanın yapısını da gözlemleyerek elde ettiği veriler ile kendi doktrinini geliştirmeye çalışırlar (Palka & Galgano, 2005, s. 76). Hindistan için bu çalışma izlenceleri nükleer silahların kullanımı, Çin'in askerî modernizasyonlarını ve yeni askerî teknolojilerini takip edebilmek ve son olarak da yeni askerî teknolojiler beraberinde izlenen askerî strateji politikalarının son dönemde belli başlı tehlikeleri engelleme kabiliyeti ile ilgilidir.

Bu göstergelerden en tehlikeli ve ağır sonuçları olması muhtemel olanı, Hindistan ve Pakistan'ın nükleer güce sahip olduktan sonra öngörülemez bir caydırıcılık ve riskler barındırmaları ile ilgilidir. Hindistan'ın Çin ve Pakistan ile giderek artan düzeyde bir nükleer caydırıcılık sarmalı içine girmesi, günümüzde

büyük bir konvansiyonel savaş riskini de azaltmaktadır (Shivane, 2021, s. 51). Kargil Savaşı sonrasında iki ülke de nükleer silahları test etmeden envanterlerine almaya başlamıştır. Bu savaş esnasında taraflar askerî stratejilerini nükleer güç nezdinde değerlendirmeden savaşa girmişlerdir. Belirli bir öngörülemezlik sonucu, iki ülkenin de çatışmanın kontrolden çıkmaması için savaşta cephelerini yerel kaynaklarla güçlendirmeye çalışmıştır (Mansingh, 1984). O zamandan günümüze Hintli politikacılar, bu nükleer tırmanışı engellemek adına izledikleri politik tutumlarda son derece hassas davrandılar. Buna karşın Pakistan ise Hindistan'a karşı çeşitli grupları destekleyerek sınırda Hint ordusunun rahat düzen alabilmesini engellemiştir. Buna rağmen Hindistan çatışmayı düşük seviyede tutmak için gerilla hareketlerine karşı askerî bir tepki vermekten düzenli olarak kaçınmaktadır. Bu konjonktürde, Ortodoks bir saldırı doktrini ile olası büyük bir çatışma içine girilmesi durumunda, mevcut nükleer güç kullanma tehdidi savaşların yıkıcı risklerini de Hindistan lehine artıracaktır. Bu durum her ne kadar büyük bir konvansiyonel savaş riskini azaltsa da Hindistan'ın bu savaş doktrininde diretmesi, mevcut kapasitesi ile ihtiyacı karşılamada yetersiz kalmaya devam edecektir.

Nükleer caydırıcılık büyük askerî kayıpları olası kıldığından, bugün Hindistan askerî modernizasyon alanında özgün proje ve strateji yönetimi yapmaktan açıkça kaçınmaktadır. 1962'den beri Hint ordusu sivil-asker ilişkilerinde daha bağımsız bir askerî politika anlayışına sahiptir. O dönemden beri Hint ordusunun düzenli bir başarı elde edememesi ve sürekli bir terör tehdidi içerisinde olması, savaş stratejisi konusunda baştan plan ve vizyon belirleyip strateji geliştirmesini de mümkün kılmamaktadır. Tabii Kargil Savaşı sonrasındaki büyük ümitler ve elde edilemeyen reel başarılar, son dönemdeki çeşitli inovasyon çalışmalarını da tetiklemiştir. Fakat bu durum günümüzde hâlen 1980'lerde başlatılan bir dizi başarısız yerlileşme ve teknoloji transferi hamlesini de beraberinde getirmiştir. Askerî ödenek ve bütçenin çoğunun kara ordusuna ayırılması; Tejas gibi bir uçağın hâlen seri üretime geçememesine, yerli helikopter projelerindeki hataları gidermek için gerekli çalışmamaların yapılamamasına, hatta düşük ve orta menzilli hava savunma füzeleri dâhil birçok projenin uzun bir dönem geliştirilememesine sebep olmuştur (S. Jayaraman, 2020). Ancak her ne olursa olsun bu başarısız inovasyon hamleleri bile Hintli politikacıları mevcut doktrinin temellerini sorgulamaya zorlamıştır.

İkinci büyük stratejik tehlike ise Çin'in askerî teknoloji ve modernleşme çalışmalarında aldığı sıra dışı mesafe ile ilgilidir. Çin ordusu, son dönemde kara sınırlarında uzun bir dönemdir devam eden tehlikelerden de öte neredeyse Hint okyanusuna komşu bütün ülkelerin karasularını tehlikeye atacak derece saldırgan

bir güce ulaştı. Deniz kuvvetlerinin modernizasyonunda navigasyon teknolojilerindeki devrim niteliğindeki haritalama metotlarındaki ilerlemeleri donanmasında oldukça verimli bir şekilde kullanan Çin ordusu, askerî uçak ve deniz gücü envanterindeki teçhizatlarla Hindistan'ı dört bir yandan sayı üstünlüğü ile kuşatmakla kalmamış; üstüne Hindistan'a komşu ülkeler ile de irili ufaklı birçok stratejik iş birlikleri ile mevcut konumunu daha da güçlendirmiştir (Luis, 2021). Bununla beraber Çin'in ürettiği bu ürünlerin birçoğunun fikri mülkiyeti de kendisinde bulunmaktadır. Çin bütün bu yatırımları yaparken aynı zamanda örgütsel birçok doktrin reformu da geliştirmiştir. Bu reformlar sadece mevcut envanterin sayısını artırmakla kalmamış; aynı zamanda daha hızlı ve çevik bir savaş performansı sağlamak için, olası bir muharebede karar alma sürecini hızlandırarak siber ve uzay desteği ile bütün askerî hizmetlerini tek bir merkezden yönetmesine yardımcı olmuştur (P. K. Singh, 2016, s. 22). Ayrıca Çin ordusu kapasite olarak büyümek ve kalkınmakla beraber, aynı zamanda Hindistan için de gün geçtikçe daha büyük bir tehdit olmaya başlamıştır. Askerî teçhizat satışı ve başka ülkelerin limanlarına yaptığı yatırımlar ile Güney Asya ve Hint Okyanusu'nda stratejik nüfuz kazanmaya başlayan Çin, Aden Körfezi'ne kadar uzanan bölgede askerî varlığını günümüzde gün geçtikçe daha fazla hissettirmektedir. Hint okyanusunda gri bölgeler savını kullanarak bölgede çatışma yaratacak faaliyetler peşinde olan Çin, bir oldubitti ile Hindistan'ı zorlayıcı bir baskı ile gerilimli bir ortamda hata yapmaya zorlama gayreti içerisindedir (Luis, 2021). Hindistan ise bu yayılmacılığa karşı Quad ve Aukus gibi ittifak oluşumlarına dâhil olarak bölgede denge kurmaya ve mevcut savaş doktrini ile bölgede Çin'e karşı stratejiler geliştirmeye çalışmaktadır. Ayrıca Hindistan'a komşu ülkelerin Çin'e bağımlı hâle gelmesi sonucu askerî alanda böyle dengeleyici ittifaklarla Çin'e karşı bir politika geliştirmeye çalışıyor. Çin'in Hint-Pasifik bölgesinde böyle bir politika izlemesindeki temel sebep bölgede kendisine bağlı bir çeşit ortaklık oluşturma girişiminden kaynaklanmaktadır (P. K. Singh, 2016). Nitekim ekonomik nedenlerle bu devletleri zorlamak ve siyasi nüfuz alanlarını etkilemek, bu ülkelerin Çin'e olan zorunlu bağımlılıklarını daha da kolaylaştırmaktadır. Borç tuzağı adı verilen bu diplomatik girişim, Çin'in bölgedeki siyasi karar alma mekanizmalarını daha kolay kontrol edebilmesini sağlamaktadır.

Hindistan her ne kadar son dönemde bu yayılmacılığa çeşitli ittifaklara dâhil olarak bir karşı duruş sergilemiş olsa da bu tepkiler Hindistan'ın bağımsız bir askerî saldırı doktrini izlemesini mümkün kılmamaktadır. Çin'in Nepal, Sri Lanka,

Maldivler ve Pakistan'a uzanan askerî ekipman ve altyapı yatırımlarına karşın, Hindistan ise kendi sınırları içerisinde altyapı ve ulaşım ağını yıllarca ihmal etmiştir. Bu bakımdan Çin'e karşı Hint-Pasifik'teki yeni vizyon ve ittifakları desteklemekte ısrarcı olan Hindistan, bu faaliyetlerde Ortodoks saldırı doktrininin bir getirisi olacağına inanmaktadır (Tarapore, 2020). Bu durumda askerî doktrinde yatırım ve modernizasyon çalışmalarının kara kuvvetlerine ayrılmasına, bu bütçenin de inovasyon çalışmalarında kullanılmak yerine askerî teçhizatı ithal yollarla edinmesine sebebiyet vermektedir. Her ne kadar Hindistan kara kuvvetleri son dönemde kuzey sınırlarındaki tehditlerden ötürü bir saldırı doktrini iyileştirmesi yapmayı bir kenara bırakıp ülkenin genelini kapsayıcı bir savunma vizyonuna daha fazla ağırlık verse de (Babar & Mirza, 2021, s. 88), Çin'den gelmesi muhtemel kapsamlı yeni bir tehdit ile sınır güvenliğinin önceliğine tekrar ağırlık verecektir.

Son önemli stratejik tehlike ise yeni askerî teknolojilerin kurumsallığı ve askerî teçhizatın birbiri ile uyum içinde kullanılabilmesi ile ilgilidir. Hindistan'ın asker teknolojilerdeki değişimlere ayak uydurabilmesi için, örgütlenmesinde ve savaş doktrininde temelden bir değişim yapması gerekmektedir. Özellikle ABD ve Çin, son dönemde muharebe hazırlığı ve dayanıklılığı ile ilgili askerî modernizasyon çalışmalarında önemli mesafe kat etmişlerdir. Keşif, gözetleme, komuta ve kontrol teknolojisine dayanan askerî teçhizatlarını ileri teknolojiye taşıyan bu ülkeler, savaş unsurlarını üstün savaş farkındalığı yaratacak teknolojik seviyelerle çok farklı bir boyuta taşımışlardır. Özellikle Çin bu teknolojiler ışığında yeni savaş kavramları ve doktrinleri geliştirmiştir. Pakistan ise özellikle Türkiye ile ortak yürüttüğü insansız hava araçları ve hava savunma sistemleri ile muharebeler sırasında tam donanımlı bir şekilde muharebe sahasında çok daha kolay plan ve stratejilerini geliştirebilmektedir. İleri teknolojik teçhizatlar, düşman toprakları olarak nitelendirilen bölgelerin derinliklerinde nispeten düşük maliyetle saldırabilmek için çeşitli kısa ve orta menzilli füzeler ve kamikaze dronelar kullanarak hassas saldırı gerçekleştirmesini mümkün kılmaktadır. Hassas sensor sistemlerinden akıllı füze başlıklarına, hatta bu teknolojileri birbirine bağlayan ağlara kadar daha karmaşık yapay zekâ ile desteklenmiş otomasyon ve insansız sistemlerini kullanan orduların sayısı da gün geçtikçe artmaktadır.

Bu sistemler elbette mevcut askerî doktrini ile kolayca elde edilebilecek ya da modernize edilebilecek sistemler değil. Bu sistemlerin etkili bir şekilde entegre edilebilmesi için mevcut askerî doktrine uyumlu bir şekilde uyarlanması gerekir. Çin çok uzun yıllar elindeki envanteri modernize edebilmek için farklı

hizmetlerdeki personelini mevcut envanteri modernize edebilmek için görevlendirdi (Luis, 2021). Çin'in bu modernize edilmiş ürünlerini test etmesi bile on yıla yakın bir zaman aldı. Bu modernize serüvenini mevcut savaş doktrininde verimli bir şekilde kullanabilmek en güçlü ordular için bile zorlu bir süreç olabilir. Örneğin ABD hem savaş zamanı hem de barış zamanlarında ordularla rekabet edebilmek için tüm kara, deniz, hava ve siber birliklerini birbiriyle ortak çalışabilmesi için yeni nesil bir savaş doktrini üzerinde çalışıyor (O'Hanlon, 2019, s. 14). Kara sahasını belirli bir çatışma alanı olarak görmeyen modern ordular, düşman sistemlerini hızla yok edebilmek için yararlanabilecekleri her elementi mevcut doktrinlerine entegre etme gayreti içerisindeler. Daha da önemlisi; bu teknolojilerin yaygın bir şekilde kullanılabilmesi, yalnızca güçlü ve adet olarak fazla olan ordularla değil, günümüzde birçok ülkenin ordusu tarafından test edilip bir çatışma ya da muharebe esnasında kullanılıp test edilmesiyle mümkündür. Şu durumda Hindistan'ın Ortodoks saldırı doktrinin mevcut inovasyon ve modernizasyon çalışmaları ışığında başarıya ulaşması Hindistan ordusunun envanterinin herhangi bir muharebede ya da çatışmada test etmesiyle mümkündür. Yeni bir savaş doktrini ile mevcut askerî yapılanmanın üstünde reform yapılması, hem mevcut askerî yatırımların daha verimli bir şekilde kullanılması, hem de ülkenin toprak güvenliğinin daha net sağlanabilmesi için büyük önem arz etmektedir.

3. YENİ VİZYONDA BAĞIL POLİTİKALAR: MODERN ASKERÎDOKTRİN ARAYIŞLARI

Her devrin konjonktürüne askerî açıdan uyum sağlamak, doğru stratejik değerlendirmeler ve politika seçeneklerini rasyonel bir şekilde analiz edilmesi ile mümkündür. Bu analizlerin teorik perspektifi, periyodik bir stratejik planlama süreci oluşturularak, mevcut askerî teçhizatların teknolojik üstünlükle coğrafi yapıda potansiyel düşman unsurlarını uzun dönemde ülke topraklarından uzak tutmasını hedeflemektedir. Örneğin Çin, bu planlama sürecinde düzenli olarak ulusal güvenlik stratejisi hazırlamakta, çıkarlarının olduğunu iddia ettiği her bölgedeki gelişmeleri yakinen takip etmekte ve mevcut düzende bir açık ya da yetersizlik gördüğü takdirde bölgedeki askerî gücünü hızlıca artırmaya yönelik bir dizi stratejik politika izlemektedir. Hindistan, Ortodoks saldırı doktrini bağlamında, düzenli bir planlama stratejisi üretemediği gibi, herhangi bir tehlike ya da çatışma anında izleyeceği bir stratejik politikadan da yoksundur. Bununla birlikte Hindistan'ın askerî stratejileri, şimdiye kadar ulusal düzeyde bir stratejik değerlendirme ve politika analizinden de yoksundur. Bu nedenle Hindistan'daki

savunma bütçeleri ve bunların misyonları kademeli olarak önceliklerinin analiz edilmesi yerine bir önceki yılın mevcut statükosunun analizi üzerinden test edilmektedir (Moitra & Chatterjee, 2022, s. 4). Böyle bir süreçte de hâliyle tehlikelerin erken tespit edilmesi mümkün olmamaktadır. Bu nedenledir ki, Çin'in askerî yeteneklerinin devam eden süreçte büyümesi sistematik olarak takip edilememiştir. Benzer şekilde mevcut Hindistan'ın askerî doktrini, ulusal stratejik gereksinimlerin birleşik bir değerlendirmesi olmaktan ziyade, hizmet tercihlerine uyacak şekilde geleneksel olarak bireysel hizmet unsurlarına odaklanmaktadır. Fakat son dönemde Hindistan'da yeni kurulan Genel Kurmay Başkanlığı pozisyonu bu düzensizlik ve plansızlığı kontrol altına alabilmek adına potansiyel bir yeterliliğe sahiptir.

Askerî hizmetlerin organizasyon şeması, doktrin değişikliklerinin önündeki en büyün engellerden biridir. Geniş çaplı bir inovasyon çalışması, orduların genellikle saldırgan doktrinler için örgütsel bir test aşamasını da gerekli kılmaktadır. Bu test aşamasında izlenen genel politika, mevcut envanterin bir doktrin çerçevesinde ne şekilde kullanacağının belirlenmesi açısından büyük önem arz etmektedir. Bundan dolayıdır ki doktrin değişiminin pekiştirilebilmesi her ülkede zaman alabilir (Clary, 2018). Ordulardaki hizmet sürelerinin kısıtlı olması, benzer reform düşüncesine sahip kişilerin görev sürelerinin erken dolması ve ardıllarının bu reformları izlemelerinin garanti bir durum olmaması, çoğu ülkenin askerî yapılanmalarının büyük bir doktrin değişikliğinde bürokratik zorluklarla karşılaşması mevcut düzenin bozulması riskinden dolayı başarısız olmaktadır. Hindistan da bu gibi temel sebeplerden ötürü Ortodoks saldırı doktrinini destekleyen köklü uygulamalarda ısrar etmektedir. Son dönemde değişim isteyen bürokrasi ve "Cold Start" oluşumları, bu doktrinin de revize edilmesi için iyi bir fırsat olarak değerlendirilmektedir (Ladwig III, 2007). Bu girişimler, Hindistan'ın askerî sisteminin stratejik faydalarını yeniden hesaplamaktan öte, Hindistan ordusunun taktiksel etkinliğinin ve hazır olma durumunun optimize edilmesine yönelik girişimlerdir. 2018 yılında Hindistan Genelkurmay Başkanı Ripin Rawat, bu reform girişimlerini daha da ileri bir seviyeye taşımakta ısrarcı olmuştur. Çeşitli reform girişimleri ile ordudaki 100 bin kadar personelin birlik oluşumları ve karargâh yapılanmalarını tekrardan düzenleyen Rawat, mevcut kara ordusunu olası bir savaş ya da çatışma durumunda operasyonel olarak hızlı hareket edilebilmesi için tekrardan örgütlemiştir (Shwkatkar Committee, 2018). Fakat 2020 yılında Rawat'ın şaibeli bir kazada hayatını kaybetmesi sonucu bu reform hareketlerinin uygulanması duraksamıştır. Son dönemde atanan yeni Genelkurmay Başkanı Anil

Chauhan ise mevcut statükoda ordunun düzeninde sivil bürokrasinin inovasyon programlarından da yararlanarak yeni bir revizyon öngörmektedir (PIB Delhi, 2022). Bu durum, doktrin değişiminin ordunun dışından bir yapılanma ile ulusal güvenlik stratejisine uyum sağlamasını gerekli kılmaktadır. Mevcut düzende bu inovasyonların ve yatırımların başarıya ulaşması için yeni bir doktrin ile daha güçlü bir düzen kurulmasının gerekliliği ve bilinciyle hareket edildiği değerlendirilmektedir.

Hindistan hükümetinin "Make in India" kampanyası, ülkenin yalnızca bir üretim merkezi olarak değil, aynı zamanda ülke genelinde programa dâhil olan sanayi sektörüne de bir imaj kazandırmıştır (Shaikh vd., 2016, s. 15). Hindistan'ın dünyanın en büyük silah ithalatçısı olması statüsünden rahatsız olan mevcut hükümet, ülkeyi bir üretim merkezine dönüştürmeyi hedefleyen gelişmiş bir savunma sanayisi kurmayı hedeflemektedir. Savunma sanayisinin üretimde kendi kendine yeterli olmasının önünü açan bu program, savunma sanayisindeki askerî birimlerin bahse konu programdan çıkan yüksek teknolojili ürünlerle verimli kullanılabilmesini hedeflemektedir (Bhardwaj, 2018). Hindistan hükümeti, yerel savunma sanayisi ürünlerinin üretimi ve yenilenmesi, Ar&Ge ve tasarım konusunda üst düzey sistemlerin geliştirilebilmesi için hâlihazırda çeşitli kampanyalar başlatmış durumdadır (Rathi vd., 2019). Gelişmiş bir füze teknolojisi, uzaktan kontrol edilebilen otonom silah sistemleri vb. birçok teknolojik sistemler Hindistan savunma sektöründe özel ve devlet destekli çeşitli kampanyalarla geliştirilmeye çalışılmaktadır. Son dönemde, Hindistan hükümeti bu çalışmalar için Doğrudan Yabancı Yatırım'a %49 oranında izin vermiş durumdadır (*Defence Manufacturing | Make In India*, t.y.). Ülkedeki özel sektör, savunma sanayisindeki ürünlerin imalatı hususunda henüz başlangıç aşamasında olmasına rağmen, savunma sanayisi envanteri için yeterli yatırımı almış durumdadır. Bu yatırım neticesinde Tata ve Boeing birçok ortak çalışma programı için çeşitli anlaşmalar yapmışlardır. Ayrıca İsrailli Rafeel firması, Kalyani grubuyla ortak bir girişim başlatmıştır. Özellikle hava savunma sistemlerinin yerelleştirilmesi için birçok projeye de onay verilmiş durumdadır. Mevcut kara kuvvetleri envanterinin 2030 yılına kadar ordunun yeterli ekipmanı yerli ürünler ile donatacak seviyeye gelmesi hedeflenmektedir. Hava kuvvetlerinin inovasyon çalışmaları da birçok prototipi seri üretime geçirmeye hazırlanmaktadır. 2015'ten 2022'ye kadar Hindistan'ın savunma sanayisine toplamda 100 milyar doların üstünde yatırım yapılmıştır (Kalyani Rafael JV Begins MRSAM Missile Kits Delivery to Armed Forces, 2021). Ayrıca özel sektörden tek kaynaktan tedarik yerine çoklu tedarik edinimleri

için çeşitli anlaşmalar yapılmıştır. Fakat tüm bu inovasyon çalışmalarından çıkan ürünler, Hindistan'ın savunma sanayisini geliştirilebilmesi için mevcut statükoda bir çatışmada ya da topyekûn savaş hâlinde uygulanacak bir doktrinde yerini almamaktadır. Kısa vadeli stratejik açıkları da ithal ürünlerle kapatmaya çalışan mevcut düzende Ortodoks saldırı doktrini, yapılan yatırımların test edilmesini ve mevcut envanterde kullanılabilmesini de imkânsız hâle getirmektedir. Son dönemde Rusya'ya olan bağımlılığın hâlen yüksek teknoloji gerektiren ürünlerde devam etmesi, eldeki envanterin mevcut doktrinde iyileştirmeler yapılarak statükoyu güçlendirmesini engellemektedir (Sharma, 2022).

Günümüzde Rusya hâlen Hindistan'ın en büyük savunma tedarikçilerinden biridir. Stimson Center tarafından 2020 yılında hazırlanan rapora göre, Hindistan'ın askerî envanterinin %85'i Rus menşeilidir (Lalwani vd., 2021). Rusya ile son dönemde yapılan anlaşmalar geçmişten günümüze kadar kara kuvvetleri ekipmanları, uçak gemisi, nükleer denizaltı, hava savunma sistemleri ve mevcut savaş uçaklarının modernizasyonunu içermektedir. 2022 yılında SIPRI'nin raporuna göre ise mevcut bağımlılık son dönemde %63 seviyelerine düşürülmüş durumdadır (Wezeman vd., 2021). Fakat bu oranın düşmesindeki temel sebep sadece kara kuvvetlerinin ürünlerinin yerlileştirilmesi sonucu yapılan değişimlerden kaynaklanmaktadır. Mevcut Ortodoks saldırı doktrinindeki kara kuvvetleri merkeziyetçiliğinin sonucu olarak bu yapılanma askerî boyutta bir kalkınma için geniş bir uygulanabilirliği de imkânsız kılmaktadır. Hindistan'da büyük doktrinler için yapılan son zamanlardaki girişimler sivil bürokrasiden kaynaklanmaktadır. Kargil savaşı sonrasında K. Subrahmenyan liderliğinde toplanan komite sonrası o dönem de bir çalışma başlatılmıştır. Son dönemde ise 2012 yılında N. Chandra liderliğinde bir uzman raporu çalıştaya dâhil edilmiştir. 2016 yılında ise mevcut hükümetin önderliğinde görevlendirilen D.B. Sheketkar mevcut askerî komutanlıkların tekrardan yapılandırılıp saldırı doktrininin mevcut savunma sanayisi ürünleri ile baştan oluşturulmasına yönelik çalışma başlatılmıştır (Tarapore, 2020). Mevcut askerî ilkelerin unsurlarının küçültülmesi ve teknolojiden daha fazla yararlanılması, siber ve uzay endüstrisinin de bu doktrine dâhil edilebilmesi için 2019 yılında geniş çaplı bir reform listesi hazırlanmıştır. Bu bağlamda atılan ilk adım ise mevcut bütün askerî birimlerin tek bir çatı altında Genelkurmay Başkanlığı kurularak buraya bağlanması olmuştur. Hindistan'ın ilk Genelkurmay Başkanı Rawat, bu kuvvetlerin birleştirilerek örgütsel reformları gerçekleştirerek yeni bir doktrin geliştirmesinin önemini zamanında belirtmiştir (Pandit, 2020). Fakat Rawat'ın bir kazada vefat etmesi sonucu bu çalışmalar da

tamamen durmuş mevcut düzenin Ortodoks saldırı doktrini ile tekrar takip edilmesine sebebiyet vermiştir.

Bu konjonktürde Hindistan ordusu, savaş ya da çatışma zamanı maliyet dayatan mevcut strateji ve doktrinlerini uygulamaya, mevcut yapıyı olduğu gibi örgütlemeye ve yeni askerî teçhizatları ithal ederek envanterine eklemeye devam etmektedir. Hintli liderler, verdikleri son konvansiyonel savaş sonrası müzakerelerde koz olarak kullanılmasını bekledikleri mevcut doktrin ile topraklarını korumak için geniş kadrolu birleşik silahlı oluşumlar inşa etmişlerdir (Ladwig III, 2007). Bu yapılanma Hint ordusunun olası bir savaşta operasyonel düzeyde siyasi yönden bağımsız olarak hareket edebilmesi için tasarlanmıştır. Son dönemde ise Hint hükümeti sınır çatışmaları sonrasında askerî güç kullanımında büyük bir konvansiyonel savaş başlatmak için bir eylemden kaçınmak yönünde politika izlemektedirler. Nükleer tehditlerden dolayı Hindistan'ın, tehlikeli bir tırmanıştan kaçınmak adına, Pakistan ve Çin'in karşılaştıkları zorluklar karşısında da hâliyle çok az sayıda kullanılabilir seçenekleri kalmıştır. Bu bağlamda ordu, personel ve savunma bütçeleri mevcut bütçeden büyük ölçüde pay alırken, yarım dönemdir hem askerî savaştan yenilgiyle ayrılan mevcut askerî doktrin hem de Aukus ve Quad gibi bölgesel üçlü ya da dörtlü askerî ittifaklar ile bölgede bir denge diplomasisi izleme çabaları Hindistan'ın güvenlik tercihleri olmaya devam etmektedir. Bu bağlamda Hindistan, yeni dönemde, Ortodoks saldırı doktrini gibi temelde dost ve düşman ayrışımının keskin çizgilerle altının çizildiği bir diplomatik vizyondan uzak askerî politikalar ile güvenliğini sağlamaya çalışmaktadır. Bu durum da günümüz konjonktüründe ekonomi politikaları ile askerî politikaların stratejik bir bütünlük içinde olabilecek bir kamu diplomasisi izlenememesi ile sonuçlanmaktadır.

SONUÇ

Hindistan ordusu, geniş ölçekli topyekûn bir savaş ihtimalini ya da kara sınırlarından gelebilecek iki cephede eş zamanlı bir tehdit olasılığını görmezden gelemez. Bu bakımdan Hindistan ordusu, büyük bir kara harbi olasılığına karşı tam kapasite olarak kara ordusunu hazır bulundurmaktadır. Hindistan'ın kara sınırlarının genişliği, Pakistan ve Çin'in ordularının büyüklüğü, sınır bölgelerdeki terör faaliyetlerinin yarattığı güvenlik tehdidi ve uç bölgelerdeki diğer devletlerin yayılmacı politikaları göz önünde bulundurulduğunda, mevcut konvansiyonel gücün sürekli desteklenmesi ve askerî harcamalara ayrılan kaynağın büyük bir kısmının kara ordusuna tahsis edilmesi kaçınılmaz bir sonuç olarak karcımıza çıkmaktadır. Ancak Hindistan, sadece en tehlikeli savaş senaryolarına değil, aynı

zamanda olası hibrit tehditlere karşı da hazırlıklı olmalıdır. Günümüzde hibrit tehditler ve gri bölgeler ülkelerin stratejik iş birliklerine ve güvenlik paradigmalarının geleceğinde önemli bir rol oynamaktadır. Bu tehditleri bertaraf etmek için büyük kaynak yatırımları yerine mevcut doktrin tehdidin büyüklüğü ve çeşidine göre kategorize planlar yapılmasını gerekli kılmaktadır. Hindistan'ın Ortodoks saldırı doktrininin mevcut yatırımlar, riskler ve yöntemler tekrardan gözden geçirilerek revize edilmesi bu bakımdan önemlidir.

Günümüzde bölgesel ya da küresel güç olarak atıf yapılan devletler arasında askerî saldırı doktrini güncellenmeyen tek devlet Hindistan'dır. Bu duruma ulusal güvenlik algısının her daim riskler barındırması da büyük bir sebep olarak gösterilebilir. Fakat kapsamlı ve uzun vadeli bir vizyon olmadan ulusal güvenlik planlarının uygulanması, hem mevcut düzende ordunun hareket kabiliyetini etkilemekte, hem de savunma sanayisinin Ar&Ge ve inovasyon çalışmalarının sürdürülebilirliklerini tehlikeye atmaktadır. Hindistan Savunma Bakanlığı'nın uygulamadaki bağıl politikalarının güncellenmemesi, yeni kurulan Genelkurmay Başkanlığının sistemde organize bir yapıya bürünememesi ve bir türlü pratiğe geçemeyen yeni saldırı doktrini çalışmaları, politik ve bürokratik yapıdan da etkilenerek, Hindistan silahlı kuvvetlerinin uzun vadeli planlar yapmasını engellemektedir. Bütün bu çalışmalar ekseninde hükümetin savunma reformlarını öncelikli hâle getirebilmesinin yolu da bütün askerî unsurların tek merkezden yönetim şeması altında toplanarak yeni bir askerî doktrin geliştirilmesinde yatmaktadır. Göreve yeni atanan Genelkurmay Başkanının bu dengeyi sağlayabilmek için hava kuvvetleri, kara ordusu ve donanmayı da genel hatlarıyla kapsayan bir askerî saldırı doktrini geliştirmesi gerekmektedir.

Sonuç olarak mevcut Ortodoks saldırı doktrininde her ne kadar birçok eksik ve atıl kalmış stratejiler ve politikalar yer alsa da Genelkurmay Başkanlığına yapılan atamalar ve hükümetin askerî vizyonu göz önünde bulundurulduğunda, günümüzde iki cepheli bir savaş durumunun yanında kapsayıcı bir askerî doktrin oluşturulma isteği de çok açık olarak görünmektedir. Dolayısıyla bu yeni oluşturulacak doktrinde Pakistan ve Çin bağlamında bir güvenlik programı belirlenmesi kara savunma sistemlerinin yanında diğer unsurlarında merkezi odak noktasında değerlendirildiğini göstermektedir. Bu makaledeki veriler ve analizlerin de gösterdiği gibi, reform çabaları ve resmî planlama süreçlerindeki aksaklıklar, ordunun örgütsel çıkarları ve sivil bürokrasinin yönlendirdiği gelişigüzel düzenlemeler sebebiyle Hindistan'ın mevcut saldırı doktrini üzerinde bir güncellemeye ya da yeni bir modern doktrin programlamalarına gidilemediğini

gösteriyor. Bir ülkenin ordusunun felsefesini belirleyen doktrinlerde modernizasyon yapılması yalnızca ekipman ve kaynak tedariğinden çok daha fazlasını gerektirmektedir. Mevcut tehlikelerin de yakinen takip edilmesi, eksikliklerini mevcut envanteri ve eldeki gücü de hesaba katarak modernize etmek ve yeni gelecek askerî envanter ile eski envanterin de uyum içinde çalışabilmesini sağlamaktadır. Bu uyumun olmaması durumunda, düşman topraklarına yapılacak olası bir saldırı dâhil tüm çatışma olasılıklarının hesaplanarak konvansiyonel bir saldırı operasyonunun planlanmasının yapılması, ulusal güvenlik politikalarının bir aracı olarak giderek önemsiz hâle gelecektir.

KAYNAKÇA

Ahmed, A. (2012). *India's limited war doctrine: The structural factor*. Institute for Defence Studies & Analyses.

Babar, S. I., & Mirza, M. N. (2021). Indian Strategic Doctrinal Transformation: Trends and Trajectory. *Journal of Security and Strategic Analyses*, *6*(2), 79-100.

Bhardwaj, D. (2018, Mayıs 7). *"Make in India" in defence sector: A distant dream*. ORF. Erişim Tarihi: 28.09.2022, https://www.orfonline.org/expert-speak/make-in-india-defence-sector-distant-dream/.

Chari, P. R., Cheema, P. I., & Cohen, S. P. (2007). *Four crises and a peace process: American engagement in South Asia*. Brookings Institution Press.

Clary, C. (2018). Personalities, organizations, and doctrine in the Indian military. *India Review*, *17*(1), 100-121. Erişim Tarihi: 16.10.2022, https://doi.org/10.1080/14736489.2018.1415283.

Connable, B., Campbell, J. H., & Madden, D. (2016). *Stretching and Exploiting Thresholds for High-Order War: How Russia, China, and Iran Are Eroding American Influence Using Time-Tested Measures Short of War*. RAND Corporation.

Defence Manufacturing | Make In India. (t.y.). Erişim Tarihi: 29.09.2022, https://www.makeinindia.com/sector/defence-manufacturing.

Hagerty, D. T. (1991). India's Regional Security Doctrine. *Asian Survey*, *31*(4), 351-363. Erişim Tarihi: 16.10.2022, https://doi.org/10.2307/2645389.

Hilali, A. Z. (2001). India's Strategic Thinking and Its National Security Policy. *Asian Survey*, *41*(5), 737-764. Erişim Tarihi: 16.10.2022, https://doi.org/10.1525/as.2001.41.5.737.

Kalyani Rafael JV begins MRSAM missile kits delivery to armed forces. (2021, Mart 16). *The Hindu*. Erişim Tarihi: 28.09.2022, https://www.thehindu.com/news/cities/Hyderabad/kalyani-rafael-jv-begins-mrsam-missile-kits-delivery-to-armed-forces/article34086468.ece.

Ladwig III, W. C. (2007). A Cold Start for Hot Wars? The Indian Army's New Limited War Doctrine. *International Security*, *32*(3), 158-190.

Lalwani, S., O'donnell, F., Sagerstrom, T., & Vasudeva, A. (2021). *The Influence*

of Arms: Explaining the Durability of India–Russia Alignment • Stimson Center. Erişim Tarihi: 29.10.2022, https://www.stimson.org/2021/the-influence-of-arms-explaining-the-durability-of-india-russia-alignment/

Lintner, B. (2018). *China's India war: Collision course on the roof of the world* (First edition). Oxford University Press.

Luis, A. (2021). *China Military Power: Modernizing a Force to Fight and Win*. Erişim Tarihi: 18.10.2022, https://www.audible.com/pd/China-Military-Power-Modernizing-a-Force-to-Fight-and-Win-Audiobook/B09BP3WMRG

Mansingh, S. (1984). *India's search for power: Indira Gandhi's foreign policy, 1966-1982*. Sage Publications.

Maxwell, N. (2015). *India's China war* (Revised and updated Indian paperback edition). Natraj Publishers.

Moitra, M., & Chatterjee, A. (2022). National Security and Privacy: Which Side Well The Debate move? *Indian Journal of Integrated Research in Law*, *2*(2), 1-9.

Mukherjee, A. (2020). *The absent dialogue: Politicians, bureaucrats, and the military in India*. Oxford University Press.

Mukherjee, A. (2022). Towards control and effectiveness: The Ministry of Defence and civil-military relations in India. *Journal of Strategic Studies*, 1-23. Erişim Tarihi: 16.10.2022, https://doi.org/10.1080/01402390.2022.2118115

O'Hanlon, M. E. (2019). *The Senkaku paradox: Risking great power war over small stakes* (First edition). Brookings Institution Press.

Palka, E. J., & Galgano, F. A. (2005). *Military geography: From peace to war*. McGraw Hill Custom Publishing.

Pandit, R. (2020, Mayıs 10). *CDS Bipin Rawat: Forces must shun imports, go for 'Make In India', says Gen Bipin Rawat | India News—Times of India*. Erişim Tarihi: 29.10.2022, https://timesofindia.indiatimes.com/india/forces-must-shun-imports-go-for-make-in-india-says-gen-bipin-rawat/articleshow/75652962.cms

PIB Delhi. (2022). *Chief of Defence Staff General Anil Chauhan visits forward posts in Rajouri sector of Jammu & Kashmir; Reviews security scenario & operational preparedness along LoC*. Erişim Tarihi: 18.10.2022, https://pib.gov.in/pib.gov.in/Pressreleaseshare.aspx?PRID=1870628

Rathi, N., Aggarwal, B., & Pandey, H. K. (2019). *Make in India Challenges in Defence Sector* (SSRN Scholarly Paper Sy 3998482). Erişim Tarihi: 29.10.2022 https://papers.ssrn.com/abstract=3998482

Romjue, J. L. (1984). *From active defense to AirLand Battle: The development of Army doctrine, 1973-1982*. University of California Libraries.

S. Jayaraman, K. (2020). The inside story of India's Light Combat Aircraft Tejas. *Nature India*. Erişim Tarihi: 28.09.2022, https://doi.org/10.1038/nindia.2020.33

Shaikh, A., Kinange, U., & Fernandes, A. (2016). Make in India: Oportunities and Challenges in Defence Sector. *International Journal of Research in Commerce & Management*, *7*(2), 13-16.

Sharma, M. (2022). *Indian Military Dependence on Russia*. Institut Montaigne. Erişim Tarihi: 28.1**0**.2022, https://www.institutmontaigne.org/en/analysis/indian-military-dependence-russia

Shivane, A. B. (2021). Restructuring for India's Disputed Borders: An Appraisal. *CLAWS Journal*, *14*(2), 46-61.

Shwkatkar Committee. (2018). *Recommendations made by Shekatkar Committee*. Press Information Bureau. Erişim Tarihi: 29.10.2022, https://pib.gov.in/newsite/PrintRelease.aspx?relid=177071

Singh, C. H. V. (2022, Eylül 22). *Evolution of Warfighting Strategy in India*. Erişim Tarihi: 30.10.2022 https://www.claws.in/evolution-of-warfighting-strategy-in-india/

Singh, P. K. (2016). *Changing contexts of Chinese military strategy and doctrine*. Institute for Defence Studies and Analyses.

Smith, C. (1994). *India's ad hoc arsenal: Arms procurement in historical perspective*. Oxford University Press.

Tarapore, A. (2020). *The Army in Indian Military Strategy: Rethink Doctrine or Risk Irrelevance* (s. 4) [Working Paper]. Carnegie India. Erişim Tarihi: 17.10.2022, https://carnegieindia.org/2020/08/10/army-in-indian-military-strategy-rethink-doctrine-or-risk-irrelevance-pub-82426

Wezeman, P. D., Kuimova, A., & Wezeman, S. T. /SIPRI. (t.y.). *Trends in International Arms Transfers, 2021*. 12.

Yadav, D. S. M. (2021, Mayıs 21). *An Assessment of India's Land Warfare*

Doctrine. Erişim Tarihi: 30.10.2022, https://www.claws.in/an-assessment-of-indias-land-warfare-doctrine/

Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2023,Cilt:12, Sayı:1, 25-44
doi:10.28956/gbd.1249381

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2023,Volume:12, Issue:1, 25-44
doi:10.28956/gbd.1249381

Makale Türü ve Başlığı / Article Type and Title
Araştırma/ Research Article
Orta Asya'nın Yapay Zekâ Jeopolitiği: Rusya ve Çin Örnekleri
The Geopolitics of Artificial Intelligence in Central Asia: Russian and Chinese Cases

Yazar(lar) / Writer(s)
Övgü KALKAN KÜÇÜKSOLAK, Assistant Professor, Department of International Relations, Yalova University, Türkiye okalkan@yalova.edu.tr, ORCID: https://orcid.org/0000-0002-3052-9728
Tuba FIRAT, Independent Researcher, tubafiraat@gmail.com, ORCID: https://orcid.org/0000-0001-7636-9232

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :09.02.2023
Makale Kabul Tarihi / Accepted :25.05.2023

Atıf Bilgisi / Citation:
Kalkan Küçüksolak Ö. ve Fırat T., (2023). The Geopolitics of Artificial Intelligence in Central Asia: Russian and Chinese Cases, *Güvenlik Bilimleri Dergisi, 12(1), ss 25-44. doi:10.28956/gbd.1249381*

THE GEOPOLITICS OF ARTIFICIAL INTELLIGENCE IN CENTRAL ASIA: RUSSIAN AND CHINESE CASES

Abstract

In the 21st century, the Artificial Intelligence (AI) technologies are increasingly transforming the instruments of power and contributing to intensifying rivalry on the dynamics of balance of power. In the context of the Central Asian geopolitics, China's expanding AI technologies do not only serve for its economic growth and national power, but embody future areas of uncertainty in the Sino-Russian relations. Despite the current state of a kind of 'entente cordiale' over their role in the Central Asia, the future developments in the AI technologies can reinforce far-reaching repercussions in their relations. In this vein, this study analyzes the implications of AI technologies in terms of power politics and discusses the future of Sino-Russian relations in the Central Asian context. It addresses the possible utilization of AI technologies under the context of military, economic, and political areas and discusses possible consequences on the future of regional systemic dynamics. Consequently, the study argues that despite ongoing harmonious relations between the two power, the development and utilization of AI as a strategic asset in the Central Asian landscape can generate new areas of strategic competition and challenges for the future of Sino-Russian relations.

Keywords: *The geopolitics of Artificial Intelligence, China, Russia, Central Asia, Sino-Russian relations*

ORTA ASYA'NIN YAPAY ZEKÂ JEOPOLİTİĞİ: RUSYA VE ÇİN ÖRNEKLERİ

Öz

Yirmi birinci yüzyılda "Yapay Zekâ" (YZ) teknolojileri güç araçlarını dönüştürmekte ve güç dengesinin dinamikleri üzerindeki rekabete katkıda bulunmaktadır. Orta Asya jeopolitiği çerçevesinde, Çin'in genişleyen YZ teknolojileri yalnızca ekonomik büyüme ve ulusal güce katkıda bulunmamakta, Rusya-Çin ilişkilerinin geleceği açısından da bilinmezlik unsurları barındırmaktadır. Hâlihazırda iki gücün Orta Asya'daki ilişkileri bir nevi 'antant kordial' çerçevesinde sürmekteyse de YZ alanındaki gelişmeler uzun dönemde söz konusu ilişkilerde olumsuz sonuçlar yaratabilecektir. Bu çalışma YZ teknolojilerinin olası sonuçlarını güç siyaseti çerçevesinde incelemekte ve Rusya-Çin ilişkilerini Orta Asya jeopolitiği düzleminde değerlendirmektedir. Araştırma kapsamında YZ teknolojilerinin askerî, ekonomik ve siyasi alanlarda araçsal olarak kullanılması ve uzun dönemde bölgesel sistemik dinamikler üzerindeki olası sonuçları konu edilmektedir. Son tahlilde, Rusya-Çin ilişkilerinin Orta Asya jeopolitiğinde uyumlu bir görüntü arz etmesine rağmen YZ teknolojilerinin stratejik bir unsur olarak kullanımının uzun dönemde söz konusu ilişkilerde meydan okumalara ve yeni stratejik rekabet alanlarına sebebiyet verebileceği tartışılmaktadır.

Anahtar Kelimeler: *Yapay Zekânın Jeopolitiği, Çin, Rusya, Orta Asya, Çin-Rusya İlişkileri*

INTRODUCTION

The 21st century is likely to be the theatre of strong technological transformations through the utilization of Internet of Things, 3D printers, Industry 4.0 and AI. Technology increasingly becomes the main source of power and area of competition in the global politics. Within the framework of technological transformation, it is seen that the next generation AI technologies are likely to play a decisive role on the future of power politics. In this context, this study aims to discuss the implications of AI technologies in terms of power politics and to make an analysis on its geopolitical impacts with a special focus on the Sino-Russian relations in the Central Asian landscape. Since Chinese technological initiatives seem to be challenging for the future of both regional and global dynamics, this study questions whether China's use of techno-political instruments with an aim to expand its engagement in the region will reinforce an area of controversy in the future of Russian-Chinese relations.

Despite the fact that, most of the studies in the IR literature emphasize a collaborative approach between China and Russia, China's rising power with a leading status in the AI technologies stands as a controversial question at the backyard of Russian Federation (RF). Therefore, in this study Chinese and Russian activities in the field of AI are examined under the context of military, economic and political issues with a special focus on the dynamics of power politics in the Central Asia. The study discusses the range of manifestations of power in AI policies and argues that Russian-Chinese relations can shift from a balanced relation of cooperation and competition to the one dominated by a strategic competition in the Central Asian landscape under the growing impacts of technological power elements in the long-term.

1. UNDERSTANDING THE CONTEXT OF THE AI STRATEGIES IN THE RUSSIAN AND CHINESE STRATEGY DOCUMENTS

AI increasingly occupies a greater role in the states' policy agendas for the future of power projection. In a quest for maximing the advanges of AI in diverse sectors, states set specific targets and institutionalize priorities in their strategic

documents. As a "strategic facilitator", the AI's huge potential in transforming the power instruments is highly recognized and increasingly found a place in the national strategy documents and power calculations of Russia and China.

In the case of RF, it is possible to see the ambitious target of achieving a global leadership role by the year 2030 as it is set out in its AI strategy of 2019. In the short-term, Russia's AI strategy includes the improvement of its position in the AI by the year 2024 and in this respect, it has already initiated a scientific agenda that combined the joint efforts of the state and the private sector (Markotkin & Chernenko, 2020). The RF's AI strategy underlines the significance of ensuring its national interests and sets out the guidelines for the development of an "information society" between 2017-2030 (Stanford University Human Centered Artificial Intelligence, 2021, p.9). The RF officially defines the AI within a broader framework by maintaining that "AI is a set of technological solutions that enables you to simulate human cognitive functions (including self-learning and search for solutions without a predetermined algorithm) and achieve results when performing certain tasks, at least comparable to the results of human intellectual activity" (Указ Президента Российской Федерации От, 2019). In addition to the strategic concerns, Russia's general AI strategy aims to utilize the commercial use of the AI facilities (Markotkin & Chernenko, 2020). In this vein, it is possible to claim that the RF perceives AI in a wider framework that ranges from human cognition to economic aspects which can have significant implications in a bid for global power competition.

China presents one of the most comprehensive AI strategy by incorporating diverse elements of AI technologies. China's AI strategy sets out ambitious targets of achieving a global leadership in the areas of unmanned aerial vehicles (UAVs), voice and image recognition, and others by 2025; and emerge as the primary center for AI innovation by 2030 (Stanford University Human Centered Artificial Intelligence, 2021, p.6). China's AI strategy outlines the significance of the areas of R&D and ethical norms, with a special emphasis on the notions of talent development and national security. China's multidimensional efforts include but not limited to the plans which aim to increase the value of its core AI sector to more than 400 billion yuan (about $58 billion), and to take the lead in the development of ethical standards for the works on AI. With this vision, China aims to double the growth in the core AI industry and to reach a value of 1 trillion yuan (about $147 billion) (Roberts et al., 2021). It is possible to say that China, which plans to make changes in laws and standards in order to realize all these targets, is

following a systematic and a comprehensive plan to become a global leader within the framework of AI. This systematic and determined vision not only underscores China's will to become a leader in the field of AI, but also raises further questions on the geostrategic implications of AI technologies and policies. In terms of power politics, the AI technologies can play an instrumental role in strengthening China's engagement with the Central Asian geography.

2. CHINA'S AI EFFORTS IN CENTRAL ASIA

With its abundant natural resources, transit routes and market capacity, Central Asia draws China's attention with its huge potential for Chinese products, investments and political ambitions (Schwartz & Montfort, 2020). The issues of access to energy sources and ensuring stability in Central Asia are crucial both for the realization of the Belt and Road Initiative (BRI) and to prevent threats emanating from the region (Mirza & Ayub, 2021, p.438). In its quest for more active role in the Central Asia, China utilizes AI technologies as an instruments of economic, political and military power. AI highlights and accelerates the dynamics of a cycle where technology and power reinforce each other, and in this context, it has the potential to help determine the international order for decades to come. Therefore, with its AI-based products and strategically holistic policies, China introduces a powerful dynamic both to the Central Asian geopolitics and to its relations with the RF.

2.1. Military Dynamics

In pursuit of new sources of competitive advantage, China not only focuses on the intelligentization of its army but also urges for increasing volume of military exports to the region. The rise of military made-in China AI technologies can have long-lasting results for the region. If China becomes the primary source of military AI technologies exporter, this can put the so-called regional de facto duopoly between Russia and China to a test and heighten the risk of new AI arms race in the region.

China and the RF have a balanced cooperation and competition in the Central Asian region. The dynamics of a balanced cooperation and competition encompass the notion of de facto duopoly between the two powers in which Russia leads the military and political stability spheres, where China leads the issue of economic development (Dubnov, 2018). However, recent years have witnessed a heightened level of China's military presence in the region through the means of joint

exercises, training of military personnel and the building of military infrastructure as well as increasing volumes of arms sales to the region. While China has previously provided 1.5 percent of the Central Asian arms imports between the years 2010-2014, this ratio has not only risen to 18 percent but even surpassed RF's arms exports volume to Turkmenistan and Uzbekistan in the last five years. Between the years 2016-2021, Central Asian states have imported modern weapons from China that included armed drones, communication equipment and UAV (Zanini, 2022, p.2). Despite the fact that the RF remains as a main security provider in the region, these developments reveal that China's spectrum of development goes beyond economic sphere to include the security sector in the Central Asia. While the RF lags behind on the development of the AI technologies, China's ambitious projects on the intelligentization of its military are likely to have future reflections on the increasing volume of its sophisticated military exports to the region. In the long-run, China's increasing profile in the security sector is likely to rise more questions on the future of the delicate balance of the so-called duopoly between Russia and China in the region.

2.2. Economic Dynamics

AI technologies constitute one of the most crucial sector of the Chinese domestic economy and its grand project of BRI. In 2020, the scale of China's AI industry has reached approximately 43.4 billion US dollars with an annual growth rate of 15 percentage (Huaxia, 2021). Considering the Plan entitled "A New Generation of Artificial Intelligence Development Plan" published by China in 2017, it is seen that China aims to become the largest economic power in the world with the contribution of AI (Westerheide, 2020). Companies like Baidu, Alibaba, and ByteDance are clearly at the forefront of AI research, and their products and services are integrating AI into the daily life in and outside of China (Marr, 2021).

Under the conditions of increasing global AI competition, the AI technologies offer broad opportunities for Chinese technology giants not only for the domestic market but also for the realization of Digital Silk Road (DSR). DSR is a digital component of BRI to promote digital connectivity and smart applications and hence plays a crucial role in China's Safe/Smart City projects in Central Asia[1].

[1] The distinction between "safe" and "smart" cities is not clear. While Safe Cities primarily aim to improve public safety through the use of cameras and digital technologies to monitor and inspect suspicious behavior, Smart City technology is mostly attributed to automating municipal functions such as traffic control, garbage collection, power distribution and water systems, along with video

Through the promotion of Safe/Smart City[2] projects in the region, China has taken a significant step in utilizing the opportunities of AI technologies as a foreign policy asset both in economic and political terms.

Started in Beijing, Jinan, Hangzhou and Suzhou as the four pilot cities in 2003, China's "Safe Cities Project" has initially aimed to meet the needs of manpower and consumers due to the urbanization in the Chinese cities (Lin, 2015). In the next phases, the process of building cyber-connected Safe/Smart Cities have developed further to spread Chinese Information and Communication Technologies (ICT) to the Central Asian landscape. In the digital age where data is the new currency, many Chinese surveillance companies take increasing parts to make profit under the umbrella of the DSR in which Smart Cities project play a prominent role (Yan, 2019). With the Smart Cities, China also aims to provide information to its industry and manufacturers on the extent of the production with the data obtained from monitoring the purchasing and social media behavior of the consumers in Central Asia. Therefore, China's considerable investment in AI technologies and digital connectivitiy through the DSR in the region reflects both the significance of AI technologies in economic growth and the strategic value of information in diverse areas.

Increasing export rates of smart technologies, such as 5G, to Central Asia create conditions of growing indebtedness and technological dependence on China. For instance, almost 40% of Kyrgyzstan's public debt and half of Tajikistan's public debt are due to Chinese banks (Hoagland et al., 2020). It should be noted that intensifying asymmetric dependencies can generate wide-reaching vulnerabilities both at the national and regional level. For example, in 2014 it was seen that China

surveillance (James Kynge, Valerie Hopkins, Helen Warrell, 2021). The term "Smart Cities" and "Safe Cities" are used interchangeably in the Chinese literature. For further info: (BBC Future, 2021), (BriefCam, 2021), (Safecity, 2021), (Jonathan E. Hillman, 2019), (卢佩珊, 2019).

[2] As one of the significant examples of Smart Cities project, the one established in Bishkek, Kyrgyzstan in 2019, has involved installations of fixed cameras at ten intersections and crossroads in the city. In the project, 15 Safe City cameras are placed on the Bishkek highway to monitor and record the actions (Ruowei, 2019). In the case of Tajikistan, a total of 1,200 cameras have been installed in the capital Dushanbe. The project was implemented by the Chinese Huawei with a cost of US$22 million, of which $20.91 million was a loan from China within the framework of the Shanghai Cooperation Organization (Ruowei, 2019). Within the Red Speed system under the scope of the Smart Cities project in Kazakhstan many violations such as crossing a red light and illegal parking have been monitored. In Turkmenistan, 133 cameras have been installed on the main roads and streets of Ashgabat under the project that has started in June 2009 (Ruowei, 2019).

has gained TBEA mining rights for gold mines after Tajikistan could not repay the loan to China (Hoagland et al., 2020). On the other side, it is noteworthy that China is very cautious on the aspects of its own vulnerabilities. As it is mentioned in the Article 11 of the State Security Law of the People's Republic of China, which provides the basis for contracting with Chinese technology companies, China may inspect electronic communication tools, equipment and other similar equipment and installations belonging to any organization or individual, when required by state security (Yi, 2021). This article states that all citizens of China, government officials, armed forces, political parties, popular groups, enterprises, public institutions and other social organizations have an obligation to ensure national security. This means that if something is labeled as a violation of national security, then the Chinese government can request information from Chinese technology companies, and the companies are obliged to provide the necessary information to the government. This fact clearly illustrates the range of China's access to variety of strategic sources, such as personal data, through the instruments of technological companies in diverse geographies, such as in Central Asia.

All arguments aside, under the conditions of technological superiority over Russia, China remains to be a principle option for the Central Asian states in the short term. However, in the long run Central Asian states can become more determined to decrease their dependence on Chinese technologies and hence choose to work with alternative companies such as the Russian ones. By diversifying different sources of technology, Central Asian states can prevent monopoly of any state and thus open the way for growing technological competition. Increasing dependencies on any state, in this case China, can be functional in exploiting vulnerabilities and achieving strategic gains.

2.3. Political Dynamics

China instrumentally uses growing number of cooperations in the areas of digital economy, e-commerce and AI to expand its presence in Central Asia. Under the context of the DSR, the Chinese project of Smart Cities have been launched with a special focus and a strategic role in adding greater value to China's leverage on Central Asia. In an atmosphere of increasing surveillance, there are sound reasons to claim that China's huge investment in Smart/Safe Cities can serve to alter the geopolitical dynamics of the region both through the increasing dependency on Chinese technologies and its increasing smart power in the region.

Despite the technological advances it provides, the scope of the China's data extraction raises serious concerns on the utilization of the AI technologies. Experts argue that although these systems promote advantages of convenience and cost savings, they still bring three basic risks in terms of socio-political spheres. Firstly, the ability of authoritarian governments to continuously monitor people brings the heightened risk of digital totalitarianism. Secondly, the usage of Chinese technologies carries the risk of access to sensitive data by the Chinese companies and the government. Thirdly, these technologies create vulnerabilities to an extent that it becomes easier for Chinese companies to press a button to shut down a city's activities (James Kynge, Valerie Hopkins, Helen Warrell, 2021).

China's role as a supplier of digital mechanisms for surveillance especially raises criticisms on the issue of exporting digital authoritarianism (Feldstein, 2019, p.48; Ramanand, 2022, p.14). By delinking trade from human rights, China's digital export policy not merely contributes to tightening control of the authoritarian regimes in the region but also reinforces increasing dependence on the Chinese technologies for the survival of these regimes. China's authoritarian control on information also reveals itself on the race for future technologies such as the AI chatbots. In the quest of developing AI tools similar to ChatGPT, Alibaba has recently released its Tongyi Qianmen AI chatbot. Following the launch of Tongyi Qianmen, the Cyber Administration of China was quick to unveil the draft rules concerning the functioning of these technologies (including the range of the content they are allowed to generate)[3]. Since these technologies can become an important stake at the future of AI race, whether countries in the Central Asia will prefer to use Chinese ones under the framework of strict regulations can become a matter of concern. In such a controversial issue, some analysts argue that these rules will slow down the technological progress in exchange for orderly society (Al Jazeera, 2023). However, in an authoritarian landscape such as the Central Asia, it will not be a surprise to see the common usage of Chinese chatbot technologies that undergo a security review by the authorities. On the fine line between innovation and censorship, this regulatory and restrictive approach can offer the opportunity to limit the content on politically sensitive issues and hence can be instrumental at the hands of authoritarian regimes.

[3]The draft rules include the prohibition of the content that questions state power, national unity, and socialist values (Bastian, 2023).

With a spatial analysis, China's advanced position in the AI is likely to produce significant geopolitical consequences in the region through its proactive digital export policy and increasing asymmetric dependencies in diverse areas. In the long run, increasing dependencies of authoritarian regimes can be weaponized in the political disputes and thus serve for China's national interests in the geopolitics of the region.

3. RUSSIA'S AI EFFORTS IN CENTRAL ASIA

By acknowledging the political implications both in the regional and global power competition, Russia highly concentrates on developing AI technology, especially on the military technology. Despite the fact that Russia seems to lag behind the US and China in the AI competition, it acknowledges very well the unlimited potential of the AI and accelerates its efforts to close the gap with the technology leaders. In that vein, the RF prioritizes investing on AI and follows the AI efforts of the US and China both in scope and expenditure (Bendett, 2018, p. 177).

Under the context of the implications of AI technologies to policy instruments, however, China and Russia follows different paths in the Central Asian landscape. While China focuses more on integrating AI technologies both to the military and civilian dimensions of its policy tools in Central Asia, Russia's AI efforts have been mostly limited to the military technologies in its regional vision. Under the conditions of RF's strong presence and interests in the region, China’s broadening role and holistic view in utilizing the AI technologies raise concerns on the risks of increasing competition within the Sino-Russian relations. To be able to grasp the emerging dynamics and the possible policy implications of the AI technologies in the region, this section analyses the RF's perception of utilizing AI technologies in the Central Asian geopolitical landscape.

3.1. Military Dynamics

The RF sees the significance of developing AI technology mostly from the security perspective (Nocetti, 2020, p.17). Under the context of increasing AI arms race for smart weapons, Russia has systematically focused on developing a robust strategy for using intelligent weapons technology, such as unmanned aircraft systems and robotic technology in warfare. The Russian drones play a critical role in monitoring the vast geography, such as the Arctic and parts of the Northern Sea Route, and the UAV is considered to be a valuable asset in responding to the asymmetrical opponents in the North Caucasus or Central Asia (Facon, 2016).

The RF has embarked on numerous initiatives to sophisticate its military, to integrate AI to its defense industry and to use these technologies in different theatres, such as in the Central Asia. The RF has begun to utilize the advanced military technologies in strengthening its engagement in the Central Asian landscape. For instance, while the Russian military base in Dushanbe-Tajikistan has received S-300 anti-aircraft missile systems in the fall of 2019, an agreement was signed between the Parliaments of Kyrgyzstan and Russia to allow the RF to deploy short and medium-range UAV unit in the Kant region in June 2020. According to the Agreement, two Orlan-10 multi-purpose UAVs are to be sent to Kyrgyzstan throughout 2020 to increase the effectiveness of the army and offensive aviation (Joint-Forces, 2020).

Despite Putin's ambitious perception of the capability of the AI technology, the RF seems to be slow to develop projects in the military aspects of the AI. While the Russian military began to conceptualize the term AI after the Army 2017 Military-Technical Forum, it was in August 2022 that the Russian Ministry of Defense has announced the official creation of an AI department for integrating the AI technology in weapons development (CNA, 2022, p.2). While it is difficult to assess the exact military AI capacity of the RF, the consequences of Russia's lag behind in the cutting-edge military technologies has already begun to be reflected in its military export to the Central Asian region. Despite the fact that the RF remains as the principal security partner and the largest arms supplier to the region (Pieper, 2022, p.30), its regional clients look for alternatives in importing UAV from different sources. For instance, to bridge the gap in unmanned aerial systems Kazakhstan has made a deal with Israeli Elbit Systems, where as Uzbekistan has opted for Chinese Wing Loong-1, and Turkmenistan has purchased Chinese CH-3 and WJ-600 armed drones (Zardykhan, 2022).

Under the current conditions of war with Ukraine and large sanctions on its defense sector, the future of the RF's defence sector to catch up with the AI military technologies seems to be ambiguous. While the RF continues to be the largest arms exporter to the region, the asymmetric power of the AI technologies as a strategic facilitator can serve to multiply the stake of the rival AI exporters in the region. Given the fact that the Central Asian region exhibits significant disruptions and dynamics of insecurities then the region carries a strong potential to become one of the most crucial theatre of operations for the AI military technologies. In this respect, it is possible to argue on the potential of the AI-based military

technology competition to pose challenges to the RF's 'dominant position' in the long run.

3.2. Economic Dynamics

Despite the fact that the RF's current AI development efforts mostly focuse on the security sector on the basis of foreign policy tools, the Russian national strategy attaches special importance to the development of AI with a view to increase its market share in the global market (Moscow, 2021). Since the range of AI based products, such as the ones used in China's Smart City Projects, can generate long term impacts on the foreign policy calculations, then the RF's domestic AI eco-system should be analyzed with a broader view.

The RF has launched a Digital Economy Programme in 2018 with an objective to use digital technologies to assist enterprises in integrating the function of automation (Sullivan, 2022).The RF frequently uses AI in industrial enterprises, banks, telecommunications, and retail sectors. Russia’s AI system is primarily managed by state-owned firms, a combination of the government and the private sector (Petrella et al., 2020). When we look at diverse examples, such as the US, the government plays a major role in funding some AI research and purchasing AI-enabled technologies, particularly in the defense sector, but most of the investments in applied AI are undertaken by private companies in the US. In China, private firms are the driving force behind technological progress, including AI, although state-owned firms play a larger role in the economy.

While Russia possesses substantial resources to devote to the AI projects, it still lags behind the main competitors in the short and medium term. Russia has some structural deficiencies that restrict the development and effective functioning of the AI ecosystem. The problematic areas in the AI sector include: shortage of personnel, weakness of venture capital market, brain drain, limited start ups and restricted space for the private sector companies. Russia's strict approach which capitalizes on state and leaves a very little room for private enterprises limits its ability to harness AI both in domestic and foreign spheres. This factor paves the way for low penetration of Russian products into foreign markets such as in the Central Asia (Bendett, 2022; Petrella et al., 2021, pp.75-79).

In the field of AI development, China has grown to be a significant partner for the RF. The technology sanctions of the US have motivated both nations to develop domestic alternatives to US semiconductors, operating systems and other technologies (Sullivan, 2022). In that vein, Russian-Chinese fund was founded to

pursue opportunities in new technologies and to invest in AI technologies such as facial recognition, computer vision, etc. Despite its technological advantages, part of the Russian elites maintain serious reservations about the future of the cooperation. In this respect the controversial issues of protection of intellectual property, share of AI innovation in military, and disaggregation of data produced in Russia are considered to be critical from the perspective of Russia's sovereignty. The concerns signalize the range of discontent on the basis of growing asymmetry between China and Russia in the technology field. Even under this cooperative framework, the long term trends of increasing asymmetry between the two powers can have repercussions not only for Russia's strategic autonomy but also for the balance of power in the Central Asia (Nocetti, 2020, p. 42).

3.3. Political Dynamics

Unlike the US and China, Russia is not positioned as a global leader in the AI technologies. Although the national strategy addresses the RF with a crucial capacity to become one of the global leaders in the development of AI technologies, it does not seem likely to succeed in this goal in the short run (Markotkin & Chernenko, 2020). According to the technology related indicators of AI, while China has 228 super-computers, the US has 117 super-computers and the RF has only 3 supercomputers that are among the 500 most powerful computers in the world currently (Markotkin & Chernenko, 2020). Therefore, despite Russia’s expertise in some of the specific areas of the AI development and applications, it is still possible to argue that it could only achieve a more pervasive success in different areas of AI as of today.

In October 2019, a national AI strategy on the development of AI was published by the Presidential Office of the RF. As Putin has stated in his speech in Moscow in 2017, Russia aims to prevent a monopoly of any country in the field of AI. The RF claims that if it stands as the leader of the development of AI, it will share its technology with the rest of the world, as it has already done previously on atomic and nuclear issues (Future of Life Institute, 2020). The RF's national strategy for the development of AI includes two crucial dates that symbolize its ambition for the leadership role in AI: the year 2024, as the RF is expected to significantly improve its position in the field, and the year 2030, a monumentary date to catch up with the developed countries and achieve its global purposes (Markotkin & Chernenko, 2020).

As compared to China's ambitious policies and assertive steps, Russia stays behind China especially on the digital arena. While China possesses a large domestic market and diverse capabilities, Russia lacks these conditions and faces technical difficulties that delay the nationwide deployment of deep package inspection tools (Weber, 2020). The Deep Packet Inspection (DPI) system reveals a systematic operation that analyzes Internet traffic and blocks the data flow of a particular service instead of blocking it all (Kolomychenko, 2018). In this term, Russia's attempt to ban Telegram in response to its refusal to comply with Russia's request to access to the encrypted messages of the users represents an example (Kolomychenko, 2018). Due to the technical insufficiencies, the Russian authorities, which have blocked access to many online services, such as Viber, Volvo, and Xiaomi, suspended the attempt to block Telegram. On the other hand, as a result of the disagreement between Kremlin and the cabinet of the federal government, there is a delay in the establishment of the DPI system. While the cabinet supports the installation of this equipment, Kremlin officials have stated that the new Internet isolation law has technically come into force but cannot be effectively implemented in all parts of the country (The Bell, 2019).

While China's approach to AI reveals its political aims related to the transition to a knowledge-based competitive economy, it can be argued that Russia basically focuses on AI-supported military weapons by improving its capabilities and subsequently aims to gain a serious advantage in AI technologies (Bekzod, 2021). Unlike China, the political leaders who are influential on Russia's AI policy have not handed over the strategy to institutional actors; instead, they directed the entire process of drafting strategies, developing AI technology, and executed related projects to politically connected people at the top of Russian state companies, such as Sberbank (Bekzod, 2021). Since internal institutional dynamics are significant in developing the architecture of the AI technologies then it is possible to discuss the possible consequences of AI technologies as a foreign policy tool in the long run. In that vein, it is likely that the strict domestic structure can pose significant challenges on the development of the RF's AI technologies which can have negative consequences on the competition of AI technology both on the regional and global scale.

CONCLUSION

The usage of AI technologies has become one of the strategic priorities for the big powers. As a strategic facilitator, the AI technologies offer wide range of opportunities to influence policy implications and geopolitical calculations. This

study argues that, the strategic utilization of AI technologies by Russia and China exhibits a strong potential to transform their cooperative relations and to fuel new areas of strategic regional competition in the long run.

Despite their crucial advantages, the AI technologies still comprise only a part of the power instruments. Therefore while a limited focus on the AI policy implications will remain insufficient to be able to explain the whole picture, it is still significant to shed light on the dynamics of transforming power relations. With a special reference to Putin's call for AI leadership on the way for global rule, this study maintains that both China and Russia devotes a special attention to the development of AI technologies for the future of balance of power.

For decades, Russia has positioned itself as the dominant power in its backyard, the Central Asia. However, despite Russia's strong presence, the patterns indicate China's growing stake in the region. China's development and utilization of AI technologies play a crucial role in its initiatives and active policies in the region. While Russia highly concentrates on the security sector of the AI under its foreign policy tools, China follows a holistic path to integrate AI technologies in diverse areas. China's strategic AI approach serves to reinforce increasing asymmetric dependencies with the regional countries and hence paves the risk of vulnerabilities in the face of China.

China systematically integrates new AI technologies to its economic and technological investments and continues to increase the export of smart weapons and military deployments in the Central Asia. By skillfully introducing the Smart Cities Project, China not only bolster economic and strategic spectrum of opportunities but also raises concerns on the issue of exporting digital authoritarianism to the region. In this respect, the instruments of AI technologies serve both to assist the authoritarian regimes and to facilitate asymmetric dependence on China. Despite the criticisms of exporting digital authoritarianism, China continues to sell surveillance technologies and increases its stake and influence in the Central Asian geopolitics.

Russia seems to lag behind China’s pace in the development of AI technologies despite its broad expertise and investments in the field. The RF has mostly focused on the AI technologies in the security sector as a foreign policy tool. Under the dynamics of Central Asian geopolitics, the RF mostly utilizes AI technologies in monitoring the vast geography and responding to asymmetrical opponents. Besides

this, Russia has been strengthening its military bases and facilities by integrating the AI based military technologies in the region.

China and Russia developed harmonious relations in recent years. The cooperative sides of the relations dominates the analysis in the literature, yet the complex and costly dynamics of the relations carry the potential to outweigh the benefits of the cooperation. In this respect, Central Asia can become a theatre of clashing national interests of the two powers and China's expanding spheres of influence can reinforce a shift in the direction of relations. While the AI is likely to transform into a competitive power instrument especially in the Central Asian landscape, the factors of China's ambitious utilization of AI technologies, increasing asymmetric dependencies in favour of China and Russia's technological inadequacy may generate serious imbalances and challenges in the upcoming period. Although the official Sino-Russian relations continue to be characterized by cooperation and strategic partnership, increasing Chinese engagement through the integrated policy instruments of AI technologies can exacerbate the competitive dynamics of the relations under the context of the Central Asian geopolitics in the long run.

REFERENCES

Al Jazeera. (2023). *As Alibaba Unveils ChatGPT Rival, China Flags New AI Rules.* Retrieved April 29, 2023 from https://www.aljazeera.com/news/2023/4/11/as-alibaba-unveils-chatgpt-rival-china-flags-new-ai-rules

Bastian, M. (2023). Alibaba Launches Its GPT-4 Competitor as Beijing Crashes the Chatbot Party. *The Decoder*. Retrieved April 30, 2023 from https://the-decoder.com/alibaba-launches-its-gpt-4-competitor-as-beijing-crashes-the-chatbot-party/

BBC Future. (2021*). Safe Cities: Using Smart Tech for Public Security*. Retrieved June 17, 2021 from http://www.bbc.com/future/bespoke/specials/connected-world/government.html

Bekzod, Z. (2021). *The Challenger and the Outsider: Why are China and Russia Interested in Promoting AI Development?* International Affairs House. Retrieved July 20, 2021 from https://www.internationalaffairshouse.org/the-challenger-and-the-outsider-why-are-china-and-russia-interested-in-promoting-ai-development/

Bendett, S. (2018). The Development of Artificial Intelligence in Russia. In N. D. Wright (Ed.), *Artificial Intelligence, China, Russia and Global Order*. Air University Press, 168-178.

Bendett, S. (2022). Russia's Artificial Intelligence Boom May Not Survive the War. *Defense One*. Retrieved April 28, 2022 from https://www.defenseone.com/ideas/2022/04/russias-artificial-intelligence-boom-may-not-survive-war/365743/

BriefCam. (2021). *Video Analytics For Safe & Smart Cities*. Retrieved June 28, 2021 from https://www.briefcam.com/who-we-serve/safe-smart-cities/

CNA. (2022). *Artificial Intelligence and Autonomy in Russia: A Year's Reflection*. Retrieved October 1, 2022 from https://www.cna.org/reports/2022/09/Artificial-Intelligence-and-Autonomy-in-Russia-A-Years-Reflection.pdf

Dubnov, A. (2018). *Reflecting on a Quarter Century of Russia's Relations With Central Asia*. Retrieved March 2, 2021 from https://carnegieendowment.org/2018/04/19/reflecting-on-quarter-century-of-russia-s-relations-with-central-asia-pub-76117

Facon, I. (2016). *A Perspective on Russia*. Retrieved March 8, 2021 from http://drones.cnas.org/reports/a-perspective-on-russia/

Feldstein, S. (2019). The Road to Digital Unfreedom: How Artificial Intelligence is Reshaping Repression. *Journal of Democracy,* 30(1), 40-52

https://doi.org/10.1353/jod.2019.0003.

Gigova, R. (2017). Who Vladimir Putin thinks will rule the world. *CNN*. Retrieved March 17, 2021 from https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html

Hoagland, R., Wolkov, N., & Karibayeva, A. (2020). *China's Growing Influence In Central Asia Through Surveillance Systems*. Retrieved May 13, 2021 from https://www.caspianpolicy.org/wp-content/uploads/2020/09/PB-Chinas-growing-influence-in-CA-through-surveillance-systems.pdf

Huaxia, E. (2021). *China's AI industry scale exceeds 40 bln USD in 2020*. Xinhua. Retrieved August 13, 2021 from http://www.xinhuanet.com/english/2021-07/09/c_1310052462.htm#:~:text=China%27s AI industry scale exceeds 40 bln USD in 2020

James Kynge, Valerie Hopkins, Helen Warrell, K. H. (2021). Exporting Chinese surveillance: the security risks of 'smart cities.' *Financial Times*. Retrieved August 18, 2022 from https://www.ft.com/content/76fdac7c-7076-47a4-bcb0-7e75af0aadab

Joint-Forces. (2020). *Orlan-10 UAV Systems For Kyrgyzstan*. Retrieved August 18, 2022 from https://www.joint-forces.com/defence-equipment-news/33546-orlan-10-uav-systems-for-kyrgyzstan

Jonathan E. Hillman, M. M. (2019). *Watching Huawei's "Safe Cities."* Retrieved August 15, 2022 from https://www.csis.org/analysis/watching-huaweis-safe-cities

Kolomychenko, M. (2018). Russia tries more precise technology to block Telegram messenger. *Reuters*. Retrieved June 20, 2022 from https://www.reuters.com/article/us-russia-telegram/russia-tries-more-precise-technology-to-block-telegram-messenger-idUSKCN1LF1ZZ

Lin, E. (2015). *China's safe cities serve as solutions and opportunities for growth*. Asmag. Retrieved July 15, 2022 from https://www.asmag.com/showpost /19628.aspx#:~:text=Safe Cities as a Solution,to as safe city projects.

Markotkin, N., & Chernenko, E. (2020). *Developing Artificial Intelligence in Russia: Objectives and Reality*. Carnegie Moscow Center. Retrieved June 21, 2022 from https://carnegie.ru/commentary/82422

Marr, B. (2021). China Poised to Dominate the Artificial Intelligence (AI) Market. *Forbes*. Retrieved May 13, 2021 from https://www.forbes.com/sites/ bernardmarr/2021/03/15/china-poised-to-dominate-the-artificial-intelligence-ai-market/?sh=23cd4d6d1b38

Mirza, M. & Ayub, S. (2021). Sino-Russian Competitive Collaboration for the Central Asian Sphere of Influence. *Journal of the Humanities and Social Sciences*, 2021, 25 (4), 437-450. https://doi.org/10.3176/tr.2021.4.04

Moscow, I. (2021). *Russian AI market overview*. Retrieved April 25, 2022 from https://ict.moscow/en/projects/ai/

Nocetti, J. (2020). *The Outsider: Russia in the Race for Artificial Intelligence*. Russie, Nei Reports, No.34, France.

Petrella, S., Miller, C., & Cooper, B. (2020). Russia's Artificial Intelligence Strategy: The Role of State-Owned Firms, *Orbis*, 65 (1), 75-100. https://doi.org/10.1016/j.orbis.2020.11.004

Pieper, M. (2022). *The Making of Eurasia: Competition and Cooperation Between China's Belt and Road Initiative and Russia*. Great Britain: Bloomsbury Publishing.

Ramanand, D. (2022). Sino-Russian Cooperation and Competition in Central Asia, *Journal of Defence Studies*, 16 (2), 3–30.

Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Luciano Floridi. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & Society*, *36*, 59–77. https://doi.org/10.1007/s00146-020-00992-2

Ruowei, L. (2019). *华为和中信国安投资超10亿美元发展乌兹别克斯坦数字基础设施 (Çev. Huawei ve CITIC Guoan, Özbekistan'ın dijital altyapısını geliştirmek için 1 milyar ABD) dolarının üzerinde yatırım yaptı*. Sliuxgc. Retrieved May 13, 2021 from http://web.siluxgc.com/UZ/20190426/16656.html

Safecity. (2021). *What is safecity?* Retrieved July 1, 2022 from https://www.safecity.in/

Schwartz, H. A., & Montfort, P. (2020). *Russia's Recent Military Buildup in Central Asia*. Center for Strategic & International Studies. Retrieved April 2, 2022 from https://www.csis.org/blogs/post-soviet-post/russias-recent-military-buildup-central-asia

Stanford University Human Centered Artificial Intelligence. (2021). *Artificial Intelligence Index Report 2021*. Retrieved April 20, 2022 from https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report-_Chapter-7.pdf

Sullivan, L. (2022). *Artificial Intelligence in Russia*. Geohistory. Retrieved May 25, 2022 from https://geohistory.today/artificial-intelligence-in-russia/

The Bell. (2019). *Russia is struggling to implement the nationwide DPI system it needs for 'Internet isolation.'* Meduza. Retrieved May 28, 2022 from https://meduza.io/en/news/2019/11/01/russia-is-struggling-to-implement-the-nationwide-dpi-system-it-needs-for-internet-isolation

Weber, V. (2020). *The Sinicization of Russia's Cyber Sovereignty Model*. Council on Foreign Relations. Retrieved June 1, 2022 from https://www.cfr.org/blog/sinicization-russias-cyber-sovereignty-model

Westerheide, F. (2020). China – The First Artificial Intelligence Superpower. *Forbes*. Retrieved May 20, 2021 from https://www.forbes.com/sites/cognitiveworld/2020/01/14/china-artificial-intelligence-superpower/?sh=3ed735cc2f05

Yan, Y. T. (2019). Smart Cities or Surveillance? Huawei in Central Asia. *The Diplomat*. Retrieved May 25, 2021 from https://thediplomat.com/2019/08/smart-cities-or-surveillance-huawei-in-central-asia/

Yi, X. (2021). *State Security Law of the People's Republic of China*. Ministry of National Defense of the People's Republic of China. Retrieved October 5, 2021 from http://eng.mod.gov.cn/publications/2021-06/29/content_4888389.htm

Zanini, A. (2022). *China's New Military Posture in Central Asia*. Retrieved July 26, 2022 from https://nesa-center.org/dev/wp-content/uploads/2022/05/2022-0426_Chinas-New-Military-Posture-in-Central-Asia.pdf

Zardykhan, Z. (2022). *Central Asia rushes into armed drone race as regional arms transfers brew: Drone diplomacy and geopolitics of arms race in Central Asia*. Global Voices. Retrieved August 30, 2022 from https://globalvoices.org/2022/07/07/central-asia-rushes-into-armed-drone-race-as-regional-arms-transfers-brew/

Указ Президента Российской Федерации от 10.10.2019 г. № 490, (2019) (testimony of ПРЕЗИДЕНТА РОССИЙСКОЙ ФЕДЕРАЦИИ). Retrieved August 30, 2022 from http://www.kremlin.ru/acts/bank/44731

卢佩珊. (2019). *2019年 中国人工智能行业政策解读概览*. Retrieved August 31, 2022 from https://pdf.dfcfw.com/pdf/H3_AP202008061396710412_1.pdf?1596711832000.pdf

Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2023,Cilt:12, Sayı:1, 45-68
doi:10.28956/gbd.1134222

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2023,Volume:12, Issue:1, 45-68
doi:10.28956/ gbd.1134222

Makale Türü ve Başlığı / Article Type and Title

Araştırma/ Research Article

AB'nin Bağımsız Bir Güvenlik ve Savunma Politikası Geliştirme Düşüncesi ve Stratejik Pusula

The EU's Thought to Develop aAn Independent Security and Defense Policy and the Strategic Compass

Yazar(lar) / Writer(s)

Gökhan AKŞEMSETTİNOĞLU, Doç. Dr., Çankaya Üniversitesi, İ.İ.B.F. Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, gokhana@cankaya.edu.tr, ORCID: https://orcid.org/0000-0002-6990-6834

Bilgilendirme / Acknowledgement:

-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :22.06.2022
Makale Kabul Tarihi / Accepted :06.09.2022

Atıf Bilgisi / Citation:

Akşemsettinoğlu G., (2023). AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesi ve stratejik pusula. *Güvenlik Bilimleri Dergisi, 12(1), ss 45-68. doi:10.28956/gbd.1134222*

AB'NİN BAĞIMSIZ GÜVENLİK VE SAVUNMA POLİTİKASI İLE STRATEJİK PUSULA

Öz

Soğuk Savaş Dönemi'nde Amerika Birleşik Devletleri (ABD) ve Kuzey Atlantik Antlaşması Örgütü – North Atlantic Treaty Organization (NATO) odaklı bir güvenlik ve savunma politikası benimsemek zorunda kalan Avrupa Birliği (AB), üzerinde uzun zamandır tartıştığı bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesini hayata geçirme fırsatı bulamamıştır. Ancak Soğuk Savaş sonrası dönemde uluslararası sistemin yapısının değişmesi, tehditlerin farklılaşması ve AB'nin özellikle son on yıl içinde yaşadığı iç ve dış krizler, üye devletlerin bağımsız bir güvenlik ve savunma politikası geliştirme konusundaki girişimlerini önemli ölçüde artırmıştır. Bu çalışmanın amacı, AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesini, zaman içinde duyurduğu stratejiler çerçevesinde hangi düzeyde hayata geçirebildiğini araştırmaktır. Çalışma, AB'nin bağımsız bir güvenlik ve savunma politikasını ABD ve NATO'ya rağmen değil, ABD ve NATO ile işbirliği içinde gerçekleştirebileceğini ortaya koymaktadır. Çalışma, bu varsayımı desteklemek için de kısa süre önce duyurulan Stratejik Pusula ile açıklanan yeni yaklaşıma vurgu yapmaktadır. Nitel araştırma metodu içinde yer alan nitel veri toplama yöntemlerinden doküman/metin analizini kullanan bu çalışma sonuç olarak, Stratejik Pusula ile duyurulan yeni anlayışın AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesini, ABD ve NATO ile işbirliği içinde ileri taşıyabileceğini ortaya koymaktadır.

Anahtar Kelimeler*: Avrupa Birliği, Ortak Güvenlik ve Savunma Politikası (OGSP), Küresel Strateji, Stratejik Pusula, Avrupa Bütünleşmesi.*

THE EU'S INDEPENDENT SECURITY AND DEFENSE POLICY AND THE STRATEGIC COMPASS

Abstract

The European Union (EU), which had to adopt a security and defense policy dependent on the United States of America (USA) and North Atlantic Treaty Organization (NATO) during the Cold War, could not find the opportunity to implement the idea of developing an independent security and defense policy, which it had been focusing on for a long time. However, after the cold war, the change in the structure of international system, alteration of threats and internal and external crisis that EU went through during the last decade increased the attempts of the member states to develop an independent security and defense policy. The aim of this study is to investigate at what level the EU implemented the security policy announced the idea of developing an independent security and defense policy. The study reveals that the EU can realize an independent security and defense policy not in spite of the USA and NATO, but in cooperation with the USA and NATO. To support this assumption, the study emphasizes the new approach described in the recently announced Strategic Compass. This study, which uses document/text analysis of the qualitative data collection method, finally reveals that the new understanding announced by the Strategic Compass can advance the EU's idea of developing an independent security and defense policy in cooperation with the USA and NATO.

Key words*: European Union, Common Security and Defence Policy (CSDP), Global Strategy, Strategic Compass, European Integration.*

GİRİŞ

1992 yılında imzalanan Avrupa Birliği (AB) Antlaşması ile Ortak Dış ve Güvenlik Politikası (ODGP) konusunda somut adımlar atan AB üyeleri, AB'nin dış ilişkilerine askerî bir boyut kazandırabilmek için de 1998 yılında yapılan St. Malo Zirvesi'nde AB'nin bağımsız bir güvenlik ve savunma politikası oluşturması yönünde ortak bir karar almıştır. Bu karar çerçevesinde AB, 1999 yılında yapılan Köln ve Helsinki Zirveleri'nde bir Avrupa Güvenlik ve Savunma Politikası (AGSP) oluşturulması hakkında ilkeler belirlemiştir. 2009 yılında yürürlüğe giren Lizbon Antlaşması, Ortak Güvenlik ve Savunma Politikası (OGSP) olarak yeniden isimlendiren söz konusu güvenlik ve savunma politikasına hukuki bir nitelik kazandırmıştır.

İkinci Dünya Savaşı'ndan sonra Avrupa'nın güvenliği 1949 yılında Amerika Birleşik Devletleri'nin (ABD) liderliğinde kurulan Kuzey Atlantik Antlaşması Örgütü (North Atlantic Treaty Organization - NATO) tarafından sağlanmaktadır. AB üyelerinin büyük çoğunluğunu bünyesinde barındıran NATO (22 devlet hem AB hem de NATO üyesidir), Soğuk Savaş dinamiklerine göre planlanmış ve Avrupa'daki devletleri Sovyetler Birliği'ne karşı kolektif güvenlik yapısı içinde korumuştur. Ancak, Soğuk Savaş sonrası dönemde Sovyet tehdidinin ortadan kalkması, bir yandan Avrupa'daki devletlerin NATO'ya olan ihtiyaçlarını sorgulamalarına neden olurken diğer yandan da AB'yi oluşturan üye devletlerin güvenlik ve savunma konusunda bağımsız politikalar geliştirme isteklerini tetiklemiştir. Özellikle son on yıl içinde sınırları dâhilinde yaşadığı terör saldırıları ile yakın çevresinde meydana gelen çatışmalar, AB'nin bağımsız bir güvenlik ve savunma politikası oluşturma kararının uygulamaya geçirilmesi ihtiyacını öne çıkarmıştır. Soğuk Savaş Dönemi'nde Avrupa'nın güvenlik ve savunmasını üstlenen ABD ve NATO ile Soğuk Savaş sonrası dönemde bağımsız bir güvenlik ve savunma politikası geliştirmek isteyen AB'nin ortaya koyduğu politikaların ve eylemlerin aynı hedefe yönelmesi, akademik çevrelerde sıkça tartışılmıştır.

Bu çalışma, AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesini, Soğuk Savaş sonrası dönemde yaşanan tarihi tartışmalar ve siyasi-askerî gelişmeler çerçevesinde araştırmaktadır. Çalışmanın amacı, AB'nin söz konusu politikasını, zaman içinde duyurduğu stratejilerle hangi düzeyde gerçekleştirebildiğini ortaya koymaktır. Çalışma, yakın zamanda duyurulan Stratejik Pusula'da da açıklandığı gibi AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesini ancak ABD ve NATO ile işbirliği içinde

gerçekleştirebileceği sonucuna varmaktadır. Bu çalışma, literatürdeki diğer çalışmalardan farklı olarak, AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesini ve bu konuda attığı somut adımları, sadece daha önce duyurduğu stratejiler çerçevesinde değil, Avrupa Konseyi'nin 24-25 Mart 2022 tarihinde yaptığı zirvede kabul ettiği "Stratejik Pusula" ile oluşan yeni çerçeveyi de içine alarak bir bütün olarak değerlendirmektedir. Nitel araştırma metodu içindeki nitel veri toplama yöntemlerinden doküman/metin analizini kullanan bu çalışma, AB'ye ait kurumsal yazılı dokümanları incelemekte, literatüre katkı sağlayan diğer araştırmacıların eserlerine referans vermekte ve tümevarım yaklaşımı içinde bütüncül bir anlayış geliştirmeyi amaçlamaktadır.

Bu çalışma üç bölümden oluşmaktadır. Çalışmanın birinci bölümü, AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesi hakkındaki tarihi tartışmalara odaklanmakta ve AB'nin Soğuk Savaş sonrası dönemde ABD'den bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesinin sebepleri üzerinde durmaktadır. Çalışmanın ikinci bölümü, AB'nin güvenlik ve savunma politikasını eyleme dönüştürmek için hazırladığı güvenlik stratejileri hakkındadır. Bu bölümde ağırlıklı olarak Küresel Strateji ile yeni duyurulan Stratejik Pusula üzerinde durulmaktadır. Çalışmanın üçüncü bölümü, makalenin genel değerlendirmesini yapmaktadır. Bu bölüm, AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme girişimini, AB'nin ABD ve NATO ile olan ilişkileri üzerinden yorumlamaktadır. Bu bölümde özellikle Stratejik Pusula ile ortaya koyulan yeni güvenlik ortamı tanımlanmış ve AB'nin güvenlik ve savunma politikası, güncel gelişmeler ışığında değerlendirilmiştir.

1. SOĞUK SAVAŞ SONRASINDAKİ TARTIŞMALAR VE GELİŞMELER

Güvenlik, her zaman topluluk hâlinde yaşayan insanlar için temel bir endişe kaynağı olmuş ve insanların istikrarlı bir güvenlik ortamı yaratma çabaları, siyasal yaşamın önemli bir parçasını oluşturmuştur (Birdişli, 2020: 255). Günümüzde ulus-devletlerin, ulus-üstü bölgesel örgütler ve ulus-altı sivil toplum kuruluşları gibi diğer aktörlerle hareket etmek durumunda kalması, egemenliklerinin ancak söz konusu aktörlerle birlikte tanınmasını gerektirmiştir (Keyman, 2006: 12). Bu da güvenlik kavramının "ulusal" ile "diğer" arasındaki farklılıklar göz önüne alınarak yeniden değerlendirilme ihtiyacını ortaya çıkarmıştır (Aydın-Düzgit, 2015: 100). Bu çerçeve içinde, ulus-üstü bölgesel bir örgüt olan AB de özellikle Soğuk Savaş sonrası dönemde bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesiyle, uluslararası güvenlik çalışmaları içinde kendine bir yer bulabilmiştir.

Tarih içinde çatışmalara çözüm bulunan dönemler istikrarlı barış ortamları yaratırken, çatışmaların olmadığı durumlar da belirsiz dönemler olarak tanımlanmıştır (Rumelili, 2018: 284). Soğuk Savaş sonrası dönem de söz konusu belirsizliğin yaşandığı bir dönem olarak, AB üyesi devletlerin güvenliklerini sağlamak için zorlanmalarına sebep olmuştur. Soğuk Savaş ertesinde AB'nin ABD'den ve NATO'dan bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesi, farklı tartışmaları gündeme getirmiştir. Bu tartışmalar, sonraki yıllarda AB'nin bağımsız bir güvenlik ve savunma politikası geliştirmesinin temel sebeplerini oluşturmuştur. Bu çerçeve içinde, önce söz konusu tartışmalar, sonra da sebepler üzerinde durmak faydalı olacaktır.

1.1. AB'nin Bağımsız bir Güvenlik ve Savunma Politikası Geliştirmesi Hakkındaki Tartışmalar

AB, Soğuk Savaş sonrasında ABD ve NATO'dan bağımsız bir güvenlik ve savunma politikası geliştirmek istediğini değişik platformlarda açıklamış ve konu ile ilgili politikaların geliştirilmesine hız vermiştir. AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme girişimi, uluslararası alanda değişik düzeylerde tartışma konusu olmuştur. AB'nin bu girişimi ilk olarak, Soğuk Savaş sonrası değişen dinamikler çerçevesinde, AB'nin ABD ve NATO'ya karşı uygulamayı planladığı bir dengeleme politikası olarak tartışılmıştır. AB'nin söz konusu girişimi ikinci olarak, transatlantik düzeyde, AB ile ABD arasında yaşanan sorunların bir yansıması olarak sorgulanmıştır. Bu konu üçüncü olarak, üye devletlerarasındaki fikir ayrılıkları çerçevesinde değerlendirilmiştir. Üye devletlerarasındaki fikir ayrılıklarıyla ilgili değerlendirme aynı zamanda AB'nin güvenlik ve savunma konusunda neden yeteri kadar başarılı sonuçlar elde edemediği hakkında bir fikir de vermektedir. Bu üç konu hakkında fikir sahibi olmak, AB'nin söz konusu girişiminin tarihi alt yapısını hatırlatmak anlamında önem taşımaktadır.

AB'nin bağımsız bir güvenlik ve savunma politikası oluşturma girişimi ilk olarak ABD ve NATO düzeyinde sorgulanmıştır. Bu girişimin ABD ve NATO'ya karşı bir dengeleme politikası olup olmadığı tartışılmıştır. Bu konuda Posen (2006: 150), AB'nin bağımsız bir güvenlik ve savunma politikası oluşturma çabasının ABD'yi uluslararası alanda dengelemek olmadığını belirtmiştir. Yazara göre AB; ABD gibi liberal politikalara sahip, hukukun üstünlüğü, demokrasi, insan hakları gibi ortak değerlere inanan devletlerin oluşturduğu bir örgüt olarak ABD'yi bir tehdit olarak görmemektedir. Bu konuda Press-Barnathan (2006: 273), AB üyesi devletlerin ABD'den kaynaklanan herhangi bir tehdit algılamadıkları için AB'nin

ABD'ye karşı güç dengesi politikası izlemesinin söz konusu olmadığını açıklamıştır. Narramore (2008: 97) da AB'nin Soğuk Savaş sonrasında Çin ile geliştirmeye çalıştığı stratejik ortaklığın, ABD'ye karşı bir girişim olarak görülmemesi gerektiğini ifade etmiştir.

Genel görüş, AB'nin söz konusu girişiminin ABD'yi uluslararası alanda dengelemeyi hedeflemediği yönündedir. Bunun bir sebebi, AB ile ABD'nin birçok konuda ortak hareket etmesidir. Calleo (2008: 10), tarafların uluslararası sistem içinde son derece başarılı olduğunu ancak her iki aktörün de başarısını diğeri sayesinde elde ettiğini vurgulamıştır. Jones (2006: 267) da AB'nin ABD'den bağımsız bir güvenlik ve savunma politikası geliştirmesinin, AB ile ABD'yi birbirine yakınlaştıracağını ifade etmiştir. Yazara göre AB, bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesi içinde, yeni teknolojiler üzerinde çalışarak ve yeni silahlar geliştirerek, ABD ile ortak politikalar yapma imkânını artıracaktır. Dolayısıyla, AB ile ABD arasındaki ilişkiler, her iki aktörün üçüncü ülkelerle olan ilişkilerinden çok, kendi aralarındaki ilişkileri tarafından belirlenecektir (Wang, 2009: 450). Benzer biçimde, hiçbir devlet uzayda tek başına başarılı olamayacağı için, ABD de uzay programı için bir ortağa ihtiyaç duymaktadır. Bu durumda, ABD'nin en yakın ortağı AB olacaktır. Drath (2007: 409), AB ile ABD'nin uzay programı gibi ortak çıkarlar üzerine daha fazla odaklanmaları gerektiğini, böylece sorunların çözümünün daha kolay olabileceğini vurgulamaktadır.

AB ile ABD arasındaki ortaklığa vurgu yapan bir başka gelişme de Fransa'nın ABD karşıtı politikasını zaman içinde değiştirmiş olmasıdır. Merand (2010: 345), Fransa'nın NATO'nun askerî kanadına geri dönmesini, Avrupa'da ABD ve NATO müttefikliğinin pekişmesi olarak açıklamaktadır. Yazara göre Fransa'nın bu kararı her ne kadar AB ile NATO arasındaki problemleri ortadan kaldırmasa da Fransa eski söylemlerini gündeme getirmeyecektir. Fransa'nın NATO'nun askerî kanadı içinde yeniden yer alması, Fransa'nın ABD'den bağımsız bir AB oluşturma sürecine destek verirken ABD'yi de tehdit etmeyeceği bir durum yaratmıştır (Mahncke, 2009: 84).

AB'nin ABD'yi uluslararası alanda dengelemeyi hedeflemediği yönündeki anlayışı destekleyen bir diğer görüş de Soğuk Savaş sonrasında ABD'nin yanında yer alma politikasının daha kazançlı olacağı yönündedir. Örneğin, Wivel (2008: 295) Soğuk Savaş ertesinde uluslararası sistemde tek güç olarak görünen ABD'ye karşı denge politikası izlemek yerine işbirliği yapmanın AB üyesi devletler için

daha kazançlı olacağını ifade etmektedir. Dyson (2008: 770), ABD'nin yanında yer alma politikasının risk-maliyet analizi yapıldığı zaman en az riske sahip politika olduğunu, bunun düşük düzeyde de olsa ABD'yi etkileme yollarından biri olduğunu belirtmektedir. Hyde-Price (2006: 224) da ABD'nin yanında yer alma politikasının özellikle güçsüz devletler için ABD'den daha çok yararlanmanın ve uluslararası sistem içinde daha fazla söz sahibi olmanın bir yolu olabileceğini vurgulamaktadır.

AB'nin bağımsız bir güvenlik ve savunma politikası oluşturma girişimi ikinci olarak AB ile ABD arasındaki transatlantik anlaşmazlıklar üzerinden tartışma konusu olmuştur. Bu konuda, AB'nin girişiminin AB ile ABD arasında yaşanan sorunların bir yansıması olup olmadığı tartışılmıştır. Bu konu ile ilgili olarak Kanet (2008: 231), AB ile ABD arasındaki anlaşmazlıkların daha çok "stratejik uyumsuzluk" ve "parçalanmış güvenlik alanı" ile ilgili olduğunu belirtmiştir. Yazara göre, AB ile ABD arasındaki ilişkiler Soğuk Savaş sonrası dönemde değişmeye başladığı için transatlantik güvenlik projesi gibi bazı girişimler, yeni gelişmelere ve tehditlere cevap veremediğinden başarısızlığa uğramıştır. Ayrıca, AB üyesi devletler ile ABD arasında ideolojik farklılıklar da vardır. ABD liberal-idealist olmasına rağmen AB üyesi devletler realisttir. Örneğin; AB, ABD'den bağımsız olarak oluşturmaya çalıştığı güvenlik ve savunma politikasını "gerçek çıkarlarını" göz önüne alarak yapmaktadır (Antoniades, 2008: 332).

AB'nin bağımsız bir güvenlik ve savunma politikası oluşturma girişimi üçüncü olarak üye devletlerarasındaki fikir ayrılıkları çerçevesinde değerlendirilmiştir. Kanet (2008: 231), AB ile ABD arasındaki anlaşmazlıkların sebebi olarak AB üyesi devletlerin kendi aralarında yaşadıkları fikir ayrılıklarını göstermiştir. Yazar, üye devletlerin kendi aralarında gruplara bölünmüş olmaları ve her grubun da kendine özgü politika tercihlerinin bulunması dolayısıyla üye devletlerin ortak politika oluşturma konusunda tereddüt yaşadıklarını belirtmiştir. Tocci (2016: 462) de üye devletlerarasındaki fikir ayrılıklarına dikkat çekmiştir. Yazara göre, bazı üye devletler güvenlik ve savunma konusunda cesur adımlar atarak bağımsız bir politika geliştirmek istemelerine rağmen, bazı üye devletler de NATO'nun üstünlüğüne meydan okunmaması konusunda ısrar etmiştir. Bu fikir ayrılıkları üye devletlerarasında çekişmelere, hatta zaman zaman düşmanlıklara sebep olmuştur.

AB üyesi devletlerin güvenlik ve savunma ile ilgili olarak farklı fikirlere sahip olmaları hem AB'nin bağımsız bir güvenlik ve savunma politikası oluşturması düşüncesinin hayata geçirilmesini zorlaştırmış hem de AB'nin ABD ve NATO ile

hangi düzeyde ilişki kurması gerektiği konusunu karmaşıklaştırmıştır. Örneğin, Fransa her zaman AB'nin ABD'den bağımsız bir savunma kapasitesine sahip olması gerektiğini ifade etmiştir. Ancak Almanya, siyasi ve askerî olarak tarihten gelen kısıtlamalar yüzünden yeteri kadar serbest hareket edemeyecek durumda olduğu için, kurumsal olarak güçlü bir AGSP düşünürken NATO ile ilişkilerinin de sağlam bir şekilde devam etmesini istemiştir (Diedrichs, 2005: 56).

Aslında Soğuk Savaş sonrasında AB üyesi devletlerarasında güvenlik ve savunma konularıyla ilgili temel farklılık, Fransa ile İngiltere arasında görülmektedir. Örneğin; bu konuda Oswald (2006: 153), Fransa'nın Saint Malo'da AGSP konusunda yaptığı önerinin gerçekten Avrupa'nın ABD'den bağımsız bir güvenlik ve savunma politikası geliştirmesi düşüncesini yansıttığını ancak İngiltere'nin daha çok NATO'yu güçlendirecek bir politika izlemesi yönünde bir düşünce benimsediğini belirtmektedir.

İngiltere ile ilgili olarak genel bir değerlendirme yapan Layne (2006: 32), İngiltere'nin İkinci Dünya Savaşı'ndan sonra ABD ile Sovyetler Birliği arasında üçüncü bir güç olarak ortaya çıkmak istediğini ancak bu isteğini destekleyecek önemli bir askerî gücü olmadığı için bu düşüncesinin başarısızlığa uğradığını belirtmektedir. 1940'lı yıllarda ABD'nin etkisinden kurtulabilmek için uğraşan ama bunu başaramayan İngiltere, sonraki yıllarda net bir şekilde ABD'nin yanında olma politikası izlemiştir. Shambaugh (2005: 12) da AB üyesi devletlerarasındaki fikir ayrılıklarının, bu devletlerin uluslararası sisteme bakışlarının farklı olmasıyla da açıklanabileceğini belirtmiştir. Yazar; Fransa, Almanya, BENELÜKS (Belçika, Hollanda, Lüksemburg) ülkeleri, İskandinavya ve Akdeniz ülkelerinin çok kutuplu bir uluslararası düzeni savunduğunu ancak İngiltere ile Merkezi ve Doğu Avrupa Ülkeleri'nin (MDAÜ) bütünleşmiş bir Avrupa özlemini dile getirmelerine rağmen, çok kutupluluğa sıcak bakmadıklarını vurgulamıştır.

AB üyesi devletlerin yaşadıkları fikir ayrılıkları, hem kendi aralarında bağımsız bir güvenlik ve savunma politikası geliştirmelerini zorlaştırmış hem de AB'nin bağımsız bir güvenlik ve savunma politikası geliştirmesi düşüncesi ile ABD ve NATO ile işbirliği yapma zorunluluğu arasında sıkışmasına sebep olmuştur. Ancak yine de üye devletler, zaman içinde değişen görüşleri ve farklılaşan uluslararası gündem sayesinde ortak bir payda altında buluşabilmişlerdir (Toje, 2008: 212). AB üyesi devletler bağımsız bir güvenlik ve savunma politikası oluşturma konusunda eyleme geçebilmenin yanında, ABD ve NATO ile işbirliğini devam ettirmenin yolunu da bulabilmişlerdir.

1.2. AB'nin Bağımsız bir Güvenlik ve Savunma Politikası Geliştirme Düşüncesinin Sebepleri

AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesinin ve güvenlik ile savunmayı bir kurumsal yapı içine oturtmaya çalışmasının en göz önündeki sebebi, ABD'nin özellikle Avrupa'nın güvenliği ve savunması ile ilgili konularda karar alırken bunu çoğunlukla kendi başına yapması ve AB'yi zaman zaman bu sürecin dışında bırakmasıdır. AB de bu olumsuz durumdan etkilenmemek için kendi bağımsız güvenlik ve savunma yapısını oluşturmayı amaçlamıştır (Wivel, 2008: 295). Bu durumda AB, ABD'nin Avrupa'ya sağladığı güvenlik desteğini daha az hissederken, ABD de Avrupa'daki askerî mevcudiyetini azaltmaya başlamıştır (Oswald, 2006: 153). Aslında AB üyeleri arasında bağımsız bir güvenlik ve savunma politikasının oluşması için en uygun ortam, ABD'nin Soğuk Savaş sonrasında güçlerini kısmi de olsa Avrupa'dan çekmeye başlamasıyla ve oluşan kısmi güç boşluğunun AB tarafından doldurulmasına fırsat tanımasıyla ortaya çıkmıştır. ABD'nin Avrupa'ya olan ilgisinin gittikçe azalması; uluslararası kriz yönetimi yeteneklerine olan talebin artması ve hem Avrupa'da hem de küresel anlamda bütün dünyada güç dengesi kavramının değişmeye başlaması AGSP konusunun önem kazanmasına sebep olmuştur (Irondelle ve Merand, 2010: 35-40).

AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesinin bir diğer sebebi, AB'nin ABD ile güvenlik ve savunma konusunda işbölümü yapmak istemesidir (Press-Barnathan, 2006: 273). Bu anlamda AB, ABD'nin ve NATO'nun uluslararası alandaki ortağı olarak değerlendirilebilir. Örneğin, Afganistan gibi siyasi-askerî konular, NATO üyelerinin enerjilerinin büyük bir kısmını aldığı için AB, AGSP aracılığıyla ABD'nin daha küçük çaplı operasyonlarını yürütme görevini üstüne almıştır (Irondelle ve Merand, 2010: 37). Askerî anlamda, AB üyesi devletler için AGSP ile tanımlanan ortak payda "kriz yönetimi" için bir araç olması (Schroeder, 2009: 492), NATO'nun askerî yeteneklerine ilave bir güç kazandırması ve AB'ye, AB'nin dış ilişkilerinde askerî araçlar sağlamasıdır (Menon ve Sedelmeier, 2010: 77). Siyasi anlamda ise AB üyesi devletler için AGSP, AB'nin ODGP ile ortaya koyduğu siyasi bütünleşme düşüncesini destekleyen önemli bir araç olmasıdır (Duke, 2008: 28).

AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesinin bir başka sebebi, AB'nin güvenilir bir uluslararası aktör olmak istemesidir. Bu konuda Posen (2006: 150), AB'nin gerçek anlamda bir uluslararası aktör olması için, ekonomik ve parasal birlik için önemli adımlar attıktan sonra dış politika konusuna

ağırlık vermesi gerektiğini vurgulamaktadır. Wivel (2008: 295) için de bir aktörün siyasi olarak söz sahibi olması, onun askerî olarak da güçlü olmasına bağlıdır. Buna göre, AB'nin, barış sağlama ve çatışma önleme yoluyla askerî yeteneğini artırması, kendisini uluslararası sistem içinde önemli bir aktör konumuna ulaştırabilecektir (Eriksen, 2006: 252). Dolayısıyla, AB'nin dış politikada işbirliğini geliştirmek için ortaya koyduğu faaliyetler, AB'nin oynamak istediği "uluslararası ilişkilerin mimarı" rolüne meşru bir örnek olarak gösterilebilir (Bickerton, 2010: 218). Çin ile kapsamlı bir stratejik ortaklığa gitmesi, Güneydoğu Asya'da enerji ile ilgili örgütlere aktif olarak katılması ve Rusya ile işbirliği konusunda anlaşmalar yapması, AB'nin çok taraflılık konusundaki somut faaliyetlerini gözler önüne sermektedir (Maull, 2005: 798). Gelişen çok taraflılık yapısı içinde AB, dış politika konusunda daha cesur adımlar atmaya başlayacak, bu da farklı bölgesel güçlerin çok kutuplu bir yapıya ayak uydurmalarını kolaylaştıracaktır (Fischer, 2006: 266).

AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesinin bir diğer sebebi, ABD'nin transatlantik ilişkiler sebebiyle yüklenmek zorunda kaldığı maliyetin, AB tarafından paylaşılması görüşüdür. AB üyesi devletler güvenlik ile ilgili yeni düzenlemeleri kendi bağımsızlıklarına katkı sağlayacak girişimler olarak algılamalarına rağmen, ABD söz konusu girişimi, üzerinde bulunan mali yükü AB kaynakları ile paylaşma fırsatı olarak görmektedir (Wivel, 2008: 295). AB, kendi başına küresel bir düzen oluşturma konusunda yeteri kadar etkili olamayacağı için AB üyesi devletlerin diğer aktörlerle işbirliği içinde çalışacağı varsayılabilir. Bu anlamda, AB ile ABD arasındaki ortaklık ilişkisinin, transatlantik zeminde son derece önemli olacağı öngörülebilir (Poettering, 2007: 29).

AB'nin geliştirmeye çalıştığı bağımsız güvenlik ve savunma politikası geniş çerçevede değerlendirildiğinde, AB'nin Avrupa bütünleşme projesi içinde önemli bir adım attığı anlaşılmaktadır (Duke, 2008: 28). Bu konu aynı zamanda bize AB'nin kurallı bir uluslararası düzen, iyi işleyen uluslararası örgütler ve güçlü bir uluslararası toplumun gelişimine katkıda bulunma amacı taşıdığını da göstermektedir (Hemmer, 2010: 55). AB'nin kısa tarihi boyunca genellikle güvenliği tüketen bir aktör konumunda olduğunu vurgulayan Duna (2010: 20), şimdi yeni güvenlik ve savunma görüşüyle güvenliği sağlayan bir aktör konumuna yükseldiğini ifade etmektedir. Sonuç olarak Soğuk Savaş sonrasında değişen küresel düzen içinde, Avrupa'nın rolünün arttığı ve AB üyesi devletlerin ABD'nin küçük ortağı olmaktan çıkarak sivil bir güç olma yolunda uluslararası güvenlik ve barışı koruma anlamında önemli adımlar attıkları görülmektedir (Toje, 2008: 212).

2. AVRUPA BİRLİĞİ'NİN GÜVENLİK STRATEJİLERİ

AB, Soğuk Savaş sonrası dönemde değişen tehdit algılamalarına göre farklı stratejiler geliştirmiştir. Bu stratejiler, AB'nin bağımsız bir güvenlik ve savunma politikası oluşturma girişimini desteklemektedir. Bu stratejilerden 2003 yılında açıklanan Avrupa Güvenlik Stratejisi daha çok AB'nin aktör olarak uluslararası arenada kendine bir yer bulma arzusu üzerine odaklandığından siyasi bir girişim olarak kabul edilebilir. Ancak değişen küresel güvenlik ve savunma dinamikleri, 2016 yılında yeni bir stratejinin oluşturulmasını gerektirmiştir. Avrupa Güvenlik Stratejisi yerine duyurulan Küresel Strateji, AB'nin askerî ihtiyaçlarına dikkat çekmiştir. Bu strateji tarafından duyurulan "stratejik bağımsızlık", AB'nin bağımsız bir güvenlik ve savunma politikası oluşturma girişimini destekleyen bir atılım olarak kabul edilebilir. Hem bir strateji hem de bir eylem planı olarak 2022 yılının Mart ayında duyurulan Stratejik Pusula ise değişen tehditleri yeniden tanımlamakta ve her düzeyde işbirliğine dikkat çekmektedir. Stratejik Pusula, güvenlik ve savunma konusunda bir yanda AB-NATO ortaklığının önemi üzerinde dururken diğer yanda AB'nin bağımsız bir güvenlik ve savunma politikası geliştirmesinin önemine vurgu yapmaktadır. AB'nin dış politikasında önemli bir gelişmeyi temsil eden Stratejik Pusula, AB'nin bağımsız güvenlik ve savunma politikasını ABD ve NATO ile işbirliği içinde, "tamamlayıcı" olarak, geliştirebileceğini ortaya koymaktadır. Buna göre, önceki iki strateji ile Stratejik Pusula hakkında bilgi vermek, zaman içinde AB tarafından atılan adımların değişen niteliklerinin anlaşılmasını kolaylaştıracaktır.

2.1. Avrupa Güvenlik Stratejisi ve Küresel Strateji

AB'nin sivil bir güç olarak, bağımsız bir güvenlik ve savunma politikası oluşturma girişimi, geleneksel devlet yapısı ile küresel güçler tarafından değişime uğratılan uluslararası toplum ikiliğinden oluşmaktadır (Rapnouil, 2009: 194). Bu genel dinamik içinde, 19-20 Haziran 2003 tarihinde Selanik'te yapılan zirvede "Daha İyi Bir Dünyada Güvenli Bir Avrupa" başlıklı bir belge sunulmuştur. Avrupa Güvenlik Stratejisi olarak tanımlanan belgede devletlerin karmaşık sorunlarla tek başlarına mücadele edemeyecekleri vurgulanmış ve etkili çok taraflılık düşüncesine dikkat çekilmiştir (Tocci, 2017: 495). Belgede sert güvenlik politikası yerine yumuşak güvenlik politikasının benimsendiği duyurulmuştur. Buna göre AB, askerî olmayan araç ve yetenekler kullanmaya karar vermiştir. Belge, uluslararası terörizmi, kitle imha silahlarının yayılmasını, bölgesel çatışmaları ve organize suçları önemli tehditler olarak açıklamıştır. Strateji, sorunların çözümü için Avrupa'nın yakın

çevresinde güvenliğin tesis edilmesi ile "etkili çok taraflılığa" dayanan bir uluslararası düzenin kurulmasını başlıca faaliyet alanları olarak benimsemiştir.

Avrupa Güvenlik Stratejisi Belgesi'nin yayımlanmasından sonraki on yıl içinde yaşanan terör olayları, iç savaşlar ve bunların sonucu olarak ortaya çıkan göç dalgaları, AB'nin güvenlik ve savunma ile ilgili konuları yeniden ele almasını gerektirmiştir. Avrupa Konseyi, farklılaşan küresel yapı içinde AB'yi tehdit eden konuların yeniden tanımlanmasını ve yeni bir stratejinin hazırlanmasını istemiştir. Buna göre, yaptığı çalışmayı 2015 yılında duyuran Dış İlişkiler ve Güvenlik Politikası Yüksek Temsilciliği, dünyayı devletlerin birbirine bağlı olduğu çalkantılı, rekabete dayalı ve karmaşık bir yer olarak tanımlamıştır. Yüksek Temsilcilik aynı zamanda 2016 yılında İngiltere'nin AB'den ayrılışını oylayacak referanduma göndermede bulunarak hazırlanan yeni stratejinin AB'ye bir birlik duygusu kazandırmasını da hedeflediğini açıklamıştır (Tocci, 2017: 489). Bu çalışmalar çerçevesinde Avrupa Konseyi, 28 Haziran 2016 tarihinde "AB Dış ve Güvenlik Politikasına İlişkin Küresel Strateji" başlıklı bir belgeyi kabul ettiğini duyurmuştur. Bu belgeye göre Küresel Strateji uluslararası ortamı; terörizmden başarısız devletlere, organize suçlardan bölgesel çatışmalara kadar değişen, daha çeşitli, daha az görünür ve daha az öngörülebilir bir ortam olarak tasvir etmiştir (Mälksoo, 2016: 378). Avrupa Güvenlik Stratejisi, AB'nin aktör olarak uluslararası arenada kendine bir yer bulma arzusu üzerine odaklanırken Küresel Strateji güvenlik ve savunma ile ilgili gelişmelere odaklanmıştır.

Küresel Strateji Belgesi'nde AB üyesi devletlerin güvenliğinin sağlanması bir öncelik olarak belirtilmiştir. Küresel Stratejinin uygulamasını içeren "Güvenlik ve Savunma Uygulama Planı", çatışmaların barışçı yollardan çözümü ve krizlerin yönetimi için bütünleşik bir yaklaşım ortaya koymuştur. Uygulama planı, barış anlaşmalarının ve ateşkes düzenlemelerinin hayata geçirilebilmesi için AB'nin sivil ve askerî operasyonlar yapması gerektiğini böylece istikrarlı ortamların yaratılabileceğini vurgulamıştır (Tocci, 2018: 131). Küresel Strateji, askerî operasyonlar ile sivil araçların kullanımı dışında hukuk, polislik, yönetim ve eğitim gibi konulara da değinmiş, dayanıklılık konusunun altını çizmiştir (Tardy, 2018: 120).

Küresel Strateji Belgesi, AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme hedefini bir adım ileri götürmektedir. Belge, "stratejik bağımsızlık" düşüncesini güvenlik ve savunma konusunun temel niteliği olarak vurgulanmıştır (Barbé ve Morillas, 2019: 760). Son yıllarda Konsey tarafından belirlenen

"stratejik bağımsızlık" hedefine ulaşmak için sarf edilen çabalar, bağımsız bir güvenlik ve savunma politikası yaratılması konusunda AB'nin en önemli gündem maddesini oluşturmaktadır. Konsey, bu anlamda siyasi-askerî görevler ve yetenekler belirlemiş, (Biscop, 2016: 432). AB de "stratejik bağımsızlık" arayışıyla tanımlanan yeni bir hedef ortaya koymuştur (Duke, 2019: 123). "Stratejik Bağımsızlık", İngiltere'nin AB'den ayrıldığı bir dönemde, üye devletleri siyasi bütünleşme hedefi altında bir araya getirebilmeyi amaçlamaktadır (Koppa, 2019: 4).

Küresel Strateji, AB'nin etkili eylemlerde bulunabilmesi için CARD (Coordinated Annual Review on Defence – Koordineli Yıllık Savunma İncelemesi) ve PESCO (Permanent Structured Cooperation – Kalıcı Yapılandırılmış İşbirliği) gibi özel araçlar geliştirmiştir. Bu araçlar, üye devletlerin "stratejik bağımsızlık" düşüncesini hayata geçirebilmek için gerekli olan siyasi ve askerî unsurların ortaya koyulmasını kolaylaştırmıştır. AB Konseyi, AB'nin sivil ve askerî görevleri arasındaki ilişkiyi güçlendirmek için Koordineli Yıllık Savunma İncelemesi (CARD) başlatmıştır. 2016 yılının Kasım ayında duyurulan CARD, üye devletlerarasında askerî yeteneklerin geliştirilmesi için bilgi paylaşımı sağlamayı ve işbirliği geliştirmeyi taahhüt etmektedir (Barbé ve Morillas, 2019: 764). CARD, üye devletlerin ulusal savunma bütçelerini inceleyerek savunma harcamaları için yeni yöntemler de önermektedir (Koppa, 2019: 5). Üye devletlerin önceliklerinin gerçekleşmesini sağlamak ve uygulamalarını denetlemek için planlanan CARD (Besch, 2019: 6) üye devletlerarasında uygulama planlarının denetlenmesi sırasında ortaya çıkabilecek işbirliği imkânlarını da değerlendirmektedir (Fiott, 2017: 1). Bu anlamda CARD, üye devletlerin ulusal savunma planlamalarıyla ilgili yetenek geliştirme uygulamalarını birbirlerine göre ayarlayabilecekleri bir mekanizma olarak işlev görecektir (Tardy, 2018: 126).

Küresel Strateji tarafından geliştirilen bir başka özel araç da Kalıcı Yapılandırılmış İşbirliğidir (PESCO). Taahhütler ve özel projeler içeren PESCO, 25 AB üyesi arasında derin işbirliği oluşturulmasını hedeflemektedir. PESCO, üye devletlerin katılımını teşvik etmek için finansman sağlayan "Avrupa Savunma Fonu" tarafından tamamlanmaktadır (Leuprecht, 2019: 79). PESCO, hükümetler arası bir yapı olmadığı ve alınan kararlar için oybirliği gerekmediği için savunma konusunda atılmış en önemli adımlardan biri olduğu söylenebilir. Bu anlamda PESCO, bütünleşme süreci içinde derinleşmeyi temsil eden bir işbirliği uygulaması olarak karşımıza çıkmakta (Csornai, 2017: 6) ve bu yönüyle de farklılaştırılmış bütünleşmeye iyi bir örnek olmaktadır (Aydın-Düzgit ve Marrone, 2018: 5).

2.2. Avrupa Birliği için Stratejik Pusula

AB'nin yanı başında 2022 yılının Şubat ayında başlayan Rusya-Ukrayna savaşı ve güvenlik ortamının düşmanca bir hâl alması, AB'nin ileriye doğru bir hamle yapmasını gerektirmiştir. AB üyesi devletler söz konusu savaşın yanı sıra, stratejik rekabetin ve istikrarsızlık kaynaklarının arttığını görmüş ve melez tehditlerin etkilerini genişlettiğini fark etmişlerdir. Üye devletler açık denizlere, uzaya ve dijital alana erişimin giderek daha tartışmalı bir hâle geldiğini ve karşılıklı bağımlılığın etkisini kaybetmeye başladığını anlamışlardır. Bu şartlar altında AB, çevresindeki varlığını ve etkinliğini artırmak zorunda kaldığını hissetmiş ve hem dayanıklılığını güçlendirmek hem de savunma yeteneklerini çeşitlendirmek için yatırım yapmaya karar vermiştir. Avrupa Konseyi, 24-25 Mart 2022 tarihlerinde yapılan zirvede AB'nin daha güçlü bir güvenlik ve savunma yapısı geliştirmesi hakkındaki ortak görüşü içeren bir belge olan Stratejik Pusula'yı kabul etmiştir. Stratejik Pusula, AB'nin önümüzdeki beş ila on yıldaki güvenlik ve savunma hedefleri için yeni bir yol haritası çizmektedir. AB'yi daha güçlü ve yetenekli bir güvenlik sağlayıcısı yapmayı amaçlayan Stratejik Pusula, AB'nin stratejik bağımsızlığını korumak amacıyla ortaklarla çalışmayı hedeflediğini duyurmuştur (https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

Stratejik Pusula, üzerinde anlaşmaya varılan ilk AB tehdit değerlendirmesini içermekte ve AB'nin güvenlik ve savunma programlarını günümüzün zorlu güvenlik ortamına uyarlamaktadır. Stratejik Pusula, hem NATO'nun AB topraklarını savunmak için oynadığı hayati toplu savunma rolüne hem de AB'nin stratejik bağımsızlığı için yetenek ve savunma yatırımı gereksinimine vurgu yapmaktadır. Stratejik Pusula ile AB üye devletleri, stratejik ortam, karşılaşılan tehditler ve zorluklar hakkında ortak bir değerlendirme yapmayı ve güvenlik alanındaki eylemlere daha fazla tutarlılık ve ortak amaç duygusu getirmeyi amaçlamakta ve bunun için de yeni yollar ve araçlar belirlemeyi hedeflemektedir. Bunun için Stratejik Pusula, dört yönde somut öneriler sunmaktadır. (https://www.eeas.europa.eu/eeas/questions-and-answers-background-strategic-compass_en.

Stratejik Pusula'nın birinci yönü, eyleme geçmektir. AB, krizlerle karşılaşıldığında daha hızlı ve kararlı bir şekilde eyleme geçmeyi ve esnek kararlar almayı hedeflemektedir. Bu amaçla, üye devletlerin komuta ve kontrol yapılarını güçlendirmesi gerekmektedir. Bu çerçeve içinde AB, 5000 askere kadar güçlü bir AB Hızlı İntikal Gücü kapasitesi oluşturmayı ve 30 gün içinde 200 tam donanımlı OGSP görev uzmanını görevlendirmeyi planlamaktadır. AB aynı zamanda karada

ve denizde düzenli canlı tatbikatlar yapmayı ve askerî hareketliliği geliştirmeyi de düşünmektedir. Benzer şekilde, üye devletler kendi aralarında daha fazla mali dayanışma sağlayarak, AB'nin sivil ve askerî OGSP görevlerini ve operasyonlarını güçlendirmeyi planlamaktadır.

Stratejik Pusula'nın ikinci yönü, güvence altına almaktır. AB, vatandaşlarını hızla değişen tehditlere karşı güvence altına almayı hedeflemektedir. AB, bunun için güvenlik çıkarlarını korumayı, istihbarat analiz kapasitesini artırmayı, melez tehditleri tespit etmeyi ve bunlara yanıt vermek için farklı araçları ve müdahale ekiplerini bir araya getirmeyi düşünmektedir. AB aynı zamanda, bir uzay stratejisi geliştirerek deniz, hava ve uzay alanlarındaki eylemleri güçlendirmeyi amaçlamaktadır. Dolayısıyla, AB üyesi devletler mevcut ve aniden ortaya çıkan tehditleri ve zorlukları öngörme, caydırma ve bunlara yanıt verme yeteneğini güçlendirmektedir.

Stratejik Pusula'nın üçüncü yönü, yatırım yapmaktır. AB, gerektiğinde yeteneklere ve yenilikçi teknolojilere yatırım yapmayı hedeflemektedir. Burada amaç, stratejik boşlukları doldurmak ve teknolojik ve endüstriyel bağımlılıkları azaltmaktır. AB üyesi devletler bunun için savunmada daha fazla harcama yapmayı ve kapasite artırmayı düşünmektedir. Üye devletler askerî yetenekleri ortaklaşa geliştirmek ve savunma için teknolojik yeniliklere yatırım yapmayı hedeflemektedir. Genel olarak AB, işbirliğine dayalı yetenekleri geliştirmeyi, karada, denizde, havada, siber alanda ve uzayda faaliyet gösterecek yeni nesil yeteneklere ortak yatırım yapmaları için üye devletleri teşvik etmeyi planlamaktadır.

Stratejik Pusula'nın dördüncü yönü, ortak olmaktır. AB, ortak tehditleri ve zorlukları ele almak ve ortak hedeflere ulaşmak için diğer aktörlerle ortak olmayı hedeflemekte ve var olan ortaklıklarını güçlendirmeyi planlamaktadır. AB, bunun için NATO ve Birleşmiş Milletler (BM) ile stratejik ortaklığını güçlendirmeyi ve diğer bölgesel örgütlerle işbirliğini artırmayı düşünmektedir. AB; ABD, Norveç, Kanada, İngiltere ve Japonya gibi kendisi ile aynı değerleri paylaşan ikili ortaklarla işbirliğini artırmayı amaçlamaktadır. Bunun yanı sıra AB; Batı Balkanlar, Doğu ve Güney komşuları ile Afrika, Asya ve Latin Amerika'da özel ortaklıklar geliştirmeyi de planlamaktadır.

Dört temel başlıkta somut öneriler ortaya koyan Stratejik Pusula, AB'nin bağımsız bir güvenlik ve savunma politikası oluşturma konusunda attığı en yeni adımı temsil etmektedir. Stratejik Pusula, bu anlamda AB'nin güvenlik sağlayıcısı

olarak uluslararası alanda neler yapabileceğinin genel hatlarını çizmektedir. Bu çerçeve içinde Stratejik Pusula'yı bir dönüm noktası olarak değerlendirmek yanlış olmayacaktır.(https://www.consilium.europa.eu/en/press/press-releases/2016/06/28/euco-conclusions.

3. AB'NİN BAĞIMSIZ GÜVENLİK VE SAVUNMA POLİTİKASI HAKKINDA BİR DEĞERLENDİRME

Soğuk Savaş sonrası dönemde AB üyesi devletlerin üzerinde en çok tartıştıkları konulardan biri, AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesi olmuştur. Söz konusu politika, Avrupa bütünleşme projesinin siyasi ayağını oluşturduğu ve AB'nin uluslararası bir aktör olmasının neredeyse ön koşulu olarak görüldüğü için, üye devletleri oldukça zorlamıştır. AB'nin bu konu ile ilgili olarak son 20 yıllık dönem içinde attığı adımlar incelendiğinde üç konuda değerlendirme yapılabilir.

AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesi ile ilgili göze çarpan ilk değerlendirme, AB ile NATO arasındaki kurumsal rekabetin AB'nin eylemlerini sınırlandırmış olmasına rağmen (Torun, 2018: 5), AB'nin ABD ve NATO'dan bağımsız bir güvenlik ve savunma politikası geliştirmeyi başaramadığıdır. Ancak AB uluslararası ortamı olmasını istediği gibi değil, olduğu gibi kabul ettikten sonra bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesini, ironik bir şekilde ABD ve NATO'ya rağmen değil, ABD ve NATO ile işbirliği içinde gerçekleştirebileceğini öğrenmiştir. AB üyesi devletlerin aynı zamanda NATO üyeleri olmaları ve bu devletlerin ABD ile önemli ikili ilişkileri olması AB'nin NATO'dan ayrı hareket etmesini engellemiştir. Ayrıca AB-NATO ortaklığının taraflar için hâlâ son derece önemli olması, AB'yi güvenlik ve savunma konusunda ABD ve NATO ile işbirliği yapmak zorunda bırakmıştır. Bu konu ile ilgili somut adımlar özellikle Küresel Strateji ve Stratejik Pusula ile atılmıştır. Küresel Strateji tarafından oluşturulan PESCO, AB ve NATO tarafından konuşlandırılacak askerî yetenekleri geliştirmek ve tarafların savunma planlarını koordine etmekle görevli bir araç olarak planlanmıştır. Stratejik Pusula da NATO'nun AB topraklarının savunulması konusunda oynadığı role dikkat çekerek AB-NATO işbirliğinin gündemdeki yerini koruduğunu belirtmektedir.

AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesi ile ilgili göze çarpan ikinci değerlendirme, AB'nin söz konusu düşünceyi gerçeğe dönüştürmek için attığı adımların genel olarak zorunluluklar neticesinde ortaya çıkmış olmasıdır. AB üyesi devletler, bağımsız bir güvenlik ve savunma politikası

geliştirme düşüncesini, AB dışından tetiklenen gelişmelerin bir devamı veya tamamlayıcısı olarak eyleme geçirebilmişlerdir. Soğuk Savaş sonrası dönemde neredeyse her on yılda bir karşımıza çıkan strateji belgeleri bize bu konuda iyi örnekler sunmaktadır. Örneğin; Avrupa Güvenlik Stratejisi, çatışmaların çözümü ve barışın sağlanması için etkili çok taraflılığa dayanan bir uluslararası düzen benimsemiştir. Bu düzen içinde bulunmanın bir koşulu, siyasi olarak sözü dinlenen, özellikle güvenlik ve savunma gibi siyasi bütünleşmenin ön koşulu olarak nitelendirilen konularda kendi başına karar verebilen bir aktör olmaktır. Diğer yandan Küresel Strateji, uluslararası sistemde yenilenen tehditler ile İngiltere'nin Birlikten ayrılmasının üye devletler üzerinde yaratacağı olumsuz etkiyi ortadan kaldırmayı hedeflemiştir. Küresel Strateji'de sert gücün kullanımına vurgu yapılması, AB'nin sivil operasyonların yanında askerî operasyonlara da yer vereceğini düşündüğünü göstermektedir. Nitekim AB, Küresel Strateji Belgesi'nde stratejik bağımsızlık düşüncesini AB'nin güvenlik ve savunma konularının temel niteliği olarak tanımlamıştır. Dolayısıyla, stratejik bağımsızlık, İngiltere'nin AB'den ayrılışı sonrası AB üyesi devletleri bir araya getiren bir araç olmuştur. Stratejik Pusula, Rusya-Ukrayna Savaşı ile çatışmacı bir nitelik kazanan yakın çevresinde AB'nin güvenliğini sağlamak için duyurulmuştur. Stratejik Pusula'da, söz konusu savaşın yanı sıra, artan istikrarsızlık kaynaklarının ve alanı genişleyen melez tehditlerin, AB'nin etkinliğini artırma ihtiyacını ortaya çıkardığı belirtilmiştir. Bu gelişme de güçlü ve bağımsız bir güvenlik ve savunma politikasının varlığını gerekli kılmaktadır.

AB'nin bağımsız bir güvenlik ve savunma politikası geliştirme düşüncesi ile ilgili olarak göze çarpan üçüncü değerlendirme, AB'nin ortaya koyduğu söz konusu politikaya ait hedeflerin ve planlanan eylemlerin gittikçe askerî bir nitelik kazanmasıdır. Örneğin, Avrupa Güvenlik Stratejisi, çatışmaların sona erdirilmesi, barışın tesis edilmesi ve istikrarın sağlanması için yumuşak güç politikasını benimsemiştir. Ancak Küresel Strateji Belgesi barış anlaşmalarının hayata geçirilebilmesi için sivil ve askerî operasyonların yapılmasının önemi üzerinde durmuştur. Küresel Strateji, bu düşünce çerçevesinde CARD ve PESCO gibi araçlar oluşturmuştur. Stratejik bağımsızlık düşüncesini hayata geçirmek üzere oluşturulan bu iki araç özellikle askerî uygulamalara vurgu yapmaktadır. Örneğin; üye devletlerarasındaki askerî görevlerin koordinasyonunu ve ilişkiyi güçlendirmeyi amaçlayan CARD, askerî yeteneklerin geliştirilmesi için bilgi paylaşımı üzerinde durmaktadır. Bir diğer araç olan PESCO da AB ve NATO yönetimi altında konuşlandırılacak askerî yetenekleri geliştirmek ve koordinasyonu

sağlamak üzere planlanmıştır. AB, Stratejik Pusula ile krizler karşısında hızlı bir şekilde eyleme geçmeyi ve esnek kararlar almayı hedeflediğini duyurmuştur. Buna göre, çatışmaların çözümü ve barışın sağlanması konusunda Avrupa Güvenlik Stratejisi ile yumuşak güç politikasını benimsediğini duyuran AB, Stratejik Pusula ile geldiği noktada canlı askerî tatbikatlar yoluyla gerçek bir askerî güç oluşturmak istediğini ortaya koymaktadır.

SONUÇ

Avrupa bütünleşme süreci içinde AB üyesi devletlerin ekonomik ve parasal konularda aldıkları ortak kararları daha fazla uygulayabildikleri ancak dış, güvenlik ve savunma konularında aynı ölçüde başarılı olamadıkları görülmektedir. Buna rağmen üye devletler Soğuk Savaş sonrası dönemde karşılaştıkları, Taliban'ın Afganistan'ı alması gibi tehditler ve Dağlık Karabağ'da yaşanan bölgesel çatışmalar ile göç krizini tetikleyen Libya ve Suriye'deki sorunlar gibi gelişmeler nedeniyle güvenlik ve savunma konularıyla ilgili olarak bağımsız politikalar oluşturmak ve bunları uygulamak ihtiyacı hissetmektedirler.

Avrupa güvenlik yapısının ABD öncülüğündeki NATO üzerine kurulu olması, AB üyesi devletlerin güvenlik ve savunma alanında kendi başlarına politika geliştirme konusundaki isteklerinin gerçekleşmesini zora sokmaktadır. Yine de AB üyesi devletler güvenlik ve savunma konularında bazı ortak kararlar alabilmiş ve bu kararların uygulamasında zorluklarla karşılaşmış olmalarına rağmen belli bir ölçüde bunları gerçekleştirebilmişlerdir. AB'nin bu konuda karşılaştığı en büyük zorluk, oluşturmak istediği bağımsız güvenlik ve savunma politikasının ABD ve NATO ile kurgulanmak zorunda kalmış olmasıdır. Bununla birlikte, AB'nin NATO ile hâlihazırda ortak politikalar üzerinde çalışıyor olması, söz konusu zorluğun üstesinden gelmeyi kolaylaştıran bir unsur olmaktadır. Strateji belgeleriyle kendine bağımsız bir güvenlik ve savunma politikası oluşturmak isteyen AB, bunu ancak ABD ve NATO ile işbirliği içinde gerçekleştirebileceğini anlamıştır.

Stratejik Pusula'da üye devletlerarasındaki ilk ortak tehdit değerlendirmesinin yapılması, üye devletlerin ortak stratejik kültüre yönelik olarak attığı önemli bir adım olarak nitelendirilmektedir. Bunun da sebebi, AB'nin dış, güvenlik ve savunma politikalarını çok daha tutarlı hâle getirmek istemesidir. Bu anlamda 2030 yılına kadar OGSP hakkında somut taahhütlerde bulunan Stratejik Pusula, aynı zamanda AB'nin bir güvenlik sağlayıcısı olarak dayanıklılık oluşturma konusundaki oynadığı rolüne de vurgu yapmaktadır.

Sonuç olarak Stratejik Pusula AB vatandaşlarının güvenliğini sağlamak için daha fazla sorumluluk almanın önemini vurgulamakta, uluslararası barış ve güvenliğin sağlanması konusunda başta NATO olmak üzere ortaklarla birlikte çalışmanın önemini ortaya koymaktadır. Stratejik Pusula, bir yanda küresel ve transatlantik güvenliğe katkı sağlayacak, diğer yanda da AB'nin ABD ve NATO ile işbirliği içinde kendi güvenlik ve savunma politikasını oluşturmasını destekleyecek bir eylem planı olarak duyurulmuştur. Bu düşünce içinde AB, üyeleri için toplu savunmanın temeli olmaya devam eden NATO'nun tamamlayıcısı olacak ancak aynı zamanda oluşturulmaya çalışılan yeni yetenekleriyle, küresel kurallara dayalı düzene verdiği desteğini artırarak, siyasi bütünleşmesi için de önemli adımlar atacaktır. Bu çerçevede Stratejik Pusula'nın da önümüzdeki dönemde araştırmacılar için önemli bir konu olacağı söylenebilir.

KAYNAKÇA

A strategic compass for security and defence (2022). Erişim tarihi: 11.05.2022 https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-1_en.

Antoniades, A. (2008). Social Europe and/or global Europe? Globalization and flexicurity as debates on the future of Europe. Cambridge Review of International Affairs, 21(3), 327-346. doi:10.1080/09557570802253492.

Aydın-Düzgit, S. (2015). Avrupa Birliği kurumlarının Türkiye söylemlerinde bir güvenlik topluluğu olarak Avrupa. Marmara Avrupa Araştırmaları Dergisi, 23(2), 99-122.

Aydın-Düzgit, S. ve Marrone, A. (2018). PESCO and security cooperation between the EU and Turkey. Global Turkey in Europe Working Paper 19, 1-7.

Barbé, E. ve Morillas, P. (2019). The EU global strategy: the dynamics of a more politicized and politically integrated foreign policy. Cambridge Review of International Affairs, 32(6), 753-770. doi:10.1080/09557571.2019.1588227.

Besch, S. (2019).The European Commission in EU defence industrial policy. Carnegie Europe, 1-7.

Bickerton, J. C. (2010). Functionality in EU foreign policy: towards a new research agenda? Journal of European Integration, 32(2), 213-227. doi:10.1080/07036330903486045.

Birdişli, F. (2020). Uluslararası güvenliğin tarihsel gelişimi ve post-modern güvenlik dönemi. Güvenlik Bilimleri Dergisi, UGK Özel Sayısı, 235-260. doi:10.28956/gbd.696034.

Biscop, S. (2016). All or nothing? The EU global strategy and defence policy after the Brexit. Contemporary Security Policy, 37(3), 431-445. doi:10.1080/13523260.2016.1238120.

Calleo, P. D. (2008). How Europe could save the world. World Policy Journal, 25(3), 3-12.

Csornai, Z. (2017). Evaluating the effects of Brexit on the EU's common security and defence policy. KKI Policy Brief, 14, 1-12.

Diedrichs, U. (2005). The development of the European security and defense policy and its implications for NATO: cooperation and competition. Journal of Transatlantic Studies, 3(1), 55-70. doi:10.1080/14794010508656817.

Drath, V. (2007). The new atlanticism: broadening horizons. American Foreign Policy Interests, 29(6), 401-409. doi:10.1080/10803920701776970.

Duke, S. (2008). The future of EU-NATO relations: a case of mutual irrelevance through competition. Journal of European Integration, 30(1), 27-43. doi:10.1080/07036330801959457.

Duke, S. (2019). The competing logics of EU security and defence. Survival, Global Politics and Strategy, 61(2), 123-142. doi:10.1080/00396338.2019.1589092.

Duna, D. (2010). Defining the European Union as a global security actor. Eurolimes, 10, 19-33.

Dyson, T. (2008). Convergence and divergence in post-cold war British, French, and German military reforms: between international structure and executive autonomy. Security Studies, 17(4), 725-774. doi:10.1080/09636410802507990.

Eriksen, E. O. (2006). The EU-a cosmopolitan polity? Journal of European Public Policy, 13(2), 252-269. doi:10.1080/13501760500451683.

European Council conclusions, 28 June 2016 (2016). Erişim tarihi: 11.05.2022 https://www.consilium.europa.eu/en/press/press-releases/2016/06/28/euco-conclusions.

Fiott, D. (2017). The CARD on the EU defence table. European Union Institute for Security Studies, 1-2.

Fischer, C. T. (2006). An American looks at the European Union. European Law Journal, 12(2), 226-278. doi:10.1111/j.1468-0386.2006.00317.x.

Hemmer, C. (2010). Balancing, bonding, and balking: the European Union, the United States, and the Israeli-Palestinian peace process. Mediterranean Quarterly, 21(2), 47-60.

Hyde-Price, A. (2006). Normative power Europe: a realist critique. Journal of European Public Policy, 13(2), 217-234. doi:10.1080/13501760500451634.

Irondelle, B. ve Merand, F. (2010). France's return to NATO: the death knell for ESDP? European Security, 19(1), 29-43. doi:10.1080/09662839.2010.499362.

Jones, G. S. (2006). The rise of a European defense. Political Science Quarterly, 121(2), 241-267.

Kanet, E. R. (2008). Still Mars, still Venus? The United States, Europe, and the future of the transatlantic relationship. International Politics, 45(3), 231-235. doi:10.1057/ip.2008.1.

Keyman, E. F. (2006). Küreselleşme, uluslararası ilişkiler ve hegemonya. Uluslararası İlişkiler Dergisi, 3(9), 1-20.

Koppa, M. E. (2019). The relationship between CSDP and NATO after Brexit and the EU global strategy. FEPS Studies, 1-29.

Layne, C. (2006). The unipolar illusion revisited, the coming end of the United States' unipolar moment. International Security, 31(2), 7-41. doi:10.1162/isec.2006.31.2.7.

Leuprecht, C. (2019). New opportunities in common security and defence policy: joining PESCO. Australian and New Zealand Journal of European Studies, 11(3), 76-96. doi:10.30722/anzjes.vol11.iss3.15109.

Mahncke, D. (2009). The United States, Germany and France: balancing transatlantic relations. The British Journal of Politics and International Relations, 11(1), 79-93. doi:10.1111%2Fj.1467-856x.2008.00356.x.

Mälksoo, M. (2016). From the ESS to the EU global strategy: external policy, internal purpose. Contemporary Security Policy, 37(3), 374-388. doi:10.1080/13523260.2016.1238245.

Maull, W. H. (2005). Europe and the new balance of global order, International Affairs, 81(4), 775-799. doi:10.1111/j.1468-2346.2005.00484.x.

Menon, A. ve Sedelmeier, U. (2010). Instruments and intentionality: civilian crisis management and enlargement conditionality in EU security policy. West European Politics, 33(1), 75-92. doi:10.1080/01402380903354106.

Merand, F. (2010). Pierre Bourdieu and the birth of European defense. Security Studies, 19(2), 342-374. doi:10.1080/09636411003795780.

Narramore, T. (2008). China and Europe: engagement, multipolarity and strategy. The Pacific Review, 21(1), 87-108. doi:10.1080/09512740701868930.

Oswald, F. (2006). Soft balancing between friends: transforming transatlantic relations. Debatte, 14(2), 145-160. doi:10.1080/09651560600841502.

Poettering, H. (2007). Europe as a global player, a parliamentary perspective, Harvard International Review, 29(1), 26-29.

Posen, R. B. (2006). European Union security and defense policy: response to unipolarity. Security Studies, 15(2), 149-186. doi:10.1080/09636410600829356.

Press-Barnathan, G. (2006). Managing the hegemon: NATO under unipolarity. Security Studies, 15(2), 271-309. doi:10.1080/09636410600829554.

Rapnouil, M. L. (2009). A European view on the future of multilateralism. The Washington Quarterly, 32(3), 181-196. doi:10.1080/01636600903025614.

Rumelili, B. (2018). Breaking with Europe's pasts: memory, reconciliation, and ontological (in) security. European Security, 27(3), 280-295. doi:10.1080/09662839.2018.1497979.

Schroeder C. U. (2009). Strategy by stealth? The development of EU internal and external security strategies, Perspectives on European Politics and Society, 10(4), 486-505. doi:10.1080/15705850903314783.

Shambaugh, D. (2005). The new strategic triangle: US and European reactions to China's rise. Washington Quarterly, 28(3), 5-25. doi:10.1162/0163660054026470.

Tardy, T. (2018). Does European defence really matter? Fortunes and misfortunes of the common security and defence policy. European Security, 27(2), 119-137. doi: 10.1080/09662839.2018.1454434.

Toje, A. (2008). The European Union as a small power, or conceptualizing Europe's strategic actorness. Journal of European Integration, 30(2) 199-215. doi:10.1080/07036330802005425.

Tocci, N. (2016). The making of the EU global strategy. Contemporary Security Policy, 37(3), 461-472. doi:10.1080/13523260.2016.1232559.

Tocci, N. (2017). From the European security strategy to the EU global strategy: explaining the journey. International Politics, 54, 487-502. doi:10.1057/s41311-017-0045-9.

Tocci, N. (2018). Towards a European security and defence union: was 2017 a watershed? JCMS, 56, 131-141. doi:10.1111/jcms.12752.

Torun, Z. (2018). Explaining the EU's security and defence policy: the need for three-level analysis. Ulisa: Uluslararası Çalışmalar Dergisi, 2(1), 1-16.

Wang, S. (2009). The making of new 'space': cases of transatlantic astropolitics. Geopolitics, 14(3), 433-461. doi:10.1080/14650040802693820.

Wivel, A. (2008). Balancing against threats or bandwagoning with power? Europe and the transatlantic relationship after the cold war. Cambridge Review of International Affairs, 21(3), 289-305. doi:10.1080/09557570802253419.

Questions and answers: a background for the strategic compass (2022). Erişim tarihi: 11.05.2022 https://www.eeas.europa.eu/eeas/questions-and-answers-background-strategic-compass_en

Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2023,Cilt:12, Sayı:1, 69-96
doi:10.28956/gbd. 1264593

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2023,Volume:12, Issue:1, 69-96
doi:10.28956/gbd. 1264593

Makale Türü ve Başlığı / Article Type and Title
Araştırma/ Research Article
İşletmelerin Maruz Kaldığı Siber Suçların Boyutu
The Size of Cyber Crimes That Businesses Are Exposed

Yazar(lar) / Writer(s)
Cem EROĞLU, Gazi Üniversitesi, Adli Bilişim Doktora Programı Öğrencisi, e-posta: cem.eroglu1@gazi.edu.tr. ORCID: https://orcid.org/0000-0001-8491-6398.

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
- Bu çalışma, yazarın "İşletmelerin Maruz Kaldığı Siber Suçların Boyutu ve İşletmelere Etkisi" başlıklı yüksek lisans tez çalışmasının bir bölümünden elde edilmiştir.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :13.03.2023
Makale Kabul Tarihi / Accepted :25.05.2023

Atıf Bilgisi / Citation:
Eroğlu C., (2023). İşletmelerin Maruz Kaldığı Siber Suçların Boyutu, *Güvenlik Bilimleri Dergisi, 12(1), ss 69-96. doi:10.28956/gbd. 1264593*

İŞLETMELERİN MARUZ KALDIĞI SİBER SUÇLARIN BOYUTU

Öz

İnsanlar teknolojik gelişmeler ve internetin yaygınlaşmasıyla birlikte alışveriş yapma, arkadaşlarıyla görüşme, bankacılık işlemleri gibi alışkanlıklarını değiştirmeye başlamıştır. Bu değişim ve siber ortam vasıtasıyla suç kavramı da dönüşüme uğramış ve siber suç kavramı insan hayatına girmiştir. Teknolojiye uyum sağlamaya çalışan işletmeler ise siber ortamın tehlikeleriyle karşılaşmıştır. Genel amacı işletmeleri bir siber suçun hedefi hâline getiren faktörleri araştırmak olan çalışmada Siber Güvenlik İhlalleri Anketi 2021'in veri setleri ikincil veri olarak kullanılmıştır. Türkiye'de işletmeler ve siber suç konularında yapılan az sayıdaki çalışma siber güvenlik ve siber risk üzerine yapılmıştır. Bu araştırmada ise işletmenin büyüklüğü, insan faktörü, dijital görünürlük, siber güvenlik önlemleri, siber farkındalık ve siber suçla mücadele eğitiminin siber suç mağduriyeti ile ilişkisi incelenmiştir. Araştırma sonucunda orta ve büyük işletmelerin daha fazla siber suça maruz kaldığı görülürken işletmelerin en yaygın maruz kaldığı siber suç oltalama suçu olmuştur. İnsan faktörünün oltalama suçu riskini artıran etken olarak çıktığı çalışmada, işletmelerin siber ortamdaki görünürlüğünün siber suç mağduriyetini artırdığı görülmüştür. Araştırmanın sonuç kısmında ise analiz sonuçları yorumlanarak bireylere, işletmelere ve siber güvenlikle ilgili politika üreten kurumlara öneriler sunulmuştur.

Anahtar Kelimeler*: Siber, siber suç, siber güvenlik, işletme.*

THE SIZE OF CYBER CRIMES THAT BUSINESSES ARE EXPOSED

Abstract

People have started to change their habits such as shopping, meeting with friends, banking transactions with the technological developments and the spread of the internet. Through this change and the cyber environment, the concept of crime has also transformed and the concept of cyber crime has entered human life. Businesses trying to adapt to technology have faced the dangers of the cyber environment. The datasets of the Cybersecurity Breaches Survey 2021 were used as secondary data in the study, the general purpose of which is to investigate the factors that make businesses the target of a cybercrime. Few studies on businesses and cybercrime in Türkiye have been conducted on cyber security and cyber risk. In this research, the relationship between the size of the business, the human factor, digital visibility, cyber security measures, cyber awareness and cybercrime training with cyber crime victimization has been examined. As a result of the research, it was seen that medium and large enterprises were exposed to cybercrime more, while the most common cybercrime that businesses were exposed to was phishing. In the study, where the human factor was found to be the factor that increased the risk of phishing crime, it was seen that the visibility of businesses in the cyber environment increased the victimization of cybercrime. In the conclusion part of the research, the results of the analysis were interpreted and suggestions were presented to the individuals, enterprises and the institutions that produce policies related to cyber security.

Keywords: *Cyber, cybercrime, cybersecurity, business.*

GİRİŞ

Kurum, kuruluş ve devletler; teknolojik gelişmelerin sonucunda sundukları kritik hizmetleri bilişim sistemleri altyapısı ile yazılım ve donanımlara dayandırmış, fiziksel bilgi alışverişi yerine bilgi ve iletişim teknolojisi (BİT) cihazlarını kullanarak elektronik bilgi alışverişini siber ortamda gerçekleştirmeye başlamıştır. İnternet ve BİT cihazlarının toplum hayatının bir parçası hâline gelmesi ile siber ortamda da yeni saldırı fırsatları ortaya çıkmış, suç da dijitalleşmeye başlamıştır. Bazı geleneksel suçlar siber ortamın mesafe ve sınır tanımazlığı sayesinde siber ortamda veya siber ortamın yardımıyla işlenmeye başlarken yeni suç çeşitleri de oluşmaya başlamıştır. Dolayısıyla faydalarını neredeyse herkesin bildiği internet ile BİT cihazlarının, faydalarının yanında bir takım riskler de taşıdığı ortaya çıkmıştır. Günümüzde doğal afetler, terör, savaş, göç gibi risklerin yanında siber risk kavramı da yer almaya başlamıştır.

İşletmelerin siber ortamı ve BİT cihazlarını kullanımı giderek artmakla beraber maruz kaldığı siber suç sayısı ile maddi kayıplarda büyük artışlar yaşanmaktadır. Literatürde işletmeler ile siber suç, siber risk veya siber güvenlik ilişkisini inceleyen bireysel araştırmacılar tarafından yapılan çalışmalar *(Anderson vd., 2012; Veenstra vd., 2016)*, kamu kuruluşları tarafından yapılan/yaptırılan çalışmalar *(Klahr vd., 2016; Klahr vd., 2017; Wang vd., 2018; Vaidya, 2019; Johns, 2020; Johns, 2021a)* ve özel şirketler tarafından yapılan/yaptırılan çalışmalar *(International Business Machines [IBM], 2014; IBM, 2015; Ponemon Institute, 2016; Willis Towers Watson, 2017; Lewis, 2018; Accenture Security & Ponemon Institute, 2019; Marsh & Microsoft, 2019; Lewis vd., 2020)* mevcuttur. Türkiye'de ise bu ilişkiyi inceleyen araştırma *(Abduladheem, 2017; Bozgeyik, 2018; Büyükkılıç, 2018; Marsh & TÜSİAD [Türk Sanayicileri ve İş İnsanları Derneği], 2020)* yok denecek kadar azdır. Bu kapsamda siber suçlar ile işletmeler arasındaki ilişkiye yeterli önemin verilmediği değerlendirilmiştir.

Ekonominin temelini işletmeler oluşturmasına karşın başta Türkiye'de olmak üzere tüm dünyada işletmelerin maruz kaldığı siber suçlarda bir anlayış eksikliği ve tedbirsizlik mevcuttur. Bu değerlendirmeye alanda yeterli çalışma yapılmamasından, işletmelerin maruz kaldığı siber suç sayısı ile maddi kayıplardaki artıştan, çalışanlara siber suçla mücadele eğitimi verilmemesinden, siber güvenlik uzmanlarından destek alınmamasından varılmıştır.

Genel amacı; işletmeleri bir siber suçun hedefi hâline getiren faktörleri araştırmak olan çalışmada üç temel araştırma sorusuna yanıt aranmıştır;

- İşletmelerin maruz kaldığı siber suç riskleri nelerdir?
- İşletmeleri siber suçlular için uygun bir hedef hâline getiren faktörler nelerdir?
- Siber suç mağduriyetinin işletmelerin siber güvenlik önlemleri üzerindeki etkileri nelerdir?

İşletmelerin en yaygın maruz kaldığı; fidye yazılımı, zararlı yazılım, bilgisayar korsanlığı ve oltalama saldırıları (Klahr vd., 2017; Wang vd., 2018; Vaidya, 2019; Johns, 2020; Johns, 2021a) araştırmada maruz kalınan siber suç çeşitleri olarak işletimselleştirilmiştir.

Araştırmanın birinci temel araştırma sorusu olan; işletmelerin maruz kaldığı siber suç riskleri, aşağıdaki araştırma sorusu ile araştırılmıştır:

Soru 1: İşletmelerin maruz kaldığı siber saldırıların (fidye yazılımı, zararlı yazılım, oltalama, bilgisayar korsanlığı) ve uğranılan zararın boyutları nelerdir?

Araştırmanın ikinci temel araştırma sorusu olan; bir işletmeyi uygun bir hedef hâline getiren faktörler ise *işletmenin büyüklüğü*, *insan faktörü* ve *dijital görünürlük* ile işletimselleştirilmiş ve çeşitli hipotezler ile araştırılmıştır.

İşletmenin büyüklüğü: Araştırmada işletmeler çalışan sayısına göre mikro, küçük, orta ve büyük olarak dört sınıfa ayrılmıştır. Büyük işletmeler sınıfına giren işletmelerde çalışan sayısı, değerli veri ve mali kaynaklar daha fazla olduğu için büyük işletmelerin siber suça maruz kalma olasılığının diğer işletmelere nazaran daha yüksek olduğu değerlendirilmiştir.

H_1: İşletmenin büyüklüğü ile uğranılan zararın büyüklüğü arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_2: İşletmenin büyüklüğü ile siber suç mağduru olma olasılığı arasında istatistiksel olarak anlamlı bir ilişki vardır.

İnsan faktörü: Siber suçlarla mücadele edecek unsurlar bir futbol metaforu ile betimlenirse son savunma hattı oyuncuları, bilgisayar kullanıcılarıdır (Jansen, 2017, s. 55). İnsan faktöründe insandan kaynaklı davranışlar esas alınmıştır. Önceki araştırmalarda da insan faktörünün siber suç mağduriyetinde en büyük paya sahip olduğu ortaya çıkmıştır (IBM, 2015; Willis Towers Watson, 2017; Tessian, 2020; Akdemir & Lawless, 2020; Karsperky, 2021c).

H_3: İnsan faktörü ile işletmelerin siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır.

Dijital görünürlük: Bir işletmenin siber ortamdaki genel varlığıdır. Yapılan çalışmada dijital görünürlüğün siber suç mağduriyeti üzerindeki etkisi Cohen ve Felson'un (1979) bir hedefin suça maruz kalma riskini açıkladığı *VIVA (*value [değer], inertia [hareket kabiliyeti], visibility [görünürlük], access [ulaşılabilirlik]) kuramı ile açıklanmıştır. Bu kapsamda dijital görünürlük; değer, görünürlük ve ulaşılabilirlik ile işletimselleştirilmiştir. Hareket kabiliyeti hedefin taşınabilirliği ile ilgili olup taşınabilirlik siber suçta hedefteki verinin boyutu olarak değerlendirilebileceğinden araştırma kapsamından hariç tutulmuştur.

H_4: Siber ortamda işletmelerin değeri ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_5: Siber ortamda işletmelerin görünürlüğü ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_6: Siber ortamda işletmelerin ulaşılabilirliği ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır.

Araştırmadaki üçüncü temel araştırma sorusunda siber suç mağduriyetinin işletmelerin güvenlik önlemleri üzerindeki etkileri araştırılmıştır. Siber ortamda bilgi teknolojileri uzmanları ya da siber güvenlik uzmanları gibi fiziksel koruyucuların yanı sıra antivirüs programı, istenmeyen mesaj (spam) filtresi, casus yazılım önleme programı, güvenlik duvarı gibi teknolojik koruyucular vardır (Yar, 2005, s. 423). Siber güvenlik önlemlerinin yanı sıra siber güvenlik farkındalığı ve siber suçla mücadele eğitimi de siber güvenlikte önem arz eden iki önemli unsurdur. Siber farkındalık bireylere siber ortamı, siber suç çeşitlerini, siber suçların işlenme şekillerini ve olası sonuçlarını anlatıp siber ortamın risklerini temel seviyede kazandırmaktır. Yapılan araştırma ve anketlerde siber güvenlik eğitimi veren işletmelerin siber suç mağduriyetinin daha düşük olduğu görülmüştür (Willis Towers Watson, 2017; Johns, 2021a).

H_7: Siber suç mağduriyeti ile işletmelerin uygulamış olduğu siber güvenlik önlemleri arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_8: Siber suç mağduriyeti ile siber farkındalık arasında istatistiksel olarak anlamlı bir ilişki vardır.

H_9: Siber suç mağduriyeti ile siber suçla mücadele eğitimi arasında istatistiksel olarak anlamlı bir ilişki vardır.

Yapılan araştırma ile siber suçlar neticesinde ciddi kayıplar yaşayan başta işletmeler ve suçun önlenmesiyle ilgili politika yapıcılar olmak üzere birey, kurum ve kuruluşlar için önemli bilgilere ulaşıldığı değerlendirilmiştir.

1. SİBER SUÇ ve İŞLETME

Araştırma; işletme ve siber suç olmak üzere iki temel kavramdan oluşmaktadır. Bu konuda çalışmanın daha iyi anlaşılması bakımından kavramsal bir bakış açısıyla siber suçun tanımı, siber suç çeşitleri, işletmenin tanımı ve işletme türlerinin açıklanmasıyla araştırmaya başlamanın daha faydalı olacağı değerlendirilmiştir.

1.1. Siber Suç Kavramı ve Tanımı

Siber suç kavramı yeni bir kavram olmasa da literatürde kavramın genel kabul görmüş bir tanımı yoktur (Gordon & Ford, 2006, s. 13). Google Akademik'te siber suç ile ilgili en çok atıf alan bazı eserler incelendiğinde; Wall (2004, s. 2) bilgisayar içeren her suçu siber suç olarak adlandırmanın yanlış olacağını, siber suçun ağ bağlantılı teknolojiler ile internetin sağlamış olduğu küresel yetenekle internet üzerinden işlenen suç olduğunu ifade etmiştir ve siber suçu, ağ bağlantılı cihazlarla aracılık edilen ve siber ortamda işlenen suç olarak tanımlamıştır (Wall, 2007, ss. 10-11).

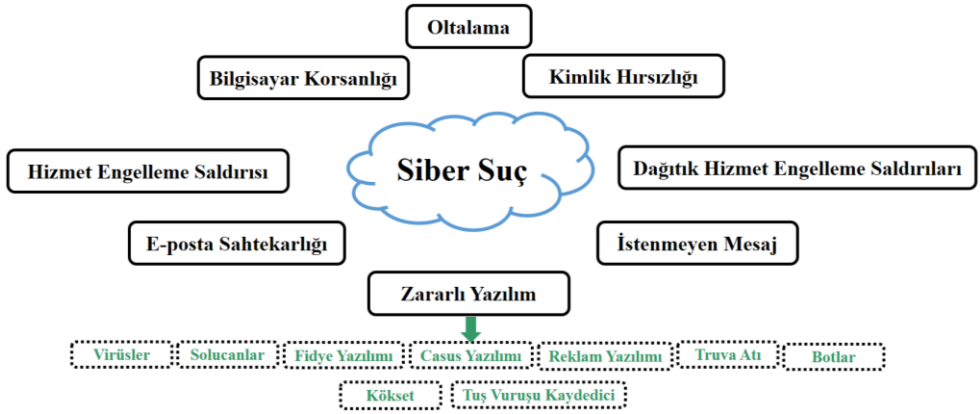
Gordon ve Ford'un (2006, s. 14) siber suç tanımında bilgisayar veya bilişim cihazlarını, Thomas ve Loader'ın (2000, s. 3) ise bilgisayar ve ağ kavramlarını ön plana çıkardığı görülmüştür. Wall (2007), Thomas ve Loader (2000) ile Gordon ve Ford'un (2006) siber suç tanımlarında siber ortam ön plana çıkmasa da suçun bilgisayar veya ağ teknolojili cihazlar vasıtasıyla icra edileceği ifade edilmiştir. Bu tanımlardan yola çıkarak siber suç; *BİT cihazlarının hedef, fail veya kolaylaştırıcı olarak kullanıldığı, genellikle internet veya ağ üzerinden işlenen suç* olarak tanımlanmıştır.

Sonuç olarak etkileriyle mekan ve sınır tanımayan (Grabosky, 2001, s. 243), bu yüzden de mevzuatta birliktelik gerektiren siber suç kavramında (Jakankhani vd., 2014, s. 152) tam bir küresel birliktelik yoktur. Ancak teknolojideki hızlı gelişmeler nedeniyle literatürde bilgisayar ve ağ teknolojisinin yardımıyla işlenen suçlar için bilgisayar suçu, yüksek teknoloji suçu, sanal suç gibi farklı kavramlar kullanılmış, siber suç da "*çok çeşitli suçları ve davranışları içeren bir şemsiye terim*" hâline gelmiştir (Marion ve Twede, 2020, s. xi). Literatürde siber suç kavramı genel kabul gören bir terim olmaya başlarken araştırmamızda da bilgisayar

ve ağ teknolojisinin yardımıyla işlenen suçlar ile ilgili siber suç terimi kullanılmıştır.

1.2. Siber Suç Çeşitleri

Siber suç; BİT cihazlarının hedef, fail veya kolaylaştırıcı olarak kullanıldığı, internet üzerinden işlenen suç olup kullanılan teknikler, hedefte istenen etki ve yayılma biçimi gibi etkenlere göre birçok çeşidi bulunmaktadır:



Şekil 1.1. Siber suç çeşitleri

Yapılan araştırmalarda işletmelerin en yaygın yaşadığı siber suçlar sırasıyla oltalama, zararlı yazılım *(fidye yazılımı hariç)*, bilgisayar korsanlığı ve fidye yazılımı saldırıları olarak ortaya çıkmıştır (Klahr vd., 2017; Wang vd., 2018; Vaidya, 2019; Johns, 2020; Johns, 2021a). Bu kapsamda dört siber suç çeşidinin tanımlarına yer verilmiştir:

1.2.1. Zararlı Yazılım

Zararlı yazılım, "özel bilgi veya verilere zarar vermek, bunlara erişmek veya bunları çalmak amacıyla, ağlara ve bilgisayarlara sızmak için kullanılan her türlü zararlı yazılım programı veya kodu" anlamına gelmektedir (Marion & Twede, 2020, s. 249). Zararlı yazılımların ortak yönü kullanıcı tarafından istenmemesi, bilinmemesi veya kullanıcıya düşman olmasıdır (Pecora, 2009, s. 121).

Zararlı yazılımlar genellikle e-posta, web tabanlı aktif içerikler, anlık mesajlaşma ve eşler arası (peer-to-peer) uygulamalar yoluyla bulaşmaktadır (Jackson, 2018, s. 619). Zararlı yazılımlar bulaştıkları cihazda verileri silme, çalma, yok etme, zarar verme, yeni siber saldırılara olanak sağlama, saldırı başlayana

kadar uykuda bekleme gibi özelliklere sahiptir. Birçok zararlı yazılım çeşidi bulunmaktadır. Bunlardan bazıları aşağıdaki gibidir:

- *Virüsler;* adını biyolojik virüsten almış olup konakçı olarak bir bilgisayar ile insan eylemine (virüslü e-postanın bir başkasına iletilmesi gibi) ihtiyaç duymakta ve insan eylemiyle ana bilgisayardan yayılmaktadır (Marion & Twede, 2020, ss. 431-432; Johansen, 2020).

- *Solucanlar;* virüslerin aksine yayılmak için de kullanıcı eylemine ihtiyaç duymadan ağlar üzerinden yayılabilen bir zararlı yazılım çeşididir (Marion & Twede, 2020, s. 450). Solucanlar bir ana bilgisayara bulaştıktan sonra güvenlik açığı olan bilgisayarları arayıp savunmasız olanlara kopyalarını yerleştirip hızlıca yayılabilme yeteneğine sahiptir (Ahmad, 2021, s. 987).

- *Fidye yazılımları;* kullanıcının bilgisayarını veya bazı dosyalarını kilitleyip kullanıcıdan fidye talep etmek amacıyla tasarlanmış bir zararlı yazılım çeşididir. Fidye yazılımcılar; kullanıcıları fidye ödenmediği takdirde bilgisayar sistemini bozma, verileri yok etme, zarar verme, dosyaları silme veya özel belgeleri ifşa etmekle tehdit etmektedir (Kharraz, 2018, s. 721).

1.2.2. Bilgisayar Korsanlığı

"Bilgisayar becerilerini başka bir kişinin veya kuruluşun bilgisayar sistemine veya ağına izinsiz veya yetkisiz olarak erişmek için kullanan kişi" *bilgisayar korsanı*, yaptığı iş de *bilgisayar korsanlığı* olarak tanımlanmıştır (Marion ve Twede, 2020, s. 205). Bilgisayar korsanları yetenekleri ile sisteme zararlı yazılım yükleyebilmekte, dosyaları silme, zarar verme, veri alma gibi işlemleri yapabilmekte, web sitelerinden kullanıcı bilgilerini çalabilmekte, bilgisayar sisteminin yazılım veya donanımını değiştirebilmekte, hatta sistemi tamamen kapatabilmektedir.

1.2.3. Oltalama

Oltalama, siber suçluların kendisini başka bir şahıs, işletme veya kurum gibi tanıtarak sahte web sitesi, sahte e-posta, sosyal medya aracılığıyla sosyal mühendislik gibi çeşitli teknikleri kullanarak kurbana ait kişisel bilgileri elde etmeye çalıştığı bir yazılım çeşididir **(**Woelk, 2009a, s. 140; Marion ve Twede, 2020, ss. 316-317). Burada siber saldırganın hedefi kurbanın kimlik ya da finansal bilgilerine erişmek olduğu hâlde yöntem olarak sosyal mühendislik, sahte e-posta, sahte web sitesi ya da başka teknikler kullanabilmektedir.

1.3. İşletme Kavramı ve Tanımı

"Tarım, sanayi, ticaret, bankacılık vb. iş alanlarında, kâr amacıyla bir sermaye yatırılarak kurulan kurum" (TDK, 2019) olarak tanımlanan işletmeler, bir ülkede sağlıklı ve güçlü bir ekonomiye sahip olmanın en önemli şartlarını oluşturmaktadır (Mucuk, 2011, s. 1). Ekonomiyi en basit tanımıyla kıt kaynakların verimli kullanımı olarak tanımlarsak işletmeler de bu kıt kaynakların üretiminden ve dağıtımından sorumlu olup ekonominin temel taşlarındandır.

İşletmelerin bir araya gelmesi ile ekonomi oluşmaktadır (Mucuk, 2011, s. 9). İşletmeler ürettikleri mal ve hizmetleri pazara sunarken aynı zamanda da yeni mal ve hizmet üretmek için de hammadde, iş gücüne ihtiyaç duymaktadır. İnsan da bir yandan işletmelerin ürettiği mal veya hizmetlerin tüketicisi konumundayken bir yandan da üreticisi konumundadır. İnsan ihtiyaçlarının sonsuz olduğu günümüzde işletmeler hem insanın mevcut ihtiyaçlarını ürettikleri mal ve hizmetler ile karşılarken hem de gelecekteki ihtiyaçları için mal ve hizmet üretmektedir (Ürper, 2018, ss. 3-4).

1.4. İşletme Türleri

Yapısı gereği işletmeler çeşitli sınıflara ayrılmaktadır. Literatürde işletmelerin ekonomik yapısı, sermaye sahipliği, büyüklükleri, faaliyet konusu, hukuki yapıları açılarından çeşitli sınıflandırmalara ayrıldığı görülmüştür. Ancak mevcut çalışmada işletmeler büyüklüklerine göre sınıflandırılıp analiz edildiğinden bu bölümde büyüklüklerine göre işletme çeşitleri açıklanmıştır.

1.4.1. Büyüklüklerine Göre İşletme Türleri

İşletmeleri büyüklüklerine göre sıralarken niteliksel ve niceliksel özellikler ön plana çıkmaktadır. "Yıllık satışlar, yıllık kârlar, varlıklar, öz sermaye miktarı, çalışanların sayısı, yatırımların toplamı" niceliksel (kantitatif) ölçütler iken, "sermaye koyanların sayısı, yönetim biçimi, bölgeye yönelik olup olmama, endüstri dalındaki nispi durum, hukuki şekil" niteliksel (kalitatif) ölçülerdir (Mucuk, 2011, ss. 94-98).

Araştırmada Türkiye'de bulunan mevzuatlar ele alınmış ve Türkiye İstatistik Kurumu (TÜİK) tarafından yapılan araştırmalarda da kullanılan *mikro, küçük, orta ve büyük ölçekli işletme* sınıflandırması kullanılmıştır.

Mikro, küçük ve orta işletmelerin tanımlarına 25997 sayılı Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik'te (2005, md. 5) aşağıdaki gibi yer verilmiştir:

- *Mikro işletmeler*: "On kişiden az yıllık çalışan istihdam eden ve yıllık net satış hasılatı veya mali bilançosundan herhangi biri üç milyon Türk lirasını aşmayan işletmeler."

- *Küçük işletmeler*: "Elli kişiden az yıllık çalışan istihdam eden ve yıllık net satış hasılatı veya mali bilançosundan herhangi biri yirmi beş milyon Türk lirasını aşmayan işletmeler."

- *Orta işletmeler*: "İki yüz elli kişiden az yıllık çalışan istihdam eden ve yıllık net satış hasılatı veya mali bilançosundan herhangi biri yüz yirmi beş milyon Türk lirasını aşmayan işletmeler."

- *Büyük işletmeler* ise 29793 sayılı Perakende Ticarette Uygulanacak İlke ve Kurallar Hakkında Yönetmelik'te (2016, md. 3/d) orta ölçekli işletme sınırını aşan işletmeler olarak tanımlanmıştır.

2. ARAŞTIRMANIN METODOLOJİSİ

Araştırmada nicel araştırma deseni kullanılmıştır. Anket veri toplama yöntemi ile işletmelerden elde edilmiş olan veriler sosyal bilimler istatistik paketi (statistical package for the social sciences – SPSS) nicel analiz yazılımı aracılığı ile analize tabi tutulmuştur. Araştırmada ikincil veri olarak Birleşik Krallık Dijital, Kültür, Medya ve Spor Dairesi Başkanlığı tarafından yaptırılan Siber Güvenlik İhlalleri Anketi 2021'in veri setleri kullanılmıştır.

Araştırmanın ilk örneklem grubu 89372 işletmeden oluşmakta iken işletmenin telefonuna ulaşılamaması, yanlış numara gibi operasyonel nedenlerden dolayı 29074 işletmeye ulaşılmıştır. Araştırmada rastgele olasılıklı olarak örnekleme seçilen 29074 işletmeden 17947 işletmeye anket uygulanmıştır. Ancak çeşitli operasyonel nedenlerle 1419 işletme anketi tamamlamıştır (Johns, 2021b, s. 15). Bu sonuç da veri toplamının zorluğunu göz önüne sermektedir.

Araştırmada, Birleşik Krallık'ın son beş yıldaki Siber Güvenlik İhlalleri Anketi araştırmaları incelenmiş ve işletmelerin en yaygın maruz kaldığı siber suç çeşitleri belirlenmiştir. Bunlar araştırmanın bağımlı değişkenlerini *(bilgisayar korsanlığı, zararlı yazılım, fidye yazılımı, oltalama saldırısı)* oluşturmuştur. Sonrasında ise işletmeleri bir siber suçun hedefi hâline getiren unsurlar literatürde taranmış ve araştırmanın bağımsız değişkenleri *(insan faktörü, dijital görünürlük, siber güvenlik önlemleri, siber farkındalık)* oluşturulmuştur.

Araştırmada öncelikle araştırma verilerinin daha kolay anlaşılmasını sağlamak maksadıyla sıklık, yüzde ve ortalamasının grafik veya tablolar ile ifade edildiği

betimsel analiz (Yıldız, 2019, s. 172) kullanılmıştır. Sonrasında ise değişkenler arasındaki ilişkilerin varlığını, gücünü ve yönünü incelemek için Pearson Ki-kare testi, çapraz tablolamalar ve değişkenler arası ilişkinin gücünü artırmak için Phi testi kullanılmıştır.

3. ARAŞTIRMANIN BULGULARI

Araştırmanın bu bölümünde Siber Güvenlik İhlalleri Anketi 2021'in nicel analiz sonuçları sunulmuştur. Bu amaçla öncelikle tanımlayıcı istatistiksel veriler açıklanacak, sonrasında ise hipotezler test edilecektir.

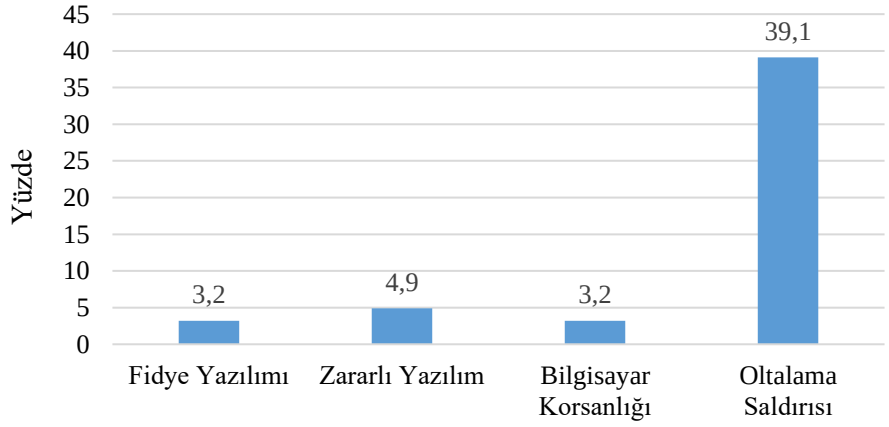
3.1. Betimsel İstatistiklerin Analizi

Örneklemdeki yapıların sıklığı hakkında bilgi sunmak amacıyla nicel analizde kullanılan değişkenlerin temel tanımlayıcı istatistiklerinin analizi bu bölümde sunulmuştur.

3.1.1. Bağımlı Değişken

Bu bölümde araştırmanın bağımlı değişkenleri olan *fidye yazılımı, zararlı yazılım, bilgisayar korsanlığı ve oltalama saldırısı* suçlarına maruz kalan işletmeler analiz edilmiştir.

Yapılan incelemede işletmelerin maruz kaldığı siber suçlarda fidye yazılımı, zararlı yazılım, bilgisayar korsanlığına maruz kalma oranlarının yakın olduğu, oltalama saldırısının ise diğer siber suç türlerine göre çok daha yaygın olduğu görülmüştür.



Şekil 3.1. Bağımlı değişkenlerin siber suça maruz kalma oranlarının karşılaştırılması

3.1.2. Bağımsız Değişken

Araştırmanın bağımsız değişkenleri insan faktörü, dijital görünürlük, siber güvenlik önlemleri ve siber farkındalık olarak dört başlıkta incelenmiştir:

- *İnsan faktörü*; siber suç açısından uzaktan veya mobil çalışma, çalışanların BT cihazlarını kullanması, fiziksel belleklerde bilgi saklama ve kişisel cihazların ticari faaliyetler için kullanılması olarak işletimselleştirilmiştir.

- *Dijital görünürlük*; bir işletmenin siber ortamdaki genel varlığı olup Felson ve Clarke'ın (1998, s. 5) VIVA (değer, hareket kabiliyeti, görünürlük, ulaşılabilirlik) kuramı ile açıklanmıştır.

- *Siber güvenlik önlemleri*; siber saldırılara karşı kişiler, kuruluşlar ya da devletler tarafından alınan tedbirler siber güvenlik önlemleridir. Siber güvenlik önlemleri; elektronik cihazların güvenliğini koruma, kurumsal verileri koruma ve çalışanlara yönelik koruma önlemleri olarak üç başlıkta incelenmiştir.

- *Siber farkındalık*; bireylerin siber ortam, siber güvenlik, siber suç ve siber suçların nasıl gerçekleştiği konusunda bilgisinin var olmasıdır (Marion ve Twede, 2020, s. 20). Bu kapsamda siber farkındalık siber suçlarla mücadele eğitimi ve siber farkındalık ile işletimselleştirilmiştir.

3.2. İki Değişkenli Analizler

İki değişkenli analizde bağımsız değişkenler ile bağımlı değişkenler arasındaki ilişki çapraz tablolar yapılarak analiz edilmiştir. Analizlerini test etmek amacıyla yapılan çapraz tablolarda H_0 (boş hipotez) bağımsız değişkenler ile bağımlı değişkenler arasında ilişkinin olmadığını ifade ederken H_a (alternatif hipotez) ilişkinin varlığına atıfta bulunmaktadır.

3.2.1. İşletmelerin Büyüklüğü ile Uğranılan Siber Suç Zararı İlişkisi

Ki-kare testi sonuçları, işletmenin büyüklüğü ile uğranılan siber suç zararı arasında istatistiksel olarak anlamlı bir şekilde ilişkili olduğunu ($\chi 2$=50,939, $p\leq$ 0,05) göstermiştir. Phi değeri ise 0,286 olup değişenler arası orta seviyede bir ilişkinin olduğu sonucu ortaya çıkmıştır. İki değişkenli analizin sonucunda P değeri 0.05'ten küçük olduğu için $H1_o$ hipotezi reddedilmiş ve alternatif hipotez kabul edilmiştir. Sonuç olarak; $H1_a$ *(işletmenin büyüklüğü ile uğranılan zararın büyüklüğü arasında istatistiksel olarak anlamlı bir ilişki vardır)* hipotezi kabul edilmiştir.

Araştırmada siber suç mağduriyeti dört siber suç için ele alınmıştır. Bu bağlamda işletmenin büyüklüğü ile fidye yazılımı, zararlı yazılım, bilgisayar korsanlığı ve oltalama saldırısı mağduriyeti arasındaki ilişki iki değişkenli çapraz tablo analizleri ile teker teker incelenmiştir.

Fidye yazılım ve *bilgisayar korsanlığı* mağduru olmada p değeri 0,05'ten büyük olduğu için işletmenin büyüklüğü ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki olmadığı sonucu ortaya çıkmıştır. Ki kare test sonuçları *zararlı yazılım* ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir şekilde ilişki olduğunu ($\chi2$=13,722, $p\leq$0,05) göstermiştir. Phi değeri 0,098 olup değişenler arası ilişki zayıftır. Zararlı yazılım ve siber suç mağduru olma oranları incelendiğinde işletmenin büyüklüğü arttıkça siber suç mağduriyetinin arttığı görülmüştür.

O*ltalama saldırısı* ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki olduğu ($\chi2$=93,293, $p\leq$0,001) görülmüştür. Phi değeri 0,256 olup değişenler arası orta seviyede bir ilişki olduğu sonucu ortaya çıkmıştır.

Siber suç mağduru olmanın ölçüldüğü dört siber suç çeşidinden sadece ikisinin değişkenler arasındaki ilişkisi istatistiksel olarak anlamlı olduğu için $H2_0$ *(işletmelerin büyüklüğü ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

3.2.2. İnsan Faktörü Siber Suç Mağduru Olma İlişkisi

Analiz sonucunda insan faktörü ile işletimselleştirilen dört özelliğin sadece oltalama saldırısı mağduriyeti ile istatistiksel olarak anlamlı bir ilişkide olduğu görülmüştür. Bu kapsamda;

- Uzaktan veya mobil çalışma ile oltalama saldırısı mağduriyeti arasındaki ilişkinin ($\chi2$=9,964, p≤0.001) istatistiksel olarak anlamlı olduğu, phi değerinin 0,12 olup değişkenler arasında orta seviyede ilişki olduğu,

- Çalışanların BT cihazlarını kullanması ile oltalama saldırısı mağduriyeti arasındaki ilişkinin ($\chi2$=16,769, p≤0.001) istatistiksel olarak anlamlı olduğu, phi değerinin 0,155 olup değişkenler arasında orta seviyede ilişki olduğu,

- Kişisel cihazların ticari faaliyetler için kullanılması ile oltalama saldırısı mağduriyeti arasındaki ilişkinin ($\chi2$=5,902, p≤0.001) istatistiksel olarak anlamlı olduğu, phi değerinin 0,092 olup değişkenler arasında zayıf seviyede ilişki olduğu,

- Fiziksel belleklerde bilgi saklama ile oltalama saldırısı mağduriyeti arasındaki ilişkinin ($\chi 2=0,176$ $p\leq 0.001$) istatistiksel olarak anlamlı olduğu, phi değerinin 0,016 olup değişkenler arasında zayıf seviyede ilişki olduğu görülmüştür.

Sonuç olarak; insan faktörü sadece oltalama saldırısının mağduru olmada istatistiksel olarak anlamlı olduğu için, diğer siber suç çeşitlerinde istatistiksel olarak anlamlı görülmediği için $H3_0$ *(insan faktörü ile işletmelerin siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

3.2.3. Dijital Görünürlük ile Siber Suç Mağduru Olma İlişkisi

Dijital görünürlük Felson ve Clark'ın (1998) VIVA kuramının *değer* (value), *görünürlük* (visibility) ve *ulaşılabilirlik* (accessibility) unsurları ile üç kategoride işletimselleştirilmiştir. *Hareket kabiliyeti* (inertia) hedefin taşınabilirliği ile ilgilidir, bu da siber suçta hedefteki verinin boyutu olarak değerlendirilebilecek olup araştırma kapsamından hariç tutulmuştur.

- Hedefin değeri ile siber suç mağduru olma ilişkisi

Değer, bir hedefin kolayca elden çıkarılıp çabucak maddi kazanç getirecek olmasıdır. Araştırmada hedefin değeri teknolojinin gelişmesiyle beraber işletmelerin sahip olma ihtiyacı duyacağı iki yetenek ile ölçülmüştür. Birincisi; *müşterileriniz/lehtarlarınız, hizmet kullanıcıları veya bağışçılarınız hakkında elektronik ortamda kişisel bilgi tutma* olup sadece oltalama suçu mağduriyeti ile aralarında ($\chi 2=28,378$, $p\leq 0.001$) istatistiksel olarak anlamlı bir ilişki olduğu sonucu ortaya çıkmıştır. Phi değeri ise 0,143 değişkenler arasında orta seviyede bir ilişki vardır. Diğer üç siber suç mağduriyetinde p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki bulunamamıştır.

İkincisi; *kuruluşunuzun veya müşterilerinizin ödeme yaptığı bir çevrim içi banka hesabı kullanımı* olup herhangi bir siber suç mağduriyeti çeşidi ile aralarında istatistiksel olarak anlamlı bir ilişki bulunamamıştır.

Sonuç olarak; hedefin değerinin işletimselleştirildiği iki değişkenden sadece birinin bir siber suç türü ile istatistiksel olarak anlamlı olduğu için $H4_0$ *(Siber ortamda işletmelerin değeri ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

- Hedefin görünürlüğü ile siber suç mağduru olma ilişkisi

Hedefin görünürlüğü işletmelerin günümüzde kullanacağı iki özellik ile ölçülmüştür. Birincisi, *sosyal medya sitelerindeki hesap veya sayfa (ör. Facebook veya Twitter) kullanımıdır*. Değişkenler arasındaki ilişki; fidye yazılımı mağduru olmada ($\chi2$=3,825, p≤0.05), bilgisayar korsanlığı mağduru olmada ($\chi2$=0,452, p≤0.05) ve oltalama saldırısı mağduru olmada ($\chi2$=27,089, p≤0.001) istatistiksel olarak anlamlıdır. Phi değerleri ise sırasıyla 0,052, 0,018, 0,138'dir. Zararlı yazılım mağduriyetinde ($\chi2$=3,825, p≥0.05) ise değişkenler arasında istatistiksel bir anlamlı bir ilişki bulunamamıştır.

Hedefin görünürlüğü ile işletimselleştirilen ikinci özellik; *müşterilerin çevrim içi ürün veya hizmetler için sipariş verme, rezervasyon yapma veya ödeme yapma yeteneğidir*. Değişkenler arasındaki ilişki fidye yazılımı mağduriyetinde ($\chi2$=7,478, p≤0.05), zararlı yazılım mağduriyetinde ($\chi2$=6,012, p≤0.05) ve bilgisayar korsanlığı mağduriyetinde ($\chi2$=11,439, p≤0.001) olup istatistiksel olarak anlamlıdır. Phi değerleri sırasıyla 0,073, 0,064, 0,090'dır. Oltalama saldırısı mağduriyetinde p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki bulunamamıştır.

Sonuç olarak siber ortamda hedefin görünürlüğünün siber suç mağduru olmayı artırdığını ifade eden $H5_a$ *(siber ortamda işletmelerin görünürlüğü ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki vardır)* kabul edilmiştir.

- Hedefin ulaşılabilirliği ile siber suç mağduru olma ilişkisi

Ulaşılabilirlik; suçlunun hedefe ulaşması ve sonrasında suç mahallinden uzaklaşma yeteneği olup iki özellik ile işletimselleştirilmiştir.

Windows'un eski sürümlerinin yüklü olduğu bilgisayarlar (ör. Windows 7 veya 8) kullanımı ile zararlı yazılım mağduriyeti ($\chi2$=4,549, p ≤0.05) arasında istatistiksel olarak anlamlı bir ilişki bulunduğu, phi değerinin 0,057 olduğu için değişkenler arasında zayıf bir ilişki olduğu görülmüştür. Fidye yazılımı mağduriyeti, oltalama saldırısı mağduriyeti ve bilgisayar korsanlığı mağduriyeti ile arasındaki ilişkide p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki bulunmamıştır.

Bazen akıllı cihazlar olarak adlandırılan televizyonlar, bina kontrolleri, alarmlar, hoparlörler vb. gibi ağa bağlı cihazların kullanımı ile fidye yazılımı mağduriyeti, zararlı yazılım mağduriyeti ve bilgisayar korsanlığı mağduriyeti

arasında p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki bulunamamıştır. Oltalama saldırısı mağduriyeti ile arasında ise ($\chi 2$=14,802, $p \leq 0.001$) istatistiksel olarak anlamlı bir ilişki olup phi değeri 0,102 olduğundan orta seviyede ilişki mevcuttur.

Sonuç olarak hedefin ulaşılabilirliğini ifade eden özelliklerden ikisi ile siber suç mağduru olma arasında istatistiksel anlamda ilişki olmadığından $H6_0$ *(siber ortamda işletmelerin ulaşılabilirliği ile siber suç mağduru olma arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

3.2.4. Siber Suç Mağduriyeti ile Siber Güvenlik Önlemleri Arasındaki İlişki

Siber güvenlik önlemleri elektronik cihazların güvenliğini koruma, kurumsal verileri koruma ve çalışanlara yönelik koruma önlemleri esas alınarak işletimselleştirilmiş ve on dört siber güvenlik önlemiyle işletmelerin almış oldukları siber güvenlik önlemleri ile siber suç mağduriyeti arasındaki ilişki analiz edilmiştir. Analiz sonucunda altı siber güvenlik tedbiri ile siber mağduriyet arasında istatistiksel olarak anlamlı ilişki olduğu görülmüştür.

Elektronik cihazların güvenliğini koruma;

- Personel ve ziyaretçiler için ayrı wi-fi ağları *(istatistiksel olarak anlamlı)*,
- Yazılım güvenlik güncellemelerini 14 gün içinde uygulamaya yönelik bir politika *(istatistiksel olarak anlamlı değil)*,
- Uzaktan bağlanan personel için sanal özel ağ tedbirleri *(istatistiksel olarak anlamlı)*,
- Şirkete ait cihazlarda (örneğin dizüstü bilgisayarlar) güvenlik kontrolleri *(istatistiksel olarak anlamlı)*,
- Tüm BT ağınızı ve ayrıca bireysel cihazları kapsayan güvenlik duvarları *(istatistiksel olarak anlamlı değil)*,
- Güncel zararlı yazılım koruması *(istatistiksel olarak anlamlı değil)*,
- Yalnızca şirkete ait cihazlar aracılığıyla erişime izin verilmesi *(istatistiksel olarak anlamlı)*.

Çalışanlara yönelik koruma;

- Personelin sahte bir e-posta veya kötü amaçlı bir web sitesi belirlediklerinde izlemesi için üzerinde anlaşmaya varılan bir süreç *(istatistiksel olarak anlamlı)*,

- Kullanıcı etkinliğinin herhangi bir şekilde izlenmesi *(istatistiksel olarak anlamlı)*,
- Kullanıcıların güçlü parolalar belirlemesini sağlayan bir parola ilkesi *(istatistiksel olarak anlamlı değil)*,
- BT yöneticisini ve belirli kullanıcılara erişim haklarını kısıtlama *(istatistiksel olarak anlamlı değil)*,

Kurumsal verileri koruma;

- Bir bulut hizmeti aracılığıyla verileri güvenli bir şekilde yedekleme *(istatistiksel olarak anlamlı değil)*,
- Verileri başka yollarla güvenli bir şekilde yedekleme *(istatistiksel olarak anlamlı değil)*,
- Kişisel veri dosyalarının güvenli bir şekilde saklanması ve taşınması için özel kurallar *(istatistiksel olarak anlamlı değil)*.

Sonuç olarak on dört siber güvenlik önleminden sadece altısı ile istatistiksel olarak anlamlı çıktığı için $H7_0$ *(siber suç mağduriyeti ile işletmelerin uygulamış olduğu siber güvenlik önlemleri arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

Ancak işletmelerin en yaygın siber suç mağduru olduğu oltalama suçu mağduriyetinin 14 siber güvenlik önlemi ile istatistiksel olarak anlamlı bir ilişkide olduğu, ayrıca değişkenler arasında orta derecede bir ilişki ortaya çıkmıştır. Bu yüzden "*oltalama suçu mağduriyeti ile siber güvenlik mağduriyeti arasında istatistiksel olarak anlamlı bir ilişki vardır"* sonucuna da erişilmiştir.

3.2.5. Siber Suç Mağduriyeti ile Siber Farkındalık Arasındaki İlişki

Siber farkındalık siber suçlarla mücadele eğitimi ve siber farkındalık ile işletimselleştirilmiştir. Siber suç mağduriyeti ve siber farkındalık ilişkisinin analizi sonucunda sadece oltalama saldırısı mağduriyeti ile siber farkındalık arasında istatistiksel olarak anlamlı ($\chi 2=30{,}562$, $p\leq 0.001$) bir ilişki olduğu görülmüştür. Phi değeri ise -0,147 olup değişkenler arasında orta seviyede negatif bir ilişki olduğu görülmüştür. Sonuç olarak dört siber suç mağduriyetinden sadece oltalama suçu ile siber farkındalık arasında istatistiksel olarak anlamlı bir ilişki olduğu için $H8_0$ *(Siber suç mağduriyeti ile işletmelerin siber farkındalığı arasında istatistiksel olarak anlamlı bir ilişki yoktur)* kabul edilmiştir.

Siber suçla mücadele eğitimi alma eğilimi ile fidye yazılımı mağduriyeti ($\chi2=3,991$ $p\leq0.05$), bilgisayar korsanlığı mağduriyeti ($\chi2=13,721$ $p\leq0.001$) ve oltalama saldırısı mağduriyeti ($\chi2=49,135$ $p\leq0.001$) arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmüştür. Phi değerleri ise sırasıyla -0,053, -0,098, -0,186'dır. Buna göre değişkenler arasındaki ilişki ile fidye yazılımı ve bilgisayar korsanlığı mağduriyeti için negatif zayıf seviyede olup oltalama suçu için negatif orta seviyededir. Zararlı yazılım mağduriyetinde ise p değeri 0,05'ten büyük olduğu için istatistiksel olarak anlamlı bir ilişki görülmemiştir. Siber suç mağduriyeti ile siber suçla mücadele eğitimi alma oranları incelendiğinde ise siber suç mağdurlarının daha az siber suçla mücadele eğitimi aldığı görülmüştür.

Sonuç olarak; dört siber suç mağduriyetinden üçü siber suçla mücadele eğitimi ile istatistiksel olarak anlamlı bir ilişkide olduğu için $H9_a$ *(Siber suç mağduriyeti ile işletmelerin siber suçlarla mücadele eğitimi alma eğilimi arasında istatistiksel olarak anlamlı bir ilişki vardır)* kabul edilmiştir.

4. SONUÇ VE ÖNERİLER

İşletmeleri bir siber suçun hedefi haline getiren faktörleri belirlemek amacıyla gerçekleştirilen bu çalışmada; işletmelerin büyüklükleri açısından siber suç mağduru olması ve yaşadığı siber suç zararının karşılaştırılması yapılmış, siber suç mağduriyeti ile insan faktörü, dijital görünürlük, siber güvenlik önlemleri ve siber farkındalık ilişkisi ölçülmüştür.

Gelişen teknoloji ile değerli veri ve mali kaynakları artan ve belli bir sayının üstünde çalışana sahip olan orta ve büyük işletmeler bir yandan BİT cihazları ve interneti daha yoğun kullanıp dijitalleşirken diğer yandan daha fazla siber suça maruz kalmaktadır. Siber suçun işletmeleri iflasa kadar sürükleyen etkileri de değerlendirildiğinde işletmelerin büyürken siber güvenlik önlemlerine daha fazla dikkat etmeleri gerektiği değerlendirilmiştir. Yapılan çalışmada işletmenin büyüklüğü ile maruz kalınan siber suç zararı arasında istatistiksel olarak anlamlı bir ilişki olduğu sonucu da ortaya çıkmıştır.

Bir diğer önemli sonuç ise oltalama suç mağduriyetinin işletmeler arasında diğer suç türlerine göre kayda değer şekilde daha yaygın olduğudur. Araştırma kapsamında işletmelerin %39,1'inin oltalama suçuna maruz kaldığı sonucu ortaya çıkmıştır. Bu oran zararlı yazılımlar için %4,9, bilgisayar korsanlığı ve fidye yazılımında %3,2'dir. Oltalama suçu mağduriyeti işletmelerin yaşadığı siber suç mağduriyetinde büyük bir paya sahip olmakla beraber oltalama suçu

mağduriyetinin insan faktörü, dijital görünürlük, siber güvenlik önlemleri ve siber farkındalık ile istatistiksel olarak anlamlı ilişkide olduğu görülmüştür.

Oltalama suçunu diğer üç siber suçtan ayıran en önemli özellik ise oltalama suçunun sosyal mühendisliğe, yani temelinde aldatmaya dayalı bir siber suç olmasıdır. Diğer üç siber suçta aldatma tekniği kullanılsa bile öncelikli yöntem değildir. Sosyal mühendisliğin öne çıktığı oltalama suçunda ise "kişisel yetenekli vesayet" kavramı ön plana çıkmaktadır. Siber suçta yetenekli koruyucu sadece siber güvenlik önlemleri değildir, BİT cihazı kullanıcısı da kendisinin koruyucusudur.

Sosyal mühendislikte insanı kandırmak esas olduğu için işletmelerdeki insan faktörünün siber suç mağduriyetine etkisi araştırılmış olup insan faktörü ile siber suç mağduriyeti arasında güçlü bir pozitif ilişki olduğu sonucu ortaya çıkmıştır. İşletmelerin siber güvenlik konusundaki en zayıf kullanıcısı kadar kuvvetli olduğu gerçeğinden yola çıkarak işletmeler tarafından BİT cihazlarının ve internetin kullanım esaslarının belirlenmesi, kullanıcı etkinliğinin izlenmesi, çalışanlara siber suçla mücadele eğitimi verilmesi gibi tedbirlerin oltalama suçu mağduriyetini azaltacağı değerlendirilmiştir.

Araştırma kapsamında siber suç mağduriyeti ile siber güvenlik önlemleri alma arasındaki ilişki incelenmiştir. Siber güvenlik önlemlerinin işletimselleştirildiği elektronik cihazların güvenliğini koruma, kurumsal verileri koruma ve çalışanlara yönelik koruma açısından ele alındığında kurumsal verileri koruma tedbirleri ile siber suç mağduriyetinin istatistiksel olarak anlamlı çıkmadığı görülmüştür. Bunun sebebinin de siber suçluların ilk önce insan hatasına, sonrasında ise elektronik cihazların güvenliğini kırmaya yönelik çabalarının olması olarak değerlendirilmiştir.

Çalışmanın bir diğer önemli bulgusu da işletmelerin siber ortamdaki görünürlüklerinin siber suç mağduriyetini artırdığıdır. İnternet kullanımı ve internet üzerinden alışveriş yapma gibi alışkanlıkların yaygınlaştığı dönemde işletmelerin görünürlüğü önem kazanırken işletmelerin siber suç mağduru olma riski de artmaktadır. Bu sonuç siber saldırganların hedef seçiminde rasyonel davrandıklarını ve daha görünür hedeflere yöneldiklerini göstermiştir.

İşletmelerin dijital görünürlüğünde değer kuramı ile işletimselleştirilen özelliklerin siber suç mağduriyeti ile istatistiksel olarak anlamlı çıkmadığı görülmüştür. Bu sonuç da her ne kadar siber suçlular değerli verileri hedeflese de öncelikli hedeflerinin insan hatasından, sonrasında elektronik cihazlardaki güvenlik

eksikliklerden yararlanarak siber saldırıyı gerçekleştirmek olduğunu gösterdiği değerlendirilmiştir. Bu kapsamda işletmeler çalışanlarına ve elektronik cihazlarına yönelik tedbirleri yeniden gözden geçirmeli ve eksiklikleri gidermelidir.

Araştırma kapsamında ele alınan dört siber suçtan üçü ile siber suçla mücadele eğitimi arasında istatistiksel olarak anlamlı bir ilişki ortaya çıkmıştır. İşletmeler siber suçla mücadele konusunda alabilecekleri tedbirleri belirlemeli, çalışanlarına bilmesi gereken prensibine göre eğitim vermelidir. İşletmeler tarafından çalışanlara siber güvenlik konularında eğitim verilerek siber suç mağduriyetinin azaltılacağı değerlendirilmiştir.

Araştırmada siber suç mağduriyeti yaşayan işletmelerin siber suç mağduriyeti ile siber farkındalıkları arasında istatistiksel olarak anlamlı bir ilişki olup olmadığı incelenmiş, sadece oltalama suçu mağduriyeti ile siber farkındalık arasında istatistiksel olarak anlamlı bir ilişki olduğu görülmüştür. Siber farkındalık; bireylerin siber ortam, siber güvenlik, siber suç gibi konularda ve siber suçların nasıl gerçekleştiği konusunda bilgi sahibi olması (Marion ve Twede, 2020, s. 20) şeklinde tanımlanmıştır. Siber farkındalık siber suçla mücadele eğitimine göre daha temel seviyededir. Siber suç mağduriyeti ile siber suçla mücadele eğitimi arasında ise istatistiksel olarak anlamlı bir ilişki olduğu sonucu ortaya çıkmıştır. Siber farkındalığın sadece oltalama suçu ile anlamlı ilişkide olmasının nedeninin oltalama suçunun araştırmada ele alınan diğer üç siber suç türüne göre, insanı aldatmaya yönelik daha basit tekniklerle işlenmekte olması olarak değerlendirilmiştir. Ancak oltalama suçunun işletmelerin maruz kaldığı en yaygın suç olması ve siber farkındalığın kolayca kazandırılabilir olması sebepleriyle işletmeler tarafından siber farkındalığı artırıcı tedbirlerin hızlı bir şekilde alınması gerektiği değerlendirilmiştir.

4.1. İşletmelere Öneriler

İşletmeler açısından etkili önleyici stratejiler geliştirmek ve uygulamak elzem hâle gelmiştir. Araştırma neticesinde büyüklükleri açısından tüm işletme çeşitlerinin siber suç zararına maruz kaldığı, orta ve büyük işletmelerin ise daha fazla siber suç zararı yaşadığı sonucu ortaya çıkmıştır. Bu kapsamda üretim, satış, tanıtım gibi süreçlerde, müşteri, tedarikçi gibi paydaşları ile ilişkide interneti ve BİT cihazlarını kullanmaya başlayan mikro, küçük, orta ve büyük işletmeler, faaliyet konularına göre ihtiyaç duydukları alanlarda makine mühendisi, fizik mühendisi çalıştırdığı gibi siber güvenlik uzmanı edinmeli veya siber güvenlik danışmanlığı hizmeti almalıdır.

Siber ortamdaki görünürlük; teknolojinin gelişmesi ve hayatın dijitalleşmesi ile beraber işletmeler için adeta zorunluluk hâline gelse de görünürlük artarken güdülenmiş siber suçlularla daha çok karşılaşılacağı için işletmeler tarafından gerekli siber güvenlik önlemleri alınmalıdır.

İşletmelerdeki siber suç mağduriyetinin büyük bir kısmının insan hatasından kaynaklanan oltalama suçu olduğu unutulmamalı, siber farkındalık ve siber suçla mücadele eğitimlerine ağırlık verilmelidir. Dış dünyaya kapalı olacak şekilde tasarlanan İran'ın Natanz Uranyum Zenginleştirme Tesisine bir çalışanın fiziksel belleğine virüs bulaştırmak vasıtasıyla gerçekleştirilen Stuxnet saldırısı, insan hatasının nelere yol açabileceğinin tarihteki sadece bir örneği olmuştur.

4.2. Birey Açısından Alınması Gereken Siber Güvenlik Önlemleri

Teknolojinin ilerlemesi ile internet ticarette araç olarak kullanılmaya başlamıştır. Artan siber suçlarda sorumluluk devlet yetkilileri veya siber güvenlik uzmanlarında olduğu kadar bireysel kullanıcıda da olduğu değerlendirilmektedir. *"İki bin yıl önce karasal uzayda olduğu gibi, bugün siber ortamda, ilk savunma hattı kendini savunma olacaktır*" (Grabosky, 2001, s. 248) sözü de bu savı desteklemektedir. Bu kapsamda bireysel kullanıcıların alması gereken siber güvenlik önlemleri hakkında Avast (2021), Kaspersky (2021b) ve Norton (2021) tarafından yapılan öneriler aşağıdaki gibidir;

- Güçlü parola kullanılmalıdır.
- Orijinal antivirüs yazılımları, güvenlik yazılımları ve güvenlik duvarı kullanılmalıdır.
- Teknolojinin gelişmesi ile beraber değişen siber suçlara karşı bilgi edinilmelidir.
- Sosyal medya hesaplarında paylaşılan kişisel veriler sınırlandırılmalıdır.
- Ebeveynleri tarafından çocuklar siber zorbalık, siber taciz, kimlik hırsızlığı gibi konularda bilgilendirilmelidir.
- Tanınmayan kişilerden gelen veya şüpheli e-postalar açılmamalı, linklere giriş yapılmamalıdır.
- Topluma açık hâlde bulunan kablosuz internet ağlarına giriş yapılmamalıdır.
- Önemli veriler fiziksel bir bellek veya bulutta yedeklenmelidir.

4.3. Politika Yapıcılara Öneriler

Siber suçu geleneksel suçtan ayıran en önemli özellikler; siber suçun mesafe ve sınır tanımazlığı, maddi olmayan dijital kanıtlar içermesi, failin tespit edilmesinin veya yakalanmasının zorluğu, siber suçun otomatik olarak binlerce, hatta milyonlarca insanı etkileyebilmesi (Ngo, 2018, s. 133) olarak değerlendirilmektedir. Bu kapsamda siber suçla mücadele edecek unsurlar için mevzuatta küresel birliktelik gerekmektedir. Birleşmiş Milletler Ticaret ve Kalkınma Konferansı'nın (United Nations Conference on Trade and Development – UNCTAD) (2022) yaptığı bir araştırmaya göre dünyadaki ülkelerin sadece %80'inde siber suç mevzuatı oluşturulmuştur. Oran yüksek gibi gözükse de bu sonuç dünyadaki ülkelerin %20'sini oluşturan ülkelerde siber suçun suç olarak tasnif edilmediği anlamına da gelebilmektedir. Siber suçun suç olmadığı bir ülkeden siber saldırı gerçekleştiren bir siber suçlu, ülkeler arasında ikili anlaşma yoksa tespit edilse dahi herhangi bir cezai yaptırımla karşılaşmayabilecektir. Dolayısıyla siber suçla mücadelede küresel mevzuatta birliktelik ve uluslararası iş birliği gerekmektedir.

Siber suç mağduru olunmaması için siber suçla mücadele eğitimi alınması gerekmektedir. Bu bağlamda okullarda siber güvenlik konusu eğitim programına dâhil edilmeli ve eğitimlere ağırlık verilmelidir.

Teknolojinin hızlı gelişmesiyle beraber hayatın her alanında dijitalleşme devam etmektedir. Şu an gelişmekte olan teknolojik gelişmeler zamanla toplum hayatına daha fazla girecektir. Bu bağlamda ceza adalet sisteminde siber suç yeniden gözden geçirilmelidir.

Siber suç konusunda gerekli güvenlik önlemlerini almayan işletmeler kimi zaman büyük zararlar yaşamakta, bazen de kapanmak zorunda kaldığından belirlenecek kriterlere göre işletmeler tarafından siber güvenlik sigortası yaptırılmasının zorunlu hâle getirilmesi değerlendirilmelidir.

4.4. Sonuç

Teknolojinin insan hayatını kolaylaştırdığı bir dönemde, bilgi ve yeteneklerini geliştiren siber suçlular sayesinde siber tehditler her geçen gün artmaktadır. Bu husus Felson ve Clarke'ın (1998) Suç Fırsatı Perspektifinin "sosyal ve teknolojik değişimler yeni suç fırsatları yaratır" varsayımı ile örtüşmektedir. İnsanların hem üretici hem de tüketici olarak iş birliği içinde bulunduğu, ekonominin temelini

oluşturan işletmeler için risk her geçen gün artmaktadır. İşletmelerin siber suçtan korunabilmesi için suça sebebiyet veren fırsatların önlenmesi gerekmektedir.

Araştırmada işletmeleri bir siber suçun hedefi hâline getiren unsurlar; işletmelerin siber suç mağduriyetine en çok maruz kalınan siber suç çeşitleri açısından ele alınarak farklı bir bakış açısı sunulmak istenmiştir. Ancak bu unsurlar siber suça neden olan tüm unsurlar olamayacağı gibi, önerilen çözümler de tüm güvenlik çözümleri değildir. Burada işletmelere genel bir çerçeve sunulmak istenmiştir. Sonrasında yapılacak çalışmalar ve işletmeler tarafından alınacak tedbirlerle bu çerçeve genişletilebilir. Ayrıca teknolojinin gelişmesi ile siber suçta yeni türler ortaya çıkmaktadır. Dolayısıyla siber suç, yaşayan bir organizma gibi evrim geçirebilen bir suç olup devamlı gözlem altında tutulmalı ve siber suç konulu çalışmalar devam ettirilmelidir.

KAYNAKÇA

Abduladheem, M. S. (2017). Farklı işletmelerin ortak siber güvenlik politikalarının karşılaştırmalı araştırması [Yayınlanmamış yüksek lisans tezi]. Atılım Üniversitesi, Ankara.

Accenture Security, & Ponemon Institute. (2019). The cost of cybercrime. Erişim tarihi: 21.08.2021, https://www.accenture.com/_acnmedia/pdf-96/accenture-2019-cost-of-cybercrime-study-final.pdf.

Ahmad, M. A. (2021). Worms. B. Warf. (Ed.). The sage encylopedia of the internet içinde (ss. 987-992). Sage Publications.

Akdemir, N., & Lawless, C. J. (2020). Exploring the human factor in cyber-enabled and cyber-dependent crime victimisation: A lifestyle routine activities approach. Internet Research, 30(6), 1665-1687. Erişim tarihi: 30.09.2021, https://doi.org/10.1108/INTR-10-2019-0400.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Eeten, M., Levi, M., Moore, T., & Savage, S. (2012). Measuring the cost of cybercrime. Erişim tarihi: 18.09.2021, https://doi.10.1007/978-3-642-39498-0_12.

Avast. (2021). What is cyber security? Erişim tarihi: 18.10.2021, https://www.avast.com/c-b-what-is-cybersecurity.

Birleşmiş Milletler Ticaret ve Kalkınma Konferansı. (2021). Cybercrime legislation worldwide. Erişim tarihi: 23.08.2021, https://unctad.org/page/cybercrime-legislation-worldwide.

Bozgeyik, A. (2018). Gaziantep'te faaliyet gösteren orta ve büyük ölçekli işletmelerin siber güvenlik yönetim yaklaşımlarının analizi [Yayınlanmamış doktora tezi]. Hasan Kalyoncu Üniversitesi Sosyal Bilimler Enstitüsü, Gaziantep.

Büyükkılıç, M. (2018). Cybersecurity framework for small and medium size enterprises [Yayınlanmamış yüksek lisans tezi]. Bahçeşehir Üniversitesi, İstanbul.

Cohen, L., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American Sociological Review. 44.

Felson, M., & Clarke, R. V. (1998). Opportunity makes the thief. Police research series, paper, 98 (1-36).

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journel in Computer Virology, 2(1). 13-20.

Grabosky, P. N. (2001). Virtual criminality: Old wine in new bottles? Social & Legal Studies, 10(2), 243-249.

IBM. (2014). IBM security services 2014 cyber security intelligence index. Erişim tarihi: 07.10.2021, https://i.crn.com/sites/default/files/ckfinderimages/userfiles/images/crn/custom/IBMSecurityServices2014.PDF.

IBM. (2015). IBM security services 2015 cyber security intelligence index. Erişim tarihi: 07.10.2021, https://securityintelligence.com/media/cyber-security-intelligence-index-2015/.

Jackson, L. A. (2018). Malware. B. Warf. (Ed.). The sage encylopedia of the internet içinde (ss. 619-624). Sage Publications.

Jakankhani H., Al-Nemrat, A., & Hosseinian-Far, A. (2014). Cybercrime classification and characteristics. Akhgar, B., Staniforth, A., & Bosco, F. (Ed.). Cyber crime and cyber terrorism investigator's handbook içinde (ss. 149-164). Elseviar.

Johns, E. (2020). Cyber security breaches survey 2020: Main report. London: Department for Digital, Culture, Media & Sport. Erişim tarihi: 12.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2020.

Johns, E. (2021a). Cyber security breaches survey 2021: Main report. London: Department for Digital, Culture, Media & Sport. Erişim tarihi: 13.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.

Johns, E. (2021b). Cyber security breaches survey 2021: Technical annex. London: Department for Digital, Culture, Media and Sport. Erişim tarihi: 13.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2021.

Kharraz, A. (2018). Ransomware. B. Warf. (Ed.). The sage encylopedia of the internet içinde (ss. 720-724). Sage Publications.

Klahr, R., Amili, S., Shah, J., Wang, V., & Button, M. (2016). Cyber security breaches survey 2016: Main report. Erişim tarihi: 16.12.2021, https://www.gov.uk/government/publications/cyber-security-breaches-survey-2016.

Kaspersky. (2021b). Siber güvenlik nedir? Erişim tarihi: 17.08.2021, https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security.

Kaspersky. (2021c). The human factor in IT security: How employees are making businesses vulnerable from within. Erişim tarihi: 18.09.2021, https://www.kaspersky.com/blog/the-human-factor-in-it-security/.

Klahr, R., Shah, J., Sheriffs, P., Tossington, T., Pestell, G., Button, M., & Wang, V. (2017). Cyber security breaches survey 2017: Main report. Erişim tarihi: 15.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2017.

Küçük ve Orta Büyüklükteki İşletmelerin Tanımı, Nitelikleri ve Sınıflandırılması Hakkında Yönetmelik. (2005, 18 Kasım). Resmi Gazete (Sayı: 25997). Erişim tarihi: 15.10.2021, https://www.resmigazete.gov.tr/eskiler/2018/06/20180624-7.pdf.

Lewis, J. A. (2018). Economic impact of cybercrime. McAffee. Erişim tarihi: 11.11.2021, https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf.

Lewis, J. A., Smith, Z. M., & Lostri, E. (2020). The hidden costs of cybercrime. McAffee. Erişim tarihi: 10.11.2021, https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

Marion, N. E., & Twede, J. (2020). Cybercrime: An encyclopedia of digital crime. ABC-CLIO.

Marsh, & Microsoft. (2019). 2019 global cyber risk perception survey. Erişim tarihi: 15.02.2022, https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.

Marsh, & TÜSİAD. (2020). 2020 Türkiye siber risk algı araştırması. Erişim tarihi: 17.02.2022, https://tusiad.org/tr/yayinlar/raporlar/item/10602-2020-turkiye-siber-risk-algi-arastirmasi.

Mucuk, İ. (2011). Modern işletmecilik (17nci basım). Türkmen Kitabevi. (Orijinal çalışma basım tarihi 1983).

Ngo, F. T. (2018). Cybercrime. B. Warf. (Ed.). The sage encylopedia of the internet içinde (ss. 128-134). Sage Publications.

Norton. (2022). Bot and botnet. Erişim tarihi: 27.07.2022, https://www.nortonlifelockpartner.com/security-center/bots.html.

Pecora, D. (2009). Malware. Mcquade, S. C. (Ed.). Encyclopedia of cybercrime içinde (ss. 121-123). Greenwood Press.

Ponemon Institute. (2016). 2016 cost of cyber crime study & the risk of business innovation. Erişim tarihi: 07.02.2022, https://www.ponemon.org/local/upload/file/2016%20HPE%20CCC%20GLOBAL%20REPORT%20FINAL%203.pdf.

Prakende Ticarette Uygulanacak İlke ve Kurallar Hakkında Yönetmelik. (2016, 6 Ağustos). Resmi Gazete (Sayı: 29793). Erişim tarihi: 02.09.2021, https://www.resmigazete.gov.tr/eskiler/2016/08/20160806-4.html.

TDK. (2019). İşletme. Sozluk.gov.tr sözlüğü içinde. Erişim tarihi: 02.08.2021, https://sozluk.gov.tr/.

Tessian. (2020). Psychology of human error. Erişim tarihi: 29.10.2021, https://www.tessian.com/research/the-psychology-of-human-error/.

Thomas, D., & Loader, B. (2000). Cybercrime: Law enforcement, security and surveillance in the information age. D. Thomas, & B. Loader. (Ed.). Cybercrime: Law enforcement, security and surveillance in the information age içinde (ss. 1-13). Routledge.

Ürper, Y. (2018). İşletmeler ve özellikleri. Z. Erdoğan, & A. Hepkul (Ed.). Genel işletme içinde (ss. 2-33). Anadolu Üniversitesi Yayınevi.

Vaidya, R. (2019). Cyber security breaches survey 2019: Main report. Department for Digital, Culture, Media and Sport, 66. Erişim tarihi: 19.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2019.

Veenstra, S., Zuurveen, R., & Stol, W. (2016). Cybercrime among companies: Research into cybercrime victimisation among small- and medium-sized enterprises and one-man businesses in the Netherlands. Eleven International Publishing.

Yıldız, A. (2019). İşletme alanında nicel araştırma yöntemleri ve yayın etiği. Gazi Kitabevi.

Wall, D. S. (2004). What are cybercrimes. The Centre for Crime and Justice Studies, 58(4). Erişim tarihi: 02.07.2021, https://www.crimeandjustice.org.uk/publications/cjm/article/what-are-cybercrimes.

Wall, D. S. (2007). Cybercrime: The transformation of crime in the information age. Polity.

Wang, V., Button, M., Finnerty, K., Motha, H., Shah, J. Y., & White, Y. F. (2018). Cyber security breaches survey 2018: Main report. Erişim tarihi: 18.12.2021, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2018.

Willis Towers Watson. (2017). 2017 siber risk anketi. Erişim tarihi: 14.10.2021, https://www.willistowerswatson.com/-/media/WTW/Insights/2017/06/WTW-Cyber-Risk-Survey-US-2017.pdf?modified=20170609193130.

Woelk, B. (2009b). Preventing cybercrime. Mcquade III, S.C. (Ed.). Encyclopedia of cybercrime içinde (ss. 144-150). Greenwood Press.

Yar, M. (2005). The novelty of cybercrime: An assessment in light of routine activity theory. European Journal of Criminology 2(4), 407–427.

Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2023,Cilt:12, Sayı:1, 97-120
doi:10.28956/gbd. 1207228

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2023,Volume:12, Issue:1, 97-120
doi:10.28956/gbd. 1207228

Makale Türü ve Başlığı / Article Type and Title
Derleme/ Reviev Article
Trafik Güvenliği Kapsamında Farklı Bir Model: Risk Dengeleme Teorisi
A Different Model Within Traffic Safety: Risk Homeostasis Theory

Yazar(lar) / Writer(s)
Tuncay ÇORAK, Öğr. Gör, Sağlık Hizmetleri Meslek Yüksek Okulu, Bartın Üniversitesi, tcorak@bartin.edu.tr, ORCİD: https://orcid.org/0000-0002-3522-6873

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :19.11.2022
Makale Kabul Tarihi / Accepted :26.05.2023

Atıf Bilgisi / Citation:
Çorak T., (2023). Trafik Güvenliği Kapsamında Farklı Bir Model: Risk Dengeleme Teorisi, *Güvenlik Bilimleri Dergisi, 12(1), ss 97-120. doi:10.28956/gbd.1207228*

TRAFİK GÜVENLİĞİ KAPSAMINDA FARKLI BİR MODEL: RİSK DENGELEME TEORİSİ

Öz

Trafik güvenliğini artırmak ve trafik kazalarını azaltmak için yapılan birçok iyileştirme, uygulama ve düzenlemeye rağmen trafikteki kazalar neden azalmıyor? Bu sorunun cevabı risklerin sürücüler tarafından nasıl algılandığına ve sürüş sırasındaki davranışlarını nasıl düzenlediklerine bağlı değişmektedir. Risk algısı sürücülerin, sürüş sırasındaki değerlendirmelerini ve dolayısıyla trafik güvenliğini etkiyen önemli bir faktördür. Bu çalışmada, risklerin sürücüler tarafından nasıl algılandığı, algılamalarını etkileyen faktörlerin neler olduğu ve bunun sonucunda sürücülerin davranışlarını risklere göre nasıl düzenledikleri Risk Dengeleme Teorisi temelinde incelenmiştir. Bu teoriye göre; sürücüler koşullara bağlı olarak algıladıkları riskleri, hedefledikleri riskler ile karşılaştırarak sürüş sırasındaki davranışlarını avantajlarını en üst seviyeye çıkaracak şekilde düzenlemekte ve riski dengelemektedirler. Karşılaştırmanın sonucunu etkileyen, algılanan riskin azalmasını ya da hedeflenen riskin artmasını sağlayan her bir uygulamanın riskli davranışları artırdığı ve bu yüzden, kaza sayılarının anlamlı şekilde azalmadığı ifade edilmektedir. Bu kapsamda çalışmanın amacı; trafik ve ulaşım psikolojisi içerisinde Risk Dengeleme Teorisi'ne göre sürücülerin risk algılarının, sürüş sırasındaki değerlendirmelerine ve davranışlarına olan etkilerini temel ve güncel ampirik araştırmaları kapsayacak şekilde açıklamak ve alternatif çalışma alanlarıyla ilgili bilgi sağlamaktır.

Anahtar Kelimeler: *Trafik Güvenliği, Risk Dengeleme Teorisi, Risk Algısı, Derleme.*

A DIFFERENT MODEL WITHIN TRAFFIC SAFETY: RISK HOMEOSTASIS THEORY

Abstract

Despite many improvements, practices, and regulations to increase traffic safety and reduce traffic accidents, why are traffic accidents not decreasing? The answer to this question depends on how drivers perceive risks and regulate their driving behavior. Risk perception is an essential factor that affects drivers' evaluations while driving, and thus traffic safety. In this study, how drivers perceive risks, what factors affect their perceptions, and as a result, how drivers regulate their behaviors according to risks are examined through the Risk Homeostasis Theory. According to this theory, drivers adjust their driving behaviors to maximize their advantage and balance the risk by comparing the risks they perceive depending on the conditions with the risks they target. It is seen, as a result of the comparison, that any practice that reduces the perceived risk or increases the targeted risk leads risky behaviors to increase, and thus, the number of accidents remains relatively high. In this context, the study aims, including primary and current empirical research, to explain the effects of drivers' risk perceptions on their assessments and behaviors according to the Risk Homeostasis Theory in traffic and transportation psychology while driving and to provide information about alternative fields of study.

Keywords: *Traffic Safety, Risk Homeostasis Theory, Risk Perception, Review.*

GİRİŞ

Günümüzde ulaşım ve araç üretimi standartları sürekli iyileştirilmesine rağmen sürücülerin yaptıkları kazalar ölüm ve yaralanma gibi çok ciddi problemlere neden olmaktadır. Bu kapsamda Türkiye İstatistik Kurumu (2022) raporları incelendiğinde son on yılda (2010- 2021) kaza sayılarının azalma eğilimi göstermediği, Emniyet Genel Müdürlüğünün [EGM] raporları incelendiğinde ise 2022 yılının ilk on ayındaki kaza sayılarının önceki yıllara göre benzer düzeyde olduğu görülmektedir. Ayrıca trafik güvenliğiyle ilgili bu kazalar başlıca ölüm nedenlerinden biri olarak değerlendirilmektedir (World Health Organization [WHO], 2021; EGM, 2022). Tüm bu istatistiklerin ve değerlendirmelerin, trafik güvenliği konusunun kapsamlı bir şekilde ele alınması gereken kamusal bir sorun olduğunu gösterdiği söylenebilir.

Trafik güvenliğinde tehlike oluşturan en önemli nedenlerden biri de riskli şekilde sürüş yapmaktır. Riskli sürüş, hız yapma, takip mesafesine uymama, ışıkta geçme gibi kaza olasılığını veya yaralanmanın şiddetini artıran eylemler olarak tanımlanmaktadır (Dula ve Geller, 2003, s. 560). Bundan dolayı trafik güvenliği kapsamında riskli sürücü davranışlarını ve temel motivasyonlarını açıklamak önemlidir. Bu amaçla yapılan çalışmaların odağında ise trafikteki risklerin öznel deneyimi olarak tanımlanan ve sürücülerin, sürüş sırasındaki duygularını, düşüncelerini (değerlendirmelerini), davranışlarını ve dolayısıyla trafik güvenliğini etkileyen risk algısı yer almaktadır (Deery, 1999, s. 226; Slovic, 1987, s. 230).

Trafik ve ulaşım psikolojisi alanında risk algısına odaklanan ve trafik güvenliğini etkileyen çeşitli teoriler mevcuttur. Bu teorilerden ilki Näätänen ve Summala (1976) tarafından kavramsallaştırılan Sıfır Risk Teorisidir *(Zero Risk Theory).* Bu teoriye göre trafikteki riskin, yeterince yüksek olmadığı sürece algılama eşiğinin altında kaldığı ve sürücülerin davranışlarını etkilemediği varsayılmaktadır. İkinci teori Fuller (1984: 1139) tarafından Tehditten Kaçınma Teorisi (Threat Avoidance Theory) olarak kavramsallaştırmıştır. Bu teoriye göre sürüşün avantajı, kaza korkusunun negatif değerinden fazla olduğu sürece sürüş sırasındaki risklerin kabul edilebilir olduğu varsayılmaktadır. Son olarak ise Wilde (1982: 209) tarafından Risk Dengeleme Teorisi *(Risk Homeostasis Theory)* kavramsallaştırmıştır. Bu teoriye göre sürücüler, koşullara bağlı olarak algıladıkları riskleri hedefledikleri riskler ile karşılaştırarak sürüş sırasındaki davranışlarını düzenlemektedirler. Tüm bu bilgiler çerçevesinde, bu derlemede trafik güvenliği özelinde Risk Dengeleme Teorisi (RDT) ile ilgili alanyazında yer alan temel ve

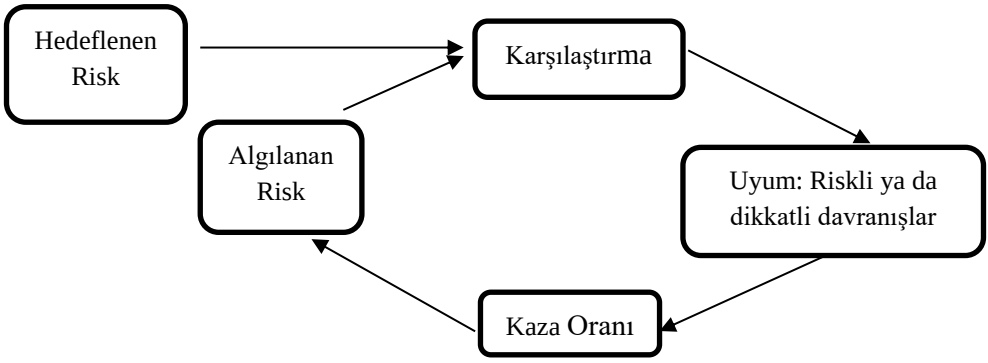
güncel deneysel araştırmaların kapsamlı bir değerlendirmesini sunmak amaçlanmaktadır.

1. RİSK DENGELEME TEORİSİ *("RİSK HOMEOSTASİS THEORY")*

Sürücü davranışlarını açıklamaya çalışan güdüsel modellerden biri olan RDT, davranışsal adaptasyon (düzenleme) teorisi olarak ele alınmaktadır (Ranney, 1994, ss. 733-736). RDT, sürücülerin riskleri değerlendirdiğini ve ardından, sürüş sırasındaki davranışlarını risklere göre düzenlediklerini varsaymaktadır. Davranışsal düzenleme ise içinde bulunulan risk seviyesine göre farklılık göstermektedir. Buna göre, algılanan yüksek risk karşısında, bireyin dikkati artmakta ve hedefledikleri risk seviyesi düşmekte, risk ortadan kalktıkça bireyin hedeflediği risk seviyesi normal seviyesine geri dönmektedir (Wilde, 2013, ss. 61-63). Sonuç olarak sürücüler, ortaya çıkan riskin belirli seviyesini kabul edilebilir olarak nitelendirmekte, davranışlarını içinde bulundukları koşullara ve bunu etkileme potansiyeline sahip diğer özelliklere göre düzenlemekte ve böylece koşullara göre riski dengelemektedirler (Wilde, 1998, ss. 89-91).

RDT'ye göre, artan güvenlik uygulamaları, sürücülerin kendilerini daha güvende hissetmelerine ve güvenlik hissiyle trafikteki riskleri daha kabul edilebilir olarak değerlendirmelerine neden olmaktadır. Böylece güvenlik uygulamalarının hedeflenen risk seviyesini artırdığı varsayılmaktadır (Wilde, 1982, s. 210). Bu varsayıma göre sürücüler; sürüş sırasındaki riskleri en aza indiren davranışa yönelmek yerine, avantajlarını en üst düzeye çıkaracak davranışa yönelme eğilimi gösterirler (Wilde, 1998, ss. 89-91). Risk içermesine rağmen zaman kazanmak, can sıkıntısını önlemek, heyecan aramak gibi isteklerini tatmin etmek için trafik güvenliğinden bir dereceye kadar fedakârlık edebilir ve riskli tercihlere yönelebilirler. Bu tercihi belirleyen değerlendirme ise dikkatli veya riskli sürüşün algılanan avantaj ve dezavantajlarının karşılaştırmalarına dayanmaktadır. Karşılaştırmalarının sonucunda ise sürücüler, davranışlarını hedefledikleri riske göre düzenleyerek dikkatli veya riskli sürüşe yönelmektedirler (Heino, Molen ve Wilde, 1996, s. 72; Simonet ve Wilde, 1997, s. 240). Ayrıca risk değerlendirmesi, olumlu-olumsuz tüm durumları kapsayan bir süreçtir. Örneğin, kötü hava koşullarında olduğu iyi hava koşullarında da risk değerlendirilmesi yapılmaktadır. Bu yüzden, risk değerlendirmesi tüm koşullara göre yapılan ve koşullara göre farklılık gösteren, sürücülerin davranışlarını etkiyen dinamik bir süreç olarak nitelendirilmektedir (Wilde, 2013, ss. 61-64).

RDT'ye göre, sürücülerin risk algısı iki düzeyli karşılaştırmanın sonucunda davranışları etkilemektedir. Bu karşılaştırmaların bir tarafında sürücünün, sürüş sırasında istekli olduğu ve hedeflediği risk seviyesi, diğer tarafında ise içinde bulunulan sürüş koşuluna göre sürücünün algıladığı ve sürüş sırasında beklenen avantaj ve dezavantajların değerlendirmesini, bunun sonucunda karar verip davranışlarını değiştirmesini sağlayan algılanan risk seviyesi vardır (Wilde, 2013, s. 69). Sürücüler içsel bir geri bildirimle etkinleştirilen davranış düzenleme mekanizmasını kullanarak hedeflenen ile algılanan risk seviyelerini karşılaştırır ve buna göre uygun kararı verirler (Ba vd., 2016, s. 24). Karşılaştırmanın sonucunda algılanan risk, hedeflenen riskten daha yüksek olduğunda sürücüler riski azaltmak için daha dikkatli (güvenli); algılanan risk, hedeflenen riskten daha düşük olduğunda ise daha riskli sürüşe yönelme eğilimi gösterir. Böylece sürücüler, algılanan ve hedeflenen risk arasında oluşan farkı en aza indirecek şekilde davranışlarını düzenlerler (Fuller, 2005, s. 462). Ayrıca sürüş sırasında sürücüler, tercih edilen davranışa bağlı olarak kaza oranı değerlendirmesi yapmaktadır. Bu durum daha sonraki bir sürüşte (gecikmeli geri bildirim) algılanan risk seviyesini etkilemektedir. Bahsedilen bu modele ilişkin detaylar Şekil 1'de gösterilmiştir.



Şekil 1.Risk Dengeleme Kuramının Dairesel Nedensellik Modeli (Wilde, 2013, ss. 67-68)

İsveç'te Şekil 1'de gösterilen model kapsamında trafik akış yönünün değiştirilmesiyle ilgili örnek bir uygulama gerçekleştirilmiştir. Bu uygulamanın ardından ise trafikteki ölüm ve yaralanma oranlarında büyük bir düşüş görülmüştür (Alexanderson, 1972). Wilde'e (2002, s. 1150) göre akış yönündeki bu değişiklik, algılanan risk seviyesinin ani şekilde yükselmesini ve sürücülerin daha dikkatli sürmelerini sağlamıştır. Ancak bir süre sonra sürücüler, yol koşullarını ve yollardaki tehlikenin düştüğünü öğrendiklerinde bu durumu, dikkatli sürüş yapılması gereken bir süreç olmaktan çıkarmıştır. Sürüş sırasındaki davranışların

öğrenilen duruma göre yeniden düzenlenmesi ise kısa sürede kaza oranlarının uygulama öncesindeki seviyeye yükselmesine neden olmuştur (Wilde, 2002, ss. 1150-1151).

Sürücülerin hedefledikleri ve algıladıkları risklerin seviyesini etkileyen faktörlerden biri de ekonomik faktörlerdir. Özellikle ekonomik refahın arttığı dönemlerde, trafikteki kaza ve ölüm oranlarında artış gözlemlenmiştir (Wilde ve Simonet, 1996, ss. 18-22). Oranlardaki bu artış ise refahın hedeflenen risk seviyesine olan etkileri üzerinden açıklanmaktadır. Buna göre, risklerin avantaj ve dezavantajları, refahın sağladığı koşullara göre değerlendirilmekte ve refah ile artan gelir, riskin avantajlarını artırırken dezavantajlarını ise azaltmaktadır. Özetle refah, trafikteki kaza ve ölüm oranlarının artmasına neden olan faktörlerden biri olarak nitelendirilmektedir (Wilde, 2002, s. 1149).

Sonuç olarak, RDT bireylerin avantaj elde etmek için sağlık ve güvenliklerine yönelik öznel olarak değerlendirilen belirli düzeydeki riski kabul ettiğini ve sürüş sırasındaki davranışlarını bu risk seviyesine göre düzenlediğini varsaymaktadır. Buna göre, bireyler koşullara bağlı algıladıkları risk seviyesini, hedefledikleri risk seviyesinin altında olduğunu değerlendirdiklerinde daha riskli; algıladıkları risk seviyesini hedefledikleri risk seviyesinin üstünde değerlendirdiklerinde ise daha dikkatli davranarak var olan riskleri dengeler ve en uygun davranış değişikliğine yönelirler (Fuller, 2005, s. 462; Wilde, 2002, s. 1150).

Trafik güvenliği kapsamında RDT'ye göre sürücülerin risk algılarının, değerlendirmelerine ve sürüş sırasındaki davranışlarına olan etkilerini temel ve güncel deneysel araştırmaları kapsayacak şekilde açıklamak ve alternatif çalışma alanlarıyla ilgili alanyazına katkı sunmak gerektiği düşünülmektedir. Bu kapsamda, ilerleyen bölümlerde RDT'nin önermelerini destekleyen ve desteklemeyen araştırmaların bulguları sunulmaktadır.

2. RİSK DENGELEME TEORİSİNİN ÖNERMELERİNİ DESTEKLEYEN ÇALIŞMALAR

RDT'ye göre sürücüler, sürüş sırasındaki riskleri tercih ettikleri davranışlarının avantaj ve dezavantajlarını değerlendirerek en uygun davranış değişikliğine yönelmektedirler (Fuller, 2005, s. 462; Wilde, 2013, ss. 61-64). Bu değerlendirmenin sonucunda hedeflenen risk seviyesi belirlenerek sürüş sırasındaki davranışlar düzenlenmektedir (Heino vd., 1996, s. 72). Trafik kazalarının nedenleri birey, araç ve çevreye bağlı olmak üzere üç temel kategoride ele alınmakta (Evans, 1996a, ss. 784–786) ve bunlar ölümlerin ve yaralanmaların en önemli

nedenlerinden biri olarak kabul edilmektedir (EGM, 2022; WHO, 2021). Bu kapsamda trafik güvenliği için belirleyici olan bu 3 kategoriye yönelik iyileştirici ve geliştirici nitelikteki her bir uygulama ile trafikteki ölümlü veya yaralanmalı kaza sayılarının azaltılması hedeflenmektedir. Buna karşın RDT'ye göre iyileştirici ve geliştirici nitelikteki her bir uygulamanın sürücülerin risk algılarını, koşullara bağlı olarak farklı şekilde etkilediği ve kaza sayılarını anlamlı şekilde azaltmadığı varsayılmaktadır (Wilde, 2013, s. 70). Bu teori kapsamında destekleyici nitelikte sonuçlar içeren araştırmalardan aşağıda bahsedilmiştir:

Trafik güvenliğiyle ilgili önemli bileşenlerden biri araç donanımlarıdır. Bu donanımların en önemlilerinden biri ise emniyet kemeridir. Güvenlik özelliğinden dolayı takılması zorunlu tutulmakta, bunun sonucunda yaralanmaları ve ölümleri azaltacağı varsayılmaktadır (Evans, 1996b, ss. 423–433). Ancak RDT'ye göre emniyet kemeri kullanımı, sürücülerin risk değerlendirmelerini farklı şekilde etkileme potansiyeline sahiptir (Wilde, 2013, s. 70). Bu kapsamda, Streff ve Geller (1988, s. 282) tarafından go-kart sürücüleriyle yapılan, emniyet kemeri kullanımı ve hız arasındaki ilişkinin araştırıldığı çalışmada emniyet kemeri kullanan sürücülerin hız ortalamalarının kullanmayan sürücülere göre daha yüksek olduğu bulunmuştur. Gerçekçi yol koşullarında yapılan farklı bir çalışmada ise emniyet kemeri kullanan sürücülerin kullanmayan sürücülere göre takip mesafesine uymadıklarını ve daha yüksek hızlarda şerit değiştirdiklerini bulmuştur (Janssen, 1994, s. 254). Azık ve Biçer (2014, s. 123) tarafından yapılan ve emniyet kemeri kullanımı ile hız arasındaki ilişkinin araştırıldığı çalışmada ise ilgili değişkenler arasında ilişki bulunmamasına rağmen araçların hız gruplarına ayrılarak emniyet kemeri kullanma sayıları karşılaştırıldığında bütün hız gruplarında emniyet kemeri kullanmama oranının emniyet kemeri kullanma oranından yüksek olduğu bulunmuştur.

Trafik güvenliğinde sadece olağandışı koşullar değil olağan koşullar da sürücü davranışlarını etkilemektedir (Wilde, 2013, ss. 61-69). Bu kapsamda RDT ile ilgili yapılan ve trafik görev koşullarının (kolay-zor) manipüle edildiği çalışmada katılımcılar, sürüş simülatöründeki görevi tamamlamışlardır. Araştırmanın sonuçları sürücü davranışlarının farklılaştığını göstermiştir. Buna göre, görevin kolay olduğu koşullar sürücülerin algıladıkları riskin düşmesine ve sürüş sırasında daha fazla riskli geçiş yapılmasına neden olurken görevin zor olduğu koşullar sürücünün algıladığı riskin artmasını ve daha az riskli geçiş yapılmasını sağlamıştır (Tränkle ve Gelau, 1992, s. 17).

Jackson ve Blackman (1994: 950) tarafından yapılan kaza maliyeti (düşük-yüksek) ve hız sınırının (düşük-yüksek) manipüle edildiği bir çalışmada katılımcılar sürüş simülatöründeki rotayı tamamlamışlardır. Araştırmanın sonuçları, koşullara göre sürücülerin davranışlarının farklılaştığını göstermiştir. Buna göre sürücüler, kaza maliyetinin yüksek olduğu koşullarda, düşük kaza maliyeti koşuluna göre daha az kaza meydana gelecek şekilde davranışlarını düzenlemişlerdir. Ayrıca hız sınırının artırılmasının ve hız cezalarının azaltılmasının, sürüş hızını önemli ölçüde artırdığı ancak kaza oranı üzerinde hiçbir etkisinin olmadığı bulunmuştur. Tüm bu sonuçlar değerlendirildiğinde motive edici değişkenin (kaza maliyetinin artırılması) manipüle edilmesinin kaza oranının azalmasını sağladığı, motive edici olmayan (hız sınırı ve hız cezası) değişkenlerin manipüle edilmesinin ise kaza oranının üzerinde etkisinin olmadığı görülmektedir (Jackson ve Blackman, 1994, ss. 950-958).

Trafik güvenliği için önemli bazı durumlar risklerin belirli seviyeye kadar kabul edilebilir olmasını sağlamaktadır (Wilde, 1982, s. 209). Bu kapsamda araç güvenliğini artıran önleyici fren sistemlerinin (*Antilock Braking System, ABS*) kullanımının sürücü davranışları üzerindeki etkisi bir dizi boylamsal araştırma ile incelenmiştir. Araştırmaların sonuçları ABS'si olan araçları kullanan sürücüler ile ABS'si olmayan araçları kullanan sürücülerin kaza sayıları arasında anlamlı bir farklılık olmadığını göstermiştir. Ancak sürüş ile ilgili sonuçlar incelendiğinde ABS'si olan araçları kullanan sürücülerin hızlanmaya bağlı ani frenleme ve tehlikeli manevraları daha fazla yaptığı, kaza sayılarının daha fazla olduğu, takip mesafesi kuralına daha az uydukları ve böylece daha fazla trafik yoğunluğuna neden oldukları görülmüştür (Hauer ve Garder, 1986, s. 471). Ayrıca bu kapsamda taksi sürücüleri ile yapılan benzer bir araştırmada ABS'si olan araçları kullanan taksi sürücülerinin ABS'si olmayan araçları kullanan taksi sürücülerine göre takip mesafesi kuralına daha az uydukları ve takip mesafesini korumadıkları bulunmuştur (Sagberg, Fosser ve Saetermo, 1997, s. 297).

Son dönemde araç güvenliğini artırmaya yönelik iyileştirmelerin sürücülerin araç kullanma tercihlerini etkilediği ifade edilmektedir (Hauer ve Garder, 1986, s. 471). Buna göre yapılan iyileştirmeler sürücülerin risk almalarına ve hız ortalamalarının daha yüksek olmasına neden olmaktadır (Azık ve Biçer, 2014, s. 123; Janssen, 1994, s. 254; Sagberg vd., 1997, ss. 293-297). Farklı bir çalışmada da güvenlik iyileştirilmelerinden biri olan hava yastığı kullanımının güvenlik hissini artırdığından dolayı sürücü davranışlarını etkilediği ve riskli sürüşü artırdığı tespit edilmiştir (Peterson, Hoffer ve Millner, 1995, s. 251).

Trafik güvenliğini ve sürüşü, dolayısıyla sürücülerin değerlendirmelerini etkileyen durumlardan bir diğeri yol koşullarına bağlı özelliklerdir. Bu kapsamda yoldaki aydınlatma düzeyinin (ışık kaynağının seviyesi) sürücülerin gece sürüş performansına olan etkileri gerçek yol koşullarında (kırsal, şehir içi, otoyol) belirlenmeye çalışılmıştır. Araştırma sonuçları, aydınlatma düzeyine göre sürücü davranışlarının farklılaştığını göstermektedir. Buna göre, aydınlatmanın yetersiz olduğu yol koşullarındaki sürücülerin, sürüş sırasındaki davranışlarını değiştirdikleri ve virajlı yollarda daha yavaş ilerledikleri ancak aydınlatmanın yeterli olduğu yol koşullarındaki sürücülerin, sürüş sırasındaki davranışlarını değiştirmedikleri bulunmuştur. Bu sonuçlar sürücülerin, aydınlatma yetersizliğinin risklerini dengelemek için yavaşladıklarını ve sürüş sırasındaki davranışlarını içinde bulundukları koşullara göre düzenlediklerini göstermektedir (Theeuwes, Alferdinck ve Perel, 2002, ss. 100-107).

Yol koşullarıyla ilgili yapılan diğer bir çalışmada ise hava durumunun sürüşe olan etkileri belirlenmeye çalışılmıştır. Bu çalışmada, saatlik yağış verileri ile otoyoldaki trafik verileri eşleştirilerek analiz edilmiştir. Elde edilen sonuçlar, yağışlı olan trafik koşulunda yağışlı olmayan trafik koşuluna göre trafik yoğunluğunun ve ortalama hızın azaldığını ve böylece trafikte ilerlemenin artığını göstermektedir. Ayrıca bu durumun yoğun trafik koşullarında gerçekleşme eğiliminin yoğun olmayan trafik koşullarına göre daha fazla olduğu bulunmuştur. Bu sonuçlar sürücülerin güvenlik seviyelerini korumak için davranışlarını var olan koşullara göre düzenlediklerini ve riskleri daha dikkatli sürerek telefi ettiklerini göstermektedir (Unrau, 2004).

Trafik güvenliği bir bütün olarak değerlendirildiğinde araç özellikleri (emniyet kemeri, hava yastığı, fren sistemleri), yol koşulları (yağış durumu, yolların aydınlığı) ve bireysel özellikler trafik sisteminin temel bileşenleri olarak sayılmaktadır (Evans, 1986, s. 105). RDT çerçevesinde yapılan yol koşullarına (Theeuwes vd., 2002, s. 100) ve araç özelliklerine (Hauer ve Garder, 1986, s. 471; Sagberg vd., 1997, s. 293) odaklanan çalışmalarda, yol koşullarının ve araç özelliklerinin sürücülerin davranışlarını düzenlemek için belirleyici bir faktör olduğu bulunmuştur. Ayrıca, sistemin bir parçası olarak sürücülerin bireysel özellikleri de riskli davranışları doğrudan etkileme potansiyeline sahiptir (Evans, 1986). Bu amaçla yürütülen çalışmada görme kapasitesinin (katarakt olan-olmayan) sürücü davranışlarına olan etkileri karşılaştırılmıştır. Araştırmanın sonuçlarına göre, kataraktı olan sürücülerin daha yavaş ilerledikleri bulunmuştur. Bu bulgu, kataraktı olan sürücülerin kötü performanslarının farkında olduklarını ve

koşullara göre davranışlarını düzenlediklerini ve riskleri daha yavaş sürerek dengelediklerini göstermektedir. Ayrıca kaza oranları karşılaştırıldığında gruplar arasında farklılık olmadığı tespit edilmiştir. Kaza oranlarıyla ilgili bu sonuçlar, kaza riskleri konusunda kataraktı olmayan sürücülerin kendilerine fazla güvendiklerini ve daha riskli sürdükleri, kataraktı olan sürücülerin ise görme eksikliklerinin farkında olduklarını ve bu durumu daha dikkatli (yavaş) sürerek dengelemeye çalıştıklarını göstermektedir (Brémond, Dommes ve Engel, 2018, ss. 61-73).

Kaza yapan ve yapmayan sürücülerin karşılaştırması ve farklılıkların ortaya konulması trafik güvenliği için önemlidir. Bu kapsamda Ba ve diğerleri (2016: 24) tarafından yapılan çalışmada kaza yapan ve yapmayan sürücülerin davranış ve görsel algı farklılıkları simülatör aracılığıyla karşılaştırılmıştır. Araştırmanın sonuçları kaza yapan ve yapmayan sürücülerin risklerin değerlendirilmesinde ve sürüş sırasındaki davranışlarda farklılaştığını göstermektedir. Buna göre, kaza yapmayan sürücülerin algılanan risk düzeyi ve davranışları farklılaşmıştır. Bu sürücülerde algılanan riskin yavaşça yükselmesi (aşina olunmayan trafik) orta yoğunlukta tepkiler (gaz pedalını bırakmak) ortaya çıkarırken, algılanan riskin hızla yükselmesi (aniden yola çıkan yaya) durumlarında güçlü tepkiler (ani fren) ortaya çıkarmıştır.

Zaman içerisinde kazaların olası etkilerini azaltıcı araç güvenlik sistemlerinden kazaların önlenmesini sağlayan yenilikçi sistemlere doğru ilerleyiş olmuştur. Bu yenilikçi sistemler sürücülerin dikkatini ve risk algılama yeteneğini geliştirmek ve hataları önlemek amacıyla gerçek zamanlı olarak sürüşü yönlendirmekte ve böylece trafik güvenliğini artırmaktadır (Inagaki, 2008). Bu yenilikçi sistemlerin kullanımının sürücü davranışlarına ve risk algısına olan etkilerini belirlemek de trafik güvenliği kapsamında önemlidir. Bu amaçla Lyu ve diğerleri (2021) gelişmiş sürüş destek sistemlerinin (kapalı-açık) deneyim düzeyine (düşük, orta, yüksek) göre kaza olasılığının olduğu koşullarda sürücü davranışlarına olan etkisini incelemişlerdir (s. 96). Araştırmanın sonuçlarına göre, sürüş destek sistemlerinin kullanımı düşük ve orta deneyim düzeyindeki sürücülerin risk algısını artırırken yüksek deneyim düzeyindeki sürücülerin risk algısını azaltmıştır. Bu bulgular yüksek deneyim düzeyindeki sürücülerin sürüş destek sistemlerini dikkate almadıklarını (algılanan riskin düşmesi) ve kaza olasılığına rağmen risk alma eğiliminde artış gerçekleştiğini göstermektedir.

Trafik güvenliği için önemli olan risklerden biri de sürüş sırasında dikkatin dağılmasına neden olan telefon kullanımıdır (Oviedo-Trespalacios vd., 2017, s.

67). RDT'ye göre sürücüler sürüş sırasındaki telefon kullanımını hızlarına göre 2 farklı şekilde değerlendirmektedir. Bu değerlendirmenin sonucunda sürücüler, (1) yüksek hızlarda telefon kullanımından kaçınarak ya da (2) sürüş sırasındaki hızlarını telefon kullanımı için düşürerek davranışlarını düzenlemektedirler. Dolayısıyla sürücüler, yüksek hızlarda telefon kullanımını riskli olarak algıladıkları için telefon kullanımından kaçınmaya, düşük hızlarda ise telefon kullanımını riskli olarak algılamadıkları için telefon kullanımına yönelmektedirler. Buna göre, sürüş sırasında telefon kullanımına yönelik risk (hız), davranışların düzenlenmesini farklı şekilde etkilemektedir (Wilde, 2013, s. 71).

Kita ve diğerleri (2022) tarafından RDT'ye göre geliştirilen ve düşük hızlarda da telefon kullanımını azaltmayı amaçlayan bir müdahale programının etkisinin incelendiği bir çalışmada sürücülere, algılanan (sürüş sırasında telefonu ne sıklıkta kullandıkları) ve hedeflenen (sürüş sırasında telefon kullanımı tehlikesi) risk düzeylerini yeniden uyarlamaları için çeşitli şekillerde geri bildirimlerde bulunulmuştur. Müdahale programının etkisi ise sürüş sırasında ekrana dokunma sayısı ve sürüş hızının ölçülmesiyle belirlenmeye çalışılmıştır. Araştırmanın sonuçları; sürüş sırasında telefon kullanımının, RDT ile tutarlı olarak düşük sürüş hızlarında daha fazla gerçekleştiğini göstermektedir. Ancak geliştirilen müdahale programının sonuçları, düşük hızlarda araç kullanırken telefon kullanımının neden olduğu riskli davranışların azaldığını göstermiştir. Bu sonuçlar, RDT'ye göre geliştirilen geri bildirim temelli bu müdahale programının düşük hızlarda araç kullanırken telefon kullanımının neden olduğu riskli davranışların azalmasını sağladığını göstermektedir. Böylece, düşük hızlar için verilen geri bildirim, telefon kullanımının, hedeflenen risk seviyesine göre daha az güvenli ya da algılanan risk seviyesini göre daha riskli bir davranış olarak değerlendirilmesini sağlamıştır (Kita vd., 2022).

3. RİSK DENGELEME TEORİSİNİN ÖNERMELERİNİ DESTEKLEMEYEN ÇALIŞMALAR

RDT, ilk yıllarında reddedilmekle birlikte günümüzde davranışsal düzenleme aracılığı ile desteklenmeye başlamıştır. Ancak teorik ve ampirik sorunlarını yeterince çözemediği için hâlen tartışılmaktadır. Bu kapsamda yapılan eleştiriler temel olarak iki gruba ayrılmaktadır. İlk grupta yer alan araştırmacılar RDT'nin doğrulanmasının veya yanlışlanmasının zor olduğuna dikkat çekerken (Adams, 1988, s. 407), ikinci grupta yer alan araştırmacılar ise DT'nin metodolojik olarak verileri analiz ve yorumlama şeklini eleştirmektedirler (Evans, 1986; O'Neill ve Williams, 1998). Bu konuda en sık yapılan eleştiriler ise metodolojik problemlerine

ve verilerin ayrıştırmadan kullanılmasına yöneliktir (McKenna, 1990, ss. 171-181). Bu kapsamda RDT'nin önermelerine yönelik destekleyici nitelikte olmayan sonuçlar içeren araştırmalardan aşağıda bahsedilmiştir:

RDT'ye göre sürücülerin, kaza olasılıklarını azaltmak için araç özelliklerine (Janssen, 1994, s. 254) ve yol koşullarına (Unrau, 2004) dikkat ederek davranışlarını düzenledikleri varsayılmaktadır. Ancak bu varsayım, Evans'a (1986, ss. 103-107) göre ilgili verilerin yanlış değerlendirilmesinden kaynaklanmaktadır. Örneğin Amerika Birleşik Devletleri'nde (ABD) araç güvenlik sistemleri uygulamalarından önce ve sonra yapılan kaza sayılarının karşılaştırılması sonucunda sürücü ölümlerinde azalma olduğu ancak yolcu ölümlerinde artış olduğu bulunmuştur (Peltzman, 1975, s. 677). Bu bulgu RDT'nin ifade ettiği gibi sürücülerin davranışlarını koşullara göre düzenlediğini doğrulamaktadır. Ancak veriler ayrıştırıldığında sadece sürücülerin değil yolcuların da ölümlerinin azaldığı tespit edilmiştir (Evans, 1986).

Robertson'a (1992, s. 188) göre RDT'ye karşı en önemli bulgulardan biri, 1964-1990 yılları arasında ABD'de trafikteki ölüm oranlarında çok büyük bir düşüşün olduğudur. Araçların teknik açıdan geliştirilmesinin (emniyet kemeri, hava yastığı, vb.), uygulanan cezaların ve yasaların analizlerinde ise bu düşüşün yaklaşık %90'ının araç geliştirmelerinden kaynaklandığını göstermektedir. Ayrıca, trafik güvenliği kapsamındaki kazaların en önemli nedeni sürücü özellikleri (kişilik) olarak ifade edilmesine karşın (Elander, West ve French, 1993: 280), Robertson'ın (1992: 188) bulgularına göre sürücülerin haricindeki diğer faktörler, trafik güvenliği standartlarının iyileştirilmesinde ve kazaların azaltılmasında daha önemlidir. Bu kapsamda, Evans (1986: 105) sürücülerin trafik güvenliği sistemindeki değişikliklerden bağımsız olarak birim zamanda riski sabit tutma eğiliminde olduklarını ve teorinin değerlendirdiği verilerin ayrıştırıldığında RDT ile uyumlu olmadığını ifade etmektedir.

O'Neill ve Williams'ın (1998: 92) RDT'nin temel varsayımlarının ve bulgularının yanlış olduğunu kanıtlarla göstermeyi amaçladıkları çalışmalarında, ilk olarak RDT'nin güvenlik donanımı olan araçları kullanan sürücülerin güvenlik hislerinden dolayı daha az risk algıladıkları ve güvenlik donanımı olmayan araçları kullanan sürücülere göre daha riskli sürüş yaptıkları yönündeki varsayımlarını, hava yastığı donanımlı araçlardaki sürücü ölümlerinin %16 azaldığını gösteren araştırma bulguları üzerinden eleştirmişlerdir (Lund ve Ferguson, 1995). İkinci eleştirileri ise kaza istatistiklerini değerlendirdikleri ve kaza oranlarının 1966-1987 yılları arasında %20 ve 1987-1998 yılları arasında %18 azaldığı ile ilgilidir.

RDT'nin güvenlik önlemlerinin kaza oranlarını anlamlı şekilde azaltmadığı yönündeki varsayımı kaza oranlarının azaldığını gösteren bu istatistikler üzerinden eleştirilmiştir. Buna göre RDT'nin ölüm oranlarındaki azalışı açıklayamadığı ve çoğu sürücünün araç donanımlarının (hava yastıkları, fren sistemleri vb.) aslında farkında olmadığını ve bu donanımlara bağlı olarak davranış değişikliği beklenilmemesi gerektiği ifade edilmektedir. Bunun yerine, davranış değişikliğinin gerçekleştiği koşulları belirlemeye yönelik çalışmalar önerilmektedir (O'Neill ve Williams, 1998, ss. 92-93).

RDT'ye göre, artan güvenlik uygulamalarının sonucunda sürücülerin davranışları farklılaşmakta, daha riskli davranışlara yönelmekte ve böylece, koşullara göre riski dengeledikleri varsayılmaktadır (Hauer ve Garder, 1986, s.471; Sagberg vd., 1997, s. 297; Streff ve Geller, 1988: 282). Bu varsayımı test etmek amacıyla yapılan bir çalışmada emniyet kemeri kullanım yasasının yürürlüğe girmesinden önce ve sonra riskli davranış sayılarında (ışık ihlali, takip mesafesine uymama vb.) farklılık olmadığı ve emniyet kemeri kullanımının %16'dan %77'e yükseldiği ve ortalama hızın ise azaldığı görülmüştür (Lund ve Zador, 1984, ss. 41-53). Devamında yapılan bir çalışmada kaza oranını azaltmayı amaçlayan güvenlik amaçlı eğitim programları karşılaştırılmış ve yine benzer sonuçlar bulunmuştur (Lund ve Williams, 1985, s. 451). RDT'nin bu varsayımını test etmek amacıyla yapılan diğer bir çalışmada ise hava yastığı olan ve olmayan araçlarda emniyet kemeri kullanımı karşılaştırılmıştır. RDT'ye göre, hava yastığı olan araçlardaki sürücülerin, hava yastığı olmayan araçlardaki sürücülere göre anlamlı şekilde daha az emniyet kemeri kullanması beklenmektedir. Ancak, araştırmanın sonuçlarına göre sürücü grupları arasında anlamlı bir farklılık olmadığı bulunmuştur (Williams, Wells ve Lund, 1990, s. 1514). Bu bulgular değerlendirildiğinde riskin dengelenmesi için sürücülerin davranışlarını değiştirmediği ve emniyet kemeri kullanımı gibi uygulamaların trafik güvenliği için önemli olduğu ifade edilmektedir (Lund ve Williams, 1985, ss. 449–460).

RDT'ye göre sürücüleri, performansları için (kaza yapmama) ödüllendirmenin (ehliyetin ücretsiz yenilenmesi) kaza riskini azaltmada etkili uygulamalardan biri olduğu değerlendirilmektedir (Harano ve Hubert, 1974). Ancak trafik güvenliğini basite indirgeyen bu yaklaşımın yol koşulları ve sürücüler arasındaki dinamik etkileşimi göz ardı ettiği ve trafik güvenliği için tek etkili stratejinin sürücü davranışları geliştirme uygulamalarının olmadığı belirtilmektedir. Buna göre trafik güvenliği için tüm faktörleri içine alan müdahaleler geliştirilmelidir. Bu yüzden, RDT'nin kazaların azalmasını sağlayan uygulamaları değerli görülmekle birlikte

sürücülerin doğru karar vermelerine yardımcı olacak yolların sağlanması, mühendisliğin sürücü davranışlarını ve trafik güvenliği sistemlerini bütünleştiren bir modele doğru genişletilmesinin daha yararlı olacağı değerlendirilmektedir. Ayrıca RDT'nin ileri uygulamaları için tek yönlü hedef risk değerlendirmelerinin çok yönlü hedef risk değerlendirmelerine dönüştürülmesi ve katılımcı yöntemlerin kullanılması önerilmektedir (Zein ve Navin, 2003, ss. 1-9).

Hoyes ve Glendon (1993: 20), artırılan güvenlik önlemlerinin etkilerinin farklılıklarına ve laboratuvar dışındaki alternatif davranışların kontrol edilmesinin zorluklarına değinmektedir. Orr (1982: 240) ise bireylerin karar verme anında risk olasılıklarını değerlendirmesinin zorluğuna işaret etmektedir. Buna göre, hedeflenen risk ile algılanan risk arasındaki karşılaştırma öznel bir bilişsel ve duygusal süreç olduğundan, risk dengelemenin gerçekleşip gerçekleşmediği sorusu sadece kazaların analiz edilmesiyle değil, sürücülerin kendileri tarafından yanıtlanabilir. Ayrıca Slovic ve Fischhoff (1982: 227) farklı bir bakış açısı ile RDT'nin riskin istenmeyen yönlerine odaklandığını; ancak riskin, istenilmeyen sonuçlarıyla beraber haz alma (adrenalin, heyecan vb.), finans ve sosyal başarı gibi durumlarla ilgili sonuçları da sağladığı ve RDT'nin risk alma davranışının çekici yönlerinin kazalar üzerindeki etkilerini açıklamada yetersiz kaldığını ifade etmektedir.

RDT ile ilgili yapılan eleştirilerden biri de trafik güvenliğini artırıcı uygulamalardan (güvenlik donanımlı araçlar, iyi yollar) bağımsız olarak sürücülerin, koşullara göre davranışlarını değiştirildikleri, hedefledikleri riskleri ve kaza oranlarını nispeten sabit tutma eğiliminde olduklarıdır (Evans, 1986, s. 104; Slovic ve Fischhoff, 1982, s. 230). Wilde (2002: 1150) ise sürücülerin davranışlarını sabit bir risk seviyesine ulaşma hedefi ile değiştirmediklerini, kaza oranlarının kabul etmeye istekli oldukları risk seviyesine (hedeflenen risk) bağlı olduğunu ifade etmektedir. Özetle RDT, sürücülerin hedefledikleri riskin, riskli veya dikkatli sürüş alternatiflerini seçmenin beklenen avantaj ve dezavantajları arasındaki dengeye bağlı olduğunu öne sürmektedir. Bu dengeleme süreci ise tüm koşullara göre farklılık göstermektedir (Wilde, 2013, ss. 61-64).

SONUÇ

Kuramsal temeller ve yukarıda da verilen örnek araştırma bulguları çerçevesinde; trafik güvenliğini artırma potansiyeline sahip önlemlerin ve uygulamaların her zaman beklenen etkiyi oluşturmadığı ve riskli davranışları artırdığı (Azık ve Biçer, 2014, s. 123; Janssen, 1994, s. 254; Sagberg vd., 1997, ss. 293-297; Tränkle ve

Gelau, 1992, s. 17), ancak veriler ayrıştırıldığında bu bulguların doğrulanmadığı (Evans,1986, s. 105), aksine güvenlik önlemlerinin ve uygulamaların beklenen etkiyi oluşturduğu ve böylece riskli davranışlarının azaldığı (Lund ve Zador, 1984; Lund ve Williams, 1985; O'Neill ve Williams, 1998) gösterilmiştir. Bu derleme, sürüş sırasında görünen riskli davranışları Risk Dengeleme Teorisi'nin (RDT) önermelerine göre temel ve güncel deneysel araştırmaları kapsayacak şekilde açıklamayı ve alternatif çalışma alanlarıyla ilgili bilgi sunmayı amaçlamıştır.

Risk dengeleme davranışı, bireyin kendisi için hedeflediği risk seviyesini belirlemesi ve hedeflediği riske göre davranışlarını düzenlemesidir (Heino vd., 1996, ss. 72-73). Düzenleme sırasında hedeflenen risk ile koşullara bağlı olarak algılanan risk aynı seviyede olmadığında davranışın, hedeflenen ve algılanan risk seviyesi arasındaki farka göre düzenlendiği varsayılmaktadır (Simonet ve Wilde, 1997, s. 241). Ancak yapılan eleştirilerde bu varsayımların yanlı olduğu ve koşullara göre farklılaşan davranışın temelinde trafik güvenliği sistemindeki değişikliklerden ziyade sürücülerin riski sabit tutma yönündeki eğilimlerinin olduğu ifade edilmektedir (Adams, 1988, ss. 407-428; Evans, 1986, ss. 104-105; O'Neill ve Williams, 1998, s. 92).

Araç güvenlik donanımlarını (hava yastığı, emniyet kemeri vb.) kapsayan birçok çalışmada (Hauer ve Garder, 1986, s. 471; Peterson vd., 1995, s. 251; Sagberg vd., 1997, s. 293; Streff ve Geller, 1988, s. 282) sürücülerin benzer eğilimler gösterdikleri ve davranışlarını riskli sürüşe yönelerek düzenledikleri bulunmuştur. Bu araştırmalara göre, araç güvenlik donanımları sürüşü daha az tehlikeli hâle getirmemekte ve trafik güvenliği için olumlu değişikliklere neden olmamaktadır. Aksine, sağladıkları kontrol ve korunma duygusu ile riskli sürüşe ve dolayısıyla kaza sayılarının benzer seviyelerde kalmasına neden olmaktadır (Wilde, 2002, ss. 1149-1150).

Trafik güvenliğini etkileme potansiyeli olan emniyet kemeri kullanımının (Azık ve Biçer, 2014, s.123; Janssen, 1994, s. 254; Streff ve Geller, 1988, s. 282), güvenlik (ABS) donanımlarının (Hauer ve Garder, 1986, s. 471; Sagberg vd., 1997, s. 293) ve gelişmiş sürüş destek sitemlerinin (deneyimli sürücülerde) (Lyu vd., 2021, s. 97) risk algısını azalttığı ve trafikteki riskli davranışların görülme sıklığını artırdığı RDT kapsamında yapılan çalışmalar ile gösterilmiştir. Ancak tam tersi olan ve belirli uygulamaların (emniyet kemeri kullanım yasası) trafikteki riskli davranışların görülme sıklığını azalttığını gösteren çalışmalar da bulunmaktadır (Lund ve Zador, 1984, ss. 41-53). Bu sonuçlar araçların güvenlik donanımlarının,

sürüş destek sistemlerinin ve belirli uygulamaların güvenli sürüşü garanti etmediğini ve bulguların tutarsız olduğunu göstermektedir.

Yukarıda trafik güvenliğini artırmayı amaçlayan araçlara özgü (emniyet kemeri, hava yastığı, fren sistemi) özelliklerin sürücü davranışlarını nasıl etkilediğine değinilmiştir. Bu bağlamda üretim standartlarının yükseltilmesinin çeşitli prosedürler ile güvence altına alınması, bu özelliklerin kontrol edilebilir bir süreç olarak nitelendirilmesini sağlayabilecektir. Trafik güvenliğini etkileyen ancak kontrol edilebilir olmayan koşullar da sürücü davranışlarını etkileme potansiyeline sahiptir. Bu kapsamda yollardaki aydınlatma seviyesinin az olduğu (Theeuwes vd., 2002, s. 100) ve yağışın fazla olduğu koşullarda (Unrau, 2004) sürücülerin davranışlarını bu koşullara göre düzenlediklerini ve bunun sonucunda sürüş sırasındaki ortalama hızlarının azaldığını gösteren araştırma bulguları mevcuttur.

Trafik güvenliğinin değişen koşullara göre nasıl etkilendiği ise gerçek yol (Alexanderson, 1972) ve sürüş simülatörü koşullarını içeren (Ba vd., 2016, s. 24) çalışmalarda gösterilmiştir. Bu araştırmalara göre, trafik akış yönünün değiştirilmesi, aniden yola birinin çıkması, aşina olunmayan yollarda sürüş yapılması gibi koşullar sürücülerin algıladıkları risklerin hızlıca yükselmesini, sürüş sırasındaki davranışların daha az riskli olacak şekilde düzenlenmesini ve kaza oranlarının azalmasını sağlamıştır. Ancak koşullara uyum sağlandıktan sonra düzenlenen davranışların eski hâline döndüğü ve kaza oranlarının yeniden yükseldiği ifade edilmiştir (Wilde, 2002, ss. 1150-1151). Trafik güvenliği ile ilgili bu bulgular (Ba vd., 2016; Theeuwes vd., 2002; Unrau, 2004), değişen koşulların algılanan riski etkilediğini ve sürücülerin güvenlik seviyelerini korumak için davranışlarını var olan koşullara göre düzenlediklerini ve daha dikkatli kullanarak riski dengelediklerini göstermektedir.

Trafik güvenliğinde belirleyici olan faktörlerden biri de gerçekleşen yaralanmalı ve ölümlü kazaların sayılarıdır (EGM, 2002). RDT kapsamında ele alındığında ise kaza sayılarının azalmasıyla ilgili farklı bulgular olduğu görülmektedir. Buna göre, araç güvenlik sistemlerinin (Hauer ve Garder, 1986, s. 471), hız cezasına yönelik düzenlemelerin (Jackson ve Blackman, 1994, s. 950) ve sürücü özelliklerinin (Brémond vd., 2018, s. 61) sürücülerde davranış değişikliği oluşturduğu ancak kaza sayılarını etkilemediği bulunmuştur. Ancak tam tersi bulgular da söz konusudur. Buna göre sürücülerin, kaza maliyetinin (motive edici) fazla olduğu durumlarda daha az kaza olacak şekilde davranışlarını düzenleme eğiliminde oldukları ve bu motive edici değişkenin kaza sayılarını azalttığı bulunmuştur (Jackson ve Blackman, 1994, s. 950). Bu bulgular kaza sayılarını azaltmak amacıyla yapılan

iyileştirmelerin ve düzenlemelerin beklenen etkiyi oluşturmadığını düşündürmektedir.

Sürücüler her zaman geleneksel güvenlik girişimlerine beklenildiği gibi tepki vermemekte ve bunun yerine davranışlarını mevcut koşullara (Unrau, 2004), cezai yaptırımlara (Jackson ve Blackman, 1994, s. 950), emniyet kemeri kullanım zorunluluğu gibi düzenlemelere (Azık ve Biçer, 2014, s. 123; Janssen, 1994, s. 254; Streff ve Geller, 1988, s. 282) ve mühendislik teknolojilerinin (Hauer ve Garder, 1986; Peterson vd., 1995, s. 251; Sagberg vd., 1997, s.293) etkilediği kendi hedef risk düzeylerine göre düzenlemektedirler. Bu düzenlemelerden dolayı RDT, geleneksel olarak nitelendirilen çoğu güvenlik müdahalesinin aslında etkisiz olduğunu iddia ederek tartışmalara neden olmaktadır (Wilde, 2013, ss. 61-86). Bu kapsamda Kanada'da alkollü araç kullanımına bağlı oluşan kazaları ve ölümleri azaltmak amacıyla uygulanan yasal önlemlerin, kamu bilgilendirme ve eğitim kampanyalarının, rehabilitasyon programlarının etkisinin değerlendirildiği bir çalışmada önleyici uygulamaların alkollü araç kullanımı üzerindeki etkisinin sınırlı olduğu ve amaçlanan etkiyi oluşturmadığı öne sürülmüştür (Liban, Vingilis ve Blefgen, 1987, ss. 159-181).

Yukarıda söz edilen geleneksel olarak nitelendirilebilecek önleyici uygulamaların (Liban, Vingilis ve Blefgen, 1987), daha fazla güvenlik sağlamadıkları için verimli olmadığı ve RDT'ye göre amaçlanan etkiyi oluşturmadığı düşünülmektedir (Wilde, 2013, ss. 61-86). Buna benzer sonuçlar fren sistemleri, hava yastıkları ve emniyet kemeri kullanımı gibi tamamen teknolojik müdahaleler için de geçerli gibi görünmektedir. Ayrıca bazı davranışlar diğerlerinden daha fazla riskli olmakla birlikte risksiz hiçbir davranışın olmadığını söylemek mümkündür. Bundan dolayı, risklerin, sürücülerin avantajlarını sağlamak için en uygun seviyede tutulması (hedeflenen risk) önemlidir. Bunu sağlamak için de çeşitli yaklaşımlar kullanılmaktadır (Wilde, 2002, s.1149).

Sürücüler için hedeflenen risk düzeyini azaltmak için dört olası yaklaşım olduğu ifade edilmektedir (Wilde, 1998, ss. 89-90). Bunlar, güvenli olan belirli davranışları ödüllendirmek, kaza yapmayan sürücüleri ödüllendirmek, riskli olan belirli davranışları cezalandırmak ve sürücüleri kaza yaptıkları için cezalandırmaktır. Bu yaklaşımlardan özellikle, kullanılan cezalandırıcı uygulamaların etkili olmadığı, kaza yapmayan sürücülerin ödüllendirilmesinin (ikinci yaklaşım) daha yararlı olacağı ve riskli davranışları azaltacağı öne sürülmektedir. Örneğin geçmiş bir araştırmada kaza yapılmadığı takdirde ehliyetin ücretsiz olarak yenilenmesi vaadi, ilk yıl kazaları %22 ve ikinci yıl ise %33

oranında azaltmıştır (Harano ve Hubert, 1974). Bu yaklaşımlar arasında yer almayan kaza maliyeti algısının yükseltilmesi uygulamasının da kaza oranlarının azalmasını sağladığı bulunmuştur (Jackson ve Blackman, 1994, ss. 950-958). Ayrıca yapılan daha yeni bir araştırmada da sürücülere verilen geri bildirimin sürüş sırasındaki riskli davranışların azalmasını sağladığı görülmektedir (Kita vd., 2022). Bu sonuçlar değerlendirildiğinde trafik güvenliği için hedeflenen risk düzeyinin azalmasını ya da algılanan risk seviyesinin artmasını sağlayan uygulamaların ve müdahale yöntemlerinin geliştirilmesinin önemli olduğu düşünülmektedir.

RDT kapsamında yapılan birçok çalışmada sürücüler, koşullara bağlı faktörleri değerlendirilmekte, değerlendirmelerine göre karar almakta ve davranışlarını daha riskli ya da daha dikkatli kullanım için düzenlemektedirler. Özellikle güvenlik hissini artıran her bir uygulama (emniyet kemeri, hava yastığı, fren sistemi, hız sınırı düzenlemeleri, vb.) sürücülerin algıladıkları risklerin azalmasına ve riskli kullanıma neden olurken (Azık ve Biçer, 2014, s. 119; Hauer ve Garder, 1986, s. 471; Jackson ve Blackman, 1994, s. 950; Janssen, 1994, s. 254; Liban vd., 1987, s.159; Peterson vd., 1995, s. 522; Sagberg vd., 1997; Streff ve Geller, 1988, s. 277) farklı bir çalışmada (sürüş destek sistemleri) sürücünün deneyim düzeyinin yüksek olmasının da riskli kullanımı artırdığı bulunmuştur (Lyu vd., 2021, s. 97). Ayrıca güvenlik hissini azaltan her bir uygulama ve değişikliğin (aydınlatma seviyesi, trafik akış yönünün değiştirilmesi, hava koşulları, vb.) algılanan riskin artmasını ve dikkatli sürüşü sağladığı da görülmektedir (Alexanderson, 1972; Ba vd., 2016, ss. 24-25; Theeuwes vd, 2002, s. 95; Unrau, 2004). Ancak bununla birlikte RDT, eleştirilmeye devam etmektedir. Bazı araştırmacılara göre elde edilen bu bulguların yanlı olduğu, artan güvenlik özellikleriyle birlikte ölüm oranlarında azalma olduğu ve RDT'nin bunu açıklayamadığı ve sürücülerin aslında güvenlik özelliklerinin farkında dahi olmadıkları ifade edilmektedir. (O'Neill ve Williams, 1998, s. 92; Robertson, 1992, s. 188).

Araç güvenlik özelliklerinin ve hukuki düzenlemelerin sürücülerin trafik güvenliğine yönelik davranışlarının sıklığını artırmadığı ve buna bağlı olarak kaza oranını azaltmadığı düşünülmektedir (Jackson ve Blackman, 1994, ss. 950-958; Janssen, 1994, s. 254). Farklı bir ifade ile yıllar içerisinde araç üretim standartlarının yükseltilmesi trafik güvenliği ve kaza sayılarını anlamlı olarak azaltmamıştır (Hauer ve Garder, 1986, s. 471; Sagberg vd., 1997, s. 293). RDT'ye göre trafik güvenliğini artırmak ve kaza sayılarını azaltmak için hedeflenen riskin azaltılması ya da algılanan riskin artırılması gerekmektedir (Kita vd., 2022). Özetle, araç güvenlik özelliklerinin ve hukuki düzenlemelerin yanı sıra davranış

değişikliği oluşturan müdahalelerin (kaza maliyeti algısının yükseltilmesi, kaza yapmayanların ödüllendirilmesi) de uygulanması (Harano ve Hubert, 1974; Jackson ve Blackman, 1994, s. 950) geleneksel yaklaşımların yeniden ele alınmasını ve trafik güvenliğinin artırılmasını sağlayabilir.

RDT'yi kapsayan temel çalışmalardan günümüze kadar olan birçok çalışmada farklı güvenlik önlemlerinin hem simülatör hem de gerçekçi koşullarda sürücü davranışlarına olan etkileri belirlenmeye çalışılmıştır. Ancak artırılan güvenlik önlemlerinin etkilerinin farklılaşabileceği (Hoyes ve Glendon, 1993, ss. 19-33), karar verme anında risk olasılıklarını değerlendirirken analiz edilmesi gerekenin sürücüler ile ilgili süreçler olduğu (Orr, 1982, ss. 239-242) ve risk alma davranışının çekici yönlerinin göz ardı edilmemesi gerekliliği de araştırmacılar tarafından vurgulanmaktadır (Slovic ve Fischhoff, 1982, s. 230). Bu kapsamda trafik güvenliği için RDT'nin kazaları azaltıcı uygulamalarının değerli olduğu ancak daha bütünleştirici bir modele geçilmesinin gerekliliği ifade edilmektedir. Ayrıca, ileri RDT uygulamaları için çoklu hedef risk değerlendirmesine geçilmesi, katılımcı yöntemlerin kullanımı ve riskin çekici yönlerinin modele dâhil edilmesi önerilmektedir (Slovic ve Fischhoff, 1982, ss. 227-234; Zein ve Navin, 2003, ss. 1-9).

Son olarak Türkiye'de ve dünyada, trafik ve ulaşım psikolojisi alanyazında RDT temelli çalışmaların sayısının oldukça yetersiz olduğu söylenebilir. Bu kapsamda alanyazındaki açığı kapatabilmek ve RDT'nin varsayımlarını yeniden değerlendirip uyarlayabilmek için sürücülerin risk algısını ve davranışlarını etkileme potansiyeline sahip farklı nitelikteki araç güvenlik özelliklerinin, yol koşullarının ve kişilik özelliklerinin araştırılmasının katkı sağlayacağı düşünülmektedir.

KAYNAKÇA

Adams, J. G. U. (1988). Risk homeostasis and the purpose of safety regulation. *Ergonomics, 31*(4). 407-428. https://doi.org/10.1080/00140138808966688

Alexanderson, S. (1972). *Some Data About Traffic and Traffic Accidents.* Stockholm: The Swedish Road Safety Office.

Azık, D. ve Biçer, D. Ö. (2014). Emniyet kemeri kullanımı ve hız arasındaki iki yönlü ilişki: Orta Doğu Teknik Üniversitesi'nde bir gözlemsel çalışma. *Karayolu Trafik Güvenliği 5. Karayolu Trafik Güvenliği Sempozyumu ve Sergisi seçilmiş bildiriler I* içinde (ss. 119-130). Ankara: İklim.

Ba, Y., Zhang, W., Chan, A. H., Zhang, T. ve Cheng, A. S. (2016). How drivers fail to avoid crashes: A risk-homeostasis/perception-response (RH/PR) framework evidenced by visual perception, electrodermal activity and behavioral responses. *Transportation Research Part F: Traffic Psychology And Behaviour, 43,* 24-35. https://doi.org/10.1016/j.trf.2016.09.025

Brémond, R., Dommes, A. ve Engel, L. (2018). Driving at night with a cataract: Risk homeostasis? *Transportation Research Part F: Traffic Psychology and Behaviour, 53*(2), 61–73. doi:10.1016/j.trf.2017.12.009

Deery, H. A. (1999). Hazard and risk perception among young novice drivers. Journal of Safety Research, 30(4), 225–236. https://doi.org/10.1016/S0022-4375(99)00018-3

Dula, C. S. ve Geller, E. S. (2003). Risky, aggressive, or emotional driving: addressing the need for consistent communication in research. Journal of Safety Research, *34*(5), 559–566. https://doi.org/10.1016/j.jsr.2003.03.004

Elander, J., West, R. ve French, D. (1993). Behavioral correlates of individual differences in road-traffic crash risk: an examination method and findings. *Psychological Bulletin*, *113*(2), 279–294. https://doi.org/10.1037/0033-2909.113.2.279

Emniyet Genel Müdürlüğü. (2022). *Aylık kaza raporları.* Erişim Tarihi: 11.11.2022, http://trafik.gov.tr/istatistikler37.

Evans, L. (1986). Comments on Wilde's notes on "Risk homeostasis theory and traffic accident data." Risk Analysis, 6(1), 103–107. https://doi.org/10.1111/j.1539-6924.1986.tb00198.x

Evans, L. (1996a). The dominant role of driver behavior in traffic safety. *American Journal of Public Health*, *86*(6), 784–786. https://doi.org/10.2105/ajph.86.6.784

Evans, L. (1996b). Safety-belt effectiveness: the influence of crash severity and selective recruitment. *Accident; analysis and prevention*, *28*(4), 423–433. https://doi.org/10.1016/0001-4575(96)00006-1

Fuller, R. (1984). A conceptualization of driving behaviour as threat avoidance. *Ergonomics*, *27*(11), 1139- 1155. https://doi.org/10.1080/00140138408963596

Fuller, R. (2005). Towards a general theory of driver behaviour. *Accident Analysis & Prevention*, *37*(3), 461–472. https://doi.org/10.1016/j.aap.2004.11.003

Harano, R. M. ve Hubert, D. E. (1974). *An evaluation of California's" good driver" incentive program*. Sacramento, CA: Department of Motor Vehicles, (NTIS No. PB-235032/AS)

Hauer, E. ve Gårder, P. (1986). Research into the validity of the traffic conflicts technique. Accident Analysis and Prevention, 18(6), 471–481. https://doi.org/10.1016/0001-4575(86)90020-5

Heino, A., van der Molen, H. ve Wilde, G. J. S. (1996). Differences in risk experience between sensation avoiders and sensation seekers. Personality and Individual Differences, 20(1), 71–79. https://doi.org/10.1016/0191-8869(95)00152-V

Hoyes, T. W. ve Glendon, A. I. (1993). Risk homeostasis: issues for future research. *Safety Science*, *16*(1), 19-33.

Inagaki, T. (2008). Smart collaborations between humans and machines with mutual understanding. *Annual Reviews in Control*, *32*(2), 253–261. https://doi.org/10. 1016/j.arcontrol.2008.07.003

Jackson, J. S. H. ve Blackman, R. (1994). A driving-simulator test of Wilde's risk homeostasis theory. Journal of Applied Psychology, 79(6), 950–958. https://doi.org/10.1037/0021-9010.79.6.950

Janssen, W. (1994). Seat-belt wearing and driving behavior: An instrumented-vehicle study. Accident Analysis and Prevention, 26(2), 249–261. https://doi.org/10.1016/0001-4575(94)90095-7

Kita, E., Luria, G., Pindek, S., Albert, G. ve Lotan, T. (2022). The use of risk homeostasis theory to reduce smartphone use during low-speed

driving. *Accident Analysis & Prevention, 168,* 106596. https://doi.org/10.1016/j.aap.2022.106596

Liban, C. B., Vingilis, E. R. ve Blefgen, H. (1987). The Canadian drinking–driving countermeasure experience. Accident Analysis and Prevention, 19(3), 159–181. https://doi.org/10.1016/0001-4575(87)90001-7

Lund, A. K. ve Zador, P. (1984). Mandatory belt use and driver risk taking. *Risk Analysis, 4*(1). 41-53. https://doi.org/10.1111/j.1539-6924.1984.tb00130.x

Lund, A. K. ve Williams, A. F. (1985). A review of the literature evaluating the Defensive Driving Course. Accident Analysis and Prevention, 17(6), 449–460. https://doi.org/10.1016/0001-4575(85)90040-5

Lund, A. K. ve Ferguson, S. A. (1995). Driver fatalities in 1985-1993 cars with airbags. *The Journal of trauma, 38*(4), 469–475. https://doi.org/10.1097/00005373-199504000-00001

Lyu, N., Duan, Z., Ma, C. ve Wu, C. (2021). Safety margins–a novel approach from risk homeostasis theory for evaluating the impact of advanced driver assistance systems on driving behavior in near-crash events. *Journal of Intelligent Transportation Systems, 25*(1), 93-106. https://doi.org/10.1080/15472450.2020.1795846

McKenna, F. P. (1990). In defence of conventional safety measures: A reply to G. J. S. Wilde. *Journal of Occupational Accidents, 11*(3), 171-181. https://doi.org/10.1016/0376-6349(90)90027-S

Näätänen, R. ve Summala, H. (1976). *Road User Behavior and Traffic Accidents.* North-Holland/American Elsevier: Amsterdam/New York

O'Neill, B.ve Williams, A. (1998). Risk homeostasis hypothesis: A rebuttal. *Injury Prevention, 4*(2), 92-93. http://dx.doi.org/10.1136/ip.4.2.92

Orr, L. (1982). Goals, risk and choices. *Risk Analysis, 2*, 239-242. https://doi.org/10.1111/j.1539-6924.1982.tb01387.x

Oviedo-Trespalacios, O., Haque, M. M., King, M. ve Washington, S. (2017). Effects of road infrastructure and traffic complexity in speed adaptation behaviour of distracted drivers. *Accident Analysis & Prevention, 101*, 67-77. https://doi.org/10.1016/j.aap.2017.01.018

Peltzman, S. (1975). The Effects of Automobile Safety Regulation. *Journal of Political Economy*, *83*(4), 677–725. http://www.jstor.org/stable/1830396

Peterson, S., Hoffer, G. ve Millner, E. (1995). Are drivers of air-bag-equipped cars more aggressive? A test of the offsetting behavior hypothesis. *The Journal of Law and Economics*, *38*(2), 251-264. https://doi.org/10.1086/467331

Ranney, T. A. (1994). Models of driving behavior: A review of their evolution. Accident Analysis and Prevention, 26(6), 733–750. https://doi.org/10.1016/0001-4575(94)90051-5

Robertson, L. S. (1992). *Injury Epidemiology*. Oxford University Press, USA.

Sagberg, F., Fosser, S. ve Saetermo, I. A. (1997). An investigation of behavioural adaptation to airbags and antilock brakes among taxi drivers. Accident Analysis and Prevention**,** *29*(3), 293–302. https://doi.org/10.1016/s0001-4575(96)00083-8

Simonet, S. ve Wilde, G. J. (1997). Risk: perception, acceptance and homeostasis. *Applied Psychology*, *46*(3): 235-252. https://doi.org/10.1111/j.1464-0597.1997.tb01228.x

Slovic, P. ve Fischhoff, B. (1982). Targeting risks. *Risk Analysis*, *2*(4), 227-234. https://doi.org/10.1111/j.1539-6924.1982.tb01385.x

Slovic P. (1987). Perception of risk. *Science (New York, N.Y.)*, *236*(4799), 280–285. https://doi.org/10.1126/science.3563507

Streff, F. M. ve Geller, E. S. (1988). An experimental test of risk compensation: Between-subject versus within-subject analyses. Accident Analysis and Prevention**,** 20(4), 277–287. https://doi.org/10.1016/0001-4575(88)90055-3

Theeuwes, J., Alferdinck, J. W. ve Perel, M. (2002). Relation between glare and driving performance. *Human factors*, *44*(1), 95–107. https://doi.org/10.1518/0018720024494775

Tränkle, U. ve Gelau, C. (1992). Maximization of subjective expected utility or risk control? Experimental tests of risk homeostasis theory. Ergonomics**,** 35(1), 7–23. https://doi.org/10.1080/00140139208967794

Türkiye İstatistik Kurumu. (2022). *Karayolu trafik kaza istatistikleri, 2021*. Erişim Tarihi: 11.11.2022, https://data.tuik.gov.tr/Bulten/Index?p=Karayolu-Trafik-Kaza-Istatistikleri-2021-45658

Unrau, D.D. (2004). Driver response to rainfall on the Gardiner Expressway. (Unpublished Master's thesis). University of Western Ontario, Waterloo.

Wilde, G. J. S. (1982). The theory of risk homeostasis: implications for safety and health. *Risk Analysis*, *2*(4), 209-225. https://doi.org/10.1111/j.1539-6924.1982.tb01384.x

Wilde, G. J. S. (1988). Risk homeostasis theory and traffic accidents: propositions, deductions and discussion of dissension in recent reactions. *Ergonomics*, *31*(4), 441-468. DOI: 10.1080/00140138808966691

Wilde, G. J. S. ve Simonet, S. L. (1996). E*conomic fuctuations and the traffic accident rate in Switzerland: a longitudinal perspective.* Berne: Swiss Council for Accident Prevention. Erişim Tarihi: 31.01.2023, https://www.yumpu.com/en/document/read/6068312/economic-fluctuations-and-the-traffic-accident-rate-in-switzerland-

Wilde, G. J. S. (1998). Risk homeostasis theory: an overview. *Injury prevention*, *4*(2), 89-91. https://doi.org/10.1136/ip.4.2.89

Wilde, G. J. S. (2002). Does risk homeostasis theory have implications for road safety? *British Medical Journal*, *324*(7346), 1149–1152.

Wilde, G. J. S. (2013). Homeostasis drives behavioural adaptation. Behavioural adaptation and road safety: Theory, evidence and action. C. Rudin-Brown ve S. Jamson (Ed.), *Behavioural adaptation and road safety: Theory, evidence and action* içinde (ss. 61-86). Boca Raton: CRC Press. https://doi.org/10.1201/b14931

Williams, A. F., Wells, J. K. ve Lund, A. K. (1990). Seat belt use in cars with air bags. *American Journal of Public Health*, *80*(12), 1514–1516. https://doi.org/10.2105/ajph.80.12.1514

World Health Organization. (2021). *World health statistics 2021: monitoring health for the SDGs, sustainable development goals.* World Health Organization. Erişim Tarihi: 11.11.2022, https://apps.who.int/iris/handle/10665/342703.

Zein, S. R. ve Navin, F. P. D. (2003). Improving Traffic Safety: A New Systems Approach. *Transportation Research Record, 1830(*1), 1–9. https://doi.org/10.3141/1830-01

YAZIM KURALLARI

1. YAYIN İLKELERİ

1.1. Genel İlkeler

Jandarma ve Sahil Güvenlik Akademisi tarafından 2012 yılında yayımlanmaya başlayan Güvenlik Bilimleri Dergisi, "güvenlik" alanındaki kuramsal ve uygulamalı özgün araştırma, inceleme, derleme türündeki yazılar ile kitap incelemelerinin yayımlandığı ulusal ve uluslararası veri tabanlarında taranan ulusal hakemli ve basılı olarak yayımlanan bilimsel bir dergidir. Mayıs ve Kasım aylarında olmak üzere yılda 2 (iki) kez basılı ve online olarak yayımlanmaktadır.

Derginin yayın dili Türkçe olmakla birlikte, Yayın Kurulunun kararına bağlı olarak yabancı dilde yazılan makaleler de derginin genel ilkeleri çerçevesinde yayımlanabilir. Yazı başlığı, anahtar kelimeler ve makalenin öz kısmı, bütün makalelerde Türkçe ve İngilizce olarak bulunmak zorundadır.

Dergide **"güvenlik"** konusuna odaklı olmak şartı ile siyasal bilgiler, hukuk, kamu yönetimi, işletme, coğrafya, tarih, iletişim, ekonomi, bilişim, psikoloji ve sosyoloji vb. sosyal, beşeri, idari bilimler alanında özgün eserler ve daha önce yayınlanmamış veya herhangi bir yayın sürecine girmemiş araştırma, inceleme ve derleme türünde yazılar ile kitap incelemeleri yayımlanır. Ancak, bilimsel toplantılarda (kongre, sempozyum, seminer vb.) sunulan ve tam metni yayımlanmamış olan bildiriler, sunulduğu yer ve tarih belirtilmek şartıyla kabul edilir.

Dergide yayımlanması istenen yazılar, Türk Dil Kurumunun güncel dilbilgisi kurallarına (imla, noktalama, açıklık, anlaşılırlık vs.) uygun olmalıdır. Bu nedenle oluşabilecek sorunlardan ve eleştirilerden tamamen yazar sorumludur. Yayımlanmak üzere gönderilen makalelerin, derginin yayın ilkeleri ve yazım kurallarına uygunluğu Yayın Kurulu tarafından öncelik sırasına göre değerlendirilir.

Yayın ilkelerine ve yazım kurallarına uygun biçimde hazırlanmayan makaleler değerlendirmeye alınmaz ve hakeme gönderilmez. Yayın Kurulu yazıyı bilimsel yönden değerlendirmek üzere hakeme veya düzeltilmek üzere yazarına geri göndermek, yazının şekil ve formatıyla sınırlı kalmak kaydıyla düzeltme ve kısaltma yapmak, yayın ve etik kurallara uymayanları yayımlamamak yetkisine sahiptir.

Kör hakem sisteminin uygulandığı Güvenlik Bilimleri Dergisi'ne gönderilen makaleler, hakem değerlendirmesinden ve kitap incelemeleri de editör

değerlendirmesinden geçtikten sonra yayınlanır. Dergiye gönderilecek yazıların en az iki hakemden kabul alması gerekmektedir. Hakem değerlendirmeleri olumlu bulunduğu halde, makale sayısının fazla olması nedeniyle yayımlanmayan makaleler bir sonraki sayıda yayımlanmak üzere editör tarafından değerlendirilir. Bu şekilde 1 (bir) yıldan fazla bekleyen makale güncelliğini yitirdiği için yayımlanmaz.

Yayınlanan makalelerin ve kitap incelemelerinin bütün yayın hakları dergiye, yayınlanan yazıların içerik sorumluluğu ise yazara aittir. Makalelerdeki görüşler, yazarlarının şahsi görüşleri olup; hiçbir kurum ve kuruluşun resmi görüşü niteliğini taşımaz.

Yayın Kurulu ile hakem ve yazarlardan gelen bilgi, belge ve değerlendirme sonuçları 5 (beş) yıl süreyle saklanmaktadır.

Güvenlik Bilimleri dergisi ücretsiz bir dergi olup, yazarlara telif ücreti ödenmemektedir.

1.2. Etik İlkeler

Güvenlik Bilimleri Dergisi, bilimsel bilginin gelişimi açısından yayın etiğine büyük önem atfetmektedir. Bu açıdan, Yayın Etiği Komitesi (COPE) (https://publicationethics.org/) ve Açık Erişim Dergiler Dizini (DOAJ) (https://doaj.org/publishers#licensing) gibi kuruluşlar tarafından belirlenmiş Akademik Yayıncılıkta Şeffaflık ve Örnek Uygulama İlkeleri'ne bağlı kalınmaktadır.

Anket, mülakat, odak grup çalışması, gözlem, deney, görüşme teknikleri kullanılarak katılımcılardan veri toplanmasını gerektiren nitel ya da nicel yaklaşımlarla yürütülen her türlü araştırmalar, insan ve hayvanların (materyal/veriler dâhil) deneysel ya da diğer bilimsel amaçlarla kullanılması ve kişisel verilerin korunması kanunu gereğince retrospektif çalışmalar için etik kurul izni gerekmektedir. Etik kurul izni gerektiren bu tür çalışmaların izin ile ilgili bilgilerine makalede yer verilmelidir.

Ayrıca, olgu sunumlarında "Aydınlatılmış Onam Formunun" alındığının belirtilmesi, başkalarına ait ölçek, anket, fotoğrafların kullanımı için sahiplerinden izin alınması ve belirtilmesi, kullanılan fikir ve sanat eserleri için telif hakları düzenlemelerine uyulduğunun belirtilmesi gereklidir.

Bu dergi açık ve ücretsiz akademik yayıncılık ilkesine bağlı olduğundan, yazarlardan makale işleme ve gönderme ücretleri talep edilmez. Tüm içeriğe internet sayfası üzerinden herhangi bir kısıtlama ve gecikme olmaksızın yayın tarihinden itibaren tam metin olarak erişilebilir.

2. HAK VE SORUMLULUKLAR

2.1. Yayın Kurulunun Hak ve Sorumlulukları

Güvenlik Bilimleri Dergisi Yayın Kurulu, dergiye gönderilen makalelerden hangilerinin yayınlanacağına karar vermekten kolektif olarak sorumludur. Yayın Kurulu, COPE tarafından tanımlanmış İyi Yayın Uygulaması Kılavuzu'nun (https://publicationethics.org) uygulanmasını önererek akademik dürüstlüğü teşvik etmektedir.

Yayın Kurulu, etik kuralları ihlal ettiğini değerlendirdiği ve intihal önleme yazılımı taramasında benzerlik oranı yüksek çıkan makaleleri geri çekme hakkını kendinde saklı tutar. Yayın Kurulu, yayınlanmış makalelere ilişkin intihal ve suistimal iddialarını her zaman incelemeye alma hakkına sahiptir.

Yayın Kurulu, dergimize gönderilen bir makalenin bir başka derginin hakem sürecine de sokulmamış olmasını zorunlu bir başvuru koşulu olarak değerlendirir. Makalenin yayın kurulunca hakem sürecine alınması bir yayın taahhüdü anlamına gelmez. Yayın için hakem süreci olumlu sonuçlansa bile mutlaka yayın kurulunun kararı gerekir.

2.2. Yazarın Hak ve Sorumlulukları

Yazarlar hazırladıkları özgün çalışmalarla dergimize başvurmalıdırlar. Yazarlar, aynı çalışmayı aynı zamanda birden çok derginin hakem sürecine göndermemelidirler. Yazarlar kaynakların orijinalliğinden ve teyidinden de sorumludurlar. İntihal hangi şekilde yapılırsa yapılsın etik dış bir davranış oluşturur ve kabul edilemez.

Yazarın makalesini, yayın kararı alınıncaya kadar, dergi yayın kuruluna bildirmek koşuluyla geri çekme hakkı saklıdır.

Çeviri olsa dahi yayımlanan tüm yazıların dil, üslup, içerik, etik gibi konularda fikrî, ilmî ve hukukî sorumluluğu eseri yazan ve çevirisini yapan yazarlara aittir.

Yazardan düzeltme istenmesi durumunda, düzeltmenin en geç 2 ay içerisinde yapılarak Yayın Kurulu'na ulaştırılması gerekmektedir.

Yazarın hakem ve Yayın Kurulu'nun eleştiri, değerlendirme ve düzeltmelerinden katılmadığı hususlar olması durumunda, yazar bunları gerekçeleri ile ayrı bir sayfada bildirme hakkına sahiptir.

2.3. Hakemlerin Sorumlulukları

Dergide kör hakemlik sistemi uygulanmaktadır. Hakemler kendilerine ulaşan makaleleri gizli tutmak ve hakemlik sürecinden elde ettikleri bilgileri kişisel

menfaatleri için kullanmamakla yükümlüdürler. Hakemlerin değerlendirmelerini 20 gün içinde yapmaları beklenmektedir.

Hakemler raporlarını veya makale hakkındaki bilgileri başkalarıyla paylaşmamalı ve editörün izni olmadan yazarlarla doğrudan iletişim kurmamalıdırlar.

Hakem makaledeki potansiyel etik meseleler konusunda özenli olmalı ve bunları editörün dikkatine sunmalıdır. Hakemlik nesnel bir şekilde yapılmalıdır. Yazar(lar)a dair kişisel eleştiriler uygunsuz olarak kabul edilir.

3. YAZIM KURALLARI

3.1. Genel Esasları

- Yazarlar unvanlarını, görev yaptıkları kurumları, haberleşme adreslerini, telefon numaralarını, e-posta adreslerini ve ORCID (Open Researcher ve Contributor ID) numarasını bildirmelidir (http://orcid.org).

- Bilimsel yayınlar Türkçe veya İngilizce olarak hazırlanabilir. Türkçe makalelerin yazım ve noktalamasında ve kısaltmalarda TDK İmlâ Kılavuzunun en son baskısı esas alınır. Gönderilen yazılar dil ve anlatım açısından bilimsel ölçülere uygun, açık ve anlaşılır olmalıdır.

- Dergiye gönderilen makaleler, dipnotlar dâhil en az 4000 en fazla 7000 kelime olmalıdır. Kitap incelemeleri 1000-1500 kelime olmalıdır.

- Yazılar, makalenin başlangıç kısmına yazılmış, Türkçe ve İngilizce olarak hazırlanmış makale başlıklarını da içeren 150-200 kelimelik Türkçe "Öz" ile İngilizce "Abstract" ve makale başlığı içermelidir. Öz ve Abstract da çalışmanın amacı, yöntemi, varsayımı ve sonucu kısaca belirtilmelidir. İngilizce çalışmalarda önce İngilizce "Abstract", Türkçe çalışmalarda ise önce Türkçe "Öz" yazılmalıdır. "Öz" ve "Abstract" tek aralık, 9 punto ve italik olarak yazılmalıdır. Ayrıca her iki dilde de üç-yedi adet "anahtar kelime" eklenmelidir.

- Yazarın akademik unvanı, görevi ve bağlı bulunduğu kuruluş e-posta adresi ile ORCID numarası ilk sayfanın altına dipnotta (footnote) (*) işareti ile 9 punto ile yazılmalıdır. (Örnek; Dr. Öğr. Üyesi, JSGA, Güvenlik Bilimleri Enstitüsü, editorgbd@jandarma.gov.tr, ORCID:...)

- Tablo ve şekillere başlık ve sıra numarası verilmeli; başlıklar tabloların üzerinde, şekillerin ise altında yer almalıdır.

- Denklemlere sıra numarası verilmelidir. Sıra numarası ayraç içinde ve sayfanın sağ tarafında yer almalıdır.

- Yazılarda dipnotlara yer vermekten olabildiğince kaçınılmalı ve burada söylenecekler metin içinde ifade edilmelidir. Zorunlu olarak verilecek dipnotlar ise numaralandırılarak sayfa sonunda verilmelidir.

- Teknik terimler tırnak içinde yazılmalı veya açıklanmalıdır. Kavramlar için kısaltma kullanımından kaçınılmalıdır.

3.2. Sayfa Düzenine İlişkin Esaslar

- Yazılar, Microsoft Word'de, tek satır aralığı, Times New Roman ve 11'lik punto; marjlar üst 4,6; sol 4; alt 4,6; sağ 4; cilt payı 0, üst bilgi 4,6, alt bilgi 5, kâğıt ölçüsü A4 olacak şekilde hazırlanmalıdır.

- Yazı "GİRİŞ" bölümüyle sayfa başından başlamalı ve uygun bölümlere ayrılmalıdır. Son bölüm, "SONUÇ" bölümü olmalı ve bu bölümü takiben "KAYNAKÇA" ile varsa "EKLER" yer almalıdır. Ekler başlıklandırılırken; "EK-A", " EK-B" şeklinde sıralanmalı ve ek içinde "Başlıklar" bölümünde ifade edilen başlıklandırma kurallarına uyulmalıdır.

- Giriş, sonuç ve kaynakçaya numara vermeden; bölümler, ardışık olarak numaralandırılmalıdır. 3'üncü seviye başlıktan sonra (*, - vb) imleçler kullanılmalıdır. Bölüm başlıkları;

1. BİRİNCİ SEVİYE (Sola yaslanmış, kalın, büyük harflerle)
1.1. İkinci Seviye (Sola yaslanmış, kalın, ilk harflerleri büyük)
1.1.1. Üçüncü Seviye (Sola yaslanmış, italik, ilk harflerleri büyük)

- Her tablo ve şekil için sıra numarası verilmeli (Tablo-1., Şekil-2. gibi); tabloların başlığı üstte, şekillerin başlığı ise altta yer almalı, başlıklar tablo veya şekle ortalanmış olarak ilk harfleri büyük yazılmalıdır.

- Tablo ve şekil içeriği Times New Roman 10 punto olarak yapılandırılacaktır (Sayfa durumuna göre 9 veya 11 punto da kullanılabilir). İstatistikler için virgülden sonra üç haneden fazlası yazılmamalıdır. Tablo, şekil, grafik ve resim için şayet alıntı yapılmışsa, mutlaka kaynak belirtilmelidir.

- İlk sayfadan sonra, çift numaralı sayfalara yazar adı, tek numaralı sayfalara makale adı 9 punto karakterinde üst bilgi olarak eklenmelidir.

3.3. Atıf ve Göndermelere İlişkin Esaslar

- Metin içinde yapılacak atıflar ayraç içinde gösterilecektir. Kaynakça da bu atıf sistemine uygun olarak hazırlanacaktır. Aşağıda farklı nitelikteki kaynaklara yapılan atıf örnekleri gösterilmiştir:

- Walsh (1998) aile yılmazlığını, ailenin başa çıkma ve fonksiyonel bir birlik olarak aktarmaktadır (s. 108).

- İlişki içerisinde özgünlük, dürüstlük, kişinin tam olarak kendisini açmasıdır (Lopez ve Rice, 2006, ss. 13-14).

- Kessler'in 2003'te yaptığı çalışmaya göre ise ruh sağlığını güvence altına alan en önemli etken sıcak bir aile ortamıdır (s. 146).

- Örgütsel nitelikteki öncüller, örgütsel adalet algısı (Brewer ve Kramer, 1986; 45; Cremer, 2005a, ss.33-45; Lipponen, 2001, s. 24) gibi faktörlerden…

- Mael ve Ashforth (1992: 88) tarafından geliştirilen…

- Aynı yazar veya yazarların farklı çalışmalarında, çalışma tarihi daha eski olan önce yazılmalıdır. Aynı yazarın veya yazarların aynı tarihlerdeki çalışmalarında "a", "b" şeklinde harfler, çalışmanın yapıldığı yılın yanına yazılmalıdır.

- Üç, dört ve beş yazarı olan çalışmalarda ilk atıfta tüm yazarların isimleri verilmeli, müteakip atıflarda "vd." şeklinde kısaltılarak verilmelidir. Beşten fazla yazar varsa ilk yazarın soyadından sonra "vd." şeklinde ifade edilebilir.

- Bir yazarın düşüncelerinin yeniden ifade edilmesi zorsa veya anlamını yitirecekse 40 kelimeden daha fazla olmayan atıflarda kaynaktan alınan ifade tırnak işareti içinde belirtilerek yazılmalı ve o ifadenin bulunduğu sayfanın numarası belirtilmelidir. Örneğin: (Öztürk, 2003, s. 147). Eğer 40 kelimeden daha fazla atıf yapılması gerekiyorsa alıntı yapılan kısım, iki sekme içeriden, tırnak içinde yazılmalı, en sonuna alıntı yapıldığı yerdeki paragraf (para. 15) veya sayfa numarası (s. 25) belirtilmelidir.

- Yazar ismi belirtilmemiş bir çalışmaya atıf yapılması gerekiyorsa ve bu çalışma süreli bir yayındaysa yayının ismi, yazar olarak belirtilebilir. Örneğin; (Wall Street Journal, 2009), (Ticaret Bakanlığı, 1999).

- Aynı parantez içinde birden fazla çalışmaya atıf yapılacaksa çalışmalar alfabetik sıraya göre ve aralarına noktalı virgül konularak yazılmalıdır. Örneğin: (Abrams, 2000; Sullivan ve Hellman, 1999).

- İkincil kaynaklar, (Blau, 1964'ten akt. Tamer, 2003). Tamer'in (2003), Blau'dan (1964) aktardığına göre... şeklinde ifade edilerek ikincil kaynaklardan atıf yapıldığı belirtilmelidir.

- Elektronik kaynaklara atıf yaparken genel atıf kuralları geçerlidir (Yazar soyadı, yıl). Bu bilgi mevcut değilse, kaynağa ulaşılan web adresi parantez içinde verilmelidir. Yani yazarı belli olmayan bir elektronik kaynağa atıf yapmak

gerektiğinde web sitesi parantez içinde verilmelidir. Şayet profesyonel bir web sitesine, veri tabanına veya bir projenin web sitesine atıf yapmak gerekiyorsa, elektronik adres parantez içinde verilmeli, kaynakçada da aşağıda ilgili bölümde verilen örnekte görüldüğü gibi belirtilmelidir. (Örneğin: UNICEF web sitesi dünya çapında çocukların iyiliği için çalışan çeşitli yararlı kaynaklara bağlantılar sunmaktadır (http://www.unicef.org).

- Eğer mali destek veya diğer yardımları için teşekkür etmek istediğiniz kişi veya kurumlar varsa, çalışmanın sonuna bir not ekleyerek teşekkürlerinizi iletebilirsiniz.

3.4. Kaynakça Yazımında Uygulanacak Esaslar

- Kaynakça 11 punto olarak düzenlenecek ve soyad alfabetik sırasına göre tasniflenerek verilecektir. Ayrıca bir kategori yapılmayacaktır.

- Kitaplarda sayfa numaraları belirtilmeyecek, makalelerde derginin ilgili sayfa aralığı belirtilecektir.

- İnternet kaynaklarında erişim tarihi belirtilecektir.

- Kaynakça ile ilgili ayrıntılı hususlar için APA'nın (American Physchology Association) bilimsel yazı kriterlerine, Publication Manual of American Psychological Association (https://www.apastyle.org/manual) veya Dergi Park Yazım Kuralları'na (http://dergipark.gov.tr/busad/page/2914) bakınız.

- Kaynakçada yazar soyadının baş harfi büyük, adının ise ilk harfi olacak şekilde aşağıda verilen örneklerde olduğu şekilde yazılacaktır. DOI numarası mevcutsa referansın en son kısmına eklenecektir.

Kitaplar

Sarı, G. (2013). *Ermeni meselesi ışığında Süryaniler*. Ankara: Barış Platin Yayınevi.

Bloch, S. ve Whiteley, P. (2010). *Düz bir dünyada yöneticilik* (2.Basım). (Ü. Şensoy, Çev.) İstanbul: İş Bankası Yayınları.

Avcı, E. (2017). Türkiye'de terörizmin tarihsel seyri. G.Sarı ve C.K.Demir. (Ed.), *Güvenlik bilimlerine giriş* (ss. 287-314). Ankara: Jandarma Basımevi.

Makaleler

Ak, T. (2018, Mayıs). Silahlı insansız hava araçlarının kullanımında karar mekanizmaları. *Güvenlik Bilimleri Dergisi, 7*(1), 111-130. doi:10.28956/gbd.422803

Ansiklopedi

Ersoy, O. (1973). Kağıt. *Türk Ansiklopedisi* içinde (c. 21, ss.112-115). Ankara: Milli Eğitim Bakanlığı.

Yayımlanmamış Çalışmalar

Aplak, H.S. (2010). *Karar verme sürecinde bulanık mantık bazlı oyun teorisi*. (Yayımlanmamış Doktora Tezi). Gazi Üniversitesi, Ankara.

Kongre Bildirileri

Sarı, G. ve Ak, T. (2018). Güvenlik alan yeterlilikleri ve akademik çalışmalar. H.Kahya (Ed.), *1.Uluslararası Eğitim ve Sosyal Bilimlerde Yeni Ufuklar Kongresi bildiriler kitabı* içinde (ss. 130-134). İstanbul: ASOS. doi:10.21733/ibad.417321

Elektronik Kaynaklar

Shotton, M.A. (1989). *Computer addiction? A study of computer dependency*. Erişim tarihi: 18 Ağustos 2011, http://www.ebookstore.tandf.co.uk/ html/index

Yazarı belli olmayan web sitesi makalesi

New child vaccine gets funding boost. (2001). Erişim tarihi: 21 Şubat 2012, http://news.ninemsn.com.au/health/story_13178.asp.

Blog

Webber, S. (2008, 10 Ekim). Information literacy in work place contexts. Erişim tarihi: 22 Ekim 2008, http://information-literacy.blogspot.com/.

3.5. Kitap İncelemelerinde Uygulanacak Esaslar

Kitap incelemesi bir kitapta yer alan temel iddialar ve konular çerçevesinde yapılan kapsamlı ve detaylı bir araştırmadır. İnceleme akademik bir yazı kurgusu içerisinde giriş, tartışma (yöntem, kapsam ve içerik) ve sonuç gibi hususları içermelidir. Giriş kısmında kitaptaki tezler ve ana hususlar ile kısa bir özete yer verilmelidir. Tartışma kısmında kitabın ilgili sayfalarına ve gerekiyor ise başka eserlere de atıf vermek suretiyle yöntem, kapsam ve içerikte yer alan konular bir bütünlük içerisinde irdelenmelidir. Sonuç kısmında ise kitaba ilişkin temel düşünceler ve yazarın alana yaptığı katkılar değerlendirilmeli ve eleştirel bir şekilde ortaya konulmalıdır.

Kitap incelemelerinde başlık bilgilerinde inceleme yapılan eserin adı, yazarı, yayımlandığı kent ve yayınevi, yayım yılı ve ISBN numarası yazılmalıdır. Sayfa altında özel işarete karşılık olarak inceleme yapan yazarın akademik unvanı, mensup olduğu kurum ve e-posta adresi yazılır.

GUIDELINES

1. PUBLISHING PRINCIPLES

1.1. General Principles

The Journal of Security Sciences is a biannual journal indexed in both national and international indexes which offers theoretical and applied research, analysis and articles on "security" and published by the Gendarmerie and Coast Guard Academy since 2012. The Journal of Security Sciences is published twice in a year, May and November, as in print and online accessible journal.

The main publishing languages of the Journal are Turkish and English. The title, keywords and the abstract of the articles submitted to the journal must be both in Turkish and English.

The Journal of Security Sciences publishes original articles and book reviews focused on **"security"** aspect from different fields including but not limited to human sciences and public sciences on politics, law, public administration, management, geography, history, communication, economy, informatics, psychology, sociology etc. Submitted articles must not be published nor submitted to any other publications before. Conference/congress/seminar papers are accepted only if they are not previously published as full text and certain info such as presentation date and place provided.

Submitted manuscripts must follow the grammar rules. Therefore, the author is responsible of problems arising from the breaches of grammar rules of their articles.

Articles which fail to follow the Journal principles and guidelines may not be accepted for reviewing process. Editorial Board has the authority to send articles to reviewers, to send back articles to authors after reviews, to change articles formats, to abbreviate it or to decide not to accept articles which fail to follow the academic integrity and publishing standarts.

The submitted manuscripts undergo a double-blind reviewing process; articles are reviewed by referees whreas book reviews are reviewed by editorial board. To be accepted for publication in the Journal of Security Sciences, articles need to be positively peer reviewed at least by two referees. After articles are accepted for publishing, if there are more articles than the quota for the immediate volume, the

articles are automatically shifted for the next volume. If an article is not published this way within a year, it is withdrawn from publishing list.

The copyright for the published articles and book reviews belongs the Journal of Security Sciences, however authors remain responsible for the contents of publications. The Journal of Security Sciences is under no circumstances responsible for the contents of the articles/book reviews. Feedbacks and all relevant information about the articles/book reviews are stored by the Journal of Security Sciences for 5 years.

The Journal of Security Sciences is free of charge, hence no money is paid to the authors for the copyrights.

1.2. Ethical Principles

Journal of Security Sciences puts great importance on publication ethics regarding the development of the scientific information. Therefore, such principles like Transparency and Best Practice in Scholarly Publishing regulated by organizations like Committee of Publication ethics (COPE) (https://publicationethics.org/) and Directory of Open Access Journals (DOAJ) (https://doaj.org/publishers#licensing) are strictly followed.

Any kind of research applying either qualitative or quantitative data collection approach and using any methods like questionnaire, interview, focus group work, observation, experiment and discussion methods and involving people or animals (including materials and the data) for scientific or experimental purposes, and retrospective studies require research ethics committee approval regarding the law on the protection of personal data.

Moreover, it is required to note not only that informed consent form was taken in case reports, and that the permission to use their scales, surveys, photographs was given by the owners, but also that the regulations on the copyright about ideas and art pieces were strictly followed.

This academic journal sticks to principles like open-access and free of charge in scholarly publishing and thus never requires any fee for the admission of articles from their writers. The complete content is open to access online and full-text at the exact date declared and without any limitation.

2. RIGHTS AND RESPONSIBILITIES

2.1. Rights and Responsibilities of the Editorial Board

The Editorial Board of Journal of Security Sciences has the right and responsibility to decide the publication of articles and book reviews by taken into accounts feedbacks received from referees. The Editorial Board recommends publishing guides on (https://publicationethics.org) and promotes academic integrity.

Editorial Board has the right to decline articles and book reviews which contain plagiairised metarials or breach principles on academic integrity.

Submitted manuscripts must not be published or scheduled to appear in any other publications. Accepting a manuscript for peer reviewing process does necessarily mean a confirmation for publication.

2.2. Rights and Responsibilities of Author

Articles and book reviews submitted to the Journal of Security Sciences have to be original works of the authors. Submitted manuscripts should not be in any kind of submitting process in any other publishing platforms. The authors are responsible for the validity and confirmation of the bibliography. Plagiarism is not tolerated.

Author has the right to withdraw submitted manuscripts at any time before Editorial Board approves publication. In such cases, authors must inform the Board as early as possible.

In case of translated manuscripts, authors who write the original work and translators are both responsible for the contents and any breaches of academic integrity principles.

In cases where the manuscripts are sent back to authors for corrections after peer reviewed, the corrected manuscripts need to be submitted within 2 months.

In cases where the authors disagree with the feedbacks given by referees and Editorial Board they have a right to object. In such cases, authors need to submit their own thoughts and critics regarding the feedbacks given by referees and Editorial Board in written for re-consideration..

2.3. Responsibilities of Referees

The Journal ensures that manuscripts are reviewed by using a double-blind peer-review method. Referees are responsible for keeping the manuscripts

confidential and not using the knowledge and information they encounter via manuscripts for personal gain.

All reviews and information on manuscripts are strictly confidential and must not be shared with others. Referees are not allowed to contact with the authors unless allowed otherwise by the Editorial Board.

Referee is expected to inform the Journal of Security Sciences immediately in case of breaches arising from academic integrity during the review process if they determine any. Referees are expected to be objective and personal criticisms towards authors are not allowed.

3. GUIDELINE ON WRITING STYLE

3.1. General Principles

- Authors are required to submit the workplace info, contact addresses/numbers/email addresses and ORCID (Open Researcher and Contributor ID) number.

- Manuscripts can be Turkish or English. Submitted manuscripts should be clear and understandable.

- Articles should be between 4000 and 7000 words including the footnotes. Book reviews are required to be between 1000-1500 words.

- Articles must have 'Öz' in Turkish and 'Abstract' in English at the beginning and they must be written in between 150-200 words. Both 'Öz' in Turkish and 'Abstract' in English need to cover the purpose, method, hypothesis and results of the study briefly. Studies written in English should present the English 'abstract' before and those written in Turkish should present the Turkish 'Öz' before. Both Turkish 'Öz' and English 'Abstract' must be typed in single space, 9 point font and in italics. Also in both versions of the articles, at least three or at most seven key words must be added to the abstracts.

- Author's academic title, position, institutional email address and ORCID number should be stated in a footnote in the first page starting with a " * " 9 points font size. (Assoc. Prof., Gendarmerie and Coast Guard Academy Security Sciences Institute, editorgbd@jandarma.gov.tr, ORCID:… i.e.)

- Tables, figures and illustrstions should be numbered consecutively, captioned and cited in the text in sequential order. Captions should before the table and after the figures/illustrarions.

- Equations should be numbered consecutively. That number should be in parenthesis on the right side of the page.

- Authors need to refrain using footnotes and incorporate them with the main body.

- Technical terms need to be used with quotation marks and authors need to refrain from using abbreviations without providing the full form of them at first appearance in the text.

3.2. Principles Regarding Page Layout

- Manuscripts should have single line spacing, Times New Roman font, 11 font size, (Top 4.6 mm, bottom 4.6 mm, left and right indent 4 mm, gutter 0, header 4.6 mm, footnote 5 mm, paper size A4.

- Manuscripts should start with an introduction section, be separated into proper sections afterwards and following with a conclusion section. Bibliography needs to continue with the conclusion section and the last section should be the attachments section.

- Without numbered to introduction, conclusion and bibliography; sections should be numbered consecutively. Symbols such as (*, -) can be used after the 3rd level segment. Section headings;

1. FIRST LEVEL SEGMENT (ALIGN LEFT, BOLD, CAPITAL LETTERS)

1.1. Second Level Segment (Align Left, Bold, First Letters are Capital)

2.1.1. Third Level (Align Left, Italic, First Letters are Capital)

- Tables, figures and illustrations should be numbered (Table-1., Chart-2. ie.). Tables names should be on top of the tables and centered; names of the figures should be under the figures and centered as well.

- Contents of the tables and figures should be Times New Roman and 9 points font size (can be used as 9 or 11 according to the page layout). Statistical numbers are expected to have no more than 3 digits after decimal point. Tables, figures and illustrations should be cited if needed.

- After the first page, authors name should be in the header in even number pages and name of the manuscript should be on the odd page headers in 9 points font size.

3.3. Guideline for Citiations

- References in the body of your manuscripts should be in (Author, Date) format. When directly quoting from a text, you must include a page number in the citation as well.

- If you are using more than one reference by the same author/authors, the earlier dated publications should be listed first in the bibliography. If it is published in the same year, authors need to assign letter suffixes after the year i.e.: "Pala (1981a) makes similar claims...".

- Citiations for the publications with 3 and more authors should have their full names written for the first citing and then use “(The first authors surname) et al. for subsequent entries. If there are more than 5 authors, first author’s name should be followed with “et al.”

- If author is directly quoting from a work, then it will need to include the author, year of publication, and page number for the reference (preceded by "p."). Introduce the quotation with a signal phrase that includes the author's last name followed by the date of publication in parentheses.

- If the author is quoting more than 40 words, it is required to start the quotation on a new line, indented two tabs from the left margin, i.e. in the same place one would begin a new paragraph.

- In case of citing a periodic publication without a specific author name, the name of the publication can be used instead of author name. (Wall Street Journal, 2009 i.e).

- In case of parenthetical citation including two or more authors, it is required to order them alphabetically, separated by a semi-colon. (Abrams, 2000; Sullivan and Hellman, 1999).

- In case the source quotes or refers to another source, indirect sources should be cited as (Blau, 1964 cited in Tamer, 2013)

- Online articles follow the same guidelines for printed articles. Citiations should include all information the online host makes available.

- Authors may add an acknowledgement section at the end of the manuscripts to express thanks and pay their tribute.

3.4. Guideline for Reference List

- Reference list should be 12 points font size and written alphabetically. There should not be any other kind of categorization in the reference list.

- Book references won't be having page numbers but the articles will show the pages of the article in where it is published.

- Online sources should show the access date.

- This Journal utilizes APA 6th Reference Style with some minor differences. Please advise the manual for further info and details. (https://www.apastyle.org/manual)

- Authors surnames first letter should be capitalized and include only the first letter of the name. If there is any DOI number of the reference, it should be included in the reference as well. Please find the below examples of common references.

Books

Sarı, G. (2013). *Ermeni meselesi ışığında Süryaniler*. Ankara: Barış Platin Publishing.

Bloch, S. ve Whiteley, P. (2010). *Düz bir dünyada yöneticilik* (2nd Edition). (Ü. Şensoy, Trans.) İstanbul: İş Bankası Publishing.

Avcı, E. (2017). Türkiye'de terörizmin tarihsel seyri. G.Sarı ve C.K.Demir. (Ed.), *Güvenlik bilimlerine giriş* (pp. 287-314). Ankara: Jandarma Publishing.

Articles

Ak, T. (2018, Mayıs). Silahlı insansız hava araçlarının kullanımında karar mekanizmaları. *Güvenlik Bilimleri Dergisi, 7*(1), 111-130. doi:10.28956/gbd.422803

Encyclopedia

Ersoy, O. (1973). Kağıt. *Türk Ansiklopedisi* içinde (Vol. 21, pp.112-115). Ankara: Milli Eğitim Bakanlığı.

Unpublished Papers

Aplak, H.S. (2010). *Karar verme sürecinde bulanık mantık bazlı oyun teorisi*. (Unpublished Doctoral Thesis). Gazi University, Ankara.

Conference Proceedings

Sarı, G. ve Ak, T. (2018). Güvenlik alan yeterlilikleri ve akademik çalışmalar. In H.Kahya (Ed.), *1.Uluslararası Eğitim ve Sosyal Bilimlerde Yeni Ufuklar Kongresi bildiriler kitabı* (pp. 130-134). İstanbul: ASOS. doi:10.21733/ibad.417321

Electronic Sources

Shotton, M.A. (1989). *Computer addiction? A study of computer dependency*. Retrieved August 18, 2011, from http://www.ebookstore.tandf.co.uk/ html/index

Unknown Authored Online Articles

New child vaccine gets funding boost. (2001). Retrieved February 21, 2012, from http://news.ninemsn.com.au/health/story_13178.asp.

Blog

Webber, S. (2008, October 10th). Information literacy in work place contexts. Retrieved October 22, 2018, from http://information-literacy.blogspot.com/.

3.5. Guideline for Book Reviews

Book reviews are detailed reviews of claims and subjects of the books. The review should include an introduction, discussion (method, scope and contents) and conclusion. Introduction section is a summary of the claims and main arguments in the book. In the discussion sections, book reviewers are expected to discuss the method, scope and contents of the book in a whole. The conclusion section talks critically about the general impressions of the reviewer on the book and the contribution the book makes.

Book Review titles should include the name of the book, author, in which city it is published, publication year and ISBN. At the bottom of the first page the book reviewers need to include their title, the institution they work and email address corresponding to an asterisk

Gendarmerie and Coast Guard Academy

Security Sciences Institute

GBD

Journal of Security Sciences

Cilt/Volume: 12

Sayı/Issue: 1

Yıl/Year: 2023

Mayıs/May

ISSN: 2147–2912

E-ISSN: 2147–5075

www.jsga.edu.tr

Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü

Jandarma ve Sahil Güvenlik Akademisi Başkanlığı Beytepe/ANKARA
Telefon/Telephone: 0312 464 74 74 /Dahili/Ext.: 7600 / 7635
www.jsga.edu.tr/gbd
e-posta/email: editorgbd@jandarma.gov.tr