Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü

Güvenlik Bilimleri Dergisi

Uluslararası Güvenlik Kongresi Özel Sayısı

Ankara 2020

Gendarmerie and Coast Guard Academy
Security Sciences Institute

G B D

Journal of Security Sciences

Uluslararası Güvenlik Kongresi Özel Sayısı

Şubat/Feb 2020

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

Güvenlik Bilimleri Dergisi

The Journal of Security Sciences

GÜVENLİK BİLİMLERİ DERGİSİ

Uluslararası Güvenlik Kongresi Özel Sayısı ISSN 2147-2912 / E-ISSN 2147-5075

Güvenlik Bilimleri Dergisi; ULUKBİM TR Dizin, Akademia Sosyal Bilimler İndeksi (ASOS), Sosyal Bilimler Atıf Dizini (SOBİAD), EBSCO ve Araştirmax Bilimsel Yayın İndeksi veri tabanlarında taranmakta olup makalelere DOI numarası alınmaktadır.

BASKI

Jandarma Basımevi Müdürlüğü/ANKARA

YAZIŞMA VE HABERLEŞME ADRESİ

Jandarma ve Sahil Güvenlik Akademisi Beytepe / ANKARA

Telefon:0312 464 74 74 Dâhili: 6900 / 6910 / 6922

Web: http://www.jsga.edu.tr/guvben/guvben-dergi

E-posta: editorgbd@jandarma.gov.tr

THE JOURNAL OF SECURITY SCIENCES

Special Issue of International Security Congress 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: 6900 / 6910 / 6970

Web: http://www.jsga.edu.tr/guvben/guvben-dergi

E-mail: editorgbd@jandarma.gov.tr

GÜVENLİK BİLİMLERİ DERGİSİ

Danışma Kurulu

Prof. Dr. Abdülkadir ÇEVİK *Ankara Üniversitesi*	Prof. Dr. Nesrin HİSLİ ŞAHİN *Başkent Üniversitesi*
Prof. Dr. Ahmet İNAM *ODTÜ*	Prof. Dr. Nurettin GÜZ *Gazi Üniversitesi*
Prof. Dr. Ali ÇAĞLAR *Hacettepe Üniversitesi*	Prof. Dr. Osman CELBİŞ *İnönü Üniversitesi*
Prof. Dr. Ayla Sevim EROL *Ankara Üniv.*	Prof. Dr. Recep AKDUR *Ankara Üniversitesi*
Prof. Dr. Canan ATEŞ EKŞİ *Hacı Bayram Veli Üniversitesi*	Prof. Dr. Sadi ÇAYCI *Başkent Üniversitesi*
Prof. Dr. Abdulkadir VAROĞLU *Başkent Üniversitesi*	Prof. Dr. Salih CENGİZ *İstanbul Üniversitesi*
Prof. Dr. Doğan KÖKDEMİR *Başkent Üniversitesi*	Prof. Dr. Sertaç Hami BAŞEREN *Ankara Üniversitesi*
Prof. Dr. Feridun YENİSEY *Bahçeşehir Üniversitesi*	Prof. Dr. Şennur TUTAREL KIŞLAK *Ankara Üniversitesi*
Prof. Dr. Gökhan KOÇER *Karadeniz Teknik Üniversitesi*	Prof. Dr. Türel YILMAZ ŞAHİN *Hacı Bayram Veli Üniversitesi*
Prof. Dr. Haldun YALÇINKAYA *TOBB Üniversitesi*	Prof. Dr. Zehra DÖKMEN *Ankara Üniversitesi*
Prof.Dr.İsmail Hakkı DEMİRCİOĞLU *Jandarma ve Sahil Güvenlik Akademisi*	Prof.Dr. Lawrence SUSSKIND *Massachusetts Teknoloji Üniv. (ABD)*
Prof. Dr. Marco GERCKE *Siber Suçlar Arş. Enstitüsü (İngiltere)*	Doç. Dr. Özgür ÖZDAMAR *Bilkent Üniversitesi*
Prof. Dr. M.Emin ÇAĞIRAN *Gazi Üniversitesi*	Doç. Dr. Nihat Ali ÖZCAN *TOBB Üniversitesi*
Prof. Dr. Mesut Hakkı CAŞİN *Yeditepe Üniversitesi*	Doç. Dr. Edalet HESENOV *Adli Tıp Kurumu (Azerbaycan)*
Prof. Dr. Hakan KARAN *Ankara Üniversitesi*	Doç.Dr.Ayça GELGEÇ BAKACAK *Hacettepe Üniversitesi*
Prof. Dr. Nevin GÜNGÖR ERGAN *Hacettepe Üniversitesi*	Doç.Dr.Özlem ÖZREMİR *Fenerbahçe Üniversitesi*

Bu Sayının Hakemleri	
Doç. Dr. Elif ÇOLAKOĞLU *Jandarma ve Sahil Güvenlik Akademisi*	Dr. Gökhan SARI *Jandarma ve Sahil Güvenlik Akademisi*
Doç. Dr. Cenker Korhan DEMİR *Jandarma ve Sahil Güvenlik Akademisi*	Dr. Engin AVCI *Jandarma ve Sahil Güvenlik Akademisi*
Doç. Dr. Tekin AVANER *Jandarma ve Sahil Güvenlik Akademisi*	Dr. Yunus Emre KARAMANOĞLU *Jandarma Genel Komutanlığı*
Doç. Dr. Gökhan İbrahim ÖĞÜNÇ *Jandarma ve Sahil Güvenlik Akademisi*	Dr. Erdem ÖZGÜR *Jandarma ve Sahil Güvenlik Akademisi*
Doç. Dr. Cenay BABAOĞLU *Niğde Ömer Halis Demir Üniversitesi*	Dr. Tarık AK *Jandarma Genel Komutanlığı*
Doç. Dr. Barış ÖVGÜN *Ankara Üniversitesi*	Dr. Bürke Uğur BAŞARANEL *Jandarma ve Sahil Güvenlik Akademisi*
Dr. Öğr. Üyesi Mehmet. Levent YILMAZ *Polis Akademisi*	Dr. Fatih DEDEMEN *Jandarma ve Sahil Güvenlik Akademisi*
Dr. Öğr. Üyesi Ahmet BARBAK *İzmir Katip Çelebi Üniversitesi*	Dr. Mehmet KAHYA *Jandarma ve Sahil Güvenlik Akademisi*
Dr. Öğr. Üyesi İlhan SAĞSEN *Bolu Abant İzzet Baysal Üniversitesi*	Dr. Yusuf DÜNDAR *Jandarma ve Sahil Güvenlik Akademisi*
Dr. Tuğba Evrim MADEN *Serbest*	Öğr. Gör. Müge BORAZAN ÇELİKBIÇAK *Jandarma ve Sahil Güvenlik Akademisi*

Referees of this Issue	
Assoc.Prof. Elif ÇOLAKOĞLU, Ph.D. *Gendarmerie and Coast Guard Academy*	Gökhan SARI, Ph.D. *Gendarmerie and Coast Guard Academy*
Assoc. Prof. C. Korhan DEMİR, Ph.D. *Gendarmerie and Coast Guard Academy*	Engin AVCI, Ph.D. *Gendarmerie and Coast Guard Academy*
Assoc. Prof. Tekin AVANER, Ph.D. *Gendarmerie and Coast Guard Academy*	Yunus Emre KARAMANOĞLU, Ph.D. *Gendarmerie General Command*
Assoc. Prof. Gökhan İ.ÖĞÜNÇ, Ph.D. *Gendarmerie and Coast Guard Academy*	Erdem ÖZGÜR, Ph.D. *Gendarmerie and Coast Guard Academy*
Assoc. Prof. Cenay BABAOĞLU, Ph.D. *Niğde Ömer Halis Demir University*	Tarık AK, Ph.D. *Gendarmerie and Coast Guard Academy*
Assoc. Prof. Barış ÖVGÜN, Ph.D. *Ankara University*	Bürke Uğur BAŞARANEL, Ph.D. *Gendarmerie and Coast Guard Academy*
Instructor M. Levent YILMAZ, Ph.D. *Police Academy*	Fatih DEDEMEN, Ph.D. *Gendarmerie and Coast Guard Academy*
Instructor Ahmet BARBAK, Ph.D. *İzmir Katip Çelebi University*	Mehmet KAHYA, Ph.D. *Gendarmerie and Coast Guard Academy*
Instructor İlhan SAĞSEN, Ph.D. *Bolu Abant İzzet Baysal University*	Yusuf DÜNDAR, Ph.D. *Gendarmerie and Coast Guard Academy*
Tuğba Evrim MADEN, Ph.D. *Work Freelance*	Instructor Müge BORAZAN ÇELİKBIÇAK, *Gendarmerie and Coast Guard Academy*

İÇİNDEKİLER

CONTENTS

EDİTÖRDEN

Güven ve güvenlik kavramları birey için söz konusu edildiğinde ve birel eylem ve işlem olarak kaldığında bile ne meşakkatli anlam ve süreçlere konu olmaktadır. Âdemoğlu bir toplumsal yaratık olmasa, hep doğa durumunda kalsa daha güvenlikli bir düzende yaşar mıydı bilinmez, imzaladığı sözleşmeyle görünürde daha medeni olmasına karşın maddi yaratımına inat değerlerini oluşturamamış görünüyor. Epik tiratlar, hamasi diskurlar, didaktik vurgular, normatif düzlemde ve bildiri ya da beyannamelerin metinlerinde istediği kadar var olsun, hafif bir baş çevirmeyle birlikte yalancı cennet yanında Hobbes'un canavarı olanca gövdesiyle kendini gösteriveriyor. Yaratıcısının elinde divit var ancak gelişmiş Leviathanlar su değil ateş saçıyor. Sadece bireye değil, bulabildiği her şeye ve herkese. Güçlü olan ve haklı olan arasındaki ilişki güçlü haklıdır biçiminde dayatıldıktan sonra istenildiği kadar postmodern savlarla güvenlik çeşitlendirilsin ve içi boşaltılsın, realpolitik olduğu yerde duruyor ve azgelişmiş dimağlar oyalanıp duruyor.

İç güvenlik ve dış güvenlik anlam ve çizgi olarak ayrışma-karışma noktasında izleri belirsizleştirilmiş olarak günümüzde sunuluyor sunulmasına karşın, sorun da çözüm de bu sorunu yaratanlarca icat ediliyor. Gelişmiş olduğu savlanan ülkeler iç güvenlik sorunlarını çoğunlukla çözmüş ya da 11 Eylül ya da benzeri bombalı hatta biyolojik ekstremite içeren vakalarla anılıyor. Ancak rövanşı, taarruzu ya da tepkisi kurama dönüştürülüveriyor. İletişim ve ulaşım sektöründen başlayarak baş döndürücü gelişmeler ve o arada teknolojik gelişmeler küreselleşerek virüs, bakteri hasılı mikroplarını saçıveriyorlar. Zehirlenen sabiler, düzensiz göçmenler, yok edilen nesiller distopik bir kurgu değil. En yanımızda, yanı başımızda. Suriye, Irak, Filistin, Doğu Akdeniz sayıp bitmeyecek böl parçala oyunlarının devamı aynı zamanda… Sonunda sirayet ediyor, etmese de adalet duygusu, vicdanlar yaralanıyor, ulusal güvenlik ve çıkarlar pragmatik zamanlarda gözü doymayanların çokluğuna rağmen unutulmaması gerekiyor.

Geleneksel zamanlar ya da bugünkü ismiyle kurulduğu günden beri ülkemizin fedakâr kanun ordusu Jandarma ve onun her düzeyde teşkilatı ve her bir neferi ülkesini canı pahasına ve bu şiarla korumak için bir yandan yeteneklerini geliştirmeyi sürdürüyor diğer yandan güvenlik ve savunmamıza yurt içinde ve dışında destek oluyor, gece gündüz çalışıyor. Bilimsel süreçler doğrultusunda en iyi eğitimlerden geçerek, yarının her düzeyde donanımlı genel kolluk kuvvetini oluşturmayı amaçlayan anlayış meyvelerini veriyor. İşte bu özel sayıda uluslararası düzeyde katılımlı ve çok kapsamlı bilimsel etkinliğin ürünlerini görmekteyiz. Anlamak, tedbir almak, ülkemizin geleceği adına vesselam.

Filhakika 19 – 20 Eylül 2019 tarihinde İçişleri Bakanlığı Jandarma ve Sahil Güvenlik Akademisi tarafından düzenlenen Uluslararası Güvenlik Kongresi, böylesine bir amaç ve hedefle, güvenlik kavramına Kuram, Yöntem ve Uygulama perspektifinden akademik yaklaşımların ve çalışmaların paylaşıldığı uluslararası bir ortam sağlamıştır. Kongrede sunulan birbirinden kıymetli bildirilerden yazarları tarafından Güvenlik Bilimleri Dergisinde yayınlanmak üzere gönderilen makalelerin hakem süreçleri tamamlanmış ve 12 makale Uluslararası Güvenlik Kongresi Özel Sayısında yayına değer görülmüştür.

SERT, DEMİR ve **AVCI** çalışmalarında Fetullahçı Terörist Örgüt (FETÖ)'ünün organizasyon modeli, stratejisi ve motivasyonlarını oluşturan dinamikleri araştırılmış ve bu doğrultuda örgütün kendine özgü özelliklerine değinilmiştir.

ATEŞ, BOSTANCI ve **GÜZEL** makalelerinde Endüstri 4.0 ile birlikte, güvenlik sorunlarının çok daha spesifik hale geleceği ve otomasyon kavramının güvenlik sorunlarına yeni paradigmalar ekleyeceği, genel anlamda siber tehdit mağduriyetlerinin artacağı değerlendirilmekte, güvenlik güçlerinin bu değişime uyum sağlaması ve yeni tehditlere karşı koyabilecek, dinamik bir siber suçla mücadele politikası benimsemesi gerektiğini ifade etmiştir.

DEMİR makalesinde uluslararası ilişkiler literatüründe yer alan anklav ve eksklav kavramlarının tanımlaması ve güvenlik kavramı ile olan ilişkisi irdelenmiştir.

AHSAN makalesinde benzer özelliklere sahip olan Dakka ve Ankara şehirlerinde iklim değişikliği etkisine bağlı olarak mevcut eğilimler, suya dayalı uyum-tabanlı stratejiler ve güvenlik konuları ele alınmıştır.

MEMİŞ ve **GÜÇ** çalışmalarında son yıllarda gündeme gelen akıllı kent kavramı ve beraberinde getirdiği büyük verinin gizliliğini, güvenliğini güçleştiren ve bunları tehdit eden unsurlar ele alınarak ortaya çıkan olumsuzlukları gidermek amacıyla gündeme gelen ilkeler ve yaklaşımlar incelenmiştir.

AKDEMİR, SUNGUR ve **BAŞARANEL** tarafından yazılan makalede günümüzde birçok ülke için birincil öncelikli konu statüsünde olan siber suçların küresel bir tehdit olması uluslararası işbirliğinin gerekliliği ortaya konulmaktadır. Bu doğrultuda AB Ağ ve Bilgi Güvenliği Ajansının yeniden yapılandırılmasıyla sağlanan fayda ile bu inisiyatifin AB üyesi olmayan ülkeleri de kapsaması gerekliliğini ortaya koymaktadır.

POLAT makalesinde bir savunma örgütü olarak kurulan NATO'nun siber uzayda üye devletlerin güvenlik ihtiyaçlarını karşılamak amacıyla yeniden yapılanması ve siber güvenlik alanında üye devletlerin sahip olduğu tecrübe ve yeteneklerin diğer üyelere de transfer edilmesinin önemini ifade etmiştir.

TATAROĞLU makalesinde Rusya kolluk teşkilatının tarihten günümüze geçirdiği yapısal ve işlevsel dönüşüm, tarih ve hukuk bilimi çerçevesinde incelenmiş, özellikle 2000'li yılların başında kolluk teşkilatında gerçekleşen reform hareketlerinin dinamikleri değerlendirilmiştir.

BAHAR ve **BİLEN** makalelerinde hiç şüphesiz birçok devletin en önemli gelir kaynağı olan turizm sektörünün başarısı için kritik öneme sahip güvenlik algısı kavramının etkisi incelenmiştir. Özellikle turizmin Türkiye ekonomisi üzerine etkileri hakkında elde edilen bulgular çerçevesinde güvenlik algısının önemi irdelenmiştir.

KAPLAN çalışmasında terörle ve suçla mücadelede sosyal medyanın kolluk tarafından kullanımı, suçla mücadelede ve suçluların tespitinde kullanılması kapsamında karşılaşılan eksiklikler ve ihtiyaçlar incelenmiştir.

BİRDİŞLİ makalesinde uluslararası güvenliğin tarihsel gelişimi, primitif, modern ve post-modern güvenlik dönemi, güvenliğin dinamik, devrimsel gelişmeler çerçevesinde değerlendirilmiştir.

YENİÇERİ ve **US** makalelerinde radikalleşme ve radikalleşmenin nedenlerinin anlaşılması, toplumsal güvenliğin sağlanması ve toplumsal düzenin sürdürülmesi açısından radikalleşme kavramının ölçülebilmesi gerektiği ifade edilmiş ve bu kapsamda dünya literatüründe kullanılan ölçeklerin Türkçe literatüre kazandırılmasına yönelik değerlendirme yapılmıştır.

Bilim dünyasına ve ülkemize hayırlı ve yararlı olması dileğiyle.

Arz ederiz.

Özel Sayı Editörleri

EDITOR'S NOTE

The terms, safety and security become a subject to toilsome processes to define them even when they are considered about the individual and remain as an action or a function. Whether the mankind was not a social creature, and he was in the natural condition, it is unpredictable whether he would still live in a secure order. Even though he became more civilized due to the contract he approved, he still seems not to have formed his values just to spite his nature of creation. No matter how much epic harangues, heroic discourses and didactic intonations exist on normative grounds and in declarations or manifestations, Hobbes' leviathan burst into sight magnificently contrary to the counterfeit heaven. His creator holds a dip pen despite leviathans do fire, not water, not only on the individual, but on anyone and anything. After the relation between the powerful and the right is exposed to as the former is the right, real politics remains the same as underdeveloped mind does no matter how diversified and meaningless security has become due to postmodern assertions.

Internal and external security are presented in a way that does not have clear borders and meanings today, yet both problems and solutions to them are also put forward by the same that causes this ambiguity. Countries claimed to be developed are mentioned to have overcome their security issues or to have undergone bombing and biological extremity incidents like 11/9. However, their revenge, attack or reactions suddenly turn out to be theory. Mind-blowing developments starting from communication and transportation, along with technological ones spread viruses, bacteria and microbes globally. Poisoned children, irregular migrants, extinction of generations are real. Near Turkey, Syria, Iraq, Palestine and East Mediterranean are stages for divide and conquer politics. Finally, it spreads; otherwise, it hurts sense of justice and conscience. Yet, national security and interests, though the great number of the greedy ones, must never be dismissed at pragmatic times. Since old times or its foundation, Gendarme has been a devoted law enforcer, and its organizations and each member continue to improve their skills to guard their country at the cost of their lives. Besides, they give support to security and defense of the country night and day. Philosophy aiming to educate and train law enforcement that is well equipped with future essentials through scientifically approved processes yield its results. In this special issue, the results of international and comprehensive congress are presented. That is to understand, take measures for the sake of our country.

The International Security Congress, held on 19th-20th September by Gendarmerie and Coast Guard Academy, Ministry of Interior, pursued the aim of providing an opportunity to discuss and share Theory, Method and Practice related to the concept of security. Refereeing processes of articles presented in the Congress that are shared by their authors to be published in the Journal of Security Sciences have been completed, and 12 of them were considered to be published in this special issue of the Journal.

SERT, **DEMİR** and **AVCI** studied in their article about Fethullahist Terrorist Organization's structure, strategy and motivations, and they mentioned abovementioned organization's typical characteristics accordingly.

ATEŞ, **BOSTANCI** and **GÜZEL**, regarding Industry 4.0, consider that security problems will become more specific and autonomy will add more paradigms to those problems. Besides, victims of cyber threats will unavoidably increase. They also consider that law enforcement agencies must keep up with abovementioned changes and they must adopt a new ever-changing policy against cyber threats and new threats.

DEMİR analyzed the terms enclave and exclave, which are specific to International Relationships, and he talked about the relation between these terms and security.

DEAHSAN compared two similar cities, Dakka and Ankara regarding climate change related current trends, water dependent adaptation strategies and security issues.

MEMİŞ and **GÜÇ** mentioned a current topic, smart cities, and issues posing a threat to security and secrecy of big data related to the topic, and they analyzed the principles and approaches so as to deal with those threats.

AKDEMİR, **SUNGUR** and **BAŞARANEL** put forward the idea that cooperation against cybercrimes that are both universal threats and among priority issues for every nation is indispensable. They, also claim that EU Network And Information Security Agency that has been recently restructured should be open not only to EU members but this entity should coven non-EU member nations to combat against cybercrimes.

POLAT expresses the idea that NATO, which was established as a security organization, is to be reorganized against cyberspace threats so as to fulfill its

members' essentials and that NATO members that have the cyberspace technology should transfer their knowledge and capabilities to other NATO member states.

TATAROĞLU, in his article, depicted the structural and functional transformation of the Russian law enforcement regarding historical and judicial perspectives. Then, he focused on and evaluated the reforms that the Russian law enforcement gone through in the 2000s.

BAHAR and **BİLEN** analyzed the tourism security that is unavoidably vital for every country's economy. They especially focused on the effect and importance of tourism on Turkish economy and perception of security in this sector.

KAPLAN in his study, writes about historical development of international security regarding primitive, modern and post-modern security periods, and dynamic and revolutionary improvements of security.

BİRDİŞLİ writes about historical development of international security regarding primitive, modern and post-modern security periods, and evaluates ever-changing and revolutionary improvements in security.

YENİÇERİ and **US**, in their article, claim that both radicalization and its causes must be unveiled, and to ensure social security and order, radicalization concept must be measured. Regarding this, they considered that scales applied in the world literature must be translated into Turkish.

Hope these studies will be beneficial and helpful for the academic world and our country.

Yours sincerely,

Special Issue Editors

STRATEJİ, ÖRGÜTLENME VE MOTİVASYONUYLA KENDİNE ÖZGÜ BİR TERÖRİST ÖRGÜT: FETÖ

Arman SERT[*], Cenker Korhan DEMİR[**], Engin AVCI[***]

Öz

Tarihsel olarak terörizm tiplerinin hemen hepsine şahitlik eden Türkiye, Fetullahçı Terörist Örgüt (FETÖ)'ün devletin çeşitli kademelerine sızdırdığı, elemanlarıyla gerçekleştirmeye çalıştığı darbe girişimi neticesinde yüzlerce şehit ve binlerce yaralı vermiştir. Her ne kadar örgüt, şiddet eylemlerini 15 Temmuz 2016 tarihinde gerçekleştirmiş olsa da kuruluşu ve gelişimi bunun çok öncesine uzanmaktadır. Terörist örgüt; uyguladığı yöntemler, eylem tipleri, eleman temini, örgütlenme, din istismarı, yurt dışı bağlantıları gibi birçok özellik sebebiyle benzerlerinden farklılık arz etmektedir. Bu nedenle FETÖ, 21'inci yüzyılın getirdiği avantajları da kullanan taktik ve stratejisiyle terörizm çalışmalarının odaklanması gereken önemli bir araştırma konusudur.

Bu çalışmanın amacı; FETÖ'nün organizasyon modelini, stratejisini ve motivasyonlarını oluşturan dinamiklerin araştırılması ve bu doğrultuda örgütün kendine özgü özelliklerinin ortaya çıkarılmasıdır. Araştırmanın temel varsayımı; bu dinamiklerin diğer terörist örgütlerle benzer yanlarına rağmen önemli farklılıklar taşıdığı, bu sebeple de FETÖ' nün kendine özgü yeni tip bir terörist örgüt olduğudur. Çalışmada tarihsel perspektif göz önünde bulundurularak çeşitli terörist örgütlerin organizasyon modelleri, stratejileri ve motivasyon kaynakları incelenmiştir. Bunlar FETÖ ile karşılaştırılarak benzerlikler ve farklılıklar belirlenmiş ve çalışmanın temel varsayımı karşılaştırmalı vaka analizleri aracılığıyla sorgulanmıştır.

Anahtar kelimeler: *FETÖ, Terör, Strateji, Motivasyon, Örgütlenme.*

A SUI GENERIS TERRORIST ORGANIZATION WITH ITS STRATEGY, ORGANIZATION AND MOTIVATION: FETO

Abstract

Turkey, which has historically witnessed almost all types of terrorism, has also suffered from hundreds of martyrs and thousands of casualties as a result of the coup attempt

[*] Araştırma Görevlisi, JSGA, Güvenlik Bilimleri Enstitüsü, Uluslararası Güvenlik ve Terörizm Ana Bilim Dalı, armansert23@gmail.com, https://orcid.org/0000-0001-7101-6702

[**] Doç. Dr., Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü, ckdemir@gmail.com, https://orcid.org/0000-0001-8016-7123

[***] Dr., Jandarma ve Sahil Güvenlik Akademisi Araştırma Merkezleri Müdürlüğü, engavci@gmail.com, https://orcid.org/0000-0002-5881-1530

Makale Geliş Tarihi: 06.11.2019 Makale Kabul Tarihi: 09.12.2019

carried out by the Fetullahist Terrorist Organization (FETO) with its members infiltrated through various levels of the state. Although the organization committed acts of violence on July 15, 2016, its organization and activities date back well before. This terrorist organization differs from its counterparts due to its methods, types of actions, recruitment and indoctrination, organization, exploitation of the religion and connections abroad. Therefore, FETO is an important research subject that should be of interest to terrorism studies with its tactics and strategy, which also uses the advantages of the 21st century.

The aim of this study is to analyze the dynamics that constitute the organizational model, strategy and motivations of FETO and to reveal the unique characteristics of the organization in this respect. The basic assumption of the research is that these dynamics, despite their similarities with other terrorist organizations, have significant differences, and therefore FETO is a new type of terrorist organization. Organizational models, strategies and motivational sources of various terrorist organizations were examined by taking historical perspective into consideration. These were compared with FETO, similarities and differences were determined and the basic assumption of the study was questioned through comparative case studies.

Keywords: *FETO, Terror, Strategy, Motivation, Organization.*

GİRİŞ

Geçmişi eskiye dayanan terörizm, günümüzde farklı tip ve yöntemlerle karşımıza çıkarak tehlike oluşturmaya devam etmektedir. Terörizmi tanımlama gayretlerindeki çeşitlilik ve ortak noktalarda buluşamama durumu, bu fenomenin anlaşılmasında kullanılan siyasal yaklaşımlar nedeniyle devam etmektedir. Bunun yanında terörizmin küreselleşen bir boyuta taşınması ile beraber, terörist örgütlerin stratejilerinin, organizasyon modellerinin ve motivasyonlarının da eşzamanlı olarak evrildiği dikkat çekmektedir.

Türkiye'nin 15 Temmuz 2016 tarihinde maruz kaldığı darbe girişimi sırasında karşılaştığı terör eylemleri de bu anlamda yeni tip bir örgüt ve stratejiyi işaret etmiştir. Bu kapsamda, varlığını devam ettiren bir tehdit olarak Fetullahçı Terör Örgütü (FETÖ)'nün incelenmesinin önemli olduğu değerlendirilmektedir. Zira bu terörist örgütün stratejisi, motivasyonu ve organizasyon modelinin ortaya konulması sonucunda bu ve benzeri örgütlerle uygun mücadele yöntemlerinin geliştirilmesi mümkün olabilecektir. FETÖ'nün dinamiklerinin analiz edilmesinden önce, tarihsel perspektifte kendinden önceki bazı terörist örgütlerin incelenmesi, yapılacak karşılaştırmalı vaka analizleri için bir ışık tutacaktır.

Bu kapsamda, çalışmanın birinci bölümünde, tarihsel perspektif içerisinde terörist örgütlerin uyguladıkları stratejiler, sahip oldukları organizasyon modelleri ve motivasyon kaynakları incelenecektir. İkinci bölümde, terörist örgütlerin stratejileri, organizasyon modelleri ve motivasyonları ile ilgili öne çıkan teorik yaklaşımlar ortaya konularak bir sonraki bölümde yapılacak analiz için çerçeve oluşturulacaktır. Üçüncü bölümde ise FETÖ'nün stratejisi, organizasyon modeli ve motivasyonu oluşturulan analiz çerçevesi dâhilinde incelenecektir.

1. MODERN TERÖRİZMİN EVRİMİ

Alanyazında terörizmin tarihsel arka planı ile ilgili değerlendirmeler sıklıkla miladi takvimin başlangıcına paralel olarak yapılmaktadır. Çok eski tarihlerden itibaren terörü benzer amaçlarla kullanan birçok örgüt olsa da terörizmin kendine özgü bir kavram olarak Fransız Devrimi ile ortaya çıktığı bilinmektedir. Walter Laqueur (2002: 22) terörizmin tarihini içeren çalışmasında, özellikle 18. yüzyıl sonları ve 19. yüzyıl başlarında monarşilere karşı oluşan tepkiler nedeniyle "zalim hükümdar" olarak nitelendirilen kral, padişah veya imparatorlara yönelik suikastların planlandığına dikkat çekmektedir.

Bununla beraber, sadece hükümdarı öldürmekle monarşinin yıkılamayacağı ve doğrudan sistemin kendisinin geniş bir cephede hedef alınması gerektiği düşüncesi ilk kez 18. yüzyıl sonlarından itibaren gizli cemiyetler (*secret societies*) tarafından tartışılmıştır (Laqueur, 2002: 22).

1.1. Gizli Cemiyetlerden Anarşistlere

Gizli cemiyetler, mistik/dini uğraşları (ama çoğu zaman da çok somut sosyal işlevlere sahip) ve ritüelleriyle birçok uygarlıkta çok eski zamanlardan beri var olmuştur (Laqueur, 2002: 23). Bunlarla ilgili dikkat çeken bir husus, gizliliklerinin bir sonucu olarak, faaliyetlerinin kapsamı ve öneminin somut verilerden ziyade çoğunlukla abartıya dayandığı, bunun da mistik veya gizli doğalarını genişletici bir etki doğurduğudur. Bir diğer husus ise, artık siyasi düzeni değiştirmeye yönelik düşüncelerle hareket etmeye başlamalarıdır. "*Zalim hükümdara karşı her yol mubah*" ve "*kutsal bir amaca ulaşmak için uygulanan yöntemlerin hiçbiri suç oluşturmaz*" benzeri önermeler bu dönemden itibaren yayılmaya başlamıştır (Laqueur, 2002: 23). Başlarda daha çok bireysel, içgüdüsel ve gelişigüzel olduğu görülen bu düşünceler, sonrasında siyasal bir içerik taşımaya başlayarak bugünkü anlamda terörizme yaklaşmıştır.

Her ne kadar kendinden önce bazı gizli cemiyetler var olsa da etkili olduğu dönemde (özellikle 19. yüzyıl başları) uluslararası sistemdeki statükoya karşı Avrupalı bazı devletlerce tehdit olarak görülen ve kanlı şiddet eylemleri sebebiyle ön plana çıkan *Carbonari*[1] örgütü bu anlamda verilebilecek ilk örneklerden biridir ve kökenleri, yapısı, öğretileri ve faaliyetlerinin anlaşılması üzerinde gizem ve belirsizlikler bulunmaktadır (Shiver, 1964: 234). Strateji, örgütlenme ve motivasyon gibi dinamikleri incelendiğinde de FETÖ ile benzerlikler gösterdiği söylenebilir.

Bir defa bu cemiyete katılanların, aile ve milliyet bağları da dâhil olmak üzere tüm bireyselliklerini yitirdikleri, tamamen "usta/efendilerine" (*master*) ait hale geldikleri ve örgütten çıkmalarının neredeyse imkânsızlaştığı bilinmektedir (Laqueur, 2002: 24). Örgüte yeni katılanlar birer "çırak" (*apprentice*) olarak adlandırılırken, çıraklardan oluşan hücrelerin sorumlularına ise usta/efendi denilmektedir. Bunların üstünde de "büyük efendi/usta" (*grand master*) bulunmaktadır (Frost, 1876: 213). Sonuç olarak örgüt elemanları, kendi ustalarının/efendilerinin tek bir işareti veya komutu ile her türlü şiddet eylemini yapabilecek bir kimliğe bürünmektedirler.

Eleman teminindeki temel hedefini, üstlerinin emirlerini yerine getirmeye hazır çok sayıda ve disiplinli bir insan grubu oluşturmak olarak belirleyen örgütte, elemanlar özenle seçilmekte ve birbirlerine "iyi kuzenler" (*good cousins*) olarak hitap etmektedirler. Keza, örgüt içerisinde hiyerarşik bir kademelenme mevcuttur. Örgütün kademeleri çok sayıda gizli hücrelerden oluşmakta ve örgüt elemanlarının isimleri kodlanmaktadır. Hücreler birbirini tanımamakta ancak entegre halde varlıklarını devam ettirebilmektedirler (Rath, 1964: 353-356). Örgüt içerisinde sürekli olarak kodlar, işaretler ve parolalar kullanılmakta ve hatta birbirlerine dokunma şekilleri ile karşılarındakilerin örgüt elemanı olup olmadığını anlayabilmektedirler (Bartholdy, 1821: 5, Shiver, 1964: 234). Bu kapsamda, birbirlerine çeşitli bağlarla entegre olmuş küçük, gizli hücrelerden oluşan, aynı zamanda da kademeler halinde hiyerarşik bir örgütlenmeye sahip oldukları söylenebilir.

[1]İtalyanca "*carbonari*" kelimesinin İngilizce karşılığı "*charcoal makers*" olup Türkçeye "kömürcüler" olarak çevrilebilir (https://www.britannica.com/topic/Carbonari, Erişim Tarihi: 23.10.2019).

Bu tip örgütler gizemlerini sadece kendilerine has örgüt içi iletişim ile sağlamamakta ayrıca dini/mistik inançlar örgütün ideolojik temelini oluşturarak buna katkıda bulunmaktadır. Bu kapsamda, örgütün kendine özgü özelliklerinden birisi de modern olarak nitelendirilebilecek devrimci hedeflerin içerisinde dini ritüeller barındıran gelenekselciliği güçlü bir şekilde barındırabilmesidir (Miller, 2003: 33). "Mesih" inancına sahip bu örgütte, tıpkı Hz. İsa gibi dünyada acı çeken, ancak öldükten sonra huzura kavuşacaklarını düşünen örgüt elemanları, örgütün dünyayı aydınlatmaya (*enlightment*) yönelik hizmet ettiğine inanmaktadırlar. Çünkü örgüt liderliğini, "Kâinatın Büyük Efendisi" (*Great Master of the Universe*) olarak algılamaktadırlar (Rath, 1964: 358).

Örgütün esasen, mevcut otoriteye paralel bir iktidar gibi hareket ettiğinden de bahsedilebilir. Bu paralel yapı bünyesinde, sözde hükümetin üçer yıllık görev süresi olan localar (*vendita*) ve bunların birbirinden ayrı başkanları bulunmaktadır. Birincisi yasama, ikincisi yürütme ve üçüncüsü de adli olmak üzere üç ayrı loca şeklindeki başkanlıkların sonuncusuna Yüksek Loca (*Alta Vendita*) denilmektedir. Bu localar da "*baracche*"[2] (baraka) adı verilen çeşitli sayılardaki alt bölümlerden oluşmaktadır (Bartholdy, 1821: 5-6).

Elemanların örgüte katılışları adeta dini bir tören gibidir ve mistik bir havada gerçekleştirilmektedir. Örgüte yeni katılacak kişiler ve diğer elemanlarla ilgili toplantılar için önceden belirlenmiş olan ormanlık alanlardaki gizli barakalarda buluşulmaktadır. Barakaları çevreleyen orman "İtalya" olarak betimlenmekte, içleri ise örgüt elemanlarının çalıştığı localar olarak kabul edilmektedir (Shiver, 1964: 235). Örgüte alınacak elemanın, locaya getirilmeden önce, ormanda belirlenmiş bir yerde kısa bir süre oturması, mistik bir "yansıma mağarası"nda (*grotto of reflection*) biraz zaman geçirmesi ve böylelikle kendisiyle yüzleşmesi istenmektedir (Rath, 1964: 357).

Mistik mağaradaki yüzleşmeden sonra, gözleri bağlı bir şekilde kendisinden sorumlu olan efendi/usta tarafından loca girişine getirilen kişi, burada adını, yaşını, ikametgâhını, dinini ve mesleğini söylemektedir. Ormandan topladığı odun, yaprak

[2] Tekil hali *baracca* olan İtalyanca kelimenin çoğulu *baracche* olmakla birlikte Türkçe karşılığı kütüklerden yapılmış küçük ev, kulübe veya baraka olarak ifade edilebilir (https://en.wiktionary.org/wiki/baracca, Erişim Tarihi: 23.10.2019) Bu kapsamda, *Carbonari* üyelerinin buluşmak için önceden planladıkları gizli yerler olarak da belirtilebilir. Çalışmada "baraka" ifadesinin kullanılması tercih edilmiştir.

ve toprak ile beraber iyi kuzenlere; inanç, umut ve yardım[3] getireceğine ve tutkularına ket vurup örgüt tarafından verilecek tüm görevleri yaparak hiçbir koşulda ihanet etmeyeceğine dair yemin ettikten sonra içeri girmektedir. Yeminini bozduğu takdirde lanetlenmiş olarak atfedileceğini de kabul etmektedir (Rath, 1964: 357).

Örgüt, eleman temininden sonra, örgüt içi radikalleşmeyi amaçlamakta ve insani fikirler, dürüstlük, onur, yardımseverlik ile hukuk ve düzene saygı gibi "maske" kavramları ön plana çıkarmaktadır. Elemanlar, bu kavramlar çerçevesinde hareket ettiğini veya hizmet ettiğini düşünmektedir. Örgüte sadakat ve adanmışlık oldukça önemlidir (Shiver, 1964: 235). İnsanları "iyi bir Hristiyan haline getirmekten ziyade Hristiyanları iyi birer *Carbonari* haline getirmek" amaçlanmaktadır (Rath, 1964: 357-358).

Finansal boyutta; elemanlarına uyguladığı para cezaları, örgüte giriş parası, elemanların aylık kazançlarından alınan aidatlar ve diğer katkılarla oldukça yüksek bir kaynak oluşturmuşlardır (Rath, 1964: 358). Örgütün eleman sayısı da o zamanki şartlara göre azımsanmayacak boyuttadır. 1810'larda 200.000 civarında elemanı olduğu değerlendirilmektedir (Shiver, 1964: 235). 1820'lere doğru etkinliğini iyice artıran örgütün elemanları arasında soylular, subaylar, küçük toprak sahipleri, devlet memurları ve hatta din adamları da bulunmaktadır. İtalya'nın yanı sıra İsviçre, Fransa, İspanya ve Almanya'da da faaliyetlerini yürüttüğü bilinmektedir (Shiver, 1964: 238-241).

Özellikle 1820 ve 1821'de *Carbonari*'nin desteğiyle önce Napoli Kralı Ferdinand'a karşı başlatılan ayaklanma esnasında bir takım siyasi hedeflere ulaşılmış, akabinde bu başarıdan cesaretle diğer İtalyan Krallıklarında da benzer faaliyetlere girişilmiştir. 1821'de, Avusturya ordusu bu şiddet eylemlerini bastırmak üzere İtalya'ya girmiş ve örgütün etkinliğini kırmıştır (Frost, 1876b: 1-2). Ancak örgüt tamamen yok olmamış, "uygun zamana kadar bekleyerek" 1830'da Fransa'daki Temmuz Devrimi'nde rol almış ve benzer şiddet eylemlerini 1831'de İtalya'da gerçekleştirmeye çalışmıştır. Burada başarısız olarak etkinliğini büyük ölçüde yitirmiştir (Frost, 1876b: 30-40). Eylemleri genel olarak, mevcut rejimi değiştirmek maksadıyla komplolar, suikastlar düzenlemek ve isyan, ayaklanma gibi halk hareketlerini yönetip yönlendirmek olarak özetlenebilir. (Frost, 1876a: 244). Tüm bunlar değerlendirildiğinde *Carbonari* örgütünün ciddi anlamda terör

[3] İnanç-Umut-Yardım (*Faith-Hope-Charity*) üçlemesi örgüt için kutsal sayılan sözlerdir (Frost, 1876: 217).

taktikleri geliştirdiği görülmektedir. Her an hazır durumda bulunan örgüt elemanlarının en çok kullandıkları silah hançer olmakla birlikte ani gelişen bir durumda kullanmak maksadıyla yanlarında zehirli malzemeler bulundurdukları da bilinmektedir (Miller, 2003: 33).

Sonuçta, *Carbonari* örgütünün özellikle organizasyon yapısı ve adeta bir yeraltı teşkilatı gibi gizliliği esas alarak hareket etmesi ile kendisinden sonraki örgütleri etkilediği söylenebilir. Öyle ki; 1814'den itibaren faaliyet gösteren *Filiki Eterya* (*Philiki Etairia/*Dostlar Cemiyeti), 1880'lerden itibaren ortaya çıkan *Naradnoya Volya* (Halkın Arzusu), 19. yüzyıl sonlarında ortaya çıkan İç Makedonya Devrimci Örgütü (*Internal Macedonian Revolutionary Organization/IMRO*) ile Armenekan, Hınçak ve Taşnak örgütleri yeraltı teşkilatı olarak örgütlenmiş ve gerçek faaliyetlerini örtmek maksadıyla gizliliğe önem vermişlerdir.

Araştırmacılar 19. yüzyıl ile ilgili çalışmalarda, "modern" terimini, herhangi bir kavramda olduğu gibi terörizmin başına da eklemekte bir sorun görmemektedirler. Bunlardan biri olan Rapoport, "Modern Terörizmin Dört Dalgası" adlı çalışmasında, aynı dönemi modern terörizmin başlangıcı olarak ele almıştır. (Rapoport, 2004: 46). Buna göre, dört ardışık ve üst üste çakışan modern terörizm dalgası 1880'de başlamakta ve her biri ayrı karakter, ideoloji, amaç ve yöntemler barındırarak günümüze kadar devam etmektedir (Rapoport, 2004: 46-73).

Çoğunlukla anarşist ideoloji motivasyonlu 1880'lerde başlayan terörizm; siyasal ve toplumsal değişikliğin, geleneksel devrimle, yazıyla veya söylemlerle değil, şiddet eylemleri vasıtasıyla mümkün olabileceği düşüncesi ile ortaya çıkmıştır. Bu düşünce akımı özellikle Rusya'da alevlenmiş ve "*Narodnaya Volya*"[4] olarak bilinen örgütün doğmasına yol açmıştır (Laqueur, 2002: 11). Aslında, anarşizm felsefesinde insan hayatına verilen önem, insanın kutsanması ve insanın zarar görmesinin yadsınması söz konusu edilmesine rağmen bir yandan da anarşist amaçlar için uygulanan şiddetin meşrulaştırılması ve insanların öldürülmesi dikkat çekici bir çelişkidir (Novak, 1954: 176-181). Bu çelişkinin, *Carbonari* örgütünün kullandığı "maske" kavramlar ile benzerlik gösterdiği de söylenebilir. Diğer taraftan, örgütün saldırılarını, askeri hedeflerden ziyade devleti/otoriteyi temsil eden sembolik hedeflere[5] yöneltmesi ve kendilerini "terörist" olarak adlandırmaları

[4] Örgüt faaliyetlerini 1878-1881 yılları arasında gerçekleştirmiştir (Laqueur, 2002: 11).

[5] Bu kapsamda gerçekleştirilen önemli eylemlere örnek olarak; ABD Başkanı Garfield (1881) ve Mckinley (1901), Fransa Cumhurbaşkanı Sadi Carnot (1984), İspanya Başbakanı Antonio Canovas

önem arz etmektedir. Uyguladıkları eylem türleri genellikle soygun ve suikasttır. Bu dönem ayrıca anarşist terör hareketlerinin özellikle Avrupa'da ve ABD'de yoğunlaştığı bir dönemdir (Laqueur, 2002: 14). Böylelikle sınır aşan bir hal aldıkları görülmektedir. Bu hareketler tarafından ulaşılması arzulanan siyasi hedef doğrultusunda uygulanan temel stratejiler ise; kitlelerin (halkın) dikkatini çekmek, siyasi tansiyonu yükseltmek ve devletin yasal çerçeve dışına çıkarak mukavemet göstermesini sağlamak olarak özetlenebilir.

19. yüzyıl sonları ve 20. yüzyıl başlarındaki örgütlerde, terörist kavramının bir çeşit kahramanlığı çağrıştırdığı, çoğu örgütün kendisini terörist olarak tanımlarken bundan övünç duyduğu da bilinmelidir. Bunlar; kural tanımayan, asimetrik yapıda olan ve "savaştıkları" sistemden herhangi bir onama ya da meşru görülme beklentisi içinde olmayan özelliklere sahiptirler (Thorup, 2008: 335). Göreli yoksunluk[6] durumunda bir değişiklik yaratmak, bir intikam duygusunu ifade etmek, bir çeşit baskıyı protesto etmek ve anarşizmin eylemle propagandasını yapmak amaçlı "bireysel terörizm" türemiştir (Novak, 1954: 177). Bireysel terörizmde en büyük eylem olarak kabul edilen "kendi hayatını bir inanç uğruna feda etme" kutsallaştırılmıştır. Öyle ki, terörist örgütlerin manifestoları ve yayınları üzerine yapılan bir araştırmada belirtildiği üzere; dönemin önde gelen Rus anarşistlerinden biri olan Mikhail Bakunin, "Devrim, Terörizm, Eşkıyalık" ismiyle 1869'da yayınladığı makalesinde fikirlerini şu şekilde belirtmektedir: "*Buna terörizm diyeceklerdir! Ses getiren bazı takma isimler de koyacaklardır! Pekâlâ, bizim için hepsi aynıdır. Biz, onların fikirlerini umursamıyoruz.*" (Laqueur, 2004: 70).

Yine bu dönemde ortaya çıkan ve liderleri *Luigi Galleani*'nin ismiyle anılan "Galleaniciler" anarşist terörizme bir başka örnektir. Bir karizmatik liderin önderliğinde fakat merkezi olmayan bir örgütlenme oluşturmuşlardır. Galleani, aşırılıkçı ve propaganda içeren yazı ve söylemleri ile sınır aşan bir boyutta destek sağlamış böylelikle de eylemlerin faaliyet alanı genişlemiştir. Bombalı araç saldırısı ve adrese bombalı paket göndermek gibi eylemlerle o döneme göre yenilikçi yöntemler denemişlerdir. Eylemlerindeki yenilikçilik, şiddetin boyutunun

(1897), Avusturya Kraliçesi, Elizabeth (1898), İtalya Kralı Umberto (1900), Rus Çarı II. Aleksandr (1881) suikastleri verilebilir.

[6] Göreli yoksunluk teorisi; kişinin kendi statüsüne ilişkin yargıların neticesinde ortaya çıkan olumsuz etkinin sadece kişinin nesnel statüsünün bir işlevi olmadığına odaklanmaktadır. Bunun yerine, kızgınlık, öfke, memnuniyetsizlik ve diğer yoksunluk ile ilgili duygular, kişinin statüsünün öznel değerlendirmesiyle değişebildiği savunulmaktadır (Bernstein ve Crosby, 1980: 442).

da gittikçe artmasına sebep olmuştur. O zamanın koşullarına göre medyayı etkin olarak kullanmış, mesajlarını geniş çevrelere iletebilmeyi başarmış ve uyguladıkları siyasi şiddet eylemlerini ise ideolojileri uğruna verdikleri "savaş" olarak nitelemişlerdir (Simon, 2008: 211).

Genel olarak değerlendirildiğinde, belirtilen dönem içerisinde FETÖ'nün; sahip olduğu mistik özellikler, organizasyon yapısındaki gizlilik ve hücreler halinde kademelenme, kodlamalar, usta/çırak ilişkisini anımsatan abi/abla yapısı, örgüte bağlılık ve adanmışlık, paralel bir otorite oluşturma ve yeraltı teşkilatı nitelikleriyle uygun zamanı bekleyerek mevcut otoriteye karşı girişilen şiddet eylemleri kapsamında *Carbonari* örgütü ile benzerlikler gösterdiği görülmemtedir. Diğer taraftan; insani değerler, insanlara hizmet etme gibi maske kavramlar, medyayı etkin kullanma ve propaganda ile anarşist örgütlerle de benzerlik gösterdiği söylenebilir.

1.2. Etnik Ayrılıkçılardan Küresel Örgütlere

İlerleyen zamanda yeni bir tip olarak bazı etnik ayrılıkçı terörist örgütler görülmüştür. Erickson'a göre (2013: 19) bu durum; nihilizmin ve anarşizmin, radikalleşmiş devrimci gruplara girmesinin bir sonucu olan "modern" gerillacılık olarak adlandırılabilecek bir olgunun yükseliş zamanı ile çakışmıştır. Örneğin, Osmanlı Makedonyası ve Anadolu'nun yoğun Ermeni nüfuslu doğu illerinde, bu bölgeleri kontrol altına almak için Osmanlılarla ve/veya kendi aralarında çatışan bir dizi grup ortaya çıkmıştır (Erickson, 2013: 9).

Özellikle gerilla teknik ve yöntemlerini kullanan bu örgütler Osmanlılar tarafından "komite/komita", örgüt elemanları da "komitacı/komiteci" olarak bilinmekteydiler (Erickson, 2013: 9-10). Keza; Ermeni Armenekan, Hınçak ve Taşnak örgütleri ile *IMRO* bu türdendir. Bu örgütlerin motivasyon kaynağı, Osmanlı'nın oldukça zayıflaması ve ulusal kimliklerin ön plana çıkarılmasıdır (Erickson, 2013: 10). Önce yeraltı teşkilatı şeklinde ortaya çıkan ve sivil propagandacı bir toplum halini alan bu örgütler, birkaç yıl içerisinde askeri bir harekete dönüşmüş ve hem sistematik teröre hem de kitlesel bir ayaklanmaya hazırlanmışlardır (Laqueur, 2002: 13). Burada örnek olarak gösterilebilecek bir diğer örgüt de İrlanda Cumhuriyetçi Ordusu (*Irish Republican Army/IRA*)'dır. Gerilla taktikleri, bombalama, suikast ve silahlı saldırı yöntemleriyle bağımsız bir devlet kurma hedefini güden örgüt, etnik ayrılıkçı motivasyonla bu dönemde faaliyetlerine başlamıştır (Kalyvas, 2003: 481).

Birinci Dünya Savaşı'nın bitişinden Vietnam Savaşına kadar geçen sürede ise self-determinasyon kavramı ve sömürge karşıtı ideolojinin baskınlığı görülmektedir (Rapoport, 2001: 423). Dönemin özelliklerinden birisi de terörizm kavramına kötü, aşağılayıcı bir anlam yüklenmesidir. Kendisini terörist olarak tanımlayan son örgüt LEHİ (*Lohamei Herut Yisrael*)'dir. Kimi zaman, bu dönemdeki örgütlerin "özgürlük savaşçısı", "partizan" gibi adlarla anıldığı da bilinmektedir (Thorup, 2008: 342-344). İrlanda, İsrail, Kıbrıs, Yemen ve Cezayir bu dönemde sömürge olmaktan çıkmıştır. Cezayir'in bağımsızlığını kazanmasında etkili olan FLN (*Front de Libération Nationale*) bu dönemde öne çıkan örgütlerden biridir.

FLN, birkaç lider ile daha alt birimler[7] ve hücrelerden oluşan bir organizasyon yapısı benimsemiş ve önceliğini örgütün hayatta kalması olarak belirlemiştir. Hücrelerin birbirini tanımaması ve gizliliğe önem vermeleri sonucu tespit, teşhis edilmeleri ve yakalanmalarını zorlaştırmıştır. Bu kapsamda, eylemlerine başlamak için belli bir seviyeye ulaşmayı beklemiş ve gayretlerini Fransızlardan önce Cezayir halkına yöneltmiştir (Crenshaw, 1972: 386). Bir ayaklanma halini alacak olan bu ortam içerisinde genel olarak "şehir savaşı"[8] stratejisinin uygulandığı söylenebilir. Ayrıca, sorunun Birleşmiş Milletlere taşınması suretiyle, yerel olarak başlayan bir çatışmanın uluslararası bir sorun haline getirilmesi, bu süreçte örgütün şiddet hareketlerini durdurması ile de hem dış destek ve sempati kazanmaya hem de meşruiyet sağlamaya çalışılması önemlidir (Hoffman, 2006: 53). Buna ek olarak, örgütün gerek nikâh kıyma ve çeşitli sosyal kurallar koyma gerekse de kendi mahkemelerini oluşturma ve kurallara uymayanları cezalandırma vb. faaliyetleri ile mevcut otorite karşısında paralel bir devlet gibi hareket etmesi söz konusudur (Crenshaw, 1972: 390).

FLN örneğinde de görüldüğü üzere, terörist örgütlerin bu dönemde genel olarak, sembolik yapılar ve şahıslardan ziyade güvenlik birimlerini (polis-asker) hedef aldıkları görülmektedir. Halkın politik tutum ve davranışlarını değiştirmek en öncelikli amaç olmuştur (Crenshaw, 1972: 385). Kırsaldan şehirlere doğru kayan şiddet ortamında terörist örgütler çoğunlukla gerilla yöntemlerini uygulamışlar ve hücresel yapılar oluşturmuşlardır. Organizasyon yapıları daha çok hiyerarşik

[7] FLN organizasyon yapısı askeri ve politik kanat olarak ikiye ayrılmıştır. Askeri kanat *"The Armée de Libération Nationale (ALN*), politik kanat ise *The Comité Révolution d'Unité ed d'Action (CRUA)* olarak adlandırılmıştır (Davis, 2007: 6)

[8] Şehir Savaşı stratejisi ile ilgili detaylı bilgi için bakınız: Carlos Marighella (2002). *Minimanual of the Urban Guerrilla*. Montreal, Abraham Guillen Press .

modeli benimsediklerini göstermektedir. Crenshaw'a göre (1972: 387), terörizm için temel gereksinimler olarak ifade edilebilecek olan gizlilik, disiplin ve organizasyon, tıpkı FETÖ'de olduğu gibi bu örgütlerde de bariz olarak görülmektedir.

1960'lardan itibaren terörist örgütler artık devrimci dünya görüşü ile ayrılıkçı amaçları birbirine bağlamıştır. İtici güç sosyalist ideoloji iken, temel motivasyon kaynağı ise yüksek dozda ayrılıkçı/milliyetçi duygulardır (Boot, 2014: 355) Bu sebeple bu döneme "Yeni Sol dalga" da denilmektedir (Rapoport, 2002: 4). Mao, Ho Chi Minh, Fidel Castro ve Che Guevara'yı kendilerine örnek alan bu gruplar, kırsal alanlarda gerilla yöntemleri veya şehirlerde terör eylemleri, bazen de her ikisini aynı anda uygulamaya çalışmışlardır (Boot, 2014: 355). Hatta, özellikle gençlerden/öğrencilerden oluşan bazı terörist örgütler, üçüncü dünya ülkelerinin savunuculuğunu dahi üstlenmekten geri kalmamışlardır.

Diğer taraftan, bu dönemde uçak kaçırma adeta bir simge haline gelmiştir. Buna ek olarak, banka soygunu, kundaklama, bombalama, adam kaçırma, suikast ön plana çıkmaktadır. Ayrıca, Alman Kızıl Ordu Fraksiyonu, İtalyan Kızıl Tugayları ve Japon Kızıl Ordusu ve DHKP-C gibi örgütlerin "iyi eğitimli" lider kadroya ve az sayıda elemana sahip olmaları da dikkat çekmektedir. ETA (*Euskadi Ta Askatasuna*) ve 1969 yılında ikiye ayrılan IRA'dan türeyen PIRA örneklerinde ise etnik ayrılıkçı amaçlar ile sosyalizmin birleştiği görülmektedir. Bu örgütlerin hiyerarşik yapıda olduğu ve doğrudan halkı hedef almadığı ancak şehir gerillası teknikleri uyguladığı bilinmektedir (Price, 1977: 59-61). ETA ve PIRA yöntemsel olarak şehir gerillacılığı ile faaliyetlerine başlamışken bunlara benzer bir örgüt olan PKK'da ise öncelik kır gerillacılığındadır (Demir, 2017: 357-363).

Bir başka örgüt olan Filistin Kurtuluş Örgütü (*PLO*, FKÖ) ise bu dönemde adeta bir şemsiye örgüt olarak faaliyet göstermiştir. Bu durum, anarşist örgütlere benzer şekilde terörizmin küresel bir nitelik alması sonucunu ortaya çıkarmıştır 1980'li yıllara gelindiğinde ise tarihi kırılma anları olarak beliren iki önemli olay, İran İslam Devrimi ve Sovyetlerin Afganistan'ı işgali, terörizme yeni bir ortam sağlamıştır (Rapoport, 2002: 423).

Bu yeni ortamda, çeşitli dini inançları motivasyon unsuru olarak benimseyen örgütler dikkat çekmektedir. Ayrıca, hangi din olursa olsun, dinin bir ideoloji olarak farklı terörist örgütler tarafından benimsenmesi sebebiyle, dini söylemle açıklanan terörizm farklı dinlerde benzer özellikler gösterebilmektedir (Avcı, 2011: 89).

Bir örnek olarak, 1987'de dini bir örgüt olarak ortaya çıkan *Aum Shinrikyo* başlangıçta; yoga, manevi rehberlik ve mucize gibi kavramları yansıtmıştır. Örgüt lideri kendisini, "yüce gerçeği edinen tek kişi" olarak tanımlamış, 1991'de kendisine doğaüstü güçler atfederek "Mesih" olarak ilan etmiştir (Box ve McCormack, 2004: 93-94).

Örgütün çokça bilinen bir eylemi, 1995 yılında Tokyo metrosunda sarin gazı saldırısında bulunulmasıdır. Genel olarak, faaliyetleri dünya çapında olmakla beraber; Budizm, Hristiyanlık, Şamanizm, Hinduizm ile bazı diğer inançlar da dahil olmak üzere farklı motivasyon kaynaklarından beslenerek şekillenmiştir. Bir çalışmaya göre; 1995'te dünya genelindeki örgüt üyeliğinin muhtemelen 20.000 ila 40.000 kişi olduğu tahmin edilmiş, aynı dönemde örgütün yaklaşık 1,5 milyar dolarlık bir kaynağı olduğu ifade edilmiştir (Olson, 1999: 514). Finans kaynakları; bağışlar, gelirinin yüzde onunu vergi olarak verme (*tithing*), dini gereçlerin pazarlanması, videokaset ve kitap satışlarıdır. Örgütün öğretilerinin sunulduğu çeşitli oturumlar, seminerler ve eğitim kursları düzenlemiş ve bunlara katılmak isteyeler yüklü miktarda para ödemişlerdir. *Aum Shinrikyo* ayrıca, bir dizi ticari işletmeye, hatta bilgisayar üreten bir şirkete de sahiptir (Olson, 1999: 515).

Bir kült olarak da nitelenen bu örgüt, eleman temininde genç kitlelere yönelmiş (Box ve McCormack, 2004: 93), Japonya'nın en parlak gençleri, önde gelen üyeleri haline gelmiştir. Bilim adamları, bilgisayar uzmanları, avukatlar, mühendisler ve diğer yüksek eğitimli kişilerin örgüte üye oldukları bilinmektedir (Hudson, 1999: 133). *Aum Shinrikyo,* elemanların örgütten kopmalarını engellemek maksadıyla, çeşitli küçük örgüt içi kural ihlallerinde dahi acımasız fiziksel ve psikolojik ceza biçimleri de dâhil olmak üzere, dünya çapında kültlere özgü zihin kontrol tekniklerini de kullanmıştır. Örgüte yeni katılan elemanlar, dış dünyayla olan tüm ilişkilerini sonlandırmak ve tüm mal varlıklarını bağışlamak zorunda bırakılmışlardır (Hudson, 1999: 136).

Buraya kadarki bölümde yer alan vaka analizleri ve yapılan karşılaştırmalar neticesinde ise FETÖ'nün; hücreler halinde organize olma, paralel devlet yapısı oluşturma ve ulusal/uluslararası meşruiyet kazanabilme maksatlı faaliyetleriyle *FLN* örgütüyle benzerlikler gösterdiği söylenebilir. Son olarak zihin kontrolü ve beyin yıkama faaliyetleri, Mesih inancı, finans kaynakları ve geniş çaplı ticaret ağı, eleman temininde parlak gençlere yönelmesi, öğretilerinin sunulduğu sohbet toplantıları ve eğitim faaliyetleri, sözde yüce değerlerden beslenen motivasyonu ve

kült grup özellikleri ile de *Aum Shinrikyo* örgütüyle benzerlikler gösterdiği sonucuna varılmıştır.

Belirtilen benzerlikler haricinde FETÖ'nün kendine özgü birtakım özellikleri de bulunmaktadır. Bu özellikler belirtilmeden önce, bütünün parçalara ayrılarak analiz edilmesi maksadıyla tümevarım yöntemi benimsenmiştir. Bu kapsamda, bir sonraki bölümde, terörist örgütlerin nihai hedefe ulaşmak maksadıyla benimsedikleri organizasyon modelleri, stratejiler ve sahip olunan motivasyonlar ile ilgili yazında sıklıkla karşılaşılan teorik yaklaşımlar ayrı ayrı ele alınacaktır.

2. TERÖRİST ÖRGÜTLERİN ORGANİZASYON MODELLERİ, STRATEJİLERİ VE MOTİVASYONLARI İLE İLGİLİ TEORİK ÇERÇEVE

Tarihsel perspektifte incelenen modern terörizm ve bahsedilen terörist örgüt örneklerinden sonra, alanyazında terörist örgütlerin organizasyon yapısı, stratejileri ve motivasyonları ile ilgili oluşturulan teorik çerçeveden bahsetmek son bölümde incelenecek olan FETÖ'nün dinamiklerini açıklamada faydalı olacaktır.

2.1. Organizasyon Modelleri

Terörist örgütler bir organizasyon modelini benimseyip faaliyetlerini yürütürler. Organizasyonel modeller, bu örgütlerin analiz edilmesi ve anlaşılabilmesi için önemli ve açıklayıcı bir karakteristik ortaya koymaktadır. Terörist örgütlerin organizasyon modeli genel olarak hiyerarşik ve ağ (*network*) olarak ikiye ayrılabilir. Ayrıca, ağ modelini; yıldız (*hub-spoke*), zincir (*market, chain*) ve dağıtık (*all-channel*) olarak ayırmak mümkündür (Kilbert, 2012: 813, Arquilla ve Ronfeldt, 2001: 8). Ağ modelin farklı biçimlerinden olan yıldız modelde hiyerarşik olmayan bir düğüme bağlılık mevcuttur. Hücreler bu düğümler vasıtasıyla iletişim veya koordinasyon sağlamaktadır. Bu modelde örgütler bir lidere sahip olmakla beraber örgüt içi fonksiyonel farklılaşma da mevcuttur. Zincir modelde ise nispeten küçük çaplı bir örgütlenme vardır. Elle tutulur bir liderlik, merkezi bir komuta kontrol yapısı ve fonksiyonel farklılaşma bulunmamaktadır. Son olarak dağıtık modelde hızlı, yoğun ve çok yönlü iletişim ağı mevcuttur (Kilbert, 2012: 813-814). Dağıtık modeldeki bu yapı iletişim ve bilgi aktarımındaki teknolojik gelişmelerin bir sonucu olarak görülmektedir (Arquilla ve Ronfeldt, 1999: 193). Bir lider olmasına rağmen hiyerarşi çok zayıftır ve merkezi komuta kontrol sistemi ile fonksiyonel farklılaşma bulunmamaktadır (Kilbert, 2012: 814).

Tablo 1'de, terörist örgütlerdeki organizasyon modelleri; liderlik, fonksiyonel farklılaşma ve merkezi komuta-kontrol özelliklerine göre tasnif edilmiştir. Liderlik; örgütte bir lider ve/veya lider kadronun olmasını, fonksiyonel farklılaşma; örgüt içerisinde farklı boyut ve seviyelerde uzmanlaşmanın mevcudiyetini ve merkezi komuta kontrol ise örgütün eylem ve faaliyetlerinin merkezden verilen talimatlar çerçevesinde yapıldığını ifade etmektedir.

Tablo 1. Terörist örgütlerde organizasyon modelleri (Kilbert, 2012: 819)

Organizasyon Modeli	Liderlik	Fonksiyonel Farklılaşma	Merkezi Komuta-Kontrol
Zincir	-	-	-
Dağıtık	+	-	-
Merkezi/Yıldız	+	+	-
Hiyerarşik	+	+	+

Hiyerarşik modelde, lider veya lider kadro hedefleri belirler ve net bir şekilde belirlenmiş politik, sosyal ve ekonomik hedefler bulunmaktadır (Kilbert, 2012: 813). En küçük birimleri olan hücreler belirlenen hedefler doğrultusunda eylem yaparlar. Eylem ile hedef arasında doğrudan bir ilişki olması gerekir ki aksi takdirde istenilen etkiyi gerçekleştiremeyen hatta örgütün kendisine zarar verebilecek bir eylem yapılmış olabilir. Net bir komuta-kontrol sistemi oluşturularak örgüt elemanları bu sisteme uymak için zorlanır ve örgüt elemanlarına çeşitli sorumluluklar verilerek bu sorumlulukların hesabının verilmesi istenir (Heger, Jung ve Wong, 2012: 747).

Hiyerarşik modelin bir diğer özelliği ise fonksiyonel farklılaşmadır. Örgüt elemanları istihbarat, propaganda, finans, medya vb. çeşitli alanlarda uzmanlaştırılır veya bu alanlardaki uzmanlardan örgüt elemanı temin edilmeye çalışılır (Heger, Jung ve Wong, 2012: 749). Hiyerarşik modeller daha kısa zamanda hızlı sonuç almak için ağ modellere göre daha elverişli bir yapı sunar. Özellikle

sömürge karşıtı, etnik ayrılıkçı ve 1960 sonrası ortaya çıkan sol ideolojiye sahip örgütlere benzer şekilde FETÖ'nün de hiyerarşik modeli benimsediği görülmektedir. Diğer taraftan lider/lider kadronun ele geçirilmesi veya etkisiz hale getirilmesi bu modeli benimseyen örgütler için bir zayıflık olarak görülebilir. Ayrıca çok fazla kollara ve alt yapılara ayrılan böyle bir modelin hiyerarşik yapısını devamlılığını sağlamanın zorlaşacağı da söylenebilir (Heger, Jung ve Wong, 2012: 748).

Ağ modelde ise bir lider olabilir veya olmayabilir. Birimler arasında net ve sınırları çizilmiş bir emir-komuta zinciri yoktur. Ancak gerektiğinde hücreler arasında koordinasyonu sağlayan kişiler olabilir. Hücreler zorunlu olarak ortak bir eyleme dâhil olmadıkça birbirleriyle görüşmez hatta birbirlerini tanımazlar. Ağ örgüt modelinde hedefler ve amaçlar elemanlara genel olarak sunulur. Hücrelerin veya elemanların esneklik ve inisiyatif kullanarak hareket etmeleri beklenir. Böylelikle herhangi bir eylem sonucunda, bir hiyerarşi ve sorumluluk olmadığı için, eğer varsa lider sorumluluktan veya hesap vermekten kaçınabilir.

Bir hiyerarşik modele sahip organizasyon, ağ modeli bir organizasyona göre bir örgütün hedeflerini daha açık şekilde analiz edilebilmesini sağlamaktadır (Dishman, 2016; s.137). Hiyerarşik organizasyonlar, lider/lider kadro vasıtasıyla koyulan kurallar ve çizilen sınırlar dâhilinde amaç ve misyonlarını sürdürmektedirler. Buna karşılık, ağ modelde ise farklı yapıları aynı anda benimseyebilmekte ve çok sayıda hatta birbiriyle çelişen hedefler güdebilmektedirler (Dishman, 2016: 137). Böylelikle ağ model organizasyona sahip örgütler analizcilerin çalışmalarını zorlaştırmaktadır. Dini ideolojiye sahip terörist örgütlerin daha çok ağ modeli benimsedikleri söylenebilir. FETÖ ise hem sahip olduğu piramit kademelenme ile hiyerarşik modelin hem de oluşturduğu hücresel yapı ile ağ modelin özelliklerini bir arada taşımaktadır.

2.2. Motivasyon Kaynakları

Terörist örgütlerin dinamiklerini incelemenin bir yolu da eylemlerinin altında yatan motivasyonlara odaklanmaktır. Bu kapsamda, motivasyonları birbirinden ayırıp sınıflandırmak, yapılacak analizlerde fayda sağlayacaktır.

Paul Wilkinson (2000: 19), terörist örgütlerin motivasyonlarını incelediği bir çalışmasında terörizmin tipini yukarıdan aşağıya ve aşağıdan yukarıya olarak ayırmıştır. Yukarıdan aşağıya terörizm aslında devlet tarafından, devlet eliyle yapılan terörist eylemlerdir (Wilkinson, 2000: 19-20). Aşağıdan yukarıya terörizm

ise devrimci amaçlarla yapılan terörist eylemlerdir ve milliyetçilik, bölücülük (ayrılıkçılık), ırkçılık, yasa düzeni tanımadan kendi çıkarına göre istediklerini zorla alma, aşırı sol ideoloji, dini köktencilik (*fundamentalism*), milenyumculuk (*millennialism/ millenarianism*) ve tek bir kamu meselesi (örneğin; hayvan haklarını savunma, kürtaj karşıtı eylemler) gibi motivasyon kaynaklarını barındırmaktadır. Terörist örgütler bu motivasyon kaynaklarından sadece bir tanesine sahip olabileceği gibi aynı anda birkaç tanesini de bünyesinde barındırabilmektedir (Wilkinson, 2000: 20).

Başka bir çalışmaya göre terörist örgütlerin motivasyonlarını dörde ayırmak mümkündür. Bunlar; sol, sağ, etnik milliyetçi/ayrılıkçı ve kutsal olarak sınıflandırılmıştır (Cronin, 2003: 39). Sol motivasyon komünizmden, sağ motivasyon faşizmden, etnik milliyetçi/ayrılıkçı motivasyon sömürge karşıtlığından ve kutsal motivasyon ise dini inançlardan beslenmektedir. Ancak terörist örgütlerin, belirtilen sınıflandırmadaki motivasyonların bir veya birkaçını aynı anda benimseyebileceğinin de altı çizilmektedir (Cronin, 2003: 39).

Diğer taraftan, ABD Eğitim ve Doktrin Komutanlığı (*TRADOC*)'nın 2007 yılında yayımladığı "21. Yüzyılda Terörizm için Askeri Rehber" isimli çalışmada, terörist örgütlerin motivasyonları ayrılıkçı, etnik-merkezli, milliyetçi ve devrimci olarak dörde ayrılmıştır (TRADOC U.S. Army, 2007: 2-5).

Crenshaw (2006: 57)'a göre ise, terörist örgütlerin motivasyonları tekdüze ve basit değil, birbirinden farklı ve karmaşıktır. Birey ve grup arasındaki ilişki, aşırılıkçılığı destekleyen inanç sistemi, şiddete yol açan dinamik süreçler, din ve siyaset arasındaki bağlantılar ve kimliklerin rolü birer motivasyon kaynağı olarak ortaya çıkabilmektedir.

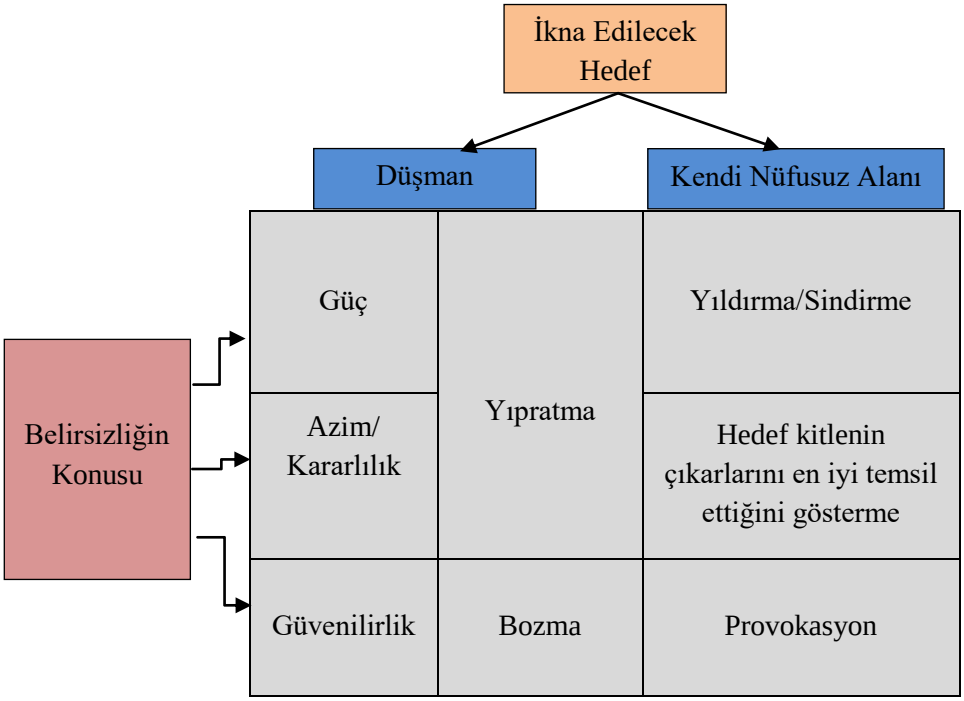
FETÖ'nün motivasyonunun ise özellikle Crenshaw (2006: 57)'un belirttiği kategorilerin tamamından beslendiği söylenebilir. Bu kapsamda, FETÖ'nün motivasyonu başlı başına diğer örgütlerden farklı ve karmaşık bir yapıdadır denilebilir. Bu yapı son bölümde ifade edilecektir. Genel olarak yukarıda bahsedilen kavramlar çerçevesinde motive olan terörist örgütler ise hedeflerine ulaşmak için doğal olarak bazı stratejiler geliştirmiş ve uygulamışlardır.

2.3. Stratejiler

Terörist örgütler siyasal saik ile hareket ederler. Şiddet eylemleri ile de nihai hedeflerine ulaşmak isterler. Hedefe ulaşmak için uyguladıkları stratejiler ise çok çeşitlidir. Örneğin, politik davranışı etkilemeyi hedefleyen örgütler, kendi

taleplerini kabul ettirmek için zorlama; otoritenin aşırı tepki vermesi için provoke etme; çatışma ortamı oluşturma, şiddeti övme ve tırmandırma; politik veya dini bir sebep ilan ederek dikkat çekme; nefret ve intikam duygularını yayma ve kendine düşman gördüğü devleti, hükümeti veya kuruluşları zayıflatma stratejilerini uygulamaktadır (Wilkinson, 2000: 19). Fromkin (1975: 691)'e göre teröristlerin temel stratejisi mevcut otoritenin provoke edilmesidir. Kydd ve Walter (2006: 59-78) ise terörist örgütlerin stratejilerini beş başlık altında toplamıştır. Çizelge 1'de belirtildiği üzere bunlar; yıpratma, yıldırma, provoke etme, bozma (barışı sabote etme) ve hedef kitle üzerindeki faaliyetlerini artırma şeklindedir.

Çizelge 1. Terörist Örgütlerin Stratejileri (Kydd ve Walter, 2006: 59)



Yıpratma ve bozma stratejileri örgütün "düşman" olarak algıladığı kesime yönelik iken, provokasyon, yıldırma/sindirme ve hedef kitle üzerindeki faaliyetlerini artırma stratejileri ise nüfuz alanı olarak gördüğü kesime uygulanmaktadır.

FETÖ için de aynı stratejiler geçerlidir. Örgütün çeşitli fişlemelerle kendisinden olmayanları ayırıp adeta düşman olarak nitelendirdiği ve bunlara yönelik her türlü

yıpratıcı ve bozucu eylemlerde bulunduğu görülmektedir. Bunun en net örnekleri; çeşitli asılsız suçlamalar veya kumpaslarla kişilerin ve kuruluşların yıpratılması ile mevcut hükümete yönelik darbe girişiminde bulunularak halihazırdaki sistem ve otoritenin bozulmaya çalışılmasıdır. Diğer taraftan; halka yönelik sürekli olarak medya kitle iletişim araçlarıyla propaganda ve provokasyon faaliyetlerinde bulunulması, bir güç odağı gibi hareket edilerek çeşitli yöntemlerle tüm kesimleri yıldırma ve sindirme gayreti ve kendi elemanları veya sempatizanlarına yönelik her türlü maddi ve manevi çıkar sağlama vaatleri ise nüfuz alanındaki faaliyetleri kapsamındadır.

3. YENİ TİP BİR TERÖRİST ÖRGÜT: FETÖ

FETÖ'nün organizasyon modeli, motivasyonu ve stratejisi ile ilgili değerlendirmelerden önce tarihsel perspektif içerisinde örgütün gelişimi ile ilgili arka plana kısa ve öz biçimde değinmek faydalı olacaktır. Bu kapsamda, örgütün gelişiminin üç safhada incelenmesi mümkündür. Birinci safha; "Kuruluş, Temellenme ve Kadrolaşma (1966-1980)", ikinci safha; "Hem Devlette Hem de Toplumda Yayılma ve Her Alanda İktidarı Ele Geçirme (1980-1997)", üçüncü safha ise; Kadrolaşmanın Tamamlanması ve Nihai Hedef İçin Harekete Geçilmesi (1997-2016) olarak belirtilebilir (TBMM Raporu, 2017: 43-44).

Örgütün birinci safhada ön plana çıkan faaliyetleri; vaaz verme, sohbet toplantıları düzenleme vb. ile halka yakından temas etme ve halkı kazanmaya çalışma, komünizm karşıtı bir dernekte görev alarak[9] tanınırlığını artırma, dini bir cemaat şeklinde örgütlenme, ışık evleri kurma, ekonomik kaynak sağlamak için hayırsever kişileri istismar ederek yardım temin etme ve adeta bir yeraltı örgütü gibi büyük bir gizlilik içerisinde süreci işletmesidir (TBMM Raporu, 2017: 41-49).

İkinci safhada örgütün; Mesihlik/mehdilik ve olağanüstülük gibi kavramlar ile kültleştiği, ışık evlerinden okul ve dershanelere doğru bir açılımı gerçekleştirdiği, şirketleşme ve holdingleşme ile kurumsallaştığı, belirli bir plan dahilinde stratejik olarak gördüğü kamu kurumlarına sızarak kadrolaştığı, ulusal boyutta hoşgörülü, barışçıl ve devletçi görünümlü bir tutum belirlediği, uluslararası boyutta ise liberalizme uygun, modern ve farklı bir hoca profili belirleyerek kendisini ılımlı İslam'ın gülen yüzü olarak tanımladığı ve en nihayetinde, 1990'lı yılların ikinci yarısından itibaren hedef büyüterek yurtdışına açıldığı görülmektedir (TBMM Raporu, 2017: 53-58).

[9] Erzurum Komünizmle Mücadele Derneği (TBMM Raporu, 2017: 45).

Üçüncü safhada ise; ABD'ye yerleşme ve örgütü buradan yönetme, "dinler arası diyalog, evrensel insan hakları, medeniyetler buluşması, ılımlı İslam" söylemlerinin artık daha belirginleştiği evrensel/küresel ifadeler kullanma ve sonunda altın vuruş-kıyam-huruç anlayışıyla nihai hedefe ulaşmak için harekete geçildiği ifade edilebilir (TBMM Raporu, 2017: 58-65). Tüm safhalarda ortak noktalar olarak; her dönemde içinde bulunduğu sosyo-politik koşullara uyum sağlayabilmiş, güç dengelerini gözetip siyasetten uzak ve bağımsız gibi görünmüş ancak kendi ifadesiyle her zaman "tekme mesafesinde" durmuş, gizlilik, tedbir ve takiyyeye azami önem verilmiş, kuruluşundaki söylem ve tavırlarda değişikliğe gitmekten, gerektiğinde geri adım atmaktan çekinilmemiştir (TBMM Raporu, 2017: 41-65).

Genel olarak değerlendirildiğinde ise örgütün sol ideolojilerin hâkim olduğu dönem içerisinde (1960'lar) faaliyetlerine başladığı ve günümüze kadar faaliyetlerini devam ettirdiği unutulmamalıdır.

3.1. FETÖ'nün Organizasyon Modeli

FETÖ'nün organizasyon modeli incelendiğinde öncelikle, nihai hedefine ulaşmak için uzun zamana yayılan bir süreci benimsediği görülmektedir. Bu uzun süre içerisinde gitgide birbirinin içine geçen karmaşık legal ve illegal yapılanmalar oluşturulmuştur. En tepede; olağanüstü haller yaşamış, seçilmiş kişi, Mesih, mehdi vb. olduğuna inanılan ve uyarıları ile tavsiyeleri birinci derecede etkiye sahip olan bir liderin varlığı ön plana çıkmaktadır. Bu durum daha önce bahsedilen *Carbonari* ve kült örgüt olan *Aum Shinrikyo*'yu hatırlatmaktadır. *Carbonari* örgütündeki usta/efendi-çırak ilişkisinin FETÖ'deki abi/abla yapısıyla örtüştüğü de söylenebilir. Ayrıca uzun süreli planlanmış hedef ve liderin varlığı hiyerarşik örgütlenme modeline benzemekle beraber karmaşık yapılanmaların bulunması ise ağ modele uymaktadır.

Örgüt içerisinde; coğrafi, sektörel ya da kurumsal anlamda, "imam" olarak ifade edilen ve piramit şeklinde sıralanan sorumlular belirlenmiştir. Bu durum kademeler halinde yapılanan *Carbonari* örgütünü ve özellikle mevcut otoriteye içerisinde paralel devlet yapıları şeklinde olarak ortaya çıkan sömürge karşıtı etnik ayrılıkçı örgütleri (örneğin *FLN*) hatırlatmaktadır. Bu kapsamda ayrıca, Sivil Toplum Kuruluşları (STK)[10] teşkil ederek kamuoyunda taraftar toplanmaya çalışılmış ve

[10] Bazı STK'lar: Kimse Yok Mu Derneği, TUSKON'a bağlı dernek ve vakıflar vb. (TBMM Raporu, 2017: 104), TUSKON'a bağlı 7 federasyon ve 211 üye dernek bulunmaktadır (TBMM Raporu,2017: 188)

mali/ekonomik kuruluşlar, okullar, dershaneler, yurtlar vb. vasıtasıyla bir yandan gelir elde ederken bir yandan da örgüt mensuplarına istihdam yaratılmıştır. Piramit kademelenme, fonksiyonel farklılaşma olarak ele alındığında, yine hiyerarşik modele benzediği söylenilebilir.

Örgüt organizasyon yapısını daha da geliştirerek, devlet dışında kendisine bağlı bir ekonomik sistem kurma, şirket birlikleri ve konfederasyonlar kurarak zenginler kulübü oluşturma, böylelikle ulusal ve uluslararası alanda söz sahibi olmaya çabalamıştır. Bazı legal faaliyetleri dışında adeta bir organize suç örgütü vasfıyla ek finans kaynağı sağlamaya çalıştığı da söylenebilir (şantaj, baskı, zorlama, uydurma kaset, video vb.) (HSYK Genel Kurul Kararı, 2016: 7-8). Dinler arası diyalog çerçevesinde, semavi dinlerin temsilcileri ile görüşerek, kendisini İslam adına muhatap/yetkili göstermeye çalışarak ulusal ve uluslararası boyutta meşru olarak algılanmayı hedeflemiştir ki aslında bu durum en çok etnik milliyetçi/ayrılıkçı örgütlerde görülmektedir.

Dahası, yaklaşık 170 ülke/bölgesinde-özerk cumhuriyetinde din-siyaset-para ekseninde faaliyet gösteren bir organizasyon hüviyetine bürünmüştür (TBMM Raporu, 2017: 73). 147 yazılı medya (internet siteleri, haber portalları ve sosyal medya uzantıları dâhil), 58 görsel ve işitsel medya kuruluşundan oluşan bir ağ ile genel hedef ve amaçları sembollerle kodlayarak elemanlarına direktifler verme yöntemine başvurmuştur. Sosyal veri ağlarını kullanarak denetlenemeyen teknik ağ sistemi üzerinden örgüt iletişimini sağlamıştır (Bylock vb.) (TBMM Raporu, 2017: 74). Sonuç olarak, aynı anda birçok ülkede eşzamanlı faaliyetler yürütebilme kapasitesine sahip olduğu görülmektedir. Bu kapsamda daha çok FKÖ ve El-Kaide gibi küresel örgütlerle benzerlik göstermekte ve ağ modele uymaktadır.

Örgütün eleman temini ve örgüt içi radikalleşme ile ilgili faaliyetleri şu şekilde sıralanabilir; göreli yoksunlukları ve dini veya mistik inançları istismar ederek halk nezdinde geniş sempatizan kitle oluşturma, öğrencileri hedef alan eleman temini ve tabandan tepeye doğru kadrolaşırken radikalleşme, devlet örgütlenmesine uygun kendine özgü paralel örgütlenme modeli ile illegal yapılanmalar oluşturma ve gizlice devletin tüm kılcal damarlarına sızma. Ayrıca, tıpkı *Carbonari* örgütünde olduğu gibi, örgüt içerisinde mutlak bir otoriteye tabi olarak hareket edilmekte, ödül ve ceza sistemi uygulanmakta, örgüt mensuplarına örgüte girerlerken yemin ettirilmektedir. Kaldı ki, örgütten ayrılanları/ayrılmak isteyenleri yıpratma, sindirme, şantaj yapma, korkutma ve tehdit etme gibi yöntemler uygulanmıştır. Eleman teminindeki seçim kriterleri ise zeki ve eğitimli öğrencilere yönelmesi bağlamında *Aum Shinrikyo* ile benzerlik göstermektedir.

Yukarıda bahsedilen hususlar göz önünde bulundurularak FETÖ'nün organizasyon modeli genel olarak değerlendirildiğinde; hiyerarşik ve ağ modelin özelliklerini bir arada taşıyan hibrit bir organizasyon modeline sahip olduğu söylenebilir.

3.2. FETÖ'nün Motivasyonu

Motivasyon kaynakları bağlamında, çarpıtılmış dini yorumlara dayalı bir ideoloji geliştirme, dini/mistik inançların istismar edilmesi suretiyle hedeflere ulaşmak için yapılacak -silahlı şiddet dâhil- her türlü eylemin meşru gösterilmesi ve göreli yoksunlukları kullanarak bir hikâye oluşturma ön plana çıkan hususlardır. Hikâye; komünizmin Türkiye'yi ele geçireceği, insanların dini duygularını tam olarak yaşayamadığı, Fetullah Gülen'in müjdelenen kişi veya Mesih vb. olduğu şeklinde özetlenebilir.

Ayrıca, FETÖ'nün motivasyon bağlamında kült örgüt özelliklerini gösterdiği de söylenebilir. Kült örgüt elemanları, eylemlerinin doğru olduğuna inanmakla beraber bu inancı dışarıya yansıtmaya da çalışmaktadırlar (Demir, 2019: 6). Bu kapsamda dikte ettikleri yüce hedefler doğrultusunda, *Aum Shrinkyo* ve *Carbonari* örgütüne benzer şekilde, kimi zaman şiddet eylemlerinde bulunmaktan çekinmemektedirler. Yine, Hilmi Demir (2019)'in kült gruplar ile ilgili çalışmasında belirttiği üzere kült örgütlerde birer maske olarak kullanılan bu yüce hedefler aslında maddi menfaat sağlamak ya da liderin narsist egosunu tatmin etmek adına maske olarak kullanılmaktadır. Örgüte sadakat ve bağlılığı temin edebilmek maksadıyla korkutma, baştan çıkarma, ödül ve ceza sistemleri uygulanmaktadır. Örgüt liderleri kendilerini, ihtiyaç duydukları her şeye ulaşabilen, metafizik, ruhani varlıklar olarak sunmakta, zihinsel ikna yöntemiyle de elemanları yönlendirmektedirler (Demir, 2019: 6).

Dini olağanüstülük, mistik harikuladelik, seçilmiş kişi/kurtarıcı olma, mehdilik, Mesihlik şeklindeki lider kültüne sahip olma, katı bir inanç sistemi oluşturarak elemanlarını etkileme, kendini örgüte "kazandıran bir güç odağı" olarak telkin etme (sosyal statü, para, siyasi güç vb.) örgüt içi motivasyonda etkili kaynaklar olarak belirmektedir. Örgütün, "hizmet" için "seçilmiş" kişiler topluluğu olarak algılanmasını sağlama, "bir elinde Kur'an bir elinde bilgisayar tutan altın nesil", "zorunlu hicret" söylemiyle algı oluşturarak ajitasyon yapma ve uluslararası alanda "dini hoşgörüyü yaymaya yönelik gönüllüler hareketi", Türkiye'de ise "İslam dinine hizmet eden bir cemaat" algılarını ön plana çıkarma şeklinde motivasyonları olduğu da bilinmelidir (TBMM Raporu, 2017: 51). Örgütün; seçilmiş kişiler, altın

nesil, gönüllüler hareketi ve hizmet vb. kavramlar ile *Carbonari* örgütüne benzediği söylenebilse de kavramlara yüklenen anlamların ise farklı olduğu unutulmamalıdır. *Carbonari* elemanları, "dünyayı aydınlatacak olan iyi kuzenlerdir" ve bunlar "önce iyi bir *Carbonari* sonra Hristiyan" olabilmek düşüncesiyle hareket etmektedirler.

Örgüt, elemanlarının veya halkın algıladığı yoksunlukları ve memnuniyetsizliklerini (özgürce yaşayamama, ekonomik sıkıntılar vb.) gidermeye yönelik söylemlerde bulunmayı da eksik etmemiştir. Elemanlarını gerçeklikten uzaklaştırarak örgüte mutlak itaat etmelerini sağlamak maksadıyla rüya simülasyonu ve rüya metaforu yöntemi sıkça kullanılmıştır (Arslan, 2017: 37). Sözde, kutsal/manevi varlık ve şahsiyetlerle görüşmeler; Allah, Hz. Peygamber, melekler ve geçmiş din büyükleri ile görüşme iddiası; rüyalar, cincilik ve metafizik mesajlar üzerinden ezoterik bir örgüt ortamı yaratılmaya çalışılmıştır (İç Güvenlik Stratejileri Dairesi Başkanlığı, 2019: 31). Bu durumu açıklayan en net örnek, örgüt elemanı ve eski bir hâkim olan bir kişinin İstanbul 18. Asliye Ceza Mahkemesinde verdiği kararla Fethullah Gülen'i mehdi ilan etmesidir (HSYK Genel Kurul Kararı, 2016: 8-9).

Hitap edilen toplumun yapısına, kültürüne, tarihine uygun olarak hareket etme ve söylem geliştirme önemli olmakla beraber diğer şemsiye örgütlere (FKÖ, El-Kaide) göre farklı ve özgün bir özelliktir. Örgütün, TBMM Raporunda belirtildiği üzere, 170'e yakın ülkede faaliyet gösterdiği unutulmamalıdır (TBMM Raporu, 2017: 73). 15 Temmuz sonrası ise özellikle "insan hakları, demokrasi, hukukun üstünlüğü" gibi söylemler üzerinden hem algı yönetme hem de örgüt mensuplarını motive etmeye gayret edilmiştir. Cezaevlerinde bulunan örgüt mensuplarının gizli haberleşme (not, mektup gönderme vb.) yöntemleri ile bağlarını koparmamaya ve tekrar organize bir şekilde hareket edecek şekilde motive etmeye çalışılmıştır.

Motivasyon kapsamında yukarıda belirtilen hususlar göz önünde bulundurulduğunda örgütün; dini söylemle açıklanan, kült grup özelliklerini barındıran ve halkın dini/mistik inançlarını istismar eden ezoterik terörist bir örgüt olduğu söylenebilir.

3.3. FETÖ'nün Stratejisi

Daha önce de belirtildiği üzere örgüt, nihai hedefine ulaşmak için uzun süreli bir strateji takip etmiştir. Bu kapsamda 19. yüzyıl sonlarındaki anarşist örgütler ve 1960'lardaki sol ideolojiye sahip örgütlerden ayrılmaktadır. Aslında, kuruluş aşaması 1960'ların ortasına denk gelmekte ve eleman temininde yöneldiği kitle

bağlamında bu dönemdeki örgütlerle benzeşmektedir. Çünkü daha önce de belirtildiği üzere, faaliyetlerini ergenlik ve ilk gençlik dönemlerinde olan öğrenci ve gençler üzerinde yoğunlaştırmaya ve çekirdek kadro oluşturmaya çalışmıştır (TBMM Raporu, 2017: 73).

Teyp ve videokasetlerine kaydedilen vaaz, konuşma, icra edilen sohbet toplantıları ve yaz kamplarında hedef kitle üzerinde faaliyetlerini artırmaya çalıştığı görülmektedir. Aynı durum, ışık evleri oluşturulması, dernekler kurulması ve dernek aracılığıyla da ve cemaat yurtlarının faaliyete geçirilmesi ile devam etmiştir (HSYK Genel Kurul Kararı, 2016: 7).

Örgüt yasadışı istihbarat elde etme (telefon dinleme, gizli kamera yerleştirme vb.) faaliyetleri ile düşman olarak algıladığı kişi ya da kurumlara karşı bozucu ve yıpratıcı eylemlere girişmiştir. Aynı zamanda, devlet örgütlenmesine paralel ve kendine özgü hibrit örgütlenme modeli ile gizlice başta siyaset, mülkiye, adliye, maliye, askeriye ve emniyet olmak üzere devletin tüm kılcal damarlarına sızma ve illegal yapılanmalar oluşturmayı gaye edinmiştir (HSYK Genel Kurul Kararı, 2016: 7).

Yurt, okul, dershane ve ışık evlerinde, beyin yıkama metotları vasıtasıyla sorgulamayan, düşünmeyen, mutlak itaati esas alan yapıya bağlı insan tipi yetiştirme stratejisini geliştirmiştir (Ankara C. Başsavcılığı 2017/3376 numaralı iddianame, 2017). Beyin yıkama metotlarına ek olarak zihin kontrolü metotlarının da uygulandığı bilinmektedir. Örgüt elemanları, zihin kontrolü ile her türlü aldatıcı ve illegal yöntemleri uygulamaktan çekinmemişlerdir. Bu kapsamda FETÖ aynı anda hem gizli cemaatler hem de kült yapıların özelliklerini içermektedir.

Diğer taraftan örgüt, günümüz teknolojileri ve medyanın etkinliğinden oldukça faydalanmıştır. Örgüt liderinin sürekli olarak sözlü açıklamalarda bulunması, röportaj yapması, kitap ve dergilerde yazılarının yayımlanması ile internet sitesi, radyo ve televizyonların aktif olarak kullanılması ön plana çıkmaktadır. Örgütün görüşlerini rahatça iletme ve propaganda maksadıyla medyayı etkin olarak araçsallaştırmış olduğu açıktır.

Modern terörist örgütlerle benzerlikleri ve farklılıkları olan FETÖ, bir yandan da organize suç örgütü vasıflarına da sahiptir. Örneğin, çeşitli sınavlarda soruları hukuka aykırı yollarla ele geçirip, kendi mensuplarının sınavlarda başarılı olarak kamu kurumlarına ve etkin okullara girmesini sağlama bunlardan birisidir (HSYK Genel Kurul Kararı, 2016: 7). Yine, ürettiği sahte belge ve delillerle, örgüt mensubu olmayan kişiler hakkında adli ve idari soruşturmaların açılmasını

sağlayarak devlet kadrolarından tasfiye etme ve bu kadrolara kendi örgüt elemanlarını yerleştirme faaliyetlerini de yürütebilmiştir. Ayrıca, gizliliğe önem verme, takiyye yapma, kod adı ve özel haberleşme kanalları/programları kullanmak suretiyle örtülü faaliyetlerde bulunulmuştur. Örgütün bu tür faaliyetler ile bir yandan siyasi hedeflerine ulaşmayı hedeflediği bir yandan da çıkar sağlama amacını güttüğü görülmektedir. Hatta örgüt, faaliyetlerinin yayıldığı coğrafi alan ve çok boyutlu işlevleri göz önünde bulundurulduğunda adeta sınır aşan bir organize suç örgütü olarak yorumlanabilir.

Nihayetinde, FETÖ'nun benimsediği stratejinin daha kuruluştan itibaren uzun süreli olarak planlandığı görülmektedir. Bu uzun süre içerisinde birçok strateji ve yöntem bir arada kullanılmıştır. Bu kapsamda, bünyesinde süreklilikten ziyade değişimi barındıran eklektik bir strateji olduğu anlaşılmaktadır.

SONUÇ

Kuruluşundan itibaren kapalı bir cemaat olarak görülen, sonrasında sınır aşan organize bir suç örgütüne dönüşen ve en sonunda da şiddet içeren eylemlere yönelen FETÖ, 1960'ların ortasında başlayan uzun süreli ve sabırla uygulanan bir stratejinin ürünüdür. Terörist örgüt; uyguladığı yöntemler, eylem tipleri, eleman temini, örgütlenme, din istismarı, yurt dışı bağlantıları gibi birçok özellik sebebiyle benzerlerinden farklılık arz etmektedir

Karşılaştırmalı vaka analizleri neticesinde elde edilen bulgularla FETÖ'nün, hem hiyerarşik hem de ağ özelliklerini gösteren karma bir organizasyon modeline sahip olduğu; hedeflerini gizlemek maksadıyla sürekli olarak söylemlerini ve tutumlarını değiştirdiği; tedbir, gizlilik ve takiyyeden oluşan bir strateji geliştirerek gerektiğinde geri adım atmaktan, gerektiğinde de her türlü baskı, şantaj, tehdit, suikast, kumpas ile şiddet uygulamaktan çekinmediği; halkı, hasımlarını ve hatta kendi elemanlarını yanıltıcı retorik kullanarak karmaşa ve bilgi kirliliğini başlı başına bir yöntem olarak benimsediği; her ne kadar sınır aşan boyutta etki ve ilgi alanı olsa da aslında motivasyon bağlamında mistik inançların hakim olduğu ezoterik grup özellikleri taşıdığı, aynı zamanda da sınır aşan organize bir suç örgütü özellikleri barındırdığı söylenebilir.

Bu kapsamda FETÖ' nün; strateji, motivasyon ve organizasyon modeli bağlamında önceki örneklerinden farklılık arz eden, hibrit özellikler taşıyan ve sınır aşan organize bir suç örgütü gibi hareket eden kendine özgü nitelikte yeni tip bir terörist örgüt olduğu sonucuna ulaşılmıştır.

KAYNAKÇA

Ankara C. Başsavcılığı 2016/109268 soruşturma numaralı, 2017/19707 esas numaralı, 2017/3376 numaralı iddianame

Army, U. S. (2007). A military guide to terrorism in the twenty-first century.*US Army TRADOC G2 Handbook*.

Arquilla, J. ve Ronfeldt, D. (2001). *Networks and netwars: The future of terror, crime, and militancy*. Rand Corporation.

Arquilla, J., ve Ronfeldt, D. (1999). The advent of netwar: Analytic background. *Studies in Conflict and Terrorism*, 193-206.

Arslan, H. (2017) Rüya Metaforu Üzerinden Din İstismarı: FETÖ Örneği. *Liberal Düşünce Dergisi*, (87), 33-47.

Avcı, E. (2011). Radikal islamcı terörizmin meşru gösterilmesi: Türkiye Hizbullahı örneği. (Yayımlanmamış Doktora Tezi). Kara Harp Okulu, Ankara.

Bartholdy, J. L. (1821). *Memoirs of the Secret Societies of the South of Italy: Particulary the Carbonari*. John Murray.

Bernstein, M., ve Crosby, F. (1980). An empirical examination of relative deprivation theory. *Journal of Experimental Social Psychology*, *16*(5), 442-456.

Boot, M. (2013). *Görünmeyen ordular: Gerilla tarihi.* İnkılap Kitabevi.

Box, M., & McCormack, G. (2004). Terror in Japan: The Red Army (1969-2001) and Aum Supreme Truth (1987-2000). *Critical Asian Studies*, 91-112.

Crenshaw, M. (2006). Have motivations for terrorism changed. *Tangled roots: Social and psychological factors in the genesis of terrorism*, *11*, 51-57.

Cronin, A. K. (2003). Behind the curve: Globalization and international terrorism. *International security*, *27*(3), 30-58.

Davis, M. (2007). The FLN's Strategy for Gaining an Independent Algeria, 1954-1962. *Ronald E. McNair Program*, 1-13.

Demir, C. K. (2017). *Sebeplerinden Mücadele Yöntemlerine Etnik Ayrılıkçı Terörizm: PIRA, ETA, PKK*. Ankara: Nobel Akademik Yayıncılık.

Demir, H. (2019). Radikal/yıkıcı kült gruplar: Kavram ve teorik bir çerçeve. 1-13.

Dishman, C. (2016). Terrorist and criminal dynamics: A look beyond the horizon. Matfess, H. and Miklaucic, M (Ed.), *Beyond Convergence: World Without Order*, 137-155.

Erickson, E. J. (2013). Ottomans and Armenians: A Study in Counterinsurgency. Springer.

FETÖ, Din İstismarı, İhanet ve Tehdit, İç Güvenlik Stratejileri Dairesi Başkanlığı

Fromkin, D. (1975). The strategy of terrorism. *Foreign Affairs*,*53*(4), 683-698.

Frost, T. (1876). *The Secret Societies of the European Revolution, 1776-1876* (Cilt. 1). Tinsley Bros.

Frost, T. (1876). *The Secret Societies of the European Revolution, 1776-1876* (Cilt 2). Tinsley Bros.

Hâkimler ve Savcılar Yüksek Kurulu Genel Kurul Kararı, Karar No: 2016/426, Tutanak No:17, 24.08.2016, https://www.resmigazete.gov.tr/eskiler/2016/08/20160825-5.pdf. Erişim Tarihi: 24.10.2019

Heger, L., Jung, D., ve Wong, W. H. (2012). Organizing for resistance: How group structure impacts the character of violence. *Terrorism and Political Violence*,*24*(5), 743-768.

Hoffman, B., *The End of Empire and the Origins of Contemporary Terrorism*, Inside Terrorism (p. 43-62)

https://en.wiktionary.org/wiki/baracca, Erişim Tarihi: 23.10.2019

https://www.britannica.com/topic/millennialism. (Erişim Tarihi: 13.09.2019)

Hudson, R. A. (1999). *The sociology and psychology of terrorism: Who becomes a terrorist and why?* Library of Congress Washington Dc Federal Research Div.

Hutchinson, M. C. (1972). The concept of revolutionary terrorism. *Journal of Conflict Resolution*, *16*(3), 383-396.

Kalyvas, S. N. (2003). The ontology of "political violence": action and identity in civil wars. *Perspectives on politics*,*1*(3), 475-494.

Kilberg, J. (2012). A basic model explaining terrorist group organizational structure. *Studies in Conflict & Terrorism*, *35*(11), 810-830.

Kydd, A. H. ve Walter, B. F. (2006). The strategies of terrorism. *International security*, *31*(1), 49-80.

Laqueur, W. (2002). *A history of terrorism*. Transaction Publishers

Laqueur, W. (2004). Voices of Terror: Manifestos. *Writings and Manuals of AL Qaeda*.

Marighella, C. (2011). *Minimanual of the urban guerrilla*. Praetorian Press LLC.

Miller, M. A. (2003). The intellectual origins of modern terrorism in Europe. *Terrorism in context*, 28-41.

Novak, D. (1954). Anarchism and individual terrorism. *Canadian Journal of Economics and Political Science*, *20*(2), 176-184.

Olson, K. B. (1999). Aum Shinrikyo: Once and Future Threat? *Emerging Infectious Diseases*, *5*(4), 513-516.

Price, H. E. (1977). The strategy and tactics of revolutionary terrorism. *Comparative Studies in Society and History*, *19*(1), 52-66.

Rapoport, D. C. (2001). The fourth wave: September 11 in the history of terrorism. *Current History*,*100*(650), 419.

Rapoport, D. C. (2002). The Four Waves of Rebel Terror and September. *Anthropoetics*, (1).

Rath, R. J. (1964). The Carbonari: Their Origins, Initiation Rites, and Aims. *The American Historical Review*, *69*(2), 353-370.

Shiver, C. (1964). The Carbonari. *Social Science*, 234-241.

Simon, J. D. (2008). The forgotten terrorists: Lessons from the history of terrorism. *Terrorism and political violence*, *20*(2), 195-214.

TBMM. (2017). ‘‘FETÖ/PDY Meclis Araştırma Komisyonu Raporu’’ http://altinoz.com.tr/wp-content/uploads/2017/05/Rapor_26.05.pdf. Erişim tarihi: 02.09.2019.

Thorup, M. (2008). The anarchist and the partisan—Two types of terror in the history of irregular warfare. *Terrorism and Political Violence*, *20*(3), 333-355.

Wilkinson, P. (2000). The strategic implications of terrorism. *Terrorism and political violence: A sourcebook*, 19-49.

SECURITY EVALUATION OF INDUSTRY 4.0: UNDERSTANDING INDUSTRY 4.0 ON THE BASIS OF CRIME, BIG DATA, INTERNET OF THING (IoT) AND CYBER PHYSICAL SYSTEMS

Emre Cihan ATEŞ[*], Erkan BOSTANCI[**] , Mehmet Serdar GÜZEL[***]

Abstract

In the past, we all witnessed that the production facilities were shifted to the countries with low employment costs due to the increasing labour costs around the world. Today, especially with the revolution of industry 4.0 initiated under the leadership of the developed countries on the basis of technology, industrial competition is tried to be provided within the framework of productivity and quality by reducing the cost of workmanship. The Industry 4.0 revolution is also defined as intelligent self-coordinating factories almost independently of people.

The entry of Industry 4.0 into our lives is expected to revolutionize many sectors especially information technologies, communication and education. In this context, the subject of crime is also a candidate to be one of the areas of change because the profitable gain structure of the Industry 4.0 environment is expected to be one of the factors that motivate criminals to take action in this field. Therefore, the industrial revolutions were aimed to be examined in terms of security, internet of things and big data with this study conducted.

In the analysis performed, it is clear that Industry 4.0, which aims at production maximization, will cause security problems with its current situation. With Industry 4.0, these security issues have become more specific problems and the concept of automation has added new paradigms to security issues and increased the possibility of being a victim of cyber threats. Currently, our industry is between Industry 2.0 and Industry 3.0. Within this scope, it is essential to enhance the technical background of the security teams in order to prevent the crimes that may occur in the future. It is expected that the most appropriate action type of security teams is the security-focused defence understanding. Regarding this understanding, a proactive attitude should be exhibited and it is necessary to use effective methods against cybercriminals. In today's world where the technology changes rapidly, it should be considered that a statical defence understanding cannot be accepted but security teams should adopt a dynamic cybercrime intervention policy in order to fight against new threats.

Keywords: *Industry 4.0, Crime, Internet of Thing (IoT), Security, Big Data, Artificial Intelligence, Cyber-physical Systems.*

[*] Gendarmerie Lieutenant, Lecturer, Gendarmerie and Coast Guard Academy, Turkey, emre_cihan_ates@hotmail.com, ORCID ID: https://orcid.org/0000-0001-9550-4532

[**] Assoc. Prof. Dr., Ankara University, Faculty of Engineering, Turkey, erkan.bostanci@ankara.edu.tr, ORCID ID: https://orcid.org/0000-0001-8547-7569

[***] Assoc. Prof. Dr., Ankara University, Faculty of Engineering, Turkey, mguzel@ankara.edu.tr, ORCID ID: https://orcid.org/0000-0002-3408-0083

Makale Geliş Tarihi: 28.10.2019 Makale Kabul Tarihi: 02.01.2020

ENDÜSTRİ 4.0'IN GÜVENLİK DEĞERLENDİRİLMESİ: ENDÜSTRİ 4.0'I SUÇ, BÜYÜK VERİ, NESNELERİN İNTERNETİ VE SİBER FİZİKSEL SİSTEMLER TEMELİNDE ANLAMAK

Öz

Dünya üzerinde işgücü maliyetlerinin artmasıyla birlikte üretim tesislerinin işçilik maliyeti düşük olan ülkelere kaydırıldığına geçmiş zamanlarda hepimiz şahit olduk. Günümüzde özellikle, teknoloji temelinde gelişmiş ülkeler öncülüğünde başlatılan endüstri 4.0 devrimiyle birlikte, söz konusu işçilik maliyeti düşürülerek üretkenlik ve kalite çerçevesinde endüstriyel rekabet sağlanmaya çalışılmaktadır. Endüstri 4.0 devrimi, neredeyse insanlardan bağımsız olarak kendi kendini koordine eden akıllı fabrikalar olarak da tanımlanmaktadır.

Endüstri 4.0'ın hayatımıza girmesiyle birlikte; bilgi teknolojileri, iletişim ve eğitim başta olmak üzere birçok sektörel alanda devrim yaşanması beklenmektedir. Bu kapsamda, suç alanı da söz konusu değişim alanlarından biri olmaya aday konumdadır. Çünkü Endüstri 4.0'ın ortaya çıkaracağı kârlı kazanç yapısı, suçluları da bu alanda harekete geçmeye motive eden unsurların başında gelmesi beklenmektedir. Yapılan bu çalışma ile Endüstri 4.0'ı anlayarak, mevcut endüstriyel devrimlerin; güvenlik, nesnelerin interneti ve büyük veri açısından incelenmesi amaçlanmıştır.

Yapılan incelemede, üretim maksimizasyonunu amaç edinen endüstri 4.0'ın, mevcut haliyle güvenlik sorunu doğuracağı ortadadır. Endüstri 4.0 ile birlikte, güvenlik sorunlarının çok daha spesifik hale gelmesi ve otomasyon kavramının güvenlik sorunlarına yeni paradigmalar eklemesi, genel anlamda siber tehdit mağduriyetini arttırmıştır. Halihazırda sanayimiz Endüstri 2.0 ile Endüstri 3.0 arasındadır. Bu kapsamda, gelecekte olması muhtemel suçların önlenmesi için güvenlik güçlerinin şimdiden teknik altyapılarını olgunlaştırmaları şarttır. Güvenlik güçleri için en uygun hareket tarzının, güvenlik odaklı savunma anlayışı olması beklenmektedir. Bu anlayış çerçevesinde, proaktif tutum sergileyerek; siber suçlulara karşı etkin yöntemlerin kullanılması gerekliliktir. Teknolojinin hızla değiştiği günümüzde, statik bir savunma anlayışının kabul edilemeyeceği, güvenlik güçlerinin her zaman yeni tehditlere karşı koyabilecek, dinamik bir siber suçla mücadele politikası benimsemesi gerektiği değerlendirilmektedir.

***Anahtar Kelimeler**: Endüstri 4.0, Suç, Nesnelerin İnterneti, Güvenlik, Büyük Veri, Yapay Zeka, Siber-Fiziksel Sistemler.*

INTRODUCTION

Throughout history, human beings have constantly changed their life habits. The changing items were behaviours, habits, goods, houses, etc., which were always described as better. In every progress in the life cycle of humanity, the old deeds were seen as more primitive and evil. In fact, this understanding can be explained by the saying "doing more with less." As a series of researchers aiming at this aphorism invented the machines that used water and steam power in England in the 18th century, the transition from the agriculture and handicrafts-

based economy, which can be called as primitive, to industry-based production was realized (Harley, 2018). On the basis of mechanization, the transition to industrial production spread to the whole world in time, and this was followed by the development of the so-called 1st Industrial Revolution (Industry 1.0). After 1870, mechanical productions became faster with the support of electrical energy and the period called the second industrial revolution (Industry 2.0) was entered (Klingenberg and Do Vale Antunes, 2017; Stearns, 2018). As a result of the widespread use of electronic and automation systems as of 1969, labour costs were further reduced and the third industrial revolution (Industry 3.0) emerged (Stearns, 2018).

The existence of industrial manufacturing is an absolute part of every economy. Since the evolution of industrialization, the industry has experienced quite different technological changes, aiming at profit maximization. Today's economy has begun to face a new industrial revolution triggered by political, technological, economic and social changes, which is defined as the 4th industrial revolution (Industry 4.0) (Morrar, Arman and Mousa, 2017). As shown in Figure 1, the complexity of the event increases with each time-related industrial revolution. With Industry 4.0, many new technologies that are pioneers in different disciplines will start to be used together (Klingenberg and Do Vale Antunes, 2017).

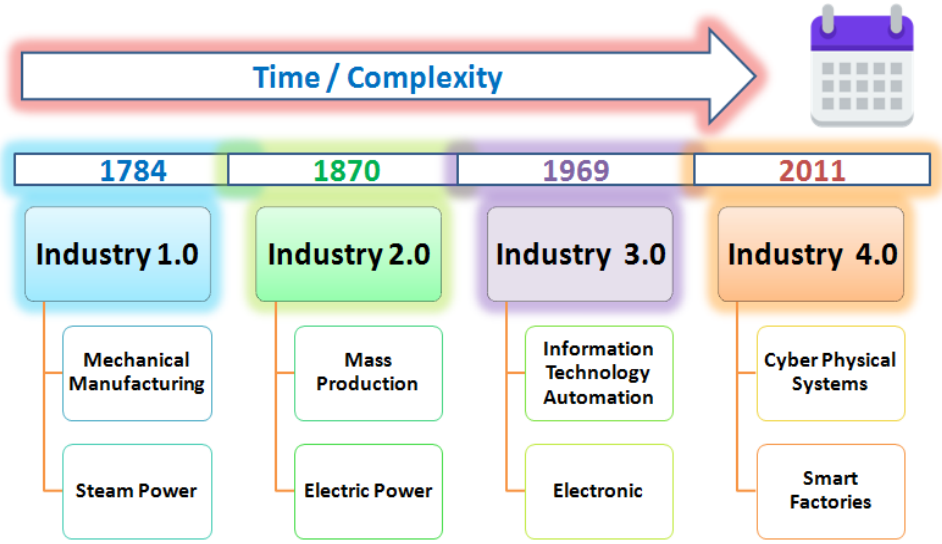


Figure-1. Time-Based Changes of Industrial Revolutions

The concept of Industry 4.0 is also defined as “smart factory" (Chen, Wan, Shu, Li, Mukherjee and Yin, 2017; Hozdić, 2015; Wang, Wan, Li and Zhang 2016) and the smart factories are expected

- To be a virtual replica of the physical world,

- Developing decentralized decision-making processes,

- All physical systems are expected to be able to communicate and cooperate with each other and people in real-time through the “Internet of Things”.

1. UNDERSTANDING INDUSTRY 4.0

The basic element in understanding Industry 4.0 is to determine why the current society and industrial order need a change. The origin of the rising paradigms of the change put forward in this context was laid in 2011. Many of the world's major economies of the past, including Germany, the USA and France, which are known for their success in industry and production, began to suffer economic defeat against China, which is the rising star of the Asian market (Wübbeke and Conrad, 2015). The low labour costs in some densely populated countries, especially China, are the main factors that render competition difficult. In addition to the existing labour costs, the fact that the age average of the world population has been increasing and the population growth rate has been decreasing gradually in many countries in the world, foremost being European countries, comprise many risk factors for industry and production for the near future (Stearns, 2018).

The first step towards changing this order that emerged was taken in 2011 at the Hannover Fair in Germany (Vogel-Heuser and Hess, 2016). The term “Industry 4.0" emerged as the strategy of decreasing competition with overseas countries and differentiating the industries of Germany and the European Union from other international markets. In this context, Germany will start to use new developments such as big data, internet of things and machine learning actively in the future productions for the sake of increasing competitive power by decreasing costs.

The main idea of Industry 4.0 is to connect cyber-physical systems (CPS), i.e. embedded actuators, sensors and microcomputer networks, to the value chain of machines (Vogel-Heuser and Hess, 2016). It is characterized by being able to restructure products by developing them digitally as well as personalized products and a well-coordinated combination of products and services (Lee, Bagheri and Kao, 2015). To put it differently, the industry 4.0 system is a centralized and

automation-oriented form of production that minimizes the difference between the real and the virtual world by using modern information technologies, thereby keeping human intervention and labour-power to a minimum (Figure 2) (Monostori et al., 2016).

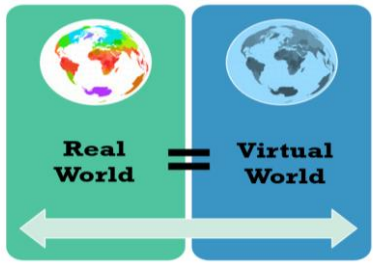


Figure-2. Reality in Cyber-Physical Systems

Cyber-physical systems (CPS) used in Industry 4.0 are likely to become one of the most important technological developments in the near future. When examined in general, these are systems in which the inputs learned by the computer are increased to maximum efficiency with machine learning and artificial intelligence and which comprise a physical environment controlled by the computer software and the software in question (Chen, 2017; Chiu, Cheng and Huang, 2017; Lee, Bagheri and Kao, 2015). The systems, as shown in Figure3, focus on (3C) computerization, inter-system communication and control of input and output (feedback loop) (Liu et al., 2017, Wan et al., 2011). Many of the systems we use today, which we call “intelligent production systems", are generally focused on the logic of continuing the same process singularly and continuously, which is also the distinguishing aspect of cyber-physical systems.

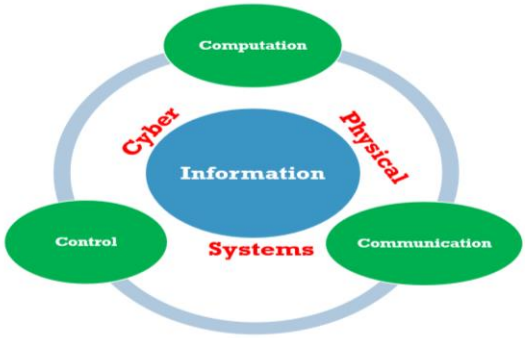


Figure-3. The Cycle of Cyber-Physical Systems (3C)

With the new cyber-physical systems put forth, the production equipment aims to improve the production process by maintaining communication with each other and employees. From this point of view, since the information processing speed of computers is much faster than the people, the aim was to get the products and the equipment that provides the production to communicate with each other (Liu et al., 2017).

In the report published by Boston Consulting Group with the title "Industry 4.0: The Future of Productivity and Growth in Manufacturing," regarding the identification of areas that Industry 4.0 will revolutionize, the nine different transformation technologies where Industry 4.0 was defined were put forth, as shown in Figure 4 (Rüßmann et al., 2015).

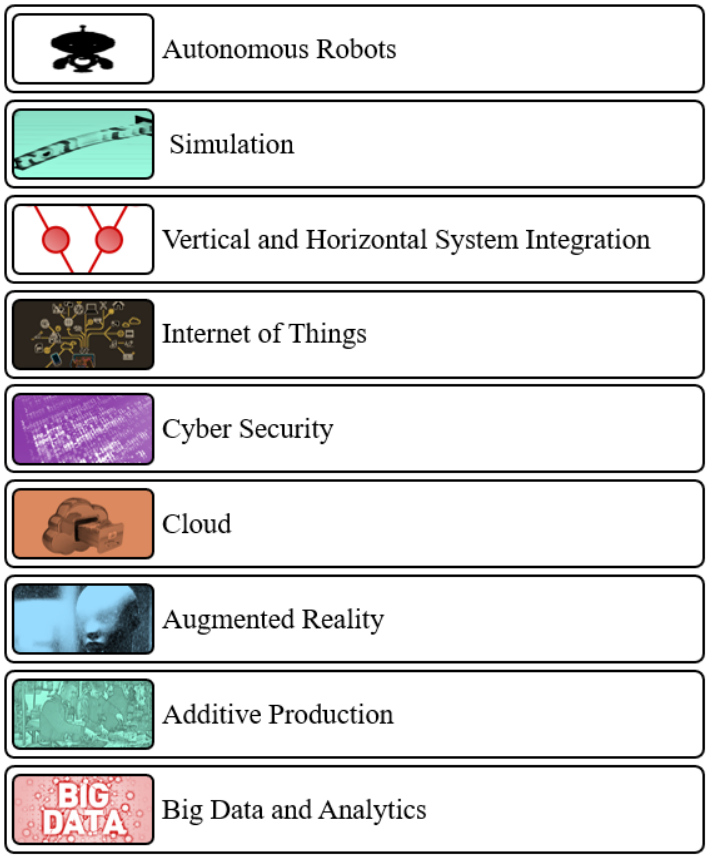


Figure-4. Nine Transforming Technology in Industry 4.0

When the transformation technologies mentioned in Figure 4 are examined, it is seen that;

- Thanks to autonomous robots, productivity will increase as the cost will decrease in the manufacturing industry. Furthermore, the robots will be able to work more autonomously and flexibly (Rüßmann et al., 2015).

- With the simulation systems, it will be possible to simulate factory, machine and products in a virtual model over real-time data. Products simulated in a virtual environment will reduce cost after testing and optimization (Schluse et al., 2018).

- Vertical and horizontal system integration is aimed with industry 4.0, and horizontal integration will establish a network connection between machines and equipment. With vertical integration, it will be possible to control different parts of the supply chain (Vaidya et al., 2018).

- With the "Internet of Things" technology, the communication of machines used in production with each other and with central control devices will be increased, and productivity will be ensured (Hozdić, 2015).

- With the concept of cybersecurity, it will be possible to protect machines and systems defined in networks within the scope of industry 4.0 against cyber attacks (Rüßmann et al., 2015; Nguyen et al., 2019).

- Cloud systems will facilitate access to all machinery and production equipment by providing data storage over the network. Their speeds will decrease down to milliseconds of reaction time, and their functionality will gradually increase (Aljawarneh, Alawneh and Jaradat, 2017).

- It will be possible to perform various services such as augmented reality-based systems, selection of parts in a warehouse and sending repair instructions to mobile devices. In addition, the creation of the replica of the physical environment in the virtual environment will reduce costs (Paelke, 2014).

- The added production will especially be used in the production of three-dimensional printers and customized products. It will be actively used to make the prototype of and produce the components in production (Rüßmann et al., 2015).

- A comprehensive evaluation by collecting data from many different sources with big data and data analytics will become the standard to support real-time decision making (Jin, Wah, Cheng and Wang, 2015).

In this study, which aims to analyze the new transformation environment that will be revealed by the concept of Industry 4.0, it is aimed to examine the concepts of the internet of things and big data, which are among the mentioned transformation areas, in terms of cybersecurity. In this context, the internet of things and big data concepts will be described in detail in the first part of the study.

1.1. Big Data and Analytics

The concept of big data is the data collection structure that emerges with the loops of event that we encounter every day and which does not make sense in the instant view (which can provide access to meaningful information through analysis). The data is meaningful only when evaluated. In other words, we can describe the data as precious metals in piles of rocks, waiting to be extracted (Yin and Kaynak, 2015).

We are in a system where almost everything we encounter in the modern age is based on data. Therefore, in order to better define the concept of big data, we should examine the 5V (Volume – Variety – Velocity – Verification - Value) rule which is accepted in the literature and defines the big data (Figure 5) (Jin et al., 2015; Mayer-Schönberger and Cukier, 2013);

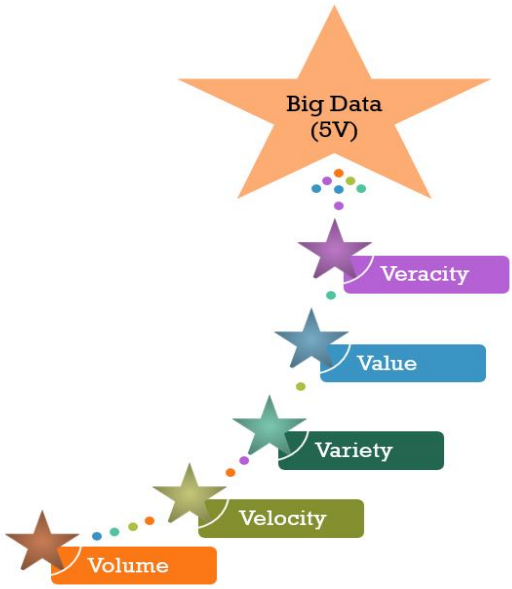


Figure-5. 5V Rule in Big Data

- Volume refers to the continuously increasing amount of data. Increase in the amount of data will make it difficult to access meaningful information from big data (Jin et al., 2015).

- Variety refers to the fact that the majority of the data constituting the big data is produced in different non-structural environments and formats. Analysis of data received from different formats and sources will also be more difficult and different from classical methods (Assunção, Calheiros, Bianchi, Netto and Buyya, 2015).

- Velocity refers to the data, the growth rate of which continuously increases. Big data is structures in which the data increases continuously.

- Verification of the data refers to the protection of the data obtained by high-level security measures and the impossibility to modify it by unauthorized interventions (Jin et al., 2015).

- Value defines the transformation of data into meaningful information by the evaluations that will be made from within the big data and its backing up decision support units (Assunção et al., 2015).

The increase in data volume together with the concept of big data leads to the problem of relativity and complexity of information. Therefore, it is becoming more and more important that accurate data that is analyzed correctly can be put forth. Big data in industrial terms are important in areas such as product and market development, operational efficiency, decision making, market demand forecasts and customer experience.

The industrial structure put forth by Industry 4.0 suggests a predictive production model (Bendel, 2015). In smart factories, machines are interconnected as a common community, and production is customer-oriented and flexible. Such a structure increases the importance of prospective forecasts. Forecasting is possible by analyzing historical data, that is, with the concept of big data. For the industry, this data is generally that which changes manufacturers' perception of value and manufacturing services and includes the production analyses of the previous years. In this decision-making process in industry 4.0, where human labour is minimized, most of the decisions will be made through artificial intelligence systems based on machine learning. Although the concept of artificial intelligence is not at the desired level today, it is considered that depending on the scientific developments to occur in this field, transformation into smarter machines will be provided in the future (Lee, Ardakani, Yang and Bagheri, 2015).

1.2. Internet of Things (IoT) Technology

The “Internet of Things” concept is a term used to refer to an object connected to any network. It can also be defined as a system that can define the physical objects that we see around us and communicate with them. As illustrated in Figure 6, in the “Internet of Things” system, the objects can connect to the network by means of the sensors they have and establish access to the system or database. The concept of the “Internet of Things” is shown as one of the greatest developments in the modern age, because an object that also has a digital identity is in contact with its environment as well as its user.

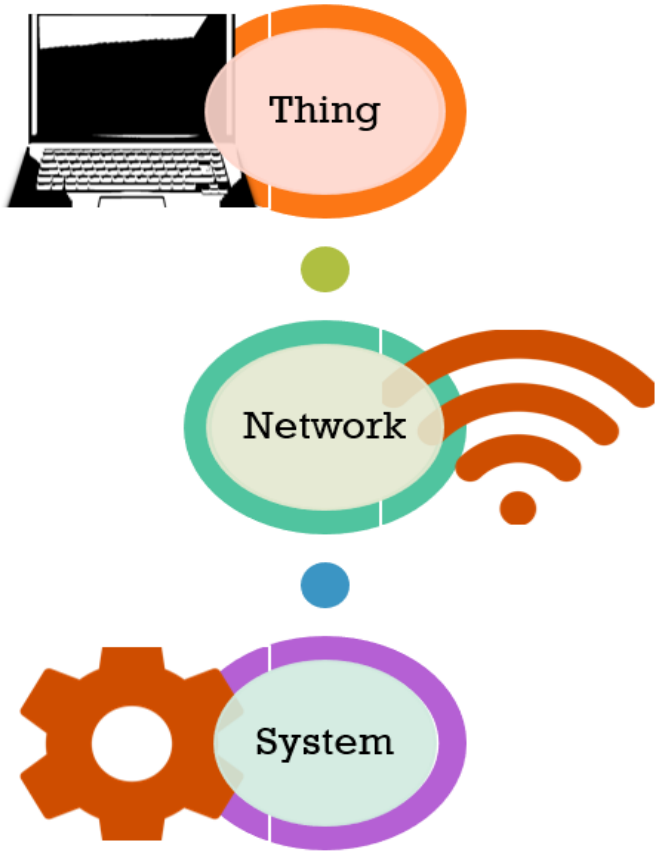


Figure-6. Internet of Things (IoT) Technology

The ability of objects to connect will bring along many positive benefits, especially in the field of production (Botta, De Donato, Persico and Pescapé, 2016; Hozdić, 2015). The following five main "Internet of Things" technologies are widely used for the distribution of network data (Lee and Lee, 2015). The Internet of things technologies in question are defined as radio frequency identification (RFID), wireless sensor networks (WSN), middleware, cloud computing and IoT application software (Hozdić, 2015).

Today we live in a world with more IoT-connected devices in number than people. Devices connected to the "Internet of Things" can communicate with each other over defined networks or cloud-based platforms. Real-time information collected through the "Internet of Things" technology may comprise many different areas, primarily health, security and commercial activities.

2. EVALUATION OF POSSIBLE CRIME AREAS ON SECURITY BASIS

In parallel with the increase in labour costs in developed countries, increasing production costs have set off humanity into a new quest. As the labour costs are high, developed countries have significantly closed the cost gap with productivity and quality in order to be able to compete with the industrial revolution led by Germany (Zhou, Liu and Zhou, 2015).

Together with industry 4.0, as social change is expected in many areas, the area of crime is also a candidate for becoming one of the areas of the social change in question. This is because the profitable earnings structure of the Industry 4.0 environment is expected to motivate criminals to take action in this area (Nguyen et al., 2019). Besides, the resulting crime environment is expected to increase the role of cybersecurity gradually. It is obvious that increasing cybersecurity measures too much will partially reduce the productivity of the factories. In this context, cost-effectiveness analysis is a must for each method to be used in the struggle against crime. The concept of Industry 4.0 will be examined from 7 different perspectives in terms of crime and security in the light of today's changing paradigms (Figure 7). In this study, the aim was to investigate the changes brought about in terms of security by Industry 4.0, which revolutionized information technologies.

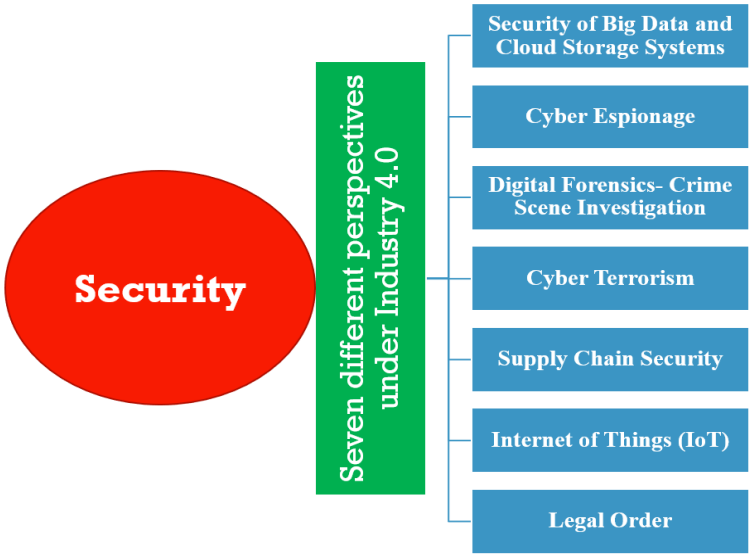


Figure-7. Security Areas in Industry 4.0

2.1. Security of Big Data and Cloud Storage Systems

Today, together with the continuous increase in the amount of data and the ability of machines to communicate with each other thanks to the Internet of Things Technology, the transition of data from singular and closed environment to cloud storage environments has become necessary (Aljawarneh et al., 2017; Yin and Kaynak, 2015). This transition brings about a series of changes in data protection habits in the field of security. Cloud-based data storage in Industry 4.0 should be “highly secure, scalable, and autonomous" (Gubbi et al., 2013).

Cloud storage systems actively use authentication methods as security. The storage areas in question, by duty, allow the processing of the data by storing big data. Cloud storage areas are the centre of the industrial production system, so only the right people should have access to the centre where the information is stored (Botta et al., 2016). Otherwise, all information can be retrieved, changed or destroyed in cyberattacks conducted by competing companies and businesses with different purposes. In this context, measures such as privileged access control, especially through flexible authentication methods, are considered to be highly effective in managing data access. As with the Internet of Things technology, the great increase in security measures leads to the disintegration of the factory's centre of gravity. In this context, it is obvious that cloud storage areas will be re-evaluated within the scope of cost-effectiveness analysis in the near future.

2.2. Cyber Espionage

The main work of cyber espionage is the capture, sabotage and unfair information acquisition of information in virtual environments, especially by malicious hackers (Wangen, 2015). Within the scope of Industry 4.0, information that the manufacturing sector defines as a trade secret is of interest to cyber espionage. Especially with the attack type defined as "Advanced Persistent Threat" (APT) in the literature, unauthorized person / group can access the network, stay unnoticed for a long time and get all the information about production (Wangen, 2015). Cyber espionage is also a threat to factories' research and development (R & D) activities and databases.

Industry 4.0 is, in general, more vulnerable to cyber espionage than conventional manufacturing, because the high number of intelligent and connected business processes increases cyber threats. For Industry 4.0-based manufacturing companies, it is very likely that specific information about the production infrastructure such as product information and technical specifications will be stolen through cyber espionage methods (Taute, 2017). In this context, the Industry 4.0-based production approach creates cost and efficiency while creating a highly open environment for cyber espionage. In the near future, factories are expected to increase their security measures against cyber-espionage activities because it seems unlikely that security forces will take preventive measures in individual and subjective dimensions within the scope of cyber defence.

2.3. Digital Forensics - Crime Scene Investigation

In the classical investigation methods, it is the duty of the security forces to determine the identity of the perpetrators and to lead them to stand before the judicial authorities after the crime has been committed. In this context, the investigation and detection of attacked computer networks and data storage environments require technical knowledge (Thames and Schaefer, 2017). The need for technical information brings along the need for regular training of security forces and the need for personnel to specialize in Industry 4.0-related digital crimes.

Specialized personnel in the current IT field have been trained in order to carry out minor forensic investigations. With Industry 4.0, performing a major forensic examination is essential, given the size of the data. In addition, the ability to perform the related major examination allows security forces to see and inspect all the data of smart factories. At this point, it is necessary to provide a sterilized environment in which security forces will not be attacked by cyber-attacks for the investigation to be conducted in a healthy manner.

In minor forensic investigations, the image of the study data is taken and work is done on the image, which secures the master data. But at a major level, it is now quite difficult and costly to physically take the image of large data, often based on cloud technology. Analyzing data without taking an image involves different risk factors.

2.4. Cyber Terrorism

Cyber terrorism is the attack on computers, networks and information stored therein which include the social and political goals of a government or a people (Al Mazari, Anjariny, Habib and Nyakwende, 2018). It is in the nature of cyber terrorism that the attack creates an impact on society and intimidates people and involves violence. For this reason, critical production facilities are within the target area of cyber terrorism (Gordon and Ford, 2002; Gordon, 2004).

Cyber terrorism is a type of attack in which cybercriminals turn into digital terrorists with political considerations. Since the Industry 4.0 system is built on efficiency, the system is vulnerable to attacks by cyber terrorists because of the low level of network security and the possibility of propaganda in society following the attack. When the targets of cyber terrorism are considered, it can infiltrate critical production facilities for different purposes, foremost being for the purpose of propaganda and destroy the technical structure of information and production or render the information invaluable by sharing this confidential information with others. It is known that existing terrorist groups are actively working on cyber terrorism techniques. There are threat analyses and many academic studies on how the cybersecurity information accessed by ISIS, which has grown in recent years, can create a disaster on critical infrastructures (Hilse, 2014).

2.5. Supply Chain Security

Together with the technology of the Internet of things and the digitalization of the supply chain with the help of sensors (Tjahjono, Esplugues, Ares and Pelaez, 2017);

- Work accidents have been reduced with automatic material circulation,

- With unmanned warehouses operating 24/7 and fast vehicle loading and unloading systems, optimization of warehouse areas and stock management has been ensured,

- And there has been an increase in the profit and productivity ratios of the factories.

With smart factories taking a series of security measures in their own right, many of the biggest security breaches started with a supplier, and mass data were often revealed with information being stolen (Pereira, Barreto and Amaral, 2017). That the criminals enter the supply chain within the scope of industry 4.0 and access the smart factory through rational actors provide more opportunities for cyber-criminals. These attacks usually occur in the form of interfering with the system and destroying data or intentionally modifying it in order to destroy the system.

Attacks by cybercriminals on smart factories can be prevented by using modern cybersecurity measures such as adaptive authentication and behaviour analysis. Furthermore, it is considered that the security system including the simultaneous recording system used in blockchain technology will become ineffective with the development of quantum computers in the near future (Aggarwal, Brennen, Lee, Santha and Tomamichel, 2017).

2.6. Internet of Things (IoT)

The concept of "Internet of Things" refers to the network connection between objects. It is an indispensable part of new business processes that emerged with Industry 4.0. It is a fact that especially the efficiency of production and the quality of people's life will increase together with the distribution of network data in the Internet of Things technology (Hozdić, 2015). However, this system contains a great number of entry points that are potentially exploitable (Vasilomanolakis et al., 2015). Especially IoT devices are known to have security vulnerabilities due to non-cryptographic sending, unsafe web interfaces, low-security software protections, and inadequate authorizations (Lee and Lee, 2015). Devices in IoT generally do not use strong data encryption techniques. Although the security structures used in the devices in the Internet of Things are stronger than conventional wireless network connections, they are not sufficient. Some IoT applications support sensitive infrastructure and strategic services such as smart grids and facility protection (Lee and Lee, 2015). In addition, devices with Internet of Things technology store all kinds of data they receive through their sensors, which will be more valuable than other physical traces in forensic examinations. For example, it will be easier to reach a lot of information such as when and from which source a product offered on the market was taken and which processes it was subjected to.

In our daily life, the problem of privacy will increase with the technology of the Internet of Things, which is becoming widespread in various devices from smartwatches to mobile phones. Although there is a partial resistance to accepting IoT by companies and individuals, especially due to its weaknesses in terms of security and confidentiality, it is still preferred because of its high gains as well as risks. However, it is difficult to say that critical facilities in industrial production are fully protected from cyberattacks before the security problem of IoT is solved. For this reason, it is necessary to take active firewall protections in every object where IoT is active. It is possible to overcome the security problems created by the Internet of Things technology with security measures that generate strong cryptography. The high safety measures cause the centre of gravity to deviate from the efficiency area. Therefore, in the near future, devices with Internet of Things technology are expected to have powerful cryptosystems that can revise themselves continuously.

2.7. Legal Order

The profitable earnings structure revealed by the concept of Industry 4.0 will motivate criminals and bring along new types of crime. In this context, it is necessary to revise the laws in order to fight against new types of crime because one of the most important steps of the fight is the deterrent force of the laws. It is important that laws are revised periodically, just like the type and methods of crime, and that criminal behaviour is defined in the law. With the changes to be made in the law, security forces are required to intervene in a reactive manner and to proactively prevent possible crimes.

The greatest uncertainty in the near future is that there is no universal agreement as to which legislation will be applied if the data within the cloud storage companies operating in different countries are subjected to judicial review. The data on the cloud storage system can be collected on a single server; besides, as opposed to the current order, firms can compartmentalize data and store them on multiple servers as a tactic of defence against cyberattacks (Lillis, Becker, O'Sullivan and Scanlon, 2016). The dispersion of cloud services may require a structure that can involve more than one legal judicial system, as it may sometimes concern more than one state. In this environment, it is still partially uncertain according to which state's laws and regulations the digital traces related to the evidences will be collected and how the coordination will be carried out. In order to combat crime effectively, it is necessary to collectively work on universal laws with international organizations, academic structures and commercial organizations.

RESULT

Before Industry 4.0, cyber-attacks were among the important problems for technology-based organizations and institutions. However, with Industry 4.0, these security issues have become more specific problems and the concept of automation has added new paradigms to security issues. As a result, the victimization of cyber threats has increased in general. In this context, together with the changes expected to occur on the basis of Industry 4.0, the followings can be put forward;

– Thanks to the Internet of Things, each object's being open to the network connection will provide production maximization, but may also cause security flaws,
– With the concept of big data, the demand status in the presence of smart factories, the importance of the analysis of the data regarding production and marketing will increase,
– Storing big data collected over the Internet of Things in cloud systems in physical or virtual environments may cause security flaws,
– The importance of cryptology will increase with the measures taken for increasing data security,
– The data analyses performed by the security teams at a minor level will reach a major level with the concept of big data and security teams are currently not sufficient to work in this field (receiving image on big data will be very difficult and costly, since performing analysis on the data without receiving image has different risk elements, the topic remains uncertain.),
– The items, which have the Internet of things technology, have more potential than the physical traces in terms of forensics for the solution of the crime,
– New cyber risks that enable destruction by remotely commanding for production lines and digital supply networks connected to automation system can emerge,
– With the gradual removal of the boundaries between the real and virtual world, the areas known as cyber-physical production systems (CPS) will become more blurred,
– A security flaw that can occur in production plants will provide some terrorist organizations, which have the concern of finding a place for themselves in the society, with the opportunity to take cyber terrorism actions,
– In case that the cloud storing services are given to the companies operating in different countries, a structure that can include more than one nation-state judicial system will be required since the forensic analysis to be performed on the cloud storing data will be a concern to more than one state,
– In parallel with the constant change of the technology, the technical information need of the security teams will increase day by day, cybercrimes will become more complicated and the solution will become more difficult.

In the analysis performed, it is clear that Industry 4.0, which aims at production maximization, will cause security problems with its current situation. Currently, our industry is between Industry 2.0 and Industry 3.0. Within this scope, it is essential to enhance the technical background of the security teams in order to prevent the crimes that may occur in the future. It is expected that the most appropriate action type of security teams is the security-focused defence understanding. Within the framework of this understanding, a proactive attitude should be exhibited and approaches similar to the ones used by cybercriminals should be adopted. In today's world where the technology changes rapidly, it should be considered that a statical defence understanding cannot be accepted and security teams should adopt a dynamic cybercrime intervention policy in order to fight against new threats.

REFERENCES

Aggarwal, D., Brennen, G. K., Lee, T., Santha, M., & Tomamichel, M. (2017). Quantum attacks on Bitcoin, and how to protect against them. Ledger, 3(3), 1-21.

Al Mazari, A., Anjariny, A. H., Habib, S. A., & Nyakwende, E. (2018). Cyber terrorism taxonomies: Definition, targets, patterns, risk factors, and mitigation strategies. In *Cyber Security and Threats: Concepts, Methodologies, Tools, and Applications* (pp. 608-621). IGI Global.

Aljawarneh, S. A., Alawneh, A., & Jaradat, R. (2017). Cloud security engineering: Early stages of SDLC. *Future Generation Computer Systems*, *74*, 385-392.

Assunção, M. D., Calheiros, R. N., Bianchi, S., Netto, M. A., & Buyya, R. (2015). Big Data computing and clouds: Trends and future directions. *Journal of Parallel and Distributed Computing*, *79*, 3-15.

Bendel, O. (2015). *Chancen und risiken 4.0*. Unternehmerzeitung, 2(21), 35.

Botta, A., De Donato, W., Persico, V., & Pescapé, A. (2016). Integration of cloud computing and internet of things: a survey. *Future generation computer systems*, *56*, 684-700.

Chen, B., Wan, J., Shu, L., Li, P., Mukherjee, M., & Yin, B. (2017). Smart factory of industry 4.0: Key technologies, application case, and challenges. *IEEE Access*, *6*, 6505-6519.

Chen, H. (2017). Applications of cyber-physical system: a literature review. *Journal of Industrial Integration and Management*, *2*(03), 1750012.

Chiu, Y. C., Cheng, F. T., & Huang, H. C. (2017). Developing a factory-wide intelligent predictive maintenance system based on Industry 4.0. *Journal of the Chinese Institute of Engineers*, *40*(7), 562-571.

Gordon, S. (2004). Privacy: A study of attitudes and behaviors in US, UK and EU ınformation security professionals. Symantec White Paper.

Gordon, S., & Ford, R. (2002). Cyberterrorism?. *Computers & Security*, 21(7), 636-647.

Gubbi, J., Buyya, R., Marusic, S., & Palaniswami, M. (2013). Internet of Things (IoT): A vision, architectural elements, and future directions. *Future generation computer systems*, *29*(7), 1645-1660.

Harley, C. K. (2018). Reassessing the industrial revolution: a macro view. In *The British Industrial Revolution* (pp. 160-205). Routledge.

Hilse, L. G. (2014). Risks of ISIS-Cyber-Terrorism. *Larshilse*, 72, 16.

Hozdić, E. (2015). Smart factory for industry 4.0: A review. *International Journal of Modern Manufacturing Technologies*, *7*(1), 28-35.

Jin, X., Wah, B. W., Cheng, X., & Wang, Y. (2015). Significance and challenges of big data research. *Big Data Research*, *2*(2), 59-64.

Klingenberg, C., & Do Vale Antunes Jr, J. A. (2017). Industry 4.0: What Makes it Revolution. In *Predavanje na konferenci 24th International EurOMA conference Edinburgh: Inspiring Operations Management, Edinburgh* (Vol. 1, No. 5).

Lee, I., & Lee, K. (2015). The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, *58*(4), 431-440.

Lee, J., Ardakani, H. D., Yang, S., & Bagheri, B. (2015). Industrial big data analytics and cyber-physical systems for future maintenance & service innovation. *Procedia Cirp*, *38*, 3-7

Lee, J., Bagheri, B., & Kao, H. A. (2015). A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing letters*, *3*, 18-23.

Lillis, D., Becker, B., O'Sullivan, T., & Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. arXiv preprint arXiv:1604.03850.

Liu, Y., Peng, Y., Wang, B., Yao, S., & Liu, Z. (2017). Review on cyber-physical systems. *IEEE/CAA Journal of Automatica Sinica*, *4*(1), 27-40.

Mayer-Schönberger, V., Cukier, K. (2013). Big data. [electronic resource] : a revolution that will transform how we live, work, and think. Res. Manag.

Monostori, L., Kádár, B., Bauernhansl, T., Kondoh, S., Kumara, S., Reinhart, G., & Ueda, K. (2016). Cyber-physical systems in manufacturing. *Cirp Annals*, *65*(2), 621-641.

Morrar, R., Arman, H., & Mousa, S. (2017). The fourth industrial revolution (Industry 4.0): A social innovation perspective. *Technology Innovation Management Review*, *7*(11), 12-20.

Nguyen, H., Tran, K., Zeng, X., Koehl, L., Castagliola, P., & Bruniaux, P. (2019, July). Industrial Internet of Things, Big Data, and Artificial Intelligence in the Smart Factory: a survey and perspective.

Paelke, V. (2014, September). Augmented reality in the smart factory: Supporting workers in an industry 4.0 environment. In Proceedings of the 2014 IEEE emerging technology and factory automation (ETFA) (pp.1-4). IEEE.

Pereira, T., Barreto, L., & Amaral, A. (2017). Network and information security challenges within Industry 4.0 paradigm. *Procedia Manufacturing*, *13*, 1253-1260.

Rüßmann, M., Lorenz, M., Gerbert, P., Waldner, M., Justus, J., Engel, P., & Harnisch, M. (2015). Industry 4.0: The future of productivity and growth in manufacturing industries. *Boston Consulting Group*, *9*(1), 54-89.

Schluse, M., Priggemeyer, M., Atorf, L., & Rossmann, J. (2018). Experimentable digital twins—Streamlining simulation-based systems engineering for industry 4.0. *IEEE Transactions on Industrial Informatics*, *14*(4), 1722-1731.

Stearns, P. N. (2018). *The industrial revolution in world history*. Routledge.

Taute, B. (2017). Improving cybersecurity for industry. *CSIR Science Scope*, *12*(3), 52-55.

Thames, L., & Schaefer, D. (2017). *Cybersecurity for industry 4.0*. New York: Springer.

Tjahjono, B., Esplugues, C., Ares, E., & Pelaez, G. (2017). What does industry 4.0 mean to supply chain?. *Procedia Manufacturing*, *13*, 1175-1182.

Vaidya, S., Ambad, P., & Bhosle, S. (2018). Industry 4.0-A Glimpse. *Procedia Manufacturing*, 20, 233-238.

Vasilomanolakis, E., Daubert, J., Luthra, M., Gazis, V., Wiesmaier, A., & Kikiras, P. (2015, September). On the security and privacy of internet of things architectures and systems. In *2015 International Workshop on Secure Internet of Things (SIoT)* (pp. 49-57). IEEE.

Vogel-Heuser, B., & Hess, D. (2016). Guest editorial Industry 4.0–prerequisites and visions. *IEEE Transactions on Automation Science and Engineering*, *13*(2), 411-413.

Wan, K., Hughes, D., Man, K. L., Krilavicius, T. & Zou, S. (2011). Investigation of Composition Mechanisms for Cyber Physical Systems. *International Journal of Design, Analysis and Tools for Circuits and Systems*, *2*(1), 30-40.

Wang, S., Wan, J., Li, D., & Zhang, C. (2016). Implementing smart factory of industrie 4.0: an outlook. *International Journal of Distributed Sensor Networks*, *12*(1), 3159805.

Wangen, G. (2015). The role of malware in reported cyber espionage: A review of the impact and mechanism. *Information*, *6*(2), 183-211.

Wübbeke, J., & Conrad, B. (2015). 'Industrie 4.0': Will German Technology Help China Catch Up with the West?. *China Monitor*, *23*, 1-10.

Yin, S., & Kaynak, O. (2015). Big data for modern industry: challenges and trends [point of view]. *Proceedings of the IEEE*, *103*(2), 143-146.

Zhou, K., Liu, T., & Zhou, L. (2015, August). Industry 4.0: Towards future industrial opportunities and challenges. In *2015 12th International conference on fuzzy systems and knowledge discovery (FSKD)* (pp. 2147-2152). IEEE.

ANKLAV, EKSKLAV VE UÇ TOPRAKLAR-GÜVENLİK İLİŞKİSİ

Dr. Öğr. Üyesi Tarık DEMİR*

Öz

Uluslararası ilişkiler literatüründe "çevreleyen ülkenin etine saplanmış kıymık" ya da "ayakkabıdaki taş" şeklinde tanımlanan anklav ve eksklavlar dünya siyasi coğrafyasının "norm dışı bir anomalisi" ya da bir nevi "ilkel bakiyesi" olarak telakki edilmektedir. Coğrafi ve politik bir fenomen olarak anklav ve eksklavların hem kendisini çevreleyen ülke ya da ülkeler ile anavatan arasındaki ikili ilişkilerde hem de uluslararası ilişkilerde güvenlik politikaları bağlamında kendi toprak ve nüfuslarının boyutlarıyla gayrı mütenasip bir şekilde etkili oldukları görülmektedir. Dünya yüzeyindeki anklav ve eksklavlar hem siyasi ve ekonomik yapıları hem de boyut, nüfus ve konumları itibariyle birtakım farklılıklara sahip olmakla birlikte, güvenlik sorunlarına sebebiyet vermeleri bakımından birtakım benzerlikler de taşıdıkları görülmektedir. Bir başka deyişle Cebelitarık, Dağlık Karabağ, Cabinda ya da Kaliningrad örneklerinde olduğu gibi uluslararası alanda "bağımsız bir mekân-politik nesne kategorisi" olarak anklav ve eksklavlar her an aktif birer volkan haline gelebilmektedir. Dolayısıyla anklav ve eksklavların çoğu mikro sahaya ve birkaç bin nüfusa sahip olsalar bile bu antitelerin jeopolitik açıdan son derece önem arz ettikleri görülmektedir. Bu çalışmada anklav ve eksklavlar tanıtılmakta ve güvenlik kavramı ile olan ilişkisine açıklık getirilmektedir.

Anahtar Kelimeler: *Coğrafi Fragmanlar, Anklav, Eksklav, Uç Topraklar, Güvenlik.*

THE RELATIONSHIP BETWEEN SECURITY AND ENCLAVE, EXCLAVE AND PANHANDLE

Abstract

In international relations literature, the enclaves and exclaves can be considered as an anomalous objects and exception to the norm. It can be defined as a region separate from the main body of the state or a region that can only be reached by passing through the territory of another country or a region that is clearly incompatible of administrative and economical life. It clearly manifests itself as a region that contradicts the idea of a contiguous nation-state. In other words, enclaves and exclaves, as both geographical and political phenomena, are described in international relations literature as small splinters in the flesh of the surrounding country or a stone in one's shoe or archaic remnants and anomalous objects as an exception to the norm of world political geography. On the other hand, it can be stated that enclaves are irrelevant with the dimensions of their own land and population in terms of security policies both in bilateral relations between the countries surrounding them and the motherland and generally in international relations. In this context, enclaves and exclaves in the the world have some differences both in terms of their political, economical structures and their size, population and location, but they have similarities in terms of causing security problems. As in the examples of Gibraltar, Nagorno-Karabakh, Cabinda and Kaliningrad, enclaves can become active volcanoes at any time as an independent space-political object category in the international arena. Therefore, although most of enclaves or exclaves have a micro-area and a population of several thousand, it can be stated that these entities are extremely important for political geography. In this study, enclaves and exclaves are introduced and their relationship with the concept of security is clarified.

Keywords: *Geographical Fragment, Enclave, Exclave, Panhandle, Security.*

* İstanbul Gedik Üniversitesi, İİSB Fakültesi, Uluslararası İlişkiler Bölümü, Türkiye, tarikdemir80@yahoo.com, ORCID ID: https://orcid.org/0000-0003-4428-2751

Makale Geliş Tarihi: 17.10.2019 Makale Kabul Tarihi: 22.01.2020

GİRİŞ

Ülkesel topraklarla ilgili literatüre bakılırsa, coğrafi fragmanları her yazarın farklı şekilde sınıflandırdığı görülecektir. Hepsinin ortak noktası istisnai bir durum olmak üzere modern devletin ülkesel bütünlüğüne aykırı bir şekilde ortaya çıkan toprağa dayalı anomaliler olmasıdır. Dünya haritası dikkatle incelenirse birçok ülkenin sıradışı ya da sahası bölünmüş sınırları ihtiva eden sıradışı coğrafi fragmanlara sahip olduğu görülecektir. Buna ilaveten bu coğrafi fragmanların ihtilaflı toprak iddialarının ve uluslararası gerginliklerin konusunu da teşkil ettiği gözlemlenmektedir. Çalışmada bu sıradışı coğrafi fragmanlardan sadece anklav, eksklav ve uç toprakların güvenlik kavramı ile olan ilişkisi tetkik edilmeye çalışılmıştır.

Anklav, siyasi coğrafyada tamamen başka bir ülkenin sınırları dahilinde yer alan yabancı toprak parçasını tanımlamak için kullanılmaktadır. Eksklav ise siyasi olarak bağlı olduğu ülkeye coğrafi açıdan bağlı olmayan, bu bölge ile arasında başka bir yabancı ülke ya da ülkeler bulunan toprak parçasını ifade etmek için kullanılmaktadır. İlk bakışta anklavlar ve eksklavlar "doğal olmayan bir durum" olarak değerlendirilebilir. Devletin ana gövdesinden ayrı bir bölge ya da sadece başka bir ülkenin topraklarından geçilerek ulaşılabilecek bir bölge ya da idari ve ekonomik hayatla çok açık uyumsuzlukları olan bir bölge şeklinde tanımlanabilir. Açıkça belirli bir birleşik ulus-devlet fikrine karşıt gelen bir bölge şeklinde tezahür etmektedir. Uç topraklar ise bir ülkenin, başka ülke ya da ülkelerin topraklarının içerisine doğru uzanan dar ve uzun şerit şeklindeki toprak parçasına verilen isimdir. Özetle çalışmada anklav teorisi çerçevesinde anklav, eksklav ve uç topraklar ile güvenlik kavramı arasında var olduğu iddia edilen ilişki örnekler yoluyla ortaya konulmaya çalışılmıştır.

1. ÜLKE TOPRAKLARI KAVRAMI

1.1. Ülke Toprakları Kavramının Tanımlanması

Ülke toprakları kavramı ile neyin kastedildiğini açıklayabilmek ve bu kavramı muayyen hale getirebilmek için öncelikle modern devlet kavramına kısaca değinmek gerekir. Modern devlet sisteminin ürünü olan sınır, toprak ve egemenlik kavramları yaklaşık 16. yüzyılda Avrupa'da yaşanan siyasi gelişmelere kadar geri götürülebilir. Bu, Avrupa dışındaki toplumların kendi siyasi ve toprağa dayalı örgütlenme sistemlerine sahip olmadıkları anlamına gelmez. Ancak Avrupa kolonyal ve emperyal sisteminin Avrupa dışı unsurların siyasi ve teritoryal

düzenlemelerini geniş ölçüde etkilediği de ifade edilmelidir. Modern dünyayı şekillendiren devlet sisteminin temellerinin geniş ölçüde Avrupa'ya özgü siyasi ve coğrafi kavramlar olduğu ifade edilebilir. Bununla birlikte modern anlamda merkezileşmiş devlet olgusu yüzlerce yıllık bir sürede evrimleşerek meydana gelmiştir. Kısaca modern devlet öncesi sisteme değinmek gerekirse Ortaçağ Avrupası'nın siyaset, hukuk ve yönetim olguları karşılıklı hak ve sorumluluklara dayalı olan vassal-süzeren ilişkisinin şekillendirdiği feodal sistemin ürünleri olduğu ifade edilebilir. Bu sistem toprağın denetimi konusunda en tepede imparatorların, kralların ve papaların bulunduğu hiyerarşik ve tevarüse dayalı bir yapıyı vaz etmiştir. Ancak feodal toprakların miras yoluyla aktarılması ademimerkezi karmaşık karar alma ağının, teritoryal bütünlükten yoksun bitişik olmayan toprakların ve çakışan bölünmüş hanedanlıkların oluşmasına sebebiyet vermiştir. Bunun neticesinde genel olarak feodal mülkler arasındaki sınırlar bulanık ve girift bir görünüm sergileyecektir. Avrupa'nın sınırları "belirsizlik ve geçirgenlik" ile çizilecektir.

Avrupa'da feodal sistemin çöküşü ve modern devlet sisteminin ortaya çıkışı merkezi hükümetlerin siyasi ve ekonomik gücü elde etmesiyle belirginlik kazanacaktır. Kapitalizm ve sanayi devriminin bir ürünü olan merkezi devlet olgusunun milliyetçilik kavramıyla yakın ilişki içinde olduğu ifade edilebilir. Gerçekten de bir devletin siyasi sınırlarının etnik-kültürel sınırlar ile özdeşleştiği her bir modern ulus-devletin belirli bir hâkim grup tarafından oluşturulduğu ifade edilebilir. Böylece siyasi gücün tek bir hâkim ulusa dayalı merkezi devletin eline geçmesiyle birlikte sınırların kontrolü ve bu sınırların feodal sistemin "muğlak, esnek ve çakışan egemenlik" kavramının aksine teritoryal bütünlüğün öne çıktığı sınır belirlemeleri önem kazanacaktır (Diener ve Hagen, 2010, s. 5).

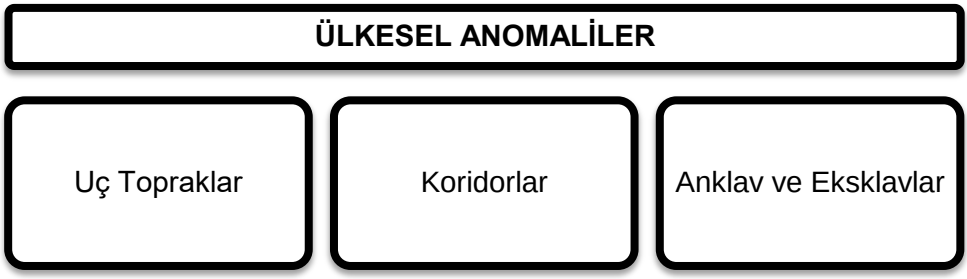
Emperyal genişlemenin bir sonucu olarak patlak veren Birinci Dünya Savaşı'nın sonrasında oluşan dramatik sınır düzenlemeleri de Avrupa'da sınır çatışmalarında artışa sebebiyet vermiştir. Askeri çatışma ihtimalini en aza indirmek amacıyla sınırların tayininde uygulanacak ölçüt konusunda bir dizi yaklaşım ortaya atılmış; ancak bu yaklaşımların çoğu doğal-yapay sınır dikotomisini aşamamıştır. Örneğin bir yazar bir devletin sınırının bitip diğerinin başladığı yerde herhangi bir doğal şekil yoksa bazı yapay sınır noktaları oluşturmak gerektiğini ifade etmiştir. Uluslararası sınırların tayininde dönemin yazarlarından kimisi doğal şekillere, kimisi jeopolitiğe kimisi de etnografik özelliklere önem atfetse de genel olarak yazarlar için doğal sınırların "iyi" buna mukabil yapay sınırların "kötü" olduğuna

dair bir inanç hâkim olmuştur. Ancak kısmen de olsa yazarların milliyetçi tarafgirliklerine ve objektif doğal sınırların tayini ve tanımlanmasındaki güçlüklerine rağmen, bazı yazarlar "bütün sınırların doğal güçlerin neticesinde değil; uzlaşımsal, öznel, insan kararlarının neticesinde oluştuğu" sonucuna varmışlardır. Örneğin Richard Hartshorne doğanın değil, insanın yaşayacağı yeri belirlediğini ve dolaysıyla "doğal ve yapay siyasi sınır ayrımını" bertaraf etmemiz gerektiğini ifade eder (Diener ve Hagen, 2010, s. 7-8). Jacques Ancel ise "sınırların siyasi bir izobar" olduğunu ileri sürerek güç mücadelesine dikkat çekmek istemiştir (Parker, 1994, s. 84).

1.2. Ülke Toprakları Kavramının Sınıflandırılması

Ülkesel topraklarla ilgili literatüre bakıldığında ülkesel fragmanları her yazarın farklı şekilde sınıflandırdığı görülmektedir. Ancak hepsinin ortak noktasının istisnai bir durum olmak üzere modern devletin teritoryal bütünlüğüne aykırı bir şekilde ortaya çıkan teritoryal anomaliler olmasıdır. Örneğin Martin Schwind ülkesel fragmanları, ülkesel anomaliler adı altında Caprivi Strip gibi uç topraklar, Danzig korridoru gibi koridorlar ve hem denizel hem de karasal olmak üzere anklav-eksklavlar olarak üç kısma ayırarak incelemiştir (Schwind, 1972, s. 37-39).

Tablo-1. Martin Schwind'e Göre Ülkesel Anomaliler (Schwind, 1972, s. 37)



Brendan White teritoryal fragmanların sınıflandırılmasında bir dizi değişken önermektedir. Bunlar karalar ile tecrit edilmişliğin derecesi, komşu bitişik birimlerin, fragmanı kapsayan siyasi birimlerin sayısı, fragmanın daha büyük bir siyasi birimini parçası olup olmaması gibi bir dizi değişkendir. White hukuki ve coğrafi çağrışımları ihtiva eden "bitişik olmayan topraklar" ibaresinin teritoryal süreksizliği tanımlamak bakımından daha kullanışlı olduğunu ifade etmektedir. Bu ifadeler bağlamında Vinokurov'un (2007, s. 47-49) aktardığına göre White tarafından ülkesel fragmanlar aşağıda gösterildiği şekilde sınıflandırılmıştır.

Tablo-2. Brendan White'a Göre Ülkesel Fragmanlar (2007, s. 48)

Alex Thomson ise *"An Introduction to African Politics"* isimli kitabında sömürgeci güçler arasındaki güç mücadelesine atfen sıradışılık ve hakemsel/uzlaşımsal sınır kavramlarına kıstas olarak almaktadır. Özellikle Afrika'da sömürgeci güçler arasındaki güç mücadelesine atfen bir tür anomali olarak gördüğü sıradışı teritoryal fragmanlardan uzlaşımsal sınır düzenlemeleri olarak bahsetmektedir. Bunun altında yatan neden ise *"arbitrary"* kelimesinin Batı dillerinde "hakemsellik/uzlaşımsallık" anlamını da ihtiva etmesinden kaynaklanmaktadır. Kelimenin Latince köküne bakıldığında *"arbitrium"* kelimesi "hakem kararı, yargı ve özgür seçim" anlamlarına gelmektedir (Marchant ve Charles, 1941, s. 49). Zaten Thomson (2010: 29) kitabının *"Glossory of Key Terms"* bölümünde "arbitrary boundaries" ifadesini "yerel ekonomik, sosyal veya politik gerçekliklerden çok emperyal çıkarları yansıtan devlet sınırları" olarak tanımlamıştır. Dolayısıyla Afrika kıtasında sınırlar genellikle ya iki taraflı hakem müesesesi ya da çok taraflı konferanslar yoluyla oluşturulduğu için uzlaşımsal ifadesinin kullanılması işlevsel olabilir. Ayrıca Thomson yukarıda zikredilen bölüm altında *"oddity"* kelimesini de kullanmaktadır. Bu da "tuhaflık, gariplik ve acayiplik" olarak çevrilebilir (Akdikmen, 1996, s. 363). Burada kastedilen şey ise çok temelde ülke sınırları bağlamında "normal olmayan durum" olgusudur. İşte sıradışılık olgusu da uzlaşımsal sınırların çiziminde ortaya çıkan "normal olmama" durumunu ifade etmektedir.

Tablo-3. Alex Thomson'a Göre Ülkesel Fragmanlar (2010, s. 14-15)

SIRADIŞI SINIR DÜZENLEMELERİ	
Uç Topraklar	Anklav ve Eksklavlar

2. ANKLAV, EKSKLAV VE UÇ TOPRAK KAVRAMLARI

2.1. Anklav ve Eksklavlar

2.1.1. Anklav ve Eksklavların Tanımlanması

Günlük kullanımda anklav tabiri farklı sosyal, kültürel, siyasi ve ekonomik fenomenleri tanımlamak için kullanılan bir kavramdır. Yani farklı sosyal, kültürel, siyasi ve ekonomik anklavların varlığından bahsedilebilir. Bu bağlamda anklav tabiri, mahiyeti itibariyle farklı fenomenler için *"tanımlanan"* konumunda bulunmaktadır. Tüm bu fenomen kategorileri için geçerli olmak üzere anklav *"bir antite ile onu kuşatan bir çevre arasındaki farka vurgu yapan bir kavram"* olarak tanımlanmaktadır (Nies, 2004, s. 20).

Siyasi coğrafyada, tamamen başka bir ülkenin sınırları dahilinde yer alan yabancı toprak parçasına anklav toprak denilmektedir (Encyclopedia Americana, 1967, s. 315). Eksklav ise, siyasi olarak bağlı olduğu ülkeye coğrafi açıdan bağlı olmayan, bu bölge ile arasında başka bir yabancı ülke/ülkeler bulunan toprak parçası olarak tanımlanmaktadır (Collin's Dictionary & Thesaurus, 1997, s. 302). Örneğin Şekil 1'de görüldüğü gibi B ülke parçası, A ülkesine göre anklav konumunda iken; B ülkesine göre eksklav konumdadır.

Şekil-1. Anklav ve Eksklav Ülke Toprakları

2.1.2. Anklav ve Eksklavların Sınıflandırılması

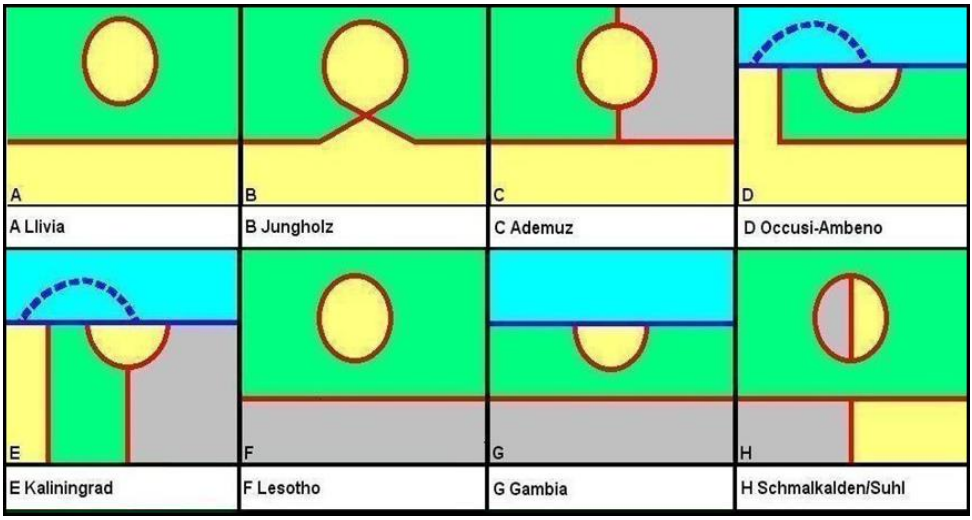
Anklavlar üzerine yapılan çalışmalar genellikle tanımlama ve sınıflandırma problemi üzerine odaklanmaktadır. Anklavlar, sınıflandırma kriterlerine bağlı olarak çok farklı şekilde sınıflandırlabilirler. Bu bölümde farklı yazarlara ait anklav tipolojileri tektik edilmiştir. Ancak konu itibariyle çalışma açısından sınıflandırmada "tip (konu) kriteri" esas alınmış ve bu bağlamda farklı tipteki anklavlar çalışma dışı tutulmak suretiyle sadece siyasi egemenliğe dayalı ülkesel (siyasi) anklavlar incelenmiştir. Ayrıca sınıflandırmada eksklav ülke toprakları, anklav başlığı altında incelenmiştir. Bu bağlamda aşağıdaki tablo ve şekiller, anklav/eksklav ülke toprakları kategorilerinin tanımlanmasında aydınlatıcı olacaktır.

Tablo-4. Vinokurov'a Göre Anklav ve Eksklavların Tipleri ((2007, s. 17)

Vinokurov'a göre teritoryal anklavlar (Bkz: Tablo-4) "egemen anklav devletler" "uluslararası anklav ve eksklavlar" ve "ulus-altı anklav ve eksklavlar" olmak üzere üç alt kategoride sınıflandırılmaktadır. "Egemen anklav devletler" de kendi içinde "egemen devletler" ile "yarım anklav egemen devletler" olarak üzere ikiye ayrılmaktadır. Egemen anklav devletlere örnek vermek gerekirse, tarihi olarak

Hong Kong ve Macao ile günümüzde ise Lesoto (Bkz: Şekil-2 F Bölmesi) San Marino ve Vatikan egemen anklav devletlere; Brunei, Gambiya (Bkz: Şekil-2 G Bölmesi) ve Monako devletleri de yarım anklav egemen devletlere örnek verilebilir.

Uluslararası anklav ve eksklavlar ise "gerçek anklav", "kıyı anklav", "mere-eksklav" ve "pene-anklav" olmak üzere dörde ayrılmaktadır: "Gerçek anklav", anklav tanımına uyan tek anklav türüdür (Bkz: Şekil-2 A Bölmesi). Kıyı anklavlara, egemen devlet şeklinde olmayan yarım anklav da denilebilir (Bkz: Şekil-2 D Bölmesi). Kıyı ankavların bir tarafı denize çıkışı bulunmaktadır. Dolayısıyla yarım anklav olarak tanımlanmasının sebebi denize çıkışı olmasıdır. Mere-eksklavlar ise sadece eksklav konumundadır. Yani kendini çevreleyen ülkelerle anklav ilişkisinde olmayıp sadece anavatan ile eksklav ilişkisi içindedir. Mere-eksklavlar kara temelli eksklav (Bkz: Şekil 2-C Bölmesi) ve denize çıkışı olan eksklav (Bkz: Şekil-2 E Bölmesi) olarak ikiye ayrılabilir. Son olarak pene-anklav ise ulaşılması zor bölgelerde ya da Alpler ve Pireneler gibi ulaşılması zor sıradağların doruk noktalarında görülür. Pene-anklavlardan anavatana sadece kendisini çevreleyen ülkenin üzerinden geçilerek ulaşılabilmektedir. Dolayısıyla pene-anklavlar teknik anlamda birer anklav olmamakla beraber, fonksiyonel özelliklerinden dolayı anklav sınıflandırmasında yer almaktadır.



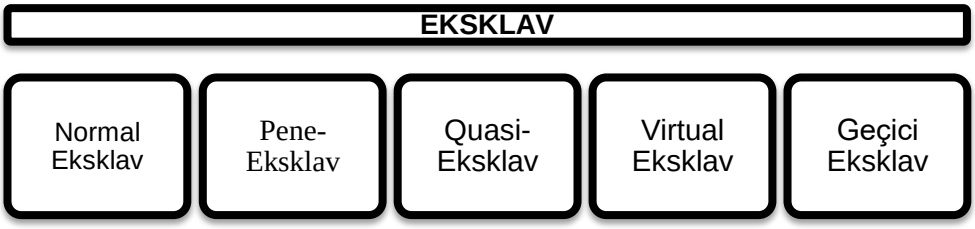
Şekil-2. Anklav ve Eksklav Kategorileri
(http://geosite.jankrogh.com/exclaves.htm)

Susanne Nies'e göre (Bkz: Tablo-5) ise anklav tipolojisi kökenlerine göre tasnif edilmiştir. Nies'in kökenlerine göre anklav tasnifi anklavların oluşma sebepleri ile de yakın ilişki içinde olduğu görülebilir. Nies'in köken tasnifine göre anklavların fetih, satın alma, miras ya da fesih yoluyla oluşabileceği ifade edilmektedir.

Tablo-5. Susanne Nies'e Göre Anklav Sınıflandırması[*]

Süha Göney'e göre (Bkz: Tablo-6) ise anklavlar, "eksklav" adı altında tasnif edilmiştir. Sahası bölünmüş devletler adı altında şu şekilde sınıflandırılmıştır: Normal eksklav tamamiyle diğer bir devletin sahası içinde kalmış ve etrafı çevrilmiştir. Bu gibi eksklavlar genellikle küçüktür. Belçika'da Hollanda'ya, Hollanda'da ise Belçika'ya ait çeşitli eksklavlar bulunmaktadır. Pene-eksklav ise bir ülkenin bazı kısımlarına tesadüf etmektedir. Bu kısımlar genellikle ulaşım güçlükleri sebebiyle ait olduğu devletin sahasından değil de, diğer ülkelerden geçen yollarla ulaşım sağlanmaktadır. Quasi-eksklav ise bazı teknik sebeplerden ötürü esas sahalarından ayrılmışlardır. Fakat gerçekte ülkesinin gerisinde kalan sahası ile sıkı ve tam bir ilişki içindedir. Virtual eksklavlar harhangi bir ülkenin içinde, hukuken bu devlete bağlı olmayan ve ayrı bir idareye sahip saha parçalarıdır. Son olarak geçici eksklav Batı Berlin örneğinde olduğu gibi bir devletin hükümranlık sahasının savaş sonucunda parçalanmasıyla ortaya çıkan eksklavlardır (Göney, 1993, s. 101-102).

Tablo-6. Süha Göney'e Göre Eksklav Listesi (1993, s. 101-102)



[*] Tablo eserdeki bilgiler doğrultusunda oluşturulmuştur.

Son olarak Dağlık Karabağ (Nagorno Karabakh) örneğinde olduğu gibi bu anklavın statüsü ve "quasi-anklav/eksklav" ile "devlet benzeri yapı" konusunda iltibasa mahal vermemek amacıyla kısa bir açıklama yapılması faydalı olacaktır. Dağlık Karabağ'ın uluslararası hukuk açısından nasıl bir statüye sahip olduğu doktrinde tartışmalı bir konudur. Hukuken Azerbaycan toprağı olmakla beraber 1993 senesinden beri Ermenistan'ın fiili işgali altında bulunan Dağlık Karabağ anklavı siyasi coğrafya ve anklav literatürüne ilişkin Batılı kaynaklarda anavatan konumundaki ülke olarak Ermenistan toprağı ve çevreleyen ülke olarak ise Azerbaycan gösterilmektedir. Dolayısıyla bu anklavın *de facto* bir anklav statüsüne sahip olduğu ifade edilmek zorundadır (Nies, 2004, s. 88).

Açıklama gerektiren ikinci husus konuya ilişkin literatürdeki bazı kaynaklarda Dağlık Karabağ'ın "devlet benzeri yapı" olarak tanımlanmasıdır. Devlet benzeri yapı "üzerinde hak iddia ettiği herhangi bir toprak üzerinde fiilen denetim sağlayıp da, hukuken uluslararası tanımadan yoksun kalan yapı" olarak tanımlanmaktadır. Dolayısıyla Dağlık Karabağ'ın quasi-anklav/eksklav tanımı dışında "devlet benzeri yapı" tanımı içinde de değerlendirildiği ifade edilmektir (Kolstø, 2006, s. 723). Dağlık Karabağ bir çeşit "öksüz, yetim anklav" olarak da tanımlanmaktadır (Nies, 2003, s. 112). Ayrıca anklavların sadece kara temelli fenomenler olmadığı ve bir ülkenin münhasır egemenlik alanında bulunan karasuları (12 deniz mili) içinde ya da sınırlı egemenlik yetkisine sahip olduğu bitişik bölge, münhasır ekonomik bölge (200 deniz mili), kıta sahanlığı ve balıkçılık bölgelerinde ya da bir göl veya akarsuda anklav oluşumlarına rastlanabileceği ifade edilebilir (Vinokurov, 2007, s. 33).

2.1.3. Anklav/Eksklav-Güvenlik İlişkisi

Bu bölüm altında anklav ve eksklavların güvenlik kavramı ile olan ilişkisi tarihi ve mevcut gelişmeler bağlamında ortaya konulmaya ve irdelenmeye çalışılmıştır. Daha önce de ifade edildiği gibi yerkürenin duyarlı ve stratejik noktalarında bulunan ülkesel fragmanların bir dizi güvenlik stratejisi neticesinde oluşmuştur. Bu noktada ülkesel fragmanların güvenlik kavramının farklı tezahürleriyle olan ilişkisinin, eşyanın tabiatı gereği coğrafyanın jeopolitik analizlerin esasını teşkil etmesi gerçeğinde yattığı görülebilir. Bir başka deyişle jeopolitiğin konusunun özel coğrafi koşullar içinde devletlerin kendi aralarındaki karşılıklı ilişkisi olduğu ifade edilebilir. Tarih boyunca coğrafya, ulusların ve imparatorlukların biribirleriyle çarpıştığı bir sahne olmuştur. Bu bağlamda coğrafya, en temel süreklilik unsuru olması hasebiyle uluslararası ilişkilerin en temel faktörü olagelmiştir. Bir devletin

coğrafyası, yani bir jeopolitik çevre içindeki coğrafi konum kendisine fırsatlar sunabileceği gibi birtakım kısıtlamaları da doğurabilir. Bu sebepten ötürü dış politika alanında coğrafya, bir devletin karar alıcılarını ve de dolayısıyla onların alacağı kararları şartlandırabilecektir (Sempa, 2002, s. 5).

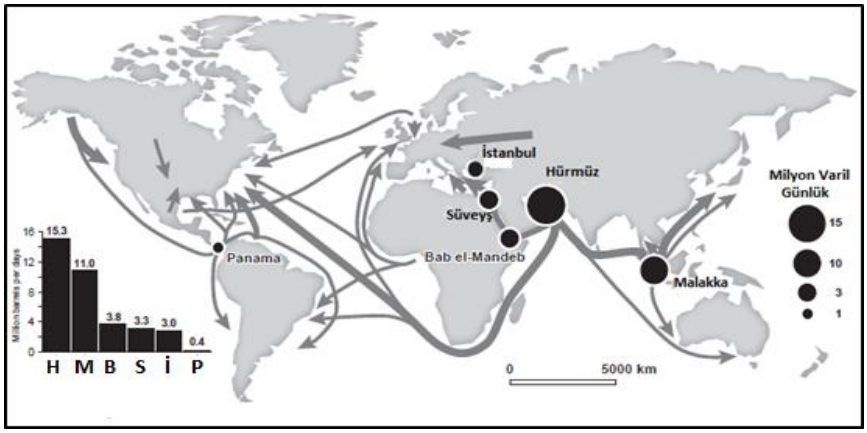
Görgül siyasi tarih incelendiğinde ülkesel toprakların güvenlik kavramıyla olan ilişkisinin çok farklı şekillerde tezahür ettiği görülebilecektir. Örneğin Cebelitarık, Musandam, Ceuta, Gwadar ve Panama gibi anklavlar hem stratejik suyolları üzerinde ya da enerji nakil hatlarının geçtiği güzergâhlar üzerinde bulunmakta hem de askeri güvenlik bakımından stratejik noktaları teşkil etmektedir. Örnekleri çoğaltılabilecek olan tüm bu görgül gerçekliklerin kendi bağlamları içerisinde ulaşım ve/veya enerji güvenliği ya da askeri güvenlik kavramlarıyla ilişkili olduğu ifade edilebilir. Ancak burada doğal olarak ulaşım, enerji güvenliği ve askeri güvenlik kavramlarının birbirleriyle; son tahlilde ise "ekonomik güvenlik" kavramıyla içsel bir ilişki içerisinde olduğu da ifade edilmelidir. Şöyle ki; anklavların özellikle kolonyal dönemden itibaren belli başlı güçlerin ulaşım yollarını hâkimiyet altına almak için giriştikleri mücadelelerin neticesinde oluştuğu ifade edilebilir. Günümüzde de anklavların ya zengin enerji kaynaklarına sahip olmaları ya deniz ticaretinin emniyetli bir şekilde gerçekleştirilmesi ya da enerji nakil hatlarının geçtiği güzergâhlarda bulunmaları hasebiyle jeopolitik etki faktörü olarak işlev görmekte oldukları gözlemlenmektedir. Bu noktada enerji güvenliğinin bizatihi tanımı güvenliğin tezahürleri arasındaki içsel ilişkiyi ortaya koymaktadır. Örneğin enerji güvenliği kısaca *"yeterli miktarlardaki enerji kaynaklarına, tutarlı fiyat ve istikrarlı bir kaynaktan, fiili olarak tehdit altında olmayan boruhattı, uygun deniz yolları ve benzeri ulaşım imkânları vasıtasıyla ve adil dağılım çerçevesinde erişilebilmesi"* şeklinde tanımlanmaktadır (Sevim, 2012, s. 4386). Dolayısıyla enerji güvenliği bağlamında enerji kaynakları, boruhatları ve deniz yolları ibarelerinin birbirleriyle olan ilişkisi göze çarpmaktadır.

Bu noktada anklav-güvenlik ilişkisi bağlamında ulaşım güzergâhları kavramı önem arz etmektedir. Esasen tarih boyunca uluslararası ilişkilerin doğasını ticaret, askeri çatışmalar ve bilgi alışverişi teşkil ettiği için coğrafya ve teknolojinin belirlediği ulaşım hatları üzerinden gerçekleşmektedir. Bir başka deyişle ulaşım hatları uluslararası ilişkilerin vuku bulduğu yerkürenin sinir sistemini teşkil etmektedir (Grygiel, 2006, s. 26). Özellikle yarım anklavların stratejik deniz ulaşım hatları üzerinde bulunmaları bu argümanı güçlendirmektedir. Özellikle de küresel ekonominin en stratejik kaynağı petrolün üçte ikisinin bu deniz ulaşım hatları

üzerinden nakledildiği düşünülürse anklavların stratejik önemi ortaya çıkmaktadır. Özellikle bazı yarım anklavların deniz ulaşım hatlarının geçtiği güzergâh üzerindeki bazı boğaz, geçit ve düğüm/tıkanma noktaları üzerinde bulunmasının rastlantısal bir durum olmadığı ifade edilebilir.

Bunun dışında deniz ulaşım hatları üzerinde bulunan birçok tıkanma noktasının siyasi açıdan istikrarsız devletlerin bulunduğu noktalara yakın konumda bulunması ulaşım güvenliğini tehdit etmektedir. Ayrıca terör tehdidi de ulaşım güzergâhlarının korunmasını daha da elzem hale getirmektedir. Tıkanma noktaları gerçekten de küresel ekonominin "coğrafi bakımdan Aşil topuğunu" teşkil etmektedir (Rodrigue, 2004, s 357). Bu noktanın da anklavların güvenlik kavramıyla olan ilişkisini ortaya koyduğu ifade edilebilir.

Enerji güvenliği ile deniz güvenliği arasındaki ilişkide ham petrolün yükleme ve boşaltma terminal limanları ile terminal arasındaki deniz ulaşım güzergâhlarının boğaz, geçit ve kanallar ile tıkanma noktalarının güvenliğinin kritik öneme sahip olduğu ifade edilebilir. Günümüzde deniz trafiğinde stratejik olarak kabul edilen ve herhangi bir sebeple kapanması halinde uluslararası enerji güvenliğine büyük zarar verme potansiyeline sahip altı farklı tıkanma noktasının bulunduğu ifade edilebilir. Bu noktaların Hürmüz Boğazı, Malacca Boğazı, Süveyş Kanalı, Babülmendeb Boğazı, İstanbul-Çanakkale Boğazları ile Panama Kanalı olduğu görülmektedir (Sevim, 2012, s. 4388). Bu noktada Hürmüz Boğazı'nda bulunan Musandam anklavı ile tarihi anklavlardan Panama ve Gwadar coğrafi konumlarının enerji ve ulaşım güvenliği bağlamında kritik önem arz ettiği gözlemlenebilir.



Harita-1. Tıkanma Noktaları (Rodrigue, 2004, s. 364)

Anklav-güvenlik ilişkisi bağlamında güvenliğin bir başka tezahürü Kaliningrad anklavı örneğinde görülebilir. Kaliningrad'ın önemi hem stratejik bir enerji güzergâhı üzerinde bulunmasından ve aynı zamanda kendisinin de hidrokarbon kaynaklarına sahip olmasından hem de askeri güvenlik kavramı bağlamında jeostratejik bir konuma sahip olmasından kaynaklanmaktadır. Şöyle ki; Kaliningrad anklavı Vyborg-Greifswald arasında inşa edilmiş olan Kuzey Akım boruhattının geçtiği güzergâh üzerinde bulunması hasebiyle stratejik öneme sahiptir (Oldberg, 2009, s. 365). Ayrıca anklav 10 milyon ton kanıtlanmış petrol rezervi D6 alanıyla birlikte dikkatleri üzerine çekmektedir. Bunun dışında SSCB döneminde Kaliningrad oblastı jestratejik konumda bulunmaktaydı.

Soğuk Savaş döneminde Baltık bölgesi Varşova Paktı-NATO eksenli mücadelenin (Bkz: Harita-2) en yoğun olarak yaşandığı bölgelerden birini teşkil etmekteydi. Özellikle Kaliningrad'ın Baltiisk limanı SSCB'nin Baltık filosu için kuzeyin donmuş sularından korunaklı bir liman işlevi görmekteydi. Anklav, Baltık filosu için günümüzde de aynı işlevini korumaktadır (Victor, 2006, s. 21). Bunun dışında askeri bakımdan Kaliningrad Rusya açısıdan Avrupa'ya konuşlandırılması düşünülen NATO füzesavar savunma sistemlerine karşı alınacak önlemler konusunda işlevsel bir mekân olarak da göze çarpmaktadır. Bu önlemler arasında Rus balistik füzelerinin uzun vadeli perspektif bağlamında donatılması Rus silahlı kuvvetlerinin Amerikan füzesavar savunma sistemlerinin enformasyon ve gönderim araçlarının tahribatına karşı hazırlanması ve Kaliningrad Oblastı'nda "İskender" füze kompleksinin konuşlandırılması sayılabilir (Altuhov, 2011, s. 81).

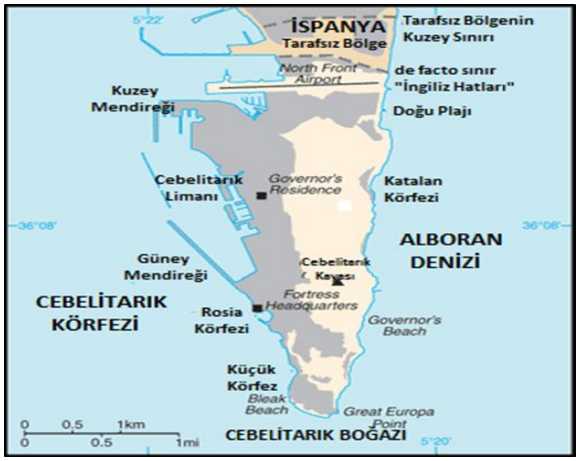
Harita-2. Baltık Bölgesi ve Kaliningrad (Archer ve Etzold, 2010, s. 330)

Anklav-güvenlik ilişkisinin görülebileceği bir diğer anklav ise petrol kaynakları bakımından zengin Angola'nın Cabinda anklavıdır. Cabinda anklavı "Batı Afrika'nın Kuveyti" (Bkz: Harita-3) olarak adlandırılmaktadır. Cabinda'dan günde 1 milyon varil petrol pompalanmaktadır. Petrolün bulunduğu ilk günden itibaren petro-kapitalizmin ve buna bağlı olarak da petro-şiddetin tesiri altında kalan Cabinda anklavı Amerikan petrol şirketlerinin tekeli altına girmiş ve ülke Cabinda menşeli ayrılıkçı hareketlerin yaşandığı istikrarsız bir bölge haline gelmiştir. Günümüzde ise Cabinda anklavı ABD-Çin rekabetinin yaşandığı bir bölge konumundadır (Maxted, 2006, s. 35). Şöyle ki; Çin'in petrol ihtiyacının %30'unu Afrika kıtası karşılamaktadır. Angola'nın bu ticaretteki payı Afrika'dan yapılan petrol ithalatının yarısını teşkil etmektedir. Dolayısıyla Cabinda'nın Çin'in enerji güvenliği ile olan ilişkisi açığa çıkmaktadır (Alpay, 2009, s. 13).

Harita-3. Cabinda Anklavı (https://www.cia.gov/library/publications/the-world-factbook/maps/maptemplate_ao.html)

Güvenlik kavramıyla irtibatlandırılabilecek olan bir diğer anklav ise İngiltere'nin Cebelitarık anklavıdır. 1704 senesinden bugüne İngiltere'nin denizaşırı topraklarından birini teşkil eden "kaya gibi sağlam" Cebelitarık anklavının (Bkz: Harita-4) Akdeniz'de sahip olduğu jeostratejik konumuyla tarih

boyunca çeşitli güçlerin özellikle de İspanya ile İngiltere arasındaki egemenlik mücadelesine sahne olduğu ifade edilebilir (Lambert, 2005, s. 206).



Harita-4. Cebelitarık Anklavı (https://www.cia.gov/library/publications/the-world-factbook/geos/gi.html)

Anklavların güvenlik kavramıyla olan ilişkisinin güvenliğin farklı tezahürleri üzerinden gerçekleşebileceği görülebilmektedir. Yukarıda zikredilen örneklere ilaveten anklavların mevcudiyeti Ceuta, Melilla, Fergana Vadisi ve Hindistan/Bangladeş anklavları örneklerindeki gibi sınır/geçiş ve göç sorunlarına sebebiyet verebileceği gibi *de facto* anklavlardan Gazze ve Dağlık Karabağ örneklerinde olduğu gibi donmuş çatışmaların konusunu teşkil edebileceği görülebilmektedir.

2.2. Uç Topraklar

2.2.1. Uç Toprak Kavramının Tanımlanması

Uç topraklar (şeritler) daha önce bir ülkenin, başka ülke ya da ülkelerin topraklarının içerisine doğru uzanan dar ve uzun şerit şeklindeki toprak parçası olarak tanımlanmıştı. Bu tür topraklar genellikle ekonomik gelişme ve askeri güvenlik yönünden sakıncalı bir toprak biçimi olarak nitelendirilmekle birlikte Alman coğrafyacılar tarafından bu tür topraklara ilerlemenin ileri uçları anlamına gelen *"wachstumspitzen"* tabiri kullanılmaktadır. Dolayısıyla bu şekildeki toprakların sakınca doğurmaktan çok saldırıya yarayan bir durum da arz ettiği ifade edilmektedir (Günel, 2002, s. 55).

Almanlar tarafından yayılmanın ileri uçları şeklinde ifade edilen uç topraklar kavramı, aynı şekilde Anglosakson literatüründe de askeri bir terminoloji olarak düşman topraklarına doğru oluşan "çıkıntı" (salient) şeklinde ifade edilmektedir (https://www.worldatlas.com/articles/what-is-a-panhandle.html).

Bu noktada çoğunlukla karıştırılan uç topraklar ile koridorlar arasındaki farka değinilmesi açıklayıcı olacaktır. Eğer yukarıda da ifade edildiği gibi ileri gelişme noktaları başka bir bölge ile temas sağlama amacını güdüyorsa bu tip uç topraklara gerçek anlamda koridor adı verilmektedir. Bu bağlamda gerçek anlamda koridorlara Polonya'nın eskiden Baltık Denizi ile bağlantısını kuran Danzig Koridoru ile Finlandiya'nın Kuzey Buz Denizi ile bağlantısını sağlayan ancak II. Dünya Savaşı'ndan sonra SSCB tarafından ilhak edilen Petsamo Koridoru örnek olarak verilebilir (Günel, 2002, s. 57).

2.2.2. Uç Topraklar-Güvenlik İlişkisi

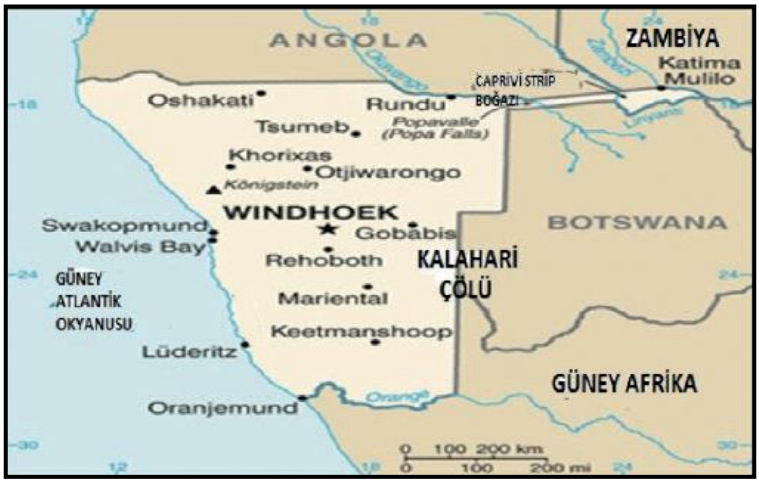
Uç topraklara ise Namibya sınırındaki Caprivi Strip (Bkz: Harita-5) ve Afganistan (Bkz: Harita-6) sınırındaki Vahan (Pamir) Vadisi örnek olarak verilebilir[*]. Bu örnekler mukayese edildiğinde böylesi bir teritoryal anomalinin bir bilincin ürünü olduğu apaçık ortada durmaktadır. Caprivi Strip uç toprağı için Namibya haritasına bakılırsa Namibya topraklarının kuzeydoğuya doğru Zambiya ile Bostwana toprakları arasında bir çıkıntı yaptığı görülebilecektir. Böylesi bir coğrafi anomalinin oluşturulmasının altında yatan neden stratejik gerekliliklerden kaynaklanmaktaydı. Kısaca bu anomaliler hakkında bilgi vermek gerekirse şunlar ifade edilebilir: Dönemin Alman Dışişleri Bakanı Kont von Caprivi mücadele içinde olduğu diğer sömürgeci güçlere karşı gambot diplomasisi uygulayabilmek için Zambezi Nehri'ne çıkış elde etmesi gerektiğinin bilincindeydi (Thomson, 2010, s. 14).

Dolayısıyla Caprivi Strip 1 Temmuz 1890 tarihli "Heligoland-Zanzibar Antlaşması" ile Almanların eline geçmiştir. Bu antlaşma ile Almanya da daha önce işgal etmiş olduğu Zanzibar'ı İngiltere'ye devretmiştir. Burada İngiltere'nin bu bölgeyi Almanya'ya devretmesinin altında yatan neden ise yükselen Rus tehdidi dolayısıyla İngiltere'nin Almanya ile ittifak arayışı içinde olmasıydı (Armaoğlu, 2007: 420). Ayrıca Almanya açısından bu bölgenin önemi Zambiya'nın ve Kongo'nun Katanga (Şaba) bölgesinin zengin bakır yataklarını elde etmek için bir köprübaşı olarak kullanmak istemesi de amaçları arasında olabilir. Dolayısıyla

[*] Vahan ve Caprivi Strip uç toprakları bazı kaynaklarda koridor adı altında da tanımlanmaktadır (y.n).

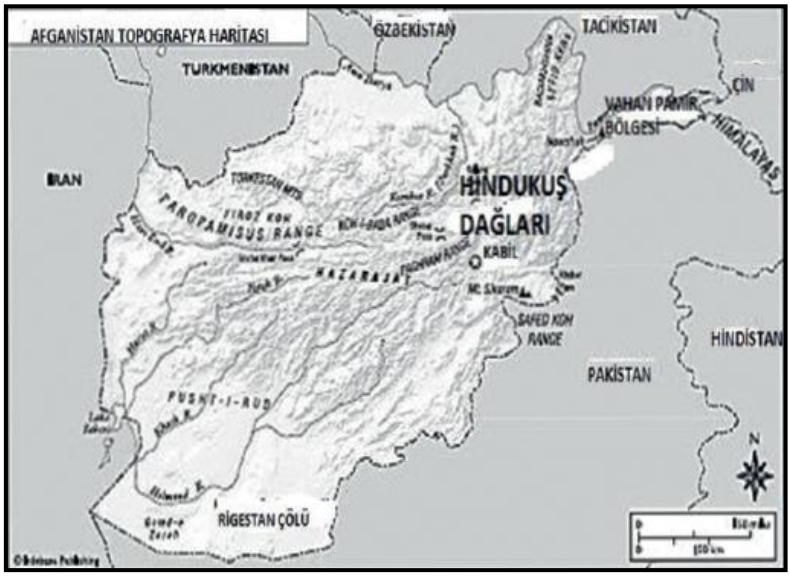
Zambezi Nehri'nin ve Lusaka ile Livingstone'u birbirine bağlayan stratejik önemi haiz demiryolları hattının mevcudiyeti Almanlar açısından Kongo'nun ve Zambiya'nın zengin bakır kaynaklarına erişimi konusunda önem arz eden bir coğrafya olduğu sonucuna ulaşılabilir (Dale, s. 485).

Ülkesel bir anomali örneği olarak Caprivi Strip uç toprağı Soğuk Savaş döneminde yaşanan Güney Afrika-Namibya çatışmasında da stratejik bir rol oynamıştır. Caprivi Strip bölgesi özellikle BM tarafından Namibya üzerindeki Güney Afrika'nın vesayetinin kaldırılmasına rağmen; Güney Afrika birliklerinin bu topraklardan çıkmaması üzerinde 1980'lerde yaşanan SWAPO ile Güney Afrika hükümet güçleri arasındaki savaşta stratejik bir bölge olarak önemli bir rol oynamıştır. Çünkü bölge birçok ülkeye geçiş sağlaması açısından coğrafi açıdan anahtar bir rol oynamıştır. Özellikle Güney Afrika SWAPO birlikleri ile olan mücadelesinde güney Angola'dan gelen gerillaların burada üslenmesi üzerine bu bölgeye askerlerini yollamış ve bu bölgede şiddetli çatışmalar yaşanmıştır (Boyd ve Comenetz, 2007, s. 102). Ayrıca günümüzde Caprivi Strip bölgesi Namibya açısından komşularıyla başka sorun ve çatışmaların kaynağını da teşkil etmektedir. Örneğin Angola-Namibya sınırı boyunca Popa Şelalesi üzerinde yapılacak olan hidroelektrik santralinin Bostwana'nın Okavango Deltası ekolojisini ve insan yerleşmesini etkilemesi iki ülke arasında anlaşmazlık noktasını oluşturmaktadır (https://www.cia.gov/library/publications/the-world-factbook/geos/wa.html).



Harita-5. Caprivi Strip Uç Toprağı (https://www.cia.gov/library/publications/the-world-factbook/maps/maptemplate_wa.html)

Namibya'nın Caprivi Strip bölgesinin oluşturulmasında gözlemlenen ve Almanya, İngiltere ve Portekiz arasında yaşanan mücadelenin ve jeopolitik kaygıların bir benzeri, 19. yüzyılda İngiltere ile Çarlık Rusya arasında Büyük Oyun adı verilen güç mücadelesinde ve Afganistan'ın Vahan-Pamir Knot bölgesinde oluşturulan statükoda da görülebilir. Caprivi Strip bölgesiyle Vahan-Pamir Knot bölgesi arasında böylesi bir mukayesenin yapılmasının nedeni sıradışı fragmanların oluşturulmasında ve anomali ihtiva eden sınırların tesisinin altında yatan ana nedenin jeopolitik kaygılar olduğu gerçeğinin ortaya konulmak istenmesidir. İki farklı coğrafyada tesis edilen benzer sıradışı fragmanların ve benzer jeopolitik kaygılardan kaynaklanan güç mücadelesinin çalışmada serdedilen iddiayı güçlendirdiği ifade edilebilir (Wahab ve Youngerman, 2007, s. 3).

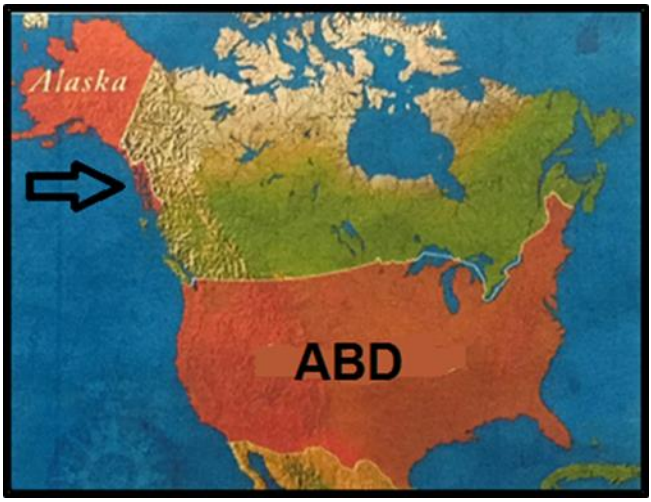


Harita-6. Vahan Pamir Bölgesi Uç Toprağı (Wahab ve Youngerman, 2007, s. 2)

Bunun dışında kendisi de aynı zamanda bir anklav toprağı olan Alaska'nın Kanada sınırı boyunca uzanan uç toprakları (Bkz: Harita-7) da ilginç bir örnek olarak verilebilir. Tarih boyunca önce Rusya ile İngiltere, 1867 tarihinde Rusya tarafından satıldıktan sonra da ABD ile İngiltere arasında Pasifik Okyanusu'na çıkış konusundaki mücadele bağlamında Alaska'nın uç toprakları jeopolitik ve jeostratejik öneme sahip olmuştur. Zira Alaska bu önemine binaen 1867-1884 tarihleri arasında Amerikan Savunma Bakanlığı'nın yetkisi altında kalmıştır (Turovsky, 2006, s. 147).

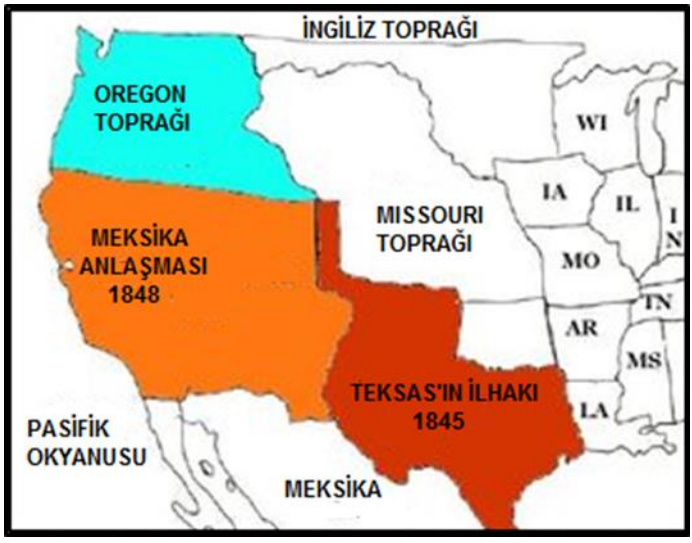
Ruslar, Asya Kıtası'ndaki genişlemesinden sonra Alaska toprakları üzerinden Amerika Kıtası'na geçiş yapmış ve buradan da İngiltere'nin egemenliğindeki Kanada'nın Pasifik kıyısındaki toprakları boyunca güneye doğru bugünkü ABD topraklarına doğru yayılım göstermiştir. Rusların Pasifik kıyısı boyunca böyle bir uç toprak formasyonu oluşturmasının altında yatan sebebin İngilizlerin Pasifik Okyanusu'na çıkışını ve coğrafi/jeopolitik bütünlüğünü tesis etmesini engellemek olduğu ifade edilebilir.

Başkan James K. Polk döneminde *Manifest Destiny* doktrini gereği genişleme stratejisine hız verilmiş ve ABD Pasifik kıyısına ulaşıp coğrafi/jeopolitik bütünlüğüne ulaşabilmek amacıyla önce 1846 tarihli Oregon Antlaşması (Bkz: Harita-8) ile İngilizlerden Oregon, daha sonra da 1848 tarihinde (Bkz: Harita-9) Meksika'dan bugünkü California topraklarını ele geçirmiştir (http://projects.leadr.msu.edu/usforeignrelations/exhibits/show/manifest-destiny /oregon-treaty-1846). Nitekim tüm bu gelişmeler 1867 tarihinde Alaska topraklarının satın alınması birlikte düşünüldüğünde yeni oluşturulan Pasifik eyaletleri ile Alaska topraklarının birleştirilip İngilizlerin tıpkı Rusların yaptığı gibi Pasifik Okyanusu'na çıkışının engellenmesinin amaçlandığı sonucuna varılabilir.



Harita-7. Alaska Uç Toprakları (Victor, 2006, s. 51)

Harita-8. Oregon Antlaşması (1846) (http://projects.leadr.msu.edu/usforeignrelations/exhibits/show/manifest-destiny/oregon-treaty-1846)



Harita-9. California Topraklarının Meksika'dan Alınması (1848) (http://hlaoo1980.blogspot.com/2016/03/stolen-mexican-territories-retaken-by.html)

Uç topraklara bir diğer kayda değer örnek olarak Ermenistan'ın Zengezur bölgesi verilebilir. Bu uç toprakların oluşmasının temel sebebi Rusya'nın

genişleme stratejisinin bir özelliği olarak enlemsel ittifakları engellemek; buna mukabil boylamsal ittifakları geliştirmek istemesidir. Nitekim bu minvalde Rusya, Balkanlar'dan başlayıp Orta Asya'ya kadar uzanan Türk coğrafyasının topraksal irtibatını ve enlemsel ittifakını kesmek amacıyla Azerbaycan'a ait Zengezur bölgesini Ermenistan'a vermiştir.

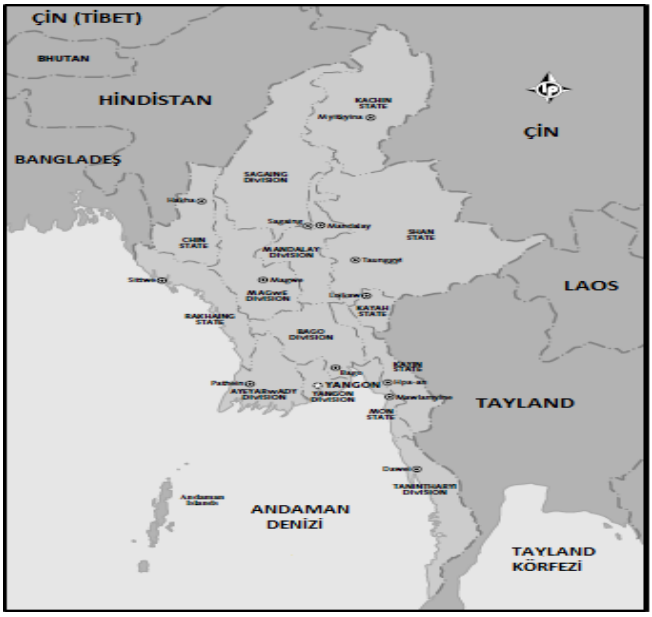
1917 ile 1921 tarihleri arasında Azerbaycan, Ermenistan ve Gürcistan'ın kısa süreli bir bağımsızlık dönemleri olmuştur. Transkafkasya ülkelerinin bu bağımsızlıklarından sonra Bolşeviklerin tam anlamıyla iktidarı ele geçirmeleri ile birlikte Azerbaycan'ın statüsü Ekim 1921 tarihinde SSCB ile imzalanan Kars Antlaşması ile bağıtlanmış ve Azerbaycan 1922 tarihinde Sovyetler Birliği'nin bir cumhuriyeti haline gelmiştir (Swietochowski, 1996, s. 148). Bolşevikler Kasım 1920 senesinde Transkafkasya'ya girdiklerinde Nahçıvan, Karabağ ve Zengezur bölgelerinin Ermenilere verilmesini kararlaştırmıştır. Ancak bu karar 1921'de değiştirilmiş; Nahçıvan ve Karabağ Azerilere verilmiştir. Böylelikle Nahçıvan Özerk Cumhuriyeti, Azerbaycan Sovyet Sosyalist Cumhuriyeti'nin bir parçası olmuştur. Ancak Azeriler ile Ermeniler arasında bir denge unsuru olarak ve Azerbaycan'ın Türkiye ile kara bağlantısını kesmek amacıyla Zengezur bölgesi (Bkz: Harita-10) SSCB tarafından tamamen Ermenilere bırakılmıştır (Hunter, 1997, s. 444).

Harita-10. Ermenistan ve Zengezur Bölgesi Uç Toprakları
(https://www.britannica.com/place/Armenia/Settlement-patterns#ref481302)

Uç topraklara bir diğer örnek olarak Myanmar'ın (Burma/Birmanya) Malay Yarımadası'nda bulunan Tenasserim (Tanintharyi) Bölgesi (Bkz: Harita-11) verilebilir. İngiliz idaresinde iken Malay Yarımadası'ndaki Tenasserim adı verilen dar kıyı şeridi güneye doğru yayılmayı sağlamak amacıyla oluşturulmuştur (Günel, 2002, s. 57). Myanmar ile Tayland arasındaki uzun bir mücadeleden sonra bölge 18. yüzyılın sonlarında Myanmar'a verilmiştir. Tenasserim, Anglo-Burma Savaşı'ndan (1824-26) sonra İngilizler tarafından ele geçirilen ilk bölgeydi. İngilizlerin Bengal Körfezi'nde ve dolayısıyla Hindistan üzerinde hegemonya kurabilmek amacıyla bu bölgeyi ele geçirmeyi istediği görülmektedir.

19. yüzyılla birlikte İngilizlerin Hindistan'daki yayılması Güneydoğu Asya'ya doğru bir yönelim göstermeye başlamıştır. İngilizler Malay Yarımadası'nın güneyinde bulunan Penang'da ve Singapur'da üsler elde etmiş ve yarımada boyunca etkisini artırmaya başlamıştır. 1820'li yıllarla birlikte İngilizler, Siyam Krallığı (bugünkü Tayland) ile bölge üzerinde bir güç mücadelesine girişmiştir. Aynı anda İngilizler Burma Krallığı ile de bir çatışmaya girmiş ve 1826 yılında Mon ve Arakan kıyılarını ele geçirmiştir. Dolayısıyla Burma Krallığı ile girişilen mücadele neticesinde Tenasserim Bölgesi'ne kadar olan kıyı şeridi denetim altına alınmıştır (Steinberg, 2010, s. 22).

Bu noktada İngilizlerin korkusunun Burma Krallığı'nın Bengal Körfezi'ni kontrol etmesi olarak tebarüz ettiği görülmektedir. Başlangıçta Siyam Krallığı Malay Yarımadası'nın en stratejik noktası olan Kra Kıstağı üzerindeki egemenliğini tekrar sağlayabilmek amacıyla eski düşmanları Burma Krallığı'na karşı İngilizlerin yanında yer almasına rağmen; Burma Krallığı'nın İngilizlere karşı yenilmesinin bölgede önemli sınır değişimlerini de beraberinde getireceğini anlamıştır (Baker ve Phongpaichit, 2014, s. 38). Başka bir deyişle İngilizlerin Tenasserim Bölgesi'ne kadar olan kıyı şeridi boyunca bir uç toprak oluşturmasının sebebi olarak güneyde daha önce ele geçirdiği Penang Bölgesi ile Tenasserim Bölgesi'ni birleştirmek suretiyle Malay Yarımadası üzerinde denetim tesis etmek olduğu çıkarsamasında bulunulabilir. Böylece İngilizler, Singapur ile Malay Yarımadası arasında bulunan ve önemli stratejik deniz ulaşım noktalarından biri olan Malacca Boğazı'nı kontrol edebilecek konuma gelmiştir.



Harita-11. Tenasserim (Tanintharyi) Bölgesi (Reid ve Grosberg, 2005, s. 51).

SONUÇ

Kolonyal dönemden günümüze siyasi tarih incelendiğinde ülkesel fragmanlardan anklav, eksklav ve uç toprakların güvenliğin farklı tezahürleri ile olan ilişkisi hemen göze çarpmaktadır. Bu bağlamda öncelikle mezkûr kavramlar arasındaki en önemli ilişki boyutunun enerji ve ulaşım güvenliği konusunda olduğu görülmektedir. Örneğin meseleye enerji jeopolitiği açısından bakıldığından çıkarılan hidrokarbon kaynakların enerji arz mahallerinden enerji talep mahallerine güvenli güzergâhlar üzerinden taşınmasında özellikle yarım anklavların önemli bir işlev gördüğü sonucuna ulaşılmıştır. Bu noktada bazı anklavların gerek enerji boruhatları ve deniz ulaşım güzergâhları üzerinde bulunması rastlantısal bir durum olmadığı ifade edilebilir. Özellikle de küresel ekonominin en stratejik kaynağı petrolün üçte ikisinin bu deniz ulaşım hatları üzerinden nakledildiği göz önünde getirildiğinde anklav ve eksklavların stratejik önemi ortaya çıkmaktadır. Dolayısıyla yarım anklavların deniz ulaşım hatlarının geçtiği güzergâh üzerindeki bazı boğaz, geçit ve tıkanma noktaları üzerinde bulunduğu sonucuna ulaşılmıştır. İkinci olarak anklav, eksklav ve uç toprakların sert güvenlik kavramı bağlamında askeri güvenlikle de irtibatlı olduğu ve özellikle de sahip oldukları jeopolitik ve

jeostratejik konumları dolayısıyla bu coğrafi fragmanların anavatan ve çevreleyen ülke/ülkeler tarafından dikkate alınması gereken unsurlar olarak telakki edildiği görülmektedir. Bu bağlamda coğrafi fragmanların boyutlarıyla gayrimütenasip oranda anavatan ve çevreleyen ülkenin genel ilişkilerine etki etme kapasitesine sahip olduğu sonucuna varılmıştır.

Çalışmada önemli anklav/eksklav alt başlığı altında örnek olarak tıkanma noktaları üzerinde bulunan Kaliningrad ve Cebelitarık anklavları ile hidrokarbon kaynakları bakımından zengin Cabinda anklavı incelenmiş ve bu coğrafi fragmanların güvenlik ile ilişkisine temas edilmiştir. Uç topraklar alt başlığında örnek olarak Alaska, Vahan (Pamir), Caprivi Strip, Zengezur ve Tenasserim uç toprakları incelenmiş ve bu coğrafi fragmanların güvenlik ile olan ilişkisine temas edilmiştir. Coğrafi fragmanlar ile güvenlik kavramı arasında mütekabil bir ilişkinin varlığı saptanmıştır. Bir başka deyişle hem belirli bir politik tutum neticesinde bu tür sıra dışı coğrafi fragmanların oluşturulduğu hem de stratejik öneme sahip belirli coğrafyaların devletleri böylesi sınır düzenlemeleri yapmalarına sebebiyet verdiği saptanmıştır. Kısaca politika coğrafyayı etkilerken coğrafyanın da politikayı etkilediği sonucuna varılmıştır.

KAYNAKÇA

Akdikmen, R. (1996). *Langenscheidt Standard İngilizce-Türkçe Sözlük*. İstanbul: İnkılâp Yayınları.

Altuhov, B. A. (2011). Anakonda Stratejisi ve Avrasyacılık (Geostrategiya "Anakonda" i Evraziya), L. V. Savin. (Ed.), *Geopolitika,* Moskova: Moskova Devlet Üniversitesi Sosyoloji Fakültesi Yayını, Moskova.

Alpay, Y. (2009). Çin Afrika'da Ne Yapıyor?. *TASAM-Stratejik Araştırmalar Dergisi*. Sayı: 14.

Archer, C. ve Etzold, T. (2010). The European Union and Kaliningrad: Taking the Low Road, Geopolitics, Alizade, 2010, Sayı: 15/2, 329-344.

Armaoğlu, F. (2007). *20. Yüzyıl Siyasi Tarihi*. İstanbul: Alkım Yayınları.

Baker, C. ve Phongpaichit, P. (2014). *A History of Thailand*. Melbourne: Cambridge Yayınları.

Collin's Dictionary&Thesaurus (1997).

Dale, D. E. (1968). Some Geographical Aspects of African Land-Locked States. *Annals of the Association of American Geographers.* Vol. (58/3).

Diener, A. C. ve Hagen, J. (2010). Introduction: Borders, Identity and Geopolitics. Alexander C. Diener and Joshua Hagen (Ed.), *Borderlines and Borderlands: Political Oddities at the Edge of Nation-State.* New York: Rowman&Littlefield Publishers.

Encyclopedia Americana (1967). Vol: 10. New York: Americana Corporation.

Göney, S. (1993). *Siyasi Coğrafya.* Cilt II. İstanbul: İÜ Basımevi ve Film Merkezi.

Grygiel, J. J. (2006). *Great Powers and Geopolitical Change*. Baltimore: The John Hopkins University Press.

Günel, K. (2002). *Coğrafyanın Siyasal Gücü*. İstanbul: Çantay Kitabevi.

http://geosite.jankrogh.com/exclaves.htm Erişim Tarihi: 01.08.2019

https://www.cia.gov/library/publications/the-world-factbook/geos/wa.html Erişim Tarihi: 04.09.2019

https://www.worldatlas.com/articles/what-is-a-panhandle.html Erişim Tarihi: 08.08.2019

https://www.cia.gov/library/publications/the-world-factbook/maps/maptemplate_ao.html Erişim Tarihi: 08.08.2019

https://www.cia.gov/library/publications/the-world-factbook/geos/gi.html Erişim Tarihi: 09.08.2019

http://projects.leadr.msu.edu/usforeignrelations/exhibits/show/manifest-destiny/oregon-treaty-1846 Erişim Tarihi 07.10.2019

http://hlaoo1980.blogspot.com/2016/03/stolen-mexican-territories-retaken-by.html Erişim Tarihi: 07.10.2019

https://www.britannica.com/place/Armenia/Settlement-patterns#ref481302 Erişim Tarihi: 17.08.2019

Hunter, S. T. (1997). Azerbaijan: Searching for New Neighbors. Ian Bremmer and Ray Taras (Ed.), *New States New Politics: Building the Post-Soviet Nations*. 437-471.

Kolstø, P. (2006). The Sustainability and Future of Unrecognized Quasi-States. *Journal of Peace Research.* Vol: 43. No. 6.

Lambert, D. (2005). As Solid As the Rock? Place, Belonging and the Local Appropriation of Imperial Discourse in Gibraltar. *Transactions of the Institute of the British Geographers*. New Series. Vol. 30. No.2. June.

Marchant, J. R. V. ve Charles, F. J. (1941). *Cassel's Latin Dictionary*. Londra: Cassell and Company Ltd.

Nies, S. (2004). *Sand in the Works: Enclaves Challenging Metropolitan States A comparative study on the governance of Cabinda, Ceuta, Kaliningrad, Nagorno Karabakh, Nakhchivan, Melilla and Gibraltar*. Paris: Institut d'Etudes Politiques.

Nies, S. (2003). Les Enclaves: "Volcans" Éteints ou En Activité. *Revue International et Strategique.* Vol: 49.

Oldberg, I. (2009). The Changing Military Importance of the Kaliningrad Region. *The Journal of Slavic Military Studie*s. Vol. 22/3.

Parker, G. (1994). Les Limites Naturelles. John O'Loughlin. (Ed.), *Dictionary of Geopolitics*. Westport: Greenwood Press.

Reid, R. ve Grosberg, M. (2005). *Myanmar (Burma).* New York: Lonely Planet.

Rodrigue, J. P. (2004). Straits, Passages, Chokepoints A Maritime Geostrategy of Petroleum Distribution. *Cahiers de Géographie du Québec*. Vol. 48. No. 135.

Sempa, F. (2002). *Geopolitics From the Cold War to the 21st Century*. Londra: Transaction Publisher.

Sevim, C. (2012). Küresel Enerji Jeopolitiği ve Güvenliği. *Journal of Yasar University*. Vol. 26 (7).

Schwind, M. (1972). *Allgemeine Staatengeographie*. Vol:8. Berlin: De Gruyter.

Steinberg, D. I. (2010). Burma/Myanmar What Everyone Needs To Know. Oxford: Oxford University Press

Swietochowski, T. (1996). The Prpblem of Nagorno-Karabagh: Geography versus Demography under Colonialism and in Decolonization. Hafeez Malik (Ed.). *Central Asia: Its Strategic Importance and Future Prospects*. 143-159.

Thomson, A. (2010). *An Introduction to African Politics*. Londra and New York: Routledge.

Turovsky, R. F. (2006). *Politicheskaya Regionalistika*. Moscow: GUVSHE.

Victor, J. C. (2006). *Le Dessous des Cartes (Atlas Géopolitique).* Paris: Arte Editions.

Vinokurov, E. (2007). *A Theory of Enclaves*. Lanham: Lexington Books.

Wahab, S. ve Youngerman, B. (2007). *A Brief History of Afghanistan*. New York: Infobadse Publishing.

CLIMATE CHANGE ADAPTATION-BASED STRATEGIES ON WATER AND ITS SECURITY: A STUDY ON DHAKA AND ANKARA

Md Moynul AHSAN*

Abstract

Adaptation strategies on climate change are one of the policy actions that can help to inform and assist individuals as well as addressing anticipated threats of climate change. These strategies can be non-regret strategies (supply and demand side), climate justified strategies to identify and resolve threats and ensuring potential alternatives as well as coping with uncertainties, increasing water supply, managing demand and use. Dhaka, the capital of Bangladesh and Ankara the capital of Turkey are facing water related challenges due to climate change impact. Therefore, various considerable adaptation-based strategies on water sector have been taken from the national to city level to ensure water security but still the adaptation practice is quite insufficient. Based on secondary based research, this study has reviewed the existing policies and strategies on water and its security, and highlighted needed adaptation-based strategies to perform. Finally, this study proposed that an effective multi-stakeholder collaboration are necessary to maintain proper co-ordination with a long term integrated adaptation program, improve water use efficiency through education and awareness campaigns, strengthen water conservation programs, impose legal restrictions, introduce incentives for consumer etc.to make Ankara and Dhaka a water secured city.

***Keywords**: Capital City, Climate Change, Water Security, Adaptation-Based Strategies.*

SU VE SU GÜVENLİĞİ KONUSUNDA İKLİM DEĞİŞİKLİĞİNE UYUM TABANLI STRATEJİLER: DAKKA VE ANKARA ÖRNEĞİ

Öz

İklim değişikliğine uyum stratejileri; iklim değişikliğinin yol açtığı tehditleri ele almanın yan sıra insanları bilgilendirmeye ve onlara yardım etmeye dayanan politika eylemlerinden biridir. İklim değişikliği tehditlerini tanımlamak, çözmek ve potansiyel seçenekler sağlamak ve bunun yanı sıra su arzını artırmaya, talebi ve kullanımı yönetmeye yardım etmek için pişman-olmama stratejileri (arz ve talep taraflı), iklim haklı stratejiler yoluyla çözülebilmektedir. Bangladeş'in başkenti Dakka ve Türkiye'nin başkenti Ankara iklim değişikliğinin etkisiyle su ile ilgili zorluklarla karşı karşıyadır. Dolayısıyla, Dakka ve Ankara'daki mevcut stratejilerin neler olduğu ve bu stratejileri formüle etmek için uyum temelli stratejilerin gerekli olduğunu açıklayan su sektörüne yönelik mevcut şehir düzeyinde uyum stratejileri ele alınmıştır ancak uyum uygulamasının hala yetersiz olduğu görülmektedir. İkincil temelli araştırmalara dayanan bu çalışmada, Dakka ve Ankara şehrindeki iklim değişikliği etkisine bağlı olarak mevcut eğilimler, suya dayalı uyum-tabanlı stratejiler ve güvenlik konuları ele alınmıştır. Son olarak bu çalışmada, her iki başkentte de sorunu çözebilecek uzun vadeli entegre uyum programı ile uygun koordinasyonu sağlamak için çok paydaşlı iş birliğinin gerekli olduğu, modern tekniklerle su koruma programlarını güçlendirmesi, eğitim ve bilinçlendirme kampanyaları ile su kullanım verimliliğini artırmaya çalışması, su kullanımını azaltmaya yönelik yasal kısıtlamalar getirilmesi, yasal kısıtlamalar empoze etmesi, tüketici için teşvikler sunulması önerilmektedir.

***Anahtar Kelimeler**: Başkent, İklim Değişikliği, Su Güvenliği, Uyum-Tabanlı Stratejiler.*

* Asst. Prof. Dr., Department of Real Estate Development and Management, , Faculty of Applied Sciences, Ankara University, Ankara, Turkey, moynulurp01@gmail.com, ORCID ID: 0000-0003-0822-3850

Makale Geliş Tarihi: 28.10.2019 Makale Kabul Tarihi: 22.01.2020

INTRODUCTION

Without an iota of doubt, the global community now recognizes the challenges arising from climate change. Achieving water security is one of such challenges where climate change is considered one of the threats for water security (Vural, 2018:61,62). Adaptation is an adjustment option that can overcome the water security challenges by reducing damage, protecting ecosystems, economy, livelihood etc. (IPCC, 2014:5). In this study, the climate change adaptation-based strategies refer to managing risk and enhancing resilience on water sector. Therefore, strategies such as increasing supply, managing demand, facilitating allocation of water resources, improving flood protection, coping with uncertainties, improving information, making robust decision etc. all helptowards a safe and secured water sector (Ahsan, 2017: 485).

Bangladesh is the ninth climate change risky country whereas Turkey ranks 72nd as per the Climate Risk Index for 2017 in the world (Eckstein, Hutfils and Winges, 2018:28,31). Though the main climate change impact occurs in water sector there is no explicit strategy on climate change impact on water sector in both Bangladesh and Turkey. However, both governments have formulated a number of adaptation strategies, plans, programs and policies for climate change. The capital cities like Dhaka in Bangladesh and Ankara in Turkey are now experiencing challenges on water sector. Changing climate, rapid urbanization, industrial growth, socio-economic development etc. are contributing to such challenges in these two big cities due to lack of availability, access to inadequate quantities and use of low quality of water.

Therefore, this study is about a number of climate change strategies of water sector in the two capital cities – Dhaka and Ankara.. The study mainly deals with the broad research question of what different adaptation-based strategies are available and how the city management is responding to climate change impacts on water sector by applying different adaptation strategies. The aim of this research is to examine water sector adaptation strategies by which adverse effects can be reduced, new and potential opportunities and strategies can be seized for Dhaka and Ankara dwellers and vulnerable people can enjoy adequate privilege. Secondary data has been considered in order to present an in-depth literary portrayal of the current issues and challenges of the chosen study topic. In this respect, peer review journal articles, policy, strategy, program and projects documents from government, non-government and international non-government organizations have been consulted. Finally, research validity has been ensured for all data collection methods through the triangulation of sources.

1. CLIMATE CHANGE AND WATER SITUATION IN DHAKA AND ANKARA

Both Dhaka and Ankara are among the fastest growing cities of the world with a total population estimated at more than 13.14 million in Dhaka (BBS, 2015: 27) and 5.5 million in Ankara (Turkish Statistical Institute, 2018: 6). Considering metropolitan area, Dhaka's population was 12.516 million in 2011and it is projected to be 14.77 in 2031 (BBS, 2016:27) whereas Ankara's population was 4.8 million in 2016, has increased to 5.5million in 2019 and it is projected to be 6.1 million in 2023 (Turkish Statistical Institute, 2018). Dhaka is one the most vulnerable cities in the world. It ranks as an Extreme Risk city as the changing temperatures and weather systems according to Maplecroft's (a specialized British firm in risk analysis) and Climate Change Vulnerability Index (CCVI). Ankara is considered a highly risky district in terms of drought in Turkey (Türkeş, 2017: 64). Both capitals are located at the center of the country poses tropical climate and continental climate respectively but hot, dry summers, incessant rainfall, flood, heat waves, droughts are negatively influence human life.

Dhaka experiences a hot, wet and humid tropical climate whereas Ankara experiences too much water during incessant rain. Both cities are experiencing floods that are mainly caused by unpredictable heavy rainfall, inadequate infrastructure, insufficient drainage system and drainage congestion (Ahsan, 2017: 485), global climate change impact has added its intensity and so on. Both Dhaka and Ankara are not directly impact with sea level rise as the consequences of climate change, however its indirect impact are quite high in Dhaka, for instance, sea level rise creates migration crisis in Bangladesh and Dhaka is the major destination of the vulnerable people (Ahsan, 2019: 106,147) therefore, climate change impact ultimately pressurizes water accessibility, availability and use of existing city dwellers and incoming climate migrants. Ankara on the other hand, has no evidence of adverse impact from the rise of sea level water. Again, Dhaka's poor, inadequate, unplanned infrastructure especially water supply, drainage, sanitation can barely support the existing population. However, Ankara is developing rapidly through its planned development and strategic process.

Ankara is located in central Anatolia region, is semi-arid and lowest precipitating area of Turkey (ÇŞB, 2018: 29). During dry season, Ankara is also considered one of the direst areas in Turkey. In 2007, Ankara faced water supply crisis during a drought. Statistics shows that Ankara can presume a drought once

every four years and that the return period for a severe drought that affects 50% of the region is five years (Franz, Tigrek and Kibaroglu, 2012:288-289). Around 98.5% Ankara city's water supply is dependent on surface water resources (Köle, 2012: 29). However, Dhaka is not only experiencing abundance of water but also huge scarcity of water; too little in the dry season and too much during monsoon (Ahsan, 2017: 485). Around 79% to 80% of the Dhaka city's water supply is dependent on groundwater resources (IWM and DevCon, 2014: ii). The groundwater level is depressing rapidly due to over extraction for industry, domestic use, public supply in this over populated, over industrialized city. Every year the groundwater table is dropping down around one to three meter due to extreme amount of withdrawal (DWASA, 2013, Alam, 2012). The continuous declining groundwater table makes pumping of groundwater costlier and technically difficult which results in lower water security of the poor dwellers of Dhaka city (IWM and DevCon, 2014:86). Therefore, the city's institutional systems, inter-dependences between multiple sectors, levels and risks in a dynamic physical, economic, institutional and socio-political environment remain to be the challenging tasks to achieve urban climate resilience.

2. RESULTS AND DISCUSSION

This study has focused on two different ways of adaptation-based strategies, one is "no-regret strategies" that have divided into supply and demand side and another is climate justified strategies that are justifiable that means these strategies are defensible during vulnerable period and reasonable in price. These strategies are aligned with the most acceptable on UN-Water proposed the water security definition which indicates the capacity of a population to safeguard sustainable access to adequate quantities of and acceptable quality water that ultimately helps to preserve ecosystem, enhance peace and political stability (UN-Water, 2013:1). The "no regrets" strategies are the aspect of climate risk management means taking climate-related decisions or action that make sense in development terms anyway, whether or not a specific climate threat actually materializes in the future, which is achieved by building resilience to changing economic, social and environmental conditions (UNDP, 2010). Besides these strategies, this study has focused intelligent and robust decision-making strategy that can help to outline policy makers to outline water and its security challenges. It tries to highlight "deep uncertainty" in which stakeholders do not know or agree on the relationships among actions, consequences, and probabilities.

2.1. No-Regret Strategies (Supply Side)

For this study, supply is referred to be able to provide water to the city dwellers. When it comes to strategy perspective, this study has considered two main aspects one is maintaining status-quo (i.e. timely preparing strategies, action plans) another is improving surface and ground water bodies that aligns to supply side of no-regret strategies. Among the developing countries in the world, Bangladesh is one of the leading countries in respect of climate change adaptation and action. The Bangladesh government prepared National Water Policy in 1999 but there is no explicit information on the relation of climate change and water in it. Later on, two broad strategies were formulated by the government such as the National Adaptation Programme of Action (NAPA) and Bangladesh Climate Change Strategy and Action Plan. The NAPA was formulated under the guidance of UNFCCC in 2005. The purpose of the NAPA formulation was the development of a countrywide programme to encompass the immediate and urgent adaptation activities required to respond both current and anticipated confrontational effects of climate change. These strategies have focused on reducing poverty and securing livelihoods while addressing gender aspects in the implementation of the NAPA recommendations (Ministry of Environment and Forest, 2005). Adaptation needs of the urban people (mainly urban poor) have not paid explicit attention. Even, policy options have not yet implemented adequately. The Bangladesh government has prepared climate change adaptation policy framework entitled as the Bangladesh Climate Change Strategy and Action Plan in 2008. It has been updated in 2009. The six pillars of national strategy have directly and indirectly focused climate change adaptation on water (MoEF, 2009). Water supply and sanitation (WSS) sector development plan in 2011-2025 has focused to incorporate climate change adaptation strategies in water sector. Dhaka Water Supply and Sewerage Authority (DWASA) have prepared Master Plan in 2014. This master plan has suggested making storm water retention ability, incorporating rain water harvesting provisions within the building code as an adaptation measure for climate change (IWM and DevCon, 2014:91).

Turkey has not prepared any NAPA yet but it has prepared the First National Communication on Climate Change in 2007 and till now it has prepared7th National Communication in 2018 under UNFCCC. This communication has mentioned that some actions on climate adaptation including local governments have been taken and put emphasize on various capacity development as well as project activities (ÇŞB,

2018:22). The National Climate Change Adaptation Strategy and Action Plan has prepared in 2011 (2011-2023) (edited in 2012), Ankara water and sewerage administration has prepared its strategy from 2010-2014 and 2015-2019. National Water Plan for 2019 and 2023 has prepared in 2019. In Climate Change Adaptation Strategy and Action Plan in Turkey, there is lack of clear information regarding the negative impact of climate change on water however it urges improving water legislation and the concept of adaptation to climate change shall be integrated into the legislation (MoEU, 2013:23). According to the National Water plan, Gerede-Ankara Drinking Water- 2 is the longest drinking water tunnel in Turkey, which is planned to meet the drinking water needs of city dwellers of Ankara by 2050 (Tarım ve Orman Bakanlığı, 2018:37) while DWASA has been preparing detailed and comprehensive Storm Water Drainage Master Plan for an efficient drainage network for greater Dhaka City, which will be treated as a basic document for storm-water/manmade drainage network plan for Detailed Area Plan 2016-2035. According to 2nd Forestry and Water Council 2017, Turkey's drinking and usable water potentiality has been determined but there is no clear information has been produced as to how this potential will be affected by the adverse effects of climate change on city water sector on the basis of quantity and quality.

Again, surface and ground water bodies improvement are the major no-regret strategies in supply side, for instance wetlands or dams supports to improve water quality, reduce depletion of ground water, provides flood protection and so on. Ultimately it makes a city more natural, stores a significant amount of carbon. During the late 70s, Dhaka city and its surrounding was blessed with the flowing water, aquatic biodiversity of over 250 canals. These canals act as a retention pond to store flood water. Now only 35 canals are surviving with unabated, unlawful encroachments by land grabbers, mindless dumping of solid wastes, pollution and complete negligence of their lawful protectors (Alam, 2018: 14). Even, most of them have lost all of its life saving matters, including water stream, and water quality and minimal amount of water to survive. In total, Dhaka lost 60% wetlands in the last 30 years due to unplanned urbanization, population growth, commercial and residential development, road construction, illegal land grabbing etc. as well as the groundwater table is dropping down due to extreme withdrawal (BSS, 2016).

The surface water area of Dhaka Central Region is about 13% of the total land area. The DWASA has got both the mandate and programs to protect the canals but no adequate reflection has found. According to DWASA Master Plan, the DWASA

is expanding its service area but the pace of industrial, domestic and other uses could not be covered as per population growth in Dhaka. To a projection estimated for the period of 2035 to 2060, there will be approximately 50% growth in demand on water (IWM and DevCon, 2014: v). On the other hand, the domestic water reservoirs in Ankara come from seven dams. However, to meet the large water demand for Ankara city dwellers, water is now being collected from the longest Kızılırmak River in Turkey. Ankara belongs to Sakarya Basin which contains the lowest water resources per capita among the basins in Turkey (Körbalta, 2019: 69). A study represents that there is a general increase in the temperature trends, while the decreasing trends are observed in Sakarya basin, and the projection for the period of 2010-2039, 2040 – 2069 and 2070-2100 represents that the precipitation will be decreased to 5.31%, 14.46% and 14.76% respectively (Köle, 2012:100). However, the temperature will increase in the above reference period by 0.79%, 1.63% and 2.63% respectively. Therefore, there will be an immense change in both precipitation and temperature in Ankara (Köle, 2012:101). The following table represents that in the last few years the water reservoirs are not increasing as per demand of the city population in Ankara. Therefore, the uncertainty of the risk on water due to climate change should be taken into consideration and government should give attention to adopt and use groundwater reservoirs as a strategic resource of option.

Table-1. Amount of Water reservation from 2011 to 2019 in Ankara (ASKİ, 2019: http://www.aski.gov.tr/TR/Baraj.aspx)

Year	Water reservation (m^3)
2011	560.327.000
2012	631.983.000
2013	581.622.000
2014	476.388.000
2015	553.934.000
2016	430.727.000
2017	322.155.000
2018	398.763.000 (05.09.2018)
2019	473.329.0 5.09.2019)

2.2. No-Regret Strategies (Demand Side)

Using soft adaptation strategies (such as education and awareness program) for climate change adaptation in water sector can lead to long-term behavioral and motivational changes. There is no explicit strategies on climate-water interaction education and awareness program despite some discouragement programs on illegal connection, water pollution control etc. in Dhaka, however some projects are being implemented in Ankara such as "Su Elçileri Eğitim ve Farkındalık Artırma Teknik Destek Projesi", climate camps, voice of meteorology, İklimIN project, climate action week etc. which marked as an effective strategy to take positive action against climate change impact, cope with uncertainties at different stages, managing demand and use.

Again, the use of grey water in households and auto switching/smart pump controllers can conserve water. The DWASA opened first time Fresh water ATM booth to reduce clean water crisis in some pockets in 2017. Around 300 such ATM booths had been planned to be installed by September 2019 (Islam, 2019). The Management Information System of DWASA is going to use SCADA (Supervisory Control and Data Acquisition) technology to provide automated water production and distribution information. Other applications such as Smart Meter, e-billing, e-connection, e-supply chain management are started to be applied by DWASA to manage water demand in Dhaka city.

On the other hand, Ankara has introduced 63 ASKİMATİK in 2017 which are providing 7/24 hr. service that increases customer interest at a pace rate and now 70 places are providing this service (http://sumatik.aski.gov.tr/i/191 /hakkimizda.html). Though the main target is not an adaptation action for climate change but to effective use of adequate quantity of water, reduce water crisis, ensure citizen rights etc. Other applications such as Smart Meter, e-billing, e-connection, e-payment, e-supply chain management are being implemented by ASKİ (Ankara Su ve Kanalizasyon İdaresi) to manage, the use of water in Ankara city.

2.3. Climate Justified Strategies

There are two types of climate justified strategies such as rainwater harvesting and wastewater treatment and disposal that have been focused in this research. These strategies can be highlighted as reasonable and defensible in uncertain climate condition. Dhaka is blessed with rain almost all-round the year but more especially

from May to August have highest amount of rainfall. However, April and May are the wettest months in Ankara. It is estimated that the artificial recharge by harvesting rainwater from concrete rooftops of 60 per cent buildings in Dhaka may replenish 250 million liters of water per day (Alam, 2012). Therefore, the government of Bangladesh has planned to make rainwater recharging mandatory for building owners in Dhaka aiming to reduce water-logging and fight fast-depleting of groundwater level. A study estimated that the rain water harvesting method is capable to reach 70% of total domestic consumption in Ankara. It is also estimated that rain water harvesting and grey water reuse altogether can offer a chance of water savings between 40% and 46% (Aybuğa and Işildar, 2017: 215). The National Water Plan has given much emphasize and encouragement on the development of rainwater harvesting projects whereas Ankara has also given policy attention to rainwater harvesting as for future demand of the growing city population.

Dhaka city has only two waste water treatment plants called Pagla Sewage Treatment Plant and Saidabad Surface Water Treatment Plant (SWTP). Pagla Sewage Treatment Plant can treat only 40,000 cubic meters of wastewater, while the other is Saidabad Surface Water Treatment Plant (SWTP) can treat only 450,000 m^3/d of wastewater. These plants are insufficient to ensure minimum level of security of Dhaka dwellers (IWM and DevCon, 2014:32). Thus, more treatment plants to a higher elevation in response to the impact of flooding and sea level rise are highly required. However, in Ankara, efforts on the treatment of domestic and urban wastewater in metropolitan cities have accelerated from 2008. According to TÜİK "2016 Municipal statistical survey", the amount of wastewater treated per capita per year as per EU standards in Ankara only 4.2 m^3 which is the lowest in Turkey (https://www.egedebir gun.com/belediye-atik-su-istatistikleri-aciklandi/ 8345/). Therefore, still a large share is beyond and inadequate treating of waste water in Ankara.

2.4. Intelligent and Robust Decision Making

Failure to adapt to climate change can jeopardize water security over the long-term and eventually make it costlier to improve, as time passes, for governments to adjust to changing circumstances (OECD, 2013). The city government of Dhaka with its limited financial capacity is executing plans, programs and policies but uncoordinated work andlack of actor-network connection reduces its sustainability and resiliency. The responsible authorities of Ankara have taken some needed

actions from time to time to executing plans, programs and policies but there is a need for strong coordinated work, actor-network connection to enhance robustness of decision making. For both Dhaka and Ankara, it has been found that inadequate dialogue and consultation among with the respective stakeholders exacerbated the crisis and prevented opportunities to reach participative and democratic management and use of limited water resource in the city (Franz, Tigrek and Kibaroğlu, 2012: 288).

3. RECOMMENDATIONS AND CONCLUDING REMARKS

The climate change impact, excessive population growth, unplanned growth, rapid industrialization, centralization of activities etc. all provides lots of challenges for city of Dhaka and Ankara. Regarding the discussion above, the following no-regret strategies, climate justified strategies, and intelligent and robust decision making proposed in order to avoid a situation in which shifting to a different measure will no longer be possible towards ensuring water security in Dhaka and Ankara city.

For no-regret strategies on the supply side, both Dhaka and Ankara justify an effective multi-stakeholder collaboration, considering all concerned ministries and government and non-government organizations engaged in different positions to develop and implement adaptation program where city corporations in Dhaka and Ankara can take leading roles as they are performing major city water governance and services (Ahsan, 2017:491). The national government should play the lead role by formulating a strategic action plan in consultation with advisors, key personnel and other stakeholders. Following a government-devised action plan, the private sector, national and international NGOs will be able to develop more robust and effective partnerships. It will also ensure long-term solutions as well as achieving sustainable development goal (Ahsan, 2017:491).

The plan, policies and strategies of both Dhaka and Ankara city should give emphasize to conserve water retention area, canals, rivers and dams. Therefore, it requires proper execution of the concerned authorities. Again, imposing legal restrictions can reduce water use. Improving access to piped water will increase the resilience or adaptability of the lower income people in the aspect of climate change and the risk of natural disasters.

Rehabilitation of existing infrastructures and construction of new infrastructure are highly required to protect from adverse effect of climate change. Again, to

achieve water security and to cope with the climate induced impacts, the use of surface water needs to be increased and the dependence on groundwater need to be shifted. In order to ensure the proper use of existing surface water bodies the small- and large-scale treatment plants are highly needed.

For no-regret strategies in demand side, both cities should expand the use of soft technologies that can lead to long-term behavioral changes with significant adaptation potential. Both city administrations should strengthen water conservation programs or dam protection programs that seek to improve water use efficiency through education, awareness or campaign programs. For instance, the city people should get aware about mindless dumping of solid waste. As city authorities are the main responsible body of collecting solid waste, therefore, they should take more initiatives for awareness raising programs.

There is no explicit information regarding climate change impact and water metering in the strategy documents. Auto switching/smart pump controllers/water metering system/fresh water ATM booth system should be expanded to reduce water consumption and crisis as well as increase rational water use. The DWASA needs to enhance sustainable operation and maintenance of the use of District Metered Areas (DMAs) systems. In addition, it must be able to monitor water quality to detect and mitigate water pollution and salinization. Again, introduction of incentives for consumers can also provide benefits regardless of additional climate change stress. Awareness program against anticipated climate risk should be increased.

In case of climate justified strategies, encouraging rainwater harvesting and grey water reuse could help to achieve water security and to cope with the climate impacts; preparing utility planning storm water system may opt to expand the capacity of its collection system in anticipation of more extreme precipitation events. Therefore, harvesting rainwater in dams or water reservoirs in a planned way could help develop water supply conservation as a strategy for uncertainty. In addition, both cities should transform its building into green buildings to reduce carbon dioxide emission and energy consumption. Measures to augment supply through wastewater recycling or the encouragement of water markets that move water to high-valued uses may provide benefits regardless of anticipated climate change related impacts as well as resiliency. In this respect, city authorities and ASKİ/DWASA should take adequate priority-based actions and programs.

In case of intelligent and robust decision making, coordinative actions and efforts are highly needed against the measures of climate change impact. Climate adaptation experts should take part in the decision-making process to robust and scale up the adaptation efforts both government and non-government level. Though the responsible authorities of Ankara have taken some needed actions in time and Dhaka with its limited financial capacities have taken some actions, there needs strong coordinated work, actor-network connection to enhance robustness of decision making. Finally, this study recommends that there is a need not only to highlight the ability to adapt with different environment and climatic event but also to reduce urbanization pressures, to make alternative water supply options. Moreover, it is needed to preserve ecosystems, increase green space and reliable and efficient use of water in a sustainable way to make Dhaka and Ankara a water secured city.

REFERENCES

Ahsan, M. M. (2017). Challenges of Local Governments on Climate Change Adaptation Strategies: A Study on Water Sector in Dhaka City, Bangladesh. Mahmut Güler ve Menaf Turan (Ed.). *Belediyelerin geleceği ve yeni yaklaşımlar* 1. cilt (pp. 483-495). Istanbul: Marmara Belediyeler Birliği Kültür Yayınları.

Ahsan, M. M. (2019). *Bangladeş ve Amerika Birleşik Devletlerinden Seçilmiş Kıyı Alanlarında Çevreden Kaynaklanan Göç*. Unpublished Doctoral Thesis. Ankara University, Ankara.

Alam, R.Q and Duti B.M (2012), Climate Change Impacts on Water Related Sectors of Dhaka City and Assessing the Plausible Adaptation Options. *In 2nd International Conference on Environmental Technology and Construction Engineering for Sustainable Development.* Sylhet, Bangladesh.

Alam, M Jahangir (2018). Rapid urbanization and changing land values in mega cities: implications for housing development projects in Dhaka, Bangladesh., *Bandung J of Global South*. 5(2). DOI: 10.1186/s40728-018-0046-0.

Alam, H. (2012). Buildings to store rainwater. Retrieved December 2015 from http://www.thedailystar.net/news-detail-235024.

Aybuğa K and Işıldar, G. Y (2017). An Evaluatıon on Rain Water Harvesting and Grey Water Reuse Potential for Ankara. *Sigma Journal of Engineering and Natural Sciences* 8 (3): 209-216.

BBS-Bangladesh Bureau of Statistics (2015), Population Projection of Bangladesh Dynamics and Trends 2011-2061. Ministry of Planning, Bangladesh.

BSS-Bangladesh Sanbad Songstha (2016). Dhaka lost 60pc wetlands in 30 years: Study. Retrieved January 2017 from http://www.thedailystar.net/city/dhaka-lost-60pc-wetlands-30-years-study-205933.

ÇŞB- T.C. Çevre ve Şehircilik Bakanlığı (2018). Türkiye'nin Yedinci Ulusal Bildirimi, Türkiye Cumhuriyeti Çevre ve Şehircilik Bakanlığı, Ankara, Türkey.

DWASA- Dhaka Water Supply and Sewerage Authority (2013), 50 years of Dhaka WASA: annual report 2012–13. Dhaka Water Supply and Sewerage Authority, Dhaka.

Eckstein, D., Hutfils M and Winges, M. (2018), Global Climate Risk Index 2019 Who Suffers Most from Extreme Weather Events? Weather-related Loss Events in 2017 and 1998 to 2017, Retrieved July 2019 from https://pdfs. semanticscholar.org/d0ef/895f44fa421593bae5d5df72cc39901c4c68. pdf.

Franz, C., Tigrek, S. and Kibaroglu, A. (2012), Water supply crisis in Ankara: Review and comparison of the "1995 master plan report on Ankara water supply project. Scientific Research and Essays. 7(3): 288-299. DOI: 10.5897/SRE10.83.

Islam, Mazharul., (2019). Drink safe from water ATM, Retrieved October 2019 from http://www.newstoday.com.bd/?option=details&news_id=2529534&date =2019-05-10.

IPCC-Intergovernmental Panel on Climate Change (2014). Summary for policymakers, In: Climate Change 2014: Impacts, Adaptation, and Vulnerability. Part A: Global and Sectoral Aspects. Contribution of Working Group II to the Fifth Assessment Report of the Intergovernmental Panel on Climate Change. NY: Cambridge University Press.

Köle, M. (2012). Ankara Örneklemi Üzerinde İklim Değişikliğinin Su Kaynakları Yönetimine Etkisi, *Doktora Tezi*, Ankara Üniversitesi Sosyal Bilimler Enstitüsü Sosyal Çevre Bilimleri Anabilim Dalı, Ankara.

Körbalta, H. (2019, Mayıs). Türkiye'de Yerel Su Güvenliği, *Güvenlik Bilimleri Dergisi*, 8 (1), 55-84. DOI:10.28956/gbd.562965.

MoEF-Ministry of Environment and Forest, (2009). Bangladesh Climate Change Strategy and Action Plan-2009. Ministry of Environment and Forests, Government of the People's Republic of Bangladesh, Dhaka, Bangladesh.

OECD (2013). Water and Climate Change Adaptation: Policies to Navigate Uncharted Waters. OECD Studies on Water, OECD Publishing.

Türkeş, Murat (2017). Drought Vulnerability and Risk Analysis of Turkey with Respect to Climatic Variability and Socio-Ecological Indicators. *Aegean Geographical Journal*, 26(2): 47-70. Izmir, Turkey.

Türkiye İstatistik Kurumu Başkanlığı, (2017). Belediye Atıksu İstatistikleri, 2016" Haber Bülteni, 22/11/2017, Sayı: 24875, Retrieved September 2019 from http:// www.tuik.gov.tr/PreHaberBultenleri.do?id=24875.

Turkish Statistical Institute, 2018, Turkey in Statistics 2018, Ankara: Türkiye İstatistik Kurumu, Turkey.

Tarim Ve Orman Bakanlığı (2018). Ulusal Su Planı (2019-2023), Ankara: Tarım ve Orman Bakanlığı.

UNDP-United Nations Development Program (2010). A 'No-Regrets' Risk-Based Approach to Climate-Proofing of Public Infrastructure: Improved National and Sub-National Planning for Resilience and Sustainable Growth. July 2010. www.a daptationlearning.net.

UN-Water, (2013). Water Security & the Global Water Agenda: A UN-Water Analytical Brief, Retrieved October 2016 from https://www.unwater.org/ publications/water-security-global-water-agenda/.

Vural, Ç. (2018, Mayıs). Küresel Iklim Değişikliği ve Güvenlik. *Güvenlik Bilimleri Dergisi*, 7(1), 57 – 85. DOI:10.28956/gbd.422726.

AKILLI KENTLERDE VERİNİN GİZLİLİĞİ VE GÜVENLİĞİ: İLKELER VE YAKLAŞIMLAR

Levent MEMİŞ[*], Melikali GÜÇ[**]

Öz

Teknolojik gelişmelerin dinamik ortamında ortaya çıkan yenilikler, toplumsal ve ekonomik alanlarda yeni durumları gündeme getirmektedir. Kentler, bu gelişmelerin yansıdığı önemli alanlardan biridir. Bu noktada akıllı kent ve büyük veri kavramları gündeme gelmekte, bu gelişmeler kentsel alanda sunulan hizmetlere yeni biçimler kazandırmaktadır. Fakat bu gelişmeler beraberinde bazı olumsuzlukları da getirmektedir. İfade edilenler kapsamında araştırmanın amacı; akıllı kentlerde ortaya çıkan büyük verinin gizliliğini, güvenliğini güçleştiren ve bunları tehdit eden unsurları ele alarak ortaya çıkan olumsuzlukları gidermek amacıyla gündeme gelen ilkeler ve yaklaşımları incelemektir. Temelde yanıt aranan soru: "Akıllı kentlerin önemli bir parçası olan, büyük verinin gizliliğini ve güvenliğini sağlamak amacıyla hangi ilkeler ve yaklaşımlar öne çıkmaktadır?". Sorunun cevabı ilgili literatür, hukuki düzenlemeler ve uluslararası oluşumların aldığı kararlar üzerinden aranmaktadır. Genel sonuçlara göre bazı düzenlemeler (AB Veri Koruma Tüzüğü gibi) öne çıkmakla birlikte, veri güvenliği konusunda küresel düzeyde üzerinde uzlaşı sağlanan standartların olmadığı anlaşılmaktadır. Fakat bazı ilkelerin ve yaklaşımların önem kazanmakta olduğu tespit edilmiştir. Çalışmanın sonunda, elde edilen sonuçlara göre politika önerileri sunulmuştur.

Anahtar Kelimeler: *Akıllı Kent, Büyük Veri, Açık Veri, Veri Gizliliği ve Güvenliği.*

DATA SECURITY IN SMART CITIES: PRINCIPLES AND APPROACHES

Abstract

Innovations emerging in the dynamic environment of technological developments lead to new situations in social and economic fields. Cities are one of the important areas where these developments are reflected. Thus, smart cities and big data concepts come up and these developments cause changes in services provided in cities. However, these developments bring along some negativities, as well. The main purpose of this study is to examine the approaches and principles that have come to fore in order to ensure the privacy and security of big data in smart cities. Basically, the answer to this question is sought: what principles, approaches and practices come to the forefront in order to ensure the confidentiality and security of big data that is an important part of smart cities? The answer is sought through the relevant literature, legal regulations and international decisions. According to the general results of the study, it is understood that there are not any consensual standards on data security at global level. However, some regulations draw attention. At this point, the "General Data Protection Regulation (GDPR)" which came into force in 2018 is important. However, some principles and approaches are gaining importance. At the end of the study, some suggestions about policies are made according to the results obtained.

Keywords: *Smart City, Big Data, Open Data, Data Privacy and Security.*

[*] Dr.Öğr.Üyesi, Giresun Üniversitesi, İİBF, Siyaset Bilimi ve Kamu Yönetimi Bölümü, levent_memis@hotmail.com, ORCID NO: 0000-0002-5438-691X.

[**] Öğr.Gör., Giresun Üniversitesi, Tirebolu Mehmet Bayrak Meslek Yüksekokulu, Bilgisayar Teknolojileri Bölümü, melikali.guc@giresun.edu.tr, ORCID NO: 0000-0003-0986-9290.

Makale Geliş Tarihi: 04.11.2019 Makale Kabul Tarihi: 22.01.2020

GİRİŞ

Son dönemlerde gündeme gelen teknolojik gelişmelerin (nesnelerin interneti, sensör, güvenlik yönetim sistemleri, coğrafi bilgi sistemleri, sanal gerçeklik gibi) kentsel alanda karşılığını bulmasıyla birçok kavram geliştirilmiş ve akıllı kent kavramı öne çıkmıştır. Adı geçen teknolojiler aynı zamanda klasik verinin ötesinde daha büyük miktarlarda verinin elde edilmesine de katkı sağlamaktadır. Bu büyük verilerden, kentlerin yönetiminde yararlandığı gibi, açık hale getirilerek (belirli sınırlılıklar dâhilinde) diğer paydaşların kullanımına da sunulduğu bilinmektedir. Bu sayede verilerin kentin karmaşık sorunlarına karşı politika geliştirmeye katkı sağlaması beklenmektedir.

İfade edilen potansiyel getirilerin yanında, büyük veriyle bağlantılı açıklar (*vulnerabilities*) ortaya çıkmaktadır. Bu bağlamda kişisel verilerin gizliliği (*privacy*) ve güvenliği (*security*) konusu öne çıkmaktadır. Verilerin dijital ortamlarda oluşması ve depolanmasıyla amacı dışında, yasa dışı erişimi kolaylaşmaktadır. Bu durum, farklı ölçeklerde (yerel, ulusal ve uluslararası) gündeme gelmekte; siber saldırı, siber savaş, siber casusluk, soygun 2.0, veri simsarlığı gibi kavramlarla nitelendirilmektedir. Bu kavramlar arasında siber saldırı öne çıkmaktadır. Farklı yöntemlerle ortaya çıkan siber saldırılar; (I) veri şifreleme ve yazılım güvenliğinin zayıflığından, (II) güvenli olmayan eski sitemlerin kullanılmasından ve bakım çalışmalarının yetersizliğinden, (III) akıllı kent bağlamında ortaya çıkan bütüncül sistemin karmaşık yapısından ve (IV) insan hatasından ve çalışanların bilinçli olarak kötüye kullanmasından kaynaklandığının altı çizilmektedir (Kitchin ve Dodge, 2019: 59-60). Diğer taraftan şu durumlarda kişisel verilerin gizliliği ve güvenliği öne çıkmaktadır: aktörler arası veri paylaşımında, veri entegrasyonu ve kullanıma hazır verilerde, verilerin depolandığı bulut alt yapısında, veri madenciliği, makine öğrenmesi ve yapay zekâ bağlamında gündeme gelen tehditler ve veriler üzerinde geliştirilen iş birliklerinde özel çıkarların öne çıkmasıdır.

İnternet ağlarının kamusal alana daha fazla entegre olması ve büyük verinin gündeme gelmesiyle oluşabilecek tehditleri durdurmaya yönelik ulusal, bölgesel ve uluslararası düzeyde çeşitli çabalar gösterilmektedir. İfade edilenler kapsamında çalışmanın temel amacı, akıllı kentlerde ortaya çıkan büyük verinin gizliliğini ve güvenliğini sağlamak amacıyla gündeme gelen ilkeleri ve yaklaşımları incelemektir. Temelde yanıt aranan soru şudur: "Akıllı kentlerin önemli bir parçası olan büyük verinin gizliliğini ve güvenliğini sağlamak amacıyla hangi ilkeler ve yaklaşımlar öne çıkmaktadır?". Bu inceleme ilgili literatür, hukuki düzenlemeler ve uluslararası oluşumların aldığı kararlar üzerinden gerçekleştirilmektedir.

Araştırmanın genel sonuçlarına göre, verinin gizliliği ve güvenliği konusunda küresel düzeyde üzerinde uzlaşı sağlanan standartların olmadığı anlaşılmaktadır. Fakat bazı düzenlemeler dikkat çekmektedir. Bu noktada 2018 yılında yürürlüğe giren "AB Veri Koruma Tüzüğü" (*General Data Protection Regulation, GDPR*) önem arz etmektedir. Bu düzenlemeyle birlikte; şeffaflık ve hesap verebilirlik prensibi, açık rıza, unutulma hakkı, veri koruma sorumluları, ağırlaştırılmış yaptırım, verilerin yurt dışına aktarılmasının sıkı kurallara bağlanması ve risk temelli yaklaşıma önem verilmektedir. Diğer taraftan genel olarak büyük verinin gizliliği ve güvenliğini sağlamak amacıyla; verilerin şifrelenmesi, kişisel verilerin anonimleştirilmesi, gizlilik bildirim sistemlerini kullanıcı dostu yapmak, verilerin saklama süresini kısaltmak, amaç sınırlılığı, algoritmik şeffaflık/hesap verebilirlik, veri minimizasyonu, dış inceleme ve denetimler öne çıkmaktadır.

1. AKILLI KENT VE KENTSEL ALANDA BÜYÜK VERİ

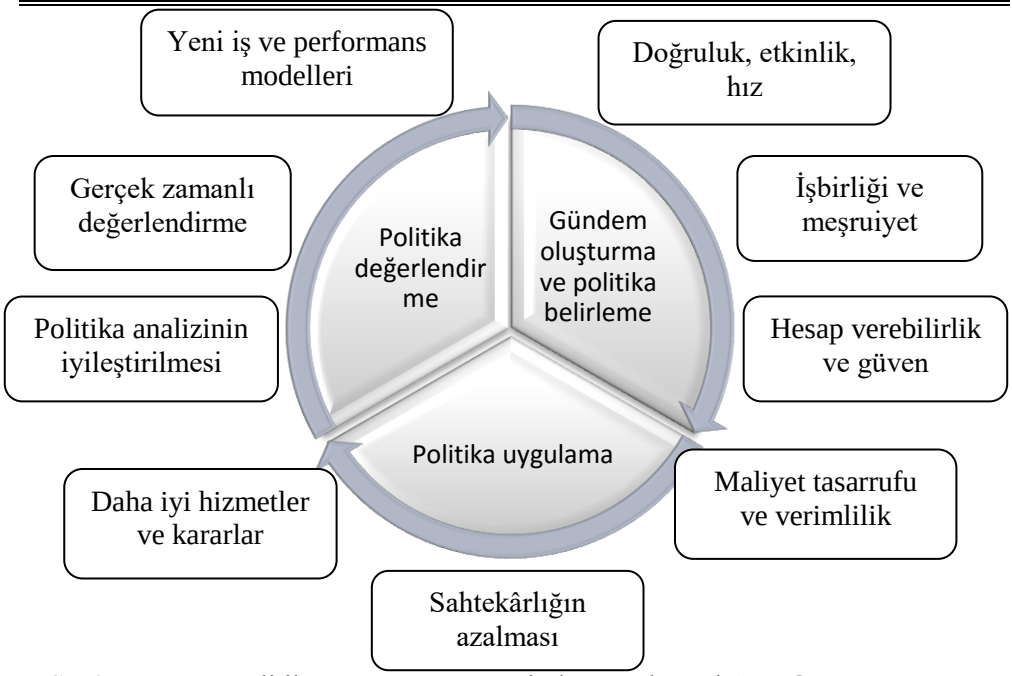
Farklı tanımlama çalışmaları olmakla birlikte genel olarak ele alındığında akıllı kent, yaşam kalitesinin artırılması amacıyla, kentin farklı fonksiyonları arasında entegrasyonu sağlayarak çözüm üreten yapıdır (Nuaimi vd., 2015: 2). Diğer bir ifadeyle yeni teknolojiler, kentin sorunlarına çözümler sunarak kent yaşamının kolaylaşmasına ve iyileşmesine katkı sağlama potansiyeli taşımaktadır. Diğer taraftan teknoloji, kentsel hizmetlere operasyonel düzeyde katkı sağladığı gibi, gerçekleştirilen faaliyetlerin verisinin oluşturulmasını ve tutulmasını da mümkün hale getirmektedir. Bu bağlamda gelişen yeni teknolojiler aracılığıyla akıllı kentlerde ortaya çıkan işlevler Lim ve Malio (2018: 168-169) tarafından 5 C (bağlantılılık/connection, biriktirme/collection, hesaplama/computation, iletişim/communications ve birlikte üretim/co-creation) şeklinde formüle edilmektedir. Bağlantılılık, özellikle nesnelerin interneti uygulamaları aracılığıyla insanlar ve nesneler arasında gerçekleşmektedir. Biriktirme, adı geçen bağlantılılık üzerinden verilere karşılık gelmektedir. Hesaplama, elde edilen verilerin makineler ve insanlar için anlaşılır hale gelmesinde, uzman bilgisine ve özel algoritmalara ihtiyaç duyulmasıdır. İletişim, insanlar ve nesneler arasında kablosuz ağlar ile gerçekleştirilen bir durumdur. Birlikte üretim, hizmet sağlayıcılar ve tüketiciler arasında değerin farklı tarafların yer almasıyla gerçekleşmesidir. Öne çıkarılan bu işlevler incelendiğinde, akıllı kentin büyük veri potansiyeline vurgu yapıldığı anlaşılmaktadır. Hatta yaşanan bu gelişmeler, veri odaklı kentleşme (*data-driven urbanism*) (Kitchin, 2016) kavramını da gündeme getirmektedir.

Temel istatistiksel teknikler üzerinden üretilen bilginin yetersiz kalması, politikalar açısından da büyük veriye yönelişi desteklemektedir. Genel olarak ele alındığında kamu sektöründe büyük verinin uygulama alanları aşağıdaki tabloda yer verildiği biçimde öne çıkmaktadır.

Tablo-1. Kamu Sektöründe Büyük Verinin Etki Alanları ve Potansiyelleri

	Büyük verinin etki alanları	**Büyük verinin taşıdığı potansiyeller**
World Bank, 2017: 2	Hizmet sunumu	Mevcut hizmetlerin iyileştirilmesi ve yeni hizmet alanlarının belirlenmesi
	Politika yapımı	Yeni ve gerçek zamanlı verilerin elde edilmesiyle politikaların belirlenmesi
	Vatandaş katılımı	Makine öğrenmesi gibi uygulamalarla vatandaşların geri bildirimine daha fazla duyarlı olunması
Maciejewski, 2017: 124; 130	Kamu denetimi	Usulsüzlüklerin, düzensizliklerin tespitinde
	Kamu düzenlemesi (politika belirleme)	Yönetilen alanların gerçek zamanlı takip edilmesini
	Kamu hizmeti sunumu	Sunulan hizmetlerin iyileştirilmesi
	Vatandaşların geri bildirimi	Kamu politikası hakkındaki düşüncelerin anlaşılması

Politika döngüsü üzerinden ele alındığında, Şekil 1'de yer verildiği gibi potansiyel katkıları barındırdığı anlaşılmaktadır. Fakat kamu örgütleri açısından; sistemsel, örgütsel ve bireysel düzeyde uyuma dikkat çekilmektedir (Pencheva, Esteve ve Mikhaylov, 2018: 6).



Şekil-1. Kamu Politikası Döngüsü Sürecinde Büyük Veri (Pencheva, Esteve ve Mikhaylov, 2018: 6).

Gelişen yeni teknolojilerin desteğiyle ortaya çıkan büyük verinin, politikaların geliştirilme sürecinde önemli bir rolünün olduğu kaçınılmaz gözükmektedir. Bu bağlamda ilgili veriler, kentin farklı politika alanlarında (ulaşım, lojistik, güvenlik, sağlık, eğitim, enerji, doğal kaynaklar, kamu yönetimi gibi) fayda sağlama potansiyeli taşımaktadır (bkz. Nuaimi vd., 2015: 7-8). İfade edilenler bağlamında Lim, Kim ve Maglio (2018: 92), akıllı kentlerde vatandaşlara, yerel yönetimlere, işletmelere ve ziyaretçilere katkı sağlamak amacıyla büyük veri kullanımını dört kategoride sınıflandırmaktadır. Birincisi (*preventive local administration*), bireysel kullanıcı aracılığıyla elde edilen veriler üzerinden sorunların ve ihtiyaçların tespit edilerek önleyici politikaların geliştirilmesine dayanmaktadır. İkincisi (*local operations management*), sunulan çeşitli hizmetler üzerinden elde edilen verilerle yerel yönetimlerin ve işletmelerin operasyonel açıdan geliştirilmesine katkı sağlamak amacıyla büyük verinin kullanımıdır. Üçüncüsü (*local network development*), kentte yaşayan tüketiciler/vatandaşların bağlantılılığı üzerinden verilerin elde edilerek hizmetlerin geliştirilmesi amacıyla verinin kullanımıdır. Dördüncüsü (*local information diffusion*), sunulan çeşitli hizmetler üzerinden elde edilen verilerin, analiz edilerek tüketicilere/vatandaşlara sunulmasıdır.

2. BÜYÜK VERİNİN İKİNCİ HALİ: AÇIK VERİ

Kentsel alanda karşılaşılan sorun ve ihtiyaçların karmaşıklığı, beraberinde farklı tarafların varlığını da önemli hale getirmektedir. Bu nedenle elde edilen verilerin farklı taraflarla paylaşımı politika geliştirme sürecinde önemli görülmekte ve açık veri kavramı söz konusu olmaktadır. Elde edilen veriler, farklı tarafların kullanımına sunulacak şekilde hazırlanan bir web portalı aracılığıyla açık hale getirilmektedir. Dünya genelinde nüfusu 1 milyonun üzerinde olan 68 yerel yönetim biriminin açık veri portalına sahip olduğu tespit edilmektedir (Erginli ve Tülek, 2019: 14). Açık veriyle birlikte; kamu hizmetlerinin iyileştirilmesi, yenilik, ekonomik büyüme ve mesleklerin ortaya çıkması, açıklığın ve hesap verebilirliğin yükselişi ve vatandaş katılımının sağlanması gibi faydalar beklenmektedir (Lee, Cyganiak ve Decker, 2014: 18). Diğer bir ifadeyle açık veri platformları sayesinde, kentleri daha iyi anlamak, bu sayede daha doğru politikalar geliştirmek ve bu süreçte vatandaşın katılımını sağlamak mümkün olabilmektedir (Erginli ve Tülek, 2019: 12). Bu noktada sürdürülebilir ve başarılı bir açık veri programının üç temel dayanağına dikkat çekilmektedir: gizlilik, veri koruma ve kamu güvenliği (EDP, 2016). Ayrıca bazı ülke uygulamaları üzerinden bazı unsurların (politika, portal, kalite ve etki) önemli olduğu tespit edilmektedir (Detaylı bilgi için bkz. EDP, 2019).

Açık verinin gündeme gelmesiyle birlikte, uluslararası düzeyde de birtakım ilkelerin, kriterlerin, düzenlemelerin ve projelerin geliştirildiği görülmektedir. Bu bağlamda 2013 yılında G8 Açık Veri Sözleşmesi (*Open Data Charter*) gerçekleştirilmiştir. Bu sözleşmeyle açık veriye yönelik şu ilkeler benimsenmiştir: Açıklığı varsayılan olarak belirleme, zamanında ve kapsamlı, erişilebilir ve kullanılabilir, karşılaştırılabilir ve birlikte çalışılabilir, yönetişimin ve vatandaş katılımının gerçekleştirilmesi, kalkınmayı ve yeniliği kapsama (https://opendatacharter.net/history/, 15. 09. 2019). Diğer taraftan akıllı kente giden süreçte kent verisi bağlamında küresel düzeyde standartlar geliştirmeye çalışan bir meclis [*The World Council on City Data* (WCCD)] oluşturulmuş ve bu oluşum kapsamında 17 farklı temada (ekonomi, eğitim, enerji, çevre, güvenlik, barınma, atık gibi) ve 100 göstergede veri standartları (ISO 37120) kabul edilmiştir (EDP, 2016b: 4). Bunların dışında bölgesel düzeyde de Avrupa Komisyonu tarafından 2003 yılında açık verinin kullanımıyla ilgili bir direktif (2003/98/EC) yayınlanmış ve çeşitli projeler [Open Cities (2011-2013), City SDK (2012-2014) ve Icity (2012-2015)] hayata geçirilmiştir (EDP, 2016b: 7-8).

3. BÜYÜK VERİYLE GÜNDEME GELEN GÜÇLÜKLER VE TEHDİTLER

Büyük verinin elde edilmesi, analitiğine/madenciliğine yönelik tekniklerin artış göstermesi, daha fazla verilerin elde edilir olması, tutulma ve işleme maliyetlerinin azalması, veri üzerinden daha fazla bir değer üretilmesi gibi gelişmeler, büyük veri üzerine ilgiyi artırmış ve dolayısıyla bu gelişmeler beraberinde kişisel düzeyde bazı ihlalleri ve endişeleri gündeme getirmeye başlamıştır (Akıncı, 2019: 33; 41; Akt. Kitchin, 2016: 6). Hatta bu gelişmeler aynı zamanda yeni bir dijital güvensizlik (*digital insecurity*) dönemi olarak da ifade edilmektedir (Joo ve Tan, 2018).

Lim, Kim ve Maglio (2018: 94) tarafından akıllı kentlerde, veriden bilgiye dönüşüm sürecinde veri kullanımının güçlükleri şu şekilde sıralanmaktadır:

- Veri kalitesinin yönetimi
- Farklı verilerin entegrasyonu
- Veri gizliliğinin sağlanması (özel hayatın gizliliği)
- Farklı tarafların (yerel yönetimler, vatandaşlar, işletmeler, ziyaretçiler gibi) ihtiyaçlarının anlaşılması
- Coğrafi bilgiyi sağlayacak yöntemlerin geliştirilmesi
- Akıllı kent hizmetlerinin tasarlanması

Nuaimi vd. (2015: 6-9) ve Morabito (2015: 33-35) ise akıllı kentlerde büyük veriyle bağlantılı olarak şu güçlüklere dikkat çekmektedir:

- Verilerin kaynağı (çeşitliliği) ve karakterleri
- Verinin sahipliği (özellikle açık verilerde)
- Veri ve bilgi paylaşımı
- Veri kalitesi
- Güvenlik ve gizlilik
- Sivil özgürlükler ve eşitlik (bir kısmının veri üretimine dahil olmaması)
- Maliyetler
- Kent nüfusunun değişkenliği
- Veri analitiğinde yetenekli kişilerin bulunmayışı

Veriyle ilişkili olarak ortaya çıkan endişeleri/riskleri Tablo 2'de yer verildiği üzere, birbirini tamamlayan gizlilik ve güvenlik başlığı altında toplamak mümkün olabilir.

Tablo-2. Verilerin Gizliliği ve Güvenliğinde Etkili Olan Unsurlar (Ijaz, Shah, Khan ve Ahmed , 2016: 615; Jansater ve Olsson, 2018: 17-18; Georgescu ve Popescul, 2016: 8-10; AlDairi ve Tawalbeh, 2017: 1089-1090).

Verilerin Güvenliği	**Teknolojik faktörler (altyapı)** • Veriyi ortaya çıkaran teknolojilerin (RFID, SCADA, GPS, Bluetooth, sensörler, mobil, vb.) güvenlik altyapı eksikliği • Güncellemelerin ve bakımların zamanında yapılmaması • Bir birine bağlı olma etkisi **Yönetim faktörler** • Bilgi eksikliğinden kaynaklı önem verilmemesi, • Gerekli insan kaynağının bulunmaması ve insan hataları • Örgütsel birimin olmayışı, • Dış kaynaklardan kaynaklanan (tedarikçilerin rekabet şartları altında güvenliğe yeterince önem vermemesi gibi) • Güvenlik sistemlerinin test edilmemesi gibi. **Sosyo-ekonomik faktörler** • Veriyi üretenlerin farkındalık eksikliği, • Maliyetlerin yüksekliği ve kaynakların kısıtlılığı
Verilerin Gizliliği	Anonimleştirilen verilerin kişilerle ilişkilendirme potansiyeli Büyük verinin amacı dışında kullanımı Verilerden çıkarımların şeffaflık ilkesi çerçevesinde yapılmaması (ayrımcılığın oluşması gibi) ve yanlış çıkarımlarda bulunma ihtimali Tüm verilerin elde edilme potansiyeli ve veri minimizasyonundan uzaklaşılması Art niyetli kullanım ve üçüncü taraflarla izinsiz paylaşımı

Tablo 2 incelendiğinde verilerin elde edilmesi, saklanması, işlenmesi ve sunulmasında yararlanılan altyapı; örgütsel yapının ve insan kaynağı ile veriyi üretenlerle ilişkili olarak sosyal bileşenlerin ve bütçenin etkili faktörler olduğu anlaşılmaktadır.

Nesnelerin, internetle bağlantılı hale gelmesi ve bu sayede üretilen verilerin bulut sisteminde depolanması, veriye yönelik uzaktan müdahaleleri kolaylaştırmakta ve akıllı kentlerde dijital sistemleri hassas hale getirmektedir (Pelton ve Singh, 2019: 7). Bu bağlamda Joo ve Tan (2018: 94) siber-fiziksel tehditler bağlamında dört kritik güvenlik açığını aşağıda yer verilen Tablo 3'de gösterildiği gibi vurgulamaktadır.

Tablo-3. Siber Alanda Güvenlik Açıkları

Güvenlik Açıkları	**Temel Özellikleri**
Endüstriyel kontrol sistemleri	Gerçekleştirilecek saldırılarla kritik alt yapının devre dışı bırakılması ve bir yerde ortaya çıkan bozulmanın diğer alanlara da yansıması.
Kaynakları kısıtlı birimler	Güvenlik konusunda gerekli önlemlerin alınmamasından dolayı saldırıların gerçekleşmesi ve saldırıların kopyalanarak devam etmesi.
Wireless iletişimi	Bağlantı kurulan cihazlara saldırıların [man in the middle (MitM)] kolaylaşması, içeriğin algılanabilir ve değiştirilebilir olması.
Bulut depolama	Verilerin sanal bir alanda toplanmasının saldırıların hedefi haline gelebilmekte ve veri güvenliğinin ilgili servis sağlayıcılara bağlı olması.

Verilerin siber ortamda dolaşıma girmesiyle siber saldırı kavramı gündeme gelmektedir. Siber saldırılar, dijital teknolojilerin barındırdığı güvenlik açıklarını (şifreleme ve yazılım güvenliğinin zayıflığı, eski sistemlerinin kullanımı, insan hataları gibi) kullanmaya çalışmaktadır (Kitchin ve Dodge, 2019: 49-51). Farklı yöntemlerle (Patel ve Doshi, 2019: 183-188) gerçekleştirilen saldırılar; nesnelerin arasında veri akışına müdahale etme (veri tabanı kontrol ve gözetleme sistemi (SCADA), RFID takip ve kontrol sistemi gibi uygulamalarda), bulut sisteminde depolanan alanlara sızarak veriyi elde etme veya zarar verme veya verilerin sunulması esnasında verilerin manipüle edilmesi, durdurulması veya elde edilmesi şeklinde ortaya çıkabilmektedir (Özdağ ve Kılıç, 2019: 11;) (2006 sonrası gerçekleşen farklı siber saldırı örnekleri için bkz. https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents, 10. 09. 2019). Ayrıca aşağıda yer verilen alanlarda farklı açılardan potansiyel saldırılara dikkat çekilmektedir (Lin vd., 2017: 28).

Tablo-4. Siber Saldırı Alanları

Kritik Sektörler	Muhtemel Saldırı Alanları			
	Kamu güvenliği	**Finans**	**Operasyonlar**	**Gizlilik**
Enerji	Güç kaynağında oluşacak bozulmayla bazı fonksiyonların etkilenmesi	Fidye veya enerji hırsızlığı	Enerji yönetim sisteminin bağlantılarına zarar vermek	Sayaç verileri ve vatandaş bilgisini çalmak
Ulaşım	Kazalara sebebiyet verme	Ücretsiz ulaşım elde etmek veya araçları rehin almak	Ulaştırma hizmetlerini kesmek ve değiştirmek	Kullanıcı verilerini ele geçirmek
Çevre	Akıllı atık su sistemine zarar vermek	Sistemleri durdurmak veya cihazları rehin almak	Komutları değiştirme ve sistem bildirimlerini bozma	Faaliyetleri izlemek için sensörlerden yararlanmak
Bağlantılılık		Sistemleri durdurmak veya cihazları rehin almak	Sistemlere zarar vermek için ağ iletişimini bozmak	Bilgileri elde etmek için bağlantılara zarar vermek
Yönetişim/Yönetim		Sistemleri durdurmak veya cihazları rehin almak	Sistemleri veya cihazları rehin tutmak; bağlantılı cihazları bots'a dönüştürmek	Açık veri ve geri bildirimlerle ilgili bilgilerin elde edilmesi

Yaşanan bu gelişmeler siber güvenlik konusuna ayrıca önem vermeyi gerekli kılmaktadır. Bu bağlamda ülkelerin farklı çabaları öne çıkmakta (Detaylı bilgi için bkz. Göçoğlu, 2019: 107-158) ve ülkelerin siber güvenlik konusundaki durumlarını yansıtan indeksler yayımlanmaktadır (bkz. Özdağ ve Kılıç, 2019: 10).

4. VERİNİN GİZLİLİĞİNİ VE GÜVENLİĞİNİ SAĞLAYAN İLKELER VE YAKLAŞIMLAR

Akıllı kent uygulamalarının yaygınlığının hızlanması, beraberinde bazı sorunların etkisini de artırmaktadır. Kentlerin internet ağlarıyla daha fazla örülmesi, siber güvenliği önemli bir unsur haline getirmeye başlamıştır (Göçoğlu, 2019). Bu nedenle akıllı kentlerde güvenlikle ilgili problemler, güncelliğini ve gerçekliğini korumaktadır (AlDairi ve Tawalbeh, 2017: 1088).

Büyük verilerin önemli bir kısmı kişisel verilerden oluşmaktadır. Bu noktada veriyi üretenlerin rızası olmadan kişisel verilerin kullanılması ve taraflarla paylaşılması, hak ihlallerini gündeme getirmektedir. Kişisel veriler bağlamında özel hayatın korunması modern devletlerin kabul ettiği temel ilkelerden biridir. Veri koruma içinde yer alan "mahremiyet", insan haklarının bir bileşeni olarak uluslararası sözleşmelerin ve ulusal düzenlemelerin önemli gündem maddesine karşılık gelmektedir (Akıncı, 2019: 57; kişisel verilerin korunması hususunda gerçekleştirilen ulusal ve uluslararası düzenlemelerin detayları için bkz. Akıncı, 2019: 59-91; Yılmaz, 2019: 149-195). Ayrıca teknolojik gelişmeler büyük verinin mekansal bağlılığını ortadan kaldırmakta ve dolayısıyla veri güvenliği konusunda ülkeler arasında daha fazla iş birliklerine ihtiyaç duyulmaktadır (Akıncı, 2019: 48). Verilerin gizliliğini ve güvenliğini artırmak amacıyla farklı ilkelerin belirlendiği anlaşılmaktadır. Çalışmanın bu kısmında uluslararası ve ulusal düzeyde öne çıkan düzenlemelere ve benimsenen ilkelere yer verilmektedir.

İfade edilenler bağlamında uluslararası alanda ilk olarak OECD tarafından 1980 yılında "*Mahremiyetin ve Kişisel Verilerin Sınırlar Arası Aktarımının Korunması Hususunda Rehber İlkeler*" yayımlanmıştır. Aşağıda yer verilen Tablo 5'te görüldüğü gibi veri koruma konusunda sekiz ilkeye yer verilmiş, bunlarla birlikte bir altyapı oluşturulmaya çalışılmıştır (Akt. Yılmaz, 2019: 124). Veri korumayı odağına alan ikinci uluslararası düzenleme ise BM'nin çalışmaları kapsamında şekillenen ve ortaya çıkan, 1990 yılında yayımlanan "*Bilgisayarda İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler*"dir. Buradaki düzenlemeyle veri koruma konusunda ilk kez yetkili bir organa yer verilmiştir (Akt. Yılmaz, 2019: 126).

AB düzeyinde 1995 yılında "*AB Veri Koruma Direktifi*" (95/46/EC) yayımlanmıştır. Sonrasında ise AB düzeyinde "*Veri Koruma Tüzüğü*" kabul edilmiş (2016) ve uygulanmaya (2018) başlanmıştır. Bu düzenlemenin büyük verideki gelişmeler üzerine şekillendiği anlaşılmaktadır. Tüzüğün temel amacı, verilerin işlenmesi ve farklı taraflar arasında dolaşımı sırasında gerçek kişilerin

temel hak ve özgürlüklerini korumak olarak ifade edilmektedir (Akıncı, 2019: 86). Tüzüğün şu üç önemli alanda yenilikler getirdiği anlaşılmaktadır: kişisel verilerin ve veri sahiplerinin daha etkin korunması, veri işleyenler ile veri kontrolörlerini artırılmış sorumluluğu ve mekansal anlamda daha geniş uygulama alanına sahip olunması (Akıncı, 2019: 79-86). Tüzük kapsamında Tablo 5'de yer verilen ilkeler pro-aktif bir yaklaşımla benimsenmiştir.

Tablo-5. Verilerin Korunmasına Yönelik Ulusal - Uluslararası Düzenlemeler ve Benimsenen İlkeler (Akıncı, 2019: 86-87; Yılmaz, 2019: 124-126).

Kararlar/Düzenlemeler	**İlkeler**
OECD Mahremiyetin ve Kişisel Verilerin Sınırlar Arası Aktarımının Korunması Hususunda Rehber İlkeler (1980)	Veri toplamanın sınırlı olması ilkesi Veri kalitesi ilkesi Amacın belli olması ilkesi Kullanmanın sınırlı olması ilkesi Veri güvenliği ilkesi, Açıklık ilkesi Bireysel katılım ilkesi Hesap verebilirlik ilkesi
BM Bilgisayarda İşlenmiş Kişisel Veri Dosyalarına İlişkin Rehber İlkeler (1990)	Kanunilik ve dürüstlük ilkesi Doğruluk ilkesi Amacın belirliliği ilkesi İlgili kişinin erişimi ilkesi Ayrımcılık yapılmaması ilkesi İstisna koyma ilkesi
6698 sayılı Kişisel Verilerin Korunması Kanunu (2016)	Hukuka ve dürüstlük kurallarına uygun olma Doğru ve gerektiğinde güncel olma Belirli, açık ve meşru amaçlar için işlenme İşlendikleri amaçla bağlantılı, sınırlı ve ölçülü olma İlgili mevzuatta öngörülen veya işlendikleri amaç için gerekli olan süre kadar muhafaza edilme
AB Veri Koruma Tüzüğü (2018)	Hukukilik, dürüstlük ve şeffaflık Amaçla sınırlılık Veri minimizasyonu Doğruluk Veri saklamanın sınırlandırılması Bütünlük ve gizlilik Veri işleyenler ile veri kontrolünün eşit düzeyde sorumluluğu Veri koruma etki değerlendirmesi Hesap verebilirlik

Türkiye özelinde ele alındığında ise kişisel verilerin korunmasına yönelik gelişmelerin Sekizinci Kalkınma Planı'yla başladığı ve Onuncu Kalkınma Planı uygulama süreci içinde somut olarak 2016 yılında 6698 sayılı *Kişisel Verilerin korunması Kanunu*'nun yürürlüğe konulduğu anlaşılmaktadır. Bu kanunda AB'nin 95/46/EC sayılı direktifinin etkili olduğu ifade edilmektedir (Akıncı, 2019: 131-135).

Benimsenen ilkeler incelendiğinde verilerin elde edilmesinde ve kullanılmasında, veriyi üreten kişileri koruma ve bu anlamda oluşabilecek tereddütleri giderme çabasının olduğu anlaşılmaktadır.

Verinin gizliliğini ve güvenliğini iyileştirmek amacıyla farklı yaklaşımların, çabaların ortaya çıktığı anlaşılmaktadır. Bu çabalar teknik ve yönetsel açıdan gündeme gelmektedir. Teknik açıdan bazı araçlar ve yöntemler öne sürülmektedir. Araçlar bağlamında güvenilir veri depolama ve işlem logları, uç nokta giriş onaylama/filtreleme, gerçek zamanlı güvenlik görüntüleme, kriptografik zorunlu veri merkezli güvenlik, ölçeklenebilir ve birleştirilebilir gizlilik korumalı veri madenciliği ve matematiksel analiz gibi tekniklere yer verilmektedir (Akt. Eyüpoğlu vd., 2017: 178). Yöntem açısından ise desen gizleme, güvenli dağıtımlı veri madenciliği, k-anonimlik veya kimliksizleştirme, homomorfik şifreleme gibi yöntemler öne çıkarılmaktadır (Akt. Eyüpoğlu vd., 2017: 179-183).

Yönetsel açıdan ele alındığında bir yöntem olarak ayrı bir örgütsel yapılanma önem kazanmaktadır. Bu sayede ilgili konuları daha iyi yönetmek mümkün hale gelebilmektedir. Bu bağlamda Dubai örneğinde oluşturulan "E-Güvenlik Merkezi" dikkat çekmektedir. Merkez; e-güvenlikle ilgili teknik araçları, veri güvenliğini, ilgili kurumlar arasında koordinasyonu, gerçekleştirilecek düzenlemelerde ve planlara katkı sağlamak gibi çabaları göstermektedir (Efthymiopoulos, 2016: 11). İkinci bir yaklaşım, dışarıdan gözetimin güçlendirilmesi şeklindedir. Bu kapsamda Hollanda'da faaliyet gösteren *Review Committee on the Intelligence and Security Services* (CTIVD) birimi önemli bir örneği teşkil etmektedir (Broeders vd., 2017: 319-320). Bir diğer önemli yaklaşım ise risk yönetimi anlayışıyla verinin güvenliğinin ve gizliliğinin sağlanmasıdır. Risk yönetimi bir tehlike ihtimalinin öncesinde sistematik ve titizlikle değerlendirildiği ve yönetildiği bir sürece karşılık gelmektedir. Bu yaklaşımın avantajı dijital sistemlerin incelenmesinin zorunlu kılınmasından kaynaklanmaktadır. Risk temelli bu yaklaşım, akıllı kentlerdeki koruma görevini azaltacaktır. Bu yaklaşım kapsamında iki strateji öne sürülmektedir: 1. Kent yönetimlerinin, saldırılara karşı daha sıkı güvenlik

önlemlerini oluşturması ve 2. Kent yöneticilerinin, gerçekleştirilen saldırıları caydırmak için cezaların artırılmasıdır (Joo ve Tan, 2018: 100-102). OECD tarafından belirlenen mahremiyet ilkeleri arasında da risk yönetimine yer verildiği görülmektedir (Akıncı, 2019: 128).

Kitchin ve Dodge (2019: 58-59) ise akıllı kentleri güvenli hale getirmenin yöntemlerini iki başlık altında ele almaktadır. Birincisi, erişim kanalarının iyileştirildiği, güvenlik yazılımlarının iyileştirildiği ve güvenliğe yönelik ayrı bir birimin oluşturulduğu geleneksel yöntemlerdir. İkincisi ise piyasa ve devlet odaklı yasal düzenlemeler ve yaptırımlardan oluşmaktadır. Burada da iki seçenek öne çıkmaktadır: özel sektör temsilcilerinin belirlediği standartlar üzerinden güvenliğin oluşturulması ve kuralların, standartların ve yaptırımların devlet öncülüğünde gerçekleşmesidir.

SONUÇ YERİNE: HENÜZ YOLUN BAŞINDAYKEN KENTLERDE NELERİ DİKKATE ALMALIYIZ?

Gelinen bugünkü noktada kentsel alanda, temel istatistikler ve ortalama değerler üzerinden sorunları ve ihtiyaçları belirlemeye çalışarak politika üretmek etkinliğini yitirmektedir. Çünkü ortaya çıkan yeni teknolojiler, yaşanan deneyimlerin verileştirilmesini mümkün hale getirmektedir. Elde edilen bu büyük veriler üzerinden gerçekleştirilecek analitik çalışmalar, kararları daha etkin hale getirerek politikaların geçerliliğini güçlendirebilmektedir. Ayrıca deneyimlerinin verileştirilmesiyle vatandaşın katılımını dolaylı olarak sağlayabilmektedir. Fakat büyük veriler tüm bu potansiyel faydalarına rağmen verilerin gizliliği ve güvenliği konusundaki bazı endişeleri/güçlükleri/riskleri beraberinde taşımaktadır. Gündeme gelen bu olumsuzluklar dikkate alınmadığında, özellikle veriyi üreten taraflar açısından çeşitli zararlara yol açması mümkün olmaktadır. Bu olumsuzlukların azaltılması amacıyla büyük veriye yönelik gizlilik ve güvenlik önlemleri geliştirirken, büyük verinin avantajları ile bireysel haklar arasında bir uzlaşı sağlayan yaklaşımlara ihtiyaç duyulmaktadır (Akıncı, 2019: 47-48).

İfade edilenler kapsamında kentsel alanda yeni teknolojileri yaygınlaştırırken ve bunlar üzerinden büyük veriyi elde ederken, aşağıda yer verilen hususlar dikkate değer görülmektedir (Lim, Kim ve Maglio, 2018: 92; Lin vd., 2017: 30-32; Kitchin ve Dodge, 2019: 59-60):

- Büyük veri kullanımı konusunda çok fonksiyonlu bir çalışma takımı oluşturmak, ayrı bir alt örgütlenmeye gitmek, ayrı bir bütçe oluşturmak,

- Risk yönetimi yaklaşımı bağlamında büyük veriyi yönetmek,
- Kalite kontrol ve penetrasyon testlerinin zamanında yapılması,
- Hizmetlere yönelik anlaşmalarda (dışarıdan hizmet satın almalarda) güvenliğin öncelikli hale getirilmesi,
- Büyük verinin de içinde yer aldığı dijital konularla ilgili bir acil durum ekibinin oluşturulması,
- Yazılım güncellemelerinin geçerliliğini ve güvenliğini sağlamak, zamanlamasına dikkat etmek, bu noktada dış paydaşlarla etkili iş birliği içinde olmak,
- Güvenlik altyapısını uzun dönemli bir bakış açısıyla ele almak,
- Farkındalık ve bilgi düzeyini artıracak eğitimlerin gerçekleştirilmek (vatandaşlara ve çalışanlara yönelik), gizlilik bildirimlerini kullanıcı dostu tasarlamak,
- Gizliliği göz önünde bulundurarak verileri işlemek,
- Ortak iletişim kanallarının şifrelenmesi, doğrulanması ve düzenlenmesini sağlamak,
- Kimi zaman manuel olarak geçersiz kılmaya izin verilmesi, bazı sistemlerin "sağır" (ağa bağlı olmayan) ve "dilsiz" (kodla otomatikleştirilmemiş) oluşturulması,
- "Kişisel verilerin korunması"nın ötesinde büyük veriyi esas alan hukuki düzenlemelere ihtiyaç duyulması,
- İletişim kanallarında "şifreleme" yönteminin etkin kullanımının sağlanması,
- Veri güvenliği konusunda daha fazla iş birliklerin geliştirilmesi, uluslararası düzeyde belirlenen standartların hayata geçirilmesi,
- Dışarıdan gözetimin güçlendirilmesi, açıklığın artırılmasıdır.

KAYNAKÇA

Akıncı, A. Ş. (2019). *Büyük Veri Uygulamalarında Kişisel Veri Mahremiyeti*. (Yayımlanmamış Uzmanlık Tezi). T.C. Cumhurbaşkanlığı Strateji ve Bütçe Başkanlığı, Sektörler ve Kamu Yatırımları Genel Müdürlüğü, Ankara.

AlDairi, A. ve Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, 109C, 1086-1091.

Broeders, D., Schrijvers, E., Sloot, B., Brakel, R. Hoog, J. ve Ballin, E. (2017). Big Data and Security Policies: Towards a Framework for Regulating The Phases of Analytics and Use of Big Data. *Computer Law & Security Review*, 33, 309-329.

EDP (2019). *Analytical Report 13: Open Data Best Practices in Europe's Top Performers: Ireland, Spain and France*. Erişim Tarihi: 16 Eylül 2019, https://www.europeandataportal.eu/en/content/report-13-open-data-best-practices-europe%E2%80%99s-top-performers-ireland-spain-and-france.

EDP (2016): *Analytical Report 3: Open Data and Privacy*. Erişim Tarihi: 16 Eylül 2019, https://www.europeandataportal.eu/sites/default/files/open_ data_ and_ privacy_v1_final_clean.pdf.

EDP (2016b): *Analytical Report 4: Open Data in Cities*. Erişim Tarihi: 16 Eylül 2019, https://www.europeandataportal.eu/sites/default/files/edp_analytical_ report_n4_-_open_data_in_cities_v1.0_final.pdf.

Erginli, B. E. ve Tülek, M. (2019). *Kentsel Politikanın Desteklenmesi için Yeni Araçlar: Açık Veri Platformları ve Dijital Kent Panelleri*. İstanbul: TESEV Yayınları.

Eyüpoğlu, C., Aydın, M. A., Sertbaş, A., Zaim, A. H. ve Öneş, O. (2017). Büyük Veride Kişi Mahremiyetinin Korunması. *Bilişim Teknolojileri Dergisi*, 10 (2), 177-184.

Georgescu, M. ve Popescul, D. (2016). The Importance of Internet of Things Security for Smart Cities. İçinde I. N. Da Silva and R. A. Flauzino (Ed.) *Smart Cities Technologies* (3-18). InTech.

Göçoğlu, V. (2019). Akıllı Şehirlerdeki Kritik Altyapıların Siber Güvenliği. *Uluslararası Yönetim Akademisi Dergisi,* 2 (1), 51-63.

Göçoğlu, V. (2019). *Türkiye'nin Siber Güvenlik Politikalarının Kamu Politikası Analizi Çerçevesinde Değerlendirilmesi*. (Yayınlanmamış Doktora Tezi). Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

Ijaz, S., Shah, M. A., Khan, A. ve Ahmed, M. (2016). Smart Cities: A Survey on Security Concerns. *(IJACSA) International Journal of Advanced Computer Science and Applications,* 7 (2), 612-625.

Jansater, G. ve Olsson, O. (2018). *Cyber Security in Smart Cities Not a Primary Concern*. Master thesis, Department of Informatics, Lund School of Economics and Management, Lund University.

Joo, Y.-M. ve Tan, T.-B. (2018). Smart Cities: A New Age of Digital Insecurity. *Survival*, 60 (2), 91-106. DOI: 10.1080/00396338.2018.1448577.

Kitchin, R. (2016). *Theethicsofsmartcitiesand Urbanscience*. Phil.Trans.R. Soc., 1-15, http://dx.doi.org/10.1098/rsta.2016.0115.

Kitchin, R. ve Dodge, M. (2019): The (In)Security of Smart Cities: Vulnerabilities, Risks, Mitigation, and Prevention. *Journal of Urban Technology*, 26 (2), 47-65. DOI: 10.1080/10630732.2017.1408002.

Lee, D., Cyganiak, R. ve Decker, S. (2014). *Open Data Ireland: Best Practice Handbook*. Erişim Tarihi: 14 Eylül 2019, https://data.gov.ie/uploads/page_images/2019-04-24-104248.848906Best-Practice-Handbook.pdf.

Lim, C., Kim, K.-J. ve Maglio, P. P. (2018). Smart Cities with Big Data: Reference Models, Challenges and Considerations. *Cities*, 82, 86-99.

Lim, C. ve Maglio, P. (2018). Data-Driven Understanding of Smart Service Systems Through Text Mining. *Service Science*, 10 (2), 154-180.

Lin, P., Swimmer, M., Urano, A., Hilt, S. ve Vosseler, R. (2017). *Securing Smart Cities Moving Toward Utopia with Security in Mind*. A TrendLabs Research Paper, Erişim Tarihi: 15 Eylül 2019, https://documents.trendmicro.com/assets/wp/wp-securing-smart-cities.pdf.

Maciejewski, M. (2017). To Do More, Better, Faster and More Cheaply: Using Big Data in Public Administration. *International Review of Administrative Sciences*, 83 (15), 120-135. DOI: 10.1177/0020852316640058.

Morabito, V. (2015). *Big Data and Analytics, Strategic and Organizational Impacts*. Switzerland: Springer.

Nuaimi, E., Al-Neyadi, H. A., Mohamed, N. ve Al-Jaroodi, J. (2015). Applications of Big Data to Smart Cities. *Journal of Internet Services and Applications*, 6 (25), 1-15.

Özdağ, H. O. ve Kılıç, G. O. (2019). Bilgi Savaşları ve Arka Plandakiler. *Bilim ve Gelecek*, Ağustos, 6-13.

Pelton, J. N. ve Singh, I. B. (2019). *Smart Cities of Today and Tomorrow Better Technology, Infrastructure and Security*. Switzerland: Springer.

Pencheva, ı., Esteve, M. ve Mikhaylov, S. J. (2018). Big Data and AI – A Transformational Shift for Government: So, What Next for Research?. *Public Policy and Administration*, 1-21. DOI: 10.1177/0952076718780537.

Yılmaz, B. (2019). *Türk Anayasa Mahkemesi Ve Avrupa İnsan Hakları Mahkemesi Kararları Işığında Kişisel Verilerin Korunması*. (Yayınlanmamış Doktora Tezi). Hacettepe Üniversitesi, Sosyal Bilimler Enstitüsü, Ankara.

World Bank (2017). *Big Data in Action for Government*, Erişim tarihi: 15 Eylül 2019, http://documents.worldbank.org/curated/en/176511491287380986/Big-data-in-action-for-government-big-data-innovation-in-public-services-policy-and-engagement.

EXAMINING THE CHALLENGES OF POLICING ECONOMIC CYBERCRIME IN THE UK

Naci AKDEMİR[*] Bülent SUNGUR[**] Bürke Uğur BAŞARANEL[***]

Abstract

Cybercrime has received the 'Tier One' national security risk status in many countries due to the increased cyber threats. In response to this severe threat, governments have announced a substantial amount of investment in cybercrime prevention programmes. It is evident that tackling cybercrime requires expertise and cybersecurity skills as the networked global nature of the Internet pose significant challenges to policing cybercrime. Previous policing cybercrime studies illustrated that local police officers lack the technical skills, which obviously hampered the fight against cybercrime. Police forces continue enhancing their ability to tackle cybercrime through specialised cybercrime units. Nevertheless, there is a dearth of empirical research examining policing problems of economic cybercrime through the lenses of expert police officers working in cybercrime departments. This empirical research addresses this knowledge gap in the literature. A thematic analysis method was employed to analyse semi-structured interviews conducted with expert police officers working at cybercrime departments in the United Kingdom.

Lack of international cooperation, underreporting of economic cybercrime incidents and lack of victim awareness emerged as key challenges. Police officers' views regarding private sector involvement in policing economic cybercrime appear to be tentative due to ethical concerns. Public-private partnership in combatting cybercrime appears to be an effective solution to enhance the effectiveness of combatting cybercrime. European Union (EU)'s new Cybersecurity Act (Regulation 2019/881), which restructures the European Union Agency for Network and Information Security (ENISA) is the latest example of public-private partnership in combatting cybercrime. However, the results of this study suggest that the scope of this initiative should be extended to non-EU countries to maintain global cybersecurity.

Keywords: *Cybercrime, Cybersecurity, Policing, Public-Private Partnership, Economic Cybercrime*

[*] Dr., Öğretim Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, naciakdemir@jandarma.gov.tr ORCID: https://orcid.org/0000-0002-4288-6482

[**] Öğretim Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, bulentsunger@gmail.com ORCID: https://orcid.org/0000-0002-0705-0049

*** Dr., Öğretim Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, bubasaranel@gmail.com ORCID: https://orcid.org/0000-0003-4760-2925

Makale Geliş Tarihi: 28.10.2019 Makale Kabul Tarihi: 09.01.2020

BİRLEŞİK KRALLIKTA SİBER EKONOMİK SUÇLARA YÖNELİK KOLLUK FAALİYETLERİ SORUNLARININ İNCELENMESİ

Öz

Artan siber tehditler nedeniyle siber suçlar pek çok ülke tarafından 'Birinci Öncelikli' ulusal güvenlik riski olarak nitelendirilmektedir. Bu ciddi riske tepki olarak hükümetler siber suçların önlenmesi programlarına ciddi yatırımlar yapmaktadır. Internetin ağlarla birbirine bağlı küresel karakterinin siber suçların kolluğuna ciddi zorluklar yaratması nedeniyle, siber suçlarla etkin mücadele için uzmanlığa ve teknik yeteneklere ihtiyaç duyulduğu aşikârdır. Siber suçların kolluğu hakkındaki önceki bilimsel araştırmalar yerel polisin uzmanlık eksikliğinin olduğunu ve bunun siber suçlarla mücadeleyi sekteye uğrattığını ortaya koymaktadır. Kolluk kuvvetleri siber suçlarla mücadele kapasitelerini arttırmak kapsamında uzman siber suçlarla mücadele birimlerini ihdas etmeye devam etmektedir. Fakat literatürde siber ekonomik suçlarla mücadele eden uzman birimlerin karşılaştığı sorunları uzman kolluk kuvvetlerinin gözünden ortaya koyan çalışma sayısının az olması dikkat çekicidir. Literatürdeki bu bilgi açığını gidermek maksadıyla Birleşik Krallık siber suçlarla mücadele birimlerinde görevli uzman polis memurları ile icra edilen yarı yapılandırılmış mülakatlardan elde edilen veriler tematik analiz yöntemi ile analiz edilmiştir.

Uluslararası işbirliği eksikliği, suç olaylarının kolluğa yeterince bildirilmemesi ve mağdurların siber suçlar farkındalık eksikliği en önemli sonuçlar olarak ortaya çıkmıştır. Özel firmaların siber ekonomik suçların kovuşturulmasına katılımı konusunda ise polis memurlarının etik kaygılar nedeniyle çekimser oldukları görülmüştür. Siber suçlarla mücadelede kamu-özel sektör işbirliğinin siber suçlarla mücadelenin etkinliğini arttıracak önemli bir çözüm olduğu değerlendirilmektedir. Avrupa Birliği (AB)'nin Ağ ve Bilgi Güvenliği Ajansı (ENISA)'nı yeniden yapılandıran yeni siber güvenlik yasası (Regulation 2019/881) siber suçlarla mücadelede kamu-özel sektör işbirliği kapsamda atılmış önemli bir adımdır. Fakat çalışmamızın sonuçları siber güvenliğin dünya çapında sağlanması için bu inisiyatifin AB üyesi olmayan ülkeleri de kapsaması gerekliliğini ortaya koymaktadır.

Anahtar Kelimeler: *Siber Suçlar, Siber Güvenlik, Suçların Kolluğu, Kamu-Özel Sektör İşbirliği, Siber Ekonomik Suçlar*

INTRODUCTION

The advent of the Internet and its commercial applications have significantly changed the way we socialise, shop or communicate. However, the widespread use of the Internet is not free from its problems. It is argued that the commercial application of the Internet has not only provided new opportunities for the commission of the traditional crime, but it has also given rise to new forms of crimes (Wall, 2007b; Lee, Holt, Burruss, and Bossler, 2019).

Recent research illustrates that cybercrime is the fastest grown crime in the world (Graham, 2017; Summerville, 2017). It is predicted that 23% of United States (US) population experienced cybercrime victimization in 2018 (Reinhart, 2018). Similarly, Action Fraud reported that Internet users lost £34.6m as a result of cybercrime between April and September 2018, which indicates a %24 rise when compared to the previous 6 months (BBC, 2019).

This increased cyber threat has caused public tension, which motivated national and international bodies to put cybercrime and cybersecurity on top of their agendas (Kshetri, 2013; Wall and Williams, 2014; Holt, Burruss, and Bossler, 2018). Hence, combatting and policing cybercrime have increasingly been stressed in many national and international documents (i.e. The Council of Europe Cybercrime Convention (ETS No. 185), The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders (2000)).

Despite growing public concern fuelled by the increased number of cyber-attacks, adverse financial and psychological impacts of cybercrime, there is a dearth of empirical research examining policing problems of economic cybercrime through expert police officers' lenses. This empirical research aims to address this knowledge gap in the literature by discerning policing problems of economic cybercrime in the UK.

1. LITERATURE REVIEW

The first part of the literature review deals with two controversial issues in cybercrime literature: definition of cybercrime and the novelty of cybercrime. The second part of the review outlines previous empirical research related to the policing problems of cybercrime and perceptions of police officers.

1.1. Defining Cybercrime

It is generally considered that there is a lack of agreement around a standard definition of the cybercrime in the literature (Wall, 2008; Anderson, Barton, Böhme, Clayton, Van Eeten et al., 2013; Williams and Levi, 2015). The Council of Europe Cybercrime Convention (ETS No. 185), which is also known as Budapest Convention, is one of the first international initiatives to create a shared understanding of cybercrime (Wall, 2013a), though the convention caused significant discomfort regarding its imbalance between public liberties and power delegated to governments about surveillance, search and seizure of computers (Taylor, 2002). Rather than providing an umbrella definition, this convention

highlights the importance of deterrence. The Convention defines the scope of the deterrence as "action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct" (The Council of Europe Convention on Cybercrime, 2001: 2), and presents sub-categories of cybercrime within four titles. A number of cybercrimes were defined within these four categories. However, this approach received criticism from the authors as it does not include some sorts of cybercrime like stalking, extortion (Brenner, 2007), online identity theft, and spamming (Clough, 2014).

Commission of the European Communities also published a communication to the European Parliament about combatting cybercrime in 2007. This report defines cybercrime as "criminal acts committed using electronic communications networks and information systems or against such networks and systems" (European Commission, 2007: 2). Contrary to the Council of Europe's broad definition, Commission perceives cybercrime in a narrow sense. This definition again excludes the cases related to illicit online activities.

United Nations is another international actor that dealt with cybercrime-related issues. The United Nations manual on the prevention and control of computer-related crime (1994) uses the terms, computer crime and computer-related crime interchangeably. This manual did not provide any definition. It emphasised the fact that traditional crimes such as theft, fraud and forgery can be associated with computer crime. The manual also stated establishing a distinction between illicit and unlawful activities was mandatory (UN Manual, 1994). The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders was another significant occasion where cybercrime-related issues were discussed. During the workshops two cybercrime definitions were formed:

a) "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them."

b) "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" (UN Congress, 2000: 5). While the former defines the cybercrime in a narrow sense as computer crime, the latter describes it in a broader sense as a computer-related crime.

A definition of the cybercrime can also be found in the Commonwealth of Independent States Agreement. The act without referring the term cybercrime defines[1] it as "a criminal act of which the target is computer information" (as cited in Akhgar, Choras, Brewster, Bosco, Veermeersch et al., 2016: 298). This definition focuses on crimes against computers and leaves out the occasions where computers or networked technologies are used to commit crimes online.

Shanghai Cooperation Organization (SCO) Agreement[2] provides a definition of cybercrime in its Annex as "the use of information resources and (or) the impact on them in the informational sphere for illegal purposes", however, agreement prefers the term information offences (as cited in Malby, Mace, Holterhof, Brown, Kascherus et al., 2013: 12). This definition also focuses on crimes related to information technologies and omits offences and illicit activities against individuals. The constant omission of the term cybercrime from these documents may be the sign of the political stances of participating countries.

With regards to academic efforts to define cybercrime, while some scholars (i.e. Thomas and Loader, 2000; Gordon and Ford, 2006; Koops, 2010; Kshetri, 2010a; Casey, 2011; Pathak, 2016) strived to create a definition of the cybercrime, some others (Gordon and Ford, 2006; Wall, 2007a; Brenner, 2010) preferred to provide a typology of cybercrime. The two most popular definitions of cybercrime will be examined below.

A search on academic databases such as Google Scholar and ProQuest was conducted to find out the most popular definition of cybercrime. The search result indicated that the definitions provided by Thomas and Loader (2000) and Gordon and Ford (2006) were the most frequently cited definitions in academic papers related to cybercrime. Thus, these two definitions will be juxtaposed to each other. Thomas and Loader (2000: 3) define cybercrime as *"computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks"* whereas Gordon and Ford (2006: 14) define it as *"any crime that is facilitated or committed using a computer, network, or hardware device"*. While the former definition involves illicit behaviours that are not defined as delinquent, the latter refers to only specific

[1] The original language of the Commonwealth of Independent States Agreement is Russian. Thus, it is cited from another source.

[2] Due to unavailability of the English version of the Shanghai Cooperation Organization (SCO) Agreement, it is cited from another source.

actions that are a crime. In this aspect, the description provided by Thomas and Loader (2000) covers a wide range of activities ranging from illicit ones like distributing Internet users' personal information (Gercke, 2012) or illegal ones such as spamming (Wall, 2005). Furthermore, the latter definition not only includes actions mediated through networked technologies but it also covers the crimes to be committed via hardware devices, though, the former does not include activities facilitated with devices like iPads or smartphones (Blanco Hache and Ryder, 2011; Dolliver and Poorman, 2018) or memory sticks containing malware (Gercke, 2012).

This section of the literature review has presented some common definitions of cybercrime. The next section aims to provide a synopsis of arguments regarding the novelty of cybercrime.

The argument that whether there is such a thing like cybercrime is one of the controversial issues in cybercrime literature. Whereas some scholars such as Grabosky (2001)) and (Brenner, 2001, 2004) argue that cybercrime is the continuum of the terrestrial crimes, others (Yar, 2005; Wall, 2007a; Sandywell, 2013) argue that cybercrime, which is driven by new Internet technologies, is a new form of crime.

1.2 The Novelty of Cybercrimes

Brenner (2001, 2004) evaluates the existence of cybercrime as a distinct type of crime from a law perspective. Brenner (2001) juxtaposed real-world crimes such as burglary, theft and fraud with their cyber counterparts. *"The mens rea"* (a culpable mental state)*, "the actus reus" (act or failure), "attendant circumstances" (conditions that lead crime) and "harm*" are the four criteria that Brenner (2001: 4) uses in her analysis. She contends that although the use of Internet technologies has slightly changed the nature of real-world crimes in cyberspace, they still cause the same harm (Brenner, 2001; 2004). It is asserted that each type of cybercrime has a correspondent crime in the real world. For instance, vandalism can be considered as the real world analogy of hacking (Petee, Corzine, Huff-Corzine, Clifford, and Weaver, 2010).

Furthermore, Grabosky (2001), who focuses on the use of the Internet technologies in the commission of the crimes, asserts that there is no qualitative distinction between real-world and cyberspace while both environments serve as a scene of the crime. He argues that Internet technologies are utilised as a tool to

commit terrestrial crimes in cyberspace; hence, cybercrimes cannot be considered as new types of crimes. They are just the continuation of real-world crimes (Grabosky and Smith, 2001).

However, Yar (2005) argues that there is a discontinuity between real-world crimes and virtual crimes. He argues that virtual space creates unique opportunities for the commission of the new genre of crimes, which cannot be committed in the real world. Phishing, malware infection or cyberstalking are examples of this kind of new types of online crimes (Yar, 2005). Wall (2007) argues that the Internet technologies have not only created new opportunities for the offenders, but they have also changed the nature of real-world crimes. Wall proposes a transformation test to distinguish between cybercrimes and real-world crimes. Based on this transformation test, he argues that there are certain types of new crimes, which are impossible to be committed in the absence of Internet technologies. He dubs these kinds of crimes as "true cybercrimes" (Wall, 2004, p.10; 2007, p.48). Malware infection or phishing would no longer be committed should the Internet, and networked technologies are removed from the content of these crimes. With his transformation test, Wall (2007) clearly shows that some forms of cybercrimes are unique to cyberspace and require special attention, as they can be the facilitator of the more severe crimes such as economic cybercrimes.

Overall, considering cybercrime as a new genre of crime has some significant implications for policymakers and law. As it will be highlighted in the following sections, the perspectives evaluating cybercrime as the continuation of terrestrial crimes hinder introduction of new laws and regulations addressing specifically to cybercrimes, which in turn pose challenges to policing cybercrime. The next section discusses the evolving concept of policing.

The concept of the policing has evolved, and it is no longer restricted to public police (Yar, 2013a; Button, 2019). Bayley and Shearing (1996: 588) argue that "police are no longer the primary crime-deterrent presence in society; they have been supplanted by more numerous private providers of security." As for policing cybercrime, the situation is no different. Several non-state actors such as Internet services providers, social network services (i.e. Facebook, Twitter) and NGOs (i.e. Internet Watch Foundation or The SANS Institute) may have several responsibilities in regulating and governing the Internet (Yar, 2013b). Wall (2010: 17) defines these bodies involved in the regulation and the governance of the Internet as "cybersecurity assemblage."

1.3. The Evolving Nature of Policing Cybercrime

Besides these non-profit organizations, the for-profit private sector has increasingly involved in the governance of the Internet. Reduced investment costs and availability of the external expertise are the rationales for the privatisation of policing cybercrime (Yar, 2013b; Boes and Leukfeldt, 2017; Finn, 2019). The increased volume of private companies providing security in cyberspace created an opportunity for governments to allocate the responsibility of providing protection for cybercrime threats through the public-private partnership. Responsibilization strategy, which Garland (1996: 452) defines as "central government seeking to act upon crime not in a direct fashion through state agencies (police, courts, prisons, social work, etc.) but instead by acting indirectly, seeking to activate action on the part of non-state agencies and organizations.", is at the heart of this approach. European Network and Information Security Agency (ENISA) and The National Cyber Security Centre of the UK are the examples of public-private partnership, which refers to the collaboration between governmental agencies and private sector, to prevent cybercrime and provide cybersecurity in Europe.

However, privatisation of law enforcement is not free from its problems. Research on the privatisation of policing of traditional crimes suggests the presence of the concerns around fair investigations, authority abuses and protecting companies' interests rather than public interest (Ruddell, Thomas, and Patten, 2011; Joh, 2019; Lam, 2019). Whether the same concerns are valid for the privatisation of policing cybercrime is vague. Identifying the advantages and the pitfalls of private policing of economic cybercrime through police officers' views in the case of the UK was another goal of this empirical study.

This section of the paper reviews the empirical research examining the challenges police officers experienced while policing cybercrime.

1.4. Challenges of Policing Cybercrime

Holt, Bossler, and Fitzgerald (2010) conducted survey-based research to investigate local law enforcement agencies' awareness of, preparedness for and perceptions of cybercrime. The result of this study suggested that a major of the police officer participants acknowledge the lack of expertise and need for expert agencies to conduct the investigations in cyberspace. Limited capacity and resources to combat cybercrime emerged to be another outcome of this study.

Bossler and Holt (2012) examined local police officers' views toward their perceived role in responding to cybercrime. Their research based on the dataset collected from the police officers working in two local police departments in the southeast part of the United States. The survey results suggested that local police officers had limited knowledge to respond to cybercrime incidents. Approximately 80% of police officers expressed a degree of reluctance to be involved in cybercrime cases. Regarding police response to cybercrime incidences, 63,5% of police officers acknowledged that most cybercrime incidents were not reported to the police.

Bond and Tyrrell (2018) analysed the national online survey of police understanding of revenge pornography UK 2017. The results of their analysis indicated that police officers lacked the knowledge pertaining to revenge pornography legislation. For example, 80,6% of respondents acknowledged that they would not know how to collect information while conducting revenge pornography cases. Moreover, while only 1,2% of police respondents reported having an excellent understanding of revenge pornography, 5,9% of the respondents acknowledged having no knowledge at all.

The findings of Hadlington, Lumsden, Black, and Ferra (2018) who interviewed sixteen frontline police officers suggested difficulties in keeping up with the pace of developments, ambiguity around the definition of cybercrime and inadequate training as the problems public police officers faced while conducting cybercrime investigations.

Holt, Lee, Liggett, Holt, and Bossler (2019) investigated police officers' views on online harassment and seriousness of the interpersonal crimes (harassment and cyberbullying) within the sample of 1,348 constables in England and Wales. Their research illustrated that most police participants perceived online harassment as a less severe crime. Constables' negative perceptions related to the seriousness of online harassment emerged to diminish their eagerness to handle online interpersonal crimes.

Lee et al. (2019) examined local police officers' attitudes toward cybercrime through a web-based survey conducted with 155 inspectors working at cybercrime departments in England and Wales. The result of this study illustrated that police officers working in cybercrime departments perceived interpersonal and online financial crimes as severe as traditional crimes. For instance, 42,6% of participants perceived stealing money from individuals' bank accounts equivalent to stealing

the same amount of money from their pockets. Additionally, 44,5% of responders agreed that online crime poses a significant threat to society. The results of this study demonstrated that experts' views significantly differed from those of local non-expert police officers' views. This difference suggests that police officers' skills related to cybercrime investigations impact their views and their willingness to conduct cyber investigations.

Nouh, Nurse, Webb, and Goldsmith (2019) conducted ten semi-structured interviews with experts from the government and private sector to examine the challenges law enforcement faces. Problems related to Action Fraud's procedures pertaining to data collection and recording the cases reported to them appeared to exacerbate reporting of problems of cybercrime. Lack of coordination between departments emerged to be another challenge faced by law enforcement bodies. Budged cuts related to Information Technologies (IT) infrastructure acknowledged as another significant challenge.

2.1. Data Collection

It is generally agreed that the networked global nature of the Internet poses significant challenges to policing cybercrime due to inherent technological complexities (Holt et al., 2019; Lee et al., 2019). Nevertheless, there is a dearth of empirical research examining policing problems of economic cybercrime through the lenses of police officers in the literature.

2. METHODOLOGY

In order to address this knowledge gap in the literature, ten semi-structured interviews were conducted with police officers working in cybercrime departments in the UK and three semi-structured interviews were done with experts working on IT departments of the local governments. The research was conducted according to the Declaration of Helsinki (World Medical Association, 2001). Interviewees were provided participant information sheets explaining interview and transcription processes prior to interviews. Participants were also asked to sign consent forms before the interviews. Interviews were conducted face-to-face at police departments. Interviews were recorded and transcribed verbatim by authors after the interviews.

2.2. Analytic Procedure

A thematic coding approach was employed to address the research question: *"What are the policing problems of cybercrime police units in the UK"*. The aims of this research were two-fold: documenting the problems experienced by police officers working in cybercrime departments and discerning police officers' perceptions related to the role of police in the wider policing assemblage.

Braun and Clarke (2006: 6) define thematic analysis as "a method for identifying, analysing, and reporting patterns (themes) within data." They categorise thematic analysis as inductive and theoretical. The former perspective is a bottom-up approach that aims to identify themes or concepts without relying on the pre-defined set of codes and themes. The latter is a top-down approach which utilises existing codes and themes informed by theory (Hayes, 1997; Maguire and Delahunt, 2017). This research applied an inductive analysis approach since the research questions and aims were explorative in nature. Initially, a single-authored coding process was applied with the help of QSR NVIVO qualitative analysis software. Codes and themes created in the first cycle of coding were revised by other authors to prevent single coder bias.

3. FINDINGS

Analysis of interviews conducted with police officers and cybercrime experts suggests that policing economic cybercrime is a multidimensional complex issue involving both national and international actors together with police forces. Participants' accounts are provided verbatim as evidence to maintain the validity and the reliability of the research.

Interviews with police officers revealed the lack of international cooperation as the key challenge to policing economic cybercrime. Participants acknowledged that non-European countries were reluctant to share information related to online perpetrators.

"The companies sit in Luxemburg, Panama or Gibraltar are reluctant to share information. So, you need to have a global agreement." (Participant 2).

"Sometimes, the suspect is out of the country. It is difficult to catch them and bring to the jurisdiction crime happened." (Participant 4).

This lack of international cooperation appears to be one of the reasons for low prosecution rates.

"Trying to find out who did it is the biggest challenge. Quite often the cybercrime extends to abroad, and obviously, we have problems with co-operating with other countries. Especially African countries are not very keen to work with us." (Participant 7).

"Cross-national nature of cybercrime is another challenge. Even if you find out the criminals, it is impossible to prosecute them due to residing out of the jurisdiction." (Participant 10).

Issues related to conducting digital forensics emerged as another explanation for failing to prosecute online perpetrators. Retrieving a large volume of data to find evidence and failures in protecting evidence appeared to exacerbate digital forensic.

"I think the difficulty is digital forensics. Naturally, we do not have the same sort of capability for digital forensics if we are to compare a theft from a shop or a burglary with a hacking case. The volume of digital evidence is huge. It requires hard work to retrieve the evidence and it also recognising the information, which could be used to support the prosecuting the offender is a very complex and time-consuming area of work." (Participant 8).

"A challenge can be that the people who are victims of cybercrime don't realise and fully understand how they had been a victim, and they got rid of the evidence. They delete it, wipe the computer because of viruses, which is good in relation to prevent further attacks, but that may stop us getting hold of some evidence." (Participant, 4).

"Victim companies are mostly concerned about getting their business back online, so they are not really concerned about preserving the evidence. Collecting evidence becomes problematic." (Participant 6).

Interviewees also reported that most of the cases were not prosecuted due to a large volume of cybercrime cases exceeding the capacity of cybercrime units located in major cities. It is evident the cases that caused significant financial harm received law enforcement attention.

"The level of response depends on the scale of the harm, which can be measured by financial and physical elements. A company having a huge economic loss because of their data being stolen will have a rapid response." (Participant 3).

Underreporting of economic cybercrime incidents appeared to be another key challenge of policing economic cybercrime. Victims' lack of knowledge about online threats appears to decrease reporting of the economic cybercrime cases.

"People's perception of what is cybercrime. People's inability to understand the differences between the crime, the threat the risk. %50 of crime we experience is cyber-enabled or cyber-dependent however, in most cases, people are not aware of it." (Participant 9).

"Sometimes, victims are not aware that they are subject to a ransomware attack, or they are exposed to malicious software. Sometimes small business run by families may not have expertise in IT issues. They have minimal technical experience. Sometimes victims find it difficult to explain what has happened." (Participant 5).

Victims' reluctance to report cases was cited as another possible reason for underreporting.

"In some cases, when the victim receives the refund, they are not willing to follow the case and go to the court, so victims' reluctance." (Participant 8).

"It happened in Northeast where a large public body had a ransomware attack. We know that they have not reported it because of reputational concerns." (Participant 4).

Interviewees were also asked about their perceptions related to the involvement of private companies in policing economic cybercrime cases. Most participants (n=7) considered public-private partnership fruitful to compensate skill gap between police officers and online perpetrators.

"I do understand why there is a need for private investigations because of their skills need private companies." (Participant 10).

"In technical aspects, most of the times, criminals are more equipped than us." (Participant 7).

However, interviewees also expressed their concerns related to the ethical issues and the extent of the privatisation of policing economic cybercrime.

"Private sectors' role should be limited to protecting. Robust security systems and educating individuals. The companies should co-operate with law enforcement

in partnership to be able to supply evidence that would help the successful prosecution of individuals." (Participant 4).

"The police should be operational independent. Therefore, when they investigate the type of evidence they secure, we look at what has motivated the offender, and the damage has been done to the victim, and we keep the balance between both sides. My concern is sometimes if you have a company doing a prosecution, they may sometimes be interested in protecting the rights of the company rather than looking at the human rights element." (Participant 9).

"As a police force, we should be doing the investigations. Private companies are more after their money, their costumers, their shareholders, but we are responsible to the public. Private companies may help digital investigations under our control". (Participant 6).

The United Kingdom's counter-terrorism strategy, CONTEST, known as the Four Ps Model, aimed to provide a strong response to the terrorist threat to the UK (Home Office, 2014, 2018) bears four components: prevent, pursue, protect and prepare. While pursue refers to prosecuting the offenders and disrupting their activities, prevent denotes safeguarding individuals from becoming an offender. Protect aims to shield the public and private sector from perpetrators by reducing vulnerabilities. Lastly, the goal of the prepare concept is to alleviate post-victimization impacts. Levi, Doig, Gundur, Wall, and Williams (2015) applied this model to policing economic cybercrime. Their research suggested that although this model needs revision to be successfully adapted to policing economic cybercrime, it still offers some valuable insight into tackling economic cybercrime. Participants were asked to evaluate the role of police on the broader cybersecurity assemblage in the light of this framework.

Most of the participants (n=8) reported protect as the primary strategy to be implemented. The belief that most of the cybercrime is preventable, protecting individuals' from experiencing harm and the investigation costs were cited as the rationale for viewing this strategy as the most vital one.

"The police should not just look at arresting people. We have responsibilities. We must look into protect and prepare people." (Participant 7).

"80% of cybercrime is preventable. So, the biggest part of our role is to protect." (Participant 2).

4. DISCUSSION

Despite the growing cyber threat and cybersecurity concerns among the public, there is a lack of empirical research on discerning the challenges of policing economic cybercrime. Previous empirical studies mostly dealt with non-expert police officers' perceptions related to policing cybercrime. The results of these studies demonstrated that local police officers lacked the technical skills to respond to cybercrime (Bossler and Holt, 2012; Bond and Tyrrell, 2018; Hadlington et al., 2018). The findings of this study that although police officers felt confident regarding their technical skills to investigate economic cybercrime cases, they still need external expertise due to the pace of developments in information technologies. This result is in line with (Lee et al., 2019) who found that expert police officers who felt confident were more willing to investigate cybercrime cases.

The lack of international cooperation in combatting cybercrime and providing cybersecurity echoed in this study replicating previous studies (Kshetri, 2010b; James and Gladyshev, 2015). This result which confirms the previous studies indicates that governments or international and transnational actors have failed to collaborate to combat cybercrime globally.

Deleting digital evidence emerged to be a reason for low prosecution. Police officers' accounts suggested Internet users' lack of knowledge as a significant reason for this problem. Some participants also acknowledged that Internet users sometimes even were not aware of their victimisation. This highlights the need for more educational programmes to improve awareness related to online threats.

Police officers' account revealed that most of the cybercrime cases happened in big cities could not be prosecuted. Thus, cybercrime units mostly focused on notorious cases that draw public attention or ended up with significant financial harm. Wall (2013b: 39) argues most of the financial loss can be characterised as "de minimis", which means that online perpetrators steal a small amount of money to evade prosecution. This strategy of online perpetrators appears to increase the workload of law enforcement, which in turn leads to escaping from law enforcement attention.

Regarding private companies' involvement to policing cybercrime, police officers were mostly concerned about private firms' attachment to ethical issues such as pursuing public interest and conducting a fair investigation. Participants

were in favour of outsourcing technical expertise when there is a need. Although outsourcing is always an option when there is lack of expertise in a specific area (Barthelemy, 2003), what combatting cybercrime requires is more than outsourcing. The European Unions' new Cybersecurity Act (Regulation 2019/881), which is in force since July 2019, redesigned ENISA to contribute to European cybersecurity and collaborate with stakeholders. To that end, the Advisory Group was established to cooperate with stakeholders. Cybersecurity certification is another novelty of this new act. ENISA will be responsible for preparing of European cybersecurity certification schemes (European Commission, 2019). The introduction of this new act is a clear indication of EU's commitment to sustain public-private partnership in combatting cybercrime.

CONCLUSION

National and international initiatives such as UK Cybercrime Strategy 2016/2021 place emphasis upon reducing disparities among national jurisdictions and creating strong coordination between policing bodies and other private and governmental actors of cybersecurity to alleviate policing problems of cybercrime (Ellis and Mohan, 2019). Despite these efforts, there is lack of empirical studies on this issue. This empirical research examining the challenges of policing economic cybercrime through police officers' lenses contributes to cybercrime/cybersecurity literature by documenting some challenges cybercrime units have experienced.

Police officers who were participated in this research highlighted the significance of the protect strategy of the Four Ps model for policing cybercrime. This emphasis indicates that police need to move beyond its predefined duties, which mainly focus on investigation and prosecution of the incidents. To that end, police forces need to collaborate with third parties more extensively. Hence, public police need to define its role in broader cybersecurity assemblage. New strategies expanding the responsibilities of police forces from the investigation of the cybercrimes to providing coordination and collaboration between cybersecurity actors, preventing cybercrime and protecting netizens should be devised. Although ENISA's new role will contribute to maintaining cybersecurity, the analysis of interviews suggests that the lack of cooperation with countries that are outside the EU jurisdiction posed a significant challenge. Hence, ENISA or another agency should actively seek to collaborate with non-EU countries.

REFERENCES

Akhgar, B., Choras, M., Brewster, B., Bosco, F., Veermeersch, E., Luda, V., Puchalski, D., and Wells, D. (2016) 'Consolidated Taxonomy and Research Roadmap for Cybercrime and Cyberterrorism', pp. 295-322 in B. Akhgar and B. Brewster (eds) Combatting cybercrime and cyberterrorism: challenges, trends and priorities: Springer.

Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M. J., Levi, M., Moore, T., and Savage, S. (2013) 'Measuring the Cost of Cybercrime', pp. 265-300 in The economics of information security and privacy: Springer.

Barthelemy, J. (2003) 'The seven deadly sins of outsourcing', Academy of Management Perspectives 17(2): 87-98.

Bayley, D. H., and Shearing, C. D. (1996) 'The future of policing', Law Society Review 30: 585.

BBC (2019) UK cyber-crime victims lose £190,000 a day. Available at: https://www.bbc.co.uk/news/uk-47016671 (Accessed: 14/09/2019.

Blanco Hache, A. C., and Ryder, N. (2011) ''Tis The Season to (be Jolly?) Wise-Up to Online Fraudsters. Criminals on The Web Lurking to Scam Shoppers this Christmas: A Critical Analysis of the United Kingdom's Legislative Provisions and Policies to Tackle Online Fraud', Information & Communications Technology Law 20(1): 35-56.

Boes, S., and Leukfeldt, E. R. (2017) 'Fighting Cybercrime: A Joint Effort' in R. M. Clark and S. Hakim (eds) Cyber-physical security: protecting critical infrastructure at the state and local level: Springer.

Bond, E., and Tyrrell, K. (2018) 'Understanding revenge pornography: A national survey of police officers and staff in England and Wales', Journal of interpersonal violence: 0886260518760011.

Bossler, A. M., and Holt, T. J. (2012) 'Patrol officers' perceived role in responding to cybercrime', Policing: an international journal of police strategies & management 35(1): 165-181.

Braun, V., and Clarke, V. (2006) 'Using thematic analysis in psychology', Qualitative research in psychology 3(2): 77-101.

Brenner, S. W. (2001) 'Is There Such a Thing as' Virtual Crime'?'.

---. (2004) 'Cybercrime Metrics: Old Wine, New Bottles?', VA. JL & TECH. 9: 13.

---. (2007) 'The Council of Europe's Convention on Cybercrime', pp. 207-221 in J. Balkin, J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman and T. Zarsky (eds) Cybercrime: digital cops in a networked environment: NYU Press.

Brenner, S. W. (2010) Cybercrime: Criminal Threats from Cyberspace: USA: Prager.

Button, M. (2019) Private policing: Routledge.

Casey, E. (2011) 'Language of Computer Crime Investigation', pp. 35-48 in E. Casey (ed.), Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. London: Elsevier.

Clough, J. (2014) 'A World of Difference: The Budapest Convention of Cybercrime and the Challenges of Harmonisation', Monash UL Rev. 40: 698.

Dolliver, D. S., and Poorman, K. (2018) 'Understanding Cybercrime', pp. 139-160 in P. L. Reichel and R. Randa (eds) Transnational Crime and Global Security [2 volumes]: ABC-CLIO.

Ellis, R., and Mohan, V. (2019) Rewired: Cybersecurity Governance: John Wiley & Sons.

European Commission (2007) Towards a General Policy on the Fight Against Cyber Crime Available at: https://eur-lex.europa.eu/LexUriServ/ LexUriServ. do?uri= COM:2007:0267:FIN:EN:PDF.

--- (2019) The EU cybersecurity certification framework. Available at: https://ec.europa.eu/digital-single-market/en/eu-cybersecurity-certification-framework (Accessed: 17/08/2019.

Finn, B. M. (2019) 'Recommendations for a hybridized public private law enforcement approach'.

Garland, D. (1996) 'THE LIMITS OF THE SOVEREIGN STATEStrategies of Crime Control in Contemporary Society', The British journal of criminology 36(4): 445-471.

Gercke, M. (2012) Understanding Cybercrimes: Phenomena, Challenges and Legal Response: International Telecommunication Union.

Gordon, S., and Ford, R. (2006) 'On the Definition and Classification of Cybercrime', Journal in Computer Virology 2(1): 13-20.

Grabosky, P., and Smith, R. (2001) 'Telecommunications Fraud in the Digital Age: the Convergence of Technologies', pp. 23-43 in D. Wall (ed.), Crime and the Internet. London: Routledge.

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

Graham, L. (2017) Cybercrime costs the global economy $450 billion: CEO. Available at: https://www.cnbc.com/2017/02/07/cybercrime-costs-the-global-economy-450-billion-ceo.html (Accessed: 06/08/2019 2019).

Hadlington, L., Lumsden, K., Black, A., and Ferra, F. (2018) 'A qualitative exploration of police officers' experiences, challenges, and perceptions of cybercrime', Policing: A Journal of Policy and Practice.

Hayes, N. (1997) 'Theory-led thematic analysis: Social identification in small companies'.

Holt, T. J., Bossler, A. M., and Fitzgerald, S. (2010) 'Examining state and local law enforcement perceptions of computer crime', *Crime on-line: Correlates, causes, and context*: 221-246.

Holt, T. J., Burruss, G. W., and Bossler, A. M. (2018) 'An examination of English and Welsh constables' perceptions of the seriousness and frequency of online incidents', *Policing and Society*: 1-16.

Holt, T. J., Lee, J. R., Liggett, R., Holt, K. M., and Bossler, A. (2019) 'Examining perceptions of online harassment among constables in England and Wales', *International Journal of Cybersecurity Intelligence & Cybercrime* 2(1): 24-39.

Home Office (2014) *The Serious and Organised Crime Strategy*, London.

--- (2018) *CONTEST: The United Kingdom's Strategy for Countering Terrorism*, London.

James, J. I., and Gladyshev, P. (2015) A Survey of International Cooperation in Digital Investigations, *International Conference on Digital Forensics and Cyber Crime* (pp. 103-114): Springer.

Joh, E. E. (2019) 'Policing the smart city', *International Journal of Law in Context* 15(2): 177-182.

Koops, B.-J. (2010) 'The internet and its opportunities for cybercrime'.

Kshetri, N. (2010a) 'The Global Cybercrime Industry and Its Structure: Relevant Actors, Motivations, Threats, and Countermeasures', pp. 1-34 in *The Global Cybercrime Industry*: Springer.

---. (2010b) 'Structure of Cybercrime in Developing Economies', pp. 165-188 in *The Global Cybercrime Industry*: Springer.

---. (2013) 'Cybercrime and cyber-security issues associated with China: some economic and institutional considerations', *Electronic Commerce Research* 13(1): 41-69.

Lam, P. T. (2019) 'Public–Private Partnerships for Fire, Police, and Ambulance Services', pp. 153-165 in *Public Private Partnerships*: Springer.

Lee, J. R., Holt, T. J., Burruss, G. W., and Bossler, A. M. (2019) 'Examining English and Welsh Detectives' Views of Online Crime', *International Criminal Justice Review*: 1057567719846224.

Levi, M., Doig, A., Gundur, R., Wall, D., and Williams, M. L. (2015) *The Implications of Economic Cybercrime for Policing*: City of London Corporation. Available at: https://www.cityoflondon.gov.uk/business/economic-research-and-information/research-publications/Documents/Research-2015/Economic-Cybercrime-FullReport.pdf. (Accessed: 11 June 2017).

Maguire, M., and Delahunt, B. (2017) 'Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars', *AISHE-J: The All Ireland Journal of Teaching and Learning in Higher Education* 9(3).

Malby, S., Mace, R., Holterhof, A., Brown, C., Kascherus, S., and Ignatuschtschenko, E. (2013) 'Comprehensive Study on Cybercrime', *United Nations Office on Drugs and Crime, Tech. Rep*.

Nouh, M., Nurse, J. R., Webb, H., and Goldsmith, M. (2019) 'Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement', *arXiv preprint arXiv:1902.06961*.

Pathak, P. (2016) 'The Review of Terms and Concepts Used to Understand Cybercrime to Safeguard Ourselves from Cybercriminals', *International Journal of Advanced Research in Computer Science* 7(1).

Petee, T. A., Corzine, J., Huff-Corzine, L., Clifford, J., and Weaver, G. (2010) 'Defining" Cyber-crime": Issues in Determining the Nature and Scope of Computer-related Offenses,"', *Futures Working Group* 5: 6-11.

Reinhart, R. J. (2018) *One in Four Americans Have Experienced Cybercrime*. Available at: https://news.gallup.com/poll/245336/one-four-americans-experienced-cybercrime.aspx (Accessed: 08/09/2019.

Ruddell, R., Thomas, M. O., and Patten, R. (2011) 'Examining the roles of the police and private security officers in urban social control', *International Journal of Police Science & Management* 13(1): 54-69.

Sandywell, B. (2013) 'On the Globalisation of Crime: the Internet and New Criminality', pp. 56-84 in *Handbook of internet crime*: Willan.

Summerville, A. (2017) *Protect against the fastest-growing crime: cyber attacks*. Available at: https://www.cnbc.com/2017/07/25/stay-protected-from-the-uss-fastest-growing-crime-cyber-attacks.html (Accessed: 06/08/2019 2019).

Taylor, G. (2002) 'The Council of Europe Cybercrime Convention a Civil Liberties Perspective', *Retrieved June* 13: 2006.

The Council of Europe Convention on Cybercrime. (2001) Convention on Cybercrime. In T. C. o. Europe (Ed.). Budapest: European Treaty Series - No. 185.

Thomas, D., and Loader, B. (2000) 'Cybercrime: Law Enforcement, Security and Surveillance in the Information Age' in D. Thomas and B. Loader (eds) *Cybercrime: Law enforcement, security and surveillance in the information age*. London: Routledge.

UN Congress. (2000) Crimes Related to Computer Networks, *10th United Nations Congress on the Prevention of Crime and the Treatment of Offenders*. Vienna: United Nations.

UN Manual (1994) *United Nations Manual on the Prevention and Control of Computer-Related Crime*. Available at: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf (Accessed: 21/03/2017).

Wall, D. S. (2005) 'Digital Realism and the Governance of Spam as Cybercrime', *European journal on criminal policy and research* 10(4): 309-335.

---. (2007a) *Cybercrime: The transformation of crime in the information age*: Polity.

---. (2007b) *Cybercrime: The Transformation of Crime in the Information Age*: Cambridge: Polity Press.

---. (2008) 'Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime', *International Review of Law, Computers & Technology* 22(1-2): 45-63.

---. (2010) 'Policing Cybercrimes: Situating the Public Police in Networks of Security Within Cyberspace (Revised May 2010)', *Police Practice and Research* 8(2): 183-205.

---. (2013a) 'Criminalising Cyberspace: The Rise of the Internet as a 'Crime Problem'', pp. 106-121 in *Handbook of Internet Crime*: Willan.

---. (2013b) 'Policing Identity Crimes', pp. 29-52 in D. S. Wall and M. L. Williams (eds) *Policing cybercrime: networked and social media technologies and the challenges for policing*: Taylor & Francis.

Wall, D. S., and Williams, M. (2014) *Policing cybercrime: networked and social media technologies and the challenges for policing*: Routledge.

Williams, M., and Levi, M. (2015) 'Perceptions of the ecrime Controllers: Modelling the Influence of Cooperation and Data Source Factors', *Security Journal* 28(3): 252-271.

World Medical Association. (2001) 'World Medical Association Declaration of Helsinki. Ethical principles for medical research involving human subjects', *Bulletin of the World Health Organization* 79(4): 373.

Yar, M. (2005) 'The Novelty of 'Cybercrime' an Assessment in Light of Routine Activity Theory', *European Journal of Criminology* 2(4): 407-427.

---. (2013a) *Cybercrime and Society*: Sage.

---. (2013b) 'The Private Policing of Internet Crime' in Y. Jewkes and M. Yar (eds) *Handbook of Internet crime*: Routledge.

NATO'NUN YENİ OPERASYON ALANI: SİBER UZAY

Doğan Şafak POLAT*

Öz

NATO (Kuzey Atlantik Antlaşması Örgütü), üye ülkelerin ortak savunma yeteneklerini geliştirmek, toprak bütünlüklerini, siyasi bağımsızlıklarını ve güvenliklerini korumak maksadıyla 4 Nisan 1949 tarihinde kurulmuştur. Bu husus NATO Anlaşma'sının 5. Maddesi'nde de açıkça ifade edilmiştir. 21. yüzyılda teknolojik gelişmeler sonucunda güvenlik parametreleri değişmiş; kara, deniz, hava ve uzay yanında beşinci bir alan ortaya çıkmıştır. Bu alan siber uzay (cyber space) alanı olarak ifade edilmektedir. Siber uzayda yapılan saldırılara karşı mücadele oldukça güç olup tek bir devletin kapasitesini aşmakta ve müşterek mücadeleyi zorunlu kılmaktadır. Başlangıçta bir savunma örgütü olarak kurulan NATO, geçen süreçte üye devletlerin de onayıyla Stratejik Konsepti'ni değiştirmiş ve Soğuk Savaş sonrası bir güvenlik örgütü haline gelmiştir. NATO, siber uzayda üye devletlerin ihtiyaçlarına cevap verecek şekilde bünyesinde çeşitli kurumlar oluşturmakta; edinilen tecrübe, birikim ve yeteneklerini de üye devletler ile paylaşmaktadır. Siber uzayda ortaya çıkan/çıkabilecek tehditlere karşı NATO bünyesinde alınan önlemler ve bu maksatla yapılan çalışmalar devamlılığı gerektirmekte; İttifak'a üye devletlerin işbirliğini, bilgi ve teknoloji paylaşımlarını zorunlu kılmaktadır.

Anahtar Kelimeler: *Siber Güvenlik, Siber Alan, NATO, Müşterek Siber Güvenlik Mükemmeliyet Merkezi (CCDCOE), Siber Operasyonlar Merkezi (CYOC)*

NATO'S NEW OPERATION DOMAIN: CYBER SPACE

Abstract

NATO (The North Atlantic Treaty Organization) was established on April 4, 1949 to develop the common defense capabilities of member countries and to protect their territorial integrity, political independence and security. This is clearly stated in Article 5 of the NATO Treaty. As a result of technological developments in the 21st century security parameters have changed; a fifth field has emerged besides land, sea, air and space. This field is referred to as cyber space. The struggle against attacks in cyber space is very difficult, and exceeds the capacity of a single state and necessitates fighting in cooperation. NATO, which was initially established as a defense organization, changed its Strategic Concept with the approval of the member states and became a security organization after the end of Cold War. NATO establishes various institutions in the cyber space to meet the needs of the member states, and it shares its experience, knowledge and skills with the member states, as well. The measures taken and the work carried out for this purpose within NATO against the threats that may arise in the cyber space require continuity, and the cooperation of the member states and information and technology sharing become a must.

Keywords: *Cyber Security, Cyber Space, NATO, Cooperative Cyber Defence Centre of Excellence (CCDCOE), Cyber Operations Center (CYOC).*

* Dr. Öğretim Üyesi, İstanbul Arel Üniversitesi, İİBF, Uluslararası İlişkiler Bölümü, doganpolat@arel.edu.tr, ORCID: 0000-0003-0786-1789

Makale Geliş Tarihi: 30.09.2019 Makale Kabul Tarihi: 27.01.2020

GİRİŞ

Harbin kara, deniz, hava ve uzay olmak üzere dört boyutu vardır. Kimi uzmanlarca kara, hava, deniz ve uzaydan sonra beşinci boyut olarak değerlendirilen siber uzay (cyber space) diğer dört boyutu da etkileme kapasitesine sahip olup günümüzde harbin ayrılmaz bir bileşeni olarak değerlendirilmektedir. Siber uzay kavramı "birbiriyle bağlantılı sistem, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için" kullanılmaktadır (Libicki, 2009: 12-13). Siber saldırılar bir ülkenin kritik olarak kabul edilebilecek haberleşme/bilişim sistemlerine, enerji ve ulaşım ağlarına, askeri komuta ve kontrol sistemlerine zarar verecek ölçüde, asimetrik bir muharebe yöntemi olarak ortaya çıkmaktadır. Teknolojik gelişmeler paralelinde siber saldırılar daha yaygın, hızlı, çok karmaşık ve zarar verici hale gelmiştir. Bunun neticesinde siber güvenlik konuları devletleri daha fazla meşgul etmeye başlamıştır. Devletler siber tehdit ve tehlikelerin oluşumundan önce bunlara karşı önlemler almaya çalışmaktadırlar. Devletlerin yanında savunma örgütünden güvenlik örgütüne dönüşen ve geniş bir bilişim altyapısına sahip olan NATO da siber uzayın güvenliği maksadıyla çeşitli çalışmalar yürütmektedir. NATO'nun bilişim altyapısı Brüksel'deki merkezi ile dünyanın çeşitli bölgelerinde askeri birliklerin bulunduğu 60'tan fazla NATO operasyon sahasını kapsamaktadır. 100.000'den fazla asker ve sivil personel NATO ağlarına bağlantılıdır. Bu durum son on yılda NATO'nun giderek daha fazla siber saldırıların hedefi olmasına yol açmaktadır. NATO siber savunma sistemleri her gün NATO ağlarına karşı yapılan basitten karmaşığa çok sayıda siber saldırıyı tespit etmekte ve bunlara engel olarak bilişim sistemlerinin kesintisiz olarak çalışmasına çaba göstermektedir.

Bu çalışmanın amacı, içinde bulunduğumuz yüzyılda siber güvenliğin önemine vurgu yaparak NATO'nun siber tehditlerle mücadelesini ortaya koymaktır. Bir zincirin sağlamlığının en zayıf halkasının sağlamlığı kadar olduğu dikkate alındığında, NATO'nun da siber güvenlik konusunda yetkinliğinin en zayıf üye devletin yetkinliği kadar olduğu çıkarımı yapılabilir. İttifak, Soğuk Savaş sonrasında 2000'li yıllarla birlikte giderek önem kazanan siber alan ile ilgili çalışmalarda önemli mesafeler kat etmiş olsa da her üye devletin siber tehditlerle mücadele kapasitesinin aynı olduğunu söyleyebilmek oldukça güçtür. Çalışma, iki ana bölümden oluşmaktadır. Birinci bölümde siber uzayla ilgili olarak siber, siber tehdit, siber uzay ve siber güvenlik gibi kavramlar ele alınacaktır. İkinci bölümde ise kronolojik olarak siber güvenlik konusunda NATO'nun almış olduğu kararlara ve yapmış olduğu çalışmalara yer verilerek çalışma sonlandırılacaktır.

1. SİBER İLE İLGİLİ KAVRAMLAR

Siber terimi, ilk defa sibernetik kelimesinin kısaltması olarak Amerikalı bilim adamı Norbert Weiner tarafından 1948 yılında yayımlanan "Sibernetik ya da Hayvanlarda ve Makinelerde Kontrol ve İletişim (Cybernetics, or Control and Communication in the Animal and Machine) başlıklı kitapta kullanılmıştır (Whittaker, 2004: 4). Söz konusu terim 1958 yılında, canlılar ve/veya makineler arasındaki iletişim disiplinini inceleyen Matematik ve Sibernetik biliminin öncüsü sayılan Fransız Louis Couffignal tarafından da kullanılmıştır. Daha sonra bilişim alanında kullanımına devam edilmiştir (Çolak, 2011: 65). Siber uzay terimi (cyber space) ise, Kanada'lı William Gibson tarafından ilk defa 1982 yılında yazdığı "Burning Chrome" adlı eserinde kullanmıştır (Bıçakçı, 2010: 106). Gibson, "Neuromancer" adlı bilim kurgu romanında (Gibson, 1984) siber uzayı "bilgilerin elektromanyetik dosyada oluşturulması ile dünyanın her yanına farklı sistemler aracılığıyla dağıtılması ve bilgiye erişim sağlanılan sanal ortamların bütünü" olarak tanımlanmıştır (Çakmak ve Altunok, 2009: 25-26).

1.1. Siber Uzay

Soğuk Savaş döneminde ABD'de uzay, füze savunma ve nükleer silahlarının testlerinin tespiti maksadıyla 1957 yılında İleri Araştırma Projeleri Ajansı (Advanced Research Projects Agency/ARPA) kurulmuştur. 1960'lı yılların başında ise Savunma Araştırma Projeleri Ajansı (Defence Advanced Research Projects Agency/DARPA) kurulmuş; 1970'li yılların ortasından itibaren bu kurumun çalışma alanı ve yetkinliği geliştirilmiştir (Van Atta, 2018: 12). 1962 yılında ise ARPANET tasarlanarak hayata geçirilmiş ve böylece siber uzayın temeli atılmıştır. ARPANET, Dağınık Servis Engelleme Saldırıları (DDoS)'na karşı dayanıklı olarak tasarlanmıştır (Yılmaz ve Salcan, 2008: 35). 1977 yılına gelindiğinde ise kullanıcı sayısı artan ARPANET, üniversite, sivil sektör ve devlet araştırma faaliyetlerini birbirine bağlayan ulusal bir ağ haline gelmiştir (Pierce, 2018: 62). 1970'li yıllardan itibaren söz konusu ağdaki sunucu sayısının artırılmasıyla birlikte daha fazla bilgisayar ARPANET'e bağlanmıştır. Sistemdeki kullanıcı sayısının giderek artması nedeniyle yavaşlayan sistemi hızlandırmak maksadıyla çeşitli yazılım ve donanım düzenlemeleri yapılmıştır.

1980'lerde ARPANET'in ticari sürümü olarak değerlendirilen internet hızla büyümüş ve 1988 yılına kadar yaklaşık 60.000 internet bağlantılı bilgisayara hizmet verir hale gelmiştir (Pierce, 2018: 63-65). ARPANET'nin kullanıcı sayısının kısa sürede artması ve ağın ABD sınırları dışına açılımı güvenlik

sorunlarını da beraberinde getirmiştir. Bu süreçte en önemli siber saldırı 2 Kasım 1988 tarihinde gerçekleşmiştir. İnternete bağlı sistemlerin yaklaşık yüzde 10'unda Morris solucanı hızla yayılmış ve sistemi olumsuz olarak etkilemiştir. ARPANET'teki tehditlerin artması üzerine, ABD Savunma Bakanlığı, söz konusu ağı korumak için çeşitli çalışmalar başlatmıştır.

1990'lı yıllarda, ABD Savunma Bakanlığı, ARPANET'in askeri operasyonları için kritik öneme sahip olduğunu kabul ederek bir taraftan ağ güvenliği ile ilgili çalışmaları arttırmış, diğer taraftan ise hızlı bir şekilde askeri bilişim sistemlerini, bilgisayar ağları üzerinden birbirleriyle irtibatlandırmıştır. Böylece her türlü yazılım, donanım ve iletişim alt yapısından meydana gelen ve birbirine bağlı ya da bağımsız bilgi sistemlerinin oluşturduğu sayısal ortam olan siber uzay oluşmuştur. Siber uzayın henüz üzerinde anlaşmaya varılmış bir tanımı bulunmamakla birlikte siber uzay kavramı, birbiriyle irtibatlı bir zaman bağımlı bilgi sistemleri kümesini ve bu sistemlerle etkileşim içinde bulunan kullanıcıları ifade etmek için kullanılmaktadır (Ottis ve Lorents, 2010: 267).

Siber uzay, sadece internet ve ona bağlı bilgi sistemlerini değil internete girmeyen bütün bilgi sistemlerini de kapsamaktadır (Çiftçi, 2013: 5). Siber uzay kavramındaki uzay terimi ise sonsuzluğu ifade etmektedir. Son dönemde ortaya çıkan Nesnelerin İnterneti (Internet of Things/IoT) kavramıyla siber uzayın sınırları bilgisayarların dışına çıkarak kamu ve özel sektör binalarına, evlere, arabalara kadar ulaşmıştır.

1.2. Siber Savaş

İnsanlık tarihi boyunca en eski savaşlar kara ve denizlerde gerçekleşmiştir. 20. yüzyılın başından itibaren havacılık alanındaki gelişmeler neticesinde bu durum değişmiş ve hava da yeni savaş alanı olarak ortaya çıkmıştır. 1950'lerden itibaren ise dünyadaki süper güçler arasındaki yeni savaş alanı uzay olmuştur. 21. yy'dan itibaren meydana gelen teknolojik gelişmeler neticesinde bilişim sistemlerindeki yenilikler artmış ve siber savaş tanımlaması yapılmaya başlamıştır(Arquilla ve Ronfeldt, 2001: 2-7). Beşinci savaş alanı olarak kabul edilen siber uzay, diğer dört alanın yanında daha fazla öne çıkmaya başlamıştır (Murphy, 2010). Bunun nedeni diğer dört alanın bilişim sistemlerini (yazılım ve donanım) giderek daha fazla kullanmaları ve siber uzaya bağımlı hale gelmeleridir. Bilgi sistemlerinin yanında bu sistemleri birbirine bağlanmasını sağlayan iletişim araçları (kablo vs.) da bu yeni savaş alanının parçalarını oluşturmaktadır (Clarke ve Knake, 2011: 43-44).

Siber savaş, kuralsız bir şekilde siber silahlar kullanılarak yürütülen asimetrik veya hibrit yaklaşımların kullanıldığı savaş şeklidir. Askeri yapıların tek başına değil sivil altyapılar ile bağlantılı olması nedeniyle siber uzaydaki bu saldırıların, askeri yapılarla sınırlı kalmadığı da bir gerçektir (Ottis, 2010: 178). Siber savaş nedeni sayılabilecek saldırının gerisindeki saldırgan devlet genellikle tespit edilememektedir (Standler, 2002). Siber savaşta amaç, "sahip olunan siber varlıkları; ulusal çıkarlar ve menfaatler çerçevesinde korumak için karşı tarafın kritik bilişim sistemlerine zarar vermek, hizmetlerini durdurmak veya bozmak için bir başka ülkenin bilişim sistemlerini yavaşlatmak, bozmak, hizmetini aksatmak veya ele geçirmek" olabilir (Clarke ve Knake, 2011: 132). Siber uzayda bilgiye erişim coğrafi sınırlardan bağımsız olarak sürekli hızlanmıştır (Çiftçi, 2013: 8-9). Bu durum dışarıdan gelen/gelebilecek tehditlerin ve saldırıların da artmasına yol açmıştır.

Üç tür siber saldırı silah olarak kullanılır. Bunlar sentaktik saldırılar, semantik saldırılar ve karışık saldırılardır (Brenner ve Goodman, 2002: 27-42). Sentaktik saldırıların hedefi bilgisayar işletim sistemleri olup, zararlı kodlar/yazılımlar (Özdemir, 2007), Dağınık Servis Engelleme Saldırıları (DDoS) (Amiri ve Soltanian, 2015:7-12) ve sisteme girmek (bilgisayar korsanlığı-hack)(Rogers ve Devost, 2005: 5-10) şeklinde yapılan saldırılardır. "Semantik saldırılar, bilgisayarların işletim sistemini hedef almazlar, bunun yerine bilgisayar kullanıcısının ulaştığı bilginin doğruluğunu hedef alırlar. Sistem sorunsuz bir şekilde çalışmasına rağmen içerdiği bilgiler doğru değildir. Bu saldırılar, özellikle resmi internet sitelerinin ya da kritik altyapı tesislerinin sistemlerini hedef aldığında ciddi sonuçlar doğurabilir. Nükleer tesisteki bir sistemin hatalı olarak elektriği kesmesi ya da havaalanında kullanılan trafik kontrol sisteminin doğru bilgi vermemesi sonucu meydana gelebilecek hatalı yönlendirmeler örnek olarak gösterilebilir. Karışık saldırılar ise sentaktik ve semantik saldırıların birlikte icra edilmesidir. Kritik işletim sistemlerinin hatalı bilgi ile beslenerek etkisiz hale getirilmesi karışık saldırıya örnek olarak gösterilebilir" (Brenner ve Goodman, 2002: 31-41).

Günümüzde siber uzayda asimetrik savaşlar devam etmekte ve siber tehditler devletler açısından büyük tehlike arz etmektedir. Hem kişiler ve şirketler hem de devletler, sıklıkla zararlı yazılım, botnetler, DDoS saldırıları, virüsler, truva atları, bilgisayar sistemleri zayıflıkları, ağ savunmasızlık problemleri, ihlaller, bilgi hırsızlıkları, kimlik hırsızlıkları vb. siber uzaydaki problemlere ve siber saldırılara maruz kalmaktadırlar. Örneğin ABD'de görülen "NIMDA" isimli saldırı, kritik

altyapılarda yıkıcı bir tahribat bırakmıştır. NIMDA, bilgisayar solucan ve virüsünün karışımı olan bir otomatik siber saldırı olarak tasarlanmıştır. İnanılmaz bir hızla tüm ülkeye yayılarak 86.000 bilgisayara saldırıda bulunmuştur (Yılmaz ve Salcan, 2008: 35-43). Siber tehditler çeşitlenerek artmakta ve devletleri gelecekte büyük tehlikeler beklemektedir. 2014 yılında yayınlanan Pew Araştırma Merkezi (Pew Research Center)'nin raporuna göre, "araştırmaya katılan 1.600 teknoloji uzmanının 3'te 2'si 2025 yılında büyük maddi kayıp ve can kaybının olacağı bir siber savaş beklediklerini ifade etmişlerdir" (Kshetri, 2016: 54).

1.3. Siber Terörizm

Siber terör, 1980'lerde Barry Collin tarafından türetilen bir kavramdır (Gedik, 2018: 34). Siber terörizmin birçok tanımı yapılmıştır. Siber terörizm, "terörist faaliyetlerin siber alan kullanılarak gerçekleştirilmesi olarak ya da terör örgütlerinin siber alanı araç olarak kullanmaları" olarak tanımlanabilir (Kravasin, 2000). Siber terör, "belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla" kullanılır (Wilson, 2003: 4). Başka bir tanıma göre siber terörizm, "politik veya sosyal hedeflerin gerçekleştirilmesi için bir devleti veya vatandaşlarını aşağılamak veya korkutmak üzere bilgisayarlara, ağlara veya bilgilerin depolandığı yerlere gerçekleştirilen kanunsuz saldırı veya saldırı tehditleri" olarak ifade edilmiştir (Denning, 2000). Siber terörizm, "bilgisayar ve iletişim teknolojisi kabiliyetlerinin politik olarak motive olmuş ulus-altı gruplar veya gizli ajanlar tarafından şiddet, bir toplumu etkilemek veya bir hükümetin politikalarını değiştirtmek maksatlı olarak silah veya hedef olarak kullanılması" şeklinde de tanımlanabilir (Andress ve Winterfeld, 2011: 198). FBI ise siber terörizmi, "alt-ulus grupları veya gizli örgütler tarafından savaşçı olmayan hedeflere karşı şiddetle son bulan bilgi, bilgisayar sistemleri, bilgisayar programları ve verilere karşı önceden planlanmış siyasi güdümlü saldırı" olarak tanımlamıştır (Singer ve Friedman, 2018: 134-135).

Terör örgütlerinin kullandıkları yöntemlerin çeşitliliği, eylemlerin zaman ve mekânlarının öngörülememesi, gelişen teknolojinin terör örgütlerine sağladığı avantajlar, terörizm kavramını da değiştirmiştir. Terör örgütleri, siber terör aracılığı ile devletlerin bilişim sistemlerini yasa dışı yollarla ele geçirmeye ve devlet kurumlarının alt yapılarına zarar vermeye çalışmaktadırlar. Bunun yanında siber teröristler, toplum düzenini bozmak maksadıyla ekonomik ve sosyal alanda da saldırılar gerçekleştirerek vatandaşların tedirgin olmalarını sağlarlar (Hatipoğlu, 2017: 165).

Teröristler, klasik yöntemlere oranla çok daha ucuz olması; ani ve beklenmeyen saldırı ile düşmanı hazırlıksız yakalaması ve savunma imkânı vermemesi; tanınma, bilinme olasılığının olmaması; sınırlar ötesine geçişin çok kolay olması gibi nedenlerden dolayı siber terörü tercih ederler. Ayrıca siber terörün bir medya potansiyeli olması da tercih edilmesini sağlamaktadır (Heickerö, 2014: 555). Terör örgütleri propaganda amacıyla da siber yeteneklerini kullanmakta ve ideolojilerini geniş mecralara taşımaktadırlar. Terör örgütleri web siteleri üzerinden yardım kuruluşu kisvesi altında örgüte finans ve insan kaynağı sağlayarak etki alanlarını artırmaya çalışmaktadırlar (Schweitzer, Siboni ve Yogev, 2011: 42).

İnternet, kimliklerini ve bulundukları yeri gizleyen teröristler (Ottis, 2011: 34) tarafından iletişim kurmak, hedef belirlemek ve örgüt için istihbarat toplamak için kullanılmaktadır (Schweitzer vd., 2011: 41-42). Teröristler, genel olarak internet aracılığı ile iletişim kurmakta ve yine internet üzerinden örgüt içi eğitim ve yönetim sağlanmaktadırlar (Kara, 2013: 6-7). Böylece terör örgütleri benimsedikleri ağ tabanlı örgüt yapısı ile örgüt içi iletişim koordinasyon sağlamakta, eylemlerini oluşturdukları bu ağ üzerinden planlayıp icra etmektedirler (Koybko, 2015: 159-161). Son dönemde El Kaide ve IŞİD/DEAŞ gibi terör örgütleri interneti etkin olarak kullanmakta ve uluslararası güvenliği tehdit etmektedirler. Siber uzayın terör örgütleri tarafından etkin olarak kullanılması ve siber saldırılar gerçekleştirmeleri karşısında devletler zor duruma düşmektedirler (Gökçe, Şahinaslan ve Dinçel, 2014: 215). Ayrıca birçok terör uzmanının da belirttiği üzere yalnızca siber terörizmle mücadele etmekle görevli kurum, kuruluş ve uzmanların sayılarının yetersiz oluşu da mücadelede zafiyet yaratmaktadır (Brenner, 2007: 468-469).

1.4. Siber Güvenlik

Siber güvenlik, bütünlük, gizlilik ve erişilebilirlik prensipleri ışığında siber uzayda kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavram ve önlemleri, kurallar, risk yönetimi yaklaşımları, eylemler, eğitimler, uygulamalar ve teknolojilerin bütünü olarak ifade edilmektedir (Hill, 2015: 119-134). Siber güvenlik kavramı kurum, kuruluş ve kullanıcıların varlıkları, bilgi işlem donanımlarını, personeli, altyapıları, uygulamaları, hizmetleri, telekomünikasyon sistemlerini ve siber ortamda iletilen ve/veya saklanan bilgilerin tümünü kapsamaktadır. Siber güvenlik, kurum kuruluş ve kullanıcıların varlıklarına ait güvenlik özelliklerinin siber ortamda bulunan güvenlik risklerine karşı koyabilecek şekilde oluşturulmasını ve idame edilmesini sağlamayı amaçlar (Çiftci, 2013: 8). Siber tehditler birçok gelişmiş devlet

tarafından milli güvenliğe karşı en büyük tehditler arasında görülmeye başlanmıştır. Ancak çok gelişmiş teknolojiye rağmen bir siber saldırının ne zaman yapılabileceğini tahmin etmek oldukça güçtür. Siber tehdit unsurlarının terör örgütleri tarafından da kullanılmaya başlaması ülkeleri yeni stratejiler belirlemeye ve daha fazla tedbir almaya itmektedir (Güntay, 2017: 88). Söz konusu alanın büyüklüğüne karşı siber saldırıları gerçekleştirecek unsurların büyük olmasını gerektirmez. Siber saldırılar asimetrik saldırılar olarak kabul edilir ve saldırganlar ne kadar küçük ise o kadar avantajlı olurlar (Geers, 2010: 15). Siber uzay diğer harekât alanlarından farklı olarak daha çok teknik (yazılım ve donanım) konuları içermesi nedeniyle askerlerden çok özel sektörün hâkim olduğu bir alandır. Bu nedenle siber güvenlik konularında askerler ile teknik personelin (özel sektör, üniversite) işbirliği içinde çalışmaları önem arz etmektedir.

Teknolojik gelişmelerle birlikte ortaya çıkan siber tehditler karşısında devletler güvenlik ihtiyaçlarının karşılanması ve menfaatlerinin devam ettirilmesi kapsamında önemli sıkıntılar yaşamaktadırlar. Siber saldırın tamamına yakınının kritik öneme sahip altyapı sistemlerine ve bilişim sistemleri üzerinde depolanan belge ve bilgilere karşı yapılmış olması devletlerin siber uzay güvenliği konusuna daha fazla yatırım yapmalarını ve işbirliği içinde hareket etmelerini zorunlu kılmaktadır. Özellikle Soğuk Savaş sonrası ortaya çıkan teknolojik gelişmeler paralelinde artan siber tehditler karşısında NATO, ağlarını ve operasyonlarını, devamlı olarak korumak için çaba göstermekte; siber güvenlik konusu ise NATO'nun en önemli gündem maddelerinden birisini teşkil etmektedir.

2. SİBER GÜVENLİK VE NATO

Soğuk Savaş sonrasında NATO, sahip olduğu güç temelinde devamlılığını sağlayacak değişiklikleri gündeme getirme ihtiyacı duymuştur. Bunun sonucunda "Stratejik Konsept" değişikliği gündeme gelmiş ve NATO için yeni görev alanları belirlenerek İttifak'ın devamlılığına karar verilmiştir (Hasgüler ve Uludağ, 2005: 204-209). 1990 Londra Zirvesi'nde "alan dışı" kavramıyla tehdit alanının ve içeriğinin genişlemesine dikkat çekilmiş ve Kuzey Atlantik bölgesi dışında da barış ve güvenliği bozabilecek tehditlere karşı mücadeleyi esas alan bir örgüt olma yolunda adımlar atılmıştır. 7-8 Kasım 1991 tarihleri arasında gerçekleştirilen Roma'daki Zirve'sinde değişen güvenlik anlayışı kapsamında "Yeni Stratejik Konsept" kabul edilmiş ve Kuzey Atlantik bölgesi dışından da gelecek tehditlerle mücadele edilebilmesi maksadıyla sorumluluk sahası genişlemiştir (Peksarı, 2007: 53).

Aralık 1994'te Rus birliklerinin Grozni'ye girmeleri ile Çeçenler başta internet olmak üzere bütün medya araçlarını kullanmış ve bilgi savaşının ilk örneklerini vermişlerdir (Bıçakçı, 2012: 205-226). Siber uzayın etkisini anlamakta geciken Ruslar, bir süre sonra bu saldırılara karşı çeşitli siteler açarak cevap vermişlerdir (Petit, 2003). Bu dönemde siber uzayın öneminin farkında olan NATO, Siber Savunma ve Yönetim Kurulu (Cyber Defence and Management Board /CDMB) ve Askeri Otoriteler ve Muhabere ve Bilgi Sistemleri Ajansı (Military Authorities and Communications and Information Agency /MACIA) gibi oluşumlar meydana getirmiştir. Üye ülkelerin ağ yapısı ve askeri yeteneklerinin farkı nedeniyle NATO Ağ ile Etkinleştirilmiş Güç Programı (Network-Enabled Capability/NNEC) ve Ağ Merkezli Savaş (NCW) için bilişim alt yapısının oluşturulmasına önem verilmiştir. Bu kapsamda 1 Haziran 1996 tarihinde NATO İstişare, Komuta ve Kontrol Ajansı (NATO Consultation, Command and Control Agency/NC3A) kurulmuştur. Ajansın amacı, teknolojik gelişmeleri takip etmek olarak belirlenmiştir. NC3A yapısı içinde siber güvenlik ve bilgi paylaşımı sağlanması maksadıyla görevli bir bölüm de yer almaktadır.

Yeni kurulan bu kurumlar "ortak savunma için müşterek planların tasarlanması; askeri kuvvetlerin görev yapabilmesi için gerekli altyapı ve tesislerinin kurulması; müşterek eğitim programları ve tatbikatların düzenlenmesi konularında daimi bir danışma ve işbirliği olanağı sunmaktadır" (Ada ve Çakır, 2017: 637). Dönemin değişen tehdit yapılarına uygun olarak NATO, ortaya çıkması muhtemel hibrit çatışmaların en önemli unsuru olan siber savaş kabiliyetini edinmek maksadıyla çeşitli toplantılar düzenlemiştir. İlk aşamada askeri komuta-kontrol ağları ve sistemleri siber savaş gereklerine göre düzenlenmeye başlanmıştır. NATO'nun 1998'de düzenlediği "Harekât Sistemlerine Enformasyon Teknolojilerinin Uygulanması" ve 1999'da düzenlediği "21. Yüzyılda NATO Enformasyon Sistemlerini Korumak" başlıklı toplantıları, "NATO'nun yeni döneme uyum sağlama çabasının yansımaları olarak kabul edilebilir" (Bıçakçı, 2016: 205-226). Çünkü 1999 yılında, Sırp hedeflerinin bombalanması sırasında Sırp bilgisayar korsanları tarafından NATO karargâhına ve üye ülkelerin askeri haberleşme sistemlerine çeşitli siber saldırılar düzenlenmiştir.

NATO'nun 50. Kuruluş yılı olan 1999 yılında Washington Zirvesi gerçekleştirilmiştir. Söz konusu Zirve sonrası açıklanan bildiride İttifak'a karşı geniş çaplı bir saldırı ihtimalinin kısa vadede gerçekleşebileceği, ittifak üyelerinin güvenliklerinin, askeri ve askeri olmayan tahmini güç birçok risklerle karşı karşıya

bulunduğunu bildirilmiştir (Pulat, 2002: 38). Bu kapsamda etkin bilgi sistemlerine sahip olunmasının İttifak'ın savunma gücünü arttıracağı vurgulanmıştır (NATO, 1999a). Zirve'de kabul edilen "Yeni Stratejik Konsept"te teknolojinin hızla yayılması ve silah üretim bilgilerine kolaylıkla erişilebilmesi nedeniyle devletler yanında devlet-dışı aktörler de tehdit algısına dâhil etmiştir. Söz konusu Konsept ile birlikte NATO, Hibrit Savaş kavramını benimsemiş ve devlet ve devlet-dışı unsurların İttifak'ın bilgi sistemlerine karşı çeşitli operasyonlar düzenleyerek zarar verebileceği ifade edilmiştir (NATO, 1999b). 1999 Zirvesi'nden hemen sonra, devlet ve hükümet başkanlarının katılımıyla Washington'da düzenlenen "21. Yüzyılda İttifak" başlıklı bir toplantı gerçekleştirilmiştir. Bu çerçevede etkili enformasyon sistemlerine sahip olunmasının savunma gücünü arttıracağı dile getirilmiştir (NATO, 1999b).

11 Eylül sonrasında en çok tartışılan konulardan birisi de NATO'ya ya da Müttefiklere karşı yapılabilecek Dijital Felaket ya da Dijital 9/11 senaryosu olmuştur (Bıçakçı, 2014: 119). Her ne kadar ilk DDoS (Distributed Denial of Service) saldırısı NATO Halkla İlişkiler web sitesine 1999 yılında gerçekleşmiş olsa da NATO'nun muhabere ve bilgi sistemlerinin korunması hususu resmi olarak ilk defa 2002 yılında gerçekleştirilen Prag Zirvesinde gündeme alınmıştır. Prag Zirvesi'nde gelişen bilgi teknolojileri ışığında NATO'nun siber saldırılara karşı savunma birimi olarak kurulan Yükselen Güvenlik Tehditleri Bölümü'nde siber güvenlik; terörizm ve kitle imha silahlarıyla birlikte beş önemli tehditten biri kabul edilmiştir.

NATO, doktrinini siber savaşa göre değiştirmiş ve konunun hukuki ve teknik yönlerinin tartışılması için çalışmalar başlatmıştır. Bu kapsamda NATO'nun siber saldırılara karşı kendini koruyabilecek şekilde yeteneklerini geliştirmesi hususu *Prag Yetenek Taahhütleri*'nin içerisinde yer almış ve Prag Zirvesi NATO'nun siber güvenlik konusuna verdiği önemi göstermesi açısından bir başlangıç olmuştur. Daha sonra NATO, İttifak'ın askeri ve sivil unsurları arasında bilgiyi hızlı ve güvenli bir şekilde bilgi sistemleri altyapısı üzerinden iletmek maksadıyla NATO Ağ ile Etkinleştirilmiş Güç Programı (Network-Enabled Capability-NNEC)'nı başlatmıştır (NATO, 2003). NATO bilişim sistemlerini ve altyapısını savunma kabiliyetlerini artırmak, zararlı yazılımlarla mücadele etmek ve siber saldırılara karşı koyma kabiliyetini artırmak maksadıyla siber tatbikatlar icra etmektedir. Bu maksatla NATO Muhabere ve Bilgi Sistemleri Ajansının bir birimi olan Bilgisayar NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident

Response Capability-NCIRC) birimi Mons'da SHAPE karargâhında bulunmakta ve NATO'nun bilgi sistem ağlarını siber saldırılara karşı 24 saat esasına göre korumaktadır (NATO, 2011). NATO bünyesinde kurulan NATO Muhabere ve Bilgi Ajansı Bilgisayar Olaylarına Müdahale Teknik Merkezi (NCIA NCIRC TC) ile NATO'nun kullandığı muhabere ve bilgi sistemlerinin tedarik, idame ve işletilmesi görevlerini yürütmektedir. Siber Savunma Birimi, NATO Muhabere ve Bilgi Ajansı (NCIA)'na bağlı görev yapan Alt Yapı Servisleri Direktörlüğü altında hizmet sağlamaktadır. 29 NATO üyesi ülkenin siber savunması, merkezi olarak NCIA NCIRC Harekât Birimi tarafından yürütülmektedir. Harekât Birimi, siber saldırılar ve bilgisayar olayları ile ilgili önleme, tespit etme, tedbir alma ve düzeltme faaliyetlerini yürütmektedir. 200 uzman kişiden oluşan söz konusu birim NATO operasyonlarını desteklemekte ve Müttefiklerinin karşılaştıkları siber saldırıların analizini yaparak çözümler üretmektedir. NATO bünyesinde kesintisiz siber güvenliğin sağlanması görevini yürüten bu Birim'nin bir diğer sorumluluğu da web sitelerinin güvenlik takiplerinin yapılmasıdır.

Tehditlerin niteliği değiştikçe uygulanan metotlarda da değişim gündeme gelmiştir. NATO da kendisini buna göre uyarlamaktadır. Siber savunmanın ulusal sınırları aşan doğası nedeniyle İttikak'ın siber savunma kapasitesini artıracak yeni küresel ortaklıklar ittifak tarafından desteklenmektedir. NATO hâlihazırda bilgi teknoloji firmaları olan Microsoft, Google ve IBM, Uluslararası Standartlar Birliği (International Standards Organization-ISO) ve Internet Mühendisliği Görev Kuvveti (Internet Engineering Task Force/IETF) ile işbirliği yürütmektedir (Huges, 2009: 4).

NATO'nun siber güvenliği yeni bir askeri alan olarak gördüğü ve buna yönelik savunma stratejisi oluşturmaya çalıştığı görülmektedir. Bu durum NATO'nun zirvelerinde dile getirilmektedir. Zirve bildirgelerinde, genişleyen güvenlik yelpazesi ile NATO'nun 29 üye ülkesinin hem siyasi hem de askeri liderlerinin ağ güvenliği ile kendi ülke güvenlikleri arasında direkt bir ilişki olduğu anlaşılırken bunun düşmanca eylemlere karşı korunması gerektiğinin kabul edildiği yorumu yapılabilir. Hatta söz konusu tehdit karşısında önlem almak isteyen dokuz NATO üyesi (ABD, Almanya, İngiltere, Fransa, Hollanda, İspanya, İtalya, Kanada, Norveç) 2003 yılında bilgi paylaşımı içeren bir anlaşma imzalamıştır. 2004 yılında Prag Zirvesinden sonra NATO İletişim ve Enformasyon Sistemleri Servisi Ajansı (NATO Communication and Information Systems Services Agency/NCSA) oluşturulmuştur. "Ajans, ağ ile etkinleştirilmiş güç kavramını hayata geçirebilmek

için merkez karargâhı ile diğer görev güçleri arasındaki iletişimi sağlamaktadır. Kosova operasyonundan anlaşıldığı üzere siber saldırılar ilk olarak iletişim kanallarına odaklanmaktadır. Prag Zirvesi'nde alınan kararlardan biri de kritik alt yapıların terörizme karşı korunması için NATO siber savunma programının oluşturulması olmuş, NCSA siber saldırılara karşı ilk müdahaleyi yapacak unsur olarak belirlenmiştir" (Bıçakçı, 2014: 205-226). "NCSA içindeki merkezlerden en önemlisi, muharip unsurların bilgi güvenliği ve ittifak genelinde güvenli iletişimi sağlamakla yükümlü NATO Bilgi Güvenliği Teknik Merkezidir (NATO Information Assurance Technical Centre/NIATC)" (NATO, 2019). NATO'nun 2007 yılına kadar iletişim, bilgisayar güvenliği ve siber güvenliği konularını birlikte değerlendirdiği görülmektedir. "NIATC, bilgisayar ağlarını Bilgi Güvenliği Operasyon Merkezi ve NATO Bilgisayar Olayları Müdahale Gücü Teknik Merkezi'yle (NATO Computer Incident Response Capability Technical Centre-NCIRC) işbirliği içinde ve 7/24 esasında takip etmektedir. Bu gelişmeye müteakip 2006'da yapılan Riga Zirvesi'nde ağ ile güçlendirilmiş komuta-kontrol kavramı üzerinde durulmuş ve bilişim alt yapısının savunmasının iyileştirilmesinin gerektiğine vurgu yapılmıştır" (NATO, 2006).

2-4 Nisan 2008 tarihleri arasında gerçekleştirilen Bükreş Zirvesi'ne üye ülkeler arasında olan Estonya'nın yaşadığı kriz damga vurmuştur. O zamana kadar hiçbir ülkede görülmeyen boyutta bir dijital saldırıya maruz kalan Estonya'da kurumlarının neredeyse tamamının dijitalleşmiş olması ve vatandaşların gündelik birçok işini internet üzerinden gerçekleştirmesi yaşanan bu saldırı sonucunda altyapının çökmesine sebep olmuştur. Rus devleti ve Estonyalı Ruslar dünya genelinde aldıkları destekle hareket ederek dünya'nın birçok farklı noktasından siber saldırılarına yaklaşık bir ay süresince (28 Nisan–23 Mayıs 2007 devam etmişlerdir. O zamana kadar böylesine bir tehdit algısı öngörmeyen ve stratejik planlar üretme gereği duymayan NATO, bir ay boyunca siber saldırılara maruz kalan müttefiki Estonya'ya anlık destek sağlayamamıştır. Yapılan bu siber saldırılar ile bir devletin kritik alt yapı sistemlerinin internet üzerinden gelebilecek siber tehditlere karşı ne kadar açık olabileceği ortaya çıkmıştır. Müttefiklerine karşı yapılan üst düzey siber saldırılar, NATO'nun siber dünyasını güçlendirmesi ve bu yönde savunmasını geliştirmesi gerektiğini ortaya koymuştur. Bunun üzerine Siber güvenlik NATO'nun Bükreş Zirvesi'nde toplantının ana gündem maddesi haline getirilmiş ve 21. yüzyılın tehditleri bağlamında siber güvenliğin bir tehdit olarak görüldüğü belirtilerek stratejik ve taktik seviyede mücadele organları oluşturulması kararı alınmıştır.

01 Ağustos–01 Eylül 2008 tarihleri arasında Gürcistan'ın bilişim sistemlerinin kritik alt yapısındaki açıklıklar kullanılarak Estonya'da yapılana benzer tarzda bir siber saldırı gerçekleştirilmiştir. Estonya'da yaşanan olay neticesinde NATO iki önemli tedbir alma yoluna gitmiştir. İlk olarak böyle bir siber saldırının tekrar yaşanması ihtimaline karşı savunmanın ortak bir strateji ile yapılabilmesi için Bürüksel'de Siber Savunma Yönetimi Otoritesi (Cyber Defence Management Authority/CDMA)'ni oluşturmuştur. İkinci olarak "Siber savunma kapasitesini bir merkezde toplayarak harekât kabiliyetini daha arttırmayı amaçlayan NATO, Ekim 2008'de Estonya/Tallinn'de bir NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence/NATO CCD COE) kurmuştur" (NATO, 2019). Bu merkezin görevleri "siberle ilgili konularda ittifak için doktrinler ve kavramlar üretmek; NATO'ya üye ülkeler için eğitim kursları, atölye çalışmaları düzenlemek; tatbikatlar yapmak; araştırmalar yapmak ve gelişmeler üzerine toplantılar düzenlemek; geçmişteki ve hâlihazırdaki saldırıları çalışarak dersler çıkarmak; devam eden saldırılarda eğer istenirse tavsiyeler vermek" olarak sıralanmıştır (NATO CCDCOE, 2019). NATO bünyesinde faaliyet gösteren ve 30 personelden oluşan CCDCOE, siber güvenlik konusunda önemli gelişmelere imzasını atmıştır. Birincisi, siber dünyanın genelini ilgilendiren konularda hukuki bir zemin oluşturmak için 2009 ve 2012 yılları arasında, uluslararası hukuk uzmanlarınca yazılan ve savaş hukuku ile uluslararası insani hukukun siber savaşa uygulanabilirliğini irdeleyen *Tallinn El Kılavuzu*'dur. İkincisi, NATO ülkelerinin katılımıyla siber güvenlik konusunda gerçekleştirdiği Uluslararası Siber İhtilaf Konferansları (Conference on Cyber Conflict/CyCon)'dır. Üçüncüsü ise, NATO üye ülkelerinin tamamının katıldığı ve müştereken icra edilen tatbikatlardır. Her yıl CCDCOE koordinasyonunda gerçekleştirilen tatbikatlara üye ülkelerin tamamından gelen bilişim uzmanları, askeri personel ve karar vericiler katılmaktadırlar. Bu kapsamda dünyanın en geniş katılımlı siber tatbikatı olan "Locked Shields" tatbikatı 2010 yılından itibaren her yıl icra edilmektedir. Böylece NATO CCDCOE koordinasyonunda icra edilen söz konusu tatbikatlarla, İttifak üyesi devletlerin ulusal bilgi teknolojisi (BT) sistemlerinin korunabilmesi için siber uzmanların becerilerinin ve yeteneklerinin geliştirilmesi amaçlanmaktadır (NATO CCDCOE, 2019).

2010'da gerçekleştirilen NATO Lizbon Zirvesi'nde, yeni güvenlik tehditlerinin tanımlanması, bu tehditlerle baş etmek için neler yapılması gerektiği konusunda kararlar alınmış ve Zirve aktif katılım ve modern savunmayı önceleyen yeni bir Stratejik Konsept'in benimsenmesiyle son bulmuştur. Zirve'de NATO'nun

savunma ve caydırıcılık konumunun gözden geçirilmesinin devam edilmesine ve siber savunma yeteneklerinin güçlendirilmesine karar verilmiştir (Lizbon Summit Declaration, 2010). Böylece NATO'nun bir yandan geleneksel toplu savunma görevini yerine getirirken bir yandan da yeni tehditlere karşı savunma ve caydırıcılık yeteneğinin modernizasyonuna karar verilmiştir. Bu kapsamda siber saldırılar ve terörist saldırılardan korunmaya yönelik güçlendirilmiş önlemler alınması ve siber savunmanın sürekli olarak NATO gündeminde tutulması kararlaştırılmıştır.

Haziran 2011 tarihinde NATO Savunma Bakanları, "Gözden Geçirilmiş NATO Siber Savunma Politikası"nı kabul etmişlerdir. Bu politika, siber savunma konusunda gerçekleştirilecek olan topluluk bazındaki çabaları içermektedir. Ekim 2011 tarihinde Bakanlar tarafından, "Siber Savunma Eylem Planı"nın detayları üzerinde görüş birliğine varılmıştır. "NATO'nun siber savunma politikasına göre İttifak'ın siber güvenlik politikasındaki öncelikler; koordinasyon temelli bir yaklaşımla siber saldırılara karşılık verecek mekanizmalar geliştirmek için plan ve kapasite gelişimi sağlamak, tüm üye devletler bazında bir politika oluşturmak adına devletlerin siber savunma politikalarını uyumlu hale getirmektir" (NATO, 2011). "Bu bağlamda NATO, kendince merkezileştirilmiş ancak üye devletlerinin her birinin asgari siber savunma gerekliliklerinin karşılandığı bir politika ortaya koymaktadır" (NATO, 2011).

Şubat 2012'de NATO, "Bilgisayar Olayları Karşılama Kapasitesinin (NATO Cyber Incident Response Capability/NCIRC) 2012 yılı sonunda tamamen operasyonel hale gelebilmesi için 58 milyon Avroluk bir kontrat imzalanmıştır" (NATO, 2012). Ayrıca, istihbarat paylaşımı ve durumsal farkındalık için bir "Siber Tehdit Farkındalık Birimi" oluşturulmuştur (NATO, 2012). 2012 yılında ABD'nin Chicago şehrinde gerçekleştirilen Zirve'de "güvenlik tehditleri bağlamında siber saldırı, nükleer silahların ve atma vasıtalarının yayılması, terörizm, enerji ulaşım yollarına saldırı ve çevreye yönelik tehditlere dikkat çekilmiş; sürekli gelişen ve karmaşıklaşan siber tehditlerle etkin biçimde ve işbirliği içinde mücadele edilmesi gerektiği vurgulanmıştır" (Chicago Summit Declaration, 2012). Zirve Sonuç Bildirisi'nden ayrı olarak yayımlanan "Savunma Yetenekleri: 2020 NATO Kuvvetlerine Doğru" başlıklı sonuç bildirisinde daha başarılı operasyonlar gerçekleştirmek amacıyla siber saldırılara karşı savunmayı artırmak için ciddi ilerlemeler sağlandığı ifade edilmiştir.

2014 Galler Zirvesi'nde sürekli daha karmaşık ve yaygın hale gelen siber saldırılarla mücadele etmek maksadıyla güçlendirilmiş siber savunma politikası onaylanmıştır. Zirvede NATO liderleri siber saldırıların ortak savunma ile ilgili 5. Maddeyi tetikleyebileceğini ifade etmişlerdir. NATO kendisine ait bir siber savunma politikası belirlemiş ve siber tehditlere karşı stratejik seviyede bir eylem planı geliştirmiştir. Teknolojinin gelişmesine paralel olarak siber tehdit konuları da artacağından Müttefikler arasındaki diyalog süreci ve koordinasyonun devam ettirilmesine karar verilmiştir. Siber tehdit unsurları ile mücadelede faydalanılabilecek hukuki bir dayanak olmadığı için bu kapsamda da çalışmaların başlatılmasına karar verilmiştir. Ayrıca siber tehditlere karşı kapsamlı siber savunma planlarının yapılması için Müttefiklerin kendi ülkelerindeki kurumları sürekli olarak desteklemelerinin önemi ifade edilmiştir.

NATO, 2016 Varşova Zirvesi'nde siber uzayı -aynen kara, deniz, hava ve uzay gibi- bir harekât sahası olarak tanımlamıştır. NATO'nun yeni güvenlik konseptinde mücadele edilmesi gereken öncelikli alanlar içerisinde yer alan "siber güvenlik alanında üye ülkelerin daha fazla işbirliği içerisinde olması gerektiğine vurgu yapılmıştır. Bu durum NATO askeri komutanlarının siber tehditlere karşı operasyonları daha iyi gerçekleştirmelerine ve görevlerini yerine getirmelerine imkân sağlamıştır. Siber tehditlerin sürekli şekil değiştirmesi; bu tehditlerin kaynaklarının belirgin olmaması ve uluslararası hukukta bu alanda ciddi boşluk bulunması NATO'nun Varşova'da aldığı daha fazla işbirliği kararının kâğıt üstünde kalmaması" gerektiğini göstermektedir (NATO, 2016). İttifak üyeleri, aynı zamanda 2016 yılında kabul edilen Siber Savunma Taahhüdü (Cyber Defence Pledge) gibi girişimlerle kendi ulusal ağlarının ve altyapılarının da siber güvenliğini güçlendirmektedirler. NATO, Müttefiklerin siber savunma yeteneklerini artırmak için ortak bir yaklaşım geliştirecek hedefler belirlemektedir. Siber Koalisyon (Cyber Coalition) gibi dünyanın en geniş savunma tatbikatına ve eğitime yatırım yapmaktadır. Zirve kapsamında, NATO-Avrupa Birliği (AB) Ortak Deklarasyonu da imzalanmıştır. Böylece iki örgüt arasında mülteci krizi ve siber tehditler gibi üst düzey işbirliği gerektiren alanlarda daha fazla işbirliğinin önü açılmıştır. Misyonlar, operasyonlar, tatbikatlar ve eğitimler dâhil olmak üzere siber güvenlik ve savunma alanında koordinasyonun artırılmasına karar verilmiştir.

2018 Brüksel Zirvesi'nde siber güvenlik alanında müttefiklerinin savunmasını güçlendirmek maksadıyla Mons/Belçika'da bir Siber Operasyonlar Merkezi'nin kurulmasına karar verilmiştir. 2023 yılında tamamen faaliyete geçecek olan bu

merkez NATO'nun siber uzaydaki askeri operasyonlarında etkin olarak kullanılacak ve durumsal farkındalık sağlayacaktır. Bu merkezin yanında halen hizmet vermekte olan Roma/İtalya'daki NATO Savunma Koleji'nde ise siber savunma kapsamında stratejilerin belirlenmesi maksadıyla çeşitli eğitimler verilmektedir. Ayrıca Oberammergau/Almanya'daki NATO Okulu'nda, İttifak'ın operasyonlarını, stratejisini, politikalarını ve doktrinlerini desteklemek üzere siber ile ilgili çeşitli eğitimler verilmektedir. NATO siber işgücünün eğitimi ise Oeiras/Portekiz'de halen inşa edilmekte olan NATO Muhabere ve Bilgi Sistemleri Akademisi tarafından sağlanacaktır.

3-4 Aralık 2019 tarihleri arasında gerçekleştirilen Londra Zirvesi'nde de siber güvenlik konusu gündeme gelmiş ve özellikle Zirve Sonuç Bildirisi'nin 3. ve 6. maddelerinde bu konuya yer verilmiştir. "Sonuç Bildirgesi'nde İttifak'ın siber tehditlerle karşı karşıya kaldığı ifade edilmiştir. Bu tehditlere karşı "güvenliğe 360 derece yaklaşımına" uygun olarak NATO'nun mevcut askeri kapasitesini ve planlarını uyarlayacağı ifade edilmiştir. Bu kapsamda NATO'nun 5G dâhil, iletişim sistemlerini siber saldırılara karşı koymak için mücadele araçlarını artıracağı ve bu saldırılara engel olmak amacıyla kabiliyetini güçlendireceği ifade edilmiştir" (NATO, 2019).

NATO, değişen ihtiyaçlar doğrultusunda siber güvenlik çalışmalarını genişletmeye devam etmektedir. NATO üyesi Estonya'ya karşı yapılan siber saldırıya karşı ABD, 2009 yılında İran'ın nükleer tesislerini hedef alarak kendi kendine kopyalanarak çoğalabilen birçok virüs ve saldırıdan çok daha etkili olan Stuxnet (solucan) yazılımını kullanmıştur. Bu saldırı siber uzayda gerçekleştirilen saldırılar içerisinde bir evrim niteliği taşımaktadır (Collins ve McCombie, 2012: 80). Bu yeni savaş düzeninde sadece iyi bir orduya sahip olmak yeterli olmadığı; bilgi ve iletişim teknolojileri konusunda da güçlü olmak gerektiği ortaya çıkarmıştır. NATO, yenilenen Stratejik Konsept'inde de siber uzaya yer vermiştir. Estonya ve Gürcistan'a karşı yapılan siber saldırılar sonrasında NATO'nun siber saldırılara karşı geleneksel uluslararası hukuktan kaynaklanan meşru müdafaa hakkını kullanacağını açıklaması tartışmaları beraberinde getirmiştir. "Siber saldırılar, yalnızca siber saldırı ile birlikte ya da siber saldırı aracılığıyla klasik anlamda askeri silah kullanıyorsa silahlı saldırı olarak kabul edilebilir. Siber saldırı sonucu yönlendirilen bir bombanın bilgisayar destek merkezini veya internet kablolarını vurması ve bu silahlı saldırının "yeterli ağırlık" (Sthan, 2003) ölçüsüne ulaşması buna örnek olarak verilebilir" (Schmitt, 1999). "Ancak bir silahlı

saldırının, konvansiyonel askeri kuvvet kullanılmasıyla gerçekleştirilmek zorunda olmadığının kabul edilmesi, potansiyel riskler ortaya çıkarmaktadır. Siber saldırıların, silahlı saldırı olarak kabul edilmesi durumunda BM Antlaşması'nın 51. maddesinin uygulama alanı genişleyecek ve uluslararası ortamı yeni karışıklıklara sürükleyecektir" (Yayla, 2013: 203). Son yıllarda siber saldırıların giderek artması karşısında NATO'nun 5'inci Madde'sinin uygulamaya geçip geçmeyeceği konusunda tartışma başlamıştır. NATO Genel Sekreteri Stoltenberg, "ciddi bir siber saldırı NATO için kuruluş anlaşmamızdaki 5'inci maddeyi tetikleyebilir. Bu, bir Müttefikimize yönelik saldırının herkese karşı yapılmış sayılmasına yönelik ortak taahhüdümüzdür." ifadesini kullanmıştır (BBC, 2019).

SONUÇ

İçinde bulunduğumuz yüzyılda güvenlik ortamında tehdit yelpazesi genişlemiş, güvenliğe yönelik risk ve tehditler, çok boyutlu ve asimetrik hale dönüşmüştür. Yeni güvenlik ortamı tahmin edilebilir olma özelliğini büyük ölçüde yitirmiş ve istikrarsız bir hale gelmiştir. Değişen bu güvenlik algısı sebebiyle siber tehdit, siber savaş, siber terörizm ve siber güvenlik konuları NATO'nun güvenlik stratejileri kapsamına girmiştir. Siber savunma konusu NATO'nun yeni Stratejik Konseptinde yer almış ve NATO'nun bünyesinde siber tehditlerle mücadele maksadıyla çeşitli stratejiler ve birimler oluşturulmuştur. Ancak NATO'nun siber savunma konusunda daha hızla ilerlemesinin önünde çeşitli engeller bulunmaktadır. NATO tarafından belirlenen stratejiler ekonomik sorunlar, teknolojik yetersizlikler ve yeterli eğitime sahip personelin bulunmaması gibi nedenlerden dolayı Müttefikler tarafından hemen kabul edilerek uygulanmamaktadır. Ayrıca siber güvenlik açısından NATO'nun üyeleri arasında dijital bir bölünmüşlük de mevcuttur. Bir yanda gelişmiş sinyal izleme sistemleri kullanan siber ordulara sahip ABD ve İngiltere gibi ülkeler yer alırken diğer tarafta dijital yarışta çok geride bulunan Romanya, Bulgaristan, Litvanya ve Çek Cumhuriyeti gibi ülkeler bulunmaktadır. NATO'nun siber savunma konusunda hızla ilerlemesinin önündeki engellerden bir diğeri de tehdidin sürekli değişken ve varlığını sürdürüyor olmasıdır. Siber tehdidin asimetrik oluşu ve saldırı yapıldıktan sonra saldırganların hızla izlerini silebiliyor olması siber tehditlerle mücadelede en önemli engellerden birisini teşkil etmektedir.

Yukarıda sayılan nedenlerden dolayı günümüzün yapılanmasıyla hem NATO'nun hem de Müttefiklerin siber saldırılara karşı hızla cevap verebilmeleri mümkün görünmemektedir. Siber tehditlerle mücadele kapsamında öncelikle siber

saldırılara karşı NATO'nun 5. Maddesinin nasıl yürürlüğe gireceğinin açıklığa kavuşturulması gerekmektedir. Bu maksatla öncelikle siber tehdit, siber saldırı gibi kavramların tanımlanması ve siber saldırılara karşı nasıl orantılı bir karşılık verileceği belirlenmelidir. Bunun yanında NATO kapsamında Siber uzay ile ilgili doktrinlerin oluşturulmasına ve geliştirilmesine devam edilmelidir. NATO tarafından alınan kararlar Müttefikler tarafından ivedilikle uygulamaya geçirilmeli ve siber güvenlik konusunda gerekli yatırım ve çalışmalar yapılmalıdır. Bunun yanında NATO'nun güçlenerek siber saldırılara karşı koyabilmesi için NATO üyelerinden teknolojik gelişmişlik açısından önde olan devletlerin kendi imkânlarını ve kabiliyetlerini diğer Müttefiklerle kıskanmadan paylaşmaları önemlidir. NATO'nun siber güvenlik konusunda yetkinliğinin en zayıf üye devletin yetkinliği kadar olduğu çıkarımı yapılabilir. NATO üyesi ülkelerden birisinin kritik altyapılarına karşı gerçekleştirilecek bir siber saldırının diğer ülkeleri de ilgilendiren sonuçları olabilecektir. Bu nedenle Müttefiklerin siber savunma imkân ve kabiliyetlerinin bir bütün olarak değerlendirilmesi önem teşkil etmektedir.

Sonuç olarak, NATO'nun daha fazla kaynak ayırarak CCDCOE koordinasyonunda icra edeceği tatbikatlar ile siber savunma yeteneğini geliştirmesinin ve 2019 Londra Zirvesi'nde de ifade edildiği gibi etkin planlama ve strateji oluşturmasının İttifak'ın siber tehditlerle mücadelesine olumlu katkı sağlayacağı değerlendirilmektedir.

KAYNAKÇA

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

Amiri, I. ve Soltanian, M. (2015). *Theoretical and Experimental Methods for Defending Against DDoS Attacks*, Elsevier.

Andress, J. ve Winterfeld, S. (2011). *Cyber Warfare*, Elsevier.

Arquilla, J. ve Ronfeldt, D. (2001). The Advent of Netwar (Reviseted). In J. Arquilla & D. Ronfeldt (Eds.), *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Santa Monica, CA: RAND, ss. 1-25.

BBC (2019.). *NATO: Cyber-attack on one nation is attack on all*. 27.Agu.2019. Erişim Tarihi: 28 Haziran 2019,.https://www.bbc.com/news/technology-49488614

Brenner, S. W. (2007). "At Light Speed: Attribution and Response to Cybercrime/Terrorism/Warfare", *Journal of Criminal Law and Criminology*, No: 2, Vol. (97), ss. 379-476.

Brenner, S. W. ve Goodman, M. D. (Bahar 2002). "In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks", *University Of Illionis Journal of Law, Technology and Policy*. Vol. 2002, Erişim Tarihi: 6 Eylül 2019, https://pdfs.semanticscholar.org/4e3a/5bb4112234fa3fb33a89eeb7e5f3a7950b6c.pdf

Bıçakcı, S. (2014). NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik. *Uluslararası İlişkiler, 10* (40), 101-130.

Clarke, R. ve Knake, R. K. (2011). *Siber Savaş Ulusal Güvenliğe Yönelik Yeni Tehdit* (Çev. M. Erduran), İstanbul Kültür Üniversitesi, İstanbul.

Collins, S. ve McCombie, S. (2012). Stuxnet: The Emergence Of A New Cyber Weapon And İts İmplications. *Journal of Policing, Intelligence and Counter Terrorism*, Vol. 7, No. 1, ss. 80-91.

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

Çiftçi, H. (2013). *Her Yönüyle Siber Savaş*, İstanbul: TUBİTAK Popüler Bilim Kitapları.

Çolak, H. (2011). Siber Terör, Yargılama Usulü ve Önleyici Tedbirler, *Kazancı Hakemli Hukuk Dergisi*. ss. 62-142.

Denning, D. E. (2001). *Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*. Erişim Tarihi: 2 Temmuz 2019, http://www.nautilus.org/info-policy/workshop/papers/denning.html

Denning P. J. ve Denning, D. E. (2010). The Profession of IT Discussing Cyber Attack, *Viewpoints*, September 2010 Vol. No.9, s. 29. Erişim Tarihi: 1 Temmuz 2019, http://calhoun.nps.edu/bitstream/handle/10945/35515/cacm Sep10.pdf? sequence=1

Gedik, D. (2018). *Siber Güvenlik ve Terörizmin Evrilişi: Türkiye Üzerine Etkileri*. (Yayınlanmamış Yüksek Lisans Tezi). Düzce Üniversitesi, Sosyal Bilimler Enstitüsü, Düzce.

Geers, K. (2010). Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL. (Yayınlanmamış Doktora Tezi). Tallinn University Of Technology Faculty of Information Technology, Tallinn.

Gibson, W. (1984). *Neuromancer*, (Çev. M. Altıntaş), Gündüz Yayınları, İstanbul.

Gökçe, K. G., Şahinaslan, E. ve Dinçel S. (2014). *Mobil Yaşamda Siber Güvenlik Yaklaşımı,* 7'nci Uluslararası Bilgi Güvenliği ve Kriptoloji ve Konferansı, (214-221).

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

Hasgüler, M. ve Uludağ, M. B.(2005). *NATO, Devletlerarası ve Hükümetler-dışı Uluslararası Örgütler*, Nobey Yayın, Ankara.

Hatipoğlu, C. (2017). Teknolojik Savaşlar: Siber Terörizm Tehditleri, 3nd International Congress on Political, Economic and Social Studies (ICPESS), 09-11 Nov. 2017.

Heickerö, R. (2014). Cyber Terrorism: Electronic Jihad. *Strategic Analysis*, 38(4).

Hill, R. (2015). *Dealing With Cyber Security Threats: International Coorporation*, ITU and WCIT. 7th International Conference on Cyber Conflict, 119-134.

Huges, R. B. (Nisan 2009). *NATO Cyber Defence*. Erişim Tarihi: 07 Temmuz 2019, https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf

Kara, M. (2013). Siber Saldırılar - Siber Savaşlar ve Etkileri. (YayımlanmamışYüksek Lisans Tezi). İstanbul Bilgi Üniversitesi, İstanbul.

Kravasin, S. (2000). *What is Cyber Terrorism?* Computer Crime Research Center. Erişim Tarihi: 18 Temmuz 2019, http://www.crime-research.org/library /Cyber-terrorism.htm

Kshetri, N. (2016). *The Quest to Cyber Superiority*. Switzerland: Springer.

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*. USA, RAND Corporation, Project Air Force. Erişim Tarihi: 16 Temmuz 2019,.https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG877.pdf

Lisbon Summit Declaration. 20.11.2010. Erişim Tarihi: 18 Temmuz 2019, http://www.nato.int/nato_static/assets/pdf/pdf_publications/20120207_strategic-concept-2010-tur.pdf

Murphy, M. (2010). 'War in the Fifth Domain; Cyberwar'.*The Economist*, 3 July 2010. Erişim Tarihi: 16 Temmuz 2019, https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain

NATO (1999a). *An Alliance for the 21st Century Washington Summit Communique issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 24th April 1999.* Erişim Tarihi: 18 Temmuz 2019, http://www.nato.int/cps/en/natolive/official_texts_27440.htm

NATO (1999b). *The Alliance's Strategic Concept, 24 Nisan 1999*. 23. Madde. Erişim Tarihi: 19 Temmuz 2019, http://www.nato.int/cps/en/natolive /official_texts_27433.htm

NATO (2003). *The Prague Summit and NATO's Transformation.* 2003. Erişim Tarihi: 2 Haziran 2019, http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf

NATO (2006). "Riga Summit Declaration, 29 Kasım 2006", http://www. nato.int/docu/pr/2006 /p06-150e.htm (Erişim Tarihi: 22.07.2019).

NATO (2011). NATO CIS Cervices Agency, *NATO Cyber Defence Management*. Erişim Tarihi: 21 Temmuz 2019, http://www.nato.int/cps/en/natolive/ news_85161.htm

NATO (2012a). *Chicago Summit Declaration*. 20.5.2012. Erişim Tarihi: 26 Temmuz 2019, http://www.nato.int/cps/en

NATO (2012b). *NATO Rapid Reaction Team to Fight Cyber Attack*. 13.3.2012. Erişim Tarihi: 23 Temmuz 2019, http://www.nato.int/cps/en/natolive/ news_85161.htm

NATO (2016). *Warsaw Summit Key Decisions.* February 2017. Erişim Tarihi: 23 Temmuz 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_ 2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf

NATO CCDCOE (2019). *Exercises*. Erişim Tarihi: 13 Ağustos 2019, https://ccdcoe.org/exercises/

NATO CCDCOE (2019). *About us*. Erişim Tarihi: 146 Ağustos 2019, https://ccdcoe.org/

NATO (2019). *NATO Cyber Defence*. Erişim Tarihi: 12 Ağustos 2019, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_190 2-factsheet-cyber-defence-en.pdf

NATO (2019). *NATO London Declaration.* Erişim Tarihi: 12 Aralık 2019, https://www.nato.int/cps/en/natohq/official_texts_171584.htm

Ottis, R. (2011). A Systematic Approach to Offensive Volunteer Cyber Militia. (Yayımlanmamış Doktora Tezi). Faculty of Information Technology, TUT Press.

Ottis, R. ve Lorents, P. (2010). "Cyberspace: Definition and Implication", International Conference on Information Warfare and Security, XII. Reading: Academic Conferences International Limited.

Petit, B. S. (2003). Chechen Use of the Internet in the Russo-Chechen Conflict. (Yayımlanmamış Yüksek Lisans Tezi). The U.S. Army Command and General Staff College Fort Leavenworth, Kansas.

Pierce, B. M. (2018). DARPA's Quest For a Beneficent Cyber Future, *DARPA Defense Advance Research Projects Agency 1958-2018*. Erişim Tarihi: 22.07.2019, https://www.darpa.mil/attachments/DARAPA60 publication-no-ads.pdf

Rogers, R. ve Devost, M. (2005). *Hacking a Terror Network: The Silent Threat of Covert Channels*, Elsevier.

Schmitt, M. N. (1999). Computer Network Attack and the Use of Force in International Law: Thoughts on a Normative Framework, Research Publication 1 Information Series, 1999, ss. 21-22. Erişim Tarihi: 12 Temmuz 2019, http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA471993

Schweitzer, Y., Siboni, G. ve Yogev E. (2011). "Cyberspace and Terrorist Organizations", *Millitary and Strategic Affairs*, 3(3).

Singer, P.W. ve Friedman, Allan (2018). *Siber Güvenlik ve Siber Savaş* (Çev. A. Atay), Buzdağı Yayınları.

Standler, B. R. (2002, September 4). *Computer Crime*. Erişim Tarihi: 25 Temmuz 2019, http://www.rbs2.com/ccrime.htm

Sthan, Carsten (2003). "Nicaragua is Dead-Long Live Nicaragua-the Rigt to Self Defence Under Article 51 of UN Charter and International Terrorism", *Terrorism as a Challenge for National and International Law: Securtiy versus Liberty*, Berlin&Heidelberg. Erişim Tarihi: 20 Temmuz 2019, http://edoc.mpil.de/conference-on-terrorism/index.cfm

Whittaker, J. (2004). *The Cyberspace Handbook***,** Oxon, Routledge.

Wilson, C. (2003). Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress. 34. No. 90. Erişim Tarihi: 20 Eylül 2019, https://fas.org/irp/crs/RL32114.pdf

Van A. ve Richard H. (2018). Darpa Innovation Icon at 60, *DARPA Defense Advance Research Projects Agency 1958-2018.* Erişim Tarihi: 22 Temmuz 2019, https://www.darpa.mil/attachments/DARAPA60publication-no-ads.pdf

Yayla, M. (2013). Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma, *TBB Dergisi* 2013 (107). Erişim Tarihi: 22 Temmuz 2019, http://tbbdergisi.barobirlik.org.tr/m2013-107-1293

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

RUSYA POLİS YAPILANMASINDA MODERNLEŞME VE KAMUOYU ALGISI[*]

Muhittin TATAROĞLU[**]

Öz

Rusya coğrafi genişliği, uluslararası siyaset alanında önemli bir aktör olması, kendine özgü siyasi, idari, sosyal ve kültürel yapısıyla önemli ülkelerden biridir. Sovyetler Birliği dağılınca, yerine kurulan Rusya ve ayrılan diğer devletler siyasi, ekonomik, idari ve toplumsal tüm yapılarını dönüştürme sürecine girmişlerdir. Bu süreçte kültürel ve ulusal değerler farklı bir yapılanma sürecine girmiştir.

Rusya kolluk yapısının 2000'li yıllarda gösterdiği değişim ve reform süreci ilk elde suç sayısında azalma, kolluk teşkilatı hakkında kamuoyunda olumlu algıların artması gibi sonuçlar vermiştir. Bu gelişme toplumların ancak güvenlik, asayiş ve huzur sağlandıktan sonra, ekonomik, siyasi, sosyal ve diğer hümanist boyutlarıyla gelişebileceği gerçeği bakımından önemlidir.

Çalışmada farklı araştırma yöntemleri kullanılmıştır. Rusya kolluk teşkilatının tarihçi-kurumsal yaklaşımla tasvir edilmesinde yazılı birincil kaynaklar ve mülakatlardan yararlanılmıştır. Rusya kolluk teşkilatının geçirdiği yapısal ve işlevsel dönüşüm ise ilgili, yasalar, kararlar, talimatlar ve diğer mevzuatın incelenmesi, kurumların incelenmesi, sahada yapılan birinci elden gözlemler ve mülakatlarla değerlendirilmiştir. Yararlanılan istatistiksel verilerin güvenilirliği ise karşılaştırma yöntemleriyle sorgulanmıştır.

***Anahtar Kelimeler**: Kolluk Hizmetleri, Polis, Reform, Rusya.*

MODERNIZATION AND PERCEPTION OF PUBLIC IN RUSSIAN POLICE STRUCTURE

Abstract

Russia is one of the important countries with its geographical width, being an important actor in the field of international politics and its unique political, administrative, social and cultural structure. After the collapse of the Soviet Union; Russia and other countries gaining their independence went through the process of transforming all their political, economic, administrative and social structures. Within this process, cultural and national values entered into a different transformation.

The change and reform process of the Russian law enforcement in the 2000s, yielded positive results such as a decrease in the number of crimes in the first hand and an increase in the public perceptions about law enforcement. This development is important in terms of the fact that societies can only develop in economic, political, social and other humanist dimensions after security, public order and peace are ensured.

Various research methods were employed in the study. In describing the Russian law enforcement organization with a historical-institutional approach, written primary sources and interviews were used. On the other hand, the structural and functional transformation of the Russian law enforcement agencies has been evaluated through various ways including the examination of relevant laws, decisions, instructions other legislation, examination of institutions, first-hand observations and interviews in the field. The reliability of the statistical data was questioned by comparison methods.

***Keywords**: Law Enforcement, Police, Reform, Russia.*

[*] Çalışmada yazarın "Rusya'nın İç Güvenlik Yönetimi" adlı eserinden geniş ölçüde yararlanılmıştır (Tataroğlu, 2019). Çalışma 19-20 Eylül 2019 tarihinde Uluslararası Güvenlik Kongresi'nde sunulan "2000'li Yıllarda Rusya Polis Yapısındaki Gelişmeler" konulu bildirinin geliştirilmiş halidir.

[**] Doç. Dr., MSKÜ, Kamu Yönetimi Bölümü, muhittintataroglu@yahoo.com, https://orcid.org/0000-0001-9071-6720

Makale Geliş Tarihi: 14.10.2019 Makale Kabul Tarihi: 31.01.2020

GİRİŞ

Güvenlik bir topluluğun en temel gereksinimidir. Güvenlik, toplumu oluşturan bireylerin birbirleriyle ilişkilerini düzenler ve bu ilişkilerde haksızlık ve adaletsizlikleri önler; toplumun bir arada yaşamasını sağlayan normların uygulanmasını sağlar. Güvenlik olmadığı takdirde toplumun bir arada yaşaması mümkün değildir; toplumsal düzen işlemez hale gelir ve toplum varlığını sürdüremez, nihayetinde dağılır.

Sovyet Birliği'nin son yıllarında kamu yönetiminin tüm boyutlarıyla işlevlerini yerine getirememesi, özellikle kolluk teşkilatının hemen tümüyle yozlaşarak toplumun güvenlik gereksinimi karşılayamaması, sistemin çökmesi ve ülkenin dağılmasının başlıca sebepleri arasındadır. Sovyetler Birliği dağıldıktan ve Rusya Federasyonu kurulduktan sonra girişilen reform çabaları 1990'lar boyunca fazla başarılı sonuçlar ortaya koyamamıştır. Art arda yapılan reform çabaları ancak 2010'lu yıllardan itibaren somut başarılara ulaşmaya sergilemeye başlamıştır.

Bu dönemde suç istatistikleri düşmeye başlamıştır. Polis teşkilatının halkla ilişkiler boyutunda gerçekleştirilen düzenlemelerin de katkısıyla kamuoyunda kolluk teşkilatı algısında da olumlu gelişmeler gözlenmiştir. Sovyet döneminde vatandaşın en gündelik yaşam detaylarına müdahale eden ve korku salan militsia döneminin ardından 1990'lı yıllarda güvenliği sağlamak ve suçtan korumaktan ziyade suç örgütlerinin nüfuzuna girmiş; suç mağduru vatandaşların tekrar mağdur olma korkusuyla polise müracaat etmekten çekindiği bir kolluk geçmişinden sonra elde edilen bu başarılar oldukça anlamlıdır.

1- RUSYA'NIN İDARİ VE SİYASİ YAPISI

Rusya Federasyonu (Rossiyskaya Federatsiya) Sovyetler Birliğinin dağılmasından sonra 24 Ağustos 1991 tarihinde kurulmuştur. Yönetim şekli federal cumhuriyettir. 7 milyon kilometrekare yüzölçümü ile dünyanın en geniş devletidir. Nüfusu 2017 yılı itibariyle 146.800.000 kişidir. Nüfusun yaklaşık dörtte üçü şehirlerde; dörtte biri ise kırsalda yaşamaktadır. Nüfus sayısı ve şehir-kırsal dağılımı uzun yıllar önemli değişim göstermemektedir (GKS, 2018). Ülkede 160'dan fazla etnik grup yaşamaktadır. Resmi dili Rusça ve başkenti Moskova'dır (Erdem, 2017:186) .

SSCB'de uygulanmaya çalışılan komünizmi, Marksist söylemli bir resmi ideoloji, siyasal sistemin Komünist Parti tarafından baskı altına alındığı, ekonominin merkezi planlamayla yürütüldüğü ve özel mülkiyetin bulunmadığı, fikir ve ifade özgürlüğünün kısıtlandığı, basının devlet tekelinde olduğu, kuvvetler

ayrılığının ve yargı bağımsızlığının sınırlandığı bir sistem olarak özetlemek mümkündür. Aynı şekilde Devlet ve Parti, vatandaşların en gündelik yaşam detaylarına kadar müdahale etmiştir.

SSCB'de yaşamın tüm boyutlarına Komünist Parti hakim olmuş; devlet organlarının faaliyet ve kararlarına fiilen yön vermiştir. SSCB kağıt üzerinde her biri bağımsız, ayrı bir devlet başkanı, hükümet, yargı ve yasama organlarına sahip 15 Cumhuriyetten oluşmaktaydı. Ancak fiiliyatta bağımsız ve egemen değillerdi. Cumhuriyetlerin hepsinde asıl güç yerel Komünist Parti teşkilatında toplanmış, Parti'de ise Rus unsurunun egemen olduğu katı bir merkeziyetçilik hüküm sürmüştür. Cumhuriyetlerde idare ve güç, fiiliyatta Moskova'daki Parti merkezinden emir alan yerel Komünist Parti'nin ve yine merkezin direktiflerine göre hareket eden ve etkin mevkilerinde genellikle Rusların bulunduğu KGB[1], polis teşkilatı ve diğer güvenlik makamlarının elinde olmuştur (Baharçiçek ve Ağır: 2016: 13)

2. RUSYA FEDERASYONU İÇ GÜVENLİK YAPISI

2010 yılında çıkan "Güvenlik Yasası", eski Sovyet tarzı militsia anlayışının terk edilmesi ve liberal demokrasi tercihine uygun düzenlemeler getirmektedir. "Güvenlik Yasası"nın 2.maddesine göre Rusya güvenlik sisteminin unsurları yasama, yürütme ve yargı makamları, tüm idari kurumlar, dernekler, yasalara göre güvenliğin sağlanmasında yer alan kişiler ve güvenlik alanında ilişkileri düzenleyen mevzuat tarafından oluşmaktadır (Zakon, 2010).

2.1. Devlet Başkanı

Rusya'da baş güvenlik sorumlusu Devlet Başkanıdır. Başkan, Güvenlik Konseyine başkanlık eder, toplumun güvenliği için kararlar alır ve talimatlar verir ve güvenlik yetkililerinin faaliyetlerini denetler, koordine eder. Rusya Güvenlik Konseyi, Devlet Başkanının güvenliğe yönelik kararların hazırlanmasından sorumludur.

2.1.1. Ulusal Muhafızlar (RosGvard)

Ulusal Muhafızlar Devlet Başkanına bağlı jandarma işlevini yerine getiren, geniş ölçekli isyanlarda ve iç silahlı çatışmalarda polis teşkilatını destekleyen kolluk birimidir. Aynı zamanda önemli yapıların (nükleer santraller vb) korumasını da sağlar. Kamu düzeninin korunmasına ve kamu güvenliğinin sağlanmasına katkı

[1] KGB, (Komitet Gosudartsvennoy Bezopasnosti) Devlet Güvenlik Komitesidir. Günümüzde yerini FSB'ye -Federal Güvenlik Hizmetleri- (Federalnaya Slujba Bezopastnosti) bırakmıştır.

sağlamak, önemli kamusal tesislerin, ulaşım ve haberleşme tesislerinin korunması, terör ve aşırılıkla mücadele, olağanüstü hal ve terörle mücadelede, kamusal düzeni sağlamaya katkıda bulunmak, devlet sınırlarının korunmasında FSB'ye destek sağlamak diğer görevleri arasındadır (Rosgvard, 2018).

2.1.2. Federal Koruma Servisi- FSO (Federalnaya Slujba Ohrahi Rosskii)

Federal Koruma Servisi, Devlet Başkanı da dahil olmakla birlikte üst düzey devlet görevlilerini ve bazı kamu binalarını korumakla görevli ve hükümete bağlı bir kolluk teşkilatıdır. Teşkilat, 1990 yılına kadar faaliyet gösteren Sovyet Dönemi KGB'sinin 9. Dairesinin yerine kurulmuştur (FSO, 2018).

2.1.3. Devlet Başkanı Güvenlik Servisi

Devlet Başkanının kişisel korunmasına hizmet eden bu örgütlenme devlet hiyerarşisi içinde resmi bir birim değil, FSO'nun (Federal Koruma Servisi) bünyesinde yer alan ve kişisel yakın koruma sağlayan personelden oluşan bir birimdir. Bu birim de FSO gibi KGB'nin 9. Dairesinden devralınmıştır. Birim, Başkan'ın yakın korunması hizmetini sağlar. Ayrıca Birim içinde yer alan Psikolojik Güvenlik Departmanı da Başkanın hayatına yönelik güvenlik tehditler ile ilgili toplanan bilgilerin analizini yapar (Agentura, 2018).

2.2. Savunma Bakanlığı

Savunma Bakanlığı, ülke savunması işlevini icra eden Rus Silahlı Kuvvetleri ve diğer birimlerden oluşur. Bakanlığın yönetimi, Savunma Bakanının başkanlık ettiği bakan yardımcıları, Bakanlığın üst düzey ana bölümlerin yöneticileri ve askeri birliklerin komutanlarından oluşan bir kurul şeklinde yönetilir.

Esas faaliyet alanı ülke savunması olmakla birlikte bünyesinde Askeri Polis (Voennoi Politsii) teşkilatını barındırmaktadır. Askeri alanda kolluk hizmetleri askeri polis tarafından yerine getirilmektedir.

Askeri polisin görevleri şunlardır:

-Silahlı Kuvvetlerde hukuk, düzen ve askeri disiplinin güçlendirilmesini sağlamak,

-Silahlı Kuvvetlerde trafik güvenliğini sağlamak, bu alandaki özel kontrol, denetim ve ruhsatlandırma işlerini yapmak,

-Asker ve yol güvenliğini sağlamak. Askeri birimlerin hareketlerini, araçların yollarda güvenli seyrini ve bakımını sağlamak ve koordine etmek.

-Acil durum, askeri saldırı veya doğrudan saldırı tehdidi durumlarında ve savaş zamanlarında askeri birimlerin ulaşım ve intikallerini koordine etmek (MİL, 2018).

2.3. Sivil Savunma, Acil Durumlar ve Doğal Felaketlerle Mücadele Bakanlığı (EMERKOM)

Acil Durumlar Bakanlığı, sivil savunmanın düzenlenmesi ve doğal afet ve yangından korunma görevlerini yerine getirmektedir. Bakanlık 1994 yılında kurulmuştur. Sovyetler Birliği'nde daha önceleri de acil durumlar ve afetler için farklı örgütlenmeler olsa da günümüz anlamında ilk merkezi yapılanma 1988 yılı Ermenistan Depremi ve 1990 yılındaki Çernobil nükleer santral felaketlerinden sonra gerçekleşmiştir. 1990 yılında Yüksek Konsey Başkanlığı, "Rusya Kurtarma Birlikleri"ni (Rossiiskii Korpus Spasatelei) kurmuştur. 1991 yılında ise İçişleri Bakanlığı bünyesinde Sivil Savunma, Olağanüstü Durumlar ve Doğal Afetlerle Mücadele Komitesi kurulmuştur. 1994 yılında Komite bakanlığa dönüştürülmüştür. 2002 yılında Rus Devlet İtfaiye Teşkilatı 278.000 itfaiyeci personeliyle birlikte İçişleri Bakanlığı bünyesine devredilmiştir (MCHS, 2018).

2.4. Federal Gümrük İdaresi (FTS. Federalnaya Tamojennaya Slujba)

Rusya Gümrük İdaresi 1865 yılında Maliye Bakanlığına bağlı Gümrük Departmanı olarak kurulmuştur. 1917'de Sovyet Gümrük İdaresi, Ticaret ve Sanayi Halk Komiserliği'nin (MKTP) bir parçası olarak faaliyet göstermiştir. 1991 yılında Sovyet Gümrükleri Ekonomik Gelişme Bakanlığı altında, Devlet Gümrükleri Komitesine dönüşmüş; 2006 yılında ise bugünkü yapısına kavuşmuştur (Customs,2018).

2.5. Federal Güvenlik İdaresi FSB (Federalnaya Slujba Bezopasnosti)

FSB, Rusya'da asli güvenlik teşkilatıdır ve 1991 -1995 yılları arasında kısa bir dönem var olan "Federal Karşı İstihbarat Teşkilatı"nın FSB adı altında örgütlenmesiyle, Sovyet dönemi KGB'nin yerini almıştır. Sovyet Dönemindeki öncülleri 1917 yılında kurulan ÇEKA, 1922 yılında kurulan GPU (1923'de OGPU), 1934 yılında NKVD (İçişleri Halk Komiserliği) bünyesine alınması, 1946 yılında İçişlerinden ayrılan Devlet Güvenlik Bakanlığı (MGB) teşkilatının, 1953 yılında tekrar İçişleri Bakanlığıyla birleşmesinden sonra 1954 yılında kurulan KGB, Sovyetler dağılıncaya kadar sürdü. (FSB, 2018). Bu derece sık değişikliğe uğramasının altında yatan neden, siyasi elitlerin güç mücadelesi ve bu teşkilatın ise dönemin en önemli iktidar denetim aracı olmasından kaynaklanmaktadır.

FSB, Devlet Başkanlığına bağlıdır. Denetimi ve FSB Başkanının atanması ve görevden alınmasında Devlet Başkanı yetkilidir. FSB'nin kuruluş yasasında, faaliyet ve yetkilerin kullanımında hukuk devleti, hümanist değerler ve temel hak ve özgürlüklere uyulması gibi konulara tekraren vurgular yapılmış ve Anayasa ve yasalarca belirtilen durumlar dışında "kişi" veya "vatandaş"ın hak ve özgürlüklerinin kısıtlanamayacağı hükme bağlanmıştır. Kurum tarafından hak ve özgürlükleri kısıtlandığını düşünen kişiler FSB, Savcılık ve mahkemelere başvurabilirler; maddi ve manevi zararlarının tazminini isteyebilirler (Zakon, 1995). Üstelik FSB personelinin davranışları ve işlemlerinden zarar görenlerin maddi ve manevi zararlarının karşılanmasını Yasa, FSB veya Mahkemelere "yükümlülük" olarak yüklemiştir (Md.6). Yasada bu ifadelerin yer almasını, sadece şekli olarak değerlendirmek çok isabeti bir değerlendirme olmaz. Daha çok Sovyet dönemi kolluk teşkilatının negatif anlayışından kurtulma isteği şeklinde yorumlamak daha gerçekçi olacaktır. Özellikle son yıllarda FSB tarafından haksızlığa uğradığı şikayetiyle FSB üst makamları ve yargı organlarına başvuran kişilerin lehine sonuçlanan pek çok idari ve yargı kararına rastlanmaktadır.

FSB'nin temel görevleri iç güvenliği sağlamak, istihbarat, karşı istihbarat, organize suçlar, terör ve uyuşturucu kaçakçılığı ile mücadele, sınır güvenliği ve bilgi güvenliğinin sağlanmasından oluşmaktadır.

Yabancı İstihbarat Servisi Ülke dışında istihbarat faaliyetlerini yürütür. Daha önce KGB bünyesinde yer alan birim, Sovyetler dağılınca iç istihbarat faaliyetleri FSB'ye bırakılarak, dış istihbarat faaliyetleriyle yetkilendirilerek Devlet Başkanına bağlı olarak örgütlenmiştir.

FSB'nin Sınır Hizmetleri Birimi PSFSB (Pograniçnaya Slujba Federalnoi Slujbi Bezopasnosti) Sınır Birlikleri ya da Sınır Muhafızları olarak da adlandırılan Sınır Hizmetleri, FSB' bünyesinde bir alt birim olarak düzenlenmiştir. Sınır birlikleri, sahil koruma birlikleri de dahil olmak üzere 170.000 aktif personelden oluşmaktadır.

Sınır Muhafızları, devlet sınırlarının korunması, sınırlardan insan, mal, araç, hayvan kargo geçişini kontrol etmek, sınırlarda gerçekleşen ticari, ekonomik ve diğer faaliyetleri denetlemek ve kural ihlallerini önlemekle görevlidir. Sınır Muhafızları, sınır ihlallerini, yasadışı insan, mal, hayvan araç vs. geçişlerini önlemek ve bastırmak için operasyonel arama, istihbarat, bilgi toplama ve diğer tedbirleri alır. Sınır ihlallerinin aktifleştiği dönemlerde diğer birimlerle birlikte özel

sınır operasyonlarını hazırlar ve yürütür. Komşu ülkelerin sınır birimleriyle ortak operasyonlar yürütür (PS, 2018). Ancak "devlet sınırı" kavramı karasal sınırlar, deniz, bölgesel deniz, su altı, münhasır ekonomik bölgeler ve kıta sahanlıklarını da kapsadığı için, birimin faaliyet alanı oldukça geniş ve karmaşıktır.

2.6. Adalet Bakanlığı–MİNYUST (Ministerstvo Yustitsii)

Rusya Adalet Bakanlığı ilk olarak 1802 yılında kuruldu. Dönemin adalet bakanı aynı zamanda Rusya İmparatorluğunun Başsavcısı unvanına da sahipti. İlk dönemlerinde adalet bakanlıkları mahkemelerin ve savcılığın faaliyetlerinin yönetilmesinin yanı sıra, yasa yapma görevine de sahip olmuştur. Sovyetler Birliği kurulduğunda bakanlık yerine oluşturulan Adalet Hak Komiserliği'ne Başsavcılık ve Yüksek Mahkeme doğrudan bağlanmıştır (Minjust, 2018).

1936 yılında Başsavcılık makamı bağımsız kılınmıştır. 1957 yılında ceza hukukunda ilk defa olarak "suçsuzluk karinesi" nosyonu kabul edilmiştir. 2004 yılında yayınlanan Başkanlık kararında, Rusya'da insan hakları ve medeni hak ve özgürlüklerin korunmasına yönelik faaliyetleri iyileştirmek ve hukuk devletinin gelişmesini sağlamak Adalet Bakanlığının görevi olarak tanımlanmıştır. Bunlardan başka, Bakanlık, uluslararası örgütlerin ve yabancı kar amacı gütmeyen örgütlerin, siyasi partilerin, dini örgütlerin ve derneklerin kaydını tutar ve bunlar hakkında bilgi sağlar, noterlik faaliyetlerini düzenler, medeni hal değişikliklerinin kaydını tutar, apostilelerin onayını sağlar, yozlaşma ile mücadele eder (Minjust, 2019).

Federal Cezaevleri İdaresi (FSIN) Cezaların infazı, tutuklu veya hükümlülerin cezai kontrol ve denetim alanında kolluk işlerini yerine getirir. Gözaltındaki sanıkların korunması, şartlı tahliye edilen mahkumların ve hükümlülerin davranışlarını denetleme faaliyetlerini de yürütür. Tutuklu ve hükümlülerin hak ve özgürlüklerini ve yasal menfaatlerini temin eder. Hükümlülere sosyal uyum desteği sağlar (Minjust, 2018).

Federal İcra Daireleri Adalet Bakanlığı bünyesinde yer almaktadır. Bazı adli işlemlerin yanında kolluk görev ve işlevlerini de yerine getirmektedir (Minjust, 2018).

2.7. İçişleri Bakanlığı- MVD (MinisterstvoVnutrennih Del)

Rusya İçişleri Bakanlığı (Ministerstvo Vnutrennih Del) yönetiminde çoğu sahada doğrudan vatandaşlarla ilişkide bulunan bir milyondan fazla personele sahip ülke çapında kolluk teşkilatını yönetmektedir. İçişleri Bakanlığı, ulusal, federe bölge ve

ilçelerde benzer şekilde yapılanmış, uzmanlaşmış alt birimlerden oluşan hiyerarşik bir örgütlenme şeklindedir. Bu alt birimlerin her biri, trafik, suç araştırma, adi suçlar, yolsuzluk ve aşırılıkla mücadele gibi spesifik kolluk faaliyetlerini icra etmektedir. Rusya genelinde her birinde 100-150 personel bulunan yaklaşık 2000 yerel birim, yaklaşık 50.000 ile 100.000 nüfusa hizmet vermektedir (McCarthy, 2014: 5).

Rus polisinin davranışları genel olarak iki önemli kurumsal karakteristik tarafından belirlenir. İlki, katı hiyerarşik itaattir. Rus polisi herhangi bir yerel, bölgesel veya ulusal hükümet memuruna karşı veya halka karşı sorumlu değildir. Bütün sorumluluğu Bakanlık içinde ve dikeydir. Polis bağlı olduğu birimin hiyerarşik olarak federal düzeye kadar üstünde bulunan her kademesine karşı sorumludur. Örneğin Sverdslovsk bölgesinde yer alan Ekaterinburg şehrindeki bir trafik polisi, kendi üzerindeki Sverdslovsk bölgesi polislerine karşı sorumludur; ancak aynı zamanda Ekaterinburg şehrindeki trafik polis amirine karşı da sorumludur. Sorumluluğu, Ekaterinburg şehrindeki, Sverdslovsk bölgesindeki ve Rusya Federasyonundaki federal düzeydeki amirlerinin tümüne karşı geçerlidir. Bu durum bazen bilgi verme yükümlülüğünde tekrarlanmalara yol açmaktadır. Aynı zamanda farklı hiyerarşi hatlarından gelen farklı talimatların nasıl değerlendirileceği konusunda da karışıklığa neden olabilmektedir. Katı hiyerarşik yapı, polis memurlarının ek ödenek veya tazminat almalarına karar verme yetkisinin amirlerde olmasına imkân sağlamıştır. Polis memurları ek ödenek ve tazminatları, kıdemlerine, rütbelerine ve geçim maliyetlerinin yüksek olduğu bölgelerde çalışmalarına göre almaktadır. Üst düzey amirler ise ek olarak çözülen suç sayısı ve işini iyi yapma kriterlerine göre de ödül verme yetkisine sahiptir. Amirini memnun edemeyenlerin ödül ve ek tazminat almaktan mahrum kalma riski söz konusu olmaktadır (age.7).

Polislerin performans değerlendirmesinde, kaydedilen suç sayısı, çözüme kavuşan suç sayısı vb. gibi istatistiksel veriler kullanılması da (paloçnaya sistema) polisin davranışlarını etkileyen bir diğer olumsuz etkendir. Bu sistemde üç ana kriter belirlenmiştir. Bunlardan ilki çözüme kavuşan vaka sayısıdır. Vakanın çözüme kavuşması, zanlının tanımlanması ve suçlanması ile gerçekleşir. İkinci kriter de vakaların kriminal süreç mevzuatınca belirlenen zaman içinde araştırılıp araştırılmadığıdır. Burada kural, suçun gerçekleşip gerçekleşmediğinin on gün içinde belirlenmesine yönelik araştırmadır. Ancak vakanın karmaşıklığı veya ne gibi soruların cevaplanması gerektiği gibi unsurlar dikkate alınmaz. Üçüncü kriter

ise vakaların ve faaliyetlerinin sayılarının geçen yıllarla karşılaştırılmasıdır. Bu durum ise polis memurlarını vaka ve faaliyet sayıları konusunda daimi strese sokmaktadır. Paloçnaya sistemi aynı zamanda aşırı bürokratik işlem ve kırtasiyeciliğe sebep olmaktadır. Polis memurları vaka soruşturma işlemlerinin her aşamasında bilgisayara girmek ve her aşamayı kayıt etmek zorundadır. Moskova polis teşkilatında yapılan bir çalışmada polislerin mesailerinin %80'ini evrak işleriyle geçirdiği gözlenmiştir (McCarthy, 2014: 6).

Rusya İçişleri Bakanlığının Teşkilat Yapısı şu şekildedir (MVD, 2019).

İçişleri Bakanlığı Hizmet Birimleri

- **Karayolları Genel Müdürlüğü**
- **Kamu Düzeninin Sağlanması ve Rusya Federasyonu'nun Yürütme Organları ile Etkileşim Koordinasyonu Müdürlüğü** Kamusal düzenin ve güvenliğinin sağlanması, suçun önlenmesi, vb. faaliyetleri yürütür. Kolluk teşkilatının ana unsurunu oluşturur.
- **Aşırılıkla Mücadele Müdürlüğü**
- **Teşkilat İçi Güvenlik Müdürlüğü** Polis teşkilat mensupları, çalışanların güvenliğini sağlama ve kurum içi yozlaşma ile mücadele.
- **Ulaştırma Genel Müdürlüğü** Kara, hava, deniz yolları nakliye ve ulaşım güvenliğinin sağlanması ve suçun önlenmesi.
- **Ceza Soruşturma Genel Müdürlüğü** Suçların tespiti, önlenmesi, bastırılması ve açığa çıkarılması faaliyetlerini yürütülmesi.
- **Ekonomik Güvenlik ve Yolsuzlukla Mücadele Müdürlüğü**
- **Göç Müdürlüğü** Ülke içi ve ülke dışı pasaportların verilmesi, denetimi, yabancı ülke vatandaşlarının ülkeye giriş, ikamet, çalışma ve davet izinlerinin denetimi.
- **Uyuşturucu Kontrol Genel Müdürlüğü** Her türlü uyuşturucu psikotropik maddenin denetimi, uyuşturucu ticaretinin önlenmesi.
- **Soruşturma Dairesi** Ön soruşturma, soruşturma, ceza soruşturması gibi faaliyetler.
- **Personel Dairesi**: İnsan kaynakları yönetimi, hizmet içi eğitim, yabancı ülke personeline eğitim verme, personel organizasyonu vb. faaliyetler.
- **Arşiv ve Dokümantasyon Dairesi**

- **Bilgi Teknolojileri, İletişim ve Bilgi Koruma Dairesi**

- **Mali ve Ekonomik Politika ve Sosyal Güvenlik Dairesi** Kurumun bütçesinin yönetimi, çalışma ve emeklilik ödemlerinin yönetimi vb.

- **Hukuk Dairesi** Kamu düzeninin korunması, suçla mücadele gibi konularda analiz, çözüm ve stratejiler geliştirme faaliyetleri.

- "**K**[2]**" Dairesi (Özel Teknik Önlemler Dairesi)** K Dairesi, bilgi iletişim, internet ve benzeri teknolojik ortamlarda siber suçlarla mücadele eder ve internet üzerindeki suçların önlenmesi, küresel internet ağındaki vatandaşların güvenlik ve hukuki korunmasını ve iyileştirmeyi amaçlar. Bu amaç doğrultusunda şu önlem ve faaliyetlerde bulunur: Bilgisayar suçlarını önlemek amacıyla yetkisiz erişimin tespiti ve bastırılması, elektronik ödeme sistemlerinin istismar edilmesine karşı önlemler, internet yoluyla yasal olmayan pornografik materyallerin dağıtımının engellenmesi, hücresel telefon ağlarının yasadışı kullanımı ve suç amaçlı kullanımının belirlenmesi ve bastırılması, uydu ve kablolu televizyon ticari ağlarına izinsiz erişim girişimlerinin bastırılması, bilgi iletişim ortamlarında yasadışı ticaretle mücadele, telif hakkı ve ilgili haklarının ihlalinin önlenmesi, bilgi teknolojileri alanında uluslararası suçlarla mücadele (MVD, 2018).

- **Devlet Korumasına Tabii Kişilerin Güvenliği Dairesi** Mağdur, tanık, hakimler, savcılar, müfettişler, kolluk ve düzenleyici otoritelerin korunması, koruma önlemlerinin geliştirilmesi.

- **Sivil Toplum ve Medya ile İlişkiler Dairesi** Bakanlığın faaliyetlerine bilgi desteğinin sağlanması, medya, bilgi ve iletişim sağları vasıtasıyla vatandaşları bilgilendirmek, Bakanlık faaliyetleri hakkında medya haberlerini izlemek ve analiz yapmak, Bakanlığın, medya, hükümet organları, kamu kurumları ile etkileşimini sağlamak, Bakanlığın basın hizmetleri, bilgi birimleri ve halkla ilişkiler faaliyetlerine kurumsal ve metodolojik destek sağlanması.

- **Büyük Uluslararası ve Kitlesel Spor Etkinliklerinin Güvenliği Dairesi** 2008 yılında kurulmuştur. Rus polis teşkilatının modernleşmesinde önemli katkılar sağlayan ancak yeterli önemi kazanmamış olan "Büyük

[2] Киберпреступность: Siber suçlar

Uluslararası Spor Etkinlikleri ve Kitle Güvenliği Dairesi, 2014 Sochi kış olimpiyatları sırasında kamu güvenliği ve kamu düzeninin sağlanması için 2008 yılında kurulmuştur. Ancak 2011 yılında Asya-Pasifik Ekonomik İşbirliği Forumu ve 2013 Vladivostok ve Kazan'da Dünya Üniversitelerarası Yaz Olimpiyatlarında görev almış; en son olarak 2018 Rusya Dünya Futbol Şampiyonasında da görev almıştır.

Birimin Rus Polis Teşkilatının Modernleşmesinde kritik rol oynaması, Rus hükümetinin geliştirdiği kamu politikasında yatmaktadır. Uluslararası organizasyonlarda kamu idaresinin kapasitesinin de aynı düzeyde yüksek olması beklenir ancak polis teşkilatında özellikle 2010'lardan sonra yapılan genel ve tümdengelimci reformlar görece başarı sağlamıştır. Öte yandan belirli bir uluslararası kitle organizasyonu için somut kriterler ortaya koymak ve ilgili kamu idarelerini bu somut kriter düzeylerine ulaşmak için motive etmek daha başarılı sonuç vermiştir. 2014 Sochi kış olimpiyatları örneğinde, Sochi şehrindeki polis, gümrük, havaalanı, trafik vb. kurumların örgütsel yapıları, işleyişleri, kapasiteleri, halkla ilişkileri, eğitimleri ve diğer ilgili kurumlarla koordinasyonlarında önemli gelişmeler kaydedilmiştir. Aynı durum 2018 Dünya Futbol Şampiyonası organizasyonunda da gözlenmektedir. Somut bir olay ve performans hedefleri belirlendikten sonra, hükümetin idari kurumları bu yönde motive etmesi daha kolay olmuş; bu hedeflere bir kez ulaşıldıktan sonra da geri dönmemesi ve daha da ileri götürülmesi için çalışmalar devam etmiştir. Kontrol edilecek küçük bir alan veya organizasyon ölçeğinde yapılan seferberlik niteliğinde reform çabalarında başarı elde etmek daha kolay olmakta; elde edilen kazanımların da ülke çapında İçişleri teşkilatına uyarlanması ve benimsenmesi daha az direnç ve zorlukla karşılaşmaktadır.

- **Personel Müdürlüğü** İçişleri Bakanlığının personel temini, geliştirilmesi, personel politikalarının oluşturulması faaliyetleri.

- **Kontrol ve Revizyon Ofisi** İç mali denetim faaliyetleri.

- **Soruşturma Dairesi** Birim, ön soruşturma, suçların tespiti, ifşası ve soruşturulması, cezai takibat faaliyetlerini düzenler. Suçun önlenmesi, tespiti, açığa çıkarılması faaliyetlerini yürütür, bu faaliyetler için gerekli organizasyonu sağlar, ilgili birimler arasında işbirliği düzenler. İçişleri

Bakanlığının tüm birimlerinin ve kolluk kuvvetlerinin kullanımlarının, acil durumlarda öncelikle alanların belirlenmesi ve değerlendirilmesi faaliyetlerini yürütür. Acil durumlarda ve sıkıyönetim hallerinde operasyonel ortamlardaki değişiklerin yanı sıra kolluk güçlerinin hazırlanması, operasyonun hızlı tepki vermesinin sağlanması, nükleer maddelerin yasadışı ticaretiyle mücadele, kapalı bölgelerdeki tesislerin korunması için gerekli birimlerle işbirliği yapma gibi görevleri vardır.

- **İnterpol Merkez Dairesi**
- **Yönetim Akademisi** İçişleri Bakanlığına bağlı olan Yönetim Akademisi, Bakanlığın faaliyet alanları kapsamında yüksek öğretim, mesleki eğitim ve ek mesleki eğitim programları yoluyla eğitim hizmetleri verir ve bilimsel faaliyetlerde bulunur.
- **Adli Tıp Merkezi**
- **Profesyonel Gelişim Enstitüsü** Üst düzey personel yetiştirmek üzere lisansüstü programlar yürütür.
- **Araştırma Enstitüsü** Operatif soruşturma, ceza yargılaması, ceza hukuku, idare hukuku ve kriminoloji alanında bilimsel faaliyetler yürütür.
- **İnformasyon ve Analiz Merkezi** Parmak izi, operasyonel araştırma, istatistik, arşiv, bilimsel ve teknik bilgileri kolluk kuvvetlerine ve diğer kamu otoritelerine temin eder.
- **Taşımacılık ve Malzeme Hizmetleri Merkezi** İçişleri Bakanlığının bina, konut, lojman, giysi, araç gereç, motorlu taşıtların temini, yönetimi ve bakımı hizmetlerini sunar.
- **Özel Taşımacılık Merkezi** Kolluk kuvvetlerinin ve askeri taşıma işlerinin organizasyonunu gerçekleştirir.
- **Özel ekipmanlar** Özel ekipmanlar ve cihazlar üretme amaçlı bir araştırma enstitüsüdür.
- **Köpek Eğitim Merkezi** Kolluk güçlerinin kullandığı hizmet köpeklerinin yetiştirilmesi faaliyetini yürütür.
- **Metroloji Merkezi** İçişleri Bakanlığı bünyesindeki ölçümlerde standardizasyonu sağlamak, yangın güvenlik alarmlarının sertifikasyonunu sağlamak.
- **Trafik Güvenliği Merkezi**

3. 1991 – 2000 ARASI DÖNEM

Sovyetler Birliği dağıldıktan sonra Rusya Cumhuriyeti 1991 yılında kuruldu. 1993 yılında kabul edilen Anayasa ile devlet "Rusya Federasyonu Cumhuriyeti" adını aldı. Ukrayna, Belarus, Gürcistan, Azerbaycan, Özbekistan, Kazakistan, Kırgızistan, Ermenistan gibi Sovyet Cumhuriyetleri bağımsızlıklarını elde etti. Ülkenin siyasi rejimi değişti. Komünizmden liberal demokrasiye doğru hızlı bir değişim yaşandı (ДАХИН, 2018). Bu çok boyutlu kökten değişim, tüm kamu yönetimine, özelde de iç güvenlik yapılanmasına da yansıdı.

Ancak 1990'lı yıllar Rusya için çalkantılı bir dönemin başlangıcıydı. İç güvenlik teşkilatlanması pek çok sorunla karşı karşıya kaldı ve etkinliğini önemi ölçüde yitirdi. Kamusal düzenin bozulması suç istatistiklerine de yansıdı. 1993 yılında 513.910 olan ağır suç sayısı, 1995 yılında üç mislinden fazla artarak 1.633.367'ye yükseldi. 1991 ile 1996 yılları arasında 550.000 ölümle sonuçlanan suç işlendi. Sadece 1992 yılında 213.590 kişi işlenen suçlar sebebiyle hayatını kaybetti (Semukhino ve Reynolds, 2012: 95).

1990'lı yıllarda İçişleri Bakanlığı bünyesinde yapılan önemli düzenlemeler şu alanlarda oldu: adli kolluk ve kamu düzeni polisinin ayrılması, merkezi federal bütçeli ve yerel bütçeli polis birimlerinin ayrı teşkilatlanması, iç soruşturma departmanının kurulması, pasaport hizmetlerinin gözden geçirilip isminin değiştirilmesi (Гонюхов ve Горобцов, 2002: 86).

Ancak yapılan düzenleme ve reform çabaları düzelme sağlamaktan uzaktı. Polis hizmetlerinden memnuniyet düzeyi %3 ila %25 arasında oldukça düşük düzeyde kaldı. Kolluğun güç istismarı ve yozlaşması, toplumda polis korkusunu arttırmıştı. Bu durumun bazı sebepleri şunlardı:

1- Bu dönemde İçişleri Bakanlığının yaptığı reform uygulamalarının polis sisteminde öngörülen değişikliği yapamadı. Kolluk teşkilatlarının halka kapalı, hiyerarşik, aşırı bürokratik ve askeri niteliklerinin değiştirilemedi.

2- Yeni sistem etkin bir iç denetim mekanizması getirilemedi. Sovyetler zamanında polis, Parti denetimi altında idi. Yeltsin, İçişleri Bakanlığı üzerindeki Parti denetimini kaldırdığında siyasileşmenin de biteceğini düşünmüştü. Ancak teşkilat bakan vasıtasıyla siyasete bağlı kaldı.

3- 1990'ların başlarında yasal boşluklar ve kaos, polis için oldukça sorunlu bir dönem yaratmıştı. Sovyet yasaları, idari komuta ekonomisi için yapıldıklarından, yeni dönemde işlevsizdi. Yeni liberal ekonomiye zemin

sağlayacak çok az yasal düzenleme yapılabilmişti. Bazı zararlı davranışların yasal dayanağı olmadığı için soruşturulması mümkün olmuyordu. Mevzuatta çok fazla gri alanlar oluşmuştu.

4- Ceza yargısının demokratikleşmesi çabalarında sanıklara ilave haklar sağlandı. Sanıklar avukata danışma ve tutukluluklarına mahkemede itiraz edebilme hakkı kazandı. Bazı davalarda jüri sistemi getirildi. Soruşturmacı kolluk, sanıklara hak tanıyan yasalara uyum sağlayamadığından çoğu zaman tereddüte düşüyor ve suç takibini gereğince yapmakta çekince yaşıyordu.

5- Maaş ödemelerinin devamlı olarak gecikmesi, dosya yüklerinin gittikçe artması, güvenlik sorunlarının artması gibi nedenlerin yarattığı stres, personelde moral bozukluğu yaratıyor ve suç çözümleme istatistiklerinde dramatik düşüşlere yol açıyordu. Deneyimli personel daha yüksek ücret ve daha düşük stresli özel sektöre geçiyorken yeni personel eğitim ve deneyim bakımından zayıftı.

6- 1980'ler boyunca gelişen organize suç hükümete ve kolluk teşkilatına sızmaya başlamıştı.

Bütün bu unsurlar, kolluk teşkilatında demokratik yasal reformların başarısız olmasına yol açmaktaydı (Semukhino ve Reynolds, 2012: 98).

4. PUTİN DÖNEMİ, 2000 VE SONRASI[3]

Yeltsin'in görevden ayrılıp yerine Vladimir Putin'i önermesi ile günümüze kadar devam eden Putin dönemi 2000 yılında başladı. 1991 yılında Rusya Cumhuriyetinin ilk başkanı olan Yeltsin, 1999 sonuna kadar olan iktidarı süresince Batı tarzı modernleşme tercihiyle ülkede Batılı demokratik bir rejim ve idari teşkilatlanma çabalarına girişmişti. Ancak bu kısa dönemde ülkenin ekonomik, siyasi, sosyal ve kültürel anlamda batılı örneklerine ayak uydurması mümkün olmadı.

Ülkede Batının demokratik yapısı, ekonomisi, idari ve siyasi teşkilatlanması ve işleyişi ile ilgili bilgi ve deneyimi olan yoktu. Total değişimi yapacak olan siyasi liderler Sovyet Dönemi devlet adamlarıydı. Neyi nasıl yapacakları hakkında çok az bilgileri vardı. Ülkede ne sivil toplum kuruluşları ne liberal ekonomi aktörleri ne demokratik siyasi kuruluşları ne batı demokrasileri literatürüne vakıf üniversite ve bilim adamları vardı. Batılı sivil ve resmi danışmanlık kuruluşlarının desteği çok

[3] 2000'den sonrasının Putin dönemi olarak adlandırılması, literatürde geniş kabul görmüştür. Rusya Anayasasına göre Devlet Başkanı arda arda iki defa görev yapabilir. Bu kısıt Medvedev ile başbakanlık ve devlet başkanlığının yer değiştirmesiyle aşılmakta ancak devlet yönetiminde Putin'in baskın rolü devam etmektedir.

etkili olmadı (Дахин, 2018a: 185). Üstelik ülkede kıtlık, sefalet, ayrılıkçı hareketlerin yol açtığı silahlı çatışmalar hüküm sürüyordu.

Kötü de olsa eski sistem yıkılmış ama yerine yeni bir sistem ve düzen kurulamamıştı. En kötü düzenin, düzensizlikten ve kaostan daha iyi olduğunu kanıtlarcasına yoksulluk, suç ve sefalet olağanüstü derecede arttı. Kamu kurumları işlevlerini yerine getiremez hale geldi. Parçalanma tehlikesi yaratan iç etnik çatışmalar baş gösterdi. Asayiş ve güvenlik kalmadı. Suç oranları büyük ölçüde arttı.

2000 yılından itibaren Putin'in dönemi başladığında da girişilen reform faaliyetlerinde kısa dönemde başarılar elde edilemedi. Bu dönemde de birbiri ardına reform program ve planları uygulanıyor ama çok az başarı elde ediliyordu. Ayrıca Putin başta Çeçenistan olmak üzere ülkedeki iç savaş sorunlarıyla da baş etmek zorundaydı.

2000'li yıllarda Rus iç güvenlik yapısına yönelik çok sayıda reform teşebbüsü yapılsa da günümüz güvenlik yapısını belirleyen etkili reformlar Putin'den sonra Devlet Başkanı olan Medvedev tarafından gerçekleştirildi. Medvedev, 2009 ve 2011 yılları arasında iç güvenlik teşkilatlanmasına yönelik bir dizi reform gerçekleştirdi ve bu reformlar günümüz Rusya'sının kolluk yapılanmasını şekillendirerek önemli ölçüde başarılı oldu.

2009 yılındaki polis reformları, Rusya'da kamu yönetiminin her kademesinde yozlaşmayı temizlemeye yönelik genel reformun bir kısmını oluşturmuştu. 2009 yılında çıkan "Polis Yasası" kolluk güçlerinin faaliyetlerini düzenlemeyi, İçişleri Bakanlığının meşruluğunu ve etkinliğini geliştirmeyi amaçlamıştı. Ancak bu Yasa, reform yürütücülerinin açık bir vizyonu olmaması, nasıl başarılacağına dair bilgilerinin ve yeterli desteğin sağlanamaması sebebiyle bekleneni veremedi (Cheloukhine, 2017: viii).

2000'li yılların başında yozlaşma Rus kamu yönetimi teşkilatının her tarafına işlemişti ve etkileri toplumda derin bir şekilde hissediliyordu. 2015 Şeffaflık Örgütü İndeksine göre Rusya 176 ülke içinde 119. sıradaydı. Rusya İçişleri Bakanlığı Ekonomik Suçlarla Mücadele Departmanına göre 2008 yılında ortalama rüşvet miktarı 9.000 Ruble, 2009 yılında 23.000 Ruble ve 2012 yılında da 236.000 Ruble /yıl miktarına ulaşmıştı (Cheloukhine, 2017: viv).

Yozlaşmayla mücadelede 2009 yılının ilk altı ayında 4.500'den fazla yolsuzluk davası açıldı; 532 kamu görevlisi ve 700'den fazla kolluk görevlisi tutuklandı. Öte

yandan aynı yıl kolluk maaşları iki mislinden fazla arttırılarak ortalama 300 Amerikan dolarına denk gelecek şekilde yükseltildi. Organize suç örgütleriyle ilişkisi bulunanlar görevden çıkartıldı; personel sayısı %30 azaltıldı. Ulaşılabilen istatistik rakamlarıyla[4] 1994 yılında Ceza Yargılama Sisteminde 1.800.000 olan personel sayısı, 2009 yılında 1.400.000'e düştü.

Medvedev'in yaptığı ikinci önemli reform, 2011 yılında kolluk teşkilatını Militsia'dan Polis'e dönüştürmesidir. Bu reformla kolluk teşkilatının denetimi daha merkezileştirildi, denetim yetkileri bakımından yerel ve belediye yetkileri kaldırıldı ve doğrudan Moskova'ya, İçişleri Bakanlığının yetkisine verildi. Aynı zamanda Cezaevlerinin sorumluluğu İçişleri Bakanlığından alınarak Adalet Bakanlığına, itfaiye teşkilatı da Acil İşler Bakanlığına devredildi.

2011 yılındaki "İçişleri Bakanlığı Hakkında" Başkanlık Kararı, İçişleri Bakanlığının yeni görevlerini, örgütsel yapısını ve Bakanlığın toplam personel sayısını belirliyordu. Karar, 2014 Sochi Kış Olimpiyatlarının güvenliğine yönelik uluslararası ve kitle spor organizasyonlarına dair yeni birimler de öngörüyordu[5]. Aynı tarihli takip eden Karar'da ise İçişleri Bakanlığının bölgesel teşkilatlanmasına yönelik standartlaşma, taşra teşkilatlanmasında ise oldukça detaylı sorumluluk ve örgütsel yapılanma tanımlamaktaydı. 2011 yılında Militsia'dan polis teşkilatına geçildiğinde her bir personel yozlaşma suçlarına karışıp karışmadığı bakımından incelendi ve Personelin suça karışmadığına dair "temiz sertifikası" aldıktan sonra polis teşkilatına transferi tamamlandı. Polis maaşları tekrar arttırıldı (Semukhina, 2014: 2).

Bu dönemde ortalama maaşlar 1000 Amerikan doları civarına yükseltildi ve maaşlar gecikmeler olmaması için merkezi bütçeden ödenmeye başlandı. Yozlaşmanın ve etkinsizliğin en büyük içsel nedenlerinden olan düşük maaş sorunu böylelikle ortadan kaldırıldı. İçişleri Bakanlığı 2011 yılının Mart ve Ağustos ayları arasında bütün polis memurlarını ayrı ayrı denetledi. Kolluk personelinin %90'ı

[4] 1990'lı yıllar ve 2000'li yılların başında Rusya'da istatistiki bilgiler sağlıklı tutulamamıştır. Yer yer boşluklar vardır ve kayıtlardan elde edilen veriler sağlıklı değildir.

[5] Sochi Kış Olimpiyatları uluslararası nitelikteydi. 2011 Kararları da Olimpiyatlar odağında kolluk hizmetlerinin uluslararası düzeye getirilmesini amaçlamaktaydı. Etkinsizlik, yozlaşma gibi eski hastalıklar, Olimpiyatlar esnasında olmamalıydı. 2014 Olimpiyatları motivasyonu ile ulaşılan polislik standartları, sonrasında büyük ölçüde korundu ve ülkenin diğer bölgelerine de yayıldı. Kolluk faaliyetlerinde elde edilen bir diğer büyük gelişmenin ise 2018 Futbol şampiyonasında gözlemlendiği kamuoyu ve basın tarafından dile getirilmektedir.

(875.000), idari personelin ise %94'ü bu denetimden başarılı çıktı ve görevlerinde kaldılar.

Aynı reform çerçevesinde İçişleri personelinin değerlendirme ve terfi sistemi de geliştirildi. O zamana değin var olan sistem, kayıtlı suç sayısı ile tutuklanan zanlı sayısının oranlanmasına dayanmaktaydı ve bu durum, verileri manipüle etme ve güç istismarına yol açmaktaydı. Kolluk görevlileri performans hedeflerine ulaşmak için çözülmesi zor olan suçları kayıt etmekten kaçınıyorlardı veya suçsuz olan vatandaşlara dahi zorla suç itiraf ettirme yöntemlerine başvuruyorlardı. Performans değerlendirme süreçlerinde bu tür istatistiklerin kullanılması kaldırıldı (Semukhina, 2014: 2).

2011 reform yasalarının hazırlanması esnasında da demokratik ve şeffaf yöntemler izlenmiş olması dikkat çekicidir (Зайцева, 2016: 180). Yasa tasarıları internet vasıtasıyla kamuoyu tartışmalarına ve görüş önerilerine açıldı. İnternet ortamında vatandaşlardan 20.000'in üzerinde yorum, katkı, eleştiri ve değerlendirme sağlandı. Pek çok Rus ve Uluslararası sivil toplum kuruluşu, üniversiteler ve ilgili kamu idareleri çalışmalar düzenledi ve yayınlarda bulundu. Tartışmalar sürecinde vatandaşlar kolluk uzmanları ve medya etkisi fazla olmasa da özgürce polis reformu hakkında eleştiriler yapabildiler (Semukhina, 2014: 3).

2013 yılında Federal Hükümet, yeni bütçe programında 2014-2020 yılları arasında kolluk teşkilatına 255 milyar dolar gibi büyük bir mali kaynak tahsis ettiğini açıkladı. Bu tahsisin hedeflerinin kayıtlı suç sayısının düşürülmesi, suçların çözülme oranlarının arttırılması, kamuoyunda güvenin ve hizmetlerden memnuniyet derecelerinin artması olduğu belirtildi. Kolluk teşkilatında merkezileşme reform hedeflerinden olduğu için ilçe bazında polis birimlerinde azaltılmaya gidildi.

2011-2014 polis reformlarının önemli kazanımlar sağladığı söylenebilir. Rusya'da "kötü polis" imajının ortadan kalktığı kabul görmüş bir değerlendirmedir. Bu dönemde polis teşkilatı hakkındaki tartışmalar gündemden düştü ve sıradanlaştı. Reformların bir diğer başarısı da polis memurları arasında mesleki tatmin düzeyinin artmasıdır. Bir taraftan bazı polis memurları "sertifikalandırma" süreciyle sıkı bir kişisel denetimden geçmekten ve kamuoyu denetiminin artmasından şikayetçi olsalar da, artık terk edilmiş hissetmedikleri ve hükümet tarafından hatırlandıkları ve özlük haklarının eskiye göre çok daha iyi olduğu düşüncesi ağır basmaktadır (Semukhina, 2014:4).

5. 2010 SONRASI DÖNEMDE KOLLUK TEŞKİLATINDA MODERNLEŞME

Sovyetler Birliği sonrası pek çok reform çabaları olmasına rağmen, günümüz modern polis yapılanmasının başlangıcı esasen 2011 Medvedev reformlarına dayanmaktadır. 2011 yılında çıkan "Polis Yasası" eski Çarlık ve Sovyet polis anlayışını değiştirme iradesini somut olarak ortaya koyan bir metindir. 2011 Polis Yasası temel olarak kolluk teşkilatının etkinliğini arttırmak, yozlaşmayı azaltmak ve kamuoyu imajını düzeltmeyi amaçlamıştır.

Polis reformu sürecinde personel sayısında %20 oranında azalmaya gidildi, bütün kolluk teşkilatı "sertifikasyon" sürecinden geçerek, her bir personel suç, yozlaşma ve organize suç örgütleriyle ilişkiler bakımından incelendi, maaş ve diğer maddi imkanları önemli derecede arttırıldı. Örgütsel yapıda dağınıklık giderildi ve teşkilat merkezi yapıya kavuşturuldu.

5.1. Polis Reformunun Ana Unsurları

-İsim Değişikliği: Reform ile Rus kolluk teşkilatının ismi Sovyet dönemi "Militsia" değiştirilmiş; daha evrensel bir kavram olan "Politsiya" (Polis) benimsenmiştir.

-Personel azaltılması ve Ücretlerin arttırılması: kolluk personelinin sayısı %20 azaltılarak 1.280.000'den, 1.100.000'e düşürüldü. Ancak daha sonra "sertifikasyon" süreciyle suça ve yozlaşmaya bulaşmış kolluk görevlileri de görevden çıkarıldı. Polis maaşları süreç içinde 1000 Amerikan dolarına kadar çıkarıldı. Eski sistemde polis birimlerinin basit ve küçük suçlar için yetki alanları bölgesel veya şehir idareleri çapındaydı; yerel bütçelerden finansmanı sağlanıyordu ve daha çok yerel otoritelere karşı sorumluydu.

-Kamuoyu Algısının Düzeltilmesi: Çarlık ve Sovyet dönemi polisinin halk nazarında algısı çok olumlu değildi. Polisle ilişkide bulunmanın kişilere zarar vereceği algısı yerleşmişti. Mağdur olanların dahi polise başvurduklarında ayrıca polisten kötü muamele, fiziki şiddet, rüşvet, suçlunun kayırılması gibi ayrıca zarar görme olasılığı yüksekti. Önceki dönemlerde polis, vatandaşı korumaktan çok, iktidarı ve ideolojiyi koruma görevini ön planda tutuyordu. Reform bu kötü algıyı değiştirmeyi amaçlamıştır. "Polis faaliyetlerini insan hak ve özgürlüklerine saygılı olarak yürütür. Vatandaşların hak ve özgürlüklerini kısıtlayan polis faaliyeti meşru hedefe ulaşınca durum derhal sona erer. Polis memurunun işkence, şiddet ve diğer zulüm ve aşağılayıcı davranışlarda bulunması yasaktır." İfadesi, bu amaca vurgu yapmaktadır. Yasada polisin faaliyet ilkeleri belirtilirken insan haklarına sivil hak ve özgürlüklere riayet ve saygı prensibi eklendi. Polisin görevini yaparken

ayrımcılık yapması da yasaklandı. Cinsiyet, ırk, milliyet, dil, köken, mülkiyet ve resmi statü, din, sabıka vb. gibi niteliklere göre vatandaşlar arasında ayrımcılık yapması yasaklandı (Md.5).

Ayrıca İçişleri Bakanlığı bünyesindeki bilim ve eğitim kuruluşları devamlı olarak halkın polis algısındaki değişimi ölçmeye, bu yolla elde edilen verileri, eksiklik ve zayıflıkları gidermekte kullanmaya başladı. Anket ve araştırma sonuçlar İçişleri Bakanlığının sitesinden düzenli olarak yayınlandı (MVD, 2018).

Polis teşkilatı kamuoyu desteğini geliştirmek amacıyla sivil toplum kuruluşlarıyla da işbirliğine girişti. St. Petersburg'da "Vatandaş Kontrolü" adlı STK'lar, insan hakları düzeyinin gelişimi için polis eğitimi faaliyetlerine katılmaya başladı. Nijni Novgorod şehrinde "Adalet Desteği" adlı sivil toplum kuruluşu, polis merkezlerinde vatandaşların polisle ilişkiye girmeden önce ilk başvuracağı "ilk kontak" masaları oluşturdu. Polis merkezine gelen vatandaşlar, şikâyet, işlem vb. gibi süreçlerde önce bu masalardaki STK uzmanlarıyla görüşüyorlar, hukuki bilgi ve destek alıyorlar, akabinde ya kendileri veya kendileri adına STK mensupları polisle iletişime geçiyordu. Bu şekilde kamuoyunda polise karşı vatandaş güveninin arttırılması planlanmaktaydı (Taylor, 2018:7).

Rusya İçişleri Bakanlığının arşivlerinde suç istatistikleri 2003 yılından itibaren tutulmaya başlanmıştır. Daha önceki zamanlara dair suç kayıtları farklı kaynaklarda bulunabilmekle birlikte güvenilirliği ve karşılaştırılabilirlik açısından sağlıklı bilgi vermekte yetersiz kalmaktadır. İstatistiklerde görüldüğü üzere Rusya'da suç oranları 2006 yılından itibaren istikrarlı bir şekilde düşmektedir. Ayrıca tabloyu daha sağlıklı yorumlayabilmek için suç kayıtlarına etki eden bazı durumsal şartları da göz önünde bulundurmak gereklidir. 2000'li yılların başlarında suç mağduru vatandaşların polise bildirimde bulunmaktan çekindikleri bir vakadır. Vatandaşlar çoğu zaman, hırsızlık, basit saldırı ev hırsızlığı vs. suçlarda polise bildirme konusunda daha isteksizdi. Öte yandan polis de suçları kayda almakta o kadar istekli değildi (Cheloukhine, 2017a: 14). Özellikle 2011'den sonra ard arda yapılan polis reformları hem vatandaşların polisten çekinmesi sorununu gidermiş, hem de polisin suç kaydı yapma isteksizliğinin nedenleri önemli ölçüde giderilmiştir. Polis- halk iletişiminde önemli ilerlemeler sağlanmıştır. Bu durumda 2003 yılı istatistiklerinin gerçek suç sayısını daha düşük gösterdiğini; 2017 yılındaki kayıtlı suç sayısında ise çeşitli nedenlerle bildirilmeyen suç sayısının daha az kaldığını düşünmek mümkündür. Bu unsurlar göz önüne alındığında suç sayısının istatistiklerin gösterdiğinden daha hızlı bir şekilde düştüğünü söylemek mümkündür.

Tablo.2 Rusya'da Yıllara Göre Suç Sayısının Değişimi (MVD, 2018a).

YIL	KAYITLI SUÇ SAYISI[6]
2017	2.058.476
2016	2.160.000
2015	2.388.500
2014	2.166.400
2013	2.206.200
2012	2.302.200
2011	2.404.600
2010	2.387.469
2009	2.944.000
2008	3.209.900
2007	3.582.500
2006	3.855.400
2005	3.554.700
2004	2.893.800
2003	2.756.400

6. KAMUOYUNDA POLİS ALGISI

1990'lar ve 2000'lı yıllar boyunca Rus vatandaşlarının polis algısı oldukça olumsuzdu. 2010 yılına kadar polis hizmetlerinden memnuniyet oranları %50'nin altında seyretmiştir. 1990 ila 2010 yılları arasında Rus vatandaşlarının polise olan güven hissi %11 ila %45 arasında seyretmiştir (Semukhina ve Reynolds, 2012: 165). 1990 yılında yapılan bir araştırmada Rus polisi "kültürsüz, kaba, ilgisiz, yozlaşmış, sahtekâr ve rüşvetçi" olarak tanımlanmıştır (Мазаев, 1997). Ancak araştırmalar, emekli, kırsalda yaşayan ve az eğitimli kişilerin polise güven duygularının daha yüksek olduğunu göstermektedir. Bazı araştırmacılar bu eğilimi, bu kesimdeki insanların daha korumasız kimseler olmaları sebebiyle polise güvenmek zorunda olmaları ile açıklamaktadır. Bu bireyler kendilerini koruyacak başka seçeneklere sahip değildirler. Ancak yine de en zayıf olanları dahil, herhangi bir nüfus grubunun üst düzey memnuniyet sergilediği gözlenmemektedir. Polise güven ve memnuniyet hisleri diğer ülkelerle karşılaştırıldığında dramatik oranda düşüktür. 1992-2002 yılları arasında karşılaştırmalı bir çalışmada Rusya'da polis memnuniyeti %24.7 iken, bu oran Kanada'da %84.6, Amerika'da %83.9,

[6] Kayıtlı suç sayısı, İçişleri makamlarına ulaşan ve suç olarak kaydedilen vaka sayısıdır. Hakkında ceza davası açılan suç sayısı daha azdır. Öte yandan İçişleri makamlarına farklı kanallardan gelen çok sayıda şikayet ayıklanarak suç kaydı yapılmıştır. Örneğin 2006 yılında İçişleri birimlerine çeşitli kanallarla 19.300.000 şikayet ulaşmış; bunların 3.855.400'ü için suç kaydı yapılmış, bu suçlardan 3.262.600'ü için ceza davası açılmıştır. Rusya İçişleri Bakanlığının Suç istatistikleri 2003 yılından itibaren başlamaktadır.

İngiltere'de %70.1 ve Almanya'da %66.7 olmuştur. Bu güvensizliğin sonucu olarak suç mağdurlarının polise başvurma oranlarında önemli düşmüştür. 1996 ve 2000 yılları arasında hırsızlığa maruz kalanların yarısından daha azı polise başvurmuştur (Semukhina ve Reynolds, 2012: 177).

Halkın polise karşı güvensizliğinin bir diğer sonucu da toplumda suç korkusunun yüksek olmasıdır. 2000'li yıllara değin resmi suç oranları arttıkça, suça uğrama korkusunda da artış olmuştur. Kamusal güvenin düşüklüğü, halk – polis işbirliğini de etkilemektedir. Bunun en büyük göstergesi, suç mağdurlarının polise başvurmayı reddetmesidir. 1992 ila 2000 yılları arasında dolandırıcılık suçuna maruz kalanların ancak %5'i polise şikayette bulunmuştur (Макарова, 2011: 64).

Sovyet dönemi ve Rusya'nın ilk yirmi yılı boyunca polisin halk gözündeki algısı oldukça olumsuzdu. Medvedev'in 2009 yılında giriştiği reform hamleleri bu sorunun da çözülmesine odaklanmıştı. Polisin imajını ve güvenilirliğini düzeltmek amacıyla eğitim faaliyetleri, bağımsız iç denetim örgütlenmesi, yasal düzenlemeler, personele yönelik yaptırımlar uygulamaya kondu. 2011'den itibaren nisbi de olsa polise duyulan güven ve imaj konusunda gelişmeler kaydedilmeye başlandı.

2011 yılında polise güven duyanların oranı %52'den 2012 %54'e çıkmıştır (VTsiOM, 2018). 2010-2014 yılları arasında polise güvenen ve olumlu bulan vatandaş oranı %52'den %66'ya yükselmiştir. Nüfusun %51'i ise son iki yılda (2012-2014 dönemi) hayatın daha güvenli olduğunu ifade etmiştir. 2014 yılında hayatın daha güvenli olduğunu düşünenlerin oranı %54'e yükselmiştir. En son 2017 yılında yapılan araştırmada ise polisin algısında önemli gelişmeler olmuştur. 2017 yılında polise olan güven vatandaşların %67'sine ulaşmıştır. Güvensizlik oranı ise %27'ye düşmüştür. Halkın olumlu algılama kriter değerlerinde de gelişmeler söz konusudur. Toplumun %66'sı polisin nazik, %66'sı dostça, %65'i dürüst, %65'i cesur ve %64'ü ise yeterli olduğunu düşünmektedir. Bu olumlu algı değişimi, halkın polisle işbirliği isteğine de yansımıştır. 2017 yılında halkın %90'ı tanık olmaya, %74'ü ise işbirliği yapmaya gönüllü olacaklarını ifade etmiştir (MVD, 2018a).

Polis ve sanık haklarında değişim Yeni, yasada sanıklar tutuklandıktan üç saat içinde telefon etme hakkını elde etti. Polise sanıkları tutuklarken hak ve yükümlülüklerini bildirme zorunluluğu getirildi. Ticari müesseselerin mali ve ticari aktivitelerini inceleme hakkı polisten alındı. Polislerin vatandaşları kimlik belirlemek için bir saatten fazla alıkoymaları yasaklandı.

Yozlaşmayla mücadele Polis teşkilatında yozlaşmayla mücadele amacıyla sıkı tedbirler uygulandı. Hemen hemen tüm polis görevlileri yozlaşma boyutuyla sıkı denetimden geçirildi (Polislerin %90'ı; idari personelin %94'ü (Semukhina, 2014:2). Şüpheli, mağdur ve polis ilişkileri, rüşvet veya diğer istismarları azaltacak şekilde sıkı prosedürlere bağlandı.

Polisin faaliyet alanları Çarlık ve Sovyet polisinde, polisin vazifeleri arasında Çar'ın, Partinin ve ideolojilerin menfaatlerini korumak da sayılmaktaydı. Sovyetlerden sonra bu tür görevler kaldırıldı. Reform yasasıyla polisin ana faaliyet alanları şu şekilde düzenlendi:

1) Bireyin, toplumun ve devletin hukuka aykırı saldırılardan korunması

2) Suçların ve idari suçların önlenmesi ve bastırılması

3) Suçların tanımlanması ve ifşa edilmesi, ceza davalarında soruşturmaların yürütülmesi

4) Kişilerin aranması

5) İdari suçlarda idari cezaların uygulanması

6) Halka açık yerlerde yasa ve düzenin sağlanması

7) Trafik güvenliğinin sağlaması

8) Silah kaçakçılığının önlenmesi

9) Özel dedektif ve özel güvenlik faaliyetlerini denetlenmesi

10) Sözleşme esası da dahil olmak üzere mülkiyet ve eşyaların korunması

11) Ceza davaları, yargıçlar, savcılar, soruşturmacılar, kolluk kuvvetleri ve denetleme görevlileri ve diğer korunan kişilerin, mağdurların, tanıkların ve diğer katılımcıların korunması

12) Uzman- kriminalistik faaliyetler.

Merkezileşme Reform sonucu polis teşkilatında federe ve bölgesel örgütlenmeler kaldırıldı ve Federal düzeyde bir kurum halinde tüm ülke çapında örgütlendi.

SONUÇ

Rusya 1990'lı yılların başından itibaren içine düştüğü türbülans ve kaos ortamında liberal demokratik devlet ve yönetim biçimine dönüşüm çabalarında önemli başarılar elde etmiştir. Öte yandan kamu yönetimi teşkilat yapısı ve işleyişinde de köklü dönüşüm süreci içine girmiştir. Bu sürecin asli bir parçası olarak Kolluk yapısında da değişim sürecine girmiştir. Ancak 1990'lı yıllarda girişilen reform çabaları başarılı sonuçlar vermemiştir. 2000'li yıllardan itibaren Putin-Medvedev ikilisiyle siyasi istikrarın oluşmasından sonra reform süreçleri etkin bir şekilde sürdürülmüştür. Bu süreçte istikrarlı ve kararlı bir siyasi irade, kamuoyu desteği ve Rusya ekonomisindeki gelişmelerin desteğiyle kolluk teşkilatında reform çabaları başarılı sonuçlar vermeye başlamıştır.

Özellikle 2010 yılında Medvedev önderliğinde siyasi iradenin kararlı tutumu ve kamuoyu desteğiyle oldukça çarpıcı başarılar elde edilmiştir. Bir defa toplumun en temel gereksinimi olan kolluk hizmetleri alanında güvenlik, asayiş ve huzuru belli derecede başarı sağladığında, siyasi istikrar, ekonomik gelişme ve sosyal bütünlüğün başarılabileceği Rusya örneğinde görülmektedir.

1990'lardan itibaren Rusya'daki dönüşüm süreci halkın tamamen edilgen olduğu, tüm kararların Parti-Devlet elitleri tarafından alındığı ve kamu hizmetlerinin toplum tarafından asla sorgulanamaz bir bürokrasi egemenliğinde sunulduğu bir anlayıştan, liberal-demokratik yapıya dönüşümü içermektedir. Vatandaşların denetleyemediği, karar alma ve hizmet sunma süreçlerine katılamadığı bir kamu yönetimi teşkilatının sağlıklı bir şekilde yapılanması, işlemesi ve hizmet sunması mümkün değildir.

Rusya kolluk teşkilatının varlık nedeni de güvenlik hizmeti sunduğu Rus vatandaşlarıdır. Kolluk teşkilatında 2010'lu yıllara kadar yapılan reform çabalarında istenen başarıların elde edilememesinin başlıca sebebi de kamuoyunun görüş, talep ve şikayetlerinin hesaba katıldığı bir kamu politikasının geliştirilmemiş olmasıdır. Ancak 2010 yılından itibaren kolluk hizmetlerinin geliştirilmesi çabalarında kamuoyunun görüş ve kanaatleri de dikkate alınmaya başlandıkça kolluk hizmetlerinin kalitesi artmaya ve vatandaş memnuniyet düzeyleri yükselmeye başlamıştır. Bu doğrultuda yapılan kritik bir değişiklik kolluk hizmetlerinin performans ölçümünde kayıtlı vaka istatistikleri yoluyla değerlendirmenin (paloçnaya sistema) terk edilmesidir. Kayıtlı vaka oranının düşmesini başarı olarak gören bu yöntem, kolluğun vatandaşlardan gelen ihbar ve şikayetleri kayıt etmeme, istatistikleri karartma, basit hırsızlık, gibi suçları işleme

koymama gibi olumsuz davranışlara yönlendirmektedir. Aynı şekilde çözülmesi güç ve failin bulunmasının zor olduğu vakaları da kolluk işleme koymakta isteksiz olmaktadır.

Paloçnaya sistemin terk edilmesi ve performans değerlendirmede vatandaş memnuniyetinin esas alınmasıyla kolluk reformunun başarılı olması, sağlıklı örgütsel düzenlemelerin yapılabilmesi, kolluk hizmetlerinin etkin ve verimli şekilde sunulması ve en önemlisi vatandaş- polis ilişkisinde olumlu gelişmeler sağlanması çok daha kolaylaşmıştır. Öte yandan gerçekçi olmayan performans değerlendirme kriterlerinden kurtulan kolluk görevlileri de kamuoyu algısı ve vatandaş memnuniyetine dayalı değerlendirme kriterlerini gözeteceğinden görevini daha motive olmuş bir şekilde yapabilmekte, mesleğinden aldığı manevi tatmin artmakta ve etkin ve verimli bir çalışma ortamına sahip olmaktadır.

Kolluk reformu sürecinde kamuoyu algısının önemini vurgulayan bir diğer göze çarpan olgu, kamuoyu ölçümleri yapan enstitünün (VTsiOM) tarafsızlığı ve güvenirliğinin sağlanması için tutarlı siyasi irade gösterilmiş olmasıdır. Bu amaçla kolluk hizmetlerinden memnuniyet düzeylerinin ölçümü İçişleri Bakanlığının dışında bağımsız bir enstitü olan VTsiOM tarafından yapılmakta, anket, sms mesajı gibi uygulamalar esnasında vatandaşlar değerlendirme sürecinin tamamen tarafsız ve mahremiyet haklarının da güvence altında olduğu konusunda temin edilmektedir. Böylece kolluk teşkilatı ve işleyişi hakkında vatandaşlardan sağlıklı geri bildirimler alınarak eksikler, hatalar, geliştirilmesi gereken unsurlar ve başarılar sağlıklı bir şekilde tespit edilebilmektedir. Rusya'da 2010'lardan itibaren kamuoyu algısında memnuniyet dizeylerinin dramatik bir şekilde yükselmesi çarpıcı bir gelişmedir.

Bu tür bir kamu politikasının siyasi iktidar açısından da iki boyutlu getirisi olmaktadır. İlki yönetmekle sorumlu olduğu kamu idaresi hakkında sağlıklı bilgi ve geri bildirim elde ederek, o idarenin daha iyi yönetilmesi mümkün olmaktadır. İkincisi ise kamu hizmetlerine yönelik kamuoyu algısının iyileşmesi siyasi destek ve oy potansiyelini arttırmaktadır.

KAYNAKÇA

Agentura (2018) *Служба безопасности Президента Российской Федерации*, http://www.agentura.ru/dossier/russia/fso/sbp/structure/ (20.9.2018).

Baharçiçek, A. ve Ağır, O. (2016) Rusyanın Başarısız Demokratikleşme Tarihi, *Birey ve Toplum Dergisi*, C:6, S:8: 5-27.

Cheloukhine, S. (2017) *Policing in Russia: Combatting Corruption Since the 2009 Police Reform*, Springer, Cham.

Customs (2018) *таможенной службы России*, http://www.customs.ru/index.php (17.9.2018).

Дахин, Андрей Васильевич (2018) *Правовая Норма, Идейная Позиция Государства И Мировоззренческий Выбор В Современном Социальном Контексте,* Юридическая Наука И Практика: Вестник Нижегородской Академии Мвд России, C:1/41: 286-288.

Erdem, K. (2017) *Yarı-Başkanlık ya da Süper Başkanlık: Rusya Federasyonu,* Karşılaştırmalı Hükümet Sistemleri: Yarı-Başkanlık Sistemi (Fransa, Polonya ve Rusya Örnekleri) (Ed: S. Gökçimen),TBMM, Ankara: 185-243.

FSO (2018) Об *Истории Создания Органов Государственной Охраны В России* ,Федеральная служба охраны России, http://www.fso.gov.ru/histori/p1.html (20.9.2018).

GKS (2018) *Federalnaya Slujba Gosudastvennoi Statistiki*, http://www.gks.ru/ (1.9.2018).

Гонюхов С.О. ve Горобцов В.И. (2002) *МВД России. 200 летнастражезакона и правопорядка*. http://regiment.ru/index.htm, (10.9.2018)

MacCarthy, L. A. (2014) *The Day Work of the Russian Police*, Russian Analitic Digest, C: 151:5-7)

Макарова М. Н. (2011) *Особенности Восприятия Органов Мвд В Общественном Мнении Региона,* Мониторинг общественного мнения, C:1/101:64-70. https://cyberleninka.ru/article/v/osobennosti-vospriyatiya-organov-mvd-v-obschestvennom-mnenii-regiona (19.9.2018)

MCHS (2018) *МЧС России*, http://www.mchs.gov.ru/ministry/tasks_functions/tasks (16.9.2018)

MİL (2018) *Минобороны России*, https://structure.mil.ru/structure/ministry_of_defence/details.htm?id=11260@egOrganization (15.9.2018).

Minjust (2018) *Федеральная Служба Исполнения Наказаний*, http://minjust.ru/structure/fedserv/fsin/regulation (20.9.2018)

Minjust (2019) *История Министерства*, https://minjust.ru/ru/history

MVD (2018) *Управление «К» МВД России*, https://xn--b1aew.xn--p1ai/mvd/structure1/Upravlenija/Upravlenie_K_MVD_Rossii (20.9.2018)

MVD (2018a) *Общественноемнение*, https://xn--b1aew.xn--p1ai/publicopinion, (20.9.2018).

MVD (2019) *Структура МВД России (схема)*, https://xn--b1aew.xn--p1ai/mvd/structure1 (4.7.2019)

PS (2018) *Главнаястраница,* Пограничнаяслужба, http://ps.fsb.ru/general.htm, (17.9.2018)

Rosgvard (2018) *Rosgvardiya*, http://rosgvard.ru/ru/page/index/okruga-vojsk-nacionalnoj-gvardii (20.9.2018)

Semukhina, Olga B. ve Reynolds, K. Michael (2012) *Understanding the Modern Russian Police*, CRC Press, New York.

Semukhina, Olga (2014) *From Militia to Police: The Path of Russian Law Enforcement Reforms*, Russian Analytical Digest, C:151:2-5).

Tataroğlu, Muhittin (2019), *Karşılaştırmalı İç Güvenlik Yönetimine Giriş: Ülke Örnekleri,* (ed.) T. Avaner, C. U. Çiner, Gazi Kitabevi, Eylül 2019, 163-225.

Taylor, B. D. (2018) *Law Enforcement and Civil Society in Russia*, Syracuse University, http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.508.4618&rep=rep1&type=pdf (22.9.2018).

Зайцева Т.В. (2016) *Материальноести мулирование государственных служащих в условиях ограниченного бюджетного финансирования*, Вопросы государственного и муниципального управления, С:4: 179-197.

Zakon (1995) *Федеральный Закон О Федеральной Службе Безопасности*, http://www.fsb.ru/fsb/npd/more.htm%21id%3D10340801 %40fsbNpa.html (22.9.2018).

Zakon, 2011) *Федеральный закон "О полиции"* http://www.consultant.ru/document/cons_doc_LAW_110165/ (21.9.2018)

Zakonoproekt (2010) *Обсуждение проекта федерального закона «О полиции»,* https://web.archive.org/web/20101113053653/http://www.zakonoproekt2010.ru/ (21.9.2018)

TURİZMDE GÜVENLİK ALGISININ TÜRKİYE EKONOMİSİNE ETKİSİ

Ozan BAHAR[*], Kamil BİLEN[**]

Öz

Turizm sektörünün, ülke ekonomisine sağladığı değer ve fayda her gün daha fazla artmaktadır. Diğer sektörlerle karşılaştırıldığında çok hızlı gelişim göstermektedir. Turistlerde seyahate çıkma fikri oluştuğunda gideceği yeri seçme konusunda çeşitli faktörler etkili olmaktadır. Bunların arasında çeşitli ihtiyaç ve beklentiler yer almaktadır. İnsan doğasının en önemli gereksinimlerinden birisi kendini güvende hissetme ihtiyacı olduğu için güvensiz koşullar altında turizmden bahsetmek zordur. Güvenlik ve güvenlik algısı turizm talebinin tercihlerine etki eden en önemli faktörler arasındadır. Bu önemi anlayan ülke ve firmalar turizmde güvenlik algısını pazarlama stratejisi haline getirmiştir. Çalışmanın amacı turizm sektöründe güvenlik algısının önemini ortaya koyarak bunun Türkiye ekonomisi üzerine etkileri hakkında bulgular elde etmek ve bu bulgular sayesinde yapılması gereken çalışmaları ortaya çıkarmaktır.

Anahtar Kelimeler: *Turizm Sektörü, Turizm Gelirleri, Turizm ve Güvenlik, Güvenlik Algısı.*

THE EFFECT OF SECURITY PERCEPTION IN TOURISM ON TURKISH ECONOMY

Abstract

The value and benefit of the tourism sector to the country's economy is increasing more and more every day. It shows a very rapid development when compared with other sectors. When tourists come up with the idea of traveling, several factors are effective in choosing their destination. These include various needs and expectations. Since one of the most important requirements of human nature is the need to feel safe, it is difficult to talk about tourism under unsafe conditions. Security and security perception are among the most important factors affecting the preferences of tourism demand. Countries and companies that understand this have made the perception of security in tourism a marketing strategy. The aim of our study is putting the importance of the tourism sector forward to obtain findings on security perceptions about the effects on Turkey's economy and regarding these findings, to depict the necessary works to be done accordingly.

Keywords: *Tourism Sector, Tourism Revenues, Tourism and Security, Security Perception.*

[*] Prof.Dr., Muğla Sıtkı Koçman Üniversitesi, Sosyal Bilimler Enstitüsü, obahar33@gmail.com, ORCİD No: 0000-0003-3349-5479

[**] Doktora Öğrencisi, Muğla Sıtkı Koçman Üniversitesi, Sosyal Bilimler Enstitüsü, kamilbilen06@gmail.com, ORCİD No:0000-0002-9527-5773

Makale Geliş Tarihi: 14.10.2019 Makale Kabul Tarihi: 03.02.2020

GİRİŞ

Turizm, istihdam alanları oluşturması, döviz girdisi sağlaması gibi ekonomiye ilişkin olumlu gelişmelerin önünü açmasıyla yıldızı devamlı parlayan bir sektör konumundadır. Yatırım maliyetinin diğer sektörlere oranla düşük olması ve doğal imkânlara ihtiyaç duyması gibi daha az karmaşık bir yapı ile kurulabilmesi sayesinde gelişmekte olan ülkeler, az gelişmiş ve neredeyse gelişme düzeyi son derece zayıf olan ülkelerin dahi kolaylıkla başvurabileceği bir sektör konumundadır. Türkiye'de olduğu gibi, tarım ülkesi konumunda olan birçok gelişmekte olan ülkede, turizmin ekonomik yararları ve etkileri gelişmiş ülke ekonomilerinde olduğundan çok daha fazla olabilmektedir (Bahar, 2007, s.2).

Turizm sektörü diğer sektörlerle önemli girdi alışverişi olan yapıya sahiptir. Bu sebeple diğer sektörlerde meydana gelen gelişmelerden etkilenmekte aynı zamanda diğer sektörlerin gelişmesine olanak sunmaktadır. Ekonomik gelişme sürecinde bu karşılıklı ilişki yapısal bağlılık kavramı içerisinde yer alarak sektörün gelişmesinde önemli bir yere sahiptir (Şen ve Şit, 2015, s.31).

Turistler, kendini güvende hissetmediği bir ortamda tatil yapmak istemezler. Turizmin duyarlı yapısı nedeniyle güvenliğe yönelik en küçük bir şüphe bile sektörü olumsuz yönde etkilemektedir. Gidilen yerde güven içinde olabilme beklentisi ve inancı turizm mekânına yönelik seyahat kararlarında birinci derecede rol oynar.

Çalışma kapsamında turizmde güvenlik algısı ile ilgili öncelikle kapsamlı bir literatür taraması gerçekleştirilmiş, benzer konuda ulusal ve uluslararası alanda yazılan akademik çalışmalar taranmış, farklı yazarların aynı doğrultudaki çalışmaları ikincil veri kaynağı olarak incelenerek araştırmanın kuramsal çerçevesi oluşturulmuştur. Bununla beraber araştırmanın verileri, Türkiye Cumhuriyeti Kültür ve Turizm Bakanlığı'ndan, Türkiye İstatistik Kurumu'ndan (TUİK) ve Dünya Seyahat ve Turizm Konseyi'nden (WTTC) elde edilmiştir. Bu istatistiki veriler incelenerek bulgular elde edilmiştir.

Çalışmanın ilk kısmında önemli makroekonomik göstergelerin karşılaştırılması yapılarak turizm sektörünün Türkiye ekonomisine etkileri araştırılmıştır. İkinci kısmında ise güvenlik algısının turizm sektöründeki yeri ve öneminin ne olduğu açıklanmaya çalışılmıştır.

1.TURİZMİN TÜRKİYE EKONOMİSİNE ETKİSİ

Turizm, insanların sürekli ikamet ettikleri yer dışında yaptıkları seyahat ve gittikleri yerlerde geçici konaklamalarından doğan ihtiyaçların karşılanması ile ilgili üretim ve tüketim odaklı bir faaliyettir (Kozak, Kozak ve Kozak, 2001, s.42). İnsanlar tarihin her döneminde seyahat etmişlerdir. Kişi başına milli gelirdeki artış, bilgiye ulaşmanın daha kolay hale gelmesi, insanların merak ettikleri ve şimdiye kadar görmedikleri yerleri görme isteklerinin artması ile hızlı trenin yaygınlaşması, havayolu taşımacılığındaki gelişmeler gibi teknolojik ilerlemeler turizmin gelişmesine katkı sağlamıştır.

Turizm özellikle gelişen ülke ekonomileri için çok önemlidir. Turizm sektörünün ülke ekonomisi içerisindeki önemini belirleyen kabul görmüş kritereler, ülkeler arasında karşılaştırma yapılmasına olanak tanımaktadır. Turizmin ülke ekonomisine etkisinin tespitinde; döviz gelirleri sağlaması, ihracat etkisi; gayri safi milli hâsıla içindeki önemi, ödemeler dengesine katkısı, istihdam sağlaması ile çarpan etkisi gibi kriterler baz alınmaktadır (Somuncu, 2004, s.167). Sonuçta ülke insanının refah seviyesinin artırılmasına katkı sağlamaktadır. Diğer sektörlerle karşılaştırıldığında turizm çok hızlı gelişim gösteren bir sektör olduğu yadsınamaz bir gerçektir.

Ödemeler bilançosunun cari işlemler hesabındaki uluslararası hizmetler kısmında yer alan turizm, görünmeyen bir ihracat kalemidir. Bu nedenle ülkeye sağladığı döviz gelirleri ile dış açıklarının giderilmesine ve bütçe açıklarının finansmanına önemli katkılarda bulunmaktadır. Turizm sektörü, emek yoğun bir sektördür buna bağlı olarak vasıfsız emeğe istihdam alanı oluşturmaktadır. Turizm sektörünün emek yoğun bir sektör olmasına rağmen sanayi sektörünün gelişmesine de katkı sağladığı bir gerçektir. Artan turist sayısı daha çok otel, ulaşım ve gayrimenkul kiralama gibi ihtiyaçları beraberinde getirecek ve bu yapılanmalar inşaat sektörünün de canlanmasına, bu sektördeki istihdam artışına neden olacaktır. Turizm faaliyetlerini önemli kılan; yemek, ulaşım, konaklama ve eğlence faaliyetlerine yönelik talep artışının yurt içi cari üretim düzeyini yükselterek gelir seviyesini arttırması ve emek yoğun olan bu sektörün istihdamına olumlu katkı sağlamasıdır.

Türkiye'nin görünmez bir ihracat kalemi olarak görülen turizm, gelişmekte olan ülkelere, ihracata göre daha zahmetsiz yollardan döviz sağlaması açısından önemli bir yere sahiptir. Üretilen herhangi bir ürünü yabancı bir ülkeye ihraç etmek için gerekli yetiştirme koşullarının sağlanmış olması, ambalajlamasının yapılması, ürün

dayanıksız bir mal ise ürünün korunması için gerekli önlemlerin alınması ve ihraç edilecek olan ülkeye ulaşımının sağlanması gibi işlemlerden geçmek zorundadır. Bu ise zorlu bir süreçtir. Teknoloji çağının getirmiş olduğu faydalarla birlikte turizmin sağlamış olduğu gelirler ihracata göre daha zahmetsizdir. İhtiyaç duyulan döviz gelirleri ihracatın artırılmasına kıyasla daha kısa sürede ve daha az kaynak kullanarak sağlanmaktadır (Uysal, Erdoğan ve Mucuk, 2003, s. 164).

Tablo-1. Türkiye'de Turist Sayısı ve Turizm Gelirleri (Kültür ve Turizm Bakanlığı, TÜİK).

YILLAR	TURİST SAYISI	TURİZM GELİRİ (1000 $)	GSYİH İÇİNDEKİ PAYI (%)	İHRACAT İÇİNDEKİ PAYI (%)
2003	16 463 623	13 854 866	4,4	29,32
2004	20 753 734	17 076 607	4,2	27,03
2005	25 045 142	20 322 111	4,1	27,65
2006	23 924 023	18 593 951	3,4	21,73
2007	27 239 630	20 942 500	3,1	19,52
2008	31 137 774	25 415 067	3,3	19,24
2009	31 759 816	25 064 482	3,9	24,53
2010	32 997 308	24 930 997	3,2	21,89
2011	36 769 039	28 115 692	3,4	20,84
2012	37 715 225	29 007 003	3,3	19,02
2013	39 860 771	32 308 991	3,4	21,31
2014	41 627 246	34 305 903	3,7	21,76
2015	41 114 069	31 464 777	3,7	21,87
2016	30 906 680	22 107 440	2,6	15,51
2017	37 969 824	26 283 656	3,1	16,74
2018	46 112 592	29 512 926	3,8	17,57

Tablo 1'de 2003-2018 yılları arasında Türkiye'ye gelen toplam ziyaretçi sayısı, turizm gelirleri ile turizm gelirlerinin GSYİH ve genel ihracat içinde pay oranlarına yer verilmiştir.

Türkiye'ye 2003 yılında 16.463.623 ziyaretçi gelmiştir. Türkiye'nin ülke ekonomisi içerisinde turizm sektörüne gereken önemi vermesi sonucunda, 2018 yılına gelindiğinde gelen turist sayısı yaklaşık 3 kat artarak bu sayı 46.112.592 kişiye ulaşmıştır. Yıllar içerisinde en önemli artış 2003-2004 yılları arasında yaşanmıştır. 2003 yılında 16.463.623 kişi olan turist sayısı % 26 artarak 20.753.734 kişiye ulaşmıştır. Ancak 2016 yılında % 25 oranında bir azalma olmuş ve 30.906.680 kişiye düşmüştür. Turist sayısında dikkat çeken diğer bir nokta ise 2008 küresel ekonomik kriz sonrasında dünya genelinde düşüş olmasına rağmen Türkiye'ye gelen turist sayısında artış görülmüştür.

Türkiye'de turizm sektöründe elde edilen gelir genel olarak artış göstermiştir. 2003 yılında yaklaşık 14 milyar dolar gelir elde edilirken 2018 yılında yaklaşık 29 milyar dolar gelir elde edilmiştir. Özellikle Kasım 2000 ve Şubat 2001 krizlerinden sonra turizm gelirlerinin önemli derecede artması krizden çıkış noktasında turizm sektörünün önemini bir kez daha göstermiştir. 2016 yılında ise Türkiye'de yaşanan terör eylemleri nedeniyle bir önceki yıla göre turizm sektöründen elde edilen gelir % 30 oranında azalarak yaklaşık 22 milyar dolar olarak gerçekleşmiştir.

Turizm gelirlerinin ülke ekonomisi içerisinde ne kadar öneme sahip olduğunun diğer bir göstergesi de turizm gelirlerinin GSYİH içerisindeki payıdır. Bu paylar 2003 yılında % 4,4 oranında gerçekleşirken 2018 yılında bu oran % 3,8 oranında gerçekleşmiştir. 2008 yılında yaşanan küresel ekonomik kriz sonrasında 2009 yılında pay oranı önceki yıllara nazaran artış göstererek % 3,9 olarak gerçekleşmiştir (Şen ve Şit, 2015, s.37).

Tablo 1'de turizm sektöründen elde edilen gelirlerin ihracat içindeki payına yer verilmiştir. 2003 yılında Türkiye turizm sektöründen elde ettiği yaklaşık 14 milyar gelirle toplam ihracatta % 29 oranda pay elde etmiştir. 2003 yılından itibaren turizm gelirlerinin toplam ihracattaki payı genel olarak düşme eğilimi göstermiştir. Genel itibari ile ihracattaki artış oranı turizm gelirlerindeki artış oranından daha fazladır. Söz konusu dönemde ihracat gelirleri % 253 artarken turizm gelirleri % 114 artmıştır. Turizm sektöründen elde edilen gelir 2003 yılında Türkiye'nin genel ihracatında yaklaşık % 30 oranında bir paya sahipken 2018 yılına gelindiğinde bu oran yaklaşık % 18'lere kadar gerilemiştir. Özellikle 2008 yılında yaşanan küresel ekonomik kriz sonrasında 2009 yılındaki % 25 oranında gerçekleşmiştir.

Turizm sektörü, kriz ortamından diğer sektörlere nazaran daha az etkilenerek ekonominin can simidi olabilecek bir yapıya sahiptir (Şen ve Şit, 2015, s.40). Yıllar itibari ile ülkemize gelen turist sayısı ve turizm gelirleri artış göstermesine rağmen,

kişi başı turizm gelirlerinde sürekli olarak bir azalış trendi söz konusudur. Burada önemli olan husus turist sayısının çok olmasından ziyade nitelikli ve ülkeye katma değeri yüksek bir profilinin olmasıdır. Turistlerin ülkemizde yapmış oldukları harcamalar sahip oldukları gelir düzeyi ile ilgili bir durumdur. Bundan dolayı ülkemize gelen turistler genellikle orta gelir düzeyine sahip kişilerden oluşmaktadır.

Turizm sektörü daha çok emek yoğun bir sektördür ve bundan dolayı istihdamın temel kaynaklarından biri olarak kabul edilmektedir. Turizm birçok faaliyet ya da iş kollarının bileşiminden meydana gelmektedir. Bundan dolayı turizm amaçlı yapılan tüketim harcaması ilk olarak doğrudan istihdama yol açarken, elde edilen gelirin sektör içinde tekrar harcanması ise dolaylı istihdama yol açmaktadır (Kozak, 2013, s. 176).

Turizmin istihdama doğrudan katkısına örnek olarak, yapılan harcamaların kapasiteyi artırıcı bir rol oynayarak otellerin veya pansiyonların istihdam kapasitesini arttırması, dolaylı istihdama örnek olarak ise turizm faaliyetlerinden elde edilen gelir sonucunda bölgede artan talebe göre ulaşım, alışveriş merkezleri, eğlence ve çeşitli sosyal faaliyetlerdeki istihdam edilen kişi sayısının artması verilebilir.

Türkiye'de turizm talebini karşılamak amacıyla birçok üst yapı tesisinin inşası ve işletmelerin yeni yatırımlara yönelmeleri, sektörde çalışacak kişilere ihtiyaç duyulması anlamına geleceğinden sektörün iyi seviyede istihdam yaratmasına imkân tanımaktadır (Kar, Zorkirişci ve Yıldırım, 2004, ss.90-91). Bu nedenle turizm sektörü, Türkiye'nin ekonomik kalkınma stratejisinde kilit bir sektör olarak kabul edilebilecek bir konumdadır (Çımat ve Bahar, 2003, s.2).

Türkiye gibi gelişmekte olan ülkelerde turizm sektöründe çalışan işçilerin gelişmiş ülkelere göre ücreti daha düşüktür. Bundan dolayı gelişmiş ülkelere turizm sektöründe işlemlerin teknolojik araçlarla yapılması tercih edilirken, gelişmemiş ya da gelişmekte olan ülkelerde bu durum daha çok insan odaklı gelişmektedir (Kozak, 2013, s. 178).

Turizmde sektöründe yapılan yatırım ve harcamalar, diğer sektörlerle kıyaslandığında yüksek oranda istihdam sağlamaktadır. Turizm sektörü emek yoğun olması ve çok sayıda düşük ücretli iş alanı bulunması, yarı zamanlı ve geçici iş imkânlarının bulunması, sezon yoğunluğu ve dönemsellik gibi nedenlerden dolayı ülke içerisinde büyük oranda istihdam sağlamaktadır (Bahar ve Özdemir, 2018, s. 268).

Tablo-2. Türkiye'de Turizm Sektöründe İstihdam (Bin Kişi) (WTTC, Kalkınma Bakanlığı).

Yıllar	Doğrudan İstihdam	Dolaylı İstihdam	Toplam İstihdam (1)	Türkiye'de Toplam İstihdam (2)	Pay (1/2)
2010	458	1.152	1.609	22.594	7,12
2011	487	1.367	1.855	24.110	7,69
2012	507	1.308	1.815	23.937	7,58
2013	531	1.450	1.981	24.602	8,05
2014	580	1.550	2.130	25.933	8,21
2015	614	1.596	2.210	27.341	8,08
2016	495	1.702	2.197	27.428	8,01
2017	484	1.634	2.118	27.153	7,8
2020*	791	1.807	2.598	-	-
2025*	915	1,902	2,817	-	-

*Tahmini Veriler.

Tablo 2'de Türkiye'de turizm sektörüyle ilgili istihdam verileri bulunmaktadır. Buna göre turizm sektörü, istihdama çok önemli katkı sağlamıştır. Bu katkılardan en önemlisi sektörün toplam istihdama sağladığı doğrudan katkıdır. WTTC verilerine göre, turizm sektörünün gelişmesiyle birlikte Türkiye'de turizm sektörünün doğrudan istihdam rakamları 201-2017 yılları arasında %7 oranında artarak 458 bin kişiden 484bin kişiye ulaşmıştır. Aynı dönemde dolaylı istihdamda 1 milyon 152 bin kişiden 1 milyon 634 bin kişiye yükselmiştir. Bu dönemde turizm sektöründe dolaylı istihdamın artış oranı %41 olarak gerçekleşmiştir. Turizm sektörünün oluşturduğu toplam istihdama bakıldığında ise; aynı dönemde % 31 oranında artış göstererek 2 milyon 118 bin kişiye istihdam sağlamıştır. Turizm sektörünün toplam istihdam içerisinde aldığı pay ise genelde %8 civarında gerçekleşmiştir.

Bununla beraber WTTC'nin tahminlerine göre; 2025 yılında Türkiye'de turizm sektöründen sağlanan doğrudan istihdamın 915 bin, dolaylı istihdamınsa 1 milyon 902 bin kişiye ulaşması beklenmektedir. Turizm sektöründen sağlanan toplam istihdamın, 2 milyon 817 bin kişiye ulaşması tahmin edilmektedir.

Turizm birçok gelişmekte olan ülke için görünmez bir ihracat kalemi olarak kabul edilmektedir. Türkiye gibi gelişmekte olan ülkelerde turizm birden fazla faaliyet kollarını etkileyerek ülke ekonomisine katkı sağlamaktadır. Bu şekilde tanımlanmasının sebebi ziyaretçilere mal ve hizmet satarak döviz kazandırmasıdır. Bu nedenle turizm diğer ihracat sektörlerine göre daha avantajlı özellikler göstermektedir. Çünkü turizm yoluyla gerçekleştirilen ihracat, tüketicinin ihracata konu olan mal ve hizmete gelmesi ve yol masraflarının olmaması gibi nedenlerle dış ülkeye yapılan mal ve hizmet ihracatından farklılıklar gösterir. Bu farklılıklar turizm sektöründe ihracat imkânı bulunmayan bazı ürünleri, ülkenin doğal, tarihi, kültürel değerleri turistler kanalıyla dış pazar oluşturarak bir döviz kaynağı haline getirmektedir (Şen ve Şit, 2015, s.31.)

Turizm sektörünü, ülke ekonomisine sağladığı katkılar doğrudan ekonomik etki, dolaylı ekonomik etki ve uyarılmış etki olarak farklı gruplara ayrılmıştır. Turizmin doğrudan etkileri yerli ve yabancı turistlerin yaptığı turizm harcamaları ve devletin müze, ulusal park gibi alanlarda yaptığı harcamaları kapsar. Doğrudan etkileri turizm sektöründe hemen hissedilir. Dolaylı ekonomik etkileri, mal ve hizmet sağlayan işletmelerin turizm gelirlerini turizm sektörü için tekrar harcaması yolu ile ortaya çıkan etkidir. Bunlar turizm yatırımları ve devletin güvenlik sağlık gibi sektörlerde yaptığı genel harcamalardır. Uyarılmış etki ise turizm faaliyetlerinin bir sonucu olarak doğrudan veya dolaylı olarak elde edilen turizm gelirin hane halkı harcamalarına yansıması sonucu sektörlerin tamamında çarpan etkisiyle oluşan gelir artışını ve turizm sektöründe çalışanların yaptığı harcamaları kapsamaktadır. Turizm sektöründe meydana gelen gelişmeler ile birlikte yeni yatırımlara olanak tanıyacaktır. Yapılan bu yatırımlar inşaat sektörünü tetikleyerek bu sektörde yeni gelişmeler meydana getirecektir. Yatırımın yapıldığı çevrede hareketlilik sağlanması maksadıyla eğlence, alışveriş ve turizm amaçlı birçok faaliyetler gelişim göstermeye başlayacaktır. Bu yaşanılan gelişmeler beraberinde istihdamı olumlu etkileyerek ekonomik büyümeye olumlu katkıda bulunacaktır (Bahar ve Kozak, 2012, s. 11).

2. TURİZM VE GÜVENLİK İLİŞKİSİ

Güvenlik, insan davranışlarında, düşünce ve algılarında tedirgin ve korku unsurların bulunmaması, insanların emin ve rahat olması durumudur (Kılıç, 2000, s.1013). Güvenlik ile ilgili kavramlar günümüzde çok geniş bir yelpazeye yayılmış durumdadır. Sağlık, eğitim, insan hakları, çevreyle ilgili değişim, terör, göç, hava kirliliği gibi birçok olgu güvenlik kavramının içerisinde değerlendirilmektedir. Hal böyle olunca güvenlik, toplumsal güvenliğe ve huzura endeksli bir boyut kazanmaktadır (McSweeny, 1999, s. 19).

İnsan doğasının en önemli gereksinimlerinden birisi kendini güvende hissetme ihtiyacıdır. Maslow'un belirttiği ihtiyaçlar hiyerarşisi piramidine göre güvenlik ihtiyacı, zorunlu ihtiyaçlardan sonrasındaki en önemli ihtiyaçtır. İnsanlar her zaman kendini güvende hissetmek isterler. Dolayısıyla insanların huzur ve güvenliğinin sağlanması, sağlanan bu güven ortamının süreklilik arz etmesini isteme düşüncesi tarih boyunca var olmuştur (Kızılkaya ve Sönmez, 2003, s. 18).

Turizm faaliyetlerinin oluşması için gerekli unsurlardan birisi güvenliktir. Güvensiz koşullar altında turizmden bahsetmek oldukça zordur. Bunun sonucu olarak güvenlik ve emniyet konuları turizm talebinin tercihlerine etki eden en önemli faktörler arasındadır. Rekabet ortamının yaşandığı turizm sektöründe destinasyon tercihinde ve seçilen destinasyonda kalış süresinde veya tekrar aynı destinasyonun seçilip seçilmemesinde güvenlik algısının önemli rol oynamaktadır. Bir destinasyon kimi turist için güvenli algılanırken bir diğeri için güvensiz olabilmektedir. Güvenliğin algılanmasındaki bu kişisel değişkenlerin bilinmesi pazar paylaşımı yapılırken işletmelere önemli bir avantaj sağlayacaktır. Turizm ve güvenlik ilişkisinin önemini kavrayan ülkeler ve firmalar güvenlik olgusunu pazarlama stratejisine dönüştürmüştür. Turistik bölgenin tanıtım kampanyalarında ve reklamlarında güvenlik ve huzur temasını güncel medya araçlarını kullanarak hedef kitlelerine duyurmaktadır (Seçilmiş, 2009, s.153).

Tüketicilerin talepleri ne kadar çok karşılanırsa tüketiciler o kadar çok tatmin olurlar, bu durumda firmalara aynı düzeyde memnuniyet olarak geri dönecektir. Güvende olma ihtiyacı insan doğasındaki en temel gereksinimlerden biri olduğu için kendini güvende hissetmeyen turist tedirgin halde olacağından dolayı turistik ürün ve hizmetlerden keyifle yararlanamayacak ve turizm faaliyetinden almış olduğun tatmin seviyesi düşük olacaktır (Bayhan ve Ünlüönen, 2016, s.2).

Turistlerde kendi yaşadıkları yerden ayrılıp yeni ve yabancı bir yere gitmenin verdiği psikolojik bir belirsizlik vardır. Böylece gittikleri yerlerde yaşadıkları ve

şahit oldukları küçük bir olay bile turistleri karamsarlığa sürükleyebilmektedir. Eğer herhangi bir turistik bölgede can ve mal güvenliği yoksa turistin oraya gelmesi beklenmemelidir (Koyunoğlu, 2003, s.23).

Ülkemizin önemli turizm pazarını teşkil eden gelişmiş ülkeler, risk konusunda son derece duyarlıdır. Bu ülkelerdeki insanların çoğunluğu, özellikle seyahat ve tatil kararlarını verirken güvenlik açısından daha az riskli bölgeleri tercih etmektedirler. Genellikle, seyahat kararını vermeden önce gitmeyi düşündükleri ülkeler hakkında detaylı bilgi toplarlar. Dışişleri Bakanlıklarının veya resmi mercilerin seyahat tavsiyeleri ve uyarıları, seyahate gidecek insanların kararları üzerinde etkili olmaktadır. Hiçbir turist, para vererek risk satın almak istemez. Güvenlik konusunda risk taşıyan bir bölgede her ne kadar modern tesisler, tarihi, doğal zenginlikler, kültürel çekicilik turistik destinasyonlarda belirleyici unsur olsa da turistler güvenlik eksiği olan riskli yerleri tercih etmemektedirler (Kuveloğlu, 2004, s. 142).

Turizm meydana gelen olumsuzluklardan en çabuk etkilenen hassas bir sektördür. Teknolojideki gelişmeler ile birlikte medya iletişim ağının güçlenmesi sonucu dünyanın bir ucunda yaşanan olaylar birkaç dakika içerisinde tüm dünyaya yayılmaktadır. Hiçbir insan turistik çekimi ne kadar güçlü olursa olsun, ya da ekonomik olarak ne kadar uygun olursa olsun kendini güvende hissetmediği bir ortamda tatil yapmak istemeyecektir. Turizmin duyarlı yapısı nedeniyle güvenliğe yönelik en küçük bir şüphe bile sektörü olumsuz yönde etkilemektedir. Gidilen yerde güvenlik içinde olabilme kanısı ve inancı turizm mekânına yönelik seyahat kararlarında birinci derecede rol oynar. Başka bir anlatımla turizm ile güvenlik arasında organik bir ilişki bulunmaktadır (Eralp, 1983, s. 2).

Seyahat edilecek ülkede yaşanan siyasal sorunlar, ekonomik kriz gibi bazı gelişmeler sonrası yaşanan grev ya da eylemler turist tercihlerinde etkili olmaktadır. Turizm sektöründeki rekabet ortamı ve alternatiflerin çeşitliliği talep esnekliğini artırmaktadır. Herhangi bir asayiş sorunu bile güvenlik endişesi ile talebin farklı ülkelere yönlenmesine sebep olmaktadır (Seçilmiş ve Ünlüönen, 2009, s. 72).

Turistik faaliyeti yapan kişilerde tatil yeri seçiminde medya önemli bir faktördür. Olumlu ve ilgi çeken haberler bölgenin tercih edilebilirliğini artırabilirken çıkan olumsuz haberlerde turizm taleplerinde engel oluşturabilmektedir. Turistik bölgelerde turistlere karşı işlenen suçlar basında

büyük yer bulmaktadır. Medyada çıkan bu haberler turistler üzerinde olumsuz güvenlik algısı oluşmasına sebep olacaktır. Bu durumda ülkenin turizm talebinde düşüş meydana getirmektedir. Bu bağlamda ülke ve turizmin çıkarları dikkate alınarak etik yayıncılık anlayışının benimsenmesinin önemi büyüktür (Seçilmiş, 2009, s.155).

Türkiye'de herhangi bir güvenlik sorununun yaşanması durumda Türkiye giriş yapacak olan turistlerin çoğunluğunun rotası Avrupa'nın diğer ülkelerine çevirmesinden dolayı Avrupa turizm sektörü açısından Türkiye imajı, değerlendirmeye alındığında oldukça önem arz eden bir sonuca varılmaktadır. Türkiye'de bir bölgede sorun oluşması durumunda Avrupalı turistler tatillerinden vazgeçmektense başka bir bölgede tatil yapmayı tercih etmektedirler. Durum böyle olunca da Türkiye'nin rekabet halinde olduğu ülkeler, ülkede meydana gelen problemleri fırsat bilip medyalarında duruma abartarak Türkiye'nin güvenli bir ülke olmadığına dair kötüleme girişimlerinde bulunabilmektedirler. Sonuç olarak Avrupa'dan Türkiye'ye doğru akan turizm dalgası sekteye uğrayarak rakip ülkelere fırsat doğabilmektedir (Kaşlı vd., 2009, s. 92).

Ülkemizde trafik hakkında seyahat tavsiyeleri, uyarıları ve diğer kaynaklar tarafından verilen bilgiler genellikle olumsuzdur. Trafik, Türkiye'de çok büyük bir risk unsuru olarak görülmektedir. Trafik sorunlarının ülkemizi ziyarete gelen yabancılar üzerinde olumsuz etki, tedirginlik ve korku yaratmaktadır. Bütün bu nedenlerle trafik, ülkemizin bütünsel ve turizm imajı arasında olumsuz etki yaratmaktadır. Çünkü gelişmiş ülke insanının nazarında trafik; insanların, toplum kurallarına, diğer insanların haklarına, insan sağlığına, kendisinin ve başkalarının hayatına duyduğu saygının, verdiği değerin göstergesi olarak görmektedirler. Trafikte güvenlik, rahat, huzur içinde ve mutlu bir seyahatin ön koşuludur. Bu nedenle trafik, ülkenin tanıtımı, imajı, seyahat kararlarının verilmesi, turistlerin o ülke hakkında edindikleri izlenimi ve genel güvenlik algısı açısından belirleyici niteliktedir (Subaşı, 2007, s.20).

Bir bölgenin ulaşım hizmetlerinin güvenirliliği, turizm güvenliğinin önemli bir parçası konumundadır. Sık sık trafik kazalarının yaşandığı ve trafik kurallarına uyulmadığı bir bölge, seyahat etmeyi düşünen insanlar tarafından ulaşım güvenliğinin olmadığı bir ülke olarak algılanacaktır. Ayrıca turistlerin bir bölgeden diğer bir bölgeye transferi esnasında yaşayabileceği ulaşım problemleri seyahat tercihlerinin değişmesine neden olabilecektir.

Sokak güvenliği sağlandığında turistler daha fazla gezme ve alışveriş imkâna sahip olacaktır. Turistler, gittikleri yerlerde güven içerisinde gezdiklerinde geçirdikleri tatilden tatmin düzeyleri daha fazla artacaktır. Tatilinde hiçbir güvenlik sorunu ile karşılaşmayan turistler, tekrar aynı turistik bölgeyi ziyaret etmek veya buradaki kalış süresini artırmak isteyeceklerdir. Turistler, sokaklarda daha rahat ve güvenilir bir ortamda gezerek alışveriş yapma imkânı bulacak bu da ülke ekonomisine daha fazla katkı sağlayacaktır.

2.1. Terörizmin Turizm Üzerine Etkileri

Turistler ziyaret ettikleri ülkenin doğal ve tarihi güzelliklerini, kültürlerini, yaşam biçimlerini tanımak ve görmek isterler. Bu nedenle ülkedeki otellerde dinlenmek yerine gezmek ve yeni yerler görmek arzusundadırlar. Turistlerin bölgede rahat ve güven içerisinde gezebilmesi için bölgenin güvenli olması gerekmektedir.

Turizm hareketlerinin, dış ödemeler bilançosu üzerindeki etkileri ve ulusal gelire katkısı, istihdamı artırıcı özelliğiyle ve turizm haricindeki sektörler üzerindeki olumlu etkisi nedeniyle ülke ekonomilerinde önemli bir yere sahiptir. Terör ve terörizmden doğan işsizlik ya da çatışmalar ve politik istikrarsızlık unsurları ile turizm hareketlerinin oluşumunu ve gelişimini sağlayan ulusal ve uluslararası barış, ekonomik kalkınma ve politik istikrar gibi unsurlar aynı ortam ve zaman diliminde bulunmazlar (Oktayer, Susam ve Çak, 2007, s. 147).

Turistik faaliyete katılacak kişiler gidilecek yer kapsamında genellikle seyahatleri süresince ne ile karşılaşacakları konusunda bilgileri olmadıkları için çekinmektedirler. Savaşlar, huzursuzluk ve negatif tanıtımlar, bir destinasyon için insanlarda korku ve şüphe düşüncesi uyandırmaktadır. Terörizm hareketleri de bu korkuların oluşmasında ve kişileri seyahat etmekten vazgeçiren önemli bir faktör olarak görülmektedir (McIntosh, Goeldner ve Ritchie,1995, s.239).

Terörizm, toplumların ekonomik, sosyal ve kültürel yapılarını doğrudan veya dolaylı bir şekilde etkilediğinden, terör eylemleri doğal olarak turizm sektörünü de olumsuz bir yönde etkilemektedir. Bazen de terörizm doğrudan turizm sektörünü hedef almaktadır. Terörizmin ortaya çıkış sebebi ideolojik, politik, etnik ya da ekonomik söylemlerini insanlara ulaştırmayı amaçlamaktadır. Terör örgütleri de uluslararası desteği sağlamak, adını duyurarak güçlü olduğunu tüm dünyaya göstermek istemektedir. Böylece terör örgütleri daha kolay ve etkili propaganda yapacak ve sempatizan sayısını artırabilecektir. Turizm sektörü sosyal, kültürel ve

ekonomik olarak uluslararası bir yapıya sahip olması nedeniyle terör eylemlerinin hedef olabilmektedir.

Terörizmin diğer önemli amacı ise hedef aldığı ülkenin ekonomisine ağır kayıp vermektir. Ülkelere döviz girdilerini sağlama ve istihdamı artırmada önemli bir role sahip olan turizm sektöründe rekabet ortamı ve alternatif çeşitlilikten dolayı talep esnekliği fazladır. Bu nedenle terör eylemlerine karşı çok hassastır. Terör eylemlerinin turizm sektörüne verdiği diğer önemli zarar ise yabancı sermayenin turizm sektörüne yatırım yapmamasıdır. Güvensiz ve gelecek konusunda kaygılı bir ortamda yabancı sermaye sahipleri ülkeye yatırım yapmak istemeyecektir.

Türkiye, coğrafi konumu bakımından çok avantajlı bir konumdadır. Fakat çevresindeki belirsizlikler ve kargaşa durumu, güvenli bir ülke olma imajını olumsuz yönde etkilemektedir. Terör ve yakın çevresindeki belirsizlik ve çatışma durumu, güvenli bir ülke olma imajını olumsuz olarak etkilemektedir. Terör olaylarının yaşandığı ülkelerde sektör çapında küçülme yaşanırken, var olan turist arzının görünüşte daha güvenli gözüken başka ülkelere yöneldiği belirtilmektedir. Turist sayısı artırabilmek amacıyla rekabet içerisinde bulunan ülkelerin bir kısmına etki edebilen askeri darbe, savaş ihtimali gibi olumsuz gelişmeler, diğer ülkeler açısından olumlu etki oluşturabilmektedir (Sivri, 2010, s. 221).

Turizm destinasyonlarına yönelik terör olaylarının sonrasında turistlerin takındığı ilk tepkinin ziyaretlerini ertelemek ya da iptal etmek olduğu ortaya çıkmaktadır. Böylece turizmden elde edilen gelirlerde düşüşler yaşanmasına, ülke ekonomisine ve sektördeki firmaların kötü yönde etkilenmelerine neden olmaktadır. Sonuç olarak istihdamın sağlanması, toplumsal dengenin oluşturulması ve ödemeler dengesi üzerinde önem arz eden turistik faaliyetlerin, terör olayları yüzünden olumsuz etkilenerek gerileme yaşanması, ekonomiye büyük zarar verilmesine sebep olmaktadır (Yılmaz ve Yılmaz, 2005, s. 47).

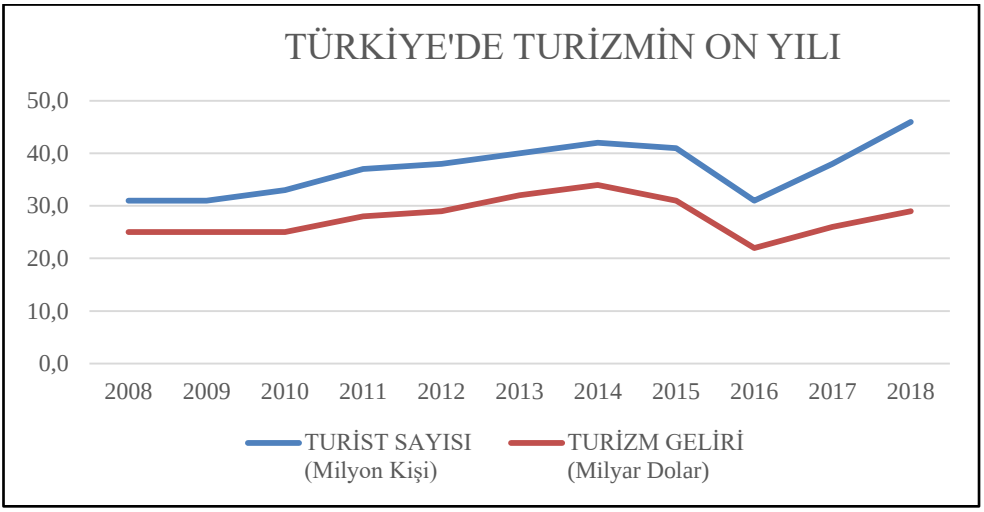
2.2. Terörün Türkiye'ye Gelen Turistler Üzerindeki Etkileri

Türkiye'nin konjonktürel açıdan terör ve turizm ilişkisine bakıldığında, terörün turizme etkisi gelecekte de günümüzdeki etkilerine benzerlik gösterecektir. Ülke içerisinde meydana gelebilecek olumsuz gelişmeler nedeniyle yabancı turist sayısında azalmaların oluşması muhtemeldir. Dolayısıyla bu durum, ülkenin turizm gelirlerini azaltıcı bir faktör olarak ortaya çıkacaktır. Terörizmin ülke sınırları dışından gelen yabancı turistlerin üzerinde daha yıkıcı etkilerinin olabileceği muhtemel görülmektedir (Drakos ve Kutan, 2001, s. 1).

Tablo-3. 2015-2017 Yılları Arasındaki Önemli Terör Saldırıları.

TARİH	OLAY
Temmuz 2015	Şanlıurfa'nın Suruç İlçesinde DAEŞ terör örgütü tarafından düzenlenen canlı bomba saldırısında 33 kişi yaşamını yitirmiştir.
Ekim 2015	Ankara'da DAEŞ tarafından düzenlenen 2 bombalı saldırıda 101 kişi yaşamını kaybetti.
Ocak 2016	Sultanahmet Meydanında Alman turist kalifesine düzenlenen saldırıda 11 kişi hayatını kaybetti.
Şubat 2016	Ankara'da askeri servis araçlarına PKK tarafından düzenlenen saldırıda 28 kişi yaşamını yitirdi.
Mart 2016	Ankara'da PKK tarafından düzenlenen bombalı saldırıda 35 kişi yaşamını yitirdi.
	İstiklal Caddesi'nde DAEŞ tarafından düzenlenen saldırıda 4 kişi yaşamını yitirdi.
Mayıs 2016	Diyarbakır Sur İlçesi'nde bomba yüklü aracın patlatılması sonucunda 16 kişi yaşamını yitirdi.
Haziran 2016	İstanbul Vezneciler'de düzenlenen saldırıda 6'si polis 12 kişi hayatını kaybetti.
Ağustos 2016	Gaziantep Şahinbey'de canlı bomba saldırısında 51 kişi yaşamını yitirdi.
Kasım 2016	Adana Valiliği yakınında bulunan otoparktaki bombalı saldırıda 2 kişi yaşamını kaybetti.
Aralık 2016	Beşiktaş Dolmabahçe stadyumu bölgesinde maç sonrası silahlı saldırıda 44 kişi yaşamını yitirdi.
	Kayseri'de bombalı saldırı sonucunda 15 asker şehit oldu, 48 asker yaralandı.
	Rusya'nın Ankara Büyükelçisi Andrey Karlov bir çevik kuvvet polisi tarafından uğradığı saldırıda öldürüldü.
Ocak 2017	Yeni yılın ilk saatlerinde Reina'da gerçekleştirilen saldırıda 39 kişi hayatını kaybetti 65 kişi yaralandı.

Tablo 3'de Türkiye'de 2015-2017 tarihleri arasında meydana gelen terör saldırı gösterilmektedir. Belirtilen tarihler arasında 14 önemli terör saldırısı meydana gelmiştir. Yapılan saldırılar incelendiğinde, eylemlerin kalabalık bölgelerde gerçekleştiği görülmektedir. Bu bölgelerin önemli bir kısmı ise yabancı turistlerin çoğunlukla ziyaret ettiği turistik yerler oluşturmaktadır. Yabancı turistler hedef alınarak gerçekleştirilen saldırılarda, Türkiye'nin güvenli bir bölge olmadığı algısı oluşturulmaya çalışılmıştır.



Şekil-1. Türkiye'de Turist Sayısı ve Turizm Gelirleri (Kültür ve Turizm Bakanlığı, TÜİK)

Şekil 1'de 2008-2018 yılları arasında Türkiye'yi ziyaret eden turist sayısına ve elde edilen turizm gelirlerine (milyon dolar) yer verilmektedir. Şekil 1 incelendiğinde Türkiye turizm gelirlerinin 2008 yılından 2014'ün sonuna kadar arttığı ancak 2015'te çok sert bir şekilde düştüğü görülmektedir. Bu düşüşe, 2015 yılında meydana gelmiş olan terör olayları ve siyasi krizlerin sebep olduğu düşünülmektedir. Bu açıdan son yıllarda ortaya çıkan küresel çapta terör olaylarının tüm dünyadaki insanları ve devletleri tehdit etmesiyle korku psikolojisinin hâkim olmasının yanı sıra hükümetlerin, ülkelere giriş çıkışlara ilişkin almış oldukları önlemler ve olağanüstü hal ilanları turizm faaliyetlerinin azalmasına neden olmuştur.

2015 yılında başlayan Türkiye'nin turizm sektöründeki gerileme 2016'da yaşanan güvenlik riski oluşturan terör saldırılarının hem yurt içinde hem de Avrupa'da giderek artması ile Avrupa'dan gelen ziyaretçileri de olumsuz etkilenmiş ve 2016 yılının Türkiye turizmi için kayıp bir yıl olmasına neden olmuştur. Kültür ve Turizm Bakanlığı'nın verilerine göre; 2016'da turizm geliri bir önceki yıla göre % 29,7 azalarak, 22 milyar 107 milyon dolar ve uluslararası ziyaretçi sayısı ise % 24,6 gerileyerek 31 milyon 365 bin kişi olarak gerçekleşmiştir.

Türkiye'de, başta ekonomisi olmak üzere özellikle turizm sektörünü olumsuz etkileyen çeşitli olaylar yaşanmıştır. 24 Kasım 2015'te Rusya Federasyonu'na ait

bir Sukhoi Su-24M tipi savaş uçağı Türk hava sahasını ihlal etmiş. Rus uçağı, Türk yetkililer tarafından 5 dakika kadar uyarılmasına rağmen, uçak uyarılara aldırış etmeden Türkiye hava sahasını 17 saniye boyunca ihlal etmiştir. Bu doğrultuda Rus uçağı Türk jetlerinin müdahalesi ile düşürülmüş ve bu durum iki ülke arasında krize neden olmuştur. Dolayısıyla Türkiye'nin bu müdahalesinden sonra Rusya resmi olarak soğuk savaş ilan edercesine hızlı bir biçimde birçok sosyal, siyasi ve ekonomik yaptırımları devreye sokmuştur. Bu doğrultuda Rusya Hükümeti, Türkiye'ye yönelik özel tedbir kararları almıştır. Rusya'nın aldığı bu kararlardan bazıları iki ülke arasında sefer sayısı uçuşlar dışındaki charter seferlerinin tamamının askıya alınmasıdır. Ayrıca Rusya tur operatörlerinden Türkiye'ye tur satmamaları talimatını vermiştir (Yenişehirlioğlu, Salha ve Şahin, 2016: 77-78). Nitekim bu durumun sonucunda Türkiye Kültür ve Turizm Bakanlığı verilerine göre; Türkiye'yi ziyaret eden yabancı turistler arasında Rus turist oranının ortalamanın üstünde olması, ülke turizm gelirlerinin 2015 yılında % 8,2 azalmasına neden olmuştur. Bu bağlamda Rusya Federasyonu'nun vatandaşlarına, Türkiye'ye yapacakları seyahatler konusunda basında yayınlanan olumsuz görüşleri, Rus turistlerin tercihlerinde değişikliğe neden olmuştur. 2015 yılında Türkiye'ye 41,6 milyon turistin geldiği ve bu rakamın 3,7 milyonunun (% 10,07) Rus turistlerden oluştuğu kayıt altına alınmıştır. Aynı yılda yabancı turist başına ortalama harcama 715 dolar olarak tespit edilmiştir. Rus turistlerin bıraktığı döviz gelirinin yaklaşık 3 milyar dolar olduğu açıklanmıştır (T.C. Kültür ve Turizm Bakanlığı, 2018).

Tablo-4. 2010-2018 Yılları Arası Türkiye'ye Gelen Rus Turist Sayıları (Kültür ve Turizm Bakanlığı, TÜİK)

IL	RUS TURİST SAYISI
2010	3.107.043
2011	3.468.214
2012	3.599.925
2013	4.269.306
2014	4.479.049
2015	3.649.003
2016	866.256
2017	4.715.438
2018	5.964.613

Tablo 4'de görüldüğü üzere 2010-2018 yılları arası Türkiye'ye gelen Rus turist sayısında 2015 yılında 2014 yılına oranla yaklaşık bir milyonluk düşüş yaşanmıştır. 2016 yılında Türkiye'yi ziyaret eden Rus turist sayısında önceki yıla göre yaklaşık %77 düşüş gerçekleşmiştir. İlerleyen yıllarda iki ülke arasında sorunların ortadan kaldırılması ile birlikte ülkeyi ziyaret eden Rus turist sayılarında önemli artış yaşanmıştır. Bu durum, yaşanan terör olaylarının yanı sıra, siyasi krizlerin de turistik destinasyonların tercih edilmesinde etkili olduğunu göstermektedir.

Turistik bölgelerde meydana gelen terör saldırıları, 6 aydan 1 yıla kadar tekrarlanmadığı takdirde turizm sektörü kendini yenilemektedir. Dolayısıyla dünya genelinde yaşanan olumsuz gelişmelere rağmen uluslararası turizm hareketleri süreklilik arz etmektedir (Arana ve Leon, 2008: 311). Nitekim Türkiye'nin terörle mücadele yapmış olduğu başarılı çalışmalar ve turizm konusunda yürütmüş olduğu politikalar neticesinde 2017 yılında turizmde hızlı bir ivme kazanmış ve bu yılda ülkenin uluslararası ziyaretçi sayıları ve turizm gelirleri ciddi miktarlarda artmıştır.

Türkiye'nin en fazla turist gelen şehir sıralamasında 3.sırada olan Muğla'da 412 kişi üzerinde anket yapılmıştır. Yapılan ankette turistlerin güvenlik açısından bir sorunla karşılaşma durumları sorulmuş % 44'ü sorun yaşadığını % 56'sı sorun yaşamadığını belirtmiştir. Sorunların çözümlenme durumu sorulduğunda % 52'si çözüldüğü % 39'u kısmen çözüldüğünü % 9'u ise sorunun çözülmediğini ifade etmiştir. Turistlere tatilleri boyunca güvenlik açısından sorun yaşayıp yaşamadığı sorulmuş % 60'ı sorun yaşarken % 12'si sorun yaşamadığını % 28'i ise emin olmadığını belirtmiştir (Bayhan ve Ünlüönen, 2016, s.10-11).

Seyahat edilecek ülkenin döviz girişine sınırlamalar getirmesi, kolluk kuvvetlerinin kontrollerinin gerek hava alanında gerekse sokaklarda fazla olması, turizm sektörünü olumsuz etkileyebilmektedir. Turistlerin güvenliği konusunda yapılan çalışmalar arttırılmalı ve çeşitlendirilmelidir. Ancak bu çalışmalar, turistlerin huzurunu ve keyfini kaçıracak boyuta ya da özgürlüğünü kısıtlayacak şekilde yapılmamalıdır. Güvenlik konusunda sorunla karşılaşan grubun % 90,8'inin sorununun çözümlendiğini söylemesi bu noktada önemli bir veridir. Unutulmamalıdır ki, güvenlik algısı güvenlik olgusuyla sınırlı değildir. Güvenlik algısında, yapılan çalışmaların turistik tüketicilere ulaşması ve onlar tarafından görünürlüğü de önemlidir.

SONUÇ

Turizm sektörünün ülke ekonomileri için sağladığı değer ve fayda her geçen gün daha fazla artmaktadır. Güvenlik ve güvenlik algısı turistik bölgelerin seçiminde etkili olan en önemli faktörler arasındadır. Turistlerin büyük bir kısmı fiyatların uygunluğu veya destinasyonların özelliklerinden ziyade, gidecekleri yerlerin güvenliğine öncelik vermektedir. Şiddetli çatışmalar yaşanan veya yoğun suç işlenen destinasyonlar, olumsuz güvenlik algısı oluşturmaktadır. Algılamalar, tutumlara dönüşebileceği için ülkeler, turizm talebinde psikolojik bir belirleyici olan algı konusuna önem vermektedirler.

Kendi konutunun bulunduğu yer dışında seyahat eden ve geçici olarak konaklayan insanın, güvenlik de içinde olmak üzere tüm gereksinimlerini en iyi biçimde karşılanması, onun seyahat ve konaklamadan beklediği manevi zevkin en üst seviyede gerçekleşmesi, turizmden beklenen bütün yararlardan önce geldiği ve turizmi koşullandırdığından dolayı gerekli özen gösterilmelidir.

Türkiye'de son yıllarda genel güvenlik ve turizm güvenliği konusunda ciddi adımlar atılmış ve Türkiye'ye olumlu bir görüntü sağlanmaya çalışılmıştır. Güvenlik konusunda, turistleri rahatsız etmemek koşuluyla, halkla ilişkiler çalışmaları yapılmalıdır. Turistlere onların güvenliği ile ilgilenildiği hissettirmek için güvenlikleri amacıyla alınan tedbirlere yönelik küçük bilgilendirmeler yapılabilir, sağlanan başarılı sonuçlar paylaşılarak güvenlik konusunda haklarının korunduğu gösterilebilir.

Türkiye'de güvenlik ortamının sağlanarak korunması ve turizmde güvenlik algısının sürekli olarak sağlanması birtakım önlemler alınmalıdır. Bunları şu şekilde sıralayabiliriz:

- Turiste sunulan güvenlik hizmetleri standartlaştırılmalı,
- Turizm alanında görevlendirilecek personel, mesleki olarak yetiştirilmeli, turizm bilinci ve eğitim düzeyi yükseltilmeli,
- Turizm destinasyonlarında yabancı dil bilen turizm sosyolojisi ile psikolojisine hakim turizm polisleri ve turizm jandarması istihdam edilmeli,
- İlgili tüm kişi, kurum ve kuruluşlarla, merkezi otorite, yerel kuruluşlar, güvenlik birimleri, turizm kurumları, yerli halk ve turistler arasında güvenlik konusunda iş birliği ve koordinasyon sağlanmalı,

- Güvenli bir ortamın oluşturulabilmesi için işsizliği ve gelir dağılımındaki adaletsizliği önleyici tedbirler alınmalı
- Güvenliği tehdit eden trafik kazalarının önlenmesi amacıyla, sürücüler eğitilmeli ve trafik kurallarına uymalarını sağlayıcı tedbirler alınmalı,
- Terör suçlarına karşı uluslararası iş birliğine gidilerek, mücadelenin sürekliliği sağlanmalı
- Türkiye'ye karşı oluşan olumsuz havanın giderilmesi için Başbakanlık – Dışişleri Bakanlığı, Kültür ve Turizm Bakanlığı, TOBB ve STK'lar tarafından tanıtım kampanyaları düzenlenmelidir.
- Özellikle tüm ziyaretçilerin ve turizm işletmelerinin denetimleri bölge/ülke imajına zarar vermeyecek şekilde arttırılmalı,
- Güvenlik zafiyeti gösteren işletmelerin tespiti noktasında gerekli cezai işlemler ağırlaştırılmalı,
- Alınacak önlemlerin tahminlerini kolaylaştırmak için dokümantasyon ve kayıtlar sağlıklı tutulmalı,
- Turistik tesislerin işletilmesine yönelik yasa dışı müdahaleler karşısında turistik tesislerin alabileceği önlemlere ilişkin rehber ilkeler konulmalı,
- Turizm bölgelerinde terör eylemlerinin önlenmesi ve tespit edilmesi için güvenlik görüntüleme sistemlerinin yüksek çözünürlük ve gece görüş sistemli olması, mümkünse yüz tanıma sistemlerine entegreli olacak şekilde düzenlenerek elde edilen anlık görüntülerin düzenli olarak kontrolü sağlanmalı,
- Pazarlama stratejileri daha az duyarlı hale getirilerek, terör saldırıları sonrası hedef alınan pazarların daha hızlı düzelme sürecine girmesi için çalışmalar yapılmalı,
- Kriz ve acil eylem planları turizm işletmelerinde etkin hale getirilmelidir.

KAYNAKÇA

Arana, E. Jorge ve Leon, C. L. (2008), "TheImpact Of Terrorism", *Annals Of Tourism Research,* 35(2), 299–315.

Bahar Ozan, Kozak Metin (2012). *Turizm ve Rekabet*, Detay Yayıncılık, Ankara.

Bahar, O. (2007, Güz). Bölgesel Kalkınmada Turizm Sektörünün Ekonomik Açıdan Yeri ve Önemi, *Muğla Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* (19), 1-19.

Bayhan, İ. ve Ünlüönen, K. (2016). Turist Tercihlerinde Güvenliğe İlişkin Tutumlarının Etkisi, *Elektronik Sosyal Bilimler Dergisi,* 15(56), 1-20.

Çımat, A. ve Bahar, O. (2003). Turizm Sektörünün Türkiye Ekonomisi İçindeki Yeri ve Önemi Üzerine Bir Değerlendirme, *Akdeniz İ.İ.B.F. Dergisi* (6), 1-18.

Drakos, K. ve Kutan M.A. (2001). *Regional Effects of Terrorism on Tourism: Evidence from Three Mediterranean Countries,* Working Paper.

Eralp, Z. (1983). *Genel Turizm*, Ankara Üniversitesi Yayın, Ankara.

Kar, M., Zorkirişçi, E. ve Yıldırım, M. (2004). Turizmin Ekonomiye Katkısı Üzene Ampirik Bir Değerlendirme, *Akdeniz İ.İ.B.F. Dergisi*. 4(8), 87-112.

Kaşlı, M. ve İlban, M. O. ve Şahin, B. (2009). Modern Pazarlama Stratejileri: AB ve Türk Turizmi, *Elektronik Sosyal Bilimler Dergisi,* 8 (27), 79-98.

Kılıç, Ö. (2000). Terörün Türk Turizmine Etkileri, *I. Milletlerarası Doğu ve Güneydoğu Anadolu'da Huzur ve Güvenlik Sempozyumu*, Elazığ.

Kızılkaya, A. ve Sönmez, N. (2003). Geçmişten Günümüze Güvenlik İhtiyacı ve Türk Polis Teşkilatı, *Çağın Polisi Dergisi,* (18), 19-23

Koyunoğlu S. (2003). *Turist Sağlığı*, Ankara, Detay Yayıncılık.

Kozak N., Kozak M. ve Kozak M. (2001). *Genel Turizm İlkeler- Kavramlar,* Ankara, Detay Yayıncılık.

Kozak, M. (2013). *Sürdürülebilir Turizm*, Ankara, Detay Yayıncılık.

Kuveloğlu, D. (2004), *Turizm@gelecek.tr*(1.Baskı). İstanbul, Elips Kitap.

McIntosh, R.W., *Goeldner, C.R. ve Ritchie, J.R.B., Tourism Principles, Practices, Philosophies (7th edition*). New York: JhonWiley&Sons, Inc, 1995.

McSweeny B. (1999*) Identity and Interests: A Sociology of International Relations,* Cambridge University Press, Port Chester, NY., USA.

Oktayer, N., Susam, N. ve Çak, M. (2007). *Türkiye'de Turizm Ekonomisi,* İstanbul, İstanbul Ticaret Odası.

Ozan, B. ve Özcan, Ö. (2018). Turizm Sektöründe İstihdam Edilen Gençlerin Meslek Algıları ve İş Doyum Performanslarının Değerlendirilmesi, *Uluslararası Toplum Araştırmaları Dergisi*, C:8 Yıl:8 s.263-298.

Seçilmiş, C. (2009) Turistlerin Kişisel Değişkenlerinin Güvenlik Algılamalarındaki Rolü, *Elektronik Sosyal Bilimler Dergisi*, (8), 152-166.

Sivri, U. (2010). Şokların Yabancı Ziyaretçi Sayısı ve Yabancı Ziyaretçi Harcamaları Üzerindeki Etkisi Kalıcı Mıdır? *TİSK Akademi*, 5(10), 220-237.

Somuncu, M. (2004). Turizmin Kalkınmaya Etkisi ve Türkiye Turizmindeki Bölgesel Farklılıklar, *Ankara Üniversitesi Türkiye Coğrafyası ve Araştırma ve Uygulama Merkezi IV. Ulusal Coğrafya Sempozyumu*, 161-178.

Subaşı, E. (2007). *Turizm Güvenliği Alanında Kolluğun Yeniden Yapılanması: Muğla Turizm Jandarması Örneği* (Yayımlanmamış Yüksek Lisans Tezi). Muğla Sıtkı Koçman Üniversitesi, Muğla.

Şen, A. ve Şit, M. (2015, Mayıs). Turizm Gelirlerinin Türkiye Ekonomisindeki Rolü ve Önemi, *Dicle Üniversitesi İktisadi ve İdari Bilimler Fakültesi, 8(8), 30-45.*

Uysal, D., Erdoğan, S. ve Mucuk, M. (2003). Türkiye'de Turizm Gelirleri ile Ekonomik Büyüme Arasındaki İlişki (1992-2003). *SÜ İBBF Sosyal ve Ekonomik Araştırmalar Dergisi*, 4(8) 163-170.

Yenişehirlioğlu, E., Salha, H. ve Şahin, S. (2016). Politik krizlerin turizm talebi üzerindeki etkisine yönelik bir araştırma: Rusya'nın değişen yüzü ve bu değişimin Türkiye turizmine etkileri, *Balkan ve Yakın Doğu Sosyal Bilimler Dergisi*, 02(03), 74-83.

Yılmaz, B. S. ve Yılmaz, D, Ö. (2005). Terörizm ve Terörizmin Hedefi Olarak Turizm Endüstrisi, *Elektronik Sosyal Bilimler Dergisi*, 4(13), 39-58.

TERÖRLE VE DİĞER SUÇLARLA MÜCADELEDE KOLLUĞUN SOSYAL MEDYA KULLANIMININ DEĞERLENDİRİLMESİ[*]

Mehmet KAPLAN[**]

Öz

Sosyal medya; düşüncelerin, fikirlerin, deneyimlerin, durumların resim, mesaj ve video gibi iletişim yöntemleri ile paylaşıldığı, internet tabanlı bir mecradır. Sosyal medyada, medya ve kullanıcıları arasında bir sınır olmadığı için herkes görüşlerini, fikirlerini, bilgilerini paylaşarak katılım sağlar, katkı yapar ve geri bildirimde bulunur. Bu nedenle kolaylıkla sosyal hareketler planlanarak başlatılır ve yönetilebilir. Sosyal medyanın böyle bir mecra olmasının birçok faydasının yanında güvenlik açısından sakıncaları da mevcuttur. Çünkü paylaşımlar kaynağın amacına yönelik olarak içerisinde zararlı içerikleri de barındırabilmektedir. Özellikle zararlı bilgilerin belli bir denetim süzgecinden geçirilmeksizin paylaşılmasına aracılık etmesi nedeniyle, toplumsal düzen, istikrar ve güvenlik açılarından büyük riskler de taşımaktadır. Teröre karşı mücadelede teknolojinin etkin kullanılması, hak ve özgürlüklerde, güvenlik adına yapılan sınırlandırmaları azaltabilir. Son dönemlerde gelişen teknoloji ile sosyal medya, kolluk kuvvetlerince de etkin olarak kullanılmaya başlanmıştır. Ülkemizde geçmişte terör örgütleri ve suçla mücadelede kolluk kuvvetleri tarafından internet ve sosyal medyanın kullanımı reaktif bir anlayışla yürütülürken günümüzde ise proaktif anlayışa doğru bir yönelme başlamıştır.

Bu çalışmada terörle ve suçla mücadelede sosyal medyanın kolluk tarafından kullanılma şekli ile ilgili mevcut durum ortaya konulmuştur. Suçla mücadele etmede ve suçluların tespitinde sosyal medyanın kullanılmasındaki eksiklikler ve ihtiyaçlar nitel araştırma yöntemleriyle incelenmiştir. Görüşme yöntemine, özellikle jandarma ve polis teşkilatlarında bilişim suçları ile mücadele kısımlarında çalışan veya çalışmış kişiler dâhil edilmiştir. Elde edilen veriler betimsel analiz metodu ile analiz edilmiştir. Bu çalışma sonucunda elde edilen bilgiler, genel kolluğu oluşturan polis ve jandarmanın terör ve suçla mücadelede sosyal medyayı daha etkin kullanmasına ışık tutabilecektir.

Anahtar Kelimeler*: *Sosyal Medya, Terör, Suç, Jandarma, Polis,

EVALUATIONS OF THE SOCIAL MEDIA USE BY LAW ENFORCEMENT IN COMBATING TERRORISM AND THE OTHER CRIMES

Abstract

Social media is an internet-based medium where thoughts, ideas, experiences, situations are shared with communication methods such as pictures, messages and videos. Since there is no limit between media and users on social media, everyone participates, contributes and gives feedback by sharing their opinions, ideas and information. Therefore, social movements can be easily planned, started and managed. In addition to many benefits of social media being such a medium, there are security drawbacks in many respects as well because the shares may contain harmful contents depending on the aim of the source. It

[*] Bu çalışma 19-20 Eylül 2019 tarihinde Jandarma ve Sahil Güvenlik Akademisi, Güvenlik Bilimleri Enstitüsünde icra edilen Uluslararası Güvenlik Kongresinde sunulan bildirinin genişletilmiş halidir.

[**] Dr. Öğretim Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, Fakülte Dekanlığı, mehmetkaplan278@hotmail.com, ORCID: 0000-0002-1064-0312

Makale Geliş Tarihi: 04.11.2019 Makale Kabul Tarihi: 06.02.2020

also carries great risks in terms of social order, stability and security, especially as it mediates the sharing of harmful information without passing through a certain audit. Effective use of technology in the fight against terrorism may reduce the limitation regarding the rights and freedom. Thanks to the recently developing technology social media has started to be used effectively by law enforcement agencies. While the use of internet and social media in the fight against crime and terrorist organizations by law enforcement agencies were carried out with a reactive understanding in the past, a trend towards proactive understanding has started in our country recently.

In this study, the current situation regarding the use of social media by law enforcement agencies in the fight against crime including terrorism was revealed. The deficiencies and needs in the use of social media in the fight against crime and in the detection of criminals were examined through qualitative research method. People who had worked or are still working on cyber-crimes in gendarmerie and police organizations were included in the interview of this study. The data was analyzed with descriptive analysis method which is among the qualitative research methods. The results of this study may shed light on the use of social media in the fight against terrorism and crime by the police and gendarmerie.

Keywords: *Social Media, Terror, Crime, Gendarmerie, Police.*

GİRİŞ

Medya, iletişim için bilgisayar ve benzeri diğer mobil cihazların internet üzerinden etkileşimli bir şekilde kullanılmasıyla yeni medyaya dönüşmüştür ve yeni medya internetin bu tarz iletişim gücünü anlatmak için kullanılan bir kavram haline gelmiştir. Yeni medya bu gücü özellikle sosyal medya programları aracılığıyla sağlamaktadır.

Günümüzde bilgiye erişimi ve bilgi paylaşımını kolaylaştırması, olgu, olay ve bilgilerle ilgili tartışma ortamı oluşturabilme ve grup kurma olanağı sunması, üçüncü kişilerin konuyla ilgili paylaşımları anlık takip edebilmesi ve bunlara kendilerinin de katılabilmesine imkân sağlaması gibi özellikleriyle sosyal medya kamuoyu oluşturmada en önemli araçlardan birisi haline gelmiştir. Hatta daha da önemlisi sosyal hareketlerin planlandığı, organize edildiği, başlatıldığı ve yönetildiği alanlara dönüşmüştür. Böylelikle birey, toplum ve devlet otoritesi içerisinde, aktif bir konuma sahip olmuştur. Cildan ve diğerleri (2012: 2), sosyal medyanın demokrasi algısını ve uygulamasını, temsili demokrasiden katılımcı (doğrudan) demokrasiye doğru dönüştürme gücüne ve imkânına sahip olduğunu ifade etmişlerdir. Özellikle Facebook ve Twitter gibi sosyal ağlar, kullanıcılarına tanışma ve mesajlaşmanın ötesinde, organizasyon kurma, organize olma, bilgi ve fikir paylaşma, inanç ve düşünceler etrafında gruplaşma imkânlarını da vermiştir (Boyd ve Ellison, 2008: 213).

Sosyal medyanın ortaya çıkmasıyla eşik bekçiliği[1] yapan ve gündem belirleyen ana akım medya kuruluşlarının hegemonyası kırılmaya başlamıştır. Eren ve Aydın, (2014) medyanın içeriğini üreten ve medyayı izleyen arasındaki katı ayrımın ortadan kalktığını, gerçeklerden ziyade fikirlerin önem kazanmaya başladığını ifade etmektedir. Geleneksel medyanın hükümetler tarafından kontrol edilebilir ve sansürlenebilir olması, yayın yasağı konabilmesi sebebiyle, terör örgütleri sosyal medyayı daha fazla tercih eder duruma gelmiştir.

Bu tercih sebeplerinden birisi de sosyal medya ile internet ortamındaki yaşanan gelişmedir. Bilginin işlenmesi yönünden, tek yönlü paylaşımların oluşturduğu ve Web 1.0[2] olarak adlandırılan internet ortamı dönüşüme uğrayarak Web 2.0[3] denilen ve kullanıcılara internet içeriklerine yorum, bilgi ekleme ve değiştirme olarak katkıda bulunabilme imkânı sağlayan ortama dönüştüğü bilinmektedir. Bu süreçte bloglar ve sözlük siteleri sosyal medyanın ilk ürünleri iken zamanla video, ses, zaman, mekân, düşünce ve durum paylaşımının yapıldığı blogların ortaya çıkması ile internet ortamının büyük bölümünü kapsar hale gelmiş ve her geçen gün üye sayılarını arttırarak daha geniş kitlelere erişebilmektedir. Dünyada sosyal medya kullanımının 2014 Mayıs tarihinden günümüze kadar yaşadığı gelişim Tablo 1.'de olduğu gibidir.

2019 Ocak tarihli rapora göre Dünya nüfusunun %57'sini oluşturan 4,388 milyar insan internet kullanırken %45'ini oluşturan 3,484 milyar insan aktif olarak sosyal medya kullanmaktadır. Türkiye'de ise nüfusun %72'si internet kullanmaktadır. Her yıl %9,3 (5.027.251 kişi) oranında internet kullanımı artmakta olup artış hızı bakımından dünyada 14. sıradadır. Nüfusun %63'ü (51 milyon kişi) ise aktif olarak sosyal medyayı kullanmaktadır. (https://wearesocial.com/).

[1] Eşik Bekçiliği (Gatekeeper): Medyanın, haber, yorum, görsel gibi yayınlayacakları içerikleri ekonomi politiğine, yayın kimliğine ve yayın politikasına uygun olarak seçerek yayınlaması, istemediği nitelikteki içerikleri ise yayınlamaması anlamına gelen bir iletişim kuramıdır.

[2] Web 1.0 web sayfalarından oluşan World Wide Web'in ilk aşamasına atıfta bulunmaktadır. Kullanıcılar internet sitelerini ziyaret eder, almak istediği bilgiyi alır ve siteden gider. Yani içeriğe katkıda bulunma veya özgün içerik üretme gibi bir imkânı söz konusu değildir. (www.bilimcag.com/)

[3] Web 2.0 önceden içerik sağlayıcıların istemcilere cevap vermesi biçiminde tek yönlü işleyen İnternet ortamının biçim değiştirmesi ve tüm istemcilerin aynı zamanda içerik sağlayıcı olabilmesi imkânının sağlanmasıdır. En önemli temsilcileri facebook, flickr gibi sosyal paylaşım ağları, youtube, google video gibi görüntü paylaşım siteleridir. (www.bilimcag.com/)

Tablo-1. Dünyada Sosyal Medya Kullanım Sayıları[4]

Sırası	Sosyal Ağ	2014 Yılı (Mayıs) Üye Sayısı	Sosyal Ağ	2019 Yılı (Ocak) Üye Sayısı
1	Facebook	900.000.000	Facebook	1.500.000.000
2	Twitter	310.000.000	Youtube	1.499.000.000
3	LinkedIn	255.000.000	Twitter	400.000.000
4	Pinterest	250.000.000	Instagram	275.000.000
5	Google Plus	120.000.000	LinkedIn	250.000.000
6	Tumblr	110.000.000	Reddit	125.000.000
7	Instagram	100.000.000	VK	120.000.000
8	VK	80.000.000	Tumblr	110.000.000
9	Flickr	165.000.000	Pinterest	105.000.000
10	Myspace	42.000.000	Google Plus	100.000.000

45 ülkede hizmet sağlayan GlobalWebIndex'in 2019 yılı sosyal medya raporuna göre 2012 yılından itibaren insanların günlük internet kullanım sürelerini gösteren bilgiler Tablo 2.'de verilmiştir. Buna göre Türkiye 3 saat 5 dakika ile 13. sırada yer almaktadır. Türkiye'de insanlar %56 oranında gündemi takip edebilmek için sosyal medyadan haber ve olayları izlemekte ve bu kategoride Filipinler, Malezya ve Tayland'ın ardından dünyada 4. sırada yer almaktadır.

Bu verilerden, dünya genelinde internet ve buna paralel olarak sosyal medyanın kullanım oranlarının hızlı bir şekilde artmakta olduğu anlaşılmaktadır. Önümüzdeki süreçte bu gelişim hızı ile devam etmesi durumunda dünya üzerindeki insanlara internet ile erişilebilirlik oranları %90'ları bulacaktır. Bu bize kitle iletişiminde sosyal medyanın gücünü açık bir şekilde göstermektedir.

[4] Veriler www.ebizmba.com/ sitesinden temin edilmiştir.

Tablo-2. 2012- 2019 Yılları Arası Ülkelere Göre Günlük İnternet Kullanım Süreleri (www.globalwebindex.com).

	2012	2013	2014	2015	2016	2017	2018	2019
Philippines	2:49	3:06	3:25	3:41	4:07	4:00	4:08	**4:01**
Brazil	2:41	2:40	2:50	3:18	3:45	3:40	3:39	**3:45**
Colombia	-	-	-	-	-	-	3:34	**3:36**
Nigeria	-	-	-	-	-	3:03	3:26	**3:36**
Argentina	2:42	2:49	2:50	3:13	3:31	3:12	3:17	**3:27**
Indonesia	2:12	2:21	2:26	2:50	3:02	3:26	3:23	**3:15**
UAE	2:21	2:29	2:48	3:01	3:24	2:56	3:00	**3:11**
Mexico	2:35	2:50	2:53	3:14	3:33	3:11	3:14	**3:10**
South Africa	1:58	2:07	2:16	2:42	2:50	2:47	2:58	**3:10**
Egypt	-	-	-	-	3:17	3:06	3:05	**3:06**
Kenya	-	-	-	-	-	2:50	2:59	**3:06**
Saudi Arabia	2:23	2:18	2:35	2:55	2:56	2:38	2:52	**3:06**
Turkey	1:56	2:17	2:25	2:34	2:57	2:49	2:52	**3:05**
Ghana	-	-	-	-	-	2:59	3:09	**3:03**
Malaysia	2:39	2:53	2:48	2:59	3:18	3:06	3:03	**3:01**
Thailand	1:59	2:34	2:41	2:49	2:46	3:06	3:14	**2:51**
Romania	-	-	-	-	-	-	2:34	**2:28**
Russia	1:40	1:46	1:49	1:52	2:17	2:20	2:21	**2:28**
India	1:44	1:57	2:03	2:15	2:30	2:25	2:28	**2:25**
Morocco	-	-	-	-	-	2:22	2:34	**2:23**
Vietnam	1:47	1:57	2:07	2:16	2:34	2:36	2:33	**2:23**
China	1:19	1:17	1:24	1:27	1:45	1:58	2:00	**2:19**
Portugal	-	-	-	1:54	2:13	2:13	2:12	**2:18**

	2012	2013	2014	2015	2016	2017	2018	2019
Singapore	1:12	1:29	1:36	1:38	1:58	2:07	2:11	**2:10**
USA	1:22	1:34	1:40	1:43	2:04	2:02	2:05	**1:57**
Hong Kong	1:34	1:26	1:27	1:29	1:39	2:00	1:53	**1:52**
Ireland	-	1:24	1:11	1:22	1:38	1:45	1:55	**1:51**
Sweden	1:13	1:13	1:22	1:33	1:37	1:54	1:49	**1:51**
Taiwan	1:28	1:30	1:41	1:50	2:03	2:06	1:52	**1:51**
UK	1:11	1:14	1:19	1:29	1:42	1:54	1:51	**1:50**
Canada	1:12	1:29	1:29	1:27	1:41	1:48	1:47	**1:49**
Poland	1:02	1:12	1:13	1:17	1:40	1:42	1:45	**1:47**
Italy	1:33	1:49	1:47	1:58	2:02	1:53	1:48	**1:46**
Australia	1:15	1:13	1:11	1:10	1:36	1:39	1:34	**1:43**
New Zealand	-	-	-	-	1:43	1:49	1:42	**1:43**
Spain	1:30	1:30	1:26	1:38	1:43	1:38	1:41	**1:43**
Denmark	-	-	-	-	-	-	1:35	**1:33**
France	1:01	1:05	1:11	1:17	1:23	1:24	1:22	**1:28**
Belgium	-	-	-	1:15	1:33	1:31	1:31	**1:24**
South Korea	0:47	0:47	0:58	1:05	1:04	1:11	1:11	**1:20**
Netherlands	0:56	0:59	1:02	1:10	1:16	1:24	1:17	**1:18**
Switzerland	-	-	-	-	-	1:18	1:19	**1:18**
Austria	-	-	-	-	-	1:16	1:15	**1:17**
Germany	0:58	1:04	1:04	1:08	1:07	1:13	1:08	**1:15**
Japan	0:23	0:18	0:17	0:20	0:33	0:46	0:40	**0:45**

Eren ve Aydın'ın (2014) çalışmalarında ifade ettikleri gibi sosyal medyanın özgürlük alanının bu kadar geniş olması birçok bakımdan iyi olduğu gibi birçok bakımdan da sakıncalar içermektedir. Çünkü hassasiyet arz eden konularda ve insanların yanlış veya kasıtlı yönlendirilmeye müsait olduğu durumlarda ortaya çıkan bilgi kirliliği, kişilere ve topluma zarar verebilecek durumlara yol açabilir. Sosyal medyada dolaşan haberlerin doğru olup olmadığını normal vatandaşın anlık olarak tespit edebilmesi mümkün değildir. Gerçek dışı veya yönlendirilmiş bilginin elde edilmesinden sonra bu insanlara doğru bilgiyi gösterebilme olanağı çok azalmakta, bu olanak sağlansa bile ilk bilginin etkisini azaltmak veya yok etmek imkânsız hale gelebilmektedir. Bu bilgilerle harekete geçen kitleleri durdurmak ya da onlarla sağlıklı iletişim geliştirmek de oldukça zorlaşmaktadır. Bilerek veya

bilmeyerek, insanlar sosyal medya aracılığıyla yalan veya yanlış bilgileri paylaşarak, kamuoyunda büyük bir bilgi kirliliği ve dezenformasyon oluşturmaktadır. Burada bahsedilen hususların en güncel örneği İstanbul Gezi Parkı eylemlerinde karşımıza çıkmıştır. İstanbul Gezi Parkı olayları 28 Mayıs 2013 tarihinde başlamış, sosyal medya aracılığıyla kısa sürede başta Ankara, İzmir gibi büyükşehirler olmak üzere Türkiye'nin diğer illerine de yayılmıştır. Protestocular eylemlerini duyurma ve organize etmede, toplumu yönlendirmede Facebook ve Twitter başta olmak üzere birçok sosyal medya aracını etkin olarak kullanmışlardır.

"#OccupyGezi ve #DirenGeziParki adlı hashtag[5] formatları oluşturulmuştur. 31 Mayıs günü akşam 16:00'dan itibaren 12 saat boyunca konu ile ilgili 3 ana hashtag grubu için 2 milyon tweet atılmıştır. Bunların 950.000'i #direngeziparkı, 170.000'i #occupygezi ve 50.000'i #geziparki'dir. Gezi parkında bekleyenlerin kalabalıklaşmasında ve benzer protestoların çeşitli şehirlere yayılmasında sosyal medyanın etkisi görülmüştür" (Barbera ve diğerleri, 2003).

Ayrıca Avrupa'da da son dönemde benzer olaylar yaşanmıştır. Fransa'da yaşanan sarı yeleklilerin gösterileri; "15 Mayıs 2011'de İspanya'nın 50 farklı şehrinde eş zamanlı olarak başlatılan ve **"(Indignados)** öfkeliler" olarak anılan grupların eylemleri sosyal medya üzerinden örgütlenip yönetilmiştir" (Eren ve Aydın, 2014). Özellikle Kuzey Afrika ile Ortadoğu ülkelerini kapsayan Arap Dünyasında baş gösteren mitingleri, protestoları, ayaklanmaları ve silahlı çatışmaları ifade eden Arap Baharı, sosyal medyanın kitleler üzerindeki gücünü en iyi şekilde ortaya koymuştur.

Sosyal Medyanın büyük kısmını oluşturan Facebook, Twitter ve Youtube gibi firmalar Tablo-1.'den de anlaşılacağı üzere, özellikle akıllı telefon teknolojisiyle daha geniş kitlelere ulaşma imkânı ve kullanım alanı bularak, pazar paylarını artırmaktadır. "Sosyal medya, güçlü ülkelere diğerlerine karşı, özellikle istihbarat elemanları ve lobiler aracılığıyla eskisinden daha masrafsız ve daha az riskle müdahale olanağı sunmaktadır. Bu amaçla dünyanın herhangi bir yerinden internet üzerinden istenilen provokasyonu başlatmak, sürdürmek ve yönetmek kolaylaşmıştır" (Eren ve Aydın, 2014). Bazı durumlarda ise sosyal medya firmaları

[5] Sosyal medya kullanıcılarının vazgeçilmez aracı haline gelen hashtag twitter'la birlikte birçok sosyal medya platformuna dâhil olmuş ve hedef kitlelere daha rahat ulaşabileceğimiz bir araç haline gelmiştir. Hashtag adı verilen "#" diyez işareti; sosyal medyadaki postların daha kolay aranmasını sağlamak için veya belirli bir konudan bahseden bir tweeti etiketlemek için kullanılır. (www.onedio.com)

olayların büyümesini veya gidişatını çeşitli sınırlamalarla engelleyebilmektedir. Örneğin Fransa'daki Sarı Yeleklilerin gösterilerinin şiddetini artırmasıyla "Sarı Yeleklilerin yoğun şekilde kullandığı Facebook mecrası da ilk zamanlardakine oranla tavrını değiştirerek aktif hesapları askıya almaya başlamış" (Özkır, 2018) ve olaylara Fransa Hükümeti lehine müdahalede bulunmuştur.

Sosyal medya bu kadar hızlı gelişerek ve dünyayı kapsayarak gündem belirlemede çok etkin bir araç haline gelmiştir. Bu gelişen duruma ayak uydurabilmek adına kolluk birimleri de teşkilatlanmalarını değiştirerek sosyal medya birimleri oluşturmuştur. Bu birimler iki farklı boyutta görev yapacak şekilde oluşturulmuştur. Birinci boyutta oluşturulanlar kolluk teşkilatının Halkla İlişkiler ve Tanıtım hedeflerine yönelik çalışmaktadırlar. Diğer boyutta oluşturulanlar ise suçla mücadeleye yönelik görev yapmaktadırlar. Özellikle ilk dönemlerde sosyal medya *açık kaynak istihbaratı*[6] amacıyla yoğunluklu olarak kullanılmıştır. Geleneksel gizli yöntemlerin riskli, maliyetli ve zaman alan işlem olması; açık kaynaktan bilgi temininin daha kolay, daha ucuz, daha güvenilir olması ve sosyal medyanın açık kaynak istihbaratında payının artmasına neden olmuştur. Daha sonraki dönemde ise sosyal medya birimleri oluşturularak sosyal medya üzerinde önleyici ve adli kolluk faaliyetleri yürütülmeye başlanmıştır.

Bu çalışmada "Kolluğun terör ve diğer suçlarla mücadelede sosyal medyayı kullanım durumu nedir ve bu durumu daha iyi bir seviyeye getirmek için neler yapılmalıdır? sorularına cevap aranması amaçlanmıştır. Bu sorular minvalinde kolluğun sosyal medyadan faydalanarak suçla mücadele etmesindeki mevcut durumu kişisel, kurumsal ve teknolojik bazda ortaya koyarak, eksiklikleri tespit etmek, personel malzeme ve yöntem ihtiyaçlarını belirlemeye çalışarak kolluğa bu alanda katkı sunmaktır. Böylelikle kolluğun suçla mücadele ederken sosyal medya kullanımı konusunda daha proaktif olmasına katkı sağlanabilecektir.

Bu kapsam doğrultusunda çalışmamızda ilk olarak alanda yapılmış araştırmalar ele alınacak ve bir değerlendirme yapılacaktır. Sonra araştırmamızın modelini, örneklemini ve evrenini, veri toplama yöntemi ile analizini içeren yöntemi ifade edilecektir. Bulgular kişisel, kurumsal ve teknolojik temalar altında değerlendirilerek sonuç kısmı oluşturulacaktır.

[6] Açık kaynak istihbaratı herkese açık olan bilgi kanallarından araştırılarak, durumsal farkındalık ile elde edilen ham verilerin çeşitli işlemlerden geçirilerek istihbarat bilgisi haline getirilmesidir.

1. ALANYAZIN

Küreselleşmenin ve küresel gelişmelerin etkisiyle terörün ve terörist eylemlerin etkileri ve yayılması tüm dünyada artmaktadır. Teknolojik gelişmeler, iletişim ve ulaşım araçlarını ucuz ve kolay ulaşılabilir hale getirerek, teröristlere eylemlerinde kolaylık ve hız sağlamaktadır. "Terör, Fransızca "terreur" kelimesinden türeyip, aşırı korku ve endişe yaratan özel etkenler ve bireye özgü ussal olmayan ve genellikle bilinçsiz tepkilerin karşılıklı etkileşimi anlamına gelmektedir" (Wilkinson, 2002: 142). Bu nedenledir ki terörist, yaptığı eylemle esasen insan ya da insanları öldürmeyi amaçlamaz. Onun için önemli olan onları öldürdüğü zaman toplumda yaratacağı etkidir (Yalçınkaya, 2008: 4). Terörist eylemler enstrümantal değil de sembolik oldukları için medya aracılığıyla çok çabuk ve etkin biçimde seyredilme, dinlenme ve okunma yoluyla içeride ve dışarıda kolaylıkla gücünü duyurma imkanına sahip olmaktadır. Bu sayede toplumda bir korku halinin ortaya çıkmasından sonra teröristler, toplumun ya da devletin tutum ve davranışlarında değişim ve dönüşüm sağlama isteklerini gerçekleştirebilmektedirler (Wilkinson, 1997). Bununla birlikte "Terörist örgütler eylemli propaganda ile hem kendi grupları içindeki bilişsel alanlarını pekiştirmekte hem de hedef kitle ya da kitleleri etkileyerek kendi fikirlerini benimseterek, grupları dışında da bir bilişsel alan oluşturarak, genişletmeye çalışmaktadır" (Kurum, 2017: 66). Sosyal medya toplumda korkutma ve endişenin en iyi yaratılacağı ortamı sunmanın ve terör örgütlerinin sesini kitlelere duyurmanın en kolay yoludur. Bu sebeple, sosyal medya terörün amacına hizmet eden en uygun araç olarak kabul edilmektedir (Akçay ve Çelenay, 2012). "Terör olaylarının sosyal medyada yer almasının olumsuz yanlarından biri de bu olayların geniş bir kitleye yayılmış olması ve bu sayede aynı düşünceye sahip kişilerin, olaylara ilişkin yöntemleri, teknikleri öğrenebilmesini ve benzer olayın tekrar etmesine yol açabilmesidir" (Aziz, 1985: 135). Tüm bu açıklamalar ışığında terör örgütleri açısından sosyal medyanın kullanılmasının en önemli nedenleri Weimann (2004: 3)'in tespitleri ile örtüşmektedir. Bunlar:

- Kolay erişim,
- Büyük bir dinleyici ve izleyici kitlesi
- İktidar sahiplerinin kontrolünün, sansürün, düzenlemenin bu mecralar üzerinde az olması veya hiç olmaması,
- Veri toplama ve bilginin hızlı akışı,
- İletişimin gizliliği,

- Web varlığının, bakımının ve gelişiminin ucuz olması,
- Multimedya ortamıdır.

Weimann (2004: 4) ABD Barış Enstitüsü için 2004 yılında hazırladığı özel rapor için terör örgütlerinin kullandığı internet sitelerini taramış ve şu hususları tespit etmiştir:

- Aktif terörist grupların tümünün internette web siteleri mevcuttur ve teröristler ile destekçilerine hizmet veren yüzlerce web sitesi bulunmaktadır.
- İnternetteki terörizm çok dinamik bir olgudur: web siteleri aniden ortaya çıkar, formatlarını sık sık değiştirir ve daha sonra hızlı bir şekilde kaybolur ya da çoğu durumda, çevrimiçi adreslerini değiştirerek ancak aynı içeriği koruyarak yok olurlar.
- Terörist web siteleri üç farklı kitleyi hedeflemektedir: mevcut ve potansiyel destekçiler, uluslararası kamuoyu, düşman halkı.

DAEŞ terör örgütünün ele alındığı bir çalışmada, örgütün kullandığı hem resmî hem de gayriresmî sitelerinde çoğunlukla da cihat kelimesini ön plana çıkardığı; Youtube, Twitter, bloglar, mesajlaşma sistemleri ve çok sayıda başka platformu kullanarak hem propaganda yaptığı hem de gerçekleştirdiği şiddet eylemlerini sergilediği, böylelikle de istediği konuyu ön plana çıkararak taraftarlarını büyük ölçüde başarıyla harekete geçirebildiği ifade edilmiştir (Kartal, 2018). "DAEŞ sosyal medya sayesinde kendi içine birçok yabancı teröristi çekebilmiştir. Yaptığı propaganda faaliyetleri ile üyelerini özellikle Müslümanlar arasında model hale getirerek eleman kazanmıştır" (Erdem, 2017). Benzer şekilde Erdin (2017) de aynı örgütün (IŞİD ismiyle) sosyal medya kullanımını incelemiştir. Görüntüleri istenilen uzunlukta yayınlayabilecek bir alan olmasından dolayı, Youtube'un IŞİD tarafından tercih edildiğini, Twitter, Youtube ve diğer sosyal medya mecralarına göre belirli bir kişi sayısı ile sınırlı olmasından dolayı Facebook'un daha az kullanıldığını; en yoğun şekilde kullanılan sosyal medya mecrasının Twitter olduğunu tespit etmiştir.

Sosyal medyanın terörizmin yayılmasındaki rolünü ve sosyal medyanın etkilerinin analizini ele alan bir çalışmada Marcu ve Bălteanu (2014) internetin sanal dünyasında aşırılık yanlısı grupların varlığının arttığını, internetteki 10 terörizm vakasının 9'unun sosyal medyaya dayandığını belirlemişlerdir. Buna tedbir olarak ise Amerika Birleşik Devletleri, Kanada ve Büyük Britanya

askerlerinin kişisel verilerini sosyal paylaşım sitelerinden silmek için eğitildiğini ifade etmişlerdir.

Tunus ve Mısır odaklı bir araştırmada, Facebook, Twitter ve Youtube'tan toplanan verilerle, Mısır'daki siyasi web siteleri, Tunus'un tüm blog küresinde gerçekleşen politik diyaloglar ve devrim esnasında gerçekleşen ve filtrelenen 3 milyon tweet değerlendirmesi sonucunda, Arap Baharı'nda sosyal medyanın kritik rolünün olduğu ortaya konulmuştur (Pesen, 2017).

Şu ana kadar belirtilen çalışmalar terör örgütleri ve terörizme yönelik sosyal medya çalışmalarını kapsamaktadır. Bu çalışmalardan farklı olarak Altunbaş (2011) yaptığı bir çalışmada suç ve suçlularla mücadelede polisin sosyal medyadan faydalanma yöntemlerini şu şekilde ana başlıklar altında sıralamıştır.

- Sosyal medyada Polis Merkezi Kayıt Defterinin sergilenmesi,
- Aranan şahısların fotoğraflarının sosyal medya ortamında yayınlanması,
- Polis için geliştirilen web tabanlı bir bildirim araç setinin kullanılması,
- Belirli anahtar kelimeler ve deyimleri kullanarak sosyal medyayı takip etmek,
- Sosyal medya platformlarında çete üyesi gibi davranarak onların içine sızması, böylece çete üyeleri ile onlardan biriymiş gibi irtibata geçerek suç işlenmeden önce önlenmesi,
- Anında bilgi paylaşımı,
- Toplumla iyi iletişim kurulması,
- Suçlularla mücadelede yeni yöntemlerin kullanılması.

Burada belirtilmiş çalışmalardan da anlaşılacağı üzere sosyal medya üzerine yapılan çalışmaların büyük çoğunluğu suçla ve terörle mücadelede sosyal medyanın güvenlik birimleri tarafından kullanımından daha çok gündem belirleme kuramı kapsamında terör örgütlerinin sosyal medyayı kullanmaları üzerinedir. Gündem Belirleme modeline göre insanlar sosyal medya araçlarının değindikleri şeyler hakkında bilgi sahibi olmaya ve farklı konulara verilen önem derecelerini benimsemeye meyilli olacaklardır. Kişiler sosyal medya vasıtasıyla sadece toplumu ilgilendiren konuların ve diğer sorunların neler olduğunu değil; ayrıca, sosyal medya üzerinde verdikleri vurgudan hareketle bir sorun veya bir konuya ne kadar önem vereceklerini öğrenirler.

Kolluğun sosyal medyadan faydalanmasına yönelik ülkemizde yapılan çalışmalarda (Özçetin ve Özçetin, 2015; Çalı ve Altunbaş, 2012; Arıkan ve Rençber, 2017) ve yurt dışında yapılan çalışmalarda (Chermark and Weiss, 2005; Mostchall and Cao, 2002) odak noktasını kolluğun halkla ilişkiler ve tanıtım bağlamında Facebook, Youtube ve Twitter gibi programları kullanması oluşturmaktadır. Son dönemde yurtdışında suçla ve suçlulukla mücadelede sosyal medyanın kullanımını üzerine araştırmalar ve çalışmalar yoğunlaşmaya başlamıştır. Ülkemizde ise bu konu üzerine yapılan çalışmaların sayısı fazla olmayıp özellikle sosyal medya ile ilgili görev yapan kolluk personelin örneklem olarak alındığı bir çalışmaya rastlanılmamıştır.

Bu çalışmada amaç; kolluğun suç ve terörle mücadelede sosyal medyayı kullanım durumunu mevcut haliyle ortaya koyarak problemleri ve ihtiyaçları tespit etmektir. Sosyal medyanın kolluk tarafından kullanılması halkla ilişkiler ve tanıtım ile bilgi alma modeli olmak üzere iki şekilde olabilmektedir. Bizim çalışmamızın odak noktasını bilgi alma modeli oluşturmaktadır. Böylelikle elde edilecek verilerin suç ve terörle mücadelede sosyal medyanın kolluk tarafından daha etkin ve verimli kullanılabilmesine yönelik yapılacak çalışmalara ışık tutabilmesi amaçlanmıştır.

2. YÖNTEM

2.1. Araştırmanın Modeli

Sosyal bilimler alanında yapılan araştırmalarda kullanılan en yaygın veri toplama yöntemlerinden biri olan görüşme metodu (Briggs, 1986) bireylerin deneyimlerine, tutumlarına, görüşlerine, şikayetlerine, duygu ve inançlarına ilişkin bilgi elde etmede oldukça etkili bir yöntem olması nedeniyle bu araştırmada tercih edilmiştir. "Görüşme önceden belirlenmiş ve ciddi bir amaç için yapılan, soru sorma ve yanıtlama tarzına dayalı karşılıklı ve etkileşimli bir iletişim sürecidir" (Steward ve Cash, 1985). Görüşme metotlarından ise standartlaştırılmış açık uçlu görüşme yöntemi kullanılmıştır. Bu yöntem "dikkatlice yazılmış ve belirli bir sıraya konmuş bir dizi sorudan oluşur ve her görüşülen bireye bu sorular aynı tarzda ve sırada sorulur" (Patton, 1987: 112) ve "bazı insanlarda daha yoğun ve çok, bazı insanlarda ise daha az sistematik ve yüzeysel bilgi edinilmesine yol açabilecek olan görüşmeci yanlılığını veya öznelliğini azaltır" (Yıldırım ve Şimşek, 2018: 132).

2.2. Çalışma Grubu

Bu çalışmada amaçlı örnekleme yöntemlerinden faydalanılmıştır. Zengin bilgiye sahip olduğu düşünülen durumların derinlemesine çalışılmasına olanak veren amaçlı örnekleme yöntemleri pek çok durumda, olgu ve olayların keşfedilmesinde ve açıklanmasında yararlı olur (Patton, 1987). Kolluğun sosyal medyayı suçla ve terörle mücadelede kullanmasında yaşanan problemleri bireysel, kurumsal ve teknolojik boyutları yönünden tespit edebilmek için özellikle jandarma ve polis teşkilatlarında görev yapmakta olan 8 personel gönüllülük esasına göre belirlenmiş ve görüşmeler gerçekleştirilmiştir. Örneklemin belirlenen birimlerdeki hizmet yılları ile statüleri farklı olup fikir ve görüş çeşitliliğini sağlayabilmek için standartlık oluşturmamasına dikkat edilmiştir. Görüşmeye katılanlardan bir kişi 5 yıldır bu görevi yapan alana yönelik en tecrübeli kişi iken 4 kişi ise bu görevlere yeni atanmıştır. Bu 4 kişi her ne kadar görevde tecrübesiz gibi gözükse de geçmiş sefahatleri incelenip mülakat sonucu alanda görevlendirildiklerinden, sosyal medya veya internet alanında uzmanlaşmış ve çalışma tecrübesi edinmiş kişiler olarak değerlendirilmiştir. Diğer üç kişinin ise ortalama 3 yıl olmak üzere farklı sürelerde alan tecrübesi bulunmaktadır. Mesleki tecrübe olarak ise ortalama görev süresi 7 yıl üzeridir. Örneklem sayısı her ne kadar az gibi gözükse de Ankara'da görev yapan jandarma personelinin evreni onsekiz kişidir. Polis evreni biraz daha büyük olmakla birlikte görüşme için gönüllü olan sadece bir kişidir.

2.3. Veri Toplama Aracı ve Analizi

Kolluğun sosyal medyayı suçla ve terörle mücadelede kullanmasında yaşanan problemleri objektif olarak tespit edebilmek amacıyla daha esnek imkân sunan yarı yapılandırılmış sorular hazırlanmıştır. Yarı yapılandırılmış görüşme tekniğinin araştırmacıya sunduğu en önemli kolaylık görüşmenin önceden hazırlanmış görüşme protokolüne bağlı olarak sürdürülmesi nedeniyle daha sistematiktir. Görüşme odaklı yapılan nitel çalışmada veriler aşağıda belirtilen yarı-yapılandırılmış görüşme soruları aracılığıyla toplanmıştır.

- Ne zamandır bu görevi yapıyorsunuz?
- Suçla ve terörle mücadelede sosyal medyayı nasıl kullanıyorsunuz?
- Gerek teknolojik gerekse diğer hususlarla ilgili yaşadığınız sorunlar nelerdir?
- Suçla ve terörle mücadelede sosyal medyanın daha iyi kullanılabilmesi için sizce başka neler yapılabilir?
- Bu hususlar haricinde kolluk olarak sosyal medyadan nasıl faydalanabiliriz?

Görüşmelerde aşağıdaki hususlara dikkat edilmiştir.

1. Görüşme öncesi katılımcılara araştırmanın amacı açıklanmıştır.
2. Görüşme soruları tüm katılımcılara belli bir sıra dâhilinde ve değişiklik yapılmadan sorulmuştur. Bu sorulara verilen cevapların durumuna göre ilave sorularla konu derinliği oluşturulmaya çalışılmıştır.
3. Görüşme esnasında ses kaydı oluşturulmuş, katılımcıların ifadeleri kayıt cihazına kaydedilmiştir. Bu kayıtlar tüm görüşmeler tamamlandıktan sonra görüşme formlarına kaydedilmiştir.
4. Katılımcıların düşünce ve ifadelerini etkileyebilecek söz, jest, mimik ve diğer bireylerin olmamasına dikkat edilerek, objektif açıdan cevapların alınmasına özen gösterilmiştir.

Daha önce benzer bir çalışma yapılmadığı için sorular belirlenmiş ve bu sorular araştırma alanında görev yapan kişilere gösterilerek yeterli olup olmadığı, ilave soru gerekip gerekmediği, soru tarzında değişim yapılmasına ihtiyaç duyulup duyulmadığı sorulmuş ve ortak görüş olarak yeterli olduğu ve herhangi bir değişim gerekmediği belirtilmiştir. Ayrıca ilave sorular görüşülen kişilerin kapalı cevaplarını daha açık hale getirmek amacıyla sorulmuş olup ana soru niteliği taşımadığı için metne dâhil edilmemiştir.

Araştırmada elde edilen veriler üç tema altında toplandıktan sonra betimsel analiz tekniğiyle çözümlenmiştir. "Betimsel analiz, çeşitli veri toplama teknikleri ile elde edilmiş verilerin daha önceden belirlenmiş temalara göre özetlenmesi ve yorumlanmasını içeren bir nitel veri analiz türüdür. Bu analiz türünde temel amaç elde edilmiş olan bulguların okuyucuya özetlenmiş ve yorumlanmış bir biçimde sunulmasıdır" (Yıldırım ve Şimşek, 2018: 239). Bireylerin görüşlerini çarpıcı bir biçimde yansıtabilmek amacıyla doğrudan alıntılara yer verilmiştir. Kolluğun sosyal medya kullanımında etken olabilecek hususlar ele alınmış ve yapılan ön değerlendirme sonucu sorunsalımıza etki edebilecek hususların kolluk personelinin *kişisel özellikleri*, kolluk teşkilatı ile sosyal medya araçlarının oluşturduğu *kurumsal özellikler* ve alanın doğası gereği *teknolojik özellikler* olmak üzere üç tema belirlenmiştir. Bu doğrultuda katılımcıların sorulara verdikleri cevaplar benzerliklerine göre gruplandırılarak, yorumlanmıştır.

5. BULGULAR

Bu araştırmanın bulguları üç tema altında toplanmıştır. Bu üç tema; kişisel özellikler içeren, kurumsal özellikler içeren ve teknolojik özellikler içeren tespitler olarak sınıflandırılmıştır. Görüşmeye katılan kişilerin tamamı jandarma ve polis teşkilatlarında suçla ve terörle mücadelede sosyal medya veya internetin

kullanıldığı bilişim veya siber kısımlarında aktif olarak görev yapmaktadır. Tüm katılımcıların görevdeki hizmet yılları farklı olmasına rağmen görüşlerinin birbirleri ile örtüştüğü anlaşılmıştır.

5.1. Kişisel Özellikleri İçeren Tespitler

Avşar (2017)'ın ifade ettiği gibi sosyal medya, istihbarat örgütleri ve istihbarat toplayan kurumların bilgi toplaması ile hedef kişilerin tespit edilmesi için geniş bir alandır. Bu yolla kişiler, kurumlar, ülkeler hakkında kolayca bilgiye ulaşılabilmektedir. Özellikle Korkmaz (2013)'ın da çalışmasında ele aldığı Facebook, program yapısı itibariyle kişilerin okulları, mesleği, arkadaşları, hobileri, ilişki durumları gibi kişisel bilgilerinin bile kişinin isteği doğrultusunda deşifre eden bir sosyal mecradır. Terör örgütlerinin kullandığı gibi kolluk mensupları da suç işlediği anlaşılan veya terör örgütü mensubu olduğu düşünülen kişileri arkadaş olarak ekleyerek kişisel bilgilerini, (adı, soyadı, fotoğrafları, çalıştığı yer, mezun olduğu okullar, dini ve siyasi düşüncesi, ilgi alanları, vb.) arkadaş listesini, oturduğu şehri, şu anda nerede olduklarını, o anki ruh durumlarını, ülke siyaseti ya da gelişmeler hakkındaki düşüncelerini kolaylıkla öğrenebilirler.

Sosyal medyada milyonlarca kişi ve grup sayısız bilgi ve düşünceyi anlık olarak ve sürekli paylaşmaktadır. Katılımcılar, bu kadar bilginin arasından kolluk açısından faydalı olan bilgileri tespit etmenin ve devşirmenin kolluk personelinin dikkatine, yeteneğine, aldığı kurs ve eğitimlerin sonucu oluşan bilgisine bağlı olduğunu bildirmiştir. Ayrıca katılımcıların genel görüşüne göre, kurumların bu görevlere tahsis ettikleri kişi sayısı çok yetersizdir. Bu nedenle bu kişilerin alanda yeterli bilgiye sahip ve gerekli kursları görmüş kişiler olması gerekmektedir. Buradan anlaşılacağı üzere çalışacak personelin belirlenmesinde özellikle alanla ilgili bilgi ve tecrübe altyapısı ile kişisel bazı kriterlerin (dikkat, durumsal farkındalık, araştırmacı kişilik vb.) aranması gerekmektedir.

"Şu anda tamamen personel dikkatine bağlı performans yürütülmekte." (A-1/A)

"Kaliteli personel seçimi yapılması lazım. Bu alanda iyi bir personelin yetiştirilmesi için uzun zaman gerekiyor. Şu anda adli bilişim uzmanları 6 farklı program kullanıyor, imajları alıyorlar. Bunu yapa yapa daha çok kendilerini geliştiriyorlar. Kendini geliştiren personel kısa zamanda daha çok iş ortaya çıkarıyor." (A-2)

"paylaşımlardan kişinin dikkatine bağlı olarak da tespit yapabiliyoruz, bu tamamen kişinin dikkatine bağlı." (A-3)

Sosyal medya tamamen teknolojiye bağlı olup gelişimi yaşayan bir süreçtir ve bu süreç durmadan devam eder. Katılımcılar, alanda yetişen personelin meslek hayatı boyunca aynı görevleri yapmasının verimliliği artıracağını, aksi takdirde ise kaynak israfı olacağını bildirmişlerdir. Bu durum alanda çalışan personelin de sürekli kendisini geliştirmesini zorunlu kılmaktadır. Gelişimi takip edemeyen ve performans kaybı yaşayan kişilerin alan dışına çıkarılması kaynak verimliliği açısından önemlidir.

"Siber ve Adli Bilişim alanında çalışan bir personel tayin olduğunda gittiği yerlerde de aynı görevlere devam etmesi gerekiyor. Alan devamlı gelişiyor, hep yeni şeyler çıkıyor. Personel ara verdiği zaman, bir yıl ara verse, sıfırdan tekrar başlamak zorunda kalır. Bu iş uzun süren ve sürekli devam ettirilmesi gereken iş." (A-2)

Yazılım ve donanım ana başlıkları altındaki birçok alt alanda çok hızlı bir teknolojik gelişim söz konusudur. Sosyal medyanın suçla mücadelede kullanılabilmesi için gerekli olan asgari bilgisayar kullanım bilgisi çok fazla insan gücü ve zaman gerektirmektedir. Personelin verimli çalışması için günümüzün şartlarına göre sürekli kendisini geliştirmesi gerekmektedir. Personel her ne kadar kendisini geliştirmeye gayret gösterse bile bilişim alanındaki bu yeniliklerin hepsine vakıf olması çok zordur. Bu nedenle alanda daha etkili olabilmek için personel haricinde, kurum dışı kaynaklardan sosyal medya uzmanları, yazılımcılar gibi uzman kişilerden destek alınmasına ihtiyaç duyulabilmektedir. Kurum dışından bu tarz kişilerin temin edilebilmesi ve çalıştırılabilmesi için gerekli düzenlemelerin yapılması gerekmektedir.

"Konuyla ilgisi ve bilgisi olan yazılım mühendisleri alınabilir…" (A-1)

Dünyaya hâkim olan ve kullanım yönünden ana payı oluşturan Facebook (www.sosyalmedya.co), LinkedIn'i alan Microsoft ve Youtube'u alan Google (www.haberturk.com) gibi sosyal medyanın patronları veya merkez ülkeleri Anglosaksondur. Bu nedenle diğer alanlarda olduğu gibi bu alanda da İngilizce hakimiyeti söz konusudur. Bilişim kısımlarında veya sosyal medyada araştırma yapacak ve kullanacak personelin İngilizce bilmesi artı değer katmaktadır.

"Bu şubede çalışan personelin kesinlikle İngilizce bilmesi gerekiyor." (A-2)

"Personelin eğitimli olması gerekiyor. İnternette ne aradığını bilen personel daha iyi mücadele eder; bazı personel suçları ve ne aradığını bilmiyor." (A-6)

5.2. Kurumsal Özellikleri İçeren Tespitler

1989 yılında www'nin (world wide web) kullanıma başlaması ve 1990'lı yılların sonunda ilk blogların ortaya çıkması ile sosyal medya kavramı ortaya çıkmıştır. 2004 yılından itibaren ise Facebook, Youtube, Flicker ve Twitter gibi sosyal ağların kurulması ile büyük bir gelişim göstermiştir. Türkiye'de ilk internet bağlantısı 12 Nisan 1993 tarihinde ODTÜ tarafından yapılmıştır. Sosyal medya kullanımı ise dünya geneliyle paralel gitmiştir.

Tüm dünyada olduğu gibi ülkemizde de güvenlik kuvvetleri siber terörizm [7] tehdidine karşı aşırı hassasiyet göstermektedir. Buna karşın, internetin günlük ve rutin kullanımlarına yeterince dikkat edilmemektedir. Halbuki teröristler ve suçluların propaganda ve psikolojik savaş, kaynak ve eleman temini, veri madenciliği ve eylemlerin koordinasyonu gibi faaliyetlerini internetin günlük ve rutin kullanım alanlarında gerçekleştirdikleri görüşmelerin ortak noktası olarak tespit edilmiştir.

Kolluğun siber suçlarla mücadele amaçlı kuruluş tarihçesi Tablo 3.'de verilmiştir. Kuruluş kronolojileri kolluğun internet ve sosyal medya araştırma ve kullanım durumunun gelişimini de ortaya koymaktadır.

Tablo-3. Kolluğun Siber Suçlarla Mücadele Amaçlı Kuruluş Tarihçesi[8]

Jandarma		**Polis**	
Bilişim Suçları Kısmı	2004	İnternet Suçları ile Mücadele Amirliği	1997
Bilişim Suçları Şube Müdürlüğü	2009	Bilişim Suçları Çalışma Grubu	1999
Siber Suçlarla Mücadele Daire Başkanlığı	2019	Bilişim Suçları Araştırma Merkezi	2000
		Bilişim Suçlarıyla Mücadele Daire Başkanlığı	2011

Kolluk internet ve sosyal medya aracılığı ile suç araştırma görevlerini bilişim ve siber kısımları ile istihbarat birimleri aracılığıyla yerine getirmektedir. Suç ve suçlularla mücadelenin ana yükünü çeken asayiş birimleridir. Suç ve terörle mücadele eden kolluğun günümüz teknoloji çağının gereği olarak her an internete ve sosyal medya sitelerine erişimi olmalıdır. Katılımcılar asayiş birimlerinde çalışan personelinin internet ortamında birçok programa erişim sağlayamadığını

[7] Belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır (Özcan, 2002: 309).

[8] Jandarma Genel Komutanlığı ve Emniyet Genel Müdürlüğünden temin edilmiştir.

belirtmişlerdir. Buna ilave olarak özellikle bilişim suçlarında görevli personelin tüm sitelere erişim izninin olması, hatta mahkeme kararlarıyla yasaklanan sitelere de girilebilmesi için düzenleme yapılması gerektiğini ifade etmişlerdir.

Kolluğun kullandığı internet hattı kurumsal internet hattıdır. Bilişim suçlarına bakan, internet ve sosyal medya ortamında araştırma yapan ve soruşturma için delil toplayan kolluk personelinin kullandığı internet hattının kurumsal olmasının bazı sakıncalarının bulunduğu tespit edilmiştir. Suç veya terör örgütleri içerisine girerek bilgi toplamaya çalışan kolluğun kullandığı internet IP adresi, örgüt elemanlarından bilgisayar kullanım bilgisi iyi olan kişilerce tespit edilebilmektedir. Kolluğun internet hattı olduğunun anlaşılması üzerine örgüt mensupları tarafından ilgili kolluk personeli sanal ortamda engellenerek veya gruba üyeliği iptal edilerek araştırma veya soruşturma çabaları sekteye uğratılmaktadır. Buna ilave olarak takip edilen bir olayda suç örgütü üyeleri böyle bir durum karşısında işleyecekleri bir suçun plan ve icrasında değişikliğe gitmektedir. Bu da kolluğun bu suça yönelik toplamış olduğu tüm bilgilerin boşa çıkmasına neden olmaktadır.

> *"…birçok siteye erişim izinle yapılmaktadır. Bilişim kısmı olarak erişimlerimiz mevcuttur ama diğer personelin böyle erişim izni yoktur. Erişimlerimiz olsa bile kurumsal ağdayız ve hareket kabiliyetimiz çok kısıtlı. Kurum ağında çalıştığımızdan dolayı suç örgütleri ile iletişime geçtiğimizde karşıdaki insanın biraz bilgisayar bilgisi mevcutsa benim bağlandığım ağı göreceğinden dolayı iletişimi keser. Bize bağımsız bir internet kesinlikle şart." (A-1)*
> *"Kullandığımız internet hattı kurumsal hat olduğu için grupları kuranlar bizim … olduğumuzu anlıyor ve bizi gruplara almıyor, engelliyorlar." (A-5)*

Sosyal medya firmaları ticari çıkarları doğrultusunda üyelerinin bilgilerini paylaşmak istememektedirler. Bunun içinde her türlü fırsatı değerlendirerek bilgi taleplerini karşılamamaktadırlar. Çocuğun cinsel istismarı ve uyuşturucu ticareti gibi suçlarda bilgi paylaşan bu firmalar diğer birçok suçta talepleri reddetmektedirler. Terörist gruplar ve suç örgütlerinin sosyal medya ortamını kullanmaları veya çocuk pornosu, uyuşturucu, işkence, cinayet gibi bazı suçların sosyal medyada yer alması durumunda bu kullanımın kısıtlanması, hesapların dondurulması, bu konulara yönelik yapılan soruşturma veya kovuşturmalarda istenilen bilgilerin ilgili makamlara verilmesine imkân sağlayacak, insanların mahremiyet ve medeni özgürlükler üzerindeki haklarının da teminat altına alacak, hukuki mevzuatın sosyal medya firmaları ile oluşturulması gerekmektedir.

"Facebook veya Twitter'dan bir şey talep ettiğimizde bunun bize dönüşü her zaman olumlu olmuyor. Resmi olarak sosyal medya firmalarından talep edildiğinde bize bilgi verilmiyor. Türkiye'de temsilcilikleri var, fakat bizimle bilgi paylaşımı yapmıyorlar. Cinsel istismar gibi bazı konularda bilgi veriyorlar ama diğer konularda geri dönüş olmuyor. Terör konusunda bilgi paylaşımı yapılmıyor." (A-3)

"Firmaların İstanbul'da büroları var. Bilgi talep ediyorsunuz. Hiçbir şey vermiyorlar." A-2

Medya halkı bilgilendirmek ve bilinçlendirmek için devletin kullanabileceği önemli güçlerden biridir. "Yalan yanlış bilgilerle halk arasında endişe yaratmak isteyen terör örgütlerine hizmet eden fısıltı gazetelerinin emelleri ve dedikoduları, yine halka doğru bilgiler verilerek, boşa çıkarılabilir. Bunun yanı sıra, medyada yer alan terör haberleri, terörün verdiği zararları ve ülke üzerindeki olumsuz etkisini ön plana çıkararak, halkın teröre karşı daha fazla kenetlenmesini sağlayabilir." (Kazan, 2016: 128). Bu gücün farkında olan Jandarma ve Polis Teşkilatı halkla ilişkiler ve tanıtım kapsamında kurumsal sosyal medya sitelerini kurmuş olup bu siteleri aktif olarak kullanmaktadırlar.

Katılımcılar, toplumsal olay, gösteri ve eylemlerin engellenmesinde veya etkisinin azaltılmasında personelin kişisel paylaşımlarının çok fazla etkisinin olmayacağını değerlendirmektedir ve bilgi kirliliğinin önüne geçilebilmesi, provokasyona maruz kalmaların engellenebilmesi ve eyleme katılım oranının azaltılabilmesi için Jandarma ve Polis ile Valilik sosyal medya hesaplarından yapılacak paylaşım ve bildirimlerin daha etkili olacağı kanısındadırlar. Bu tarz kriz durumlarında sosyal medya hesapları halkla ilişkiler ve tanıtım amacından ziyade gündem belirleme modeli olarak kullanılabilecektir. Bu doğrultuda kolluğun sosyal medya sitelerinin takipçi sayılarını artırmak için çalışmalar yapılmalıdır. Bilhassa Halkla İlişkiler faaliyetlerinde sosyal medyaya daha fazla ağırlık verilmelidir.

"Bizim paylaşım yaparak toplumun yönlendirilmesini engellememiz zor. Bunun yerine kurumsal hesaplar Jandarma, Polis, Valilik gibi buralardan resmi bilgi paylaşımı yapılarak engellenmeye çalışılmalıdır ki bu daha etkili olacaktır." (A-3)

"Özellikle yaptığımız faaliyetler ile ilgili reklam yapmaya ihtiyacımız var. Bunu sağladığımız takdirde insanlar ister istemez bu konularla ilgili bizlere ihbarda bulunacaklardır. Böylece iş döngümüz artacaktır."(A-7)

"Öncelikle yapılan faaliyetlerin reklamı yapılması gerekiyor hem kurumun adını duyurmak hem de caydırıcı bir etki bırakmak için." (A-4)

5.3. Teknolojik Özellikleri İçeren Tespitler

Günümüzde teknoloji çok hızlı bir şekilde ilerliyor. 1989'da başlayan internet Web 1.0 olarak adlandırılırken sosyal medyanın da dâhil olduğu Web 2.0'a dönüşmüş, arkasından çok kısa bir sürede yapay zekanın rol oynadığı Semantik Web denilen Web 3.0[9] çağı başlamıştır. Son dönemde ise Web 4.0[10] sanal çağına girilmiştir. Bu hıza kolluğun da ayak uydurması gerekmektedir. Bunu yapabilmesi için de güncel programlar ve bilgisayar sistemleri kullanılmalıdır. Kolluk insan kaynağının çok az bir kısmını bu mücadeleye ayırabilmektedir. Bir kişinin günlük 8 saat mesai yaptığı göz önünde bulundurulduğunda bilgisayar karşısında dikkatini kaybetmeden yapacağı araştırma süresi 8 saatten daha azdır. Kişinin tüm mesaisinde bilgisayar karşısında inceleme yaptığı kabul edilse bile gün boyunca bir alanda en az 3 kişinin görev yapması gerekir. Binlerce alan olduğu düşünülürse bu incelemeler için insan kaynağı yetersiz kalır. Bu nedenle güncel tarama ve analiz programlarının kullanılması sosyal medyada suç ve terörle mücadelede kaçınılmaz hale gelmiştir.

"Milyonlarca paylaşımı analiz etmeniz ve incelemeniz kişisel olarak çok zor. Bunları bir programla yapmak her zaman daha kolay oluyor." (A-3)

"İnternet üzerinde kullanılan ... programlar şu anda paralı hale gelmiştir. Bu da araştırmalarınızı zorlaştırmaya başlamıştır. Yeni programların alınmasıyla suçla ve suçluyla mücadelede daha iyi çalışacağımıza inanıyorum." (A-6)

"....sosyal medya sitelerinde tarama yapan programlar mevcut. Bu programlar sayesinde Türkiye'de ve dünyada yapılan paylaşımları tarayarak girdiğimiz anahtar kelimeleri tarayarak tespit eden programlar var." (A-1)

"Siz insan olarak 8 saat takip edebilirsiniz ama 24 saat takip edemezsiniz. 24 saat esasına göre çalışan değişik programlar var; sizin vermiş olduğunuz kod kelimelerle süzme işlemi yaparak size rapor çıkaran programlar kullanılması gerekiyor." (A-2)

[9] "Web 3.0 içerik kontrolünün yazılımların eline geçtiği bir dünya olarak adlandırılabilir. Birbiriyle iletişim halinde olan veritabanı sistemleri sayesinde nelerden hoşlandığımızı anlayabilen ve buna göre bizlere çözüm sunan bir Web sistemidir. Web 3.0, eski hali Web 2.0'ın sanal dünyaya aktardıklarını anlamlandıran bir 'Yapay Zeka' olarak adlandırılır hale gelmiştir." (www.bilimcag.com/ para. 7)

[10] "Web 4.0, en kapsamlı ve kişiselleştirilmiş, sadece bilgileri görüntülemekle sınırlı olmayan, ancak kullanıcının ihtiyaç duyduğu şeylere somut çözümler sunan akıllı bir ayna gibi davranmayı öneren yeni bir kullanıcı etkileşimi modeli sunar." (***www.prezi.com/*** Elekoğlu, WEB 4.0 Nedir?)

Teknolojinin güncel tutulabilmesi için yapılacak yazılımsal ve donanımsal alımlar veya ihalelerin sürelerinin kısa olması gerekmektedir. Mevcut ihale kanunu ile yapılan alımlarda süreç altı ay veya daha fazla sürebilmektedir. İhalesi yapılan sistemler en son teknoloji ürünü iken bu süreç esnasında daha hiç kullanılamadan güncelliğini yitirebilmektedir. Ayrıca kurum dışından, ihtiyaç halinde, program yazılımcısı ve donanımcı insan gücü temin edilebilmelidir. Bu kişiler vasıtasıyla teknoloji güncel kılınabilir. Gerektiğinde alana yönelik eğitim faaliyetleri ve kurslar ile kurum personelinin bilgilerinin güncelliği sağlanabilir, ihtiyaç duyulan alanlarda eksiklikleri tamamlanabilir.

"Güncel yazılımların olması gerekiyor ve bu yazılımlarla ilgili kurslar verilmesi gerekiyor." (A-4)

"İhaleye çıkılan bilgisayar sistemlerinin alınması biraz daha kolay olması gerekiyor." (A-6)

Bazı katılımcılar sosyal medya üzerinden yapılan araştırma ve operasyonlar sayesinde yakalanan faillerin kitle medyasında yer almasının terör ve suç örgütü üyelerini başka mecralara yönlendirmeye başladığını bildirmişlerdir. Bunlardan bazıları online oynanan oyunların mesajlaşma bölümleridir. Bir diğer yöntem ise deepweb ortamlarıdır. Bu nedenle kolluk internet içerisinde devamlı araştırmacı ve yaratıcı düşünce ile sanal devriyesini icra etmek zorundadır. Suçluların veya teröristlerin kimliklerini gizlemek için kullandıkları bir yöntem de VPN[11] **(Virtual Private Network)** Sanal Özel Ağ'dır. En temel anlamıyla internete başka bir IP adresi üzerinden bağlanmanızı sağlayan hizmettir. VPN, bağlantınızı güvenli hale getirir ve herhangi bir ağa bağlanırken sizin bağlantınızı şifreler ve kimliğinizin bulunamamasını sağlar. Kolluk internet ortamında, suçla ve terörle mücadele ederken sadece sosyal medya ile sınırlı kalmamalı ve internetin diğer alanlarına yönelik çalışmalar da yapacak şekilde yapılanmalıdır.

[11] Genellikle iş ortamı dışında yapılan bağlantılarda iç ağdayken sahip olunan yetkilerin dış ağdayken de devam etmesini sağlamayı amaçlayan bağlantı türüdür. Bunu gerçekleştirmek için noktadan noktaya bağlantı tekniği ve bu bağlantı sırasında da verilerin kapsüllenmesi yöntemi kullanılır (Baykal 2001'den akt. Erol, 2019)

SONUÇ

Teröristler ile suçlular kıyaslandığında sosyal medyanın kullanım amaçlarında farklılıklar bulunmaktadır. Teröristler sosyal medyayı gündem oluşturma kuramı çerçevesi içerisinde eylemlerini duyurmak, propaganda yapmak için kullanırken diğer suçlularda böyle bir düşünce yoktur. Bununla birlikte suçluların büyük bir çoğunluğu sosyal medyayı farklı amaçlar için kullanabilmektedir. Bunlar genelde iletişim kuramlarından Westley-Maclean Aracılanmış İletişim Modeli ile çok örtüşen bir yöntem oluşturmaktadır. Burada bariz bir farklılık varsa o da aracılık yapanların çoğu bunu kasıtlı aracılık şeklinde yapmalarıdır. Suç örgütleri veya suçlular diğer suçlularla iletişim kurmak veya irtibat sağlamak, kaçakçılık suçunu teşkil eden malzemelerin tanıtımını ve pazarlamasını yapmak; suç işlemeden önce suçun işlenme yöntem ve teknikleri hakkında bilgi almak, suç işlemeden önce yanlış ve yalan bilgiler kullanarak suç ortamını sağlamak amaçlarıyla bu iletişim yöntemi ile sosyal medyayı kullanmaktadırlar.

Bunun yanında kolluk personeli ise suçla ve suçlularla mücadelede sosyal medyayı bilgi arama modeli kapsamında kullanmaktadır. Bunun kolluktaki karşılığı kısmen açık kaynak istihbaratı olarak ifade edilebilir. Açık kaynak istihbaratı gizli istihbari faaliyetlerden başka yöntemlerle toplanan bilgiler olarak kabul edilir ve kitle medyasının gelişmesi ile önemi de artmıştır. Sosyal medyanın açık kaynak istihbaratında payı da artmaktadır. Açık kaynak bilgisini bulmak daha kolay, daha ucuz ve daha güvenilirdir. Açık kaynaklardan elde edilen bilgiler ile diğer istihbari faaliyetler yönlendirilebilir ve maliyetleri azaltılabilir.

Bu amaçla sosyal medyayı kullanacak personel istihdam etmek verimlilik ve etkinlik açısından yeterli olmayacaktır. İstihdam edilecek personelin kolluk tecrübesi yanında bilgisayar altyapısı olan, sosyal mühendislik yetenekleri gelişmiş, mümkünse İngilizce bilen kişiler arasından seçilmesi etkinlik ve verimliğin sağlanması için ana unsurlardır. Bu seçimle sağlanan verimliliğin daha ileri seviyeye çıkarılması için gerekli kurs ve eğitimlerle personelin yetiştirilmesi gerekmektedir. Bu personelin sürekli değişen sosyal medya formları hakkında bilgilerini güncel tutması sağlanmalı ve kurum içindeki atamalarda personel bu görevlerini aralıksız sürdürebileceği kadrolara atanmalıdır. Böylece özellikle suç örgütlerinin kullanmış oldukları ve Westley-Maclean Aracılanmış İletişim Modelinde sözü geçen özellikle kasıtlı aracıların tespitinde daha tecrübeli olacakları ve verimli çalışabilecekleri değerlendirilmektedir.

Bunun yanında mevcut durum olarak personelin genel itibariyle niteliksel olarak yeterli olmasına rağmen niceliksel olarak yeterli olmadığı tespit edilmiştir. Gelişen teknolojik altyapı ile sosyal medyanın kapsamı ve içeriğinin gittikçe büyüdüğü göz önünde bulundurulursa personel istihdamında bir ivmeye ihtiyaç duyulacağı açıktır.

Terör ve suç örgütleri üyeleri sosyal medya hesaplarının takip edildiğini ve bu vasıtayla bazı faillerin yakalandığını bildikleri için eylem organizasyonu ve iletişim için başka mecralara yönlenmişlerdir. Bu mecralar online oyunların içinde bulunan mesajlaşma eklentileri veya oyun forumlarıdır. Oyunların içindeki mesajlaşma yöntemlerinde grup veya ittifak oluşturularak yapılan haberleşmeler diğer oyunculara kapalı olmakta ve istenilen şekilde bilgi alışverişi yapılabilmektedir. Başka bir yöntem olarak ise VPN programları kullanılarak internete bağlanılması veya Deepweb alanında faaliyet yürütülmesidir. Bu alanda araştırma ve soruşturma yürüten personel gerek teknolojinin gelişimi ile ilgili gerekse suçluların yeni yol ve yöntemleri ile ilgili daima bilgilerini güncellemelidir. Bu güncellemeyi yapamayan ve kendini bu alanda geliştiremeyen kolluk her zaman suçla ve suçlularla mücadelede reaktif olarak kalacaktır ve proaktif olamayacaktır.

Kurumsal özellikleri içeren bulgular ele alındığında iki farklı yön ortaya çıkmaktadır. Birincisi kolluk teşkilatlarının kurumsal yönü ile ilgili tespitler:

– Sosyal medya araştırmalarına yönelik kurumsal teşkilatlanma istenilen seviyede olmasına rağmen mevcut şartlarda kolluk personelinin görevle alakalı internet erişim seviyesinin istenilen seviyede olmadığı anlaşılmıştır. Asayiş birimlerinde çalışan personelinin özellikle suç araştırmaları için internet ortamından istenilen seviyede yararlanamamaları, bulunduğumuz bilişim ortamında çelişkili bir durumdur. Kurumsal olarak kolluk personeline, özellikle de bilişim suçlarında görevli personele tüm sitelere erişim izninin olması, suçla mücadelede büyük kolaylık sağlayacaktır. Bunun yanında soruşturmaların selameti açısından kolluk personeline kurumsal olmayan IP adresli internet hatlarının temin edilmesi gerekmektedir.
– Kolluk teşkilatlarının kurumsal yönünün diğer bir boyutu ise sosyal medyanın güvenlik kuvvetleri ve halk arasında iki yönlü iletişim sağlayan ve bilgi paylaşımının yapıldığı önemli bir kanal olmasıdır. Kolluk yaptığı faaliyetleri halka sosyal medya aracılığı ile aktararak kendi reklamını yapmalı ve sosyal medya kamusunu genişletmelidir. Böylelikle ihtiyaç duyulduğu anda gündem kurma yetkinliğini kendi elinde bulundurabilecektir. Bu sayede kriz durumlarında veya

önemli olaylarda halka doğru bilgiler aktarılabilir; provokasyonlar engellenebilir; oluşabilecek bir toplumsal olayın önüne geçilebilir. Bu sağlanamasa bile olayın çapı ve kapsamı daha büyümeden engellenebilir. Ayrıca eylem ve suç öncesi olayların haber alınması, yani ihbar miktarı ve kalitesi artırılabilir. Halkla ilişkiler kurularak toplum polisliği yaratılabilir.

İkincisi sosyal medya firmalarının kurumsal yönü ile ilgili tespitler:

– Sosyal medya firmaları terörist ve aşırılık yanlısı gruplara karşı paylaşım kuralları belirleyerek, terörist faaliyetler için hizmetlerinin kullanılmasının yasaklanması gibi önlemler alabilmektedirler. Paylaşılan içeriklerin gerçek zamanlı olarak izlemenin imkânsızlığı nedeniyle uygulamada bu önlemlerin etkinliği tartışma konusu olabilmektedir.

– Kurumsal tespitlerde en göze çarpanı sosyal medya firma temsilciliklerinin kollukla bilgi paylaşımına yanaşmamasıdır. Sosyal medya firmalarının kurulum merkezleri başka ülkelerde bulunmaktadır. Bu nedenle suç ve terör tanımlamaları bizim ülkemizle birebir eşleşmediği için bilgi paylaşımında sorunlar yaşanmaktadır. Sorunların aşılması için sosyal medya ile ilgili kapsamlı bir mevzuatın hazırlanması gerekmektedir. Terörist grupların veya suç örgütlerinin sosyal medya ortamını kullanmaları ve çocuk pornosu, uyuşturucu, işkence, cinayet gibi bazı suçların sosyal medyada yer alması durumunda, kullanımın kısıtlanması, hesapların dondurulması, bu konulara yönelik yapılan soruşturma veya kovuşturmalarda istenilen bilgilerin ilgili makamlara verilmesine imkân sağlayacak, insanların mahremiyet ve medeni özgürlükler üzerindeki haklarını da teminat altına alacak, hukuki mevzuatın sosyal medya firmaları ile oluşturulması ihtiyacının olduğu tespit edilmiştir. Bu ihtiyaç doğrultusunda hukuksal düzenleme yapılırken dikkat edilecek en önemli hususlardan birisi de evrensel ilkelerden uzaklaşılmaması gerekliliğidir. Aksi durum terör örgütlerinin istismar alanlarını genişletmesine, amaçlarını haklı hale getirmesine ve eleman temininde güçlük çekmemesine olanak tanır.

Teknolojik özellikleri içeren bulgular ele alındığında ise kolluğun elinde bulunan cihaz ve makinaların teknolojik olarak yeni olduğu fakat teknolojik gelişim ivmesi nedeniyle kısa süre sonra teknolojinin gerisinde kalacağı anlaşılmaktadır. Bu ivmenin yakalanabilmesi amacıyla yeni malzeme alımları yapılabilmektedir. Burada tespit edilen ana nokta; yapılan alımlardaki cihazların teknolojisinin ihale alım süreci nedeniyle güncelliğini kaybetmesidir. Problemin

aşılabilmesi için özellikle bu tarz teknoloji ürünlerinin alımının anlık yapılabilmesine yönelik düzenlemelerin oluşturulması gerekmektedir.

Diğer bir husus ise terör ve suç örgütlerinin iletişim sağlamak amaçlı Deepweb, online oyun programları ve VPN alanlarına kaymaya başlamalarıdır. Gündem oluşturmak, yönlendirme yapmak ve aldatma tedbirleri uygulamak için sosyal medyanın kullanımına devam edileceği, eylem planı ve koordinesi, suç alet ve ürünlerinin pazarlaması için ise bu yeni alanların tercih edileceği anlaşılmaktadır. Bu nedenle kolluk personeli bu alanlarda kendilerini yetiştirirken proaktif anlayışla terör ve suç örgütlerinin teknolojik yöntem arayışlarını belirleyerek tedbir almalıdır.

Genel anlamda değerlendirme yapılacak olursa; sosyal medyanın sosyal hayata bu kadar katkısı ve faydası olmakla birlikte birey, toplum ve devlet açısından sosyal mühendislik saldırıları, provokasyon, dezenformasyon ve bilgi kirliliği, bağımlılık ve buna bağlı ailevi sorunlar, tehlikeli bilgi paylaşımı ve manipülasyonlar, ekonomik zararlar, kişisel ve özel sırların deşifre olması, özel hayatın gizliliğinin ortadan kalkması gibi önemli tehditleri de içinde barındırmaktadır. Bu tehditlerin ortadan kaldırılabilmesi için sosyal ağlarda kişisel bilgilerin korunması amacıyla kullanıcıların bilgi güvenliği farkındalığının artırılması, korumaya dayalı sosyal ağ modelleri geliştirilmesi önemli hususlardan bazılarıdır. Bunların yanında sosyal medya okur-yazarlığının geliştirilmesi, bilgi kirliliğinin önüne geçilebilmesi için doğru bilgiye erişim alt yapısının güçlendirilmesi, kurum ve kuruluşlarca nitelikli personelin yetiştirilmesi, sosyal medyaya yönelik yasal düzenleme eksikliklerinin giderilmesi büyük önem taşımaktadır.

Sosyal medya ve internetin bu önemine binaen kolluk suç ve terörle mücadelede bu alana daha çok önem vermelidir. Bu önem yeterli ve eğitimli insan gücü planlaması, çağın teknolojik gereklerini uygun bilgisayar yazılımları ve donanımları ve diğer ihtiyaçları da karşılayabilecek maddi kaynakları sağlayarak oluşturulabilir.

KAYNAKÇA

Akçay, E.Y. ve Çelenay Ö.E. (2012). Terör ve Medya İlişkisinin 2003 Yılında İstanbul'da Meydana Gelen Saldırılar Örneğiyle İncelenmesi, NEÜ Sosyal Bilimler Enstitüsü Dergisi 2, 183-197.

Altunbaş, F. (2011). Toplum Destekli Polislikte Yeni Bir Boyut: Suç Ve Suçlularla Mücadelede Sosyal Medya Platformları, Suç Önleme Sempozyumu, 361-371

Arıkan, Ü. ve Rençber, H. (2017),Social Media as the Escape Area for İllegality, (31-52). (Edt. Emrah Doğan ve Ercan Geçkin, Current Debates in Public Relations Cultural & Media Studies, Vol.9, London: Ijopec Publication.

Avşar, Z. (2017), İnternet Çağında Medya, Terör ve Güvenlik, Ankara: TRT Akademi Dergisi, Cilt.2, Sayı.3, (116-132).

Aziz, A. (1985). Terör ve Kitle İletişim Araçları, Ankara: BM Türk Derneği Yıllığı.

Barbera, P., Metzger, M., Tucker, J.A. (2003). A Breakout Role for Twitter in the Taksim Square Protests? El Cezire, https://www.aljazeera.com/indepth/ opinion/2013/06/201361212350593971.html, Erişim tarihi: 08.09.2019.

Baykal, N. (2001), Bilgisayar Ağları. (Akt. Beytullah Erol, 2019, Ağ Trafik Özelliklerinin Analizini Yaparak Anormalliklerin Tespit Edilmesi, Yüksek Lisans Tezi), Ankara : Sas Bilişim.

Boyd, D. M. ve Nicole B. E. (2008). "Social Network Sites: Definition, History, and Scholarship", Journal of Computer-Mediated Communication, 13, 210-230.

Briggs, C. (1986). Learning How to Ask: A Sociolinguistic appraisal of the role of the İnterview in Social Science research. Cambridge University Press

Chermark S.M. and Weiss, A. (2005), Maintaining Legitimacy Using External Communication Strategies: An Analysis of Police-Media Relations, Journal of Criminal Justice, 33(5), (501-5012).

Cildan, C. M., Tumuçin, E. H. K. Küçük, E. Albayrak, D. (2012). "Sosyal Medyanın Politik Katılım ve Hareketlerdeki Rolü", Akademik Bilişim, Erişim: 05.09.2013, ab. org.tr/ab12/bildiri/205.doc

Cybercrimes: Infrastructure Threats from Cyberspace Lawyer, 4 No:2, Cyberspace Law 23. (Akt. Mehmet Özcan, Siber terörizm ve Ulusal Güvenlik: İnternet ve Hukuk, İstanbul: Bilgi Üniversitesi Yayınları, (2002), 309.

Çalı, H.H. ve Altunbaş, F. (2012), Güvenlik Hizmetlerinde Yönetişim Aracı Olarak Sosyal Medya Platformları, Sosyal Bilimler EKEV Akademi Dergisi, Sayı: 50, 2012/1, (1-10).

Elekoğlu, A.A. (2018), Web 1.0, Web 2.0, Web 3.0, Web 4.0 nedir? Aralarındaki fark nedir? Eğitime katkısı nedir?, https://prezi.com/p/2fxkwakcdgch/web-10-web-20-web-30-web-40-nedir-aralarndaki-fark-nedir-egitime-katks-nedir/ Erişim tarihi 02 Şubat 2020

Erdem, T. (2017). Sosyal Medya'da Terör Propagandası: DEAŞ Örneği, Gümüşhane Üniversitesi İletişim Fakültesi Elektronik Dergisi, (728-731).

Erdin, Ç. (2017). Radikal Selefi Örgütlerin Sosyal Medya Kullanımı: IŞİD Örneği, Bilge Uluslararası Sosyal Araştırmalar Dergisi, 1(2), (124-130).

Eren, V., Aydın, A., (2014). Sosyal Medyanın Kamuoyu Oluşturmadaki Rolü ve Muhtemel Riskler KMÜ Sosyal ve Ekonomik Araştırmalar Dergisi 16 (Özel Sayı I): 197-205.

Kartal, A. B., (2018). Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye'de DAEŞ ve YPG Örneği, Güvenlik Stratejileri, Sayı 27, (39-77).

Kazan, H. (2016). Terör Medya İlişkisi ve Medya Terör Haberciliği, Güvenlik Stratejileri Dergisi, Yıl 13, Sayı 24, 109-147.

Kernighan, B.W. ve Ritchie, D., (1978). The C Programming Language. Prentice Hall. s. 86, 207. ISBN 0-13-110163-3.

Korkmaz, İ. (2013), Facebook ve Mahremiyet: Görmek ve Gözetle(n)mek, Yalova Üniversitesi Sosyal Bilimler Dergisi, Vol.3, Sayı. 5, (107-122).

Kurum, M. (2017). Terörist Örgütlerin Güvenli Ortamları ve PKK. Ankara, Nobel Bilimsel Eserler.

Marcu, M. ve Bălteanu, C. (2014). Social Media–A Real Source Of Proliferation Of International Terrorism, Annales Universitatis Apulensis Series Oeconomica, 16(1), (162-169).

Mostchall, M. and Cao, L. (2002), An Analysis of the Public Relations Role of the Police Inquiry Information Officer, Sage Journal: Police Querterly, 5(2), (152-180).

Özçetin, D. ve Özçetin, B. (2015), Polis ve Sosyal Medya: Türkiye'de İl Emniyet Müdürlüklerinin Twitter Kullanımı, Uluslararası Kıbrıs Üniversitesi, Folklor/Edebiyat Dergisi, Lefkoşe, Cilt:21, Sayı:83, (19-48).

Özkır, Y., (2018). Fransa'da Basın Özğürlüğü Sarı Yelek'e Takıldı, https://www.aa.com.tr/tr/analiz-haber/fransada-basin-ozgurlugu-sari-yelek-e-takildi/1338759 Erişim tarihi 08 Eylül 2019

Patton, M.Q. (1987). How to use qualitative methods in evaluation, Newbury Park, CA: Sage

Pesen, M., (2017). Sosyal Medyanın Arap Baharı'ndaki Rolünün Bilimsel Kanıtı, www.e-siber.com Erişim Tarihi 08 Eylül 2019.

Steward C.J. ve Cash, W.B. (1985). Interviewing: Principles and Practices (4. Baskı), (Akt. Ali Yıldırım ve Hasan Şimşek), Dubuque, 10: Wn.C. Brown Pub

Yalçınkaya, İ. A. (2008). Medya-Terörizm İlişkisi, Yayınlanmamış Yüksek Lisans Tezi, Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü, Trabzon.

Yıldırım, A. ve Şimşek, H. (2018). Sosyal Bilimlerde Nitel Araştırma Yöntemleri, Ankara: Seçkin Yayınları.

Weimann, G. (2004). Special Report, How Modern Terrorism Uses the Internet, United States Institute of Peace, Washington.

Wilkinson, P. (1997). "The Media and Terrorism: A Reassessment", Terrorism and Political Violence, Vol. 9, No.2, 51-64.

Wilkinson, P. (2002). Terör ve Terörizm: Kavramlar, Özellikler ve Tipoloji, Silinen Yüzler Karşısında Terör (s. 142-163), Cemal Güzel (der.), Ankara: Ayraç Yayınları.

http://www.blog.isimtescil.net/vpn-nedir-ne-ise-yarar/ Erişim tarihi 14 Eylül 2019

http://www.ebizmba.com/articles/social-networking-websites Erişim tarihi 14 Eylül 2019

http://wearesocial.com/global-digital-report-2019 Erişim tarihi 12 Eylül

https://www.google.com/search?q=global+web+index+flagship+report+2019&oq=global+web+index+flagship+report+2019&aqs=chrome..69i57.40840j1j7&sourceid=chrome&ie=UTF-8 Erişim tarihi 11 Eylül 2019

http://www.onedio.com/haber/hashtag-nedir-nasil-olmalidir--308322 Erişim tarihi 02 Şubat 2020

https://www.haberturk.com/ekonomi/teknoloji/haber/1255438-satista-sira-twittera-geldi Erişim tarihi 02 Şubat 2020

https://sosyalmedya.co/facebook-ortaklar/ Erişim tarihi 02 Şubat 2020

https://www.bilimcag.com/nedir/web-1-0-2-0-3-0-nedirfarklari-nelerdir/ Erişim tarihi 02 Şubat 2020

ULUSLARARASI GÜVENLİĞİN TARİHSEL GELİŞİMİ VE POST-MODERN GÜVENLİK DÖNEMİ

Fikret BİRDİŞLİ*

Öz

Güvenlik insanoğlunun ontolojik kaygılarının başında yer aldığı gibi devletin varlık nedenlerinden de biridir. Bu nedenle güvenlik insanlık tarihiyle eş değer bir derinliğe sahip dinamik bir sosyo-politik olgudur. Bu bağlamda ilk çağlardan itibaren tehditler ve koruma alanlarında yaşanan değişime bağlı olarak güvenliğin içeriği ve icra biçimi de gelişerek önemini korumaya devam etmiştir. Özellikle ulus devletlerin ortaya çıkmasından itibaren uluslararası politikanın değişen nitelikleri ilk önce güvenlik alanında kendini hissettirmiş güvenlik kaygısı tamlayan ve tamlanan bir olgu halinde tüm devlet faaliyetlerine eklemlenerek ulusal ve uluslararası politikanın anahtar kavramlarından biri haline dönüşmüştür. Güvenlik olgusunun politikaya yansımasında yaşanan gelişmelere bağlı olarak güvenlik çalışmalarının nicelik ve nitelikleri de eşdüzeysel bir gelişim seyri izler. Bu kapsamda, epistemolojik düzlemde giderek gelişen kavramsal ve kuramsal çalışmalara rağmen güvenlik olgusunun tarihsel gelişimini açıklayan ve sınıflandıran çalışmalar göreceli olarak geri planda kalmıştır. Bu makale tarihsel ve betimsel analiz yöntemlerine dayalı olarak güvenlik olgusunun gelişimini antropolojik sınıflandırmalar yaparak açıklamayı hedeflemektedir. Bu bağlamda güvenlik tarihsel olarak Primitif Güvenlik, Modern Güvenlik ve Post-Modern Güvenlik dönemlerine ayrılmış ve her dönemin öznel niteliği ve evrimsel aşamaları özgün bir anlatımla açıklanmıştır. Bu kapsamda çalışmanın temel varsayımı güvenliğin dinamik, devinimsel gelişime tabi bir olgu olduğu yönünedir.

Anahtar Kavramlar: *Güvenlik, Ulusal Güvenlik, Uluslararası Güvenlik, Güvenlik Politikaları, Strateji.*

HISTORICAL DEVELOPMENT OF INTERNATIONAL SECURITY AND POSTMODERN SECURITY PERIOD

Abstract

Security is one of the ontological concerns of mankind and the reasons of existence of the state. Therefore, the security is a dynamic socio-political phenomenon which has profound value like human history. In this context, the security has kept its value and importance while changing and improving its content and implementations depending on the threats and protection areas since the early ages. Especially since the emergence of nation-states, the changing qualities of international politics have first been felt in the field of security. And the security concern has become one of the key concepts of the national and international politics by integrating to the state activities as a kind of descriptive concept. The Security studies also has followed similar trend and classified in different aspect in related with historical developments. But, studies on history of security has been shadowed by prevalence of political and practical aspect of the security phenomenon. Therefore this works firstly, leaning on the history of the security as an ontological and political phenomenon by developing a typology and then focuses on the last developments in context of the postmodern period by using of the descriptive analysis method. According to the findings of this researches anthropological sub categories of security phenomenon may be summaries by three stage as the Primitive Security Era, Modern Security Era and Post-Modern Security Era. In this context, the main assumption of the research is that the security is a phenomenon subject to dynamic development.

Keywords: *Security, National Security, International Security, Security Politics, Strategy*

* Doç.Dr., İnönü Üniversitesi, Staretjik Araştırmalar Merkezi, fikretbirdisli@inonu.edu.tr, ORCID ID: 0000-0003-3832-7749

Makale Geliş Tarihi: 04.11.2019 Makale Kabul Tarihi: 10.02.2020

GİRİŞ

Güvenlik, siyaset biliminde devletin var olma nedenlerinden ve uluslararası alanda ise aktörlerin karşılıklı ilişkilerini belirleyen temel referanslardan biri olarak karşımıza çıkmaktadır. Realist teorilerde merkezi bir kavram olan gücün ve güce dayalı sistem ve politikaların çerçeve kavramı olan güvenlik, koruma alanları, referans nesneler ve objektif amaçlar doğrultusunda anlam ve derinlik kazanır. Bu nedenle teori ve pratik açısından güvenlik ve güvensizlik hali arasındaki ilişki sonsuz bir açılıma sahiptir.

Güvenlik olgusunun epistemolojik zenginliği, güvenlik politikalarının üst düzey politika olarak kamu politikaları arasında önceliğe ve ayrıcalığa sahip olması akademisyenleri cezbederek bu alana yöneltmiş ve güvenlik çalışmalarının zenginleşmesine neden olmuştur. Özellikle askeri güç ve strateji çalışmalarının ağırlıklı olarak öne çıktığı Soğuk Savaş yılları güvenlik çalışanları için tarihsel fırsatlar yaratmıştır (Walt, 1991:213). Bu kapsamda güvenlik çalışmaları Soğuk Savaş yıllarından itibaren niteliksel olarak çeşitlenmeye başlamış; stratejik güvenlik, insani güvenlik, eleştirel güvenlik ve inşacı yaklaşımlar gibi başlıklar altında toplanan çalışmaların sayısı hızla artmıştır. Fakat bu içeriksel zenginliğe rağmen literatürde güvenliğin tarihsel gelişimi hakkında yapılan antropolojik çalışmalar oldukça sınırlı kalmıştır. Bu kapsamda yapılan az sayıda çalışmada ise daha çok etnisite ve kimlik gibi antropolojinin öznel alanlarına odaklanılmış, güvenliğin tarihsel evrimine yeterince değinilmemiştir. Örneğin Hurtado ve Ercolani (2013:12) tarafından yapılan *Antropoloji ve Güvenlik Çalışmaları* isimli editoryal çalışma güvenliğin tarihsel evrimine değil, bazı antropolojik kavramların güvenlik politikalarına olan etkisine odaklanmıştır. Benzer çalışmalar incelendiğinde güveliğin bir kavram ve olgu olarak tarihsel deviniminin dikkatten kaçtığı açıkça görülmektedir. Bu alanda en çok bilinen Barry Buzan ve Lene Hansen tarafından yazılmış olan "The Evolution of International Security Studies" isimli kitap ya da Ole Waever, Alan Collins, Stephen M. Walt gibi önde gelen güvenlik araştırmacılarının çalışmaları da daha çok Soğuk Savaş yılları gelişen Güvenlik alanını irdelemeye yöneliktir.

Bu çalışma ise literatürdeki bu eksiklikten yola çıkarak güvenlik olgusu ile güvenlik politikaları arasındaki antropolojik boşluğu tarihsel dönemler halinde sınıflandırarak doldurma amacını taşımaktadır. Bu maksatla çalışmada ilk olarak güvenlik olgusu tarihsel açıdan incelenerek ortaya dönemler halinde açıklanan yeni bir tipoloji çıkartılmıştır. Bu tipolojiye göre tarihsel başlangıçtan ulus devletlerin

ortaya çıktığı 17'nci yüzyıla kadar olan geniş dönem *Primitif Güvenlik Dönemi* olarak adlandırılmıştır. Bu dönem öncelikle kendi içinde *Pre-Teolojik Dönem* ve *Proto-Teolojik Dönem* olarak ikiye ayrılmıştır. 17'nci yüzyıl için başlangıç olarak kabul edilen 1648 yılından 1990 yılına kadar olan dönem ise *Modern Güvenlik* ya da *Sistemik Güvenlik Dönemi* olarak tanımlanmaktadır. Bu dönem de kendi içinde *Güç Koalisyonları Dönemi* ve *Güç İttifakları Dönemi* olmak üzere iki alt başlığa ayrılmış ve her birinin önde gelen dönemsel özelliklerine dikkat çekilmiştir. 1990'dan sonra devam eden süreç ise bu çalışmada *Post-Modern Dönem* olarak adlandırılmaktadır.

Çalışmada Post Modern dönem özel bir anlam ve ağırlık taşımaktadır. Çünkü Post-Modern dönem uluslararası sistem açısından güçler dengesi sistemine benzemekle birlikte tehditlerin farklılaşması, uluslararası alanın aktörleri, tehditler ve yeni koruma alanları ile güvenlik stratejileri açısından kendinden önceki dönemlerden oldukça farklıdır. Askeri açıdan Hibrit Savaş teknolojilerinin daha çok konuşulduğu bu dönemde uluslararası güvenlik açısından önem taşıyan şey uluslararası alanda var olan ya da ortaya çıkan risk ve tehlikelerin güvenlikleştirilerek uluslararası müdahaleye uygun hale getirilmesidir. Bu bağlamda Post Modern dönemde uluslararası politika, Yük Paylaşımına dayalı Ad-Hoc Koalisyonlar üzerinden işlemektedir. Ayrıca bu dönemi açıklamak için klasik teoriler yetersiz kaldığından bunlara ek olarak Güç Geçişi Teorisi, Yumuşak Dengeleme Teorisi, Keskin Güç (Sharp Power) gibi konseptlerden de yararlanılmıştır.

Post-Modern Güvenlik döneminde Soğuk Savaş yıllarına ait bazı stratejilerin güncellenerek hayata geçirildiği de görülmektedir. Bu stratejiler Tehdit Dengesi, Yeni Çevreleme, Önalıcı Savunma, Sessiz Sızma, Tutunma Bölgeleri ve Kültürel Angajman şeklinde sınıflandırılarak açıklanabilir. Post-Modern döneme ait teorik açıklamalar ve stratejik tanımlar İki Kutuplu Sistemin ardından uluslararası alanın yeniden biçimlendirilmesine intibak ettirici evrim (adaptive evolution) rolünü oynamaktadır. Bu nedenle Post-Modern döneme ait açıklamalar 1990 sonrası uluslararası sistemin olası yapısı hakkında bir meta teori niteliği taşır.

Çalışmanın genel içeriği ilk çağlardan itibaren ele alınan devinimsel ve evrimsel epistemoloji üzerine oturtulmuştur. Bu kapsamda bir sınıflandırmaya gidilerek ortaya özgün bir tipoloji çıkartılmıştır. Bu tipolojinin güvenlik çalışmalarında güvenlik kavram ve olgusunun anlaşılmasını, açıklanmasını kolaylaştırmanın yanı sıra geniş bir zaman dilimini içeren dağınık bir alanı toparlayacağı düşünülmüştür.

Çalışmanın temel sorunsalı güvenliğin antropolojik gelişimi hakkında yapılacak olan bir sınıflandırmanın ilk çağdan itibaren insan topluluklarının ekonomik ve sosyal gelişimi ile ilişkilendirilerek açıklanabileceği düşüncesine dayandırılmıştır. Çünkü ontolojik güvenlik, zaman içinde insan varlığına eklemlenen değerleri de koruma alanı içine alarak genişlemeye devam etmiştir. Bu kapsamda güvenlik olgusunun tarihsel değişimi bu çalışmada şu şekilde sınıflandırılmıştır:

1. Primitif Güvenlik Dönemi (MÖ - MS 1648)
   1.1. Pre-Teolojik Güvenlik Dönemi
   1.2. Proto-Teolojik Güvenlik Dönemi
2. Modern/Sistemik Güvenlik Dönemi (1648-1990)
   2.1. Güç/Güvenlik Koalisyonları Dönemi (1815-1945)
   2.2. Güç İttifakları Dönemi (1945-1990)
3. Post Modern Güvenlik Dönemi ve Yeni Güvenlik Stratejileri (1990'dan sonra)

1. PRİMİTİF GÜVENLİK DÖNEMİ

Primitif güvenlik dönemi, savunma, beslenme ve üreme sorunlarının insanın temel kaygıları arasında yer aldığı fakat tüm bunların karşılanmasına yönelik henüz örgütlü bir yapının oluşmadığı ilkel dönemden, devletlerin ortaya çıktığı ve geliştiği zamanlara kadar olan geniş bir zaman dilimini içermektedir. Bu zaman dilimi içinde insanın sosyolojik evrimi sırasında doğa koşullarına ve üretim biçiminin gelişmesine bağlı olarak algılanan tehditler de artarak derinleşmiştir. Bu nedenle bireysel güvenliğin zamanla kollektif güvenliğe evrildiği bu zaman dilimi, *Primitif Güvenlik Dönemi* olarak adlandırılmıştır. Ortak yaşamın gelişmesi zaman içinde kabileleri, etnik konsorsiyumları ve konviksiyumları daha gelişmiş bir model olarak devlete dönüştürürken bu gelişimin itici nedenlerinin başında güvenlik gereksinimlerinin geldiği unutulmamalıdır. Bu nedenle gerçek anlamda ilk güvenlik yapılanmasının devletin kendisi olduğu söylenebilir (Heywood, 2018:116).

Primitif güvenlik dönemi kendi içinde *Pre-Teolojik* ve *Proto Teolojik* dönemler olmak üzere ikiye ayrılır. Bu dönemlerin *teoloji* ile ilişkilendirilerek adlandırılmasının nedeni modern öncesi dönemlerde devlete itaatin aşkın güçler üzerinden sağlanmasıdır. Bu ayrım, çalışmalarında teolojiye yaptığı yoğun vurguyla dikkat çeken Agusto Comte'un "Üç hal yasası" ile de örtüşmektedir. Comte (1852)'a göre insan düşüncesinin gelişim evreleri olay ve olguları yorumlayış biçimiyle yakından ilişkilidir. Bu bağlamda ilk olarak insan etrafında olan biteni kendisi ile kıyaslanabilecek varlık ve güçlere mal ederek açıklamıştır. Doğada geçerli olan yasaları henüz keşfedemeyen insan, etrafında olan biteni

anlamak ve anlamlandırmak konusunda zihinsel olarak onu metafizik bir evreye sokan bir üst ve güçlü irade arayışına yönelmiştir. Fakat *Pre-Teolojik* olarak adlandırılan bu dönemde insan, doğadaki olayları açıklamak için Tanrı fikri yerine öncelikle tabiat kuvveti, cevher gibi niteliği belli olmayan olgusal kavramlardan yararlanmaktadır. Sonraki aşamalarda zamanla soyut düşünceyi geliştiren insanların soyut anlamlar yerine örgütlü dinler ile yaşamaya başlamasını Comte (1852,7), metafizik evre olarak tanımlamış, güvenlik bağlamında yürütülen bu çalışmada ise bu evre *Proto-Teolojik* evre olarak adlandırılmıştır.

Proto-Teolojik dönemin en önemli özelliği güvenlik bağlamında koruma alanlarının genişlemesidir. Yani Primitif dönemdeki güvenlik anlayışı bu dönemde ontolojik bağlamından öteye geçerek artı sermayeyi, üretimin temel kaynağı olan toprağı ve yeni toplumsal, üretimsel ilişkileri düzenleyen devlet aygıtını güvenliğin koruma alanı içine almıştır. İlerleyen dönemlerde Sosyo-politik gelişmeler *Proto-Teolojik* dönemi modern devletlerin ortaya çıkışıyla sonlandırmakla kalmayıp onu teolojik motivasyonundan soyutlayarak seküler bir anlayışla temellendirecektir. Bu aşama Comte'un pozitivist aşaması ile de örtüşmektedir.

Primitif Güvenlik dönemi *Pre-Teolojik* ve *Proto-Teolojik* dönemler şeklinde şu şekilde detaylandırılabilir.

1.1. Pre-Teolojik Güvenlik Dönemi

Pre–Teolojik dönemde insan doğaya karşı sürekli savunma durumunda olmuştur. İnsanın doğa karşısında güçsüz ve yetersiz olması onu dayanışmaya ittiğinden yaşamla ilgili her şeyde kolektif eylem ve sorumluluk duygusu hâkim olmuş ve ayrıca insanlar etrafında açıklayamadığı olayları aşkın bir güçle (sihir) ilişkilendirmiştir. Güvenlik olgusu açısından bu dönemin önde gelen özelliği güvenliğin koruma/savunma duygusu içinde bireysel ve küçük gruplar halinde sağlanmaya çalışılmasıdır. Zamanla diğer gruplarla olan işbirliği gelişerek siyasal toplulukların ilk nüvesi oluşturulmuşsa da bu ittifaklar oldukça gevşektir. Çünkü ortak tehdidin ortadan kalkmasıyla kolaylıkla çözülebilen bir yapılanmaya sahiptir. Bu nedenle *Pre-Teolojik* Dönem merkezileşmeden uzak çözülgen, akışkan gruplardan oluşan bir güvenlik yapılanmasına sahiptir (Fischer, 1994; Lewellen, 2011).

Pre-Teolojik Dönemde ilk olarak savunma silahları yapılırken uzmanlaşmanın artışıyla birlikte saldırı silahları ortaya çıkmış ve insanlar için toplayıcılıktan avcılık dönemine geçme olanakları yaratılmıştır (Şenel, 2001: 58).

Avcılık döneminde doğadan kaynaklanan dış tehditler azalmamakla birlikte buna avcı guruplar arası çatışma da eklenmiştir. Gruplar arasındaki çatışmalar ve savaşlar ise daha çok öç alma savaşları biçimindedir. Algılanan tehditler yine doğadan kaynaklanmakta ve yaşamı doğrudan etkilemektedir. O nedenle grup içi ve gruplar arası dayanışma herkes tarafından aynı şekilde algılanan somut egzojenlerden kaynaklanır. Bu dönemi inceleyen kimi bilim adamları avcılığın insanın bencil doğasından kaynaklanmadığı tersine ortak çalışma, işbirliği, paylaşma ve dayanışmaya yol açan bir olgu olduğu sonucuna ulaşmışlardır. Toplumda siyasal farklılaşma olmadığı için bu evrede henüz siyasal yapıdan söz edilemez.

Pre-Teolojik dönemde İnsan doğa arasındaki ilişki edilgen bir ekonomik ilişkiye dayalı olduğundan ve teknolojik yetersizlik nedeniyle insanlar kontrol edilemeyen bir yapı ile asimetrik ilişki içine girmişler, insan doğa ilişkisi düzensiz ve anarşik olarak tanımlanmıştır (Şenel, 2001:96). Buna karşın insanlar etrafında olan biteni anlayabilmek için bu olaylar arasında bir ilişki arayışına girerek kaostan, anarşiden kurtulmaya çalışmış ve bu ilişkiyi doğayı aşan güçlerle tanımlamışlardır. Bu nedenle antropologlar "sihirsel" düşünüşü teolojinin primitif formu ve insan topluluklarının ilk düşünsel biçimi olarak tanımlamışlardır (Şenel, 2001:99 ve Pritchard, 1965).[1]

1.2. Proto-Teolojik Güvenlik Dönemi

Bu dönemde öç alma savaşları bir grubun üretim kapasitesini bir başka grubun hilafına olarak artırmaya başladığı toprak savaşlarına dönüşmüştür. Bu nedenle grup içi ve gruplar arası dayanışma için başka motivasyonlara ihtiyaç duyulmaya başlanmış ve dini inanışlar kabile entegrasyonunun başlıca kaynağı haline gelmiştir.

Bu dönemde daha üst bir örgütlenme modeli olarak devletin ortaya çıkışı nüfus, çevre, teknoloji ve sulama gibi belirli ön koşulların ardışık biçimde belirli etkilere yol açtığı fikrine dayalı sentetik modellerle açıklanmaya çalışılırken güvenlik gereksinimi ise yeni koruma alanları ve savaş tehdidi gibi dış etkenler ve beslenmesi gereken daha büyük nüfusun varlığı ve tarımsal ilkel sermaye birikimi gibi iç etkenlere bağlı olarak açıklanmaya çalışılmıştır (Lewellen, 2011:83).

Proto-teolojik dönem üretim biçimine bağlı olarak iki farklı yapılanmayı bünyesinde barındıran düalist bir dönemdir. Şenel (2001:167)'e göre bitkilerin ve

[1] Teolojiyi sosyal evrim içinde ele alan antropologlar bu süreci totemizm, animizm, polytheism, monotheism olarak açıklamışlardır (Pritchard, 1965).

hayvanların evcilleştirilmeye başlanması neolitik çiftçiler ile neolitik çobanlar olmak üzere iki farklı toplumu ortaya çıkartmıştır. Çiftçiler için toprak sadece yararlanılan bir yer olmaktan çıkarak üzerinde sürekli yaşanılan, emek harcanarak biçimlendirilen ve geleceğe yatırım yapılan yer olmanın yanı sıra anıların yaşandığı gerektiğinde savunulması hatta uğrunda can verilmesi gereken yer haline gelmiş ve bu kapsamda vatan kavramı ile sınır algısını ortaya çıkartmıştır. Ayrıca çiftçilik, avcılık ve toplayıcılıktan daha fazla ve disiplinli çalışmayı gerektiren; içinden zanaat, ev ekonomisi ve zaman mefhumunu çıkartan, gelişmeye açık bir yaşam biçimidir. Bu durum insan ve toprak arasındaki bağı giderek güçlendirmiş ve ontolojik güvenliğin koruma alanı içine "toprağı" da "vatan" kavramı altında dâhil etmiştir. Bu aşamada insanlar artık diğer canlılardan farklı olarak, gündelik yaşam yerine yarını düşünen ve yarına hazırlanan varlıklardır.

Yaşam biçimindeki bu değişim, davranışların bu yeni hayat algısına göre uyarlanmasını gerektirmiş, yardımlaşma, dayanışma, hatta kan gütme gibi kurumların gelişmesine yol açmıştır. Hatta gelecek düşüncesi yarını da aşarak ölümden sonrasını içerecek biçimde genişlemiştir. Bu düşünceye ilham veren somut olgu kuşkusuz kendini sürekli yenileyen doğa olmuştur. Antropologlar öldükten sonra yeniden yeşeren doğanın bir analojiye neden olarak tohumlar gibi insanların da yeniden yaşama döneceği düşüncesini pekiştirdiği düşüncesindedirler (Krader,1968: 36). Bu düşünce monotheist dinlere doğru ilerleyen teolojik evrim sürecinin önemli bir katalizörüdür.

Neolitik çiftçilik kendine yeten bir ekonomi hatta gelecek yıl için ürün fazlası olarak ilkel bir sermaye birikimine elverişli bir yaşam biçimi iken, neolitik çobanların yaşam biçimi, üretmeye ve artı ürüne elverişli değildir. Neolitik çoban topluluklar taşıdıkları nicel ve nitel yetersizliği önce köyler arasında, ardından kentler arasında yapılan ticaret yoluyla geliştirdikleri barışçı ilişkiler veya yağmacılık yoluyla geliştirdikleri savaşçı ilişkiler yoluyla aşmaya çalışılmışlardır. Bu nedenle neolitik çoban toplulukların ekonomi ve yaşam biçimleri gurup içi dayanışmayı çiftçi toplumlardan daha farklı ve ileri boyuta taşıdığından egemen olma azmi ve tutkusu içeren bu durumu ifade etmek için İbn-i Haldun (2013: 172) Asabiyet kavramını kullanmıştır.

Araştırmacılar asalak ekonomiden üretici ekonomiye geçişin ve kabileden aşirete geçişin düşüncenin sihirden daha örgütlü bir düşünüş biçimi olan dinlerin ortaya çıkışını hazırladığını ileri sürmektedirler. Bu aşamada artık insanda doğaya direnme ve ona hâkim olma düşüncesi yerini, toplum içinde konumunu koruma,

güç edinme ve topluma egemen olmaya bırakmış, ilk sermaye birikimiyle birlikte de ticaret doğarak mülkiyeti güvenliğin koruma alanı içine almıştır.

Bu dönemin en önemli özelliklerinden bir diğeri de devletin ortaya çıkışıdır. Düalist toplum yapısının neden olduğu çelişkiler ve tehditler aynı zamanda bir güvenlik örgütlenmesi olarak devleti ortaya çıkartmıştır. Bu nedenle devlet her tür bireysel ve kolektif güvenliğin sağlanması hususunda zorunlu bir varlık halini almıştır.

Zaman içinde devletin güçlenerek zora dayalı dar bir iktidar erkine dayanması ve bu erke bağlı tüm unsurların toplumun büyük bir kesimi için güvenlik sorunu halini alması eleştirel düşüncelerin başlıca kaynağını oluşturur. Bazı düşünürler bu durumu insanın doğasına yükledikleri spekülatif anlamlarla açıklamaya çalışmışlar ve bu durumu devletin ortaya çıkış nedeninde yaşanan sapmaya bağlı bir anomali olduğunu ileri sürmüşlerdir. Örneğin; Marchel Gaucet (2005: 35-56)'e göre toplum halinde olma ihtiyacı insanın kendinden başka insanlara gereksiniminden kaynaklanmaktadır. Devlet ise insanın insana başka anlamlar yüklemesi, kendi var oluşları üzerinde söz söyleme yetkisinden yoksun ve kendi iç örgütlenmelerinin dışarıdan belirlendiğine, meşru kılındığına inanan toplumların ardılı olarak ortaya çıkmıştır. Leon Duguit (2005: 380-400) ise devletin bir sözleşme ile değil, egemen kılınmış buyurucu bir irade ile vücut bulduğunu ve bu iradenin topluma karşı ödevlerinden çok, haklara sahip olduğunu iddia ederek egemen bir devletin bir dışsal tarafından mutlak anlamda kontrol edilemez bir varlık olduğunu ileri sürmüştür.

Aslında devlete yönelik tüm bu ve benzeri spekülatif açıklamalar devleti ortaya çıkartan ontolojik güvenlik kaygılarını perdeleyerek zaman içinde devleti kendisiyle açıklanır bir fenomen haline getirmiştir. Nitekim devleti kendini oluşturan toplumdan ve ontolojik gereksinimden bağımsız olarak açıklamaya çalışan vurgular, onu bir araç olmaktan çıkartarak bizatihi amaç haline sokmuştur. Bu tarz yaklaşımların ve bizzat devlete yapılan aşırı vurgularla yapılan açıklamaların başında ise devleti din bağlamında açıklamaya çalışan teolojik yaklaşımlar gelir. Nitekim bu tarz yaklaşımın bir sonucu olarak Tanrı ve devlet arasında doğrusal bir ilişkinin kurularak devleti de aşkın bir değer haline getiren anlayışın doğduğu ve yaygınlaştığı bu dönem, bu çalışmada *Proto-Teolojik* dönem olarak adlandırılmıştır. *Proto-Teolojik* dönem dini kurumlar vasıtasıyla devleti öncelikle korunması gereken bir özne olarak sosyo-politik yaşamın ağırlık merkezi haline getirmiştir. Bu nedenle *Proto-Teolojik* dönemde güvenliğin referans nesnesi insan değil, devlettir.

2. MODERN/SİSTEMİK GÜVENLİK DÖNEMİ (1648-1990)

Modern Güvenlik Dönemi, siyasal toplumun birliğinin dini kurumlar üzerinden sağlanmasının son bularak iktidarın kaynağının toplum dışından bir olguya değil, bizzat topluma dayandırıldığı bir dönemi ifade eder. Teolojik kavramlarla ifade edilen ve tahkim edilen devletin varlığı, egemenliğin hukuki kaynağı olarak görülen ulus üzerinden açıklanmaya başlanmış fakat bu değişim devlete atfedilen önemi azaltmamıştır. Bu nedenle güvenliğin referans nesnesi yine insan değil bu kez egemenliğin hukuki kaynağı olarak görülen ulustur (Duguit, 2005: 387).

Bu yeni devlet anlayışı içinde iktidar, kendi toprakları üzerindeki zorlayıcı gücünü ilahi bir otoriteden azade olarak bir dizi kamusal yapıya atfederek kullanmaya başlamıştır (Spellman, 1998: 135). Fakat bu şekilde devletin güçlenen kamusal kişiliği ona kendi güvenliğini sağlamak konusunda önceki dönemlere kıyasla daha fazla esneklik sağlamıştır. Çünkü 1648 Westfalya Barışı'ndan sonra rasyonel ve kamusal bir varlık olarak ortaya çıkan sınırsal (teritorial) devletler diğer devletlerle kolaylıkla işbirliğine girebilen teolojik bağlardan azade yapılar halinde uluslararası alanda kolektif güvenlik yapılanmaları içinde yer almaya başlamıştır. 1789'da gerçekleşen Fransız devrimi ise teritoryal devletlere egemenlik ruhu olarak ulusal iradeyi aşılayarak uluslararası alanda işbirliği ya da çatışmanın nedeni olarak en az teolojik nedenler kadar güçlü ve onun kadar muğlak bir olgu olarak "ulusal çıkarları" yerleştirmiştir. Artık devletler diğer devletlerle ittifak geliştirebilecek genel iradeye sahip ve bu iradeyi başka bir güce karşı sorumluluk hissetmeden kullanabilecek yeni bir metafizik kült/bütün haline gelmiştir.

Modern Güvenlik Dönemi 1648'den başlayan ve 1990'lara kadar uzanan bir dönemi kapsamaktadır. Kendi içinde *Güç Koalisyonları Dönemi* ve *Güç İttifakları Dönemi* olarak ikiye ayrılan bu zaman diliminin en dikkat çekici ve travmatik yönü güvenlik açısından insanlık tarihinin en kanlı ve yıkıcı savaşlarını içermesidir. Bu kapsamda siyasal düşünceleri, devrimleri, akademik teorileri barındıran bir epistemolojik evren yaratan Modern Güvenlik Dönemi, düşünce tarihi ve pratikleri ile açıklayıcı teoriler açısından en hızlı yaşanan bir dönemi de içerir. Uluslararası alanın doğası, güç dağılımı, kurumlar, etkileşim gibi konular bu dönemde güvenlik bağlamında en çok tartışılan akademik konular olarak öne çıkmaktadır (Waltz,1988: 615-628; Wendt, 1992: 391-425).

Modern Güvenlik dönemi uluslararası alanın yapılanması, devletlerarası ilişkilerin sistemleşmesi açısından Güç/Güvenlik Koalisyonları ve Güç ittifakları şeklinde iki döneme ayrılarak incelenebilir.

2.1. Güç/Güvenlik Koalisyonları Dönemi (1792-1945)

Uluslararası alanda güç koalisyonları dönemi Napolyon savaşları ile birlikte 1792'de başlar, İkinci Dünya Savaşı'nın sonuna kadar devam eder. Bozulan Avrupa coğrafyasını yeniden düzenlemek üzere 1815'te yapılan Viyana Kongresi uluslararası alanda bir devletin diğer devletler tarafından tehdit ve tehlike olmaktan çıkartılması yönünde atılan ilk organize girişimdir (Uçarol, 2013:40). Bu nedenle Viyana'da ortaya çıkartılan statü, bir sürekli güvenlik yapılanması olarak var olan devletin yerine ya da yanına ad-hoc güvenlik koalisyonlarını eklemiştir. Bu yapı gerçekte, uluslararası alanda güvenliği güçlendirmekten çok uluslararası hukuku güçlendirecek koşulları yaratmıştır. Nitekim Kırım Savaşı sonucu toplanan Paris Barış Konferansı, Birinci Dünya Savaşı sonunda ortaya çıkacak olan ilk kolektif güvenlik yapılanmasının uluslararası hukuk açısından alt yapısını güçlendirerek, uyuma dayalı bir güçler dengesi ortaya çıkartmıştır.

Fakat uluslararası güvenlik açısından koalisyonlar kısa vadeli sonuçlar üretmiştir (Goldstein, 2014: 107). Bu koalisyonların daha dayanıklı ve dengeye kavuşması 2. Dünya Savaşı sırası ve sonrasında oluşan ittifaklarla mümkün olmuştur.

1792-1797 tarihleri arasında Avrupalı güçler arasında gerçekleşen Birinci Koalisyon Savaşları iç statükolarını korumak isteyen Avusturya ve Prusya'nın Fransa'ya karşı dayanışmasıyla başlamış Avrupa Güçler Dengesini tehlikede gören İngiltere, İspanya, Hollanda, Napoli, Toskana ve bazı Alman devletlerinin katılımıyla genişlemiştir. İkinci Koalisyon Savaşı ise 1798-1802 yıllarında yine Fransa karşısında güç birliği yapan Avusturya, Rusya, İngiltere arasında gerçekleşmiştir. Koalisyonların gevşek yapısı burada hızlıca kendini göstererek Rusya'nın savaştan erken ayrılmasına neden olmuştur. İkinci Üçüncü ve Dördüncü Koalisyon savaşları da statükoyu yani Güçler Dengesi sistemini korumaya yöneliktir (Uçarol, 2013: 23). Fakat bu dönem 1806-1807 yıllarında Fransa'nın öncülüğünde kurulan Ren Federasyonuyla bir güvenlik ittifakını ortaya çıkartması açısından da dikkat çekicidir. Napolyon'un devrilmesine kadar devam eden bu ittifakın sonu, Sovyetler Birliği'nin dağılması sonucu Varşova Paktı'nın uğradığı akıbete benzer.

Dördüncü Koalisyon Savaşı ise üç yeni güvenlik stratejisini ortaya çıkartmıştır. Fransa tarafından ilan edilen *Kıta Ablukası*, İngiltere tarafından ilan edilen *Deniz Ablukası* ve yine Fransa tarafından Rusya'ya karşı oluşturulan "*Doğu Avrupa Seddi*". Bu stratejiler ileride, Soğuk Savaş yıllarında Batı ittifakı tarafından kullanılan Çevreleme Politikasını çağrıştırmaktadır.

Avrupa'da yaşanan Koalisyonlar dönemi 1815'te Yedinci Koalisyon'un ardından ve Napolyon'un yenilgisi üzerine bir süreliğine ara vermiş oldu. Fakat 1856 yılında Osmanlı İmparatorluğu ve Rusya arasında başlayan savaşta İngiltere, Fransa ve İtalya, Rusya'ya karşı Osmanlı İmparatorluğu'nun yanında yer alarak 1856 yılında yapılan Paris Konferansı'nda Güçler Dengesini yeniden korumuş oldular. 1918'de başlayan Birinci Dünya Savaşı ise Ad Hoc kurulan Güç/Güvenlik Koalisyonları döneminin sonunu getirdi.

Birinci Dünya Savaşı'nın güvenlik tarihi ve güvenlik yapılanması açısından önemi uluslararası alanda güvenlik amacıyla kurulan ilk uluslararası örgütü, Milletler Cemiyeti'ni ortaya çıkartmasından kaynaklanır. Bu yapı her ne kadar uluslararası güvenliği korumada başarısız olmuş olsa da 1945 yılında kurulan halefi Birleşmiş Milletler için bir zemin ve birikim teşkil etmiştir.

1918 ve 1939 arasında geçen yirmi bir yıllık süre Birinci Dünya Savaşı'nın sonuçlarının ortaya çıkarttığı politik anomalinin kronik hale gelmesi ve yeni bir savaşın patlak vermesinin nedenleri ile dolu geçer. İkinci Dünya Savaşı boyunca kurulan savaş ittifakları ise Koalisyon dönemlerini hatırlatan biçimde konjonktürel olmuştur. Savaşın yaygınlığı ve yıkıcılığı uluslararası alanda cari olan güçler dengesinde yer alan devletleri her yönüyle zayıflatarak Savaş sonu oluşacak iki kutuplu yapılanma için gerekli koşulları hazırlamıştır.

Uluslararası İlişkiler disiplininde koalisyonlar dönemi Güçler Dengesi Sistemi adında bir makro model altında açıklanmıştır. Buna göre kurulan sistemin amacı öncelikle güvenliğin optimizasyonudur. Fakat koalisyonlar bazı devletlere stokastik avantajlar sağlayabilir. Bu durumun giderilmemesi koalisyonlara dayalı olan güçler sistemini zaman zaman dengesizleştirerek savaşlara neden olmuştur. Kaplan (2005,35)'a göre ad-hoc koalisyonlara dayalı güçler dengesi sisteminin öncelikli olarak dikkat çeken özelliği sistemin nükleer silahlanmaya dayanmaması ve sistemin koalisyonlar mantığına göre işlemesi için güçler dengesinde en az beş devletin yer almasıdır. Bu dengenin korunması için koalisyon mantığı gereği sisteme yeni bir aktörün girişi ya da daha önce sistem dışı kalmış bir aktörün yeniden sisteme girmesi mümkündür. Nitekim Birinci Dünya Savaşı'nın ardından Osmanlı İmparatorluğu, Alman İmparatorluğu ve Rusya gibi imparatorluklar sistemden düşmüş ve Japonya ile ABD gibi iki yeni aktör güçler dengesi sistemine dâhil olmuşlardır.

2.2. Güç İttifakları Dönemi (1945-1990)

Uluslararası Güvenlik tarihi bakımında 2. Dünya Savaşı bir dönüm noktasıdır. Çünkü bu savaş uluslararası alanda BM'yi içeren örgütsel bir monopol ile düalist bir güvenlik ittifakını ortaya çıkartmıştır. NATO-Varşova Paktı çerçevesinde oluşan bu düalist yapılanma İki Kutuplu Sistem olarak anılmaktadır.

NATO ve Varşova paktları uluslararası politika konusunda her biri kendine özgü ideolojik bir dünya görüşü ve stratejik birer vizyon içeren ittifaklardan oluşmaktadır. Güç dengesi sistemindeki koalisyonlarla karşılaştırıldığında Güç İttifakları döneminin her iki kutbun merkez ülkeleri etrafında oluşan devletlerle stratejik ortaklık içeren oldukça sıkı bir yapılanmaya sahip olduğu görülür. Bu dönemin önceki dönemden diğer bir farkı da güvenlik ittifakının konvansiyonel değil, nükleer silahlanmaya dayalı olmasıdır. Kaplan (2005: 38) iki kutuplu sistemin etkin bir lojistik ve büyük bir organizasyonel yapıya sahip olduğuna da dikkat çeker. Tüm bunlar güç ittifaklarının koalisyonlara göre daha dayanıklı, sıkı ve uzun ömürlü olmasının nedenlerini açıklar.

Güç ittifaklarının diğer bir özelliği de ittifak içinde yer alan devletlerin rakip bloğa karşı tek tek değil, blok olarak güçlerini geliştirme çabalarıdır. Bu kapsamda ittifak üyeleri grup içinde ağırlık kazanmaktan çok, kitle olarak karşılıklı büyük bir savaşa angaje olmuşlar ve ittifak içi teknoloji transferi mümkün olmuştur. Bu sayede bir devlete ait silah sistemi başka bir devletin topraklarında konuşlandırılarak ulusal güvenliğin blok güvenliği ile kaynaşmasına neden olmuştur.

Güç İttifakları döneminin diğer bir dikkat çeken yönü ise tarafsız ülkelerle ilgilidir. Koalisyon dönemlerinde koalisyon dışı kalan ülkeler uluslararası politikanın hızlandığı savaş ya da çatışma dönemlerinde tarafsız ya da işlevsiz kalmışlardır. Güç ittifakları döneminde ise blok dışı kalan ülkeler tarafsız kalmanın ötesine geçerek bloklar arası bir olası savaş tehlikesinin önüne geçmeye çalışmışlardır.

Özet olarak güç ittifakları döneminde devletlerin daha uzun vadeli, daha kalıcı ve ortak çıkarlara odaklandıkları; ittifakların silah sistemleri olarak nükleer güce dayandığı ve döneme uygun bir güvenlik yapılanmasının da katalizör olarak işlev gördüğü ve son olarak her iki ittifakta yer alan ülkelerin uluslararası politikayı ideolojik bir motivasyona dayalı olarak sürdürdükleri görülmektedir.

3. POST MODERN GÜVENLİK DÖNEMİ VE YENİ GÜVENLİK STRATEJİLERİ (1990'DAN SONRASI)

Post-Modern Güvenlik 1990'da İki Kutuplu sistemin ve dolayısıyla Güç İttifakları döneminin sona ermesinin ardından başlayan ve halen takip eden süreçtir. Bu dönemin Post-Modern Dönem olarak adlandırılmasının nedeni öncelikle postmodernizmin tanımıyla, ikinci olarak İki Kutuplu sistemin dağılmasının ardından uluslararası sistemde yaşanan belirsizliklerle alakalıdır.

Öncelikle postmodernizmin tanımından başlayarak yola çıkacak olursak, Postmodernizm sosyal ya da politik gerçekliğin özgün zaman ve mekân düzleminde eğreti bir biçimde sosyal olarak inşa edildiğini savunur (Devetak, 2005:162). Soğuk Savaş yıllarında İki kutuplu yapılanmaya olanak sağlayan ideolojik ve ekonomik motivasyonlar, Neoliberalizm'in "evrensel gerçekliği" ile Komünizmin "abartılı gerçekliği" üzerine sosyopolitik enstrümanlar kullanılarak inşa edilmişti. Sovyetler Birliği'nin dağılmasının öngörülemeyen zamanlaması Varşova Paktı hakkında inşa edilmiş sosyopolitik ve ekonomik "gerçekliğin" çökmesine neden olmuş ve yeni bir "öteki" inşa etmeye ise yeterli zaman kalmamıştır. Özellikle iletişim ve ulaşım teknolojilerinin gelişmesi, toplumların eskiye oranla uluslararası politika hakkında daha fazla ve farklı kaynaklardan fikir sahibi olmalarına olanak sağlamıştır. Bu nedenle Soğuk Savaş yıllarının ideolojik kutuplaşmasının dayandırıldığı resmi argümanlar zaman içinde esneyerek etkisini kaybetmiştir.

Varşova Paktı'nı oluşturan ittifakın ekonominin aşırı militarizasyonu nedeniyle dağılması ideolojik rekabeti de sona erdirmiş, ortaya çıkan bu durum NATO Paktı'nın oluşturan ittifakta da gevşekliğe neden olmuştur. Özellikle Varşova Paktı ittifakında yer alan çevre ülkelerin Batı ittifakında yer alan ülkelerle serbest ilişkiler geliştirebilme fırsatı elde etmesi, Batı ittifakında yer alan ülkelerin de yeni pazarlar edinme fırsatını değerlendirmeye çalışması ittifak üyelerinin birbirine penetrasyonunu artırmıştır.

Post Modern güvenlik dönemi iki kutuplu sistemin göreceli stabilizasyonundan mahrum kalınca özellikle eski Doğu Blokuna ait çevre ülkelerde sosyal hareketlenme ve reform talepleri yer yer iç çatışmalara ve savaşlara neden olmuştur. Diğer bir gelişme ise daha önce güç ittifakları içinde yer almayan, tarafsız kalmaya çalışan üçüncü dünya ülkelerinde, özellikle Arap ülkelerinde baş gösteren reform talepleri ve iç çatışmaların eski Sovyet ülkelerinde başlayan kitlesel halk hareketlerinin ardından baş göstermesidir.

Küresel güçlerce hazırlıksız yakalanılan ve kontrol edilmesinde güçlük çekilen bu dönemin yönetilmesi için eski ittifaklar yerine yeniden uluslararası koalisyonlara dönülmüştür. Bunun en önemli nedenlerinden biri de başta ABD olmak üzere küresel güçlerin yeni sistem arayışının ekonomik ve askeri maliyetini tek başlarına karşılamak istememeleridir (Waltz, 1993:54). Bu kapsamda Soğuk Savaş sonrası ortaya çıkan sistemsizlik ve hegemonik boşluk büyük güçleri ad-hoc koalisyonlarla ve vekâlet savaşlarıyla uluslararası sorunları yönetmeye yönlendirmiştir.

Post-modern dönem, uluslararası sistemde bir ara geçiş formu olarak görülebilir. Bu nedenle kendine has özellikler sergiler. Uluslararası alanda denge arayışlarının dayandırıldığı ya da ortaya çıkardığı reel politik düzlem farklı teorilere ve stratejilere dayalı olarak açıklanabilir. Bu kapsamda Post-modern dönemin teori ve stratejileri takip eden paragraflarda kısaca açıklanmaktadır.

3.1. Post-Modern Dönemi Açıklayıcı Teoriler

3.1.1. Güç Geçişi Teorisi

Güç geçişi teorisi uluslararası ilişkilere yapısal ve dinamik bir yaklaşımdır. Uluslararası alanda güçler arasındaki ilişkiyi ve sistem değişimini açıkladığı için realist teori içinde değerlendirilir. Fakat Güç Geçişi Teorisi sistem değişimini güçlerin işbirliği ve rekabeti ile açıkladığı için anarşi konusunda realizmden biraz farklılaşır. Bununla birlikte teori, dünya siyasetini yatay ve dikey bütünleşmiş olarak görmekte ve uluslararası alanda bir güç hiyerarşisine dayanmaktadır (Organski, 1968: 171).

Teoriye göre eski sistem içindeki hiyerarşide yer alan devlet ya da devletlerin göreceli olarak bir güç eşiğine ulaşması durumunda statüko ile olan ilişkisi bir çatışma potansiyeli taşır. Bu teoriyi ispatlamak için kullanılan makro veriler değişimin dinamiklerini ölçmek için kullanılır.

Ek olarak güç geçişi perspektifi iç savaşları öngörmek, ulus inşa sürecini anlamak, savaşın sonuçlarını hesaba katmak ve nükleer çatışma potansiyelini araştırmak için yaygınlaştırılmış ve başarıyla uygulanmıştır. Post-modern dönemde ise İki Kutuplu yapılanmanın merkez ülkeleri olan ABD ve Sovyet Rusya'nın hegemonik güçlerinin zayıflaması ve uluslararası alanda farklı kriterler dikkate alınarak tanımlanan yükselen güçlerin uluslararası politikanın geleceği üzerindeki olası rollerinin açıklanması için kullanılan bir teoridir.

3.1.2. Yumuşak Dengeleme Teorisi (Soft Balancing Theory)

Robert Pape ve T. V. Paul tarafından ortaya atılmıştır. 2003'te yaşanan Irak'ın işgalinin ardından ABD'nin tek taraflı müdahaleciliği karşısında diğer ülkelerin ABD'ye karşı geliştirdikleri tutum ve açıklamalardan yola çıkarak geliştirilmiştir. Thomas Mowle ve David Sacko (2007) "yumuşak dengelemeyi" "hiç dengelenmeyen dengeleme" olarak tanımlamaktadır.

3.1.3. Keskin Güç (Sharp Power)

Uluslararası İlişkiler literatüründe yer alan Sert Güç (Hard Power) kavramı askeri ve ekonomik gücün uluslararası politikada zorlayıcı bir unsur olarak kullanımını içermektedir. Yumuşak Güç (Soft Power) ise zorlamadan ziyade siyasal idealler ve politikalar başta olmak üzere güç unsurlarının yarattığı çekiciliğe dayandırılmıştır. Soğuk Savaş yıllarının ideolojik rekabet ortamında Yumuşak Güç de Sert Güç kadar kendisinden yararlanılan orta ve uzun vadeli bir strateji unsuru olarak öne çıkmıştır. Soğuk Savaşın sona ermesiyle askeri ve ideolojik rekabet yerini ağırlıklı olarak ekonomik rekabete bırakırken Yumuşak Güç unsurları ekonomik rekabetin bir katalizörü olarak daha fazla önem kazanmış ve Rusya, Çin gibi otoriter ülkeler liberal demokrasilerle kurulan ekonomik ilişkilerden yararlanarak uluslararası toplumdaki olumsuz imajlarını manipülasyon ve saptırma yoluyla değiştirmeye çabasına girmişlerdir. Bu bağlamda siyasal çoğunluğu ve ifade özgürlüğünü sistematik olarak baskılayan ülkelerin haber ve iletişim vasıtaları ile kültürel angajman unsurlarını kullanarak uluslararası alanda imaj ve itibar mühendisliği yapmaları Keskin Güç (Sharp Power) olarak adlandırılmıştır (Walker, 2017).

Keskin güç vasıtaları Post-modern dönemde uluslararası sorunlar karşısında ad-hoc ittifaklar kurmayı kolaylaştıran bir unsur olarak görülmektedir.

3.2. Post Modern Dönem Güvenlik Stratejileri

Küreselleşmenin etkilerine bağlı olarak uluslararası alanın aktörleri daha da artarak çeşitlenmiştir. Post Modern Güvenlik dönemi güçler dengesi ve ad-hoc koalisyonlar için yatkın bir dönem olduğundan devletler uluslararası alanın her türlü aktörleri ile örtülü ya da açık işbirliğine girmekte tereddüt göstermezler.

Uluslararası Örgütlerin sayısının artması, çok uluslu şirketlerin sayı ve sermayece etkin bir konuma ulaşmaları, teknolojiye ulaşım kolaylığı ve asimetrik avantajlar nedeniyle terör örgütlerinin uluslararası alanda bir aktör gibi etkinlik kazanmaları, kabile/aşiret bağlantıları, otonom yönetimler ve ulus üstü

örgütlenmeler uluslararası alanın geleneksel aktörleri olan devletlere yeni angajman alanları açmıştır (Goldstein, 2014: 16). Nitekim 1990 sonrası özellikle Ortadoğu'ya yapılan müdahalelerde müdahaleci güçlerin bölgede yer alan aşiret, kabile ya da etnik unsurlar gibi ulus altı yapılarla işbirliğine girdikleri görülmektedir. ABD ve müttefikleri tarafından Irak'a yapılan müdahale sırasında Kürt etnisitesinden ve hükumet karşıtı aşiretlerden yararlanılması ve Libya operasyonu bunun yakın örneklerindendir. Post-modern dönemde kullanılan güvenlik stratejileri, tehdit dengesi, yeni çevreleme, ön alıcı savunma, sessiz sızma, tutunma bölgeleri edinme ve kültürel angajman gibi yöntemleri içermektedir.

3.2.1. Tehdit dengesi (Balance of Therats)

Stephan Walt (1985) tarafından ortaya atılan bu teoriye göre coğrafi ve askeri konumu nedeniyle diğer bir devletten tehdit algılaması durumunda bir devletin izleyeceği tutumu ifade etmektedir.

3.2.2. Yeni çevreleme (Neo Containment)

ABD'nin 2001 sonrası Rusya, Çin ve İran'a karşı izlediği politika yeni çevreleme olarak adlandırılmaktadır (Wallender, 2005). Bu politikanın eski çevreleme politikasından farkı bu ülkelerin ideolojik bir tehdit değil, politik ve ekonomik bir tehdit olarak görülmeleridir.

3.2.3. Önalıcı Savunma (Forward Defence)

Amerikalı politika analisti Edward Luttwak tarafından tanımlanan bu strateji MS.4-5 yüzyıllarda Roma'nın uyguladığı defansif stratejiden türetilmiştir. Roma İmparatorluğunda barbar saldırılarının Roma sınırlarına dayanmadan önlenmesi amacını taşıyan bu taktik, günümüz uluslararası hukuk açısından oldukça tartışmalı sonuçlar üretir. ABD 11 Eylül saldırıları sonrasında Afganistan'a yönelik politikasını bu stratejiye dayandırmıştır.

3.2.4. Sessiz Sızma (Peaceful Penetration)

Askeri taktiklerden biri olan sessiz sızma, düşman hatlarına görünmeden yaklaşarak avantaj sağlayacak bilgi toplama ya da sorgulama amaçlı esir ele geçirme olarak bilinir. Post-modern güvenlik uygulamasında sessiz sızma post-modern angajman ve siber güvenlik önlemeleri ile birlikte yürütülmektedir.

3.2.5. Tutunma Bölgeleri (Foothold) Oluşturma

Küresel ve bölgesel güçlerin politik etki alanlarını kendi bölgelerinin dışına taşıyarak uluslararası politikada etkinlik kazanma çabaları sonucu ortaya çıkan askeri ve politik yerleşim alanları tutunma bölgeleri olarak adlandırılır.

Tablo-1. Büyük ve Bölgesel Güçlerin Tutunma Bölgeleri

Ülke	**Tutunma Bölgesi**
ABD	36 ülkede 550 askeri üssü var.
Rusya	Ermenistan, Belarus, Gürcistan, Kazakistan, Kırgızistan, Moldova, Suriye, Tacikistan, Ukrayna
İngiltere	Belize, Burunei, Bahreyn, Kanada, Kıbrıs, Almanya, Kenya, Nepal, Sigapur, Katar
Fransa	Çad, Cibuti, Gabon, Fidişi sahilleri, Lübnan Nijer, Senehgal, BAE
Çin	Tacikistan(Wakhan Koridoru yakını) , Cibuti/Deniz üssü
Hindistan	Buhutan, Madagaskar, Mauritius, Seychelles, Tacikistan
İtalya	BAE, Cibuti, Afganistan, Libya
Japonya	Cibuti
Türkiye	Kuzey Kıbrıs, Azerbaycan, Irak, Katar, Somali, Sudan, Suriye, Afganistan, Kosova/Bosna-Hersek

Tablo 1'de dokuz ülkenin tutunma bölgelerine yer verilmiştir. Bu ülkeler arasında en dikkat çekici olan Çin, Japonya ve Türkiye'dir. İkinci Dünya Savaşı'nın Amerikalılar tarafından hazırlatılan Japon Anayasasının 9'uncu maddesi gereği öz savunma güçlerinin dışında bir ordusu olmayan, devletin savaş açma hak ve yetkisi bulunmayan Japonya'nın güvenlik politikalarında 1980'lerin sonundan itibaren değişiklikler yaşanmaya başlanmıştır. BM'nin Barış gücünde bile yer almayan Japonya ilk kez 1990 yılında ABD'nin talebiyle Körfeze mayın tarama gemisi ve mühendisleri göndermiştir (Katzenstein, 1993: 108). 2011 yılında Çin'in yanı sıra Japonya da yurt dışındaki ilk askeri üssünü Cibuti'ye kurmuştur (Aslan, 2018).

Türkiye ise uzun süredir BM ve NATO kapsamında yurtdışına asker göndermesine karşın Katar, Somali ve Sudan'da kurmuş olduğu askeri üsler Türkiye'nin bölgesel bir güç olarak uluslararası politikada daha aktif rol almak istemesinin birer sonucudur (Ahval, 2019).

3.2.6. Kültürel Angajman

Kültürel angajman gerek Soğuk Savaş yıllarında yaşanan ideolojik rekabet ortamında Yumuşak Güç stratejisi olarak gerekse Soğuk Savaş sonrası hem Yumuşak Güç hem de Keskin Güç Stratejisi olarak kullanılan yöntemlerden biridir.

Post-Modern dönemde Kültürel Angajman unsuru olarak başvurulan en yaygın araçlar Öğrenci Değişim Programları ve Kültür Enstitüleridir. Örneğin Çin 2004 yılında yabancı ülkelerde Çin dilini ve kültürünü teşvik etmeyi amaçlayan Konfüçyüs Enstitüleri adında kar amacı gütmeyen kamu kurumları kurarak kendi araştırmalarına başladı. Bu kurumun Amerika Kıtasında 152, Avrupa'da 158, Asya'da 102, Afrika'da 42, Avustralya'da 17 olmak üzere toplam 471 şubesi bulunmaktadır (CI, 2019). Benzer şekilde Rusya'da Rus dilini ve kültürel mirasını yaymak, Rus sanat ve kültürünün örneklerini tanıtmak, yurt dışındaki Rus topluluklarını anavatanlarıyla yeniden bütünleştirmek amacıyla 2007 yılında Russkiy Mir Foundation kurulmuştur. Dünyanın tüm kıtalarında yüzlerce şubesiyle faaliyet gösteren bu merkez web siteleri, tarayıcılar, haber siteleri ve sosyal medyanın tüm olanaklarını kullanmaktadır (RM, 2019). Almanlar tarafından kurulan ve 1951 yılından itibaren faaliyet gösteren Goethe Enstitüsü, 1948'de kurulan Amerikan Heritage ve 1934'te kurularak bu tür etkinliklerin en eskisi olan British Council kültürel angajman faaliyetlerine verilebilecek örneklerin en önde gelenleridir. Bu faaliyetlere Türkiye'de 2007 yılında Yunus Emre Enstitüsünü kurarak katılmıştır. Türkiye'yi, Türk dilini, tarihini, kültürünü ve sanatını tanıtmak; bununla ilgili bilgi ve belgeleri dünyanın istifadesine sunmak; Türk dili, kültürü ve sanatı alanlarında eğitim almak isteyenlere yurt dışında hizmet vermek; Türkiye'nin diğer ülkeler ile kültürel alışverişini arttırıp dostluğunu geliştirmek amacıyla kurulan bu enstitü diğer ülkelerde ellinin üzerinde şubeye sahiptir (YEE, 2019).

3.3. Ulusal Güvenlik Devletleri

Ulusal güvenlik devletleri ulusal güvenlik kaygılarının veya çıkarlarının devlet politikaları için temel motivasyon ya da referans olarak kabul edildiği devletlerdir. 1947 yılında ABD'de çıkartılan Ulusal Güvenlik Yasasıyla birlikte Ulusal Güvenlik Konseyi, istihbarat birimleri, koordinasyon birimleri ve ulusal güvenlik danışmanları gibi güvenlik yapılanmaları devlet teşkilatı içinde yer almaya başlamış ve ulusal güvenlik prensipleri referans politika olarak tüm devlet faaliyetlerini etkilemeye başlamıştır (Birdişli, 2017: 43). Nelson-Pallmayer (1992) ABD örneğinden yola çıkarak ulusal güvenlik devletleri ile ilgili ayırt edici nitelikleri açıklamıştır.

Sovyetler Birliği'nin dağılmasının ardından eski Sovyet coğrafyasından on beş bağımsız devlet ortaya çıkmıştır. Bu devletler bağımsızlıklarının ardından ekonomik ve finansal çöküş yaşamışlar, zayıf devlet yapılanmaları ve sınır sorunları nedeniyle iç çatışmalar yaşamışlardır. Rüşvet, yolsuzluk, siyasal istikrarsızlık, sosyal parçalanmışlık Doğu Avrupa ve Orta Asya'da Renkli devrimler olarak adlandırılan sosyo-politik hareketlenmelere ve kitlesel eylemlere neden olmuştur (Goldstein, 2014: 34). İlk kez Sırbistan'da başlayan ve ardından Gürcistan, Abhazya, Ukrayna, Kırgızistan'a sıçrayan bu kitlesel eylemler içerdiği yöntemler ve karşı önlemler açısından adeta eski ile yeni dönemin karşılaşmasıdır. Rusya bu eylemlere karşı yerel yöneticileri askeri, ekonomik ve politik açıdan desteklemiş ya da Ukrayna'da olduğu gibi bizzat güç kullanarak bastırmıştır (Berzina, 2014).

1991'de Doğu Avrupa ve ardından Orta Asya'da başlayan bu kitlesel eylemler 2001'de Kuzey Afrika yoluyla Arap ülkelerine sıçramıştır. Arap Baharı olarak adlandırılan bu süreçte daha önce Batı öncelikle eylemcileri desteklemiş, fakat bu ülkelerde yapılan demokratik seçimlerin sonucunda İslamcıların iktidara gelmesi ya da güçlenmesi sonucunda bu desteğini geri çekmiştir. Yaşanan bu gelişmelerden sonra Arap Baharının yaşandığı ülkelerde bazı yapısal değişimler yapılmışsa da bunlar kozmetik düzenlemelerin ötesine geçmemiştir. Bu nedenle iç politikaları parçalı hale gelen bu devletler, siyasal konsensüsü sağlamak amacıyla ülkelerini maceracı dış politikaya yönlendirerek siyasi gündemi ulusal güvenlik sorunları ile meşgul etmeye başlamışlardır.

Ulusal güvenlik devletlerinin ilk özellikleri sosyal ve politik açıdan parçalı bir yapıya sahip olmalarıdır. Bu nedenle merkezi otorite yasa ve kurumsallık yerine

lider kültüne dayandırılmıştır. İkinci özellikleri ise ordunun siyaset üzerindeki etkinliği ya da ulusal güvenlik çıkarları bağlamında dış politika konularda en yüksek otorite olmasıdır. Bir Ulusal Güvenlik Devletinde, ordu devletin bütün iç ve dış düşmanlara karşı güvenliğini garanti etmekle kalmaz, toplumun genel yönünü belirlemeye de yetecek güce sahiptir. Ulusal Güvenlik Devletinde, ordu, siyasi, ekonomik ve askeri işler üzerinde önemli bir etkiye sahiptir. Ulusal Güvenlik Devletlerinin üçüncü özelliği ise bu ülkelerde demokrasinin, seçimin ya da diğer liberal demokrasi formlarının küçümsenmesi itibar görmemesidir. Bu devletler demokratik görünümünü korumakla birlikte karar sürecinde asıl güç ordu ya da daha geniş bir Ulusal Güvenlik Kuruluşuna aittir.

Ulusal Güvenlik Devletinin diğer bir özelliği de savunma sanayi ve ilgili sektörlerin siyaset ve ekonomi üzerinde önemli etkilerinin olmasıdır. Bu devletlerde belirli ellerde sermaye birikimi oluşmasının ülkenin gelişmesine katkı sağlayacağı düşüncesine dayalı olarak makul karşılarlar.

Ulusal güvenlik devletlerinin diğer bir önemli özelliği ise ulusal kimliklerini de güvenlik üzerinden tanımlamalarıdır. Sürekli düşman tehdidi altında ya da hiç dostlarının olmadığına olan inanç etraflarıyla olağan ilişkiler geliştirmelerine mani olur. Hatta bu nedenle kendi bölgelerinde yer alan ülkelerle yaşadıkları karşılıklı sorunları güvenlikleştirerek bölge dışında ittifak arayışı içindedirler.

Ulusal Güvenlik Devletinin diğer bir özelliği iç politikada muhalefete karşı tutumun tahammülsüz oluşudur. Bu kapsamda siyasete sivil katılım ve tartışmayı ulusal güvenlik gerekçeleriyle sınırlayarak kamuoyunun tek taraflı bilinmesine neden olmalarıdır. Bu noktada ulusal güvenlik tartışılmaz ve temel bir gerekçe olarak fikir, ifade, basın basta olmak üzere pek çok özgürlüğe kısıtlama ve denetim getirir.

Ulusal Güvenlik devletleri karar sürecinde merkezileşme ve toplumda çoğulculuğun baskılanması nedeniyle diğer devletlerle olan ilişkilerini bir denetim ve kontrol mekanizmasından bağımsız olarak yürüttüklerinden dış etkilere, manipülasyona ve yönlendirmelere açık biçimde yürütürler. Bu tür devletler iç politikada otoriter uluslararası politikada ise edilgendirler. Bu nedenle ulusal güvenlik devletleri ad-hoc koalisyonlar için yatkın ve vekâlet savaşları için uygun hedeflerdir.

Tablo-2. Modern Güvenlik ve Post-Modern Güvenlik Dönemleri Karşılaştırması

	Modern Güvenlik Dönemi, 19-20'nci Yüzyıl (1815/1856-1990)	**Post-Modern Güvenlik Dönemi 21'nci Yüzyıl, (1990-)**
Açıklayıcı Teori	Hegemonik İstikrar Teorisi (Hegemonic stability Theory), Sert Güç/Yumuşak Güç	Güç Geçişi Teorisi (Power Transistion Theory), Yumuşak Dengeleme Teorisi (Soft balancing theory), Keskin Güç (Sharp Power),
Güvenlik Stratejileri	Güç Dengesi (Balance of Power) Çevreleme (Containing theory) Nükleer Caydırıcılık (Nuclear deterence)	Tehdit dengesi (Power of threats) Yeni çevreleme (Neo-containing) Önalıcı savunma (Forward Defence) Sessiz Sızma (Peaceful Penetration) Tutunma Bölgeleri (Foothold) Kültürel Angajman
Güvenlik Yapılanması	Güvenlik Koalisyonları Güvenlik İttifakları	Ad-hoc koalisyonlar ve Ulusal Güvenlik Devletleri
Uluslararası Sistem	Avrupa Uyumu/İki Kutuplu Sistem	Tek kutupluluk/ ?
İdeoloji	Liberal Demokrasi/Komunizm	İl-liberal Demokrasi/Yeni muhafazakârlık

SONUÇ

Güvenlik insanın temel kaygılarından biri olduğu gibi insan topluluklarının antropolojik gelişimiyle uyumlu bir sosyopolitik evrime sahiptir. Bu kapsamda güvenlik öncelikle bireysel ontolojik kaygı, toplumsal kolektif eylem, daha sonra devlet için üst düzey politika haline dönüşmüştür. Güvenlik insan ve toplulukları için temel bir duygu, kaygı ve sürekli bir arayış olduğu için her zaman birey ve toplumların amaçlı davranışlarında içkin olarak yer almış ve bu nedenle de siyasal yaşamda bir aksiyom olarak kabul edildiğinden siyasette varlığı öznel anlamda çok dikkat çekmemiştir. Fakat zaman içinde devlete yüklenen anlam ve amaç açıklık kazandıkça güvenlik, ilk kez 17'nci yüzyılda Thomas Hobbes tarafından devletin varlık nedenlerinden biri olarak açıkça ifade edilmiş, 19'uncu yüzyıla yaklaşırken uluslararası politikanın sistematik bir hal almasıyla reel politika içinde öncelikle takip edilen bir ulusal çıkar olarak tüm devlet davranışlarını yönlendirmeye başlamıştır.

Soğuk Savaş döneminde iki kutuplu sistemin rekabet ortamında güvenlik, ittifak tutumu içinde gözetilen ortak bir eyleme dönüşerek uluslararası güvenlik halinde ifade edilmeye başlanmış ve uluslararası politikanın temel unsuru haline

dönüşmüştür. Güvenliğin kutuplar arası rekabettin merkezinde yer alması başta askeri uzmanlar, stratejistler olmak üzere akademisyenlerin de dikkatini çekmiş ve güvenlik çalışmaları başlıca bir alan olarak uluslararası ilişkiler disiplini içinde yerini almıştır. Zaman içinde eleştirel ve inşacı çalışmalar güvenliğin kapsam ve içeriğini genişletirken multidisipliner çalışılmaya başlanan güvenlik konusu bir olgu, politika ve disiplin olarak tehditler, çıkarlar ve koruma alanları bağlamında ele alınan, çalışılan modern bir fenomen haline dönüşmüştür.

Güvenliğin insanlık tarihiyle başlattığımız bu tarihsel derinliğine rağmen güvenlik çalışmaları yakın bir dönemde, Soğuk Savaş yıllarında başlamıştır. Fakat güvenlik konusu akademik çalışmalarda analitik ve vizyoner bir kavram olarak kullanıldığından tarihsel gelişimine ait çalışmalar göreceli olarak kısır kalmıştır. Bu nedenle bu makalede güvenlik olgusunun tarihsel seyri insan topluluklarının antropolojik gelişimiyle ilişkili olarak başlangıçtan itibaren ele alınarak güvenliğin evrimini günümüze kadar içeren bir sınıflandırma yapılmıştır. Buna göre güvenlik üç dönem altında incelenebilecek bir tarihsel olgudur. İnsanlığın ilk dönemlerinden modern devletin ortaya çıkışı için bir başlangıç olan 17'nci yüzyıla kadar geçen geniş zaman dilimi Primitif Güvenlik olarak adlandırılmaktadır. Primitif Güvenlik Dönemi kendi içinde Pre-Teolojik Dönem ve Proto-Teolojik Dönem olarak ikiye ayrılır. Primitif Dönem bireysel güvenliğin kolektif güvenliğe dönüştüğü ve güvensizlik duygusu ile ilgili algının insan düşüncesinin gelişimini anlatan sosyolojinin üç hal yasası ile uyumlu gelişim seyrettiği bir dönemdir. Bu dönem devletlerin ortaya çıkışını da içerdiği için güvenliğin devlet davranışı içinde içkin olarak yer aldığı fakat neden ve sonuçlarının toplum dışı ve siyaset üstü unsurlarla ilişkilendirildiği bir dönem olduğu düşünülmektedir.

Modern güvenlik dönemi ise modern devletlerin ortaya çıkışıyla birlikte güvenliğin rasyonel bir politika olarak devlet davranışını yönlendirmeye başladığı dönemi ifade eder. Artık güvenliğin motivasyonu ilahi irade ya da aşkın devlette değil ulusal iradede aranmaktadır. Bu dönem devletlerin güvenlik çıkarlarını diğer devletlerle olan ilişkilerinde oluşturdukları dengeler üzerinden ve kolektif devlet davranışlarıyla gerçekleştirdikleri bir dönemdir. Bu denge siyasetinin ve kolektif tutumun niteliğine göre Modern Güvenlik Dönemi kendi içinde Güvenlik Koalisyonları ve Güvenlik İttifakları olarak ikiye ayrılmıştır. Güvenlik Koalisyonları devletlerin güvenlik çıkarlarını geçici işbirlikleri içinde gerçekleştirmeye çalıştıkları bir dönemdir. Güvenlik İttifakları ise koalisyonlara göre daha dayanıklı ve uzun süreli stratejik ortaklıkları içerir. Soğuk Savaş

yıllarında ortaya çıkan iki kutuplu yapılanma birer güvenlik ittifakı olan NATO ve Varşova Paktı etrafında şekillenmiştir. 1990 yılında iki kutuplu yapılanmanın sona ermesi güvenlik ittifaklarının da sonunu getirmiş fakat uluslararası alanın nasıl bir sistemsel yapıya bürüneceği zaman içinde açıklığa kavuşacağından ulusal ve uluslararası güvenlik yeniden ad-hoc koalisyonlarla sağlanmaya başlanmıştır. Soğuk Savaş döneminin ardından yaşanan bu döneme ise bu makalede Post-Modern güvenlik dönemi adı verilmiştir.

Post-Modern Güvenlik Döneminin en önemli özelliği uluslararası güvenliğin ad-hoc koalisyonlarla sağlanmasıdır. Dönemin koşullarına uygun strateji ve politikalar içeren Post-Modern Dönem insanlığın tüm teknolojik birikiminin güvenlik amaçları doğrultusunda birlikte kullanıldığı bir dönem olduğu için içerik ve yöntem olarak oldukça kapsamlı ve farklılaşmış politikalar ihtiva etmektedir. Ayrıca bu dönem uluslararası sistemin bir dengeye ulaşmasına kadar geçen bir ara geçiş formu niteliği taşır. Bu kapsamda Güç Geçişi Teorisi, Yumuşak Dengeleme Teorisi, Keskin Güç Post-Modern dönemi açıklamak için kullanılabilecek teorilerdir.

KAYNAKÇA

Ahval News, (2019). "Turkish Military", https://ahvalnews.com/turkish-military/significance-turkeys-overseas-military-bases (Erişim: 27.09.2019).

Aslan, A. (2018). " Kızıldeniz'deki askeri üsler ve Türkiye'ye teslim edilen Sevakin Adası", https://www.gzt.com/dunya-politika/kizildenizdeki-askeri-usler-ve-turkiyeye-teslim-edilen-sevakin-adasi-2953315 (Erişim tarihi: 27.09.2019).

Berzina, I. (2014). *Color Revolutions: Democratization, Hidden Influence, or Warfare?* 01. Riga. https://www.naa.mil.lv/sites/naa/files/document/1_WP2014 Color revolutions.pdf. (Erişim:27.09.2019).

Birdişli, F. (2017). *Teori ve Pratikte Uluslararası Güvenlik*. 3'ncü baskı. Ankara: Seçkin Yayınları.

Comte, A. (1852). *Catechisme Positiviste*, http://classiques.uqac. ca/classiques/ Comte_auguste/catechisme_positiviste/catechisme_positiviste.pdf (Erişim: 10,02,2020).

CI, (2019). *Confucius Institutes: A decade of Culture*. http://www.bjreview.com.cn/special/confucius_institutes_a_decade_of_culture.html (Erişim: 25 Ekim 2019).

Devetak, R. (2005). *Theory of International Relation*. 3rd edn. Edited by S. and others Burchil. New York: Palgrave Mc Millian.

Duguit, L. (2005). 'Egemenlik ve Özgürlük', in Cemal Bali Akal (ed.) *Devlet Kuramı*. 2'nci baskı. Ankara: Dost Kitapevi, ss. 379–400.

Fischer, J. (1994). *Risiko Deutschland: Krise und Zukunft der deutschen Politik*. Köln: Verlag Kiepenheuer & Witsch.

Gaucet, Marcel (2005). 'Anlam Borcu ve Devletin Kökenleri. İlkellerde Din ve Siyaset', *Devlet Kuramı* (Ed. C.Bali Akal) Ankara: Dost Kitapevi, ss. 33–67.

Goldstein, Joshua S., J. C. P. (2014). *International Relations*. 10'ncu baskı, New Jersey: Pearson.

Heywood, Andrew (2018). *Siyaset*. (19'ncu baskı), Ankara: BB101 Yayınları.

Hurtado, F. A. ve G. E. (2013). *Antropoloji ve Güvenlik Çalışmaları*. USA: Universidad de Murcia.

İbn-i Haldun, (2013), *Mukaddime*, İstanbul: İlgi Kültür Sanat Yayıncılık.

Katzenstein, P. J. and N. O. (1993). 'Japan's National Security: Structures, Norms, and Policies', *International Security*, 17(4), The MIT Press.

Krader, L. (1968). *Formation of The State*. Nrw Jersey: Prentice Hall.

Kaplan, Morton A. (2005). *System and Process in International Politics*. Colchester: ECPR Press.

Lewellen, T. C. (2011). *Siyasal Antropoloji*. Ankara: Bileşik Yayınevi.

Organski,A.F.K (1968), *World Politics*, (2d ed.) New York: Alfred A. Knopf.

Pallmeyer, J. N. (1992). *Brave New World Order: Must We Pledge Allegiance?* Oregon: Orbis Book.

Pritchard, E. E. E. (1965). *Theory of Primitive Religion*. London: Oxford University Press.

RM (2019). *Russkiy Mir Foundation*. Available at: https://russkiymir.ru/en/rucenter/what-is.php (Accessed: 25 October 2019).

Spellman W. M. (1998). *The Emergence of the Modern State*. London: Palgrave Publication.

Şenel, A. (2001). *İlkel Topluluktan Uygar Topluma*. 6th edn. Ankara: Bilim ve Sanat Yayınları.

Uçarol, R. (2013). *Siyasi Tarih*. Ankara: Der Yayınları.

Walker, C. and J. L. (2017). 'The Meaning of Sharp Power', *Foreign Affairs*, (Nov 16). https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power. (Erişim 27.09.2019).

Walt, S. M. (1985). "Alliance Formation and the Balance of World Power", *International Security*, Vol. 9, No. 4 (Spring, 1985), pp. 3-43.

Walt, S. M. (1991). 'The Renaissance of Security Studies', *International Studies Querterly*, 35(2), pp. 211–239.

Waltz, K. N. (1993). 'Emerging Structure of International Politics', *International Security*, 18(2).

Waltz, K.N., (1988). "The Origins of War in Neorealist Theory", *The Journal of Interdisciplinary History*, Vol. 18, No. 4, (Spring, 1988), pp. 615-628.

Wendt, Alexander, (1992). "Anarchy is What States Make of it: The Social Construction of Power Politics", *International Organisations*, v.46/2. pp.391-425.

YEE (2019). *Yunus Emre Enstitüsü*. Available at: https://www.yee.org.tr/ (Erişim: 25 Ekim 2019).

RADİKALLEŞMENİN ÖLÇÜLMESİ: AŞIRICILIK ÖLÇEĞİNİN VE AŞIRICILIK ÖLÇEĞİ İLE İLİŞKİLİ ŞİDDET YANLILIĞI VE YASA DIŞI DAVRANIŞLAR ÖLÇEĞİNİN TÜRKÇEYE UYARLANMASI

Zuhal YENİÇERİ[*], E.Öykü US[**]

Öz

Radikalleşme, özellikle terörizm ile olan ilişkisi nedeniyle son yıllarda farklı disiplinler tarafından dikkatle mercek altına alınan bir kavram olmuştur. Radikalleşmenin ve radikalleşmenin nedenlerinin anlaşılması, toplumsal güvenliğin sağlanması ve toplumsal düzenin sürdürülmesi açısından büyük önem taşımaktadır. Bu nedenle, bu konularda yapılacak araştırmalara ve bu araştırmalara yön verecek ölçüme araçlarının oluşturulmasına ve geliştirilmesine ihtiyaç duyulmaktadır. Mevcut araştırmanın amacı, radikalleşme kavrama ilişkin farklı boyutların ölçülebilmesi için iki ölçeğin Türkçeye kazandırılmasıdır. Bu amaçla iki çalışma yapılmıştır. Birinci çalışmada Aşırıcılık Ölçeği ve Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeği Türkçeye uyarlanmıştır ve Etnik Kimlikle Özdeşim Ölçeği, Sosyal Mesafe Ölçeği ve gruplararası ayrımcılığı ölçen Tajfel Matrisinin varyasyonu ile ilişkileri incelenerek geçerlik ve güvenirlik analizleri yapılmıştır. İkinci çalışmada ise bu ölçeklerin doğrulayıcı faktör analizleri yapılarak sosyal baskınlık yönelimi ile ilişkileri incelenmiştir. Söz konusu ölçeklerin, radikalleşme konusunda Türkiye'de gerçekleştirilecek görgül çalışmalara ölçme aracı sağlayacağı düşünülmektedir.

Anahtar Kelimeler: *Terörizm, Radikalleşme, Aşırıcılık, Aşırıcılık Ölçeği, Sosyal Psikoloji*

MEASURING RADICALIZATION: ADAPTATION OF THE EXTREMISM SCALE AND PRO-VIOLENCE AND ILLEGAL ACTS IN RELATION TO EXTREMISM SCALE TO TURKISH

Abstract

In recent years, radicalization has become a topic of interest which has been carefully put a spotlight on by many different scientific disciplines, especially due to its relationship with terrorism. Understanding radicalization and its causes is of great importance for maintaining social order and security. Thus, there is a need for research and development of measurement tools that will guide these researches. The aim of the current study is to adapt two scales used for measuring radicalization into Turkish. With this purpose in mind, two studies were conducted. In the first study, the Extremism Scale and Pro-Violence and Illegal Acts in Relation to Extremism Scale were translated into Turkish; and their psychometric properties were examined by interpreting their relations with Ethnical Identity Scale Social Distance Scale and a variation of a Tajfel Matrix measuring intergroup discrimination. In the second study, confirmatory factor analyses of these scales were conducted, and their relationships with social dominance orientation were investigated. It is assumed that these abovementioned scales will provide as a tool for empirical studies of radicalization in Turkey.

Keywords: *Terrorism, Radicalization, Extremism, Extremism Scale, Social Psychology*

[*] Dr. Öğr. Üyesi, Başkent Üniversitesi Fen Edebiyat Fakültesi Psikoloji Bölümü, zuyen@baskent.edu.tr, https://orcid.org/0000-0001-9228-9961

[**] Arş. Gör., Başkent Üniversitesi Fen Edebiyat Fakültesi Psikoloji Bölümü, elifoyku@baskent.edu.tr, https://orcid.org/0000-0002-6671-2129

Makale Geliş Tarihi: 28.10.2019 Makale Kabul Tarihi: 17.02.2020

GİRİŞ

Terörizmin geçmişi çok eskilere dayanmakla birlikte modern terörizm, gündemden hiç düşmeyen evrensel bir tehdit olmayı sürdürmektedir. Farklı dönemlerin çeşitli evrensel etkilere sahip olayları ile birlikte değişen ve dönüşen terörizm (Rapoport, 2004), özellikle 11 Eylül 2001'de ABD'de gerçekleştirilen terör saldırılarının ardından akademik çevrelerce daha fazla tartışılmaya başlanmıştır. Terörizmin nedenleri, diğer bir ifadeyle bireyleri ve grupları terörist eylemlerde bulunmaya yönlendiren unsurlar mercek altına alınmıştır. Birçok araştırmacı, bireylerin ve grupların terörist olmalarıyla sonuçlanan süreçlerin anlaşılmasının, terörizmle mücadelede büyük öneme sahip olduğunu vurgulamaktadır. Bu nedenle, söz konusu süreci ifade eden radikalleşme konusunun son yıllarda çalışmaların odak noktası olduğu görülmektedir (McCauley ve Moskalenko, 2017).

Psikoloji alanında radikalleşme kavramıyla ilgili yapılan eski çalışmalarda, radikalleşmenin bireylerin akıl sağlığında ortaya çıkan sorunlardan kaynaklandığı öne sürülmektedir. Ancak güncel araştırmalar eski söylemlerin bütünüyle doğru olmadığını ortaya koymaktadır (Borum, 2012; Webber ve Kruglanski, 2018). Psikolojik rahatsızlıklar, tek bir bireyin radikalleşmesinin ve aşırı uç (extremist) davranışlarının nedenlerini kısmen açıklayabilmektedir ancak terör örgütlerine katılan bireylerin çoğunun davranışları çeşitli değişkenlere dayanmaktadır (Corner ve Gill, 2015). Çoğu araştırmacı, radikalleşmenin tanımı üzerinde ortak bir fikre sahiptir. Borum (2012) radikalleşmeyi aşırıcılık tutumlarının oluşmasını sağlayan ve terör olaylarına neden olan süreç olarak tanımlarken Webber ve Kruglanski (2018) radikalleşmenin teröristlerin oluşmasına neden olduğunu söyleyerek bu tanımı desteklemiştir.

Bu alanda yapılan güncel çalışmalarla uzmanların normal olarak kabul ettikleri kişilik özelliklerinin terörizme nasıl neden olabileceği araştırılmaktadır. Borum (2014), bireylerin psikolojik süreçleri ve kişilik özelliklerinin yetişkinlikte sabitleşmesiyle oluşan bir "zihniyete (mindset)" sahip olduğunu öne sürmektedir. Bu "zihniyet", bireyin dünya görüşüyle birleştiğinde, meydana gelen psikolojik iklimdeki kırılganlıklar ve eğilimler, aşırıcı davranışlar göstermeyi yordamaktadır. Bireyin karşılaşabileceği psikolojik kırılganlıklar, anlamlı bir kimliğe sahip olma ihtiyacı, bir gruba ait olma ihtiyacı ve adaletsizlik veya küçük düşme algısı olarak

sıralanabilir (Borum, 2014). Bunun yanı sıra bireyler ait oldukları grubun diğer üyelerinin fikirlerine de büyük bir önem verme eğilimindedirler (Abrams ve Hogg, 1990). Ayrıca, şiddet içeren davranışları sosyal olarak onaylandığında, bireyler davranışlarının sonucunda daha az suçluluk hissetme eğiliminde olmaktadırlar (Webber, Schimel, Martens, Hayes ve Faucher, 2013). Buna ek olarak ekonomik ve sosyal kayıpların ideolojik motivasyonla işlenmiş suçları yordadığı görülmektedir. Bireyin aşırıcı davranışlarda bulunma olasılığını artıran bir diğer değişken ise, üyesi olduğu grubun diğer üyelerinin radikal olmasıdır (Jasko, LaFree ve Kruglanski, 2017).

Radikalleşme, gittikçe daralan ve en üst katında terörizm bulunan bir merdivene de benzetilmektedir (Moghaddam, 2009). Bu benzetmeye göre her kat, o kattaki farklı psikolojik süreçlere ve katta "yaşayanların" davranışlarına göre farklı özelliklere sahip olmaktadır. Bir toplumdaki bütün bireyler zemin katta yaşamakta, ancak birkaç kişi iki uçlu (siyah-beyaz) düşünme tarzının giderek daha fazla görüldüğü üst katlara çıkmaktadır. Son kata çıkan bireyler ise terör örgütlerine üye olmakta ve bu örgütlerin amaçları, motivasyonları ve inançları doğrultusunda terör eylemlerinde bulunmaktadırlar. Bu bağlamda, radikalleşme, terörist eylemlere giden süreç olarak da değerlendirilmektedir.

Aşırıcı davranışların gösterilmesindeki en önemli sebeplerden biri de iç-grubun normlarının ve fikirlerinin, dış-grubun normlarından ve fikirlerinden daha üstün olduğuna dair oluşan algıdır. Bireyler söz konusu algı sayesinde dış-gruba uyguladıkları şiddeti meşrulaştırabilmektedirler (Doosje ve ark., 2016). Radikalleşme süreciyle oluşan aşırıcılık beş türe ayrılabilir: (1) bir bölgeyi ele geçirmeyi amaçlayan aşırı milliyetçi ya da ayrılıkçı gruplar; (2) göçmenlerin "üstün" beyaz ırka karşı tehdit oluşturduğu algısına sahip olan aşırı sağ-kanat gruplar; (3) kapitalizmi kötülüğün temel kaynağı olarak gören ve kaynakların eşit olarak paylaştırılmasını savunan aşırı sol-kanat gruplar; (4) aşı, kürtaj veya hayvan hakları gibi tek bir konuya odaklanan gruplar ve son olarak (5) dine dair katı algıları olan ve bu sayede diğerlerine uyguladıkları şiddeti meşrulaştırabilen dinî motivasyonlu gruplar. Bu grupların ideolojileri birbirlerinden oldukça farklı olmasına rağmen her biri mevcut durumu kabul edilemez bulduğu için değiştirmek istemekte ve bunun için şiddet uygulamaya hazır bulunmaktadır.

Radikalleşme, görece yakın zamanlarda daha çok mercek altına alınan bir konu olduğundan, bu kavramla ilgili yapılan çalışmaların çoğunlukla belirli gruplarla sınırlı kaldığı görülmektedir. Öte yandan, radikalleşmenin şiddet yanlılığına doğru yol alış sürecini belirleyebilmek de büyük bir önem kazanmaktadır. Radikalleşmenin merdiven modelinde de belirtildiği gibi, kişiler ilk başta sadece kendi haklarına yönelik algılanan saldırıya karşı ve şiddet yönelimli olmayan bir savunma kullanırken, kimi bireyler için algılanan baskı arttıkça radikalleşme beraberinde şiddeti getirmektedir (Moghaddam, 2005). Bu durumda kişinin radikalleşme seviyesi de oldukça önemli hale gelmektedir. Terör örgütlerine sempati duyan bireylerin radikallik seviyeleri ile aktif bir şekilde terör olaylarında yer alan bireylerin radikallik seviyeleri arasında fark olduğu açıktır. Bazı araştırmacılar, terör örgütlerine katılan bireylere kıyasla daha az radikal olan bireylerin terör örgütünün hedefleri yanında kendi temel ihtiyaçlarını ve yaşamlarını göz ardı edemediklerini, ancak daha radikal olan bireylerin bu ihtiyaçlarını tamamen yok sayarak terör örgütünün hedeflerine odaklanabildiklerini vurgulamaktadırlar (Sageman, 2004). Bu durumda şiddet yanlısı radikal bir birey, kendi grubunun amacını o kadar önemli görmektedir ki, diğer grupların amaçlarını dikkate almamaktadır. Ancak daha az radikal bireyler için diğer grupların da amaçları önem taşımaktadır. Ayrıca, şiddet yanlısı bir kişi grubunun hedefi söz konusuysa bir insana zarar vermeyi meşru görürken; daha az radikal bir kişi kendi ahlaki değerlerini de grubunun hedefleri kadar önemsediğinden, başkasına zarar verme konusunda çok daha hassas davranmaktadır (Kruglanski ve diğerleri, 2014). Bunun yanında Kruglanski ve diğerleri (2014), bireylerin yaşadığı kayıpların, kültürlerinin ve ideolojilerinin de radikalliğe yol açabileceğini düşünmektedirler. Bu nedenle her radikal birey terör örgütünde aktif bir rol oynamak zorunda değildir, ancak terör örgütlerinde yer alan her bireyin radikal olduğu söylenebilir.

Ozer ve Bertelsen (2018), bireyin aşırı uç davranışlar gösterebilme eğilimini araştırdıkları çalışmalarında, şiddet yanlısı radikalleşmeyi değerlendirebilen iki ölçüm aracı geliştirmişlerdir. Bunlardan ilki olan Aşırıcılık Ölçeği (Extremism Scale), sosyokültürel değişime olan tutumu ve diğerlerine olan tahammülsüzlüğü ölçerken; ikincisi olan Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeği (Pro-Violence and Illegal Acts in Relation to Extremism Scale) ise aşırıcılıkla ilişkili şiddeti ve yasa dışı davranışı onaylama eğilimini ölçmektedir.

İlgili literatür incelendiğinde, radikalleşmeyi ölçen araçların eksikliği göze çarpmaktadır. Mevcut çalışmada, yukarıda bahsedilen iki ölçeğin Türkçeye uyarlanması amaçlanmıştır. Ölçekleri Türkçeye uyarlamak için gerekli izinler, özgün çalışmanın araştırmacılarından alınmıştır. Ölçeğin yapı geçerliğinin ölçülebilmesi için (a) Leach ve diğerleri (2008) tarafından geliştirilen ve Balaban (2013) tarafından Türkçeye uyarlanan, bireylerin grup kimliklerini ne kadar benimsediklerini ölçen Türklükle Özdeşim Ölçeği (Turkish Identification Scale), (b) Bogardus (1925) tarafından tanımlanan ve Güler (2013) tarafından geliştirilen, bireylerin farklı etnik kimliğe sahip insanlara yönelik tutumlarını ölçen Sosyal Mesafe Ölçeği (Social Distance Scale) ile (c) Tajfel (1970) tarafından geliştirilen ve gruplar arası ayrımcılığı kaynak paylaştırma yöntemi ile ölçen Tajfel matrisinin bir varyasyonu kullanılmaktadır. Daha önce de belirtildiği üzere, radikalleşmenin altında yatan genel aşırıcı davranışların anlaşılmasını sağlayacak herhangi bir Türkçe ölçek olmadığından, mevcut çalışmanın hem uluslararası hem de Türkiye'deki psikoloji literatürüne önemli bir katkıda bulunacağı düşünülmektedir. Araştırma sonuçları, ilgili kuramsal çerçeve sunularak tartışılmaktadır.

Çalışma 1: Aşırıcılık Ölçeğinin ve Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeğinin Türkçeye Uyarlanması

Örneklem

Örnekleme hem üniversiteden hem de sosyal medya üzerinden ulaşılmıştır ve ölçek Qualtrics çevrimiçi platformu aracılığıyla katılımcılara iletilmiştir. Örneklem sayısı, temel bileşenler analizi için Comrey ve Lee (1992) tarafından en az 300, Cattell (1978) tarafından en az 250, Gorsuch (1983) tarafından ise an az 100 olarak belirlendiğinden 300 kişiden veri toplanılmasına karar verilmiştir. Yukarıda belirtildiği üzere Qualtrics çevrimiçi platformu aracılığıyla 362 kişiden veri toplanmıştır. Ancak 135 katılımcı Aşırıcılık Ölçeği ile Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeği'ni tamamlamadıkları için analizlerden çıkarılmıştır. Ek olarak, tek değişkenli uç boyut analizleri sonucunda Türk katılımcılar içerisinde üç uç değer bulunmuştur ve bu katılımcılar da analizlerden çıkarılmıştır. Çok değişkenli uç değer analizi sonucunda Türk katılımcılar arasında 5, Kürt ve Türk dışındaki diğer etnik gruplara ait katılımcılarda ise 1 adet uç değer tespit edilmiş ve bu uç değerler de analizden çıkarılmıştır. Sonuç olarak analizler 218 katılımcı ile gerçekleştirilmiştir (171

kadın, 45 erkek, 2 cinsiyet belirtmek istemeyen katılımcı; $Ort_{yaş}$ = 30). 177 katılımcı kendilerini Türk olarak, 15 katılımcı ise kendilerini Kürt olarak tanımlamıştır ve 26 katılımcı ise bu iki etnik gruba da ait olmadıklarını belirtmiştir.

Veri Toplama Araçları

Aşırıcılık ölçeği. Aşırıcılık Ölçeği Ozer ve Bertelsen (2018) tarafından geliştirilmiş bir ölçüm aracıdır. Tek boyuttan ve on dört sorudan oluşan bu ölçek, bireyin aşırıcılığı desteklemeye ne kadar yakın olduğunu ölçmektedir. Ölçekten alınan yüksek puan bireyin daha aşırı uçta olduğunu göstermektedir. Ölçeğin Cronbach alfa değeri .92 bulunmuştur. Ölçek, orijinal çalışmanın araştırmacınlardan izin istenerek Türkçeye uyarlanmıştır. Ölçeğin Türkçeye uyarlanma sürecinde orijinal ölçek, iki dil uzmanı tarafından Türkçeye çevrilmiş, ardından bu Türkçe çeviriler iki farklı uzman tarafından tekrar İngilizceye çevrilerek orijinal ölçek ile karşılaştırılmıştır. Ölçek maddelerinin Türkçeleri, son olarak araştırmacılar tarafından değerlendirilerek karar verilmiştir.

Aşırıcılık ölçeği ile ilişkili şiddet yanlılığı ve yasa dışı davranışlar ölçeği. Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeği, Ozer ve Bertelsen (2018) tarafından geliştirilmiş ve bireylerin aşırıcılığa bağlı şiddeti veya yasa dışı davranışları ne kadar onayladığını ölçen bir ölçektir. Ölçek iki boyuttan oluşmakta ve her boyutta altı soru bulunmaktadır. Ölçeğin birinci boyutu aşırıcılık bağlamında başkalarına şiddet uygulamaya olan tutumu, ikinci boyutu ise aynı bağlam kapsamında yasa dışı davranışlara olan tutumu incelemektedir. Şiddet boyutundan alınan yüksek puan Ölçeğin her iki boyutunun da Cronbach alfa değerleri .92 olarak bulunmuştur. Ölçek, orijinal çalışmanın araştırmacılarından izin istenerek Türkçeye uyarlanmıştır. Ölçeğin Türkçeye uyarlanma sürecindeki çeviri işlemlerinde, Aşırıcılık Ölçeği'nde izlenen süreç uygulanmıştır.

Etnik kimlikle özdeşim ölçekleri. Etnik Kimlikle Özdeşim Ölçeği Leach ve diğerleri (2008) tarafından geliştirilen ve Balaban (2013) tarafından Türkçeye uyarlanan, bireyin etnik kimliğiyle ne kadar özdeşim yaşadığını ölçen bir ölçektir. 14 soru barındıran ve tek boyuttan oluşan bu ölçeğin Türkçeye uyarlama çalışmasında Cronbach alfa katsayısı .94 bulunmuştur. Kürt ve Türk etnik kimlikler ile özdeşimi ölçmek için ölçek maddelerinin başındaki etnik grup ifadesi değiştirilmiş, Kürt grubu için "Kürt", Türk grubu için "Türk" ifadesi kullanılmıştır.

Sosyal mesafe ölçeği. Sosyal Mesafe Ölçeği, Bogardus (1925) tarafından geliştirilen ve Güler (2013) tarafından Türkçeye uyarlanan bir ölçektir. Ölçeğin Cronbach alfa değeri .90 olarak bulunmuştur. Ölçek, farklı etnik kimlik veya dinî inanışa sahip olan bireylere komşuluk yapma, arkadaş olma veya evlenme gibi konuların birey tarafından ne kadar onaylandığını ölçmektedir. Toplam dokuz maddeden ve tek boyuttan oluşan bu ölçekten alınan yüksek puan, bireylerin farklı etnik kökenlerden olan bireylerle yakın ilişki kurmayı onayladığını göstermektedir.

Kaynak paylaştırma ve gruplararası ayrımcılık. Bireylerin gruplararası ayrımcılığı, Tajfel (1970) tarafından önerilen bir Tajfel matrisi varyasyonu ile ölçülmüştür. Bu matris, araştırmacılar tarafından mevcut araştırma için oluşturulmuştur. Bu matriste, katılımcılardan iki halk oyunu grubuna (Kürt halk oyunu grubu ve Türk halk oyunu grubu) kaynak paylaştırmaları istenmiştir. Ölçeğin sağ tarafına doğru gidildikçe Kürt halk oyunu grubuna verilen kaynak azalır, Türk halk oyunu grubuna verilen kaynak artarken; sol tarafında Kürt halk oyunu grubuna verilen kaynak artmakta, Türk halk oyunu grubuna verilen kaynak azalmaktadır.

Bilgilendirilmiş onam ve demografik bilgi formu. Bilgilendirilmiş onam formunda çalışmanın süresi, araştırmacıların iletişim bilgileri, araştırmanın konusu gibi bilgiler yer almaktadır. Demografik formda ise katılımcıların doğum yılları, cinsiyetleri, etnik kimlikleri, politik görüşleri gibi bilgileri belirtmeleri istenmiştir.

İşlem

Araştırma verisi, Qualtrics çevrimiçi veri toplama aracı ile toplanmıştır. Katılımcılar çalışmanın doğası ile ilgili bilgilendirildikten sonra demografik bilgi formunu doldurmuşlardır. Şayet katılımcılar kendilerini Türk olarak tanımlamışlarsa Türklükle Özdeşim Ölçeğini, Kürt olarak tanımlamışlarsa Kürtlükle Özdeşim Ölçeğini tamamlamışlar, eğer her iki etnik gruba da ait değillerse söz konusu ölçekleri doldurmaları istenmemiştir. Katılımcılar diğer ölçekleri de doldurduktan sonra çalışma sona ermiştir. Demografik formdan sonraki tüm ölçekler, katılımcılara seçkisiz bir sırayla gösterilmiştir. Veri toplandıktan sonra yapılan temel bileşenler analizleri, korelasyon ve varyans analizleri IBM SPSS Statistics 25 programıyla, doğrulayıcı faktör analizi ise IBM SPSS AMOS 23 ile gerçekleştirilmiştir.

Bulgular

Aşırıcılık Ölçeğinin Temel Bileşenler Analizi

Aşırıcılık Ölçeğinin (AÖ) Türkçeye uyarlanmış halinin ölçeğin orijinaliyle aynı yapıya sahip olup olmadığını görebilmek için temel bileşenler analizi uygulanmıştır. Kaiser-Meyer-Olkin değeri, .6'nın üzerinde olup, .69 olarak bulunmuştur. Bunun yanında Bartlett'in küresellik testi istatistiksel olarak anlamlı bulunmuş ve verinin temel bileşenler analizine uygun olduğuna karar verilmiştir, $\chi^2(91) = 557.15$, $p < .001$.

İlk bileşen matrisinde dört adet bileşen olduğu görülmüştür ve bu bileşenlerin özdeğerinin varyansı sırasıyla %23.39, %13.08, %8.57 ve %8.19'unu açıkladığı bulunmuştur. Ancak özdeğer çizgi grafiğine (scree plot) bakıldığında, iki bileşenli bir yapının daha açıklayıcı olduğu görülmüş ve bu nedenle temel bileşenler analizinin ikinci aşaması olarak iki bileşenli bir yapı incelenmiştir. Orijinal araştırmaya benzer bir sonuç örüntüsü yakalamak için promax rotasyonu kullanılmıştır (Kappa = 4).

Orijinal çalışmada, araştırmacılar AÖ için (1) kapsamlı sosyokültürel değişime olan tutum ve (2) grup dinamikleri kapsamında diğerlerine karşı hoşgörüsüzlük başlıkları kapsamında soru hazırlamış olmalarına rağmen tek bileşenli bir yapı bulmuşlardır. Mevcut çalışmada ise bu iki başlık birbirinden bağımsız iki bileşen olarak ortaya çıkmıştır. Mevcut çalışmada, maddelerin iç geçerliği Cronbach alfa değerlerinin hesaplanması ile değerlendirilmiştir. Bu analizlerin sonuçları Tablo 1'de gösterilmektedir.

Tablo-1. Türkçe AÖ'nün Temel Bileşen Analizi Sonuçları, Ortalamalar, Standart Sapmalar

Maddeler			Bileşenler	
	Ort.	*S. Sapma*	1	2
Eninde sonunda bir yüzleşme olmalıdır; bir birey, yaşamaları gereken hayattan tamamen farklı bir yaşam sürenlerle sonsuza kadar barış içinde yaşayamaz.	2.66	1.64	.75	
İyi ve doğru bir hayat yaşamayanlarla beraber barış içinde yaşamak yanlış ve ahlaka aykırıdır.	2.00	1.45	.72	
Yaşamla ilgili düşünceleri bizden tamamen farklı olan insanlarla ortak çözümler bulmaya çalışmak zaman kaybıdır.	1.97	1.49	.65	

İyi ve doğru bir hayat yaşamanın sadece tek bir yolu vardır.	1.72	1.42	.64	
Toplumlarda iyi ve doğru yaşamı desteklemeyen gruplar, haklarından mahrum bırakılmalıdır.	2.28	1.67	.55	
Eğer bir birey iyi ve doğru bir hayata göre yaşamıyorsa, o kişi toplumdan uzaklaşmayı seçmiştir.	2.42	1.61	.52	
Ben ve benim gibi düşünenlerin toplumun geri kalanıyla hiçbir ortak yanı yoktur.	2.08	1.40	.47	
Kişinin kendi görüşlerinden taviz vermesi yanlıştır.	3.28	1.85	.44	
Benim gibi düşünenler, hayatımızın temelini oluşturan öğeleri (ekonomi, iş, tüketim, refah) tamamen değiştirmek zorundadır. Toplumun geri kalanı istediğini yapabilir.	2.95	1.68		.68
Toplumun temeli olan ekonomik sistemi tamamen değiştirmek gereklidir.	4.89	1.66		.64
Bırakın toplumun geri kalanı demokrasiyi seçsin; ben ve benim gibi düşünenler, kendi sosyal çevremiz için yeni bir sistem oluştururuz.	2.00	1.43		.63
Eğer bir kişi çoğunluğun yaşam tarzı ve kültürüyle uyumlu yaşayamıyorsa, kendisi ve kendisi gibi düşünenler için tamamen farklı bir yaşam tarzı ve kültür yaratması gerekir.	3.16	1.64		.61
Eğer düzgün bir toplum istiyorsak, devletin demokratik formundan kurtulmalıyız.	2.53	1.71		.47
Bu ülkedeki çoğu insan, tamamen değişmesi gereken bir yaşam tarzına ve kültürüne sahiptir.	4.40	1.74		.38
		Özdeğer	3.38	1.83
		Varyans (%)	23.39	13.08
		Alfa	.74	.60

Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeğinin Temel Bileşenler Analizi

Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeğinin (ŞYYDÖ) Türkçeye uyarlanmış halinin ölçeğin orijinaliyle aynı yapıya sahip olup olmadığını görebilmek için temel bileşenler analizi uygulanmıştır. Kaiser-Meyer-Olkin değeri, .6'nın üzerinde olup, .86 olarak bulunmuştur. Bunun yanında Bartlett'in küresellik testi istatistiksel olarak anlamlı bulunmuş ve verinin temel bileşenler analizine uygun olduğuna karar verilmiştir, $\chi^2(91) = 557.15$, $p < .001$.

İlk bileşen matrisinde iki adet bileşen olduğu görülmüş ve bu bileşenlerin özdeğerinin varyansın sırasıyla %50.12 ve %16.08'ini açıkladığı bulunmuştur. Özdeğer çizgi grafiğinin (scree plot) incelenmesi sonucunda da, iki bileşenli bir yapının daha açıklayıcı olduğu görülmüş ve temel bileşenler analizinin ikinci aşaması olarak iki bileşenli bir yapı incelenmiştir. Orijinal araştırmaya benzer bir

sonuç örüntüsü yakalamak için promax rotasyonu kullanılmıştır (Kappa = 4).

Maddelerin bileşenlere orijinal çalışmaya benzer bir şekilde dağıldığı görülmüştür. Bütün maddeler için bileşen yükleri .30'un üzerinde olarak bulunmuştur. Bu ölçek için yapılmış olan temel bileşenler analizinin sonuçları ve yapı geçerliği analizlerinin sonuçları Tablo 2'de gösterilmektedir.

Tablo-2. Türkçe ŞYYDÖ'nün Temel Bileşen Analizi Sonuçları, Ortalamalar, Standart Sapmalar

Maddeler			Bileşenler	
	Ort.	*S. Sapma*	1	2
Yasaları çiğnemek, yeni ve daha iyi bir toplum oluşturmada işe yarayan tek şeydir.	2.86	1.91	.87	
Yasaları çiğnemek, halkıma baskı ve saldırıyı önlemede işe yarayan tek şeydir.	3.17	1.98	.85	
Yasaları çiğnemek, bireyin kendi hakları ve güvenliğine saygı duyulmasını sağlamasında işe yarayan tek şeydir.	2.73	1.78	.82	
Yasaları çiğnemek, daha büyük bir ideali (ideolojik, dini) savunmada işe yarayan tek şeydir.	2.16	1.61	.78	
Yasaları çiğnemek, bireyin yakın olduğu kişiler için uygun koşullar oluşturmasında işe yarayan tek şeydir.	2.14	1.56	.77	
Yasaları çiğnemek, kişinin dayanışma içerisinde olduğu bireyler için uygun koşullar oluşturmasında işe yarayan tek şeydir.	2.21	1.52	.73	
Fiziksel şiddet kullanmak, kişinin dayanışma içerisinde olduğu bireyler için uygun koşullar oluşturmasında işe yarayan tek şeydir.	1.50	1.18		.92
Fiziksel şiddet kullanmak, yeni ve daha iyi bir toplum oluşturmada işe yarayan tek şeydir.	1.60	1.30		.90
Fiziksel şiddet kullanmak, bireyin yakın olduğu kişiler için uygun koşullar oluşturmasında işe yarayan tek şeydir.	1.42	1.04		.86
Fiziksel şiddet kullanmak, daha büyük bir ideali (ideolojik, dini) savunmada işe yarayan tek şeydir.	1.50	1.11		.80
Fiziksel şiddet kullanmak, bireyin kendi hakları ve güvenliğine saygı duyulmasını sağlamasında işe yarayan tek şeydir.	2.00	1.50		.77
Fiziksel şiddet kullanmak, halkıma baskı ve saldırıyı önlemede işe yarayan tek şeydir.	2.78	1.88		.50
		Özdeğer	6.02	1.96
		Varyans (%)	50.12	16.35
		Alfa	.89	.88

AÖ ve ŞYYDÖ'nün Yapı Geçerliği

AÖ ve ŞYYDÖ'nün yapı geçerliği, Kutuplaşma Ölçeği ile korelasyon katsayılarının hesaplanması ile değerlendirilmiştir. Kutuplaşma Ölçeğinden alınan yüksek puan, bireyin daha az kutuplaştığını gösterdiğinden, Aşırıcılık Ölçeği ve ŞYYDÖ'den yüksek puan alanların Kutuplaşma Ölçeğinden daha düşük puan alacağı beklentisi karşılanmıştır. AÖ ile (*Ort.* = 2.74, *S. Sapma* = .74) ile Kutuplaşma Ölçeği (*Ort.* = 4.56, *S. Sapma* = .79) arasında istatistiksel olarak anlamlı negatif bir korelasyon bulunmuştur, r = -.22, p = .001. ŞYYDÖ'nün şiddet yanlılığı boyutu (*Ort.* = 1.80, *S. Sapma* = 1.08) ile Kutuplaşma Ölçeği arasında herhangi bir anlamlı korelasyona rastlanılmamıştır, r = -.10, p = .144. Söz konusu ölçeğin yasa dışı davranışları boyutu (*Ort.* = 2.54, *S. Sapma* = 1.40) ile Kutuplaşma Ölçeği arasında da herhangi bir anlamlı korelasyon bulunmamıştır, r = .04, p = .532. Bu nedenle ŞYYDÖ'nün yapı geçerliğinin değerlendirilebilmesi için bu ölçek ile AÖ arasındaki korelasyona bakılmıştır. AÖ'de yüksek puana sahip olan bireylerin ŞYYDÖ'den de yüksek puan alacağı öne sürülmüştür. Beklendiği gibi, AÖ ile yasa dışı davranışlar boyutu arasında istatistiksel olarak anlamlı pozitif bir korelasyon görülmüş, r = .22, p = .001; benzer bir ilişkiye şiddet yanlılığı boyutu ile AÖ arasındaki ilişkide de rastlanılmıştır, r = .25, p < .001. Bunun yanında AÖ, ŞYYDÖ, farklı gruplara kaynak paylaştırma ve politik ideolojileri arasındaki ilişkilerin incelenebilmesi için hesaplanan Pearson korelasyon katsayıları, Tablo 3'te sunulmaktadır.

Tablo-3. AÖ, ŞYYDÖ, Politik İdeoloji, Kaynak Paylaşımı ve Kutuplaşmanın Korelasyon Değerleri

Değişkenler	1	2	3	4	5	6
1. AÖ	1					
2. ŞYYDÖ (Şiddet)	.25**	1				
3. ŞYYDÖ (Yasadışı Davranış)	.22**	.53**	1			
4. Politik İdeoloji	-.16*	.001	-.15*	1		
5. Kaynak Paylaşımı	.03	.03	.06	-.01	1	
6. Kutuplaşma	-.22**	-.10	.04	-.24**	-.22**	1
Ort.	2.74	1.80	2.54	3.93	6.09	4.46
S. Sapma	.74	1.08	1.40	1.89	.46	.79

*p < .05, **p < .01

AÖ, ŞYYDÖ, Politik İdeoloji, Kaynak Paylaşımı, Etnik Köken ve Kutuplaşma Arasındaki İlişki

Etnik kimlikle özdeşim, AÖ, ŞYYDÖ, politik ideoloji, kaynak paylaşımı ve kutuplaşma arasındaki ilişkiyi incelemek için, her etnik kimlik grubuna ait Pearson korelasyon katsayısı ayrı ayrı hesaplanmıştır. Türk kimlikleşmesi, Kürt kimlikleşmesi ve diğer kimlikleşmeler için oraya çıkan sonuçlar sırasıyla Tablo 4, Tablo 5 ve Tablo 6'da sunulmaktadır. Kürt etnik grubu için kaynak paylaşımının hesaplanmamasının sebebi, Kürt etnik grubuna ait olanların tamamının kaynak paylaştırmada 6 puan vermiş olmasıdır.

Tablo-4. Türk Katılımcılarda Türk Kimlikleşmesi, AÖ, ŞYYDÖ, Politik İdeoloji, Kaynak Paylaşımı ve Kutuplaşmanın Korelasyon Değerleri

Değişken	1	2	3	4	5	6	7
1. Türk Kimlikleşmesi	1						
2. AÖ	.14	1					
3. ŞYYDÖ (Şiddet)	.04	.33**	1				
4. ŞYYDÖ (Yasadışı Davranış)	-.14	.26**	.49**	1			
5. Politik İdeoloji	.27**	-.19*	-.02	-.22**	1		
6. Kaynak Paylaşımı	.28**	.04	.11	.12	-.04	1	
7. Kutuplaşma	-.38**	-.24**	-.14	.02	-.27**	-.22**	1
Ort.	4.25	2.74	1.70	2.40	3.94	6.12	4.41
S. Sapma	1.43	.77	.90	1.32	1.89	.50	.85

*$p < .05$, **$p < .01$

Tablo-5. Kürt Katılımcılarda Kürt Kimlikleşmesi, AÖ, ŞYYDÖ, Politik İdeoloji ve Kutuplaşmanın Korelasyon Değerleri

Değişken	1	2	3	4	5	6
1. Türk Kimlikleşmesi	1					
2. AÖ	.26	1				
3. ŞYYDÖ (Şiddet)	.55**	.18	1			
4. ŞYYDÖ (Yasadışı Davranış)	.67**	.40	.73**	1		
5. Politik İdeoloji	.32	.47	.37	.45	1	
6. Kutuplaşma	-.02	-.44	-.10	-.26	-.13	1
Ort.	4.59	2.46	2.30	3.29	4.13	4.64
S. Sapma	1.40	.48	1.60	1.62	2.36	.42

*$p < .05$, **$p < .01$

Tablo-6. Diğer Etnik Gruplarda AÖ, ŞYYDÖ, Politik İdeoloji, Kaynak Paylaşımı ve Kutuplaşmanın Korelasyon Değerleri

Değişken	1	2	3	4	5	6
1. AÖ	1					
2. ŞYYDÖ (Şiddet)	.12	1				
3. ŞYYDÖ (Yasa Dışı Davranış)	.04	.50**	1			
4. Politik İdeoloji	-.19	-.18	-.22	1		
5. Kaynak Paylaşımı	-.06	-.22	-.10	.31	1	
6. Kutuplaşma	.04	-.18	.13	.002	.12	1
Ort.	2.83	2.22	3.06	3.73	5.92	4.67
S. Sapma	.67	1.60	1.56	1.66	.27	.42

*$p < .05$, **$p < .01$

Bunun yanında, bu grupların birbirlerinden aşırıcılık, aşırıcılığa bağlı şiddet yanlılığı ve yasa dışı davranışlara eğilim, gruplar arası kaynak paylaştırma, politik ideoloji ve kutuplaşma açısından ayrılıp ayrılmadığını görebilmek için tek yönlü varyans analizi yapılmıştır. Kaynak paylaşımı; $F(2,215) = 2.51$, $p = .084$; aşırıcılık; $F(2,215) = 1.28$, $p = .282$; kutuplaşma; $F(2,215) = 1.73$, $p = .181$; ve politik ideoloji; $F(2,215) = .23$, $p = .792$; için oluşturulan modeller istatistiksel olarak anlamlı bulunmamıştır. Ancak şiddet yanlılığı; $F(2,215) = 4.57$, $p = .011$ ve yasa dışı davranışlara eğilim; $F(2,215) = 5.00$, $p = .008$ istatistiksel olarak anlamlı bulunmuştur.

Etnik grupların AÖ, ŞYYDÖ, politik ideoloji, kaynak paylaşımı ve kutuplaşma açısından nasıl farklılaştıklarını görmek için tek yönlü varyans analizi uygulanmıştır. Kaynak paylaşımı modeli; $F(2,215) = 2.51$, $p = .084$; aşırıcılık modeli; $F(2,215) = 1.28$, $p = .282$; kutuplaşma modeli; $F(2,215) = 1.73$, $p = .181$; ve politik ideoloji modeli; $F(2,215) = .23$, $p = .792$, istatistiksel olarak anlamlı bulunmamıştır. Ancak ŞYYDÖ (Şiddet) modeli $F(2,215) = 4.57$, $p = .011$ ve ŞYYDÖ (Yasa Dışı Davranış) modeli, $F(2,215) = 5.00$, $p = .008$ istatistiksel olarak anlamlı bulunmuştur. Yapılan Tukey testi sonucunda, diğer etnik gruplara ait olan katılımcıların (*Ort.* = 2.22, *S. Sapma* = 1.60) Türk katılımcılarla (*Ort.* = 1.70, *S. Sapma* = .90) kıyaslandıklarında şiddet kullanımını daha fazla destekledikleri ortaya çıkmıştır ($p = .049$); Kürt ile Türk ve Kürt ile diğer etnik gruplar arasında herhangi bir istatistiksel fark görülmemiştir. Bunun yanında, bir başka Tukey testi de Kürt katılımcıların (*Ort.* = 3.29, *S. Sapma* = 1.62) Türk katılımcılara (*Ort* = 2.41, *S. Sapma* = 1.32) aşırıcılığa bağlı yasaları çiğneme

davranışını istatistiksel olarak daha fazla desteklediklerini ortaya koymuştur (p = .046). Son olarak diğer etnik kimliğe sahip katılımcılar (*Ort.* = 3.06, *S. Sapma* = 1.56) ve Türk katılımcılar aşırıcılıkla ilişkili olarak yasa dışı davranışları destekleme eğilimleri açısından kıyaslandıklarında, diğer etnik kimliklere sahip olan katılımcıların yasa dışı davranışları desteklemeye dair eğilimleri olduğu görülmüştür (p = .059). Tukey testinin sonuçları Tablo 7'de sunulmaktadır.

Tablo-7. Türk, Kürt ve Diğer Etnik Grupların ŞYYDÖ Şiddet ve ŞYYDÖ Yasadışı Davranış Açısından Karşılaştırılması

Değişken	Etnik Grup				
	Türk	Kürt	Diğer	F	η^2
ŞYYDÖ Şiddet	1.70 (.90)	2.30 (1.60)	2.22 (1.60)	4.57*	.04
ŞYYDÖ Yasadışı Davranış	2.41 (1.32)	3.29 (1.62)	3.06 (1.60)	5.00*	.04

*$p < .05$

Not. Standard sapmalar, ortalamaların altındaki parantezlerde verilmiştir.

Çalışma 2: Aşırıcılık Ölçeğinin ve Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeğinin Doğrulayıcı Faktör Analizleri

Örneklem

Araştırmanın örneklemini üniversite öğrencileri ve sosyal medya aracılığıyla ulaşılan 227 katılımcı oluşturmaktadır. Ancak bu katılımcılardan 10 tanesi, AÖ'yü veya ŞYYDÖ'yü tamamlamadığı için analizden çıkarılmıştır. Yapılan çok değişkenli uç değer analizi sonucunda altı uç değere sahip olan katılımcı analizden çıkarılmıştır. Sonuç olarak tüm analizler 211 katılımcı üzerinde yapılmıştır (184 kadın, 26 erkek, 1 cinsiyetini belirtmek istemeyen birey; Ortyaş = 21). Katılımcıların 185'i kendisini Türk olarak, 4'ü Kürt olarak, 22'si ise bu etnik gruplardan ikisine de ait olmadıklarını belirtmişlerdir. Örneklem sayısı, temel bileşenler analizi ve doğrulayıcı faktör analizi gibi analizler için sınırlı olmakla birlikte kabul edilebilir düzeydedir (Cattell, 1978; Comrey ve Lee, 1992; Gorsuch, 1983).

Veri Toplama Araçları

Bir önceki çalışmada kullanılan ölçekler bu çalışmada da kullanılmıştır. Ancak bu ölçeklere ek olarak Sosyal Baskınlık Yönelimi Ölçeği de, veri toplama araçlarına dahil edilmiştir

Sosyal baskınlık yönelimi ölçeği. Sosyal Baskınlık Yönelimi Ölçeği, Pratto ve diğerleri (1994) tarafından geliştirilmiş, Karaçanta (2002) ve daha sonra Akbaş (2010) tarafından Türkçeye uyarlanmış bir ölçüm aracıdır. Ölçek, sosyal baskınlık yönelimini *gruba dayalı baskınlık* ve *eşitliğe karşı gelme* olarak tanımlanan iki alt boyut üzerinden ölçmektedir. Gruba dayalı baskınlığı ölçmek için 8, eşitliğe karşı gelmeyi ölçen 8 ters kodlanmış madde bulunmaktadır. Ölçekten alınan yüksek puanlar, bireyin sosyal baskınlık yöneliminin daha yüksek olduğunu ifade etmektedir. Ölçeğin gruba dayalı baskınlık boyutunun Cronbach alfa katsayısı .81, eşitliğe karşı gelme boyutunun Cronbach alfa katsayısı ise .91 olarak bulunmuştur.

İşlem

İkinci çalışmada da birinci çalışmadaki desenin aynısı uygulanmıştır. Katılımcılar önce demografik bilgi formunu doldurduktan sonra diğer ölçekleri seçkisiz bir sırayla tamamlamışlardır. Bir önceki çalışmada olduğu gibi kendisini Kürt olarak tanımlayan katılımcılar Kürtlükle Özdeşim Ölçeğini doldurmuş, Türk olarak tanımlayan katılımcılar ise Türklükle Özdeşim Ölçeğini doldurmuşlardır.

Bulgular

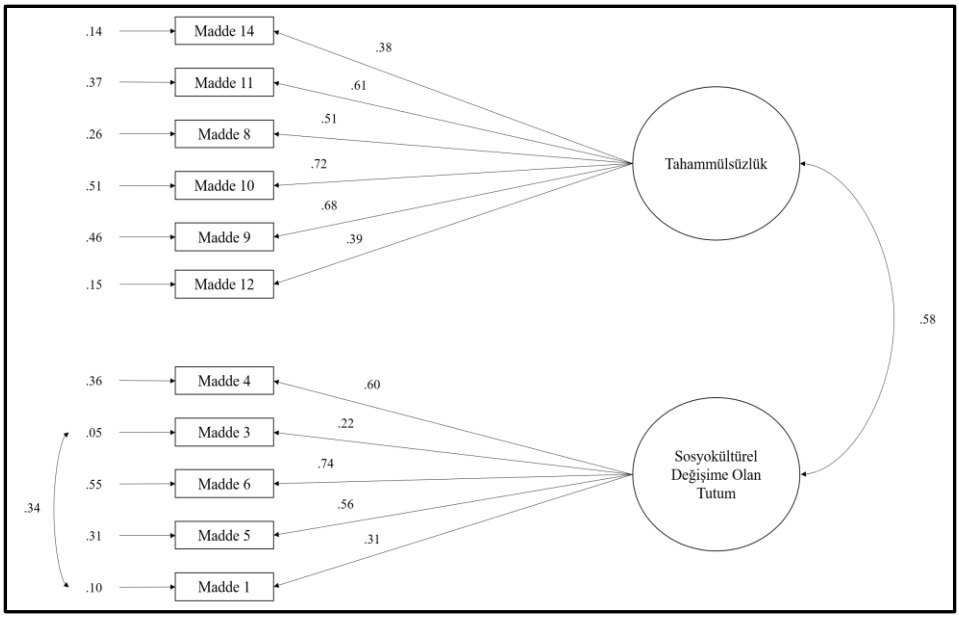
AÖ'nün Doğrulayıcı Faktör Analizi

Bir önceki çalışmada yapılmış olan temel bileşenler analizinin sonucunda, AÖ'nün ve ŞYYDÖ'nün iki bileşenli bir yapıya sahip oldukları bulunmuştu. Bu yapıyı doğrulamak için doğrulayıcı faktör analizi yapılmıştır. Model uyumuna bakıldığı zaman, χ^2/s değerinin model uyumu için uygun olduğu görülmüştür, χ^2 (76, N = 211) = 225.62, χ^2/s = 2.97, p < .001; GFI = .86, CFI = .78, RMSEA = .097. Bu model uyumu problemlerini düzeltebilmek için model dizini(model indices) değerlendirilmiştir. Değişiklik dizininde AÖ'nün 1. maddesi ile 3. maddesi arasındaki hata değerleri ilişkilendirilmiş ve modelin uyumuna yeniden bakılmıştır. χ2/s değerinin biraz daha iyileştiği gözlenmiştir, χ^2(75, N = 211) = 205.97, χ^2/s = 2.75, p < .001; GFI = .88, CFI = .81, RMSEA = .091. GFI ile CFI .90'a yükselemediği, RMSEA ise .08'in altına düşemediği model dizini yeniden

değerlendirilmiştir. Model dizininde ilişkilendirilebilecek herhangi bir hata değeri bulunamadığı için standardize edilmiş eşdeğişkenlik değerlerine bakılmıştır. Eşdeğişkenlikleri 2'nin üzerinde olan 2. 7. ve 13. maddeler modelden çıkarılmıştır. Model uyumu yeniden değerlendirildiğinde χ^2/s değerinin uygun olduğu görülmüştür, $\chi^2(42, N = 211) = 75.016$, $\chi^2/s = 1.79$, $p = .001$; GFI = .94, CFI = .92, RMSEA = .061. Değerler uygun bir model uyumuna işaret ettiği için daha fazla işlem yapılmamıştır. Sonuç olarak doğrulayıcı faktör analizi tamamlanmış olan AÖ'nün hoşgörüsüzlük boyutunda 6 madde, sosyokültürel değişim boyutunda ise 5 soru bulunmaktadır. Aşırıcılık Ölçeğinin doğrulayıcı faktör analizi sonuçları Tablo 8'de, yapısı ise Şekil 1'de görülebilir.

Tablo-8. Aşırıcılık Ölçeğinin Model İndeks Değerleri

Model	χ^2	sd	χ^2/sd	GFI	CFI	RMSEA
2 Faktörlü Model	225.62	76	2.97	.86	.78	.097
2 Faktörlü Model (1 hata korelasyonu)	205.97	75	2.75	.88	.81	.091
2 Faktörlü Model (madde çıkarılması)	75.02	42	1.79	.94	.92	.061



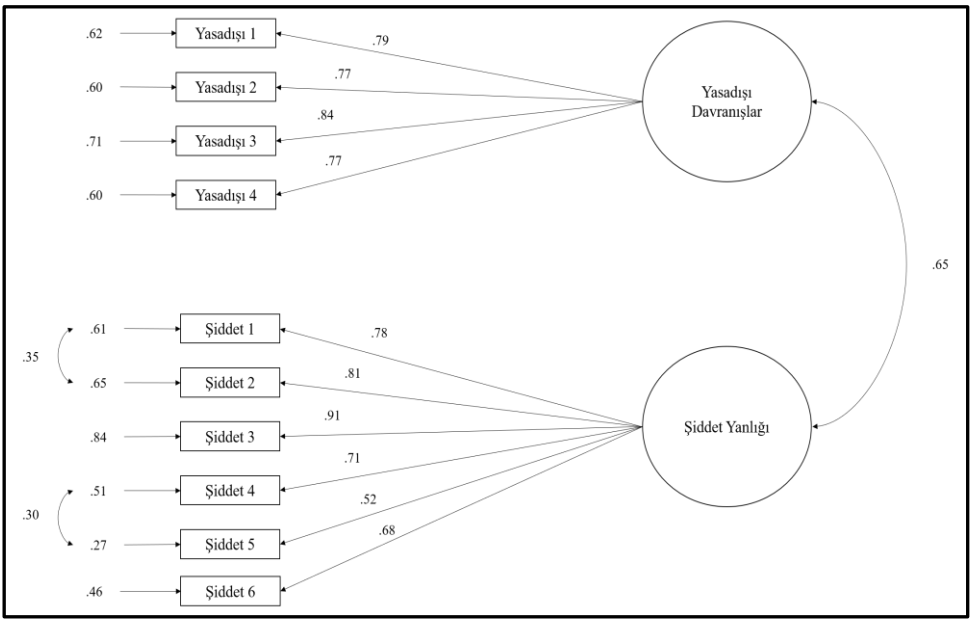
Şekil-1. Aşırıcılık Ölçeğinin Faktör Yapısı

ŞYYDÖ'nün Doğrulayıcı Faktör Analizi

ŞYYDÖ'nün doğrulayıcı faktör analizinde, ilk modelin $\chi^2(53, N = 211) = 303.79$, $\chi^2/s = 5.73$, $p < .001$; GFI = .81, CFI = .84, RMSEA = .15 olduğu bulunmuştur. Model uyumu ile ilgili değerleri düzeltmek için model dizini incelenmiştir. Değişiklik dizininde yapılan inceleme sonucunda şiddet yanlılığı alt boyutunun 5. ve 4. sorularının hata değerleri ilişkilendirilmiştir. Model yeniden test edildiğinde $\chi^2(52, N = 211) = 285.79$, $\chi^2/s = 5.50$; $p < .001$; GFI = .82, CFI = .85, RMSEA = .15 olduğu görülmüştür ve bu nedenle model dizinine yeniden bakılmıştır. Şiddet yanlılığı boyutundaki 1. ve 2. maddelerin hata değerlerinin eşleştirilmesinden sonra model yeniden test edilmiştir, $\chi^2(51, N = 211) = 268.25$, $\chi^2/s = 5.26$, $p < .001$; GFI = .83, CFI = .86, RMSEA = .14. Daha iyi bir model ulaşabilmek amacıyla model dizinine yeniden bakılmıştır. Ancak model dizininde eşleştirilebilecek herhangi bir hata değeri olmadığından standardize edilmiş eşdeğişkenlik değerlerine bakılmıştır. Eşdeğişkenlik değerleri ideal sınırı aşan yasa boyutundan 5. ve 6. soru modelden çıkarılmış ve model uyumuna tekrar bakılmıştır, $\chi^2(32, N = 211) = 122.61$, $\chi^2/s = 3.83$, $p < .001$, GFI = .91, CFI = .93, RMEA = .12. GFI ve CFI değerleri iyi bir model uyumu olduğunu göstermekle birlikte RMSEA değeri .12 olarak kalmış ve aşağıya indirilememiştir. Sonuç olarak ŞYYDÖ'nün yasa dışı davranış boyutunda 4 madde, şiddet yanlılığı boyutunda ise 6 madde bırakılmıştır. ŞYYDÖ'nün doğrulayıcı faktör analizi sonuçları Tablo 9'da, yapısı ise Şekil 2'de sunulmuştur.

Tablo-9. Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasadışı Davranışlar Ölçeğinin Model İndeks Değerleri

Model	χ^2	sd	χ^2/sd	GFI	CFI	RMSEA
2 Faktörlü Model	303.79	53	5.73	.81	.84	.15
2 Faktörlü Model (1 hata korelasyonu)	285.79	52	5.50	.82	.85	.15
2 Faktörlü Model (2 hata korelasyonu)	268.25	51	5.26	.83	.86	.14
2 Faktörlü Model (madde çıkarılması)	122.61	32	3.83	.91	.92	.12



Şekil-2. Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasadışı Davranışlar Ölçeğinin Faktör Yapısı

Sosyal Baskınlık Yönelimi, AÖ ve ŞYYDÖ Arasındaki İlişki

Aşırıcılık, aşırıcılık ölçeği ile ilişkili şiddet yanlılığı ve yasa dışı davranışlar ve sosyal baskınlık yöneliminin arasındaki ilişkinin incelenmesi için bu değişkenlerin Pearson korelasyon katsayıları hesaplanmıştır. AÖ ve ŞYYDÖ için doğrulayıcı faktör analizinin sonucu oluşan ölçekler kullanılmıştır. İkili ilişkiler incelendiği zaman sosyal baskınlık yönelimi (*Ort.* = 2.23, *S. Sapma* = .66) ile aşırıcılık (*Ort.* = 2.90, *S. Sapma* = .84) arasında istatistiksel olarak anlamlı pozitif bir korelasyon olduğu görülmüştür, $r = .35$, $p < .001$. Bunun yanında sosyal baskınlık yönelimi ve şiddet yanlılığı (*Ort.* = 2.21, *S. Sapma* = 1.27, $r = .24$, $p < .001$) ile sosyal baskınlık yönelimi ve yasa dışı davranışlar (*Ort.* = 2.91, *S. Sapma* = 1.59, $r = .22$, $p = .001$) arasında da istatistiksel olarak anlamlı, pozitif ilişkiler olduğu görülmüştür. Aşırıcılık ile şiddet yanlılığı ($r = .30$, $p < .001$), aşırıcılık ile yasa dışı davranışlar ($r = .31$, $p < .001$) ve yasa dışı davranışlar ile şiddet yanlılığı ($r = .57$, $p < .001$) arasında da istatistiksel olarak anlamlı pozitif bir korelasyon olduğu görülmüştür. Değişkenler arasındaki korelasyonlar Tablo 10'da sunulmuştur.

Tablo-10. Sosyal Baskınlık Yönelimi, Aşırıcılık, Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeği

Değişkenler	1	2	3	4
1. Sosyal Baskınlık Yönelimi	1			
2. AÖ	.35**	1		
3. ŞYYDÖ Şiddet	.24**	.30**	1	
4. ŞYYDÖ Yasa Dışı Davranış	.22**	.31**	.57**	1
Ort.	2.74	1.80	2.54	3.93
S. Sapma	.74	1.08	1.40	1.89

*$p < .05$, **$p < .01$

Tartışma

Radikalleşmenin terörizm çalışmalarındaki önemi, akademik çevreler tarafından görece yeni anlaşılmaya başlanmıştır. Bu nedenle radikalleşme kavramına ve süreçlerine yönelik çalışmaların son yıllarda arttığı görülmektedir. Radikalleşme, terör davranışının ortaya çıkmasına neden olan temel sebeplerden biri olduğundan, bu süreci değerlendiren ölçüm araçları da konuyla ilgili literatür için büyük bir önem taşımaktadır (Borum, 2012). Bunun yanında, radikalleşmeyi değerlendirebilecek araçların terörizmle mücadele ve terörizmi önleme faaliyetleri bakımından önem taşıdığı açıktır; söz konusu araçlar özellikle terörizm olaylarını daha fazla deneyimleyen ülkeler için bir ihtiyaçtır. Daha önce de belirtildiği üzere, her radikal birey terörist değildir ancak her terörist radikaldir. Bu ayrımın netleştirilebilmesinde "fiziksel şiddet" belirleyici unsur olarak karşımıza çıkmaktadır. Bu nedenlerle mevcut çalışma, aşırıcılığı ve şiddet yanlılığını değerlendirerek radikalleşmeyi ölçen güncel bir ölçüm aracının Türkçeye uyarlanmasını ve radikalleşme ile ilişkili değişkenlerle ilişkisine bakarak radikalleşme konusuna ışık tutmayı amaçlamıştır.

Çalışmanın ilk aşamasında Aşırıcılık Ölçeği (AÖ) ile Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeği (ŞYYDÖ) uzmanlar tarafından Türkçeye çevrilmiş ve çeviri kontrolleri yapılmıştır. Ardından ölçeğin güvenirlik ve geçerlik değerleri kontrol edilmiştir. Psikometrik açıdan değerlendirildiğinde, AÖ'nün Cronbach alfa değerleri yeterli seviyede olsa bile, maddelerin bileşenlere yüklenme katsayısının istenenin altında olduğu görülmektedir. ŞYYDÖ'de ise böyle bir durumla karşılaşılmamıştır. Radikalleşme ile ilişkili diğer değişkenlerle ölçekler arasındaki ilişkiye bakıldığında ise kayda

değer sonuçlar elde edilmiştir. Aşırıcılık ile kutuplaşma arasındaki negatif ilişki, kutuplaşma arttıkça aşırıcılığın da arttığını göstermektedir; bu bulgu literatürü destekler niteliktedir (Krieger ve Meierrieks, 2010). Bunun yanı sıra politik ideolojide sağ ideolojiye yönelimin artması ile yasa dışı davranışlara olan olumlu tutumun ve aşırıcılığın azaldığı görülmüştür. Bu durum, sol ideoloji yönelimli bireylerin kendilerini daha azınlıkta hissediyor olmasından kaynaklanıyor olabilir. Şayet bireyler kendilerini azınlık olarak görüyor ve haklarının ihlal edildiğini düşünüyorlarsa, haklarını savunmak için şiddeti veya yasa dışı davranışları meşrulaştırabilmektedirler (Moghaddam, 2009). Değişkenler arasındaki ilişkiler etnik kimlik bakımından incelendiğinde; ideoloji, aşırıcılık ve yasa dışı davranışlara olan olumlu tutum arasındaki bu ilişkiye kendisini Türk olarak tanımlayan katılımcılarda da rastlanmıştır. Genel örneklemde ortaya çıkarılan bu ilişkinin kendisini Türk etnik kimliği ile tanımlayan katılımcılarda da bulunması, bu olası sebebi güçlendirmektedir.

Diğer yandan, kendisini Kürt etnik kimliği ile tanımlayan katılımcılarla Türk etnik kimliği ile tanımlayan katılımcılar arasındaki en önemli farklardan biri; Türk katılımcılarda etnik kimlikleşme ile aşırıcılık, şiddet yanlılığı veya yasa dışı davranışları meşrulaştırma arasında herhangi bir ilişki yokken, Kürt katılımcılarda kimlikleşme ile yasa dışı davranışları meşrulaştırma ve şiddet yanlılığı arasında ilişki olmasıdır. Kürt katılımcılarda kimlikleşme arttıkça şiddet yanlılığının ve yasa dışı davranışları meşrulaştırmanın da arttığı görülmüştür. Bu bulgu, sol ideolojiye sahip olan bireylerin deneyimlediği olası azınlık algısıyla benzer bir nitelik göstermektedir. Kürt etnik kimliğine sahip olan bireyler kendilerini azınlık olarak gördüklerinde, haklarının çiğnendiği algısıyla karşı karşıya kaldıklarında sadece şiddetin veya yasa dışı davranışların haklarını korumada işe yarayabileceği algısına sahip olabilirler. Bu durum, Moghaddam (2009)'ın modelini destekler niteliktedir. Gruplar birbirleriyle karşılaştırıldığında, Kürt katılımcıların Türk katılımcılara kıyasla aşırıcılıkla ilişkili yasa dışı davranışları daha fazla destekledikleri bulunmuştur. Bu durum, yukarıdaki söylemleri destekleyecek bir bulguyu da ortaya koymuştur.

İkinci çalışmada ise modelin uygunluğunu test etmek için doğrulayıcı faktör analizi yapılmıştır. Yapılan analizler, hem AÖ'nün hem de ŞYYDÖ'nün model uygunluğu bakımından birtakım sorunları olduğunu göstermiştir. Bu sorunlar, modelin düzenlenmesi sırasında çözülmüş olsa bile, yaşanan sorunlar, ölçek

uyarlama çalışmalarındaki kültürel uyuşmazlık problemini bir kez daha gün yüzüne çıkarmıştır. Buradan yola çıkarak, içinde yaşadığımız kültürün insanlarıyla yapılacak çalışmalar doğrultusunda bir ölçeğin geliştirilmesinin daha uygun olacağı düşünülmektedir. Bu durum, radikalleşme kavramını ve sürecini daha iyi anlamak amacıyla ortaya konacak ölçüm araçlarına ne kadar ihtiyaç olduğunu bir kez daha vurgulamaktadır.

İkinci çalışmada AÖ'nün ve ŞYYDÖ'nün sosyal baskınlık yönelimiyle ilişkisine de bakılmıştır. Sosyal baskınlık yönelimi, sağ kanat yetkeciliğinden farklı olarak azınlıkların çoğunluğun içinde asimile olması yerine tamamen toplumdan ayrıştırılması gerektiğini savunan bir düşünce biçimidir. Yapılan analizler sonucunda sosyal baskınlık yöneliminin hem aşırıcılıkla, hem şiddet yanlılığıyla, hem de yasa dışı davranışları meşrulaştırma ile pozitif bir ilişkisi olduğu bulunmuştur. Azınlıkları ülkelerinde istemeyen bir çoğunluğun radikalleşme olasılığının yüksek olabileceği ve böyle bir çoğunluğun azınlıklara karşı yapılacak şiddet eylemlerini destekleyebileceği de düşünülecek olursa, bu ilişki oldukça anlamlıdır.

Yukarıda bahsedilen bütün bu bulguların yanı sıra çalışmanın bazı sınırlılıkları da mevcuttur. Bu sınırlılıklardan ilki katılımcı sayısı ve katılımcıların doğasıdır. Katılımcı sayısı, özellikle ölçek uyarlama çalışmalarında önemli bir değişken olduğundan, ileride yapılacak çalışmaların daha büyük bir örnekleme uygulanmasında fayda olacaktır. Bunun yanında radikalleşme gibi bir konuda, örneklemin çeşitlendirilmesi ve grupların homojen olması da önem taşımaktadır. Türkiye'de yaşayan ve kendilerini farklı etnik kimliklerle ifade eden bireylerle bu konuda yapılacak çalışmalar, radikalleşmenin açıklanabilmesinde önemli bir rol oynayacaktır. Mevcut çalışmanın örneklemi hem üniversite öğrencilerini hem de yetişkin katılımcıları kapsamasına rağmen -örneklemdeki çeşitlilik, popülasyonu daha iyi yansıtacağından- ileride yapılacak araştırmalarda demografik özellikleri açısından daha çeşitli bir örneklemden veri toplanması önerilmektedir.

Tüm bulguları ve sınırlılıkları değerlendirildiğinde, mevcut çalışmanın en önemli katkısı Türkçe literatüre geçerliği ve güvenirliği test edilmiş bir radikalleşme ölçeğini kazandırmasıdır. Türkiye'de geçmişten bugüne faaliyet gösteren terörist gruplar ve gerçekleştirilen terör eylemleri göz önünde bulundurulduğunda, sonu terörizme çıkan basamakları barındıran radikalleşme

sürecini anlamayı, açıklamayı ve ölçmeyi amaçlayan farklı bilimsel disiplinlerce yapılacak araştırmalara ihtiyaç olduğu açıktır. Mevcut çalışma, bu ihtiyacı karşılamaya yönelik yapılacak araştırmalara bir ölçüm aracı sunarak, önemli bir katkıda bulunmaktadır.

Teşekkür: Araştırmada kullanılan ölçüm araçları konusunda yardımları için Dr. Öğr. Üyesi Selen Aktari Sevgi, Arş. Gör. Deniz Kırpıklı ve Arş. Gör. Fatih Bayrak'a teşekkür ederiz.

KAYNAKÇA

Abrams, D. ve Hogg, M. A. (1990). Social identity, self categorization and social influence. *European Review of Social Psychology, 1*(1), 195-228. doi:10.1080/14792779108401862

Akbaş, G. (2010). *Social identity and intergroup relations: The case of Alevis and Sunnis in Amasya*. Yayımlanmamış yüksek lisans tezi, Orta Doğu Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Balaban, Ç. D. (2013). *The roles of intergroup threat, social dominance orientation and right-wing authoritarianism in predicting Turks' prejudice toward Kurds.* Yayınlanmamış yüksek lisans tezi, Orta Doğu Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Bogardus, E. S. (1925). Measuring social distance. *Journal of Applied Sociology, 9*, 299-308.

Borum, R. (2012). Radicalization into violent extremism I: A review of social science theories. *Journal of Strategic Security, 4*(4), 7-36. doi:10.5038/1944-0472.4.4.1

Borum, R. (2014). Psychological vulnerabilities and propensities for involvement in violent extremism. *Behavioral Sciences and Law, 32*, 286-305. doi:10.1002/bsl.2110

Cattell, R.B. (1978). *The scientific use of factor analysis in behavioral and life sciences*. New York: Plenum Press.

Comrey, A.L. ve Lee H.B. (1992). *A first course in factor analysis*. London: Taylor and Francis.

Corner, E. ve Gill, P. (2015). A false dichotomy? Mental illness and lone-actor terrorism. *Law and Human Behavior, 39*(1), 23-24. doi:10.1037/lhb0000102

Doosje, B., Moghaddam, F. M., Kruglanski, A. W., de Wolf, A., Mann, L. ve Feddes, A. R. (2016). Terrorism, radicalization and de-radicalization. *Current Opinion in Psychology, 11*, 79-84. doi:10.1016/j.copsyc.2016.06.008

Gorsuch, R.L. (1983). *Factor analysis*. Hillsdale NJ: Lawrence Erlbaum Associates

Güler, M. (2013). *Gruplararası temas, kaygı ve yanlılığın sosyal mesafeye etkisi: Türk ve Kürt kökenli gruplar üzerine bir çalışma*. Yayınlanmamış doktora tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Jasko, K., LaFree, G. ve Kruglanski, A. (2017). Quest for significance and violent extremism: The case of domestic radicalization. *Political Psychology, 38*(5), 815-831. doi:10.1111/pops.12376

Karaçanta, H. (2002). *Üniversite öğrencilerinin sosyal baskınlık yönelimi ve başka bazı değişkenler açısından karşılaştırılması.* Yayımlanmamış doktora tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü, Ankara.

Krieger, T. ve Meierrieks, D. (2010). Terrorism in the worlds of welfare capitalism. *Journal of Conflict Resolution, 54*(6), 902-939. doi: 10.1177/0022002710367885

Kruglanski, A. W., Gelfand, M. J., Belanger, J. J., Sheveland, A., Hetiarachchi, M. ve Gunaratna, R. (2014). The psychology of radicalization and deradicalization: How significance quest impacts violent extremism. *Advrances in Political Psychology, 35.* doi: 10.1111/pops.12163

Leach, C. W., van Zomeren, M., Zebel, S., Wliek, M. L. W., Pennekamp, S. F., Doosje, B. ve Ouwerkerk, J. W. (2008). Group-level self-definition and self-investment: A hierarchical (multicomponent) model in in-group identification. *Journal of Personality and Social Psychology, 95*(1), 144-165.

McCauley, C. ve Moskalenko, S. (2017). Understanding political radicalization: The two-pyramids model. *American Psychologist, 72*(3), 205-216.

Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. *American Psychologist, 60*, 161–169. http://dx.doi.org/10.1037/0003-066X.60.2.161

Moghaddam, F. M. (2009). De-radicalization and the staircase from terrorism. D. Canter, (Ed.), *The faces of terrorism: Multidisciplinary perspectives* içinde (277-292). New Jersey: John Wiley & Sons Ltd. doi:10.1002/9780470744499.ch16

Ozer, S. ve Bertelsen, P. (2018). Capturing violent radicalization: Developing and validating scales measuring central aspects of radicalization. *Scandinavian Journal of Psychology, 59*, 653-660. doi:10.1111/sjop.12484

Pratto, F., Sidanius, J., Stallworth, L. M. ve Malle, B. F. (1994). Social dominance orientation: A personality variable predicting social and political attitudes. *Journal of Personality and Social Psychology, 67*, 741-763.

Rapoport, D. (2004). The four waves of modern terrorism. A. K. Cronin ve J. M. Ludes (Ed.), *Attacking terrorism: Elements of a grand strategy* içinde (46-73). Washington: Georgetown University Press.

Sageman, M. (2004). *Understanding terror networks.* Philadelphia: University of Pennsylvania Press

Tajfel, H. (1970). Experiments in intergroup discrimination. *Scientific American, 223*(5), 96-103.

Webber, D. ve Kruglanski, A. W. (2018). The social psychological makings of a terrorist. *Current Opinions in Psychology, 19*, 131-134. doi:10.1016/j.copsyc.2017.03.024

Webber, D., Schimel, J., Martens, A., Hayes, J. ve Faucher, E. H. (2013). Using a bug-killing paradigm to understand how social validation and invalidation affect the distress of killing. *Personality and Social Psychology Bulletin, 39*(4), 470-481. doi:10.1177/2F0146167213477891

Ek A

Aşırıcılık Ölçeği

Yaşam ve toplum ile ilgili aşağıdaki yönergeleri dikkatlice inceledikten sonra, diğer insanların da bu konudaki görüşlerini dikkate alarak yönergeleri puanlayınız.

		Kesinlikle Katılmıyorum						Kesinlikle Katılıyorum
1	Bu ülkedeki çoğu insan, tamamen değişmesi gereken bir yaşam tarzına ve kültürüne sahiptir.	1	2	3	4	5	6	7
2	Eğer bir kişi çoğunluğun yaşam tarzı ve kültürüyle uyumlu yaşayamıyorsa, kendisi ve kendisi gibi düşünenler için tamamen farklı bir yaşam tarzı ve kültür yaratması gerekir.	1	2	3	4	5	6	7
3	Toplumun temeli olan ekonomik sistemi tamamen değiştirmek gereklidir.	1	2	3	4	5	6	7
4	Benim gibi düşünenler, hayatımızın temelini oluşturan öğeleri (ekonomi, iş, tüketim, refah) tamamen değiştirmek zorundadır. Toplumun geri kalanı istediğini yapabilir.	1	2	3	4	5	6	7
5	Eğer düzgün bir toplum istiyorsak, devletin demokratik formundan kurtulmalıyız.	1	2	3	4	5	6	7
6	Bırakın toplumun geri kalanı demokrasiyi seçsin; ben ve benim gibi düşünenler, kendi sosyal çevremiz için yeni bir sistem oluştururuz.	1	2	3	4	5	6	7
7	Ben ve benim gibi düşünenlerin toplumun geri kalanıyla hiçbir ortak yanı yoktur.	1	2	3	4	5	6	7
8	İyi ve doğru bir hayat yaşamanın sadece tek bir yolu vardır.	1	2	3	4	5	6	7
9	Eğer bir birey iyi ve doğru bir hayata göre yaşamıyorsa, o kişi toplumdan uzaklaşmayı seçmiştir.	1	2	3	4	5	6	7
10	Toplumlarda iyi ve doğru yaşamı desteklemeyen gruplar, haklarından mahrum bırakılmalıdır.	1	2	3	4	5	6	7
11	Yaşamla ilgili düşünceleri bizden tamamen farklı olan insanlarla ortak çözümler bulmaya çalışmak zaman kaybıdır.	1	2	3	4	5	6	7
12	Kişinin kendi görüşlerinden taviz vermesi yanlıştır.	1	2	3	4	5	6	7
13	İyi ve doğru bir hayat yaşamayanlarla beraber barış içinde yaşamak yanlış ve ahlaka aykırıdır.	1	2	3	4	5	6	7
14	Eninde sonunda bir yüzleşme olmalıdır; bir birey, yaşamaları gereken hayattan tamamen farklı bir yaşam sürenlerle sonsuza kadar barış içinde yaşayamaz.	1	2	3	4	5	6	7

Ek B

Aşırıcılık Ölçeği ile İlişkili Şiddet Yanlılığı ve Yasa Dışı Davranışlar Ölçeği

Bazı durumlarda bireylerin hukuka aykırı eylemlerde bulunmasının iyi veya gerekli olabileceği tartışmaya açık olabilir. Söz konusu durumlarla ilgili olarak aşağıdaki açıklamalara ne kadar katılıyorsunuz? Puanlama sırasında otorite (polis, ordu) tarafından yasal çerçevede kullanılan güçten değil, **sıradan insanların şiddet kullanımından** bahsedildiğini unutmayınız.

	Fiziksel şiddet kullanmak *Aşağıdaki durumlar söz konusu olduğunda işe yarayan tek seçenektir:*	Kesinlikle Katılmıyorum						Kesinlikle Katılıyorum
1	Kişinin dayanışma içerisinde olduğu bireyler için uygun koşullar oluşturmasında	1	2	3	4	5	6	7
2	Yeni ve daha iyi bir toplum oluşturmada	1	2	3	4	5	6	7
3	Bireyin yakın olduğu kişiler için uygun koşullar oluşturmasında	1	2	3	4	5	6	7
4	Bireyin kendi hakları ve güvenliğine saygı duyulmasını sağlamasında	1	2	3	4	5	6	7
5	Halkıma baskı ve saldırıyı önlemede	1	2	3	4	5	6	7
6	Daha büyük bir ideali (ideolojik, dini) savunmada	1	2	3	4	5	6	7

	Yasaları çiğnemek *Aşağıdaki durumlar söz konusu olduğunda işe yarayan tek seçenektir:*	Kesinlikle Katılmıyorum						Kesinlikle Katılıyorum
1	Kişinin dayanışma içerisinde olduğu bireyler için uygun koşullar oluşturmasında	1	2	3	4	5	6	7
2	Yeni ve daha iyi bir toplum oluşturmada	1	2	3	4	5	6	7
3	Bireyin yakın olduğu kişiler için uygun koşullar oluşturmasında	1	2	3	4	5	6	7
4	Bireyin kendi hakları ve güvenliğine saygı duyulmasını sağlamasında	1	2	3	4	5	6	7
5	Halkıma baskı ve saldırıyı önlemede	1	2	3	4	5	6	7
6	Daha büyük bir ideali (ideolojik, dini) savunmada	1	2	3	4	5	6	7

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.

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 150-250 kelimelik Türkçe "Öz" ile İngilizce "Abstract" ve makale başlığı içermelidir. 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 academic integrity therefore it is strictly committed to follow the publishing principles stated at COPE (https://publicationethics.org/) and DOAJ (https://doaj.org/publishers#licensing)

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.

- Article manuscripts should include abstracts both in Turkish and English between 150 and 250 words in the beginning of the manuscirpts. Turkish abstracts

are titled as "Öz" and English abstracts are titled as "Abstract". "Öz" and "Abstract" are written with single line spacing, 9 points font size and italic.

- 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

Journal of Security Sciences

Uluslararası Güvenlik Kongresi Özel Sayısı

Şubat/Feb 2020

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.: 6910 / 6970
www.jsga.edu.tr/guvenlik_bilimleri_dergisi/index.html
E-posta/Email: editorgbd@jandarma.gov.tr