ISSN 2792-0518

TERÖRİZM VE RADİKALLEŞME ARAŞTIRMALARI DERGİSİ

Terörizm ve Radikalleşme ile Mücadele
Araştırma Merkezi Derneği
Ankara 2025

T

Journal of Terrorism and Radicalization Studies

R

Cilt/Volume: 4
Sayı/Issue: 2
Yıl/Year: 2025
Haziran / June

A

www.tradergisi.com

D

editortrad@teram.org

Terörizm ve Radikalleşme Araştırmaları Dergisi

TRAD

Journal of Terrorism and Radicalization Studies

ISSN 2792-0518 (Basılı/Print)

ISSN 2822-2334 (Çevrimiçi/Online)

Cilt / Volume: 4 Sayı / Issue: 2 Yıl / Year: 2025

TERÖRİZM ve RADİKALLEŞME ARAŞTIRMALARI DERGİSİ

TRAD

ISSN 2792-0518 (Basılı) ISSN 2822-2334 (Çevrimiçi)

KÜNYE

(SOYADINA GÖRE SIRALANMIŞTIR)

SOSYAL MEDYA KOORDİNATÖRÜ

Betül ULAŞ

YAZIŞMA VE HABERLEŞME ADRESİ

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği

(TERAM)

Adres: Beytepe Mah. Kanuni Sultan Süleyman Bulvarı 5387. Cadde No:15A D:58

06800 Çankaya/Ankara

web sayfası: www.tradergisi.com

e-posta: editortrad@teram.org

BASKI

Vadi Grafik Tasarım Reklam Ltd.Şti.

İvedik Organize Sanayi Bölgesi 1420. Cadde No:58/1 Yenimahalle / ANKARA

Tel: 0312 395 85 71

DİZİNLER

TRAD halen "Index Copernicus", "Directory of Research Journals Indexing (DRJI)", "Advanced Sciences Index (ASI)", "EuroPub", "ASOS", "İdealonline", "IJIFACTOR", "Cosmos", "International Institute of Organized Research (I2OR)", "Directory of Open Access Scholarly Resources (ROAD)", "Academic Resource Index", "Semantic Scholar", "Cite Factor", "Eurasian Scientific Journal Index-ESJI" ve "Acarindex" bünyesinde taranmaktadır.

JOURNAL of TERRORISM and RADICALIZATION STUDIES

TRAD

ISSN 2792-0518 (Print) ISSN 2822-2334 (Online)

SOCIAL MEDIA COORDINATOR

Betül ULAŞ

CORRESPONDENCE AND COMMUNICATION

Research Center for Defense Against Terrorism and Radicalization Association (TERAM)

Address: Beytepe Mah. Kanuni Sultan Süleyman Bulvarı 5387. Cadde No:15A D:58

06800 Çankaya/Ankara

web page: www.tradergisi.com

e-mail: editortrad@teram.org

PRINTED BY

Vadi Grafik Tasarım Reklam Ltd.Şti.

İvedik Organize Sanayi Bölgesi 1420. Cadde No:58/1 Yenimahalle / ANKARA

Tel: 0312 395 85 71

INDEXES

TRAD is indexed in the “Index Copernicus”, "Directory of Research Journals Indexing (DRJI)", "Advanced Sciences Index (ASI)", "EuroPub", "ASOS", "Idealonline", "IJIFACTOR", "Cosmos", "International Institute of Organized Research (I2OR)", "Directory of Open Access Scholarly Resources (ROAD)", "Academic Resource Index", "Semantic Scholar", "Cite Factor", "Eurasian Scientific Journal Index-ESJI" and “Acarindex” indexes.

İÇİNDEKİLER / TABLE OF CONTENTS

EDİTÖR'DEN

Değerli Okuyucular,

Terörizm ve Radikalleşme Araştırmaları Dergisi'nin (TRAD) 2025 yılı Haziran sayısı olan 4. cilt 2. sayısıyla karşınızdayız. Dergimiz, kuruluşundan bu yana Türkiye'de terörizm ve radikalleşme çalışmalarına akademik bir zemin kazandırmak amacıyla yayın hayatına devam etmektedir. Disiplinlerarası yaklaşımı esas alan ve hem teorik hem uygulamalı çalışmalara yer veren TRAD, her geçen yıl daha geniş bir akademik çevrenin katkısıyla zenginleşmektedir. Bu sayımızda da terörizmin farklı boyutlarını ele alan değerli yazılara yer vermekten memnuniyet duyuyoruz.

Bu sayının ilk bölümü, radikalleşme psikolojisi alanının en saygın isimlerinden biri olan Prof. Dr. John Horgan ile gerçekleştirdiğimiz kapsamlı söyleşiye ayrılmıştır. Horgan, bireylerin terör örgütlerine katılım süreçlerinde etkili olan sosyal ve psikolojik etkenleri değerlendirmekte; aynı zamanda örgütten kopuş süreçlerini, gönüllü ve zorunlu ayrışma senaryolarını ayrıntılarıyla tartışmaktadır. Röportajda, "terörist kişilik" diye genellenebilecek bir profilin var olup olmadığı, tekil bireylerin örgütle ilişkilerinde deneyimledikleri çeşitlilik, yalnız kurt saldırganlar ve terörizmin toplumsal bağlamda nasıl içselleştirildiği gibi pek çok başlığa değinilmiştir. Deradikalizasyon programlarının etkinliğine dair eleştirileri ve alanda bilimsel yönteme dayalı ölçme-eğerlendirme eksikliğine dair uyarıları da literatüre yön veren niteliktedir. Bu röportaj, özellikle karşı şiddet stratejileri geliştirmek isteyen politika yapıcılar ve güvenlik uzmanları için önemli içgörüler sunmaktadır.

Bu sayının ilk araştırma makalesi, Pınar Begüm Koncagül tarafından kaleme alınan "DAEŞ Terör Örgütünün Yumuşak Hedef Saldırılarının İncelenmesi" başlıklı çalışmadır. Bu makale, DAEŞ'in özellikle 2014-2020 yılları arasında Türkiye'de gerçekleştirdiği şehir merkezli saldırılarını mercek altına alarak, örgütün şehir eylem stratejisini detaylandırmaktadır. Koncagül, şehirlerdeki kalabalık nüfus, sembolik yapılar ve medya görünürlüğünün terör eylemlerinde nasıl bir stratejik avantaja dönüştüğünü kapsamlı biçimde tartışmakta; DAEŞ'in özellikle yumuşak hedeflere yönelmesinin ardındaki örgütsel ve ideolojik gerekçeleri Küresel Terörizm Veritabanı (GTD) verileri üzerinden incelemektedir. Bu çalışma, terör örgütlerinin hedef belirleme süreçlerine dair literatüre hem kavramsal hem ampirik katkılar sunmaktadır.

Sayının ikinci makalesi, Büşra Beyoğlu tarafından yazılan "Terörizm ve Radikalleşmede Psikolojik ve Sosyolojik Faktörler: El-Kaide Örneği" başlığını taşımaktadır. Bu çalışma, El-Kaide'nin örgütsel yapısı ile bireysel katılım motivasyonları arasında bağ kurarak, radikalleşmenin bireysel-psikolojik ve toplumsal-sosyolojik düzeyde nasıl biçimlendiğini göstermektedir. Beyoğlu, ideolojik bağlılık, aidiyet arayışı, kimlik bunalımı, dini motivasyon ve toplumsal dışlanmışlık gibi faktörlerin bireyin terörizme yöneliminde nasıl birbirine eklemlendiğini özgün bir şekilde tartışmakta; bu bağlamda hem klasik radikalleşme modellerine hem de güncel çok faktörlü yaklaşımlara atıf yapmaktadır. Makale, özellikle radikalleşme sürecinde sosyal çevrenin ve dijital alanın etkisine de vurgu yaparak, El-Kaide gibi hiyerarşik yapıların birey üzerindeki dönüştürücü etkisini ortaya koymaktadır.

Üçüncü araştırma makalesi, Seçkin Aköz ve Hatice Sürüri imzalı "Kritik Altyapılarda Siber Güvenlik ve Siber Terörizm: Türkiye Üzerine Stratejik Bir İnceleme" başlıklı çalışmadır. Yazarlar, günümüzde devletlerin karşı karşıya kaldığı siber tehditlerin boyutlarını ve bu tehditlerin özellikle kritik altyapılar üzerinde yarattığı güvenlik açıklarını kapsamlı biçimde analiz etmektedir. Çalışma, enerji, sağlık, ulaşım gibi stratejik sektörlerdeki dijitalleşmenin siber saldırılar karşısında ne denli kırılgan hale geldiğini Türkiye bağlamında örneklerle göstermektedir. Makale, hem siber terörizm kavramının kuramsal temellerini irdelemekte hem de Türkiye'nin bu alandaki mevcut güvenlik politikalarını ve iyileştirme önerilerini değerlendirmektedir.

Bu sayıda teknoloji ve güvenlik ilişkisini ele alan bir diğer çalışma ise Hatice Varol Dağdelen tarafından kaleme alınan "Terörizmle Mücadele Alanında Yapay Zekânın Öngörücü Taktik Avantajları ve Dezavantajları" başlıklı araştırma makalesidir. Varol Dağdelen, yapay zekâ temelli teknolojilerin, özellikle tehdit öncesi veri analizi ve davranışsal örüntülerin tahmini gibi konularda sunduğu potansiyeli tartışmaktadır. Bununla birlikte yapay zekâ algoritmalarının önyargılarla şekillenme riski, etik sorunlar, hukuki sınırlılıklar gibi zorluklara da değinerek bu teknolojilerin kullanımında dikkat edilmesi gereken noktaları vurgulamaktadır. Makale, yalnızca teknik değil, aynı zamanda etik ve politik düzeyde çok katmanlı bir değerlendirme sunarak, güvenlik teknolojilerinin geleceğine dair önemli tartışmalara kapı aralamaktadır.

Son olarak, Özdemir Akbal'ın "Understanding the PKK Terrorist Organisation: Capabilities, Propaganda, and System" başlıklı kitap incelemesine yer veriyoruz. Bu inceleme, PKK'nın örgütsel kabiliyetleri, propaganda stratejileri ve eylem mekanizmaları üzerine yayınlanan akademik bir eseri kapsamlı biçimde değerlendirmektedir. Akbal, kitabın içeriğini sistematik olarak tanıtarak, bu alanda çalışan araştırmacılar için metodolojik ve kuramsal bir harita sunmaktadır. Kitapta sunulan kavramsal çerçeve, örgütün hem tarihsel dönüşümünü hem de çağdaş güvenlik algılarına etkisini anlamak isteyenler için önemli bir kaynak niteliğindedir.

TRAD Dergisi olarak, hem akademik titizliğe hem de güvenlik çalışmalarının güncel sorunlarına duyarlı olmaya devam edeceğiz. Dergimize katkı sunan tüm yazarlarımıza ve değerlendirme sürecine katkı sağlayan hakemlerimize içten teşekkür ederiz. Bir sonraki sayımızda yeniden görüşmek dileğiyle, keyifli okumalar dilerim.

Prof.Dr. Serhat ERKMEN

TRAD Editörü

INTERVIEW WITH DR. JOHN HORGAN: COMPLICATED FACTORS OF INDIVIDUALS' ENGAGEMENT IN AND DISENGAGEMENT FROM TERRORISM

ABSTRACT

John Horgan is Distinguished University Professor at Georgia State University's Department of Psychology. A psychologist by training, his research focuses on terrorist behavior. His work is widely published, with his critically acclaimed book, 'The Psychology of Terrorism' available in over a dozen languages worldwide. Dr. Horgan's research focuses on psychological issues in terrorism and political violence. He is especially interested in understandings the processes through which people become involved in and disengage from terrorism, as well as the psychological mechanisms through which people cope with involvement in terrorist activity. His current projects involve the development of interventions to counter terrorist recruitment. In May of 2025, Dr. Horgan received the FBI Director's Community Leadership Award. His most recent book is Terrorist Minds: The Psychology of Violent Extremism from al Qaeda to the Far Right, published by Columbia University Press.

Keywords: *Terrorism, Terrorist, Psychology, Process, Pathway, Profile.*

TRAD: Professor, thank you for accepting the interview request from the Journal of Terrorism and Radicalization Studies (TRAD). We see that you have a very broad perspective on terrorism and that you have produced many publications about terrorism and political violence. In this context, our first question will be about your precious book 'The Psychology of Terrorism', which has been translated into many languages. I would like to ask you the questions in the introduction of this book, which I assume is the result of a very long and arduous work. How and why does someone become a terrorist? Are there common causes? Is there a terrorist personality? If you were to briefly answer a very long topic, how would you answer these questions?

Dr. John Horgan: Thanks for having me here! Well, once upon a time we used to think that to be a terrorist, you needed to be mad. And we were wrong. We eventually came to realize that these were (for the most part) people making rational decisions about what they wanted to do. But the violence associated with terrorism often makes it hard for us to accept that it's not the product of warped minds. In reality, when someone becomes involved in terrorism, it's typically the result of a process that people gradually work their way through, either on their own, or with help.

We also used to think that there might be a simple profile, or personality type. And we were wrong about that too. Terrorists are mostly young, angry

men who want to fight against what they view as some gross injustice, on behalf of a wider people or community. But today's terrorists are quite diverse. Men, women, adolescents, even children, from all backgrounds, all ages, all different kinds of lifestyles and prior experiences, now have multiple opportunities to be involved in terrorism. If anything, diversity is the new terrorist profile. What involvement looks like and feels like tends to vary from person to person. Even in the smallest of movements, there's a variety of roles, tasks, jobs to be done, and so, there are different opportunities open to people who might be suited to different kinds of involvement.

There isn't one single pathway to terrorism, nor is the experience of 'being a terrorist' the same from person to person. People experience it in different ways, and as a result, are affected by their involvement in different ways. Even within a specific terrorist group, there tends to be a few different routes or pathways in. Some people must do research and find ways in from afar. Others are simply at the right place at the right time and take advantage of whatever local opportunities present themselves.

Terrorism is a strategy used by a wide variety of actors, groups and movements today, so it stands to reason there would be lots of different ways in which someone could get involved. And like I say, it also tends to be a gradual process. Nobody becomes a terrorist overnight. It involves working through a whole range of social and psychological issues. Sometimes people do all this in isolation. Other times people do this with the help of friends, or a recruiter, or with the help of online content of some kind. We now that getting involved in terrorism can come at an enormous cost to oneself or family.

For some people, though, getting involved is just a rite of passage. If you live in a community facing conflict on a daily basis, it may well be that you have some near or distant family members already involved. It's almost like it's something you are expected to do when you reach a certain age – for someone in that kind of context, getting involved just seems like a perfectly normal thing to do. It's also the case that some people get involved in terrorism because they are initially motivated by ideological issues or some shared grievance.

Many people get involved purely for social reasons, because they are in search of excitement, company, camaraderie or something else. But for those people, for whom ideology isn't the main driver, at least some of them might become more ideological the more time they spend in a movement. Nobody is motivated to become a terrorist because of one factor alone. It's typically a mix of ideological and non-ideological reasons, both public and private.

These specific factors, and their dynamics, vary a lot between different types of group, place and context. Across the ideological spectrum, terrorists have several features in common. They are motivated by moral outrage at some injustice. They identify with the plight of a bigger, wider community that they feel are victimized by some other entity, like a government. They view violence as a legitimate, necessary, and urgent response. All terrorists believe that their actions will help bring about a better future for themselves and for the community they claim to represent. I know I've said a lot here, but I promise that's a very brief answer to several big questions!

TRAD: As one of the academics who know this subject best, the second question we will ask you is about disengagement from terrorist organizations. How and why people leave terrorism and terrorist activity? Regardless of an individual's motivation, is it possible for them to join a terrorist organization, participate in the terrorist acts, and then leave that organization? In your words, is it possible to walk away from terrorism? And more importantly, is it really possible for terrorists to integrate into society and daily life?

Dr. John Horgan: In a word, yes. This is an area on which there's quite a lot of very good research now. Just as there are multiple pathways into a movement, there are also multiple pathways out. Regardless of what motivated someone to get involved, whether they were ideologically driven or motivated by friends and family, just about anyone at any level can decide they want to disengage, or leave terrorism behind.

People leave for lots of reasons. Sometimes it's because involvement is not quite what they imagined. They may be disillusioned at their new day-to-day reality. Jealousy, competition, personal rivalries happen in terrorist movements just like they do in any group or organization. Disillusionment is a very common theme in accounts of why people leave. Mind you, there are also people who have a very good time as terrorists – they enjoy it. It ends

up being everything they ever imagined it could be. We just don't know a lot about them. But overall, yes, it's very possible for people to walk away from terrorism. Some do it voluntarily, while others leave involuntarily, because they may have been caught or otherwise incapacitated through counter-terrorism action. And reintegration is certainly possible. There are many former terrorists who quietly re-enter the society they once claimed to hate. It's a lot easier to re-integrate when you have support, whether through opportunities, or some social structure to help you navigate that re-entry. For anyone who leaves terrorism behind, there are lots of obstacles and challenges to face on that journey, but it is possible.

TRAD: Professor Horgan, another question we have is about lone actor terrorism. When we examine your article titled 'Bombing Alone: Tracing the Motivations and Antecedent Behaviors of Lone-Actor Terrorists', which you prepared together with a few academics, we understood that, so many lone-actor terrorists were socially isolated. How do you define lone actor terrorism? We see that the majority of the Lone Actor terrorists are men. What could be the reason for this? Another observation we made is that the majority of lone actor terrorists committed their acts of terrorism with religious motivation. Is this correct? If so, what are the reasons for this? Could it be easier for lone actor terrorists to distance themselves from terrorism than for terrorists who have participated in organizational terrorism?

Dr. John Horgan: When we talk about lone actors we don't really mean people who are 'alone'. We're talking about people who take action not necessarily directed or shaped by the terrorist movement itself. These are people who are obviously influenced by a particular cause, grievance, or ideology, but they take it upon themselves to act independently of the movement.

The term 'lone actor' is misleading because in an age where social media can inspire and sustain terrorism, nobody is ever truly alone. But the term emerged as a way to distinguish those people who didn't seem to *belong* to an organization or movement in any formal sense. I would add that just about any movement can have lone actors, not just religiously motivated groups. It's not the ideology that determines how such strategies are deployed. Sometimes movements will call on lone actors to mobilize because, as in the case of the late stages of the Islamic State movement, it

became harder for westerners to travel to ISIS territory undetected. So instead, ISIS put effort into inspiring people to act out at home, where they might (at least in theory) have a much greater chance of successfully executing a violent act. So, the use of lone actors, or the promotion of lone actors, is as much a strategic choice as anything else. It's not easier for lone actor terrorists to distance themselves from terrorism. The whole point of terrorism is that the world knows that you did it, and you did it on behalf of a cause, or a movement.

And, interestingly, lone actors are often far quicker than group-based actors to leak their intentions to those around them. We don't quite understand what may be causing this, but group-based actors on the whole tend to be better at concealing their intent. Maybe that's because of training. We just don't know.

TRAD: Professor, in one of your articles 'Deradicalization or Disengagement? A Process in Need of Clarity and a Counterterrorism Initiative in Need of Evaluation' you argue that the concept of deradicalization should be distinguished from disengagement. Could you please explain the differences between these two concepts?

Dr. John Horgan: Of course. These are related but distinct concepts. Disengagement simply means stopping terrorist activity. Or, put another way, leaving terrorism behind. What I realized early on in my research was that you can disengage from terrorism, but you may or may not have had a change of views. So, on the one hand, you can have people who disengage from terrorism and have abandoned the ideology, or their support for the movement. We could say that those people are disengaged and de-radicalized. But alternatively, someone can leave terrorism behind while still maintaining their ideological commitment. So, those could be described as disengaged but *not* de-radicalized. It's also possible of course for people to be de-radicalized but not disengaged. There are many disillusioned people in terrorist groups who just don't have the opportunity to get out.

TRAD: Dr Horgan, what makes a terrorist stop being a terrorist? Is there an easy recipt to answer this question?

Dr. John Horgan: I wouldn't say there's an easy recipe, but it's not as complicated as we might think. It's a lot easier to understand why people get out of terrorism than why they get in. People either stop of their own accord,

or they stop because they are forced to. We could say that disengagement can be voluntary or involuntary. Involuntary disengagement might be when someone is caught or captured, so they have no choice but to disengage. We are still trying to learn more about the reasons people voluntarily stop, but so far, the research suggests that disillusionment is a very common theme. In simple terms, they just don't feel like being involved any more. We need to do a lot more research to verify just how widespread disillusionment is among all those who disengage, but the people who disengage and are willing to talk to researchers like me tend to share accounts that suggest they've become deeply disillusioned with some part of their lives as terrorists. It may be that they just don't believe in the cause anymore, or that they are burned out from the lifestyle.

Sometimes, it's just because they are fed up, bored, and want to do something else with the rest of their lives. Like I say, it's often not as complicated as we think. But so far the research on disengagement has been very promising. We must do a lot more work on this topic because it has such practical relevance for counterterrorism. If we know more about the causes of disengagement, we might be able to do something more pro-active to either stop people getting involved in the first place, or to facilitate exit for people who are already involved.

TRAD: What are the factors that psychologically draw individuals to terrorist organizations? Are individuals aware that when they join a terrorist organization, they will be involved in acts of violence and that other people may die or be injured as a result? In light of all this information, why do individuals join terrorist organizations?

Dr. John Horgan: That's a great question. Although I've studied terrorist psychology for a long time now, I struggle to give an easy answer. First, not everyone who wants to join a terrorist movement does so because they want to do violence. There's a role for everyone, especially in some of the bigger movements. Some want to be involved in the action, or at least they think they do. Others just want to help out in some way. They absolutely want to be involved, but just not involved in committing violent acts. They might be involved in training or fundraising or something else.

Believe it or not, but the people who do the violence for terrorist movements are actually few and far between. Terrorist organizations are

made up of lots of different people who occupy lots of different roles. Sometimes a person can hold multiple roles, and people will often move from one kind of role into another, depending on what the organizational needs are, or if the person seems to have a particular skill that might make them especially valuable in some way. As to why people join terrorist groups, well, there's no one single factor that causes this. It's typically a mix of big reasons and little reasons, or public reasons and private reasons. Yes, it's a story about the role of ideology, the cause that resonates with someone, that urge to want to fight back on behalf of a community. But it's also a story about what's going on in someone's own life, how they think and feel about it. It's about the lure of feeling part of something bigger that oneself, but it's also about the feeling one gets of being in a group of people who think and feel the same way as you to. It's a place to belong. It's a way to get revenge against one's enemies. There's a sense of adventure, excitement, purpose, status, power. It varies somewhat from person to person, but it's typically a mix of different factors.

TRAD: We know that many countries have implemented various deradicalization programs. We also know that states and communities such as the European Union have allocated large amounts of resources for these programs. How effective do you think the deradicalization programs have been? How accurate is it to claim that individuals who have gone through these programs will not engage in violent acts again? For example, is it possible to integrate into society those who have been members of a terrorist organization for 40 years, who have operated in various positions from militancy to management, and who have given orders for terrorist acts, through deradicalization programs?

Dr. John Horgan: Well, I guess what I would say is that it doesn't matter what I think. What matters is whether the evidence suggests these programs are effective. I wish I could say that evidence existed. A challenge of these programs is that quite frankly, we don't know that they work, nor do we know if the ones that seem to work, works for the reasons they suggest.

We need rigorous, scientific, and independent evaluations of these programs, and we just don't see much interest in entertaining such evaluations. So, to answers your question, do they work? Some do, many don't. But of the ones that are effective, they often work for reasons that have nothing to do with the actual programs. For instance, we know (for

reasons we still don't quite understand) that terrorist recidivism is very low, much lower than rates for non-terrorist crimes. It's often the case that terrorist deradicalization programs claim credit for outcomes that would have happened irrespective of whether the program existed. But there's still far too much speculation around what constitutes a successful program and why. We need a lot more research here.

TRAD: Dr. Horgan, we read that you interviewed a lot of terrorists in your research. Do you have any difficulties while and before interviewing terrorists? What was the most interesting thing you came across during your interviews? What is your general impression about terrorists as a result of these interviews?

Dr. John Horgan: I wouldn't say I've interviewed a *lot*. It felt like a lot at one time, but I am constantly trying to find more people to interview about their experiences. Even now, as I am researching for a new book, I'm working hard to find people who could be interviewed. And it's not easy. Ideally, as the researcher Jeff Victoroff recommends, if we are to be systematic about developing a psychology of terrorist behavior, we would need to interview people at all levels of a terrorist movement, to try to analyze accounts according to their roles, and levels of commitment. But I would say that interviewing really is an under-used tool in our arsenal. Interviewing is hard because it's just not easy to find many people who are willing to be interviewed about their experiences in terrorist movements. Some researchers travel to conflict zones to do this, while others can access prison populations.

It's sometimes possible to access former terrorists after they are released from prison, but many former terrorists just want to get on with their lives and not have to relive their experiences for a researcher. I understand that, especially because I've seen examples of researchers doing very irresponsible and unprofessional things during interviews. Just because a researcher has access to terrorists, doesn't mean they know how to conduct a proper interview. So, for many reasons, doing interviews, or rather, *relying* on interviews as a primary source of data, is often just not very practical. It can be very, very time consuming to even set up these interviews, and it can take years to finally access a particular person or group. There's no clear recipe for success here, but when we can get access, it's very important to use rigorous, scientific methods to collect our data. There are so many

factors to consider. Is the researcher relying on gatekeepers to find interviewees for them? Will the terrorist organization provide their own translator? Will the organization choose people *they* feel will give an interview that is sympathetic to their movement? So going into an interview with a very careful plan of action, knowing your subject, and being willing to listen while subtly knowing how and when to gently direct the conversation, are all very important elements for successful interviews. The general impression I've gotten from the interviews I've done is that people are willing to talk and are willing to offer frank and open accounts of what they did and why (in their minds) they did what they did. I think that in itself is surprising! But from my experience so far, I think the role of a good interviewer is really about learning to shut up and listen.

TRAD: Dr. Horgan, thank you for answering our questions. Is there anything you would like to add?

Dr. John Horgan: Thank you for asking. I have to take advantage of the opportunity to highlight my recent book, *Terrorist Minds.* If any of your readers want to learn more about terrorist psychology, please do check it out. And thanks for the opportunity to talk about the work!

Terörizm ve Radikalleşme Araştırmaları Dergisi-TRAD, 2025, 4(2) : 165-185 Araştırma Makalesi
Journal of Terrorism and Radicalization Studies-TRAD, 2025, 4(2): 165-185 Research Article
DOI: 10.61314/traddergi.1622651

DAEŞ TERÖR ÖRGÜTÜNÜN YUMUŞAK HEDEF SALDIRILARININ İNCELENMESİ

Pınar Begüm KONCAGÜL*

ÖZET

Terörizm siyasi, dini veya ideolojik amaçlarla korku ve dehşet yaratmak için şiddet kullanma eylemlerini ifade eden bir terimdir. Son yıllarda terörizm olgusunun dünya çapında yükselişe geçmesiyle birlikte eylemler insanların bir araya geldiği korunmasız yerlere doğru yönelmeye başlamıştır. Bu bağlamda çalışmanın ilk başlığında terör örgütlerinin şehirlerde eylem gerçekleştirmesinin nedenleri ve şehir eylem stratejisinin kavramsal çerçevesi incelenecektir. Bu strateji, özellikle 20. yüzyılın ikinci yarısında Latin Amerika'da ve diğer bölgelerde gerilla savaşı yürüten gruplar arasında etkili olmuştur. İkinci başlıkta yumuşak hedef kavramı tartışılacaktır. Yumuşak hedefler, genellikle güvenlik önlemlerinin düşük olduğu, sivil nüfusun yoğunlukla bulunduğu ve kolayca saldırıya uğrayabilecek yerlerdir. DAEŞ, ideolojik hedeflerini gerçekleştirmek, korku yaymak ve propaganda etkisini artırmak için özellikle bu tür hedeflere saldırılar düzenlemiştir. Son başlıkta ise DAEŞ terör örgütünün tarihsel arka planı anlatılıp ardından 2014-2020 yılları arasında Türkiye'de gerçekleştirmiş olduğu yumuşak hedef saldırıları Global Terrorism Database (GTD)/ Küresel Terör Endeksi üzerinden yapılan inceleme ile analiz edilecektir. Çalışmada nitel veri toplama yöntemlerinden doküman analizi yöntemi kullanılacaktır. Çalışmanın temel amacı, DAEŞ'in yumuşak hedef saldırılarını hem teorik hem de örnek olaylar üzerinden değerlendirmek ve bu tür saldırıların önlenmesine yönelik stratejiler geliştirilmesine katkı sunmaktır.

Anahtar Kelimeler: *Terörizm, Terör, Güvenlik, Yumuşak Hedefler, DAEŞ*

INVESTIGATION OF SOFT TARGET ATTACKS OF ISIS TERRORIST ORGANIZATION

ABSTRACT

Terrorism is a term that refers to acts of violence used to create fear and terror for political, religious, or ideological purposes. In recent years, with the global rise of terrorism, attacks have increasingly targeted unprotected places where people gather. In this context, the first section of this study examines the reasons why terrorist organizations carry out attacks in urban areas and the conceptual framework of urban attack strategies. This strategy has been effective among groups waging guerrilla warfare in Latin America. The second section discusses the concept of soft targets. Soft targets are typically locations with low security measures, where civilians gather in large numbers and are more vulnerable to attacks. ISIS has specifically attacked such targets to achieve its ideological goals and increase its propaganda effect. The final section provides the historical background of the ISIS terrorist organization and analyzes its soft target attacks in Türkiye between 2014 and 2020 through an examination based on the Global Terrorism Database (GTD). The study employs qualitative research methods, specifically document analysis. The primary objective of the research is to evaluate ISIS's soft target attacks both theoretically and through case studies, contributing to the development of strategies to prevent such attacks.

Keywords: *Terrorism, Terror, Security, Soft Targets, ISIS*

* Araştırma Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, pnrbgm01@hotmail.com, ORCID: 0000-0003-0756-9454

GİRİŞ

Terörizm, terör saldırısının doğrudan kurbanları yerine rakip etnik veya dini grubu, bir ulusal hükümeti, siyasi partiyi veya genel olarak kamuoyunun tümünü de içeren geniş kapsamlı psikolojik etkilere sahip olacak şekilde hedef kitleye korku aşılamayı amaçlayan bir siyasal şiddet hareketidir (Hoffman, 2006, ss.40-41). Bu bağlamda teröristler, uyguladıkları şiddetin yarattığı tanıtım aracılığıyla ulusal veya uluslararası ölçekte siyasi değişimi etkilemek için normalde sahip olmadıkları etki, nüfuz ve gücü elde etmeye çalışmaktadırlar. Gerçekleştirdikleri eylemlerle de ölen/yaralanan kurbanlardan ziyade eylemi seyreden insanlar üzerindeki etkileri önemsemektedirler. Terörist örgütler, sembolik veya sivil hedeflere karşı sürekli şiddet kullanarak korku yayma, siyasi haksızlıklara mümkün olduğunca fazla dikkat çekme ve şiddete karşı aşırı veya toplum tarafından kabul edilemeyecek şiddetle karşılık verilmesini kışkırtarak kitleleri harekete geçirmeye çalışmaktadır (Kiras, 2007, ss.187-188).

Günümüzde terör saldırıları ele alındığında ağırlıklı olarak şehir merkezli bir strateji ön plana çıkmaktadır. Şehir eylem stratejisi olarak adlandırılan bu stratejide kalabalık nüfus ilk stratejik unsur olarak değerlendirilebilir. Şehirlerde artan nüfus terör örgütleri için militan toplayabilecekleri ve eyleme geçebilecekleri gizli bir protesto ortamının varlığını doğurmuştur (Blanc, 2013, s.799). Teröristler için cazip hedefler şehirlerde yoğunlaşmıştır ve bu tür saldırılar gerçekleştiğinde ulusal ve uluslararası bir izleyici kitlesine sahip olunmuştur. Bu noktada nüfusun büyük ölçüde azaldığı kırsal bölgelerde sayısal olarak üstün kolluk güçleri tarafından etkisiz hale getirilen teröristler, özellikle 11 Eylül saldırısı sonrası uzun süreli halk savaşı stratejisini şehir eylem stratejisine uyarlamıştır (Taw ve Hoffman, 2007, s.73). İkinci stratejik unsur şehirlerde kamufle olmanın daha kolay olması ve doğal olarak tespit edilmenin de daha zor olmasıdır. Üçüncü stratejik unsur ise terör örgütlerinin şehirlerde yaptıkları eylemlerle medyada ve uluslararası alanda daha fazla ilgi çekme fırsatlarına sahip olmalarıdır. Bu bağlamda şehir merkezlerinde gerçekleştirilen terör eylemleri kırsal alanlara göre hem insani hem de fiziki açıdan çok daha büyük zayiata yol açmakta ve şehirlerde gerçekleşen bir terör eyleminin etkileri domino etkisi yaratarak çevre şehirlere ve hatta başka ülkelere sıçrayabilmektedir (Kurum, 2023, s.136).

Şehirler, terör örgütleri için kolaylıkla saldırabilecekleri pek çok hedef barındırmaktadır. Bu hedefler alan yazında '*yumuşak hedef*' kavramı ile tanımlanmaktadır. Yumuşak hedeflerin yumuşak olarak adlandırılmasının nedeni bu mekanların terör saldırılarına karşı savunulmasının görece zor olması ve teröristler için kolay hedefler olmasıdır. Terör örgütleri metropollerde mümkün olduğu kadar çok insanı yaralama veya öldürme amacıyla yumuşak hedeflere yönelik şiddet içeren saldırılar gerçekleştirilmektedir.

Çalışmada terör örgütlerinin hedef seçimlerindeki değişim incelenecek ve yumuşak hedef kavramı açıklanacaktır. Bu kavram DAEŞ (ed Devlet'ul İslamiy el-Irak veş-Şam) terör örgütü üzerinden ifade edilecektir. DAEŞ, çoğunlukla Irak ve Suriye'de faaliyet gösteren ve bir hilafet devleti kurma amacı doğrultusunda eylem gerçekleştiren selefi ve cihatçı bir terör örgütüdür (Ünsal ve Olçar, 2019, s.128). DAEŞ, küresel terörizmin en dikkat çeken ve yıkıcı aktörlerinden biri olarak özellikle 2014-2020 yılları arasında gerçekleştirdiği eylemlerle uluslararası güvenlik ve barışa yönelik ciddi tehditler oluşturmuştur. Bu bağlamda çalışmanın amacı DAEŞ'in yumuşak hedef saldırılarını hem teorik hem de örnek olaylar üzerinden değerlendirmek ve bu tür saldırıların önlenmesine yönelik stratejiler geliştirilmesine katkı sunmaktır.

Bu bilgiler ışığında DAEŞ terör örgütünün tarihsel gelişimi, ideolojik temelleri ve saldırı stratejileri ele alınarak Türkiye'de 2014-2020 yılları arasında gerçekleştirdiği yumuşak hedef saldırıları analiz edilecektir. Araştırma kapsamında, Küresel Terör Endeksi (Global Terrorism Database-GTD) verilerinden yararlanılarak örgütün Türkiye'deki saldırılarının niteliği değerlendirilecektir. Bu bağlamda Küresel Terör Endeksi (GTD), 1970'ten 2020'ye kadar dünya genelinde gerçekleşen terör olayları hakkında bilgi içeren açık kaynaklı bir veri tabanıdır. Çalışmada nitel veri toplama yöntemlerinden doküman analizi yöntemi kullanılacaktır. Çalışma, DAEŞ'in saldırı stratejilerini anlamaya yönelik bir zemin sunarken yumuşak hedeflerin korunmasına yönelik güvenlik politikalarının geliştirilmesine de katkı sağlamayı hedeflemektedir.

Çalışmanın araştırma soruları:

- DAEŞ terör örgütü zamansal ve mekânsal sınırlılıklar kapsamında kaç saldırı gerçekleştirmiştir?

- Bu saldırıların kaçı yumuşak hedeflere yönelik olmuştur?
- Örgüt neden şehir eylem stratejisini tercih etmiştir? şeklinde seçilmiştir.

Çalışma alan yazında yumuşak hedef olarak tanımlanan hedeflere yönelik saldırıların terör örgütleri tarafından toplumun tipik caydırıcı politikalarını aşmanın bir yolu olarak son dönemlerde sıklıkla kullanıldığı hipotezi üzerine şekillenecektir. Sonuç ve değerlendirme kısmıyla da çalışma tamamlanacaktır.

1.ŞEHİR EYLEM STRATEJİSİ VE TERÖR ÖRGÜTLERİNİN HEDEF SEÇİMİNDEKİ DEĞİŞİM

Terörizm kavramının kullanımı oldukça eskilere dayanmaktadır. 18 ve 19. yy'da daha çok ulusal boyutta kullanılan terörizm, 20. yy ile uluslararası bir hal almıştır. Bu noktada uluslararası terörizm olgusu, 2000'li yıllarda özellikle 11 Eylül saldırısı sonrasında terör örgütlerinin dünya çapında nüfusun fazla olduğu şehir merkezlerinde büyük çaplı saldırılar düzenlemesiyle birlikte uluslararası bir endişe kaynağı haline gelmiştir.

Terör örgütlerinin şehirlerde yürüttükleri eylemleri şehir eylem stratejisi ile açıklamak mümkündür. Bu noktada şehir eylem stratejisi sahada etkili olan ve stratejinin teorisyenliğini yapan Carlos Marighella'nın yazdığı '*Şehir Gerillasının El Kitabı'* üzerinden açıklanabilir. Şehir eylem stratejisi, özellikle 20. yüzyılın ikinci yarısında Latin Amerika'da ve diğer bölgelerde gerilla savaşı yürüten gruplar arasında etkili olmuştur. Carlos Marighella, Brezilyalı Marksist bir devrimci ve ALN (Ação Libertadora Nacional/Ulusal Kurtuluş Hareketi) örgütünün lideri olarak yazdığı bu kitapta şehirlerde örgütlenmenin amaçlarını, hedeflerini ve taktiklerini paylaşmıştır. Marighellaya göre şehir gerillasının temel stratejisi, iktidardakileri ülkenin siyasi durumunu askeri bir duruma dönüştürmeye zorlayacak şiddet içeren eylemler gerçekleştirerek siyasi krizi silahlı çatışmaya dönüştürmektir (Marighella, 2003, s.26). Bu durumun halkın orduya ve polise karşı isyan etmesine ve mevcut yönetimin meşruluğunun azalmasına neden olacağını öngörmüştür.

Şehir gerillalarının bu amaç doğrultusunda silahlı propaganda da dahil olmak üzere çeşitli hedeflere (grevler ve iş kesintileri; suikastlar; adam kaçırma; okulların, fabrikaların ve radyo istasyonlarının geçici olarak işgal edilmesi) yönelik saldırılara, sabit hedeflere (bankalar, işletmeler, askeri

kamplar, polis karakolları ve hapishaneler) yönelik saldırılara ve ekonomik varlıkların sabote edilmesi vb. eylemlere girişeceğini ifade etmiştir (Marighella, 2003, s.63). Marighella'ya (2003) göre şehirlerdeki eylem hayati önem taşımaktadır ancak mücadele eninde sonunda kırsala aktarılmalıdır (s.63). Bu noktada şehir gerillalarının görevi 'devrimci savaşta belirleyici rol oynamaya mahkûm olan' kırsal gerilla savaşının ortaya çıkmasına ve hayatta kalmasına izin vermektir (Williams, 2008, s.7).

Şehir eylem stratejisinin bir diğer savunucusu David Killcullen ise kırsal ayaklanmanın yerini kentsel ayaklanmanın aldığını ve buna birbiriyle ilişkili dört sürecin yol açtığını ifade etmiştir. Bunlar: nüfus artışı, kentleşme, sahilleşme ve bağlantılılıktan oluşan dört mega trenddir (Killcullen, 2013, s.28). Killcullen, güncel çatışma ortamının değiştiğini ve geleneksel olmayan savaşların daha sık yaşandığını belirtmekte ve bu noktada alınacak tedbirlerin yeni tehdit ortamına uygun hale getirilmesini ve sadece askeri olmaması gerektiğini çünkü askeri çözümlere uygun olmayan düşmansız tehditlerin de olduğunu vurgulamaktadır (Killcullen, 2013, s.239-240). Şehirlerde güvenliğin ancak bu faktörlere de önem vererek sağlanabileceğini savunmaktadır.

Terör örgütlerinin şehir eylem stratejisini benimsemesinin pek çok sebebi vardır. Bunlar:

- Şehirlerdeki kalabalık nüfus,
- Şehirlerde terör örgütlerinin eleman temini noktasında zorlanmaması,
- Şehirlerde medyanın ve kalabalık nüfusun etkisiyle terör örgütlerinin yaptıkları eylemlerle daha çok dikkat çekmesi,
- Şehirlerin genellikle sembolik öneme sahip binalar, anıtlar, meydanlar ve gelişmiş ulaşım ve iletişim altyapı içermesi,
- Teknolojik yeniliklerin kırsal kesimlerdeki teröristlerin çoğunun takip edilmesine ve eylemlerinin sınırlı kalmasına sebep olmasıdır.

İlk stratejik unsur şehirlerdeki kalabalık nüfustur. Dünya nüfusunun yarısından fazlası kentsel yerleşim alanlarında yaşamaktadır. Gelişmiş ülkelerin çoğu yüksek düzeyde kentleşmiştir. BM (Birleşmiş Milletler) Dünya Kentleşme Beklentileri Raporuna göre dünyadaki kentsel nüfusun payı her beş yılda bir %2 artmakta ve 2030 yılında dünya nüfusunun neredeyse %61'inin kentsel alanlarda yaşayacağı tahmin edilmektedir

(Valiyev, 2007, s.3). Bu bağlamda kırsal bir hedefe yönelik bir saldırıyı uzak bir ülkede yaşayan insanları ilgilendiren bir saldırıyla ilişkilendirmek zor olabilir. Fakat şehirlerde meydana gelen yıkım görüntüleri ve büyükşehirdeki tahribata ilişkin açıklamalar dünyanın pek çok yerinde şehirlerde yaşayan insanlar tarafından dikkat çekmekte ve endişe duymalarına sebep olmaktadır.

1960'lardaki kırsal gerillayı bırakıp şehir eylem stratejisine geçişin ana nedenlerinden biri şehirlerde teröristler için her zaman bir gazetecinin, kameranın veya geniş bir izleyici kitlesinin varlığının olmasıdır (Laquer, 2001, s.109). Bu noktada şehir eylemleri, terör örgütlerine daha geniş bir görünürlük sağlar. Bu noktada Latin Amerikalı bir terörist 'Kasabadaki bir binaya küçük bir bomba bile koysak basında manşetlere çıkacağımızdan emin olabilirdik. Ama kırsal gerillalar otuz kadar askeri tasfiye etse bile son sayfada sadece küçük bir haber olurdu. Bu yüzden şehir hem siyasi mücadele hem de propaganda açısından son derece önemlidir.' ifadelerini kullanmıştır (Blanc, 2013, s.802).

İkinci stratejik unsur şehirlerde terör örgütlerinin eleman temini noktasında zorlanmamasıdır. Şehirler, farklı kültürlerin, etnik grupların ve sosyal sınıfların bir arada yaşadığı kompleks ortamlardır (Bauman, 2004, s.115). Bu çeşitlilik, sosyal gerilimlere ve bireylerin daha kolay radikalleşmesine zemin hazırlayabilir. Bu bağlamda şehirlerdeki bu sosyal gerilimler, terör örgütlerinin destek bulmasına zemin hazırlamaktadır. Kırsal kesimdeki küçük kasaba ve köylerden gelen, yerinden edilmiş ve kültürel olarak yabancılaşmış kişiler ekonomik kazanç ve iyileştirilmiş yaşam koşulları vaat eden terörist grupların manipülasyonuna bu noktada son derece açıktır (Taw ve Hoffman, 2007, s.73). Banka soygunu, gasp veya uyuşturucu kaçakçılığı gibi faaliyetlerden elde edilen gelir işsiz, yabancılaşmış ve hoşnutsuz gençler için güçlü bir çekim sağlamaktadır.

Üçüncü stratejik unsur ise şehirlerde medyanın ve kalabalık nüfusun etkisiyle terör örgütleri yaptıkları eylemlerle daha çok dikkat çekmektedir. Olaylara tanık olan insanların sosyal medya aracılığıyla yayınladıkları görüntüler ve videolar dünya çapında saldırıların yarattığı kaosu, paniği ve korkuyu arttırmaktadır. Saldırıya tanık olan insanlar önceden güvenli ve risksiz olarak niteledikleri bölgeleri saldırı sonrası tehdit ve riskin yüksek olduğu bölgeler olarak değerlendirmekte; umutsuzluk, sosyal hayatı kısıtlama, yaşam kalitesini düşürme gibi duygulara kapılmaktadır (Çardak, 2022, ss.763-764). Bu doğrultuda şehirlerde gerçekleştirilen terör eylemleri

kırsalda gerçekleştirilen eylemlere kıyasla daha büyük psikolojik etki yaratmaktadır.

Dördüncü stratejik unsur şehirler genellikle sembolik öneme sahip binalar, anıtlar, meydanlar ve gelişmiş ulaşım ve iletişim altyapısı içermektedir. Terör örgütleri, bu altyapıları kullanarak hızlı ve etkili saldırılar düzenleyebilir ayrıca politik veya ideolojik mesajlarını iletmek ve simgesel bir zafer elde etmek amacıyla bu tür sembolik hedeflere saldırabilirler (O'Neill, 2005, s.75). Ek olarak gelişmiş ulaşım ve altyapıları saldırılarını planlama, koordine etme ve gerçekleştirme açısından avantaj olarak da kullanabilirler. Bu doğrultuda hem kolluk kuvvetlerinin kentsel alanlarda manevra yapma yeteneğinin olmaması hem de terör örgütleri için kırsal bir alana göre şehirlerde daha kazançlı hedeflerin olmasından dolayı terör örgütleri eylemlerini şehirlere yöneltmiştir.

Beşinci stratejik unsur ise teknolojik yenilikler kırsal kesimlerdeki teröristlerin çoğunun takip edilmesine ve eylemlerinin sınırlı kalmasına sebep olmuştur (Valiyev, 2007, s.4). Fakat şehirlerde terörist örgütler topluluk içinde kolayca gizlenip kamufle olabilir ve hareket edebilirler. Devlet her ne kadar teknolojik açıdan üstün olsa da çağdaş şehirler özellikle de hızla büyüyen gecekondu mahalleleri teröristlere kaçma, saklanma veya karşı saldırı için en iyi fırsatları sunmaktadır (King, 2021, s.16). Bu bağlamda büyük şehirlerdeki karmaşık coğrafi yapı, teröristlerin kaçmasına ve aşırı kalabalık yerlerde saklanarak güvenlik güçleri tarafından yakalanmamasına yardımcı olmaktadır.

Terör örgütlerinin şehirlerde eylem gerçekleştirmesi geniş bir perspektiften değerlendirilmelidir. Bu noktada yukarıda sayılan unsular çerçevesinde şehir eylem stratejisinin terör örgütleri tarafından günü birlik veya popülariteden kaynaklanan bir amaçla gerçekleştirilmediği anlaşılmalıdır. Şehir eylem stratejisi kırsal mücadeleye temel oluşturmaktadır. Devletler terörle mücadelede, teknolojik gelişmelerin ve şehirleşmenin potansiyel etkilerini anlayarak ve bu bağlamda etkili stratejiler geliştirerek hareket etmelidir.

2.YUMUŞAK HEDEF KAVRAMI

Günümüzde terörizmin dünya çapındaki yükselişine sınırlı koruma tedbirleriyle karakterize edilen hedeflere yönelik bir dizi saldırı eşlik

etmektedir. Bu saldırılar daha iyi planlama, daha büyük destek ve fon gerektiren ve başarı şansının daha düşük olabileceği sertleştirilmiş yapılar yerine alan yazında yumuşak hedef olarak adlandırılan yapılara karşı gerçekleştirilmektedir. Bu bağlamda terör örgütleri, metropollerde mümkün olduğu kadar çok insanı yaralama veya öldürme amacıyla saldırılarını yeni ve daha çekici hedefler olan kalabalık yerlere yönlendirmiştir.

Sert hedeflerden yumuşak hedeflere yönelik bu geçiş hem ulus ötesi hem de ülke içi terörizm olaylarında meydana gelmiş ancak bu eğilim ülke içi terörizmde daha belirgin bir hal almıştır (Sandler, 2014, s.263). Bu noktada 2000-2016 yılları arasında dünyada gerçekleştirilen terör saldırıları incelendiğinde %46'sının yumuşak hedeflere yönelik gerçekleştiği görülmektedir (Cuesta vd, 2019, 878). Bu saldırıların en bilinenleri ise 2015 yılında gerçekleştirilen Charlie Hebdo Saldırısı, 2016 yılında gerçekleştirilen Brüksel saldırıları, 2017 yılında gerçekleştirilen Barselona Las Ramblas saldırısı, 2017 yılında gerçekleştirilen Manchester Arena saldırısı ve 2019 yılında gerçekleştirilen Yeni Zelanda'daki cami saldırısıdır (Petra, Hoskova-Mayerova ve Navratil, 2019, s.453).

Avrupa Komisyonu yumuşak hedefleri 'savunmasız ve korunması zor olan ve aynı zamanda bir saldırı durumunda kitlesel ölüm olasılığının yüksek olduğu' yerler olarak tanımlamıştır (Avrupa Komisyonu, 2023). Fagel ve Hesterman'a göre de yumuşak hedefler genellikle 'saldırıya karşı savunmasız olan ancak korunmayan herhangi bir kişi veya şey; savunmasız ve korunması zor olan ve aynı zamanda bir saldırı durumunda kitlesel kayıpların yüksek olasılığı ile karakterize edilen yerler' olarak tanımlanabilir (Fagel ve Hesterman, 2016, s.4). Santifort, Sandler ve Brandt en fazla risk altındaki alanların pazar meydanları, toplu taşıma, alışveriş merkezleri gibi kamusal alanlar ve muhtemelen kentsel alanlara yakın konumdaki diğer halka açık toplanma alanları olduğunu belirtmiştir (Santifort, Sandler ve Brandt, 2013, s.15). Bu yerler, teröristler tarafından kitlesel toplanma özelliklerine sahip olmalarının yanı sıra temsili veya sembolik değerleri olması ve çok sayıda can kaybına yol açma olasılıkları nedeniyle seçilmektedir (Cuesta vd, 2019, s.878).

Devlet kontrolünde korunan tüm hedefler katı ve resmi hedefler olarak sınıflandırılırken devlet aygıtında hiçbir resmi rolü olmayan tüm kuruluşlar ve bireyler yumuşak hedef kapsamında değerlendirilmektedir. Bu noktada yumuşak hedefler insanların ders çalışmak, alışveriş yapmak, yemek yemek, eğlenmek, ibadet etmek veya seyahat etmek için bir araya geldiği toplumu

ve ekonomik refahı destekleyen yerlerdir. Kamuya veya özel mülkiyete ait olabilirler ve doğaları gereği bir terör saldırısına karşı savunmasızdırlar. Tipik yumuşak hedefler arasında dini merkezler (cami, kilise, sinagog, cenaze törenleri vs.), eğitim kuruluşları, sağlık merkezleri (hastaneler), kültürel aktivite alanları (konser salonları, stadyumlar, müzeler, düğün salonları vs.), ulaşım merkezleri (havalimanları, tren ve otobüs garları, metro istasyonları vs.) gibi çok sayıda insanı içeren alanlar yer almaktadır (Zeman, 2020, s.110).

Yumuşak hedeflere olan saldırı eğiliminin 11 Eylül saldırısı sonrasında arttığı söylenebilir. 11 Eylül saldırısı sonrasında ABD, askeri tesisler, hükümet binaları ve ulaşım sistemleri, kritik alt yapı gibi hali hazırda sert olan hedefleri daha da güçlendirmek için büyük adımlar atmıştır (Hesterman, 2018, s.6). Bu tesisler daha fazla güvenlik kamerası ve daha fazla insan gücüyle korunmaya başlanmıştır. Ancak sert hedef olarak adlandırılan bu alanların yeni teknoloji ve taktiklerle daha fazla korunması teröristlerin ilgisini sivil merkezli yumuşak hedeflere yöneltmiştir. Bu noktada yumuşak hedeflere olan erişim kolaylığı, yumuşak hedef çeşitliliğinin fazla ve cazip olması, daha kolay, daha ucuz ve daha kısa planlama döngüsü içermesi teröristlerin bu hedeflere yönelmesine zemin hazırlamıştır (Martin, 2016, s.274).

İnsanların yoğun olarak bulunduğu yerlere yönelik terörist saldırıların sayısının son yıllarda artması nedeniyle bu yerlerin güvenliğinin sağlanması ve saldırılara karşı önlem alınması gerekmektedir. Bu nedenle son yıllarda yumuşak hedeflerin güvenliğinin artırılmasına yönelik tedbirler konusuna büyük önem verilmekte ve yumuşak hedeflerin korunması konusu güncel bir noktada yer almaktadır. Fakat şöyle de bir gerçek vardır ki kiliseler, sinagoglar, camiler veya Noel pazarı gibi fazlaca insanın bulunduğu yumuşak hedefleri korumak büyük bir zorluktur. Ayrıca yumuşak hedeflerin sayısının neredeyse sonsuz olması ve bir yumuşak hedef sertleştirilirse dahi teröristlerin sınırsız sayıdaki bir başka yumuşak hedefi seçebileceği gözden kaçırılmamalıdır (Schmid, 2021, s.820). Bu noktada bir toplumu özgür tutmak ile vatandaşlarını ve ziyaretçilerini güvende tutmak arasında ince bir denge vardır. Özellikle saldırı araçları yüksek hızla kalabalığa doğru sürülen bir kamyonet gibi gündelik nesnelerse olay gerçekleşmeden önce dakikalar veya saniyeler içinde yapılabilecek pek bir şey yoktur. Kaldırıma gizlenmiş fiziksel güvenlik bariyerleri gibi proaktif önlemler ise yaya olarak gelip

saldıran teröristler için geçerli olmayacaktır. Bu nedenle alınacak tedbirlerin ve önlemlerin ciddi anlamda düşünülerek tasarlanması gerekmektedir.

3.DAEŞ TERÖR ÖRGÜTÜ VE YUMUŞAK HEDEF SALDIRILARI

DAEŞ terör örgütü kurulduğu ilk günden beri pek çok isimle anılan ve Suriye ve Irak'ta faaliyet gösterip bu bölgede bir İslami halifelik kurarak nüfuzunu dünyaya yaymayı amaçlayan selefi-cihatçı bir örgüttür (Hashim, 2014, s.70). Tarihsel arka plan olarak DAEŞ'in tarihini dört döneme ayırmak mümkündür. İlk dönem 2006'da Irak İslam Devleti adıyla kurulana kadar geçen dönemi kapsamaktadır (Pinos ve Steven, 2020, s.1037). Bu dönem Ebu Musab Ez-Zerkavi'nin öncülüğünde tanımlanmıştır. Bu dönemde örgüt, Afganistan'daki eğitim kamplarından Irak'a taşınmış ve burada Cemaat el-Tevhid ve'l-Cihad adı altında faaliyetler yürütmüştür (Byman, 2003, s.145). 2004 yılında Zerkavi, El Kaide'ye bağlılık yemini etmiş ve Irak El Kaidesini kurmuştur (Sevinç ve Çitfçi, 2015, s.30). O tarihte Saddam Hüseyin'in devrilmesinin yarattığı iktidar boşluğu terör örgütlerin gelişmesi için ideal koşulları sağlamıştır. 2006 yılında Irak El Kaidesi, ABD ve müttefik güçlerin işgaline karşı birçok Sünni aşırıcı grupla bir araya gelerek ocak ayında 'Mücahidin Şûra Konseyi', ekim ayında ise 'Irak İslam Devleti (ISI)' adını almıştır (Pinos ve Steven, 2020, 2.1038).

2006-2011 yılları arası örgütün gerilediği dönem olarak ikinci dönem şeklinde ele alınmıştır. Aynı zamanda bu dönem Ebu Ömer el-Bağdadi'nin örgütün başında olduğu ve örgütün eski gücünü yeniden kazanmayı istediği bir dönemdir. Nisan 2010'da Ömer el-Bağdadinin ölümünün ardından Şura Konseyi, Ebu Bekir el Bağdadi'yi Irak İslam Devleti'nin yeni lideri olarak atamıştır (Doğaner ve Yoldaş, 2023, s.51).

Örgüt varlığının 2011'den 2016'ya kadar olan üçüncü dönemine ise küresel genişleme damgasını vurmuştur. Amerikan ordusunun Aralık 2011'de Irak'tan çekilme kararı, bölgede yaşanan Arap Baharı, Libya lideri Muammer Kaddafi'nin ölümü ve Şii Başbakan Nuri el-Maliki'nin Irak'taki Sünni topluluğa yönelik baskıcı politikası Irak'ta önemli bir etki yaratmıştır. Bunlara ek olarak Suriye çatışması Irak İslam Devleti'nin 2011 yılı itibariyle Rakka'daki varlığını geliştirmesini sağlamıştır.

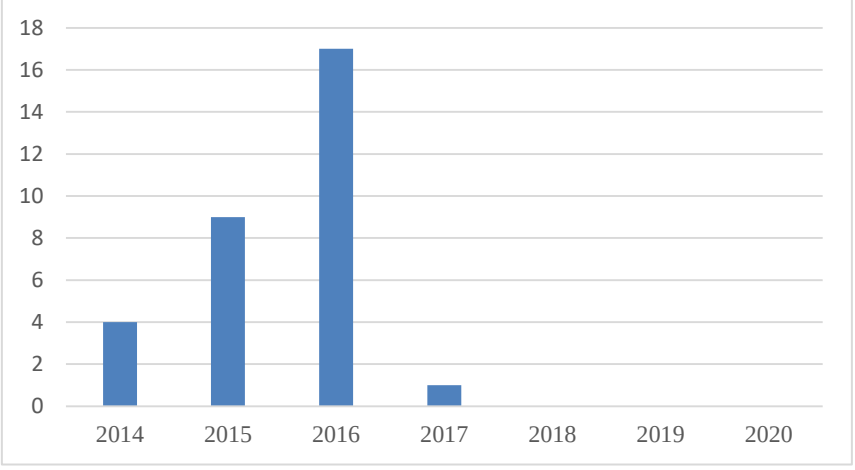
Nisan 2013'te Ebu Umar el-Bağdadi, Irak İslam Devleti'nin adını Irak ve Şam İslam Devleti (IŞİD) olarak değiştirmiştir (Mccants, 2015, s.36). Bu bağlamda örgüt, Arapça olarak DAEŞ 'ed Devlet'ul İslamiy el-Irak veş-Şam', İngilizce olarak da ISIS 'Islamic State of Iraq and al-Sham" şeklinde

ifade edilmektedir (Atun, 2016). Fakat bu isim değişikliği El-Kaide tarafından tanınmayınca aynı yıl ikili ilişkiler kesilmiştir. Örgüt, Haziran 2014'te Musul'u ele geçirdikten kısa bir süre sonra halifelik ilan ederek adını bir kez daha İslam Devleti (İD) olarak değiştirmiştir (Chaliand ve Blin, 2016, s.598). Ancak çok geçmeden uluslararası güçlerin DAEŞ'e karşı mücadeleyi desteklemesiyle örgüt topraklarının kontrolünü kaybetmeye başlamıştır.

DAEŞ tarihinin 2016'dan 2019'a kadar olan dördüncü dönemi ise örgütün Suriye ve Irak'taki bölgesel kontrolünü kaybetmesi, hilafetin yıkılması ve örgütün geleneksel terör taktiklerine geçişiyle devam etmiştir. Örgüt, gerçekleştirdiği eylemlerle 2016 yılında 9.150 kişinin ölümüne sebep olurken bu sayı 2017'de 4.350 ve 2018'de 1.328'e düşmüştür (McCarthy, 2019). Mart 2019'da ise sözde kurulan İslam Devleti halifeliğinin yıkılması ve lider Ebu Bekir el Bağdadi'nin öldürülmesinin ardından odak noktasını Kuzey Afrika'daki Cezayir, Mısır, Libya, Mali, Mozambik, Nijer ve Nijerya'daki bağlı kuruluşlarını ve destekçilerini kapsayacak şekilde genişlemeye doğru kaydırmıştır.

DAEŞ, aktif olduğu dönemlerde Brüksel, İstanbul, Londra, Nice, Orlando, Paris ve Sidney gibi dünyanın farklı yerlerinde terör saldırıları düzenleyen küresel bir terör örgütü olarak faaliyet göstermiştir. Bu bağlamda Küresel Terör Endeksine göre DAEŞ'in 2014-2020 yılları arasında Türkiye'de gerçekleştirdiği 31 saldırı ve 3 saldırı girişimi mevcuttur.

Şekil 1. DAEŞ'in 2014-2020 Yılları Arasında Türkiye'de Gerçekleştirdiği 31 Saldırının Yıllara Göre Analizi (Kaynak: Küresel Terör Endeksi, 2024).



Saldırılar 2016 yılında en yüksek noktaya ulaşmış ve bu kapsamda saldırıların 4 tanesi 2014, 9 tanesi 2015, 17 tanesi 2016 ve 1 tanesi 2017 yılında gerçekleştirilmiştir.2018-2020 yılları arasında saldırı kaydı bulunmamıştır. Saldırı girişimleri ise grafiğe dahil edilmemiştir. Bu bağlamda veriler, DAEŞ'in Türkiye'de gerçekleştirdiği saldırıların 2014-2016 yılları arasında tırmanışa geçtiğini, 2016 yılında zirveye ulaştığını ve 2017 itibarıyla keskin bir düşüş yaşadığını göstermektedir. 2016 yılı örgütün Suriye ve Irak'taki en güçlü olduğu dönemlerden biri olup Türkiye'yi doğrudan hedef alma kapasitesine sahip olduğu bir süreçtir. 2017 yılı itibarıyla ise Fırat Kalkanı Harekâtı, sınır güvenliğinin artırılması, istihbarat faaliyetlerinin güçlendirilmesi örgütün hem Suriye'de hem de Irak'ta büyük kayıplar yaşamasına ve kontrol ettiği toprakları büyük ölçüde kaybetmesine sebebiyet vermiştir. Bu durum örgütün Türkiye'de saldırı yapabilme kapasitesini doğrudan etkilemiştir.

Saldırı girişimlerinin ilki 6 Eylül 2017 tarihinde Mersin Yenişehir ilçesinde polis karakoluna yönelik bombalı eylem planıdır (Anadolu Ajansı, 2017). Terörist etkisiz hale getirilerek saldırı önlenebilmiştir. İkincisi 28 Ekim 2017 tarihinde Bayrampaşa'daki Forum İstanbul Alışveriş Merkezine yönelik planlanan bombalı eylem planıdır (Can ve Kaya, 2018). Üçüncüsü ise 23 Haziran 2017 tarihinde Türkiye'ye yönelik canlı bomba eylemi hazırlığında olan ve Suriye'den Türkiye'ye geçen 5 örgüt üyesinin operasyonla yakalanmasıdır (Milliyet, 2017).

Gerçekleştirilen 31 saldırının 13 tanesi sınır şehirlerine (Kilis, Gaziantep, Şanlıurfa) yönelik atılan roket saldırılarından oluşmaktadır (BBC, 2016; Aljazeera, 2016; Avrupa Raporu, 2020). 3 tanesi muhalif gazetecilere karşı gerçekleştirilen eylemlerden oluşmaktadır. Bu kapsamda 30 Ekim 2015 tarihinde Şanlıurfa'da 'Ayn Vatan' gazetesinin yazı işleri müdürü İbrahim Abdulkadir ile muhabiri Firaz Hamadi DAEŞ'in sözde dış istihbarat üyeleri tarafından öldürülmüştür (NTV, 2015). 27 Aralık 2015 tarihinde DAEŞ'e karşı yaptığı belgesellerle bilinen Suriyeli gazateci Naji Jerf öldürülmüştür (Arslan, 2016). Son olarak 12 Nisan 2016 tarihinde ise Suriyeli gazeteci Muhammed Zahir el Şerkat DAEŞ tarafından öldürülmüştür (BBC, 2016).

5 saldırı ise askeri personellere karşı gerçekleştirilen saldırılardan oluşmaktadır. Bu saldırıların ilki ve aynı zamanda DAEŞ'in Türkiye'deki ilk eylemi olarak değerlendirilen 20 Mart 2014 tarihli Niğde Ulukışla saldırısıdır (Kızılgül, 2020). Hatay'dan İstanbul'a gitmeyi hedefleyen 3 DAEŞ militanı Niğde/Eminlik uygulama noktasında jandarma görevlileri ile

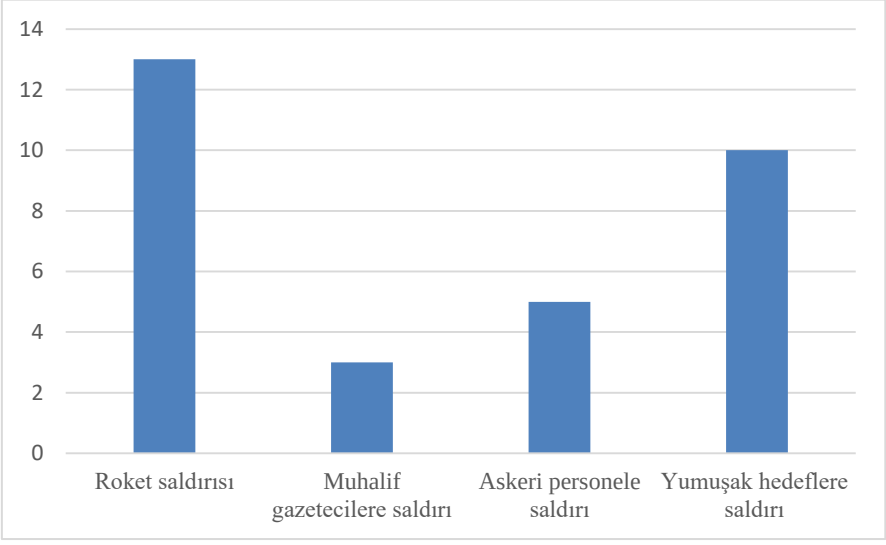
çatışmaya girmiş ve çıkan çatışmada 1 astsubay, 1 polis memuru şehit olmuş ve 1 sivil vatandaş hayatını kaybetmiştir (Bayraktar, 2014). İkinci saldırı 23 Temmuz 2015 tarihinde Kilis'in Elbeyli ilçesi Suriye sınırında görev yapan askerlere karşı DAEŞ'in kontrolündeki bölgeden ateş açılmasıdır (Anadolu Ajansı, 2015). Bu saldırı sonucunda 1 astsubay şehit olmuş ve 2 asker yaralanmıştır. Üçüncü saldırı 1 Eylül 2015 tarihinde Kilis'in sınır hattında bulunan Şehit Memet Hudut Karakolu'nda görevliyken devriye atan askerlere karşı DAEŞ'in kontrolündeki bölgeden ateş açılmasıdır (BBC, 2015). Dördüncü saldırı 6 Ocak 2015 tarihinde İstanbul Sultanahmet'de bulunan Turizm Şube Müdürlüğüne yönelik el bombaları kullanılarak gerçekleştirilen saldırı sonucunda 1 polis memurunun şehit olduğu ve 2 polis memurunun yaralandığı saldırıdır (BBC, 2015). Bu eylem DAEŞ terör örgütünün ülkemize yönelik gerçekleştirdiği ilk bombalı eylem olma özelliği taşımaktadır. Beşinci saldırı ise 1 Mayıs 2016 tarihinde Gaziantep İl Emniyet Müdürlüğüne yönelik araçlı bombalı saldırısıdır ve saldırı sonucunda 3 polis memuru şehit olmuştur (Avrupa Raporu, 2020).

10 saldırı ise yumuşak hedef saldırısı olarak ön plana çıkmaktadır. Bu saldırılar Küresel Terör Endeksinde yer alan hedef kategorilere bakılarak analiz edilmiştir. Bu kapsamda ulaşım merkezleri, eğitim kurumları, dini merkezler, sağlık merkezleri ve kültürel aktivite alanları saldırıları değerlendirilmiştir. Tarihsel olarak saldırılar aşağıdaki gibidir:

- 08.07.2014: İstanbul Esenyurt ilçesinde bir cami ateşe verilmiştir. Saldırıda can kaybı bildirilmemiş ancak caminin kütüphanesi hasar görmüştür (Habertürk, 2014).
- 18.05.2015: Adana Seyhan ilçesi ve Mersin illerinde bulunan Halkların Demokratik Partisi (HDP) il binalarına eş zamanlı olarak düzenlenen bombalı eylem sonucunda 4 kişi yaralanmıştır (Ercan, 2019).
- 05.06.2015: Diyarbakır'da HDP mitingine yönelik bombalı saldırı gerçekleştirilmiş ve saldırı sonucunda 4 kişi hayatını kaybederken 215 vatandaş yaralanmıştır (BBC, 2022).
- 20.07.2015: Şanlıurfa ilinin Suruç ilçesinde Amara kültür merkezi önünde bir intihar saldırısı gerçekleştirilmiş ve 31 kişi hayatını kaybetmiştir (BBC, 2015).
- 10.10.2015: Ankara tren garı önünde toplanan kalabalığa yönelik iki intihar saldırısı düzenlenmiş ve saldırı sonucunda 100 kişi hayatını kaybetmiştir (NTV, 2023).

- 12.01.2016: İstanbul Sultanahmet meydanı Alman çeşmesi ve Dikilitaş arasında kalan bölgede intihar saldırısı gerçekleştirilmiş ve saldırı sonucunda 12 Alman vatandaşı hayatını kaybederken 16 vatandaş da yaralanmıştır (Ercan, 2019). Bu eylem DAEŞ terör örgütünün ülkemizde turistlere yönelik gerçekleştirdiği ilk eylem olma özelliği taşımaktadır.
- 19.03.2016: İstanbul İstiklal caddesinde gerçekleştirilen intihar saldırısı sonucunda 4 kişi (3'ü İsrail, 1'i İran vatandaşı) hayatını kaybetmiş ve 1'i polis memuru olmak üzere 45 kişi yaralanmıştır (BBC, 2022).
- 28.06.2016: Üç intihar bombacısı, İstanbul Atatürk Havalimanı'nda patlayıcı yüklü yeleklerini patlatmadan önce etrafa ateş açarak gerçekleştirdikleri saldırıda 45 kişi hayatını kaybetmiştir (BBC, 2016).
- 20.08.2016: Gaziantep'te bir sokak düğününde intihar saldırıyla 51 kişi hayatını kaybetmiştir (Euronews, 2016).
- 01.01.2017: İstanbul'un Ortaköy semtindeki Reina Gece Kulübünde yeni yılı kutlayan sivillere yönelik gerçekleştirilen saldırıda 39 kişi ölmüştür (Sputnik, 2017).

Şekil 2. DAEŞ'in 2014-2020 Yılları Arasında Saldırdığı Hedef Türleri (Kaynak: Küresel Terör Endeksi, 2024).



Gerçekleştirilen eylemler incelendiğinde yumuşak hedef saldırıları tüm saldırıların %32,2'sine denk gelmektedir. Bu bağlamda verilerin analizi, DAEŞ'in Türkiye'de uyguladığı saldırı stratejisinin çok boyutlu olduğunu göstermektedir. Sınır illerine yönelik roket saldırıları, örgütün Suriye ve

Irak'taki varlığının Türkiye'ye yansıyan etkilerini ve örgütün Türkiye ile olan jeopolitik gerilimini gösterirken askeri personel ve muhalif gazetecilere yönelik suikastlar, örgütün güvenlik birimlerini ve fikirsel karşıtlarını doğrudan hedef aldığını ve güvenlik güçlerini yıpratma stratejisini ortaya koymaktadır. Ancak en dikkat çekici unsurlardan biri örgütün aktif olduğu yıllar içinde 10 farklı noktada yumuşak hedeflere saldırmasıdır. Bu saldırılar doğrudan sivilleri hedef aldığı için terörün temel amacı olan maksimum korku ve kaos yaratma gayesini taşımaktadır. Bu bağlamda yumuşak hedef saldırılarının seçilmesinde saldırının psikolojik etkisinin yüksek olması etkili olmuştur.

DAEŞ'in 2014-2020 yılları arasında Türkiye'de gerçekleştirmiş olduğu saldırılar incelendiğinde görülmektedir ki örgütün yumuşak hedeflere olan saldırı eğilimi azımsanamayacak kadar fazladır. Örgüt kalabalık yerleri tekrar tekrar hedef almış ve bu saldırılar ölüm sayısında da ciddi bir sayıya yol açmıştır. Bu bağlamda örgüt yumuşak hedeflere saldırma stratejisiyle varlığını gösterme, dünya genelinde korku yaratma ve medya üzerinden mesajlarını ileterek destek toplama çabası içine girmektedir. Bu amaçla da ağırlıklı olarak alışveriş merkezlerinde, çarşılarda, düğünlerde, kültür merkezlerinde ve okullarda eylem gerçekleştirme yoluyla yumuşak hedeflere saldırmıştır.

SONUÇ

Çalışmanın birinci başlığında terör örgütlerinin büyükşehirlerde eylem gerçekleştirmesinin ve şehir eylem stratejisinin sebepleri incelenmiştir. İnceleme sonucunda şehirlerin genellikle yoğun nüfuslu, medya odaklı ve stratejik öneme sahip hedefleri barındıran yerler olmasından dolayı terör örgütlerinin eylemlerini şehirlerde gerçekleştirerek daha fazla dikkat çekmeyi ve medyada daha geniş bir şekilde yer bulmayı hedefledikleri ve kendi ideolojilerini veya taleplerini daha geniş bir kitleye duyurabilmeyi amaçladıkları sonucuna ulaşılmıştır. Bu bağlamda DAEŞ'in 2014-2020 yılları arasında Türkiye'de gerçekleştirdiği eylemler şehir merkezlerinde gerçekleşmiş ve örgüt, şehir içi terör eylemlerini sistematik bir şekilde kullanmıştır. DAEŞ'in kırsal alanlardan ziyade şehirlerde eylem yapmayı tercih etmesinin nedeni daha büyük psikolojik ve siyasi etki yaratma amacına dayanmaktadır. Bu kapsamda örgüt şehirdeki eylemleri ile daha fazla korku yayarak toplumda panik oluşturmayı, medya yoluyla küresel

çapta propaganda yapmayı, güvenlik güçlerini yıpratmayı ve şehir yapılanmaları sayesinde operasyonel esneklik sağlamayı hedeflemiştir.

Çalışmanın ikinci başlığında yumuşak hedef kavramı incelenmiştir. Bu bağlamda yumuşak hedefler, genellikle askeri tesisler veya devlet kurumları gibi daha güçlü savunma sistemlerine sahip olmayan, korumasız veya daha açık hedefleri ifade etmektedir. Alışveriş merkezleri, okullar, toplu taşıma araçları, konser alanları, ibadet yerleri gibi sivil alanların da yumuşak hedef olarak kabul edilen hedefler olduğu sonucuna ulaşılmıştır.

Çalışmanın üçüncü başlığında ise DAEŞ terör örgütünün 2014-2020 yılları arasında Türkiye'de gerçekleştirmiş olduğu saldırılar GTD üzerinden incelenmiştir. Bu incelemede toplam 31 saldırı ve 3 saldırı girişiminin olduğu ve bu saldırıların 10 tanesinin yumuşak hedeflere yönelik olarak gerçekleştirildiği görülmüştür. Yüzdelik olarak incelendiğinde de 6 yıllık zaman diliminde Türkiye'de gerçekleştirilen tüm saldırıların %32,2'sinin yumuşak hedef saldırısı olduğu sonucuna ulaşılmıştır.

Mevcut durum ve son dönemde yaşanan olayların analizinden de anlaşılacağı üzere terör saldırıları son yıllarda daha fazla yumuşak hedeflere odaklanmıştır. Bu noktada potansiyel yumuşak hedeflerin çok çeşitli olması nedeniyle diğer saldırıların nerede ve ne zaman gerçekleştirileceğini belirlemek oldukça zordur. Fakat gelecekteki saldırı tehdidi hala yüksek olduğu için kayda değer önlemlerin alınması zorunludur. Bu noktada hükümet binaları gibi sembolik veya yüksek değerli hedeflerin aksine yumuşak hedefleri gerçek anlamda güçlendirmenin net bir yolu yoktur. Parklar eğlence amaçlı, kolay erişimli ve hareket imkânı sağlayacak şekilde tasarlanmıştır. Toplu taşımalar, insanları verimli bir şekilde taşımak için tasarlanmıştır. Ağır güvenlik önlemlerinin uygulanması durumunda her ikisi de tasarlanmış işlevlerini yerine getirmeyi bırakacaktır. Ayrıca yumuşak bir hedefin çevresine güvenlik eklemek saldırı bölgesini basitçe değiştirecektir. Bu nedenle yapılabilecek en temel ve kritik birinci şey çalışanlara terör saldırılarına karşı farkındalık ve eğitim sağlamaktır. Özellikle güvenlik personeli ve halka açık yerlerde çalışan personel şüpheli durumları tanıma, raporlama ve güvenlik prosedürlerini uygulama konularında eğitilmelidir. Çünkü güvenlik görevlileri, en basit şekliyle saldırı öncesinde muhakkak yapılan gözetleme/keşif yönüne dikkat ederek gelecekteki bir saldırıyı tespit edip önüne geçebilir.

Gözetleme/keşif aşaması hedefin profilini çıkarmak, en uygun saldırı yaklaşımını belirlemek ve saldırı için en uygun zamanı belirlemek amacıyla gerçekleştirilir. Bu bağlamda teröristler, bir saldırı başlatmadan önce hedefi birkaç kez ziyaret ederler. Bu nedenle personeller ve güvenlik görevlileri, yaklaşan bir saldırının habercisi olabilecek şüpheli davranışları tespit etme konusunda dikkatli davranarak önemli bir rol oynayabilir. Bu noktada örneğin aynı bölgeye veya konuma gün içinde birden fazla kez park edilmiş herhangi bir arabanın bilincinde olmak, güvenlik kameralarından kaçınma çabalarına şüpheyle yaklaşmak, çıkış ve giriş noktalarına, yoğun günlere, çalışma saatlerine, güvenlik görevlilerine ve diğer çalışanlara alışılmadık bir ilgi konusunda tetikte olmak, personel arasında güvenlik bilincini arttırmak ve şüpheli faaliyetlerin bildirilmesini teşvik etmek gibi önlemler alınabilecek en temel önlemlerdir.

İkinci olarak yapılabilecek önemli şey ise yumuşak hedeflerin iyi aydınlatılmış olmasıdır. Teröristlerin kamufle olamayacakları bir yerde saldırı öncesi gözetleme/keşif yapması ve saldırı sonrası kaçması oldukça zordur. Bu noktada aydınlatma, potansiyel saldırıları önlemede ve güvenlik personelinin daha etkili bir şekilde gözlem yapmasına yardımcı olabilir.

Üçüncü olarak hükümet yetkilileri, güvenlik güçleri ve özel sektör kuruluşları arasında etkili bir istihbarat paylaşımı ve iş birliği potansiyel tehditlere karşı daha hızlı ve etkili bir tepki sağlayabilir. Bu nedenle elde edilen her istihbarat kaynaklı bilginin önemli olarak değerlendirilmesi ve bilmesi gereken prensibi kapsamında paylaşılması gerekmektedir.

Dördüncü olarak da işletmelerin veya kuruluşun bulunduğu bölgedeki güvenlik risklerini değerlendirmek önemlidir. Bu değerlendirme, potansiyel tehditleri ve güvenlik zayıflıklarını belirlemekte yardımcı olacaktır. Bu kapsamda güvenlik kameraları, alarm sistemleri, kapı kontrolleri, bariyerler vb. güvenlik önlemleri gibi fiziksel önlemler de alınabilir.

Bu noktada güvenlik önlemleri bir bütün olarak ele alınmalı ve sürekli olarak gözden geçirilmelidir. Yumuşak hedeflere yönelik terör saldırılarından korunmanın başarılı çözüm koşulları, bilgi ve beceri edinerek kritik kriz durumlarını yönetmeye yönelik teknik ve teknolojik hazırlığa hâkim olarak yaratılabilir.

KAYNAKÇA

Aljazeera. (2 Mayıs 2016). *Kilis'e yeni saldırı: 1 ölü, 3 yaralı.*

Anadolu Ajansı. (23 Temmuz 2015). *Suriye Tarafından Askere Ateş Açıldı: 1 Şehit, 2 Yaralı.*

Anadolu Ajansı. (6 Eylül 2017). *Mersin'de Bombalı Saldırı Girişimi Önlendi.*

Arslan, R. (12 Ocak 2016), *Öldürülen Suriyeli gazetecinin hikayesi: Naji Jerf.* Erişim Tarihi: 11 Kasım 2024. https://www.bbc.com/turkce/haberler/2016/01/160111_naji_jerf_profile_arslan#:~:text=38%20ya%C5%9F%C4%B1nda%20%C3%B6ld%C3%BCr%C3%BClen%20gazeteci%20Naji,s%C4%B1rada%20susturuculu%20silah%20ile%20%C3%B6ld%C3%BCr%C3%BCld%C3%BC.

Atun, A. (21 Ekim 2016). *DAEŞ Yolun Sonuna Geliyor*. Erişim Tarihi: 11 Kasım 2024. https://tasam.org/Files/Icerik/File/DAES_Yolun_Sonuna_Geliyorr_pdf_a30698a3-1f54-42c6-85fa-ee26ccbcc4c4.pdf

Avrupa Raporu. (29 Haziran 2020). *IŞİD'e Katılıp Dönen Türkiye Vatandaşları: Mevcut Yaklaşımları Geliştirmek.* ERİŞİM tarihi: 11 Kasım 2024. https://www.crisisgroup.org/sites/default/files/258-calibrating-the-response-turkish.pdf

Bauman Z. (2004). Living (Occasionally Dying) Together In An Urban World, S. Graham (Ed.), *Cities, War, And Terrorism: Towards An Urban Geopolitics* içinde (s.115-116). Blackwell Publishing.

Bayraktar, B. (20 Mart 2014), *Niğde'de Terörist Saldırı.* Erişim Tarihi: 11 Kasım 2024. https://tr.euronews.com/2014/03/20/askere-saldiri-uc-sehit

BBC. *(1 Eylül 2015). Kilis'e Suriye'den ateş: Bir asker hayatını kaybetti.*

BBC. (12 Nisan 2016). *Gaziantep'te vurulan Suriyeli gazeteci öldü.*

BBC. (14 Kasım 2022). *Türkiye'de Son Yıllarda Düzenlenen Büyük Saldırılar.*

BBC. (18 Nisan 2016). *IŞİD bölgesinden Kilis'e roket: 4 ölü.*

BBC. (20 Temmuz 2015). *Suruç'ta Katliam: 31 ölü, 104 Yaralı*.

BBC. (29 Haziran 2016). *Atatürk Havalimanı saldırısı: Tam olarak ne oldu?*

BBC. (6 Ocak 2015). *Sultanahmet'te İntihar Saldırısı: 1 Polis Öldü.*

Benova P. Hoskova-Mayerova S. ve Navratil J. (2019). Terorıst Attacks On Selected Soft Targets. *Journal of Security ve Sustainability Issues,* 8(3): 453-471.

Byman, D. L. (2003). Al-Qaeda As An Adversary Do We Understand Our Enemy? *World Politics*, 56(1): 139-163.

Can, M. E. ve Kaya, M. (13 Mart 2018), *DEAŞ'ın AVM'ye bombalı saldırı girişimine iddianame*. Erişim Tarihi: 11 Kasım 2024. https://www.aa.com.tr/tr/turkiye/deasin-avmye-bombali-saldiri-girisimine-iddianame/1087208

Chaliand, G. ve Blin, A. (2016). *The History Of Terrorism: From Antiquity To ISIS*. University of California Press.

Cuesta, A. vd. (2019). A New Approach To Protect Soft-Targets From Terrorist Attacks, *Safety Science*, 120: 877-885.

Çardak, B. (2022). Terör Örgütlerinin Hedef Seçimlerindeki Değişim: Yumuşak Hedeflere Kavramsal Perspektiften Bakış, *International Journal of Eurasia Social Sciences/Uluslararası Avrasya Sosyal Bilimler Dergisi*, 13(48): 753-768.

Doğaner, M. ve Yoldaş, Y. (2023). DEAŞ Terör Örgütünün Dini İdeolojik Alt Yapısı ve Örgütsel Üyelik Stratejileri, *Türkiye Siyaset Bilimi Dergisi*, 6(1): 48-64.

Ercan, R. (11 Ekim 2019), *DEAŞ'ın Hedef Aldığı Türkiye'den Örgüte Büyük Darbe*. Erişim Tarihi: 11 Kasım 2024. https://www.aa.com.tr/tr/turkiye/deasin-hedef-aldigi-turkiyeden-orgute-buyuk-darbe/1609884#

Euronews. (21 Ağustos 2016). *Terör Gaziantep'te Bir Düğünü Kana Buladı*.

Fagel, M. ve Hesterman, J. (2016). *Soft Targets and Crisis Management: What Emergency Planners and Security Professionals Need to Know?* Routledge.

Habertürk. (9 Temmuz 2014). *İstanbul Esenyurt'taki Camiye İkinci Kez Saldırı Düzenlendi.*

Hashim, A. S. (2014). The Islamic State: From al-Qaeda Affiliate to Caliphate, *Middle East Policy*, 21(4): 69-83.

Hesterman, J. (2018). *Soft Target Hardening: Protecting People From Attack*. Routledge.

Hoffman, B. (2006). *Inside Terrorism*. Columbia University Press.

Kızılgül, P. B. (2020). Balkanlarda Yabancı Terörist Savaşçılar. *Güvenlik Bilimleri Dergisi*, *9*(1): 101-124.

Killcullen, D. (2013). *Out Of The Mountains: The Coming Age Of The Urban Guerrilla*. Oxford University Press.

King, A. (2021). *Urban Warfare In The Twenty-First Century*. Polity Press.

Kiras, J.D. (2007). Irregular Warfare: Terrorism and Insurgency, J. Baylis, J. J. Wirtz ve C. S. Gray (Ed.), *Strategy In The Contemporary World: An Introduction To Strategic Studies* içinde (ss.185-207). Oxford University Press.

Kurum, M. (2023). Teori ve Pratikte Terörist Örgütlerin Şehir Eylem Yönelimleri ve Stratejileri, *SAVSAD Savunma ve Savaş Araştırmaları Dergisi*, 33(1): 101-144.

Laquer, W. (2001). *A History Of Terrorism*, Transactions Publishers.

Marighella, C. (2003). *Şehir Gerillasının El Kitabı.* Eriş Yayınları.

Martin, R. (2016). Soft Targets Are Easy Terror Targets: Increased Frequency Of Attacks, Practical Preparation, And Prevention. *Forensic Research Criminology International Journal*, 3(2): 273-278.

McCants, W. (2015). *The ISIS Apocalypse: The History, Strategy, And Doomsday Vision Of The Islamic State*, St. Martin's Press.

McCarthy, N. (10 Aralık 2019). *The Rise And Fall Of ISIS*. Erişim Tarihi: 20 Kasım 2024. https://www.statista.com/chart/20255/the-rise-and-fall-of-isis/

Milliyet. (24 Haziran 2017). *Son dakika: Hatay'da 5 canlı bomba yakalandı.*

NTV. (10 Ekim 2023). *Ankara gar saldırısının üzerinden 8 yıl geçti*.

NTV. (11 Şubat 2015). *IŞİD Şanlıurfa'daki Gazeteci Cinayetlerini Üstlendi.*

O'Neill, B. (2005). *Insurgency And Terrorism: From Revolution To Apocalypse,* Potomac Book.

Pinos, J. C. ve Steven, M. R. (2020). The Territorial Contours Of Terrorism: A Conceptual Model Of Territory For Non-State Violence. *Terrorism And Political Violence*, 32(5): 1027-1046.

Sandler, T. (2014). The Analytical Study Of Terrorism: Taking Stock. *Journal of Peace Research*, 51(2): 257-271.

Santifort, C. Sandler, T. ve Brandt, P. T. (2013). Terrorist Attack And Target Diversity: Changepoints And Their Drivers. *Journal Of Peace Research*, 50(1): 75-90.

Schmid A. (2021). Layers Of Preventive Measures For Soft Target Protection Against Terrorist Attacks, A.P. Schmid (Ed.), *Handbook Of Terrorısm Preventıon And Preparedness* içinde (ss.816-841). ICCT Press Publication.

Sevinç, B. ve Çiftçi, İ. (2015). *Terör ve Şiddet Sarmalında Orta Doğu ve Afrika*, Karınca Yayınları.

Sputnik. (7 Ocak 2017). *Reina saldırısını IŞİD'in Özbek hücresi planladı*.

Taw, J. ve Hoffman, B. (2007). The Urbanisation Of İnsurgency: The Potential Challenge To US Army Operations. *Small Wars and Insurgencies*, 6(1): 68-87.

Ünsal, Z. E. ve Olçar, K. (2019). Avrupa'da Radikalleşme ve DAEŞ: DAEŞ'in Evrilmesi ve Avrupa Güvenliğine Yönelik Tehditler. *Güvenlik Stratejileri Dergisi*, 15(29): 115-150.

Valiyev, A. (2007). *Urban Terrorism: Do Terrorists Target Cities And Why*. (Doktora Tezi). University of Louisville, ABD.

Williams, J. W. (2008). Carlos Marighela: The Father Of Urban Guerrilla Warfare, *Studies in Conflict and Terrorism*, 12(1): 1-20.

Zeman, T. (2020). Soft Targets: Definition And Identification. *Academic and Applied Research In Military and Public Management Science*, 19(1): 109-119.

Terörizm ve Radikalleşme Araştırmaları Dergisi-TRAD, 2025, 4(2) : 186-222 Araştırma Makalesi
Journal of Terrorism and Radicalization Studies-TRAD, 2025, 4(2): 186-222 Research Article
DOI: 10.61314/traddergi.1673740

TERÖRİZM VE RADİKALLEŞMEDE PSİKOLOJİK VE SOSYOLOJİK FAKTÖRLER: EL-KAİDE ÖRNEĞİ

Büşra BEYOĞLU[*]

ÖZET

İnsanları terör örgütü mensubu olmaya ve şiddetle radikalleşmeye iten ve çeken birçok psikolojik ve sosyolojik temelli neden bulunmaktadır. İhtiyaçlar hiyerarşisi teorisini oluşturan Maslow (1943), fizyolojik, güvenlik, sevgi ve ait olma, saygınlık, bilişsel, estetik, kendini gerçekleştirme ve kendini aşma ihtiyaçlarının; insanları bu ihtiyaçları karşılayacak yöntemler aramasını motive eden bireysel ve psikolojik etmenler olduğunu belirtmektedir. Bunlar dışında, 3N yaklaşımını oluşturan Webber ve Kruglanski (2017), anlatıların ve grup dinamiklerinin terörizm süreçlerine etki eden sosyolojik faktörler olduğunu ifade etmektedirler. Bu iki teoriyi kullanarak El-Kaide terör örgütünün yayınlanmış mektupları üzerinden söylem analizi yöntemiyle incelenen psikolojik ve sosyolojik dinamikler neticesinde, insanların kendi temel ihtiyaçlarını karşılama, hem fiziksel hem de psikolojik olarak güvende hissetme, aile ve aitlik ihtiyacı, önem kazanma motivasyonu, düşüncelerinin uyumu için olayları yorumlama ve anlamlandırma ihtiyacı, güzellik ve doğallık arayışı, kimlik arayışı ve aşkınlığa ulaşma ihtiyacı gibi psikolojik süreçlerin örgüte katılım ve şiddet yoluyla radikalleşme üzerinde etkili olduğu görülmüştür. Ayrıca sosyolojik perspektiften incelendiğinde ise seçilmiş travmalar ve zaferler, dini kitaptan alıntılama ve insanlıktan çıkarma gibi şiddeti meşrulaştıran anlatıların yanı sıra örgütün sistematik yapısı, fikir birliğinin sağlanması ve grup kimliği ile bütünleşme faktörlerinin terörizm olgusunda etkili olduğu tespit edilmiştir.

Anahtar Kelimeler: *El-Kaide, Terörizm, Radikalleşme, İhtiyaçlar Hiyerarşisi, 3N Yaklaşımı*

PSYCHOLOGICAL AND SOCIOLOGICAL FACTORS IN TERRORISM AND RADICALIZATION: THE EXAMPLE OF AL-QAEDA

ABSTRACT

There are many psychological and sociological reasons that push and pull people to become members of terrorist organizations and radicalized through violence. Maslow (1943), who created the theory of the hierarchy of needs, states that physiological, security, love and belonging, esteem, cognitive, aesthetic, self-actualization and self-transcendence needs are individual and psychological factors that motivate people to seek methods to satisfy these needs. Apart from these, Webber and Kruglanski (2017), who created 3N approach, state that narratives and group dynamics are sociological factors that affect terrorism processes. As a result of the psychological and sociological dynamics examined by using the discourse analysis method on the published letters of the Al-Qaeda terrorist organization using these two theories, it has been seen that psychological processes such as meeting people's basic needs, feeling safe both physically and psychologically, the need for family and belonging, the motivation to gain importance, the need to interpret and make sense of events in order to harmonize their thoughts, the search for beauty and naturalness, the search for identity and the need to reach transcendence are effective in attending the organization and radicalization through violence. Moreover, when examined from a sociological perspective, it has been determined that the factors that legitimize violence, such as selected traumas and victories, quoting from religious books and dehumanization, as well as the systematic structure of the organization, ensuring consensus and integrating with group identity, are effective in the phenomenon of terrorism.

Keywords: *Al-Qaeda, Terrorism, Radicalization, Hierarchy of Needs, 3N Approach*

[*] Yüksek Lisans Öğrencisi, Milli İstihbarat Akademisi, İstihbarat Çalışmaları Ana Bilim Dalı, busrabeyoglu34@gmail.com, ORCID: 0009-0007-8921-4492

GİRİŞ

Terörizm, özellikle 11 Eylül saldırılarıyla beraber önemi artan araştırma konularından birisi olmuştur. Şiddet yöntemlerini kullanarak birçok insanın sürekli korku halinde yaşamasına, yaralanmasına ve ölmesine sebep olan terör örgütü üyelerini bunu yapmaya iten ve çeken siyasi, psikolojik, sosyolojik ve diğer birçok farklı neden de bu araştırma konularından birisidir. Bu doğrultuda, 11 Eylül terör saldırılarını düzenleyerek uluslararası düzeyde terörizm, radikalleşme ve bunlarla mücadele hususunda çalışmaların hız kazanmasında rolü olan El-Kaide terör örgütü, akademik alanda da farklı araştırmalara konu olan bir örgüt olmaya devam etmektedir.

El-Kaide terör örgütü, 1979 yılında Sovyetler Birliği'nin Afganistan'ı işgali neticesinde Afganistan'ı işgalden kurtarmak için toplanmaya başlayıp 1988 yılında Usame bin Ladin'in liderliğinde kurulmuştur. 1989'da Sovyetler Birliği'nin çekilmesi ile yönünü baş düşmanı olarak gördüğü ABD'ye çeviren örgüt, 1991 yılında Körfez Savaşı gerekçesiyle ABD askerlerinin Suudi Arabistan'a konuşlanması ile şiddet eylemlerini arttırmaya başlamıştır. Cihat anlayışı ile hareket eden örgütün amacı İslam'ın düşmanları olarak tanımladığı devletlere karşı mücadele ederek geniş bir coğrafyada Sünni şeriat kuralları ile yönetilen bir İslam devleti kurmaktır. 11 Eylül saldırıları ile küresel tanınırlık elde eden örgüt, Bin Ladin'in 2011 yılında ABD tarafından Pakistan'da yerleşkesinde öldürülmesine kadar dünyanın birçok yerinde şiddet eylemlerinde bulunmuştur. Bin Ladin'in öldürülmesi sonrası yerine geçen yardımcısı Eymen ez-Zevahiri için Bin Ladin'in aksine liderlik etkisinin güçlü olmadığı söylenmektedir (Thomas, 2024). 2022'de Zevahiri'nin öldürüldüğü duyurulmuştur. Bu tarihlerden sonra örgütün faaliyetleri kademeli olarak azalsa da geçmişteki eylemleri güncelliğini sürdürmektedir. Örgüte katılım ve şiddet yoluyla radikalleşme davranışları hakkında yapılan araştırmalar ile literatürde de tartışılmaya devam etmektedir.

Davranışlar söz konusu olduğunda hem motivasyonlar hem de kültürel ve durumsal faktörlerin etkili olduğu belirtilmektedir (Maslow, 1943, s. 371). Bu yüzden, eylemler ve davranışlar ile bir bütünlük oluşturan terörizm olgusundaki şiddetle radikalleşme gibi süreç içeren konularda araştırmalar yapılırken motivasyonlara ek olarak kültürel ve grup odaklı kavramlar da bu süreçleri anlamlandırmada etkilidir. Bu süreçlerdeki bireysel motivasyonları anlamlandırabilmek için Maslow (1943)'un "ihtiyaçlar hiyerarşisi" ve sadece

bireysel ihtiyaçlara değil aynı zamanda kültürel unsurların ve grup dinamiklerinin terörizm sürecinde etkili olduğunu ifade eden ve Webber ve Kruglanski (2017) tarafından ortaya konulan "3N" yaklaşımı birbirlerini tamamlamaktadır. Dolayısıyla bu araştırmada, mikro (bireysel) düzeyden mezo (grup/sosyal) düzeye doğru bir anlatım yapılmıştır. Bunun için "terörizm ve radikaleşmede etkili olan psikolojik ve sosyolojik dinamikler nelerdir?" sorusu, 3N yaklaşımındaki bireysel motivasyon kısmı ve Maslow'un ihtiyaçlar hiyerarşisindeki psikoloji odaklı kavramlarla beraber yine 3N yaklaşımındaki sosyolojik süreçler üzerinden Bin Ladin'in öldürülmesi sonrası yerleşkesinde ele geçirilmiş olan; 2015 ve 2016 yıllarında Ulusal İstihbarat Direktörü Ofisi'nin internet sitesinde gizliliği kaldırılmış örgüte ait 196 mektup (Office of the Director of National Intelligence, 2015; 2016) üzerinden söylem analizi yöntemi ile incelenip tartışılmıştır. Bu mektuplara ek olarak, içerisinde El-Kaide ile ilgili Youtube'da yer alan üç röportaj da incelenmiştir. Literatürde, bu iki teorinin bütünleşmesi ile El-Kaide terör örgütü incelenmemiştir. Bu yüzden de literatür boşluğunun giderilebilmesi için bu araştırma yapılmıştır.

1. TERÖRİZM VE RADİKALLEŞME OLGULARININ PSİKO-SOSYAL YAKLAŞIMLAR ÜZERİNDEN İNCELENMESİ

Bu kısımda, literatürde yer alan terörizm ve radikalleşme olgularına farklı yaklaşımlar, bu yaklaşımlar içerisinde yer alan psiko-sosyal yaklaşımlar ve psiko-sosyal bakış açısıyla terör örgütleri üzerine yazılmış vaka çalışmaları içeren araştırmalara yer verilmiştir.

Terörizm kavramı için literatürde çeşitli tanımlar bulunmaktadır. Schmidt ve Jongman (1988), 109 tanımın kelime frekans analizini yapmıştır. Bu analize göre en çok kullanılan ilk 10 kavram "şiddet/güç", "siyasi", "terör/korku", "tehdit", "psikolojik", "kurban", "sistematik", "taktik", "insani sınırı olmayan" ve "baskı/zorlama"dır (ss. 5-6). Aynı zamanda terörizm kısaca "terörün sistematik bir şekilde örgütlü bir yapı tarafından kullanımı" (Önenli Güven, 2022, s. 132) olarak da ifade edilmektedir. Radikalleşme kavramı için ise "şiddetin bir ideoloji etrafında meşrulaştırılarak süreklileştirilmesi" (Önenli Güven, 2022, s. 132) şeklinde terörizmi biçimlendiren bir olgu olduğu yönünde literatürde tanımlamalar bulunmaktadır. Borum (2011) ise, radikalleşme ve terörizm kavramlarını birbirinden ayrı tutarak radikalleşmeyi "aşırı ideolojilerin ve inançların geliştirilmesi süreci" (s. 9) yani "ideolojilerin benimsenmesini" içeren bir

"süreç" olarak tanımlarken "eylem yolları (*action pathways*)" kavramını "terörizme veya şiddet içeren aşırılıkçı eylemlere katılma süreci" (Borum, 2011a, s. 9) şeklinde ifade etmiştir. Dolayısıyla her radikalleşme sürecinin terörizmle sonuçlanmayacağı ve şiddet eyleminin terörizmdeki radikalleşme olgusunu diğer radikalleşme türlerinden ayıran özelliklerden birisi olduğu belirtilmektedir. Bu noktada "şiddetli radikalleşme" kavramı öne çıkmaktadır. Schmid (2013), "şiddetli radikalleşme (*violent radicalisation*)" teriminin "şiddetle radikalleşme (*radicalisation by violence*)" kavramı ile karıştırıldığını ve bu terimin "şiddete giden radikalleşme (*radicalisation to violence*)" anlamına gelecek şekilde kullanıldığını belirtmiştir (s. 1). Öte yandan şiddetli radikalleşme kavramı için "doğası gereği somut şiddeti kapsayan davranışları içeren yol" şeklinde "eylem/davranış" odaklı tanımlamalar bulunurken "şiddeti onaylayan veya meşrulaştıran belirli fikirlerin kabulü" olarak "düşüncede" benimsenen bir süreç olarak da ifade edilmektedir. (European Commission's Expert Group on Violent Radicalisation, 2008, s. 5). Dolayısıyla, terörizm olgusundaki şiddet içeren radikalleşme süreci için hem düşüncede benimsenen hem de davranışlar ile somutluk kazanan "terörist kimliğinin" oluşum sürecini ifade etmektedir.

Terörizmde radikalleşme sürecini anlatan modeller literatürde bulunmaktadır. Borum'un (2011b) dört aşamalı "terörist zihniyetin oluşma süreci" olarak tanımladığı modelinde; kişinin doğru olmadığını düşündüğü bir durum hakkında "şikâyet" etmesi, bu durumu "adaletsizlik" olarak tanımlaması, bir "hedefi" suçlaması ve son olarak da suçladığı hedefi ötekileştirerek "değersizleştirmesi" şeklinde aşamalar ifade edilmiştir (s. 35). Moghaddam (2005) ise "terörizmin merdiven modeli" olarak radikalleşme sürecini açıklamıştır. Bunun için "maddi koşulların psikolojik yorumu" yani bir durumun adaletsizlik olarak yorumlanması, bu adaletsizlik için "algılanan seçenekler", bu seçeneklerin işe yaramadığı düşüncesi neticesinde yaşanan hayal kırıklığı ve öfkenin "bir hedefe yansıtılması", algılanan adaletsizlik için mücadeleyi meşrulaştırmak için kişinin "kendisini ve eylemlerini haklı görmesi", kategorik düşünmenin sağlamlaşması ("biz" olarak belirtilen "kendi grubu" ve "onlar" şeklinde tanımlanan "düşmanlar" ayrımı) ve son aşamada başkalarına zarar vermeyi "engelleyici içsel mekanizmaların devre dışı bırakılması" şeklinde ifade edilmiştir (Moghaddam, 2005, ss. 162-166). Bu iki modelde de ortak olan adımlar; bir durumun kişinin zihinsel mekanizmaları tarafından anlamlandırılması (haksızlık olarak yorumlama), bunun sonucunda duyguların oluşumu (hayal kırıklığı, öfke), bu duyguların

dışsallaştırılması (hem adaletsizliğin gerçek sorumlusu olarak görülen hem de bu sorumlu ile bağlantılı olarak "atfedilen" diğer hedeflere olumsuz duyguların yansıtılması) ve hedeflere yönelik düşüncelerin ve davranışların meşrulaştırılması için yöntemler kullanılması (ötekileştirme gibi) şeklinde sıralanabilir.

Terörizmin nedenleri konusunda literatürde farklı yaklaşımlar vardır. Schmid (2013), bu nedenleri mikro (bireysel faktörler), mezo (sosyal çevrenin etkisi/grup bazlı süreçler) ve makro (hükümet ve toplumla ilişkiler) bakımından kategorilere ayırmıştır (s. 4). Ross (1993) ise literatürdeki çalışmaların yapısal nedenler (sosyal/siyasi/kültürel/ekonomik yapıda bulunan nedenler), psikolojik durumlar (örgüte katılım nedenleri, örgüt üyelerinin terör eylemlerindeki etkisi) ve rasyonel seçim (maliyet-fayda hesaplamalarının sonucu olarak terör örgütlerine katılım) olmak üzere üç kategoride incelendiğini ifade etmiştir (s. 317). Ayrıca literatürde terörizme iten ve çeken nedenler bakımından da araştırmalar mevcuttur. Terörizme "iten nedenler" olarak kimlik sorunları, adaletsizlik duygusu ve hayal kırıklığı gibi psiko-sosyal faktörlerin yanında sosyal, siyasi ve ekonomik durumlar gibi çevresel faktörler de itici güç olabilmektedir (European Commission, 2024, s. 8). Öte yandan "çeken nedenler" ise örgütün ideolojisi ve yapısı gibi örgütün bireye sunabileceği faktörler olarak belirtilmektedir (Al-Attar, 2019, s. 6). Aynı zamanda Ross (1993) terörizme "izin veren sebepler" ve "tetikleyici sebepler" olarak yapısal nedenleri gruplandırmıştır. Makalede terörizme izin veren nedenler; coğrafi konum (şehir ortamlarında lojistik ve insan kaynağı ulaşımının kolaylığı), siyasi sistem türü (demokrasilerde ve ulusal/etnik çatışmaların olduğu sistemlerde) ve modernleşme düzeyi (teknoloji/iletişim gibi kolaylaştırıcı faktörler) olarak gruplandırılmıştır (Ross, 1993, ss. 320-322). Tetikleyici sebepler ise sosyal/kültürel/tarihsel kolaylaştırıcılar (ortak inançlar ve gelenekler), örgütsel ayrılma ve gelişme (mevcut örgütlerin bölünmesi ile yeni çıkan örgütler arası rekabet), diğer siyasi huzursuzluk biçimleri (protestolar, isyanlar, savaş), destek (devletlerden, kurumlardan, kişilerden), terörle mücadele kurumlarının başarısızlığı (kolluk kuvvetleri, askeri birimler, istihbarat servislerinin yetersizliği), silah ve patlayıcıların mevcudiyete (bunlara kolay erişim sağlanabilmesi) ve şikayetler (gerçek ya da algılanan aşağılama/ayrımcılık gibi tutumlar) olarak ifade edilmiştir (Ross, 1993, ss. 322-326). Hudson (1999) ise terörizmin nedenlerini anlamak için çok nedenli yaklaşım (farklı alanlardan nedenlerin birleşimi), siyasi yaklaşım

(ulusal/uluslararası çevreler, üniversiteler gibi ortamlar), organizasyonel yaklaşım (grup/kolektif dinamikler), psikolojik yaklaşım (terörist zihni/kişiliği, katılım nedenleri, motivasyonlar) ve fizyolojik yaklaşım (özellikle nörofizyolojik süreçler) olmak üzere beş yaklaşım olduğunu belirtmektedir (ss. 15-19). Buradaki fizyolojik yaklaşım, özellikle uluslararası ilişkiler, psikoloji ve sosyoloji alanlarındaki terörizm literatüründen farklılaşan bir yaklaşım olarak öne çıkmaktadır. Bu yaklaşım, psikoloji ve nörofizyolojik süreçlerin birlikte açıklanmasını içermektedir. Bu hususta Oots ve Wiegele (1986), medyanın rolüne vurgu yaparak medyanın teröristlerin yöntemlerini ve hedeflerini geniş bir çevreye yayması yoluyla terörizmi "bulaştırabilecek" bir uyarana dönüşebileceğini belirtmektedirler. Ayrıca stres altında beyinde üretilen ve "savaş ya da kaç" tepkisinin kimyasal uyarıcısı olan norepinefrin gibi maddelerin terörizmle de ilişkili olduğunu savunmaktadırlar. Algılanan adaletsizlik durumunun bir sonucu olan hayal kırıklığı duygusunun sürekli uyarılma haline yol açabileceğini ve bu uyarılma halinin de hayal kırıklığını pekiştirebileceğini ve bu şekilde "savaş ya da kaç" sendromunun devamlı olarak tekrarlanabileceğini belirtmektedirler. Burada ifade edildiği gibi sürekli olarak maruz kalınan "hayal kırıklığı-uyarılma kısır döngüsü", bireyleri agresif eylemler aracılığıyla rahatlamaya itebilecek bir durum olarak ifade edilmektedir (Oots & Wiegele, 1986, ss. 16-17). Dolayısıyla bu durumun, terörizme de neden olabilecek etkenlerden birisi olabileceği belirtilmiştir.

Terörizmin psiko-sosyal dinamikler çerçevesinde ele alınması konusunda Abbasi vd. (2017) beş farklı teoriyi; motivasyonel, bilişsel ve sosyal olarak üç kategoride değerlendirmişlerdir. Bunlardan ilki motivasyonel bir yaklaşım olan ve Berkowitz (1989) tarafından oluşturulan "hayal kırıklığı-saldırganlık hipotezi"dir. Bu hipotez, bireylerin haklarından mahrum bırakılmasının ve buna karşı mücadele araçlarının engellenmesinin yol açtığı hayal kırıklığı duygusunun dışarıya atılarak rahatlamanın sağlanabilmesi için saldırganlık güdüsünün oluşabileceğini ve bu durumun da terörizme sebebiyet verebileceğini belirtmektedir (Abbasi vd., 2017, ss. 321-322). İkinci olarak verilen motivasyonel yaklaşım ise "terörizmin göreceli yoksunluk teorisi"dir. Ziemke (2006) tarafından ortaya konan bu teori; algılanan sosyal, ekonomik ve siyasi yoksunlukların terörizme neden olabileceğini belirtmektedir. Üçüncü olarak hem sosyal hem de psikolojik süreçleri içeren "negatif kimlik hipotezi"dir. Bu hipotez Erikson (1982)' ın, kimlik gelişim süreçleri ile ilgili olarak oluşturduğu teorisinden alınmıştır.

Bireyin kim olduğunu ve toplumdaki rolünü çözemediği durumlarda oluşan kimlik krizlerinin, hem toplumun kişiye dayatmaya çalıştığı rollerle hem de sorunlarla mücadeledeki başarısızlığının sebep olduğu hüsranın etkisiyle terörizme yöneltebileceği ifade edilmektedir. Örneğin dini motivasyonlu terör eylemlerinin kökeninde modernleşmenin "dini kimliğe" bir tehdit olarak görülmesinin mevcut olduğu belirtilmektedir (Abbasi vd., 2017, ss. 330-331). Dördüncü olarak belirtilen "narsisistik öfke hipotezi" ise Morf ve Rhodewalt (2001) tarafından ortaya konulmuş olan "narsisizmin dinamik öz düzenleyici işleme modeli" kullanılarak oluşturulmuştur. Bu hipoteze göre, öz saygısının parçalanması ve buna bağlı olarak deneyimlenen öfke duygusunun, kişinin sürekli olarak kendisini yüceltmesi ve diğer kişileri küçümsemesi ile sonuçlanabileceği belirtilmiştir. Zarar görmüş benlikten kaynaklanan "narsisistik yaralanma ve öfkeyi" çözmek için teröristlerin kendilerini üstün görerek ve diğerlerini değersizleştirerek narsisistik öfkelerini besledikleri savunulmaktadır (Crayron, 1983).

Terörizm olgusuyla ilgili olarak değerlendirilebilecek bir diğer yaklaşım hem sosyal hem de bilişsel dinamikleri içeren ve Bandura (1977)'nın ortaya koyduğu "sosyal öğrenme teorisi ve sosyal bilişsel teori"dir. Bu teori bireyin, çevresinden gözlemlediklerini kendi algılarıyla şekillendirerek davranışlarını belirlediğini ifade etmektedir. Teröristlerin de çevrelerindeki gözlemledikleri durumları kendi bilişleriyle anlamlandırarak bulundukları ortamı "terörizme izin verici" bir bağlam olarak değerlendirdikleri belirtilmektedir (Crenshaw, 1981). Dolayısıyla teröristler, gözlemledikleri sosyal ve siyasi birçok durumu zihinsel süreçleri içinde yorumlayarak "kendi gerçekliklerini" oluştururlar. Buradaki gibi çevre ve birey etkileşiminin terörizmle ilişkisi bağlamında literatürde çalışmalar bulunmaktadır. Örneğin, Kerküklü (2023) literatürde birey-çevre ilişkisi çerçevesinde oluşturulan savları dini motivasyonlu terör örgütlerinden olan El-Kaide'nin ve DEAŞ'ın üst düzey yöneticilerinin özelliklerini inceleyerek ifade etmiştir. Makalede El-Kaide'nin kurucu lideri olan Usame Bin Ladin'in öğretmeninden etkilenerek "Müslüman kardeşler" ideolojisi ile ilgili toplantılara katıldığı ve bu şekilde El-Kaide ideolojisinin de temellerinin atıldığı; Irak El-Kaide'sinin eski lideri Ebu Musab El Zarkavi'nin ise gençliğinin yoksulluk ve şiddet olaylarının olduğu bir yerde geçmesinin ve saldırgan kişiliğinin terörizme eğilimini arttırmış olabileceği ve DEAŞ'ın eski liderlerinden olan Ebu Bekir El Bağdadi'nin, kendisinin doğduğu yere Amerika tarafından hava saldırısı düzenlemesinin intikam ve nefret duygusuyla beraber gelen "mağduriyet"

duygusuna neden olarak terörizm sürecini tetiklemiş olabileceği belirtilmiştir (Kerküklü, 2023). Dolayısıyla bahsedilen bu durumlar, terörist kimliğinin oluşmasında bireylerin etraflarındaki durumları bilişsel mekanizmalarındaki süzgeçlerden geçirerek "kendi gerçekliklerini" oluşturmalarını sağlayan süreçlerin bir parçası olmuştur. Bunun sonucu olarak da kendi düşüncelerini ve eylemlerini meşrulaştırmak için "kendi gerçekleri" çerçevesinde yorumlamalar yapmaktadırlar. Örneğin dini ideolojiye sahip terör örgütlerinde, dinin orijinaline yönelik tehdit olduğu düşüncesiyle dinin "güvenlikleştirilmesinin" söz konusu olduğu (Kurt & Demirat, 2024, s. 319) ve El-Kaide'nin söylemlerinde dini kitaptan yaptılan alıntılarında "kendi yorumları ile güncel şartlara uygun hale getirdikleri" belirtilmektedir (Kaşıkcı & Bülbül, 2023, s. 126).

Psiko-sosyal bakış açısıyla farklı terör örgütleri üzerine yazılmış çalışmalar literatürde yer almaktadır. Örneğin, "3N teorisi" bağlamında DEAŞ terör örgütünün şiddet yoluyla radikalleşme sürecine neden olan faktörlerden bahsedilmektedir (Dagher vd., 2023). Bu bağlamda önem kaybı ve insani ihtiyaçlarının karşılanacağı algısının, sosyal çevre ile pekişen önemsenme duygusunun ve anlatılar ile sunulan ideolojik çerçevenin (sorunun çerçevelenmesi, suçlunun belirlenmesi, ihtiyaçların karşılanması ve önem kazanmak için yöntemin sunulması) bu süreçte etkili olduğu ifade edilmektedir (Dagher vd., 2023). Ayrıca DEAŞ'a katılımı ve şiddet eylemlerini sürdürmeyi teşvik eden farklı psiko-sosyal faktörlerden de bahsedilmektedir. Irak gibi savaş ve sömürü gibi şiddet içerikli olayların yaşandığı ülkelerde uzun süre yaşamanın, buradaki toplumlarda ve insanlarda hayal kırıklığı ve güvensizlik hissine sebep olarak terör örgütlerine katılmak için bir neden olabileceği ifade edilirken Batı Avrupa'dan örgüte katılanların birçoğunun ise ailelerinin göçmen olduğu ve düşük eğitim seviyesi, kısıtlı iş imkanları gibi nedenlerle sosyal olarak alt sınıfa mensup olduğu söylenen bu bireylerin reddedilmişlik algısıyla kimlik ve anlam arayışı, bir yere ait olma gibi motivasyonlarla hareket ettikleri belirtilmektedir (Kizilhan & Steger, 2021, ss. 28-30). Öte yandan Özyılmaz Kiraz (2016), El-Kaide terör örgütü için şiddet eylemlerinin devam etmesinde "şiddeti engelleyen vicdani bariyerlerin yıkılmasının" etkili olduğunu belirtirken "kolektiflik fikrinin" ve "ahlaki çözülme mekanizmalarının" bu vicdani bariyerlerin yıkılmasında rolü olan iki psiko-sosyal durum olduğunu belirtmektedir. "Kolektif kimlik" ile gruba bağlılığın sürekli kılınması sağlanırken "ahlaki çözülme" için eylemlerin ahlaki

amaçlara hizmet olarak tanımlanması, sorumluluğun otorite olarak görülen figüre kaydırılması, grupla birlikte hareket edilerek sorumluluğun yayılması, sonuçların önemsenmemesi veya çarpıtılması ve insanlıktan çıkarma başlıca mekanizmalar olarak ifade edilmektedir (Özyılmaz Kiraz, 2016). Koltko-Rivera (2006) ise şiddet kullanımının, "kendinin ötesinde bir davaya veya amaca bağlılık" olarak tanımladığı "kendini aşma ihtiyacı" çerçevesinde, 11 Eylül terör saldırılarının ve genel olarak dini motivasyonlu şiddet eylemlerinin "kendini aşma" durumunun negatif kutbunu ifade ettiğini belirterek (s. 311) motivasyon temelli bir neden ortaya koymaktadır.

Sonuç olarak literatürdeki terörizm olgusu ile ilgili tespit edilen bu çeşitlilik, terörizme ve radikalleşme süreçlerine etki eden dinamiklerin anlaşılmasında çeşitli alanlardan çıktıların bir arada değerlendirilmesinin önemine işaret etmektedir. Bu araştırmada ise, psiko-sosyal teoriler kullanılarak psikoloji ve sosyoloji alanlarının bütünleştiği bir yaklaşım ile incelemeler yapılmıştır. El-Kaide terör örgütüne katılım davranışı ve örgüt içinde radikalleşmeye sebep olan nedenler psiko-sosyal teoriler üzerinden incelenmiştir. Bu doğrultuda literatürde terörizm konusuyla ilişkili olarak az kullanıldığı tespit edilen "ihtiyaçlar hiyerarşisi" ve "3N yaklaşımı" diğer bölümde açıklanmıştır.

2. RADİKALLEŞME SÜREÇLERİNDE İHTİYAÇLARIN, ANLATILARIN VE NETWORK'ÜN ROLÜ

Bu makalede, El-Kaide terör örgütüne katılımı ve şiddet yoluyla radikalleşmeye neden olan psikolojik motivasyonlar "Maslow'un ihtiyaçlar hiyerarşisi" teorisi ve sosyolojik unsurlar "3N yaklaşımı" çerçevesinde incelenmiştir. Terörizm ve radikalleşme olgularında psikolojik ve sosyolojik etkileri anlamlandırabilmek amacıyla, literatürde eksik olduğu tespit edilen bu iki teori ile bağlantılı şekilde El-Kaide terör örgütü üzerine yapılan bu araştırmanın teorik çerçevesi bu bölümde ifade edilmektedir. "İhtiyaçlar hiyerarşisi" psikoloji temelli bir yaklaşımken "3N teorisi" daha çok sosyolojik unsurları barındıran bir yaklaşım olması nedeniyle bir arada kullanılmıştır. İhtiyaçlar bakımından "ait olma", "anlatılar" çerçevesinde "ait olma hissiyatının pekiştirilmesi" ve "gerçekliğin inşası", "network" bağlamında ise "grup aidiyet bilincinin güçlendirilmesi" gibi mikro (psikolojik) ve mezo (sosyolojik) düzeylerde pek çok psiko-sosyal durumun, seçilen vakanın anlaşılması hususunda çerçevelendiği tespit edilmiştir. Bunun için bu kısımda öncelikle kullanılan bu iki teorinin açıklamaları

yapılırken diğer bölümde El-Kaide terör örgütü vakası bağlamında bu iki teori değerlendirilmiştir.

2.1. Maslow'un İhtiyaçlar Hiyerarşisi

Maslow (1943)'a göre her insan, ihtiyaçlarını karşılamak için motivasyona sahip olur ve bu ihtiyaçlar belli bir dizilim oluşturur; bir önceki aşamadaki ihtiyacı karşılayarak sonraki aşamaya geçerler. Maslow bu ihtiyaçları göstermek için piramit modelini kullanmıştır. Bir önceki aşamadaki ihtiyaçlar tamamlanırsa sonraki aşama için arayışın başlayacağını belirterek hedef temelli bir yaklaşım benimsemiştir. İnsanları motive eden beş ihtiyacı, en alttan üste doğru sırasıyla "fizyolojik", "güvenlik", "sevgi/ait olma", "saygınlık" ve "kendini gerçekleştirme" ihtiyaçları olarak sıralamıştır. İkinci versiyonunda saygınlık ve kendini gerçekleştirme ihtiyaçları arasına sırasıyla "bilişsel" ve "estetik" ihtiyaçlarını eklemiştir (Maslow, 1970). En son olarak ise "kendini aşma" ihtiyacını en üste ekleyerek ihtiyaçları sekiz kategoride ifade etmiştir (Maslow, 1976).

Maslow (1943), "fizyolojik ihtiyaçlar" olarak nefes alma, yemek, su, uyku ve barınma gibi fiziksel olarak hayatta kalınmasını sağlayan faktörler (s. 372), "güvenlik ihtiyacı" için güvenli bir çevre ve güvende hissetme (ss. 376-380), "sevgi ve ait olma ihtiyacı" için arkadaş ve aile ortamlarında sevme ve sevilme isteği (ss. 380-381), "saygınlık ihtiyacı" olarak öz saygı ve başkalarından saygı görme gibi faktörler ifade edilmektedir (ss. 381-382). Ardından sırasıyla, bilme ve anlama isteği yani "bilişsel ihtiyaçlar", güzellik ve düzen arayışı olarak "estetik ihtiyaçları" eklenmiştir (Maslow, 1970, ss. 82-86). Bu aşamalardan sonra ise, "kendini gerçekleştirme ihtiyacı" yani kendi potansiyeline ulaşma ve kim olduğunu anlama isteği (Maslow, 1943, s. 13) ve son olarak "kendini aşma ihtiyacı", insanın kendi potansiyelinin üstüne çıkması, manevi ihtiyaçlar ve "zirve deneyimler" olarak ifade edilmektedir (Maslow, 1976). Burada bahsedilen durum aşkın bir karaktere ulaşma yolundaki isteği ifade etmektedir. Bu şekilde sekiz aşamalı bir ihtiyaçlar piramidi oluşturulmuştur.

2.2. 3N Yaklaşımı

Webber ve Kruglanski (2017)'nin "3N yaklaşımı", bireyleri radikal olmaya iten ve çeken nedenleri üç temel faktöre bağlamaktadır: ihtiyaçlar (*needs*), anlatılar (*narratives*) ve bağlantılar (*network*). İhtiyaçlar, bireysel motivasyonları; anlatılar, kültürel unsurları ve bağlantılar, grup bazlı sosyal etkiyi ifade etmektedir (s. 33). Bireysel ihtiyaçlar olarak "onur, aşağılanma,

adaletsizlik, intikam, sosyal statü, finansal yarar, lidere sadık olmak ve cennete girme isteği" (s.34) gibi nedenler belirtilirken bunların altında yatan ana nedenin "önem arayışı" olduğu ifade edilmektedir (s.34). Önem arayışı da üç alt başlık altında incelenmiştir: Önem kaybı, önem kaybı ihtimali ve önem kazanma ihtimali (s.35). Önem kaybı, grup bazlı kayıp ve kişisel kayıp olarak ikiye bölünmüştür: Grup bazlı kayıp durumunda, grup kimliği üzerinden aşağılanma ve onur kaybının kişileri önem arayışına ittiği ifade edilirken kişisel kayıp durumunda, kişinin kendi kimliği üzerinden yaşadığı önem kaybı ile motive olması olarak belirtilmiştir. Önem kaybı ihtimali ise bir kişinin, bir durumu gerçekleştiremediğinde yaşayacağını düşündüğü utanç olasılığı için motive olmasıdır. Önem kazanma ihtimali ise kişinin kahramanlık, şehitlik gibi statüler ile önem kazanma isteği sonucu oluşan motivasyondur (s.35).

Anlatılar ise radikalleşmeye iten süreçlerin kültürel boyutudur. Kültürel normlar ve ideolojik anlatımlar terörizmi meşrulaştıran bir güç haline gelebilmektedir. Terörizmi meşrulaştıran dört anlatıdan bahsedilmektedir. Bunlar, gruba yönelik tehdit olan aktörleri tanımlamak, şiddetin uygun bir cevap olarak gösterilmesi, düşman olarak atfedilen grubun meşruiyetini kaybettirme ve hedefe ulaşmada yüksek başarı olasılığı algısıdır (Webber ve Kruglanski, 2017, s. 40-41).

Bağlantılar ise grup içi dinamikleri ifade etmektedir. Grup içinde aykırı olma korkusu, dolayısıyla da diğerleri tarafından aşağılanma, ötekileştirilme ve önem kaybı korkusu nedeniyle yaşanacak stresli durumdan kaçınmak amacıyla bireyler, grup içi kararları ve eylemleri sorgulamama yoluna giderek fikir birliğini sürdürme çabasına girerler (Webber ve Kruglanski, 2017, s. 41). Bu sorgulamama halinin getirdiği fikir birliği, zamanla kişisel kimliğin grup kimliği ile bütünleşmesine neden olarak bireylerin grubu korumak için fedakârlık yapma ihtimalini arttırır (s. 42). Buraya kadar anlatılan bireysel motivasyonlar, anlatılar ve grup dinamikleri, şiddetle radikalleşme yolunda psikolojik ve sosyolojik etmenlerin etkileşiminin önemini göstermektedir.

3. EL-KAİDE TERÖR ÖRGÜTÜNÜN PSİKOLOJİK VE SOSYOLOJİK BOYUTLARDA İNCELENMESİ

El-Kaide örgütüne katılım davranışına ve örgüt içerisinde şiddet yoluyla radikalleşmeye neden olan süreçler; örgütün 2011 yılı öncesini kapsayan ve Bin Ladin'in öldürüldüğü yerleşkede ele geçirilen 2015 ve 2016 yıllarında

gizliliği kaldırılarak Ulusal İstihbarat Direktörü Ofisi'nin internet sitesinde İngilizce'ye çevrilerek yayınlanan örgüt üyelerine ait 196 mektuba ek olarak Youtube kanalı "Channel 4 News" tarafından yayınlanan "*I was an MI6 spy inside Al-Qaeda"* ve" LADbible Stories" isimli Youtube kanalının yayınladığı "*Life As A Spy Inside Al-Qaeda"* isimli videolardaki, eski bir El-Kaide üyesi olan ve sonrasında Birleşik Krallık dış istihbarat servisi olan MI6 için çalışmaya başlayan Aimen Dean isimli kişinin hem örgüte katılım süreçlerini hem de katıldıktan sonra deneyimlediği durumları anlatan bu röportajlar ve Channel 4 News kanalı tarafından yayınlanan "*Inside Al Shabaab: The extremist group trying to seize Somalia"* isimli belgesel içerisinde El-Kaide'ye bağlı olan Eş-Şebab terör örgütü üyeleri ile yapılan röportajlar da incelenmiştir. Bu araştırmada, mikro düzeyden mezo düzeye doğru bulgular belirtilmiştir. Mikro düzey çerçevesinde bireysel ve psikolojik ihtiyaçlar ve mezo seviyede sosyolojik dinamikler ifade edilmiştir. "Söylem analizi" yöntemiyle "Maslow'un ihtiyaçlar hiyerarşisi" ve "3N yaklaşımı" doğrultusunda bu teorilere denk gelen ögelerin mektuplarda ve diğer kullanılan kaynaklarda olup olmadığı incelenerek bulgular ifade edilmiştir.

Bu araştırmada kullanılacak yöntemin sebebinin anlaşılabilmesi için öncelikle "söylem" ve "söylem analizinin" neler olduğundan bahsedilecektir. Söylem "sosyal, kültürel ve tarihsel kullanım kalıpları ve gelişmeleriyle bağlantılı olarak görülen her türlü anlamlı semiyotik insan etkinliği" (Blommaert, 2005, s.3) olarak ifade edilirken söylem analizi "dilin uzantılarının, tam metinsel, toplumsal ve psikolojik bağlamları içinde ele alındığında, kullanıcıları için nasıl anlamlı ve birleşik hale geldiğini" (Cook, 1989, s. ix) inceleyen bir analiz tekniği olarak belirtilmektedir. Dolayısıyla söylem analizi yöntemi dilin kullanımının eleştirel bir biçimde irdelenmesi yoluyla psikoloji ve sosyoloji temelli dinamiklerin de anlaşılmasına olanak sağlayabilecek bir yöntem olarak ifade edilmektedir. Bu araştırmada, El-Kaide terör örgütüne katılım davranışının ve şiddetin meşrulaştırılarak örgüt tarafından yöntem olarak kullanılmasının nasıl olduğu ve bunların altında yatan psiko-sosyal gerekçelerin neler olduğu birincil kaynak olan örgüt üyelerine ait mektuplar ve röportajlar üzerindeki söylemlerden analiz edilerek "ihtiyaçlar hiyerarşisi" ve "3N yaklaşımı" çerçevesinde açıklanmıştır. Özellikle mektuplar, kişilerin duygularının ve düşüncelerinin anlaşılabilmesine olanak sağlayan bir belge türü olması nedeniyle hem psikolojik süreçlerin anlamlandırılmasında hem de mektubu yazan kişinin

kendi grubu ile ilgili gözlemlediği ve algıladığı durumları da ifade edebilmesi bakımından sosyolojik faktörlerin de anlaşılabilmesine olanak sağlamaktadır. Bu sebeple bu çalışmada El-Kaide örgüt üyeleri tarafından birincil ağızdan yazılan mektuplar ve yapılan röportajlar söylem analizi yöntemi ile psiko-sosyal bir perspektiften araştırılmıştır. İlk olarak psikolojik/bireysel faktörleri ifade eden yani mikro düzeyde bir bakış açısı içeren "ihtiyaçlar hiyerarşisi" çerçevesinde El-Kaide terör örgütüne katılım ve radikalleşme süreçleri değerlendirilecek ve sonrasında sosyolojik/grup temelli dinamikleri içeren yani mezo düzeyde bir perspektiften ifade edilebilecek olan "3N yaklaşımı" bağlamında tartışılacaktır.

3.1. Mikro Düzey: El-Kaide'de Psikolojik Faktörler

Bu kısımda, El-Kaide mensuplarının örgüte katılımındaki ve şiddetle radikalleşmedeki bireysel motivasyonları Maslow'un ihtiyaçlar hiyerarşisindeki adımlar üzerinden incelenmiştir. Söylem analizi sonucu bulunan veriler sırasıyla fizyolojik, güvenlik, sevgi/ait olma, saygınlık, bilişsel, estetik, kendini gerçekleştirme ve kendini aşma ihtiyaçları doğrultusunda açıklanmıştır.

3.1.1. Fizyolojik İhtiyaçlar

İnsanın hayatta kalmasının en temelinde nefes alma, yemek yeme, temiz su, uyku ve barınma gibi ihtiyaçlar vardır. Bu ihtiyaçların en zor karşılandığı yerler, savaş ve çatışma bölgeleri, kırılgan ve yoksul olan ülkelerdir. El-Kaide'nin ilk olarak çıktığı yer olan Afganistan, işgallerin ve savaşın olduğu insanların temel ihtiyaçlarının karşılanmasının zor olduğu bir ülkedir. Örgütün çağrı mektuplarında Afganistan, Pakistan, Sudan, Yemen, Filistin, Irak, Suriye ve Somali gibi iç karışıklıkların yaşandığı ve dolayısıyla da temel ihtiyaçların karşılanmasının zor olduğu ülkelere seslenilmesi ve buralardan örgüte katılanların olması, temel ihtiyaçların karşılanması için örgütün çekici bir faktör olduğunu göstermektedir. Sovyetler Birliği'nin Afganistan'ı işgali sırasında Afganistan'da El-Kaide'ye katılımın olmasının nedenlerinden birisi de budur. "Bin Ladin para konusunda cömertti…bize, fakirlere, dullara, yetimlere yardım ediyordu, bazı ihtiyaç sahibi insanlara yardım fonu düzenliyordu" (National Geographic, 2008) şeklinde ifade edilen durum, ihtiyaçların karşılanması motivasyonuna sahip insanları örgüte katılmaya teşvik edebilecek bir unsur olarak ifade edilebilir. Aynı zamanda El-Kaide'nin Somali'deki yapılanması Eş-Şebab'ın insanlara yiyecek dağıttığı ve kendi açtıkları okuldan mezun olarak örgüte katılanlar için

ziyafet sofrası kurdukları görülmektedir (Channel 4 News, 2022). Gıdaya ulaşmanın zor olduğu bir bölgede örgütün, örgüte katılanlar için "ziyafet sofrası" hazırlayabilmesinin sembolik bir anlamı da vardır. Devletin aksine kendilerinin gıdaya ulaşabildikleri ve bunları halka dağıttıkları mesajını vererek bölgede gıda ihtiyacı gibi temel ihtiyaçları karşılanmayan insanları yanlarına çekme amacında oldukları söylenebilir. Aynı zamanda, örgüte üye olabilmek amacıyla çalışıp katılanlar için ziyafet sofrası hazırlanarak gıda ihtiyacının getirdiği motivasyonun kullanılmasının yanı sıra katılım sağlayabildikleri için örgüt üyelerinin olduğu bir sofra etrafında toplanarak hem "başarı hissi" hem de "önemsenme algısı" ile ödüllendirilmektedirler.

3.1.2. Güvenlik İhtiyacı

Güvenlik ihtiyacı fiziksel ve psikoloji olarak iki kategoriye ayrılabilir. Fiziksel güvenlik, insanların savaş ve iç karışıklıkların olduğu ortamlarda sahip olamadıkları ve ihtiyaç duydukları bir unsurdur. El-Kaide, "Cihat dini desteklemek ve Müslümanları savunmak için yapılır, ülkenin güvenliğinin din tarafından zorunlu kılındığının farkına varmak için yapılır" (*Letter to the Muslim Nation on Eid al-Adha*, t.y., s.2) diyerek kendi ideolojileri olan cihat anlayışını güvenlik ile eş değer tutmuşlardır. Dolayısıyla özellikle kırılgan bölgelerde yaşayan ve güvende hissetmek isteyen insanlarda cihat yolu ile güvenliğin sağlanabileceği algısının oluşturulması ve bunu sağlayabilmek için de örgüte katılma motivasyonunun oluşması muhtemeldir.

Psikolojik olarak güvende hissetme ise algılarla ilgilidir. Tehdit algısı yüksek olduğunda kendilerine fiziksel ve direkt bir saldırı olmasa bile kişiler, psikolojik olarak güvende hissetmeyebilir. Bin Ladin'in ve örgüt üyelerinin başta Amerika olmak üzere Müslüman olmayan ülkelere karşı geliştirdiği tehdit algısı buna örnek olarak verilebilir. 1979'da Sovyetler Birliği'nin Afganistan'ı işgali, 1991 yılında Körfez Savaşı için Arabistana konuşlanan ve kutsal kabul edilen şehirlerde dolaşan ABD askerleri, Afganistana ve Irak'a müdahale eden ABD askerleri (The Infographics Show, 2023) Bin Ladin ve örgüt üyeleri tarafından güvenliklerine tehdit olarak algılanmıştır. Dahası, mektupların birinde Suudi Arabistan'ın Cidde şehrinde açılan uluslararası bir üniversite için "bu okulların açılması kiliselerinin ve kültürlerinin etkisini genişletmek için atılmış agresif bir adımdır" (al-Libi, t.y, s.4) diyerek bunu dışarıdan bir işgal ve güvenlik sorunu olarak algılamışlardır.

Öte yandan tehdit algısını örgüt kendisi de oluşturarak güvensizlik hissini ortaya çıkartmaktadır. Bu güvensizlik hali sonucu güvenlik ihtiyacını gidermek isteyen bireylerin örgüt mensubu olması ya da halihazırda mensup olanların şiddeti içselleştirebilmesinin önü açılabilir. Örneğin; ABD'nin eski başkanı Bush'a ve Bush'un terörizmle mücadele operasyonlarına karşı nefret söylemleri içeren bir mektupta, "Yalancı Haçlı, iki yıllık Haçlı Seferi'nden sonra Taliban'ın hala Afganistan'daki en büyük tehdit olduğunu neden kabul ediyorsun?" (*Message for all Muslims following US State of the Union Address*, t.y., s. 5) denilerek 11 Eylül sonrası Bush'un "terörizmle mücadele" adı altındaki operasyonları için "Haçlı Seferi" benzetilmesi yapılmıştır. Aynı zamanda örgütün "Siyonist Haçlıların bizim milletimize karşı savaşı" (al-Zawahiri, 2003, s. 5) şeklindeki söylemleri, tarihte Müslümanlara karşı gerçekleşen Haçlı Seferleri'nin şu anda da gerçekleştiği yönünde bir anlatı oluşturduklarını göstermektedir. Bu anlatı ile Müslümanlara seslenilerek onları örgütün yanında olmaya teşvik etme yönünde bir amaçlarının olduğu söylenebilir. Buna ek olarak, mektuplar üzerinden yapılan kelime frekansı analizi sonucu, "Haçlı" kelimesinin (152 kere) "Hristiyan" kelimesinden (52 kere) çok daha fazla kullanıldığı görülmüştür. "Hristiyan" diyerek dini ve kabul edilmiş bir kimliğe atıfta bulunmak yerine tarihi olarak Müslüman kimliğine tehdit oluşturmuş "Haçlılar" kavramı kullanılmıştır. Bu şekilde, geçmişte olan olayların hatırlatılarak başta radikalleşmemiş ve sadece örgüt mensubu olan kişiler olmak üzere Müslüman kesimin tehdit algısının yükselmesinin sağlanılması aracılığıyla şiddetin araç olarak meşrulaştırılmasına zemin hazırlama çabasında olunduğu sonucuna ulaşılabilir.

3.1.3. Sevgi ve Ait Olma İhtiyacı

Fizyolojik ve güvenlik gibi temel ihtiyaçlardan sonraki aşama sevme, sevilme ve ait olma ihtiyacıdır. El-Kaide'nin mektuplarında dikkat çeken en önemli unsurlardan birisi de örgüt üyeleri birbirlerine hitap ederken isimlerin önüne "kardeş" kelimesini getirerek "aile" olduklarının vurgusunu yapmalarıdır. "Sizinle bir oğulun babasına, bir kardeşin kardeşlerine konuştuğu gibi konuşuyorum" (Al-Qar'awi, 2010, s.1) ve "Mücahit kardeşler" şeklinde örgüt üyelerine seslenerek bir aileye ait oldukları algısı oluşturulmaktadır.

El-Kaide üyesi olup daha sonrasında MI6 için çalışan Aimen Dean, "benzer düşünen insanlarla çevrili olmam bir lütuftu" (LADbible Stories,

2021) diyerek ait hissetme ihtiyacının terör örgütüne katılmada iten bir faktör olduğunu göstermiştir. Ait olma ihtiyacına bir diğer örnek; siyahi bir İngiliz olan Richard Reid'in, ırkçılığa maruz kalan ve küçük yaşlarda hapishanelere giren sistemden dışlanmış birisi olması, Reid'in babasının hapisteki Müslümanlar için "sana insan gibi davranıyorlar" demesi ve Reid'in daha sonrasında El-Kaide üyeleri ile etkileşimi sonucu örgüte katılması (Elliott, 2002) ötekileştirmeden kurtularak bir yere ait olma motivasyonunun etkisini göstermektedir.

Özellikle genç yaşlardaki bir yere ait hissetme ihtiyacı, arkadaş gruplarında radikalleşmeye neden olabilecek bir faktör olarak gösterilebilir. Örneğin Bin Ladin'in annesi ile yapılan röportajda, "üniversitedeki insanlar onu değiştirdi... 20'li yaşlarının başında neredeyse tamamen beyin yıkayan bazı insanlarla tanıştı. Buna bir tarikat diyebilirsiniz" (Chulov, 2018) diyerek genç yaşlarda arkadaş çevresinin önemli olduğuna işaret etmektedir. Bu yaşlarda kimlik arayışının getirdiği ait olma ihtiyacının radikalleşmeye götürebilecek bir faktör olarak ortaya çıktığı ifade edilebilir. 11 Eylül saldırılarını düzenleyen kişilerin, Hamburg'da üniversite okuyan öğrenciler olması ve birbirleriyle tanışıp "Hamburg Hücresi" grubunu kurmaları (McDermott, 2005), genç kesimin benzer düşüncelere sahip insanlarla arkadaşlık kurarak bir gruba ait hissetme isteğinin radikalleşmeye götürebilecek faktörlerden birisi olduğunu göstermektedir.

3.1.4. Saygınlık İhtiyacı

Saygınlık ihtiyacı, "öz saygı" ve "başkalarından saygı görme" ihtiyacı olarak ikiye ayrılmaktadır. Öz saygı, "güç, başarı, yeterlilik, bağımsızlık ve özgürlük isteği", başkalarından saygı görmek ise "ün/prestij, tanınma, dikkat, önem ve takdir edilme isteği" ile ifade edilmektedir (Maslow, 1943, ss. 381-382). Mektuplarda geçen "hayatlarını kaybetmeleri özgürlüklerini kaybetmelerinden daha kolay ve daha az acı vericiydi" (*Message for general Islamic nation, t.y.)* söylemi öz saygı için önemli bir unsur olan özgürlüğün, örgüttekiler için motivasyon kaynağı olduğunu göstermektedir. Buna ek olarak, 1994 yılında Bosna Savaşı'na katılan Aimen Dean, "görev orada ölmekti, bu yüzden başarısızlık duygusu hissettim" (Channel 4 News, 2018) diyerek ve "ilk cihat deneyimim bitti ve halen yaşıyordum,ve şimdi bir sonraki cihat deneyimine atlamalıyım" (Channel 4 News, 2018) şeklinde ifade ederek El-Kaide'ye katıldığını belirtmiştir. Burada öz saygının bir alt

faktörü olarak başarı ihtiyacının bir örgüte katılmaya ve örgüt için hayatını feda etmeye iten bir sebep olduğu görülmektedir.

Başkalarından saygı görme ise statü, tanınma ve takdir edilme gibi ihtiyaçları içermektedir. Bu ihtiyaçların ortak noktasının 3N yaklaşımında terörzime iten motivasyonlardan biri olarak bahsedilen "önem arayışı" kavramı ile örtüştüğü söylenebilir. Önem arayışını motive eden dolayısıyla da terörizme iten faktörler, "önem kaybı (grup ve bireysel)", "önem kaybı ihtimali" ve "önem kazanma ihtimali" olarak belirtilmektedir (Webber ve Kruglanski, 2017, s. 35). İlk olarak, aşağılanma, küçük düşürülme ve onurun zedelenmesi gibi durumlar ile önem kaybının olması terörizme iten nedenlerden birisidir. Bu önem kaybı "ait olunan grubun aşağılanması" ya da "bireyin aşağılanması" olarak ikiye ayrılmaktadır. Bireysel aşağılanma noktasında ırkçılık ve ötekileştirme gibi durumlar söz konusudur. Öte yandan mektuplar incelendiğinde grup yani dini kimlik üzerinden, diğerleri tarafından aşağılanma neticesinde öfke hali söz konusudur. "Diğer uluslar kutsal mekanlarımıza saldırırken biz aşağılanma içinde yaşıyoruz ve yoksulluk ve işsizlik çekiyoruz" (*Afghani Opportunity,* t.y., s. 8). Burada, dini mekanlara saldırılarak küçük düşürüldükleri belirtilmektedir. "Amerika tek kutup ve tek süper güç haline geldiğinden beri, Doğu ve Batı'da korku ve terör yayarak, aşağılanma, boyun eğme ve onur kırıcı bir atmosferde erkekleri, kadınları ve çocukları öldürüyor" (*To the Islamic Community in General,* t.y., s. 1). Mektuplarda görüldüğü üzere aşağılanma ve onur kırıcı bir atmosferin olması ile oluşan önem kaybının, insanları önem arayışına iterek hem örgüte katılmaya motive edebilecek hem de örgüt anlatılarının bunun üzerine oluşturulması ile şiddet yoluyla radikalleşmeyi sağlayabilecek önemli bir neden olduğu söylenebilir. Çünkü bu durumun adaletsizlik duygusunu uyandırması ve intikam arayışına itmesi muhtemeldir. Örneğin, "Şii liderinden gelmediği sürece neden adaletsizliğin sona erdirilme çağrıları yanıtlanmıyor?" (Al-Qar'awi, 2010, s. 4) diyerek adaletsizlik vurgusu yapılmıştır. Aynı zamanda "Irak, Afganistan ve Pakistan'da haksız yere öldürülen, yaralanan ve yerinden edilen kadınlar ve çocuklar" (Bin Ladin, 2002b) tasviri mektupta çeşitli şekillerde geçerek intikam ihtiyacını körüklemektedir. Dolayısıyla aşağılanarak önem kaybına uğradığını ve başkalarından saygı görmediğine inanan kişilerin hissettiği adaletsizlik duygusu ve intikam motivasyonu terörizme iten bir neden olarak ifade edilebilir.

Saygınlık çerçevesinde önem arayışına iten bir diğer neden ise önem kaybı ihtimalidir. Bir eylem yapılmadığında ya da bir durum gerçekleştirilmediğinde oluşabilecek utanç sonucu önem arayışı içinde olan bir insanın radikalleşmesinde etkili olabilir. "Geri çekilmenin ve ilişki ve bağlantılar yoluyla uzlaşmanın getirdiği utanç verici son konusunda uyardığınızın farkındayız" (Tayib, t.y., s. 7). Burada örgüt için uzlaşmanın bir araç olarak kabul edilmediği ve bunun kullanılması sonucu utanç verici bir son olacağının vurgusunun yapılması, başarısızlıktan kaçınmak için terörizmin unsurlarından olan şiddete başvurulmasına neden olmaktadır. "Amerika'yı yenmek için size çok fazla umut yatırılıyor…Bu yüzden bugün Müslümanları utandırmayın" (*Second letter to Muslim brothers in Iraq*, t.y., s. 9). Burada da görüldüğü üzere istenilen bir hedefe ulaşamamanın sonucu olarak utanç hissi ile oluşabilecek önem kaybı ihtimaline değinilmiştir. Dolayısıyla da terörizmde kullanılan şiddetin, bu ihtimali yok etmek amacıyla örgüt mensupları tarafından meşru bir araç olarak görülmesi muhtemeldir.

Diğer bir husus ise şehitlik kavramı üzerinden kahramanlık sıfatı kazanabilme ihtimalidir. El-Kaide'nin mektupları incelendiğinde öne çıkan önem kazanma aracının "şehitlik" olduğu görülmektedir. Mektuplarda, "din uğruna gönüllerini veren ilk şehitlerden olmak için elinizden geleni yapın" (*Second letter to Muslim brothers in Iraq*, t.y., s. 9) denilerek yapılan çağrı ve sonrasında bunu desteklemek ve meşrulaştırmak için eklenen hadis, "şehitlerin en iyileri cephede savaşanlardır; öldürülene kadar dönmeyin. Onlar cennetin en yüksek odalarından yararlanırlar" (*Second letter to Muslim brothers in Iraq*, t.y., s. 9), şehitlik makamına ve cennette statüye ulaşma motivasyonuna vurgu yapmaktadır. "İyi haber şu ki kardeşlerimden biri Veziristan'da şehit oldu. Babam haberi duyduğunda, Büyük ve Yüce Tanrı'ya şükretti" (al-Qurashi, t.y., s. 3). Görüldüğü üzere, El-Kaide'nin mektuplarda sık sık bahsettiği ve yüksek bir makama ulaşmanın göstergesi olarak görülen şehitlik kavramına yüklenen anlam, üyelerin bu statüye ulaşabilmek için başvurduğu intihar saldırıları gibi eylemi gerçekleştirenin de öldüğü şiddet yöntemlerine başvurması yönünde teşvik edici bir unsurdur. "Mücahitler onu anacak ve onlar onun için dua edecekler, gizlice ve alani şiirler yazacaklar, biz de onun hakkında bildiklerimizden dolayı onu öveceğiz" (Bin Ladin, 2006, s. 2) şeklinde bizzat El-Kaide'nin kurucusu Bin Ladin tarafından, öldürülen bir mensup için yapılan övgüler ve "ulusun şehidi" (Bin Ladin, 2006, s.1) olarak betimlenmesi, diğer örgüt üyelerinin de

önem kazanabilme ihtimali ile örgütün şiddet eylemlerine katılması için motivasyon kaynağı olabilir. Dolayısıyla örgüt üyeleri için ölüme yüklenen anlam, şehitlik statüsüne ulaşarak önem kazanmaktır.

Aynı zamanda "diğerlerine rol modeli olmak" örgütün eylemlerinde yer almayı teşvik edici bir unsur olarak belirtilmektedir. "O, savaşta tebessümle savaştı, bu yüzden Allah onu yüceltti ve ismini daha da yüceltti ve kendisinden sonrakilere örnek oldu" (Bin Ladin, 2006, s. 3) şeklinde yüceltilmeye ve kendisinden sonrakilere "rol model" olmaya yapılan vurgu önem kazanabilmeye yapılan bir vurgudur. Aynı şekilde, Bosna'ya 16 yaşındayken savaşmaya giden ve sonrasında El-Kaide'ye katılan bir mensup, "yabancı bir ülkede savaşa gitme fikri, savunmasız sivilleri savunmak onurlu bir davranış olarak görülüyordu" (LADbible Stories, 2021) ve "seyirci olmaktan ziyade tarihin bir parçası olmak, onu oluşturan ve şekillendiren biri olmak istedim" (LADbible Stories, 2021) şeklinde belirterek insanların onu onurlu birisi olarak tanıma ve tarihi şekillendiren bir kahraman olarak görme ihtimalinin bir motivasyon kaynağı olduğunu göstermektedir. Bu durumu başkalarından saygı görerek statü kazanma kaynağı olarak değerlendirip sonrasında da örgüte katılarak bunu başarma yoluna gitmiştir.

3.1.5. Bilişsel İhtiyaçlar

İnsanlar hem etraflarında olanları yorumlama ve anlamlandırma ihtiyacına hem de kendi düşüncelerinde tutarlılık arama motivasyonuna sahiptir. Yani burada "anlam arayışı ve ihtiyacından" bahsedilebilir. İnsanlar anlamı; kendini güvende hissetme, sevme ve sevilme, ait olma, saygı görme gibi ihtiyaçları karşılayarak da bulabilir. İçinde bulunduğu durumu algılamak ve ihtiyaçlarını düşünmek, bunları karşılayabilmek için yöntemler aramak da bu anlam arayışının bir parçasıdır. Aynı zamanda, kişinin düşüncelerinin, yorumlarının ve algılarının neticesinde oluşan anlam dünyasının, ihtiyaçlarını karşılamak için belki de tek yol olarak gördüğü yöntem ile uyumlu olması da bilişsel bir ihtiyaçtır. Bu duruma örnek olarak, El-Kaide'nin tehdit olarak algıladığı kişilere karşı şiddet eylemlerini meşrulaştırabilmek için "sivil" kavramını yorumlamaları verilebilir. "Kongre ve Beyaz Saray tarafından temsil edilen Amerikan halkının ABD'deki en yüksek gücü elinde tuttuğu ve nihai karar vericilerin onlar olduğu bilinen bir gerçektir. Bu nedenle, Amerikan halkını öldürmeye ve onlarla savaşmaya odaklanmalıyız" (*Letter to Uthman*, t.y., ss. 1-2) şeklinde belirtilerek "sivil" kavramını kendi eylemlerini meşrulaştıracak şekilde yorumladıkları

görülmektedir. Kendi düşüncelerinin eylemleri ile tutarlı olabilmesi için kavramları farklı şekillerde yorumlama yoluna gidilmiştir. Bu tutarlılık, ihtiyaçlar hiyerarşisindeki sonraki adım olan "estetik ihtiyaçları" ile de bağlantılıdır; çünkü estetik sadece fiziksel değil aynı zamanda bilişsel temelli de olabilir ve tutarlılık kavramı düzen ve uyum ihtiyacı ile de bağlantılıdır.

Düşünceler arasındaki uyum ve uyumsuzluk ile ilgili çalışmalar "bilişsel uyumsuzluk" kavramı altında kavramsallaştırılmıştır. Hem düşünceler arasındaki hem de düşünce ve eylem arasındaki çelişki durumunda "bilişsel uyumsuzluk" şeklinde ifade edilen bir durum ortaya çıkmaktadır (Festinger, 1957). Bu uyumsuzluk halinin verdiği rahatsızlıktan kurtulabilmek için başvurulan yöntemlerden ikisinin rasyonelleştirme ve "doğrulama yanlılığı" olduğu söylenebilir. El-Kaide için Amerika baş düşman olarak düşünülmekte ve şiddet de bu düşmanı yenebilmek için tek çözüm olarak görülmektedir. Dolayısıyla Amerika'nın düşman olduğu düşüncesi ve kullanılan araç olan şiddetin uyumlu olabilmesi için aralarında çelişki yaratabilecek meselelerin yeniden yorumlanarak meşrulaştırılması ihtiyacı söz konusudur. Arada çelişki yaratan konu, sivillerin de kullanılan araçlar neticesinde öldürülmesidir. Bu yüzden "sivil" kavramının yeniden yorumlanması yoluyla hedefe ulaşmada kullanılan aracın rasyonelleştirilmesi gerekmektedir. Mektuptan alınan yukarıdaki alıntıda, Amerikan halkının yöneticileri seçen kişi olduğu ve bu yüzden de onları sivil olarak tanımlamadıkları görülmektedir. Bu yüzden, bir El-Kaide üyesinin belirttiği gibi, örgütte verilen indoktrinasyon derslerinde "vuracakları yerlerde sivillerin olmadığı telkin ediliyor" (LADbible Stories, 2021) ve Amerikada vergi ödeyenlerin, oy kullananların ve Müslüman ülkelerdeki bombalamaları destekleyen hükümeti seçenlerin masum olmadığı, dolayısıyla da Batı'da sivillerin olmadığı sonucuna varıldığı söylenerek (LADbible Stories, 2021), bu şekilde bir anlamlandırma ile yapılan meşrulaştırmanın bilişsel çelişki yaşayan örgüt üyelerinde çelişkiyi azaltmayı sağladığı söylenebilir.

Bilişsel çelişkiyi azaltma noktasında başvurulan bir diğer husus, sadece düşünceleri destekleyen kanıtları aramak ve diğerlerini görmezden gelmek anlamına gelen "doğrulama yanlılığı"dır (Nickerson, 1998). El-Kaide'nin kendi eylemlerini rasyonelleştirebilmek için başvurduğu yöntemlerden birisi de Kur'an'dan yapılan alıntılardır. Bir mektupta, "ve onlara karşı gücünüz yettiğince savaş atları (tanklar, uçaklar, patlayıcı maddeler, füzeler, toplar) hazırlayın. Bunlar Allah'ın düşmanını ve sizin düşmanınızı ve bunların

dışında sizin bilmediğiniz, fakat Allah'ın bildiği diğer düşmanları tehdit edecektir" (Al-Somali, t.y., s. 10) diyerek verdiği örnekte parantez içinde yazılan yer Kur'an'ın orijinalinde yoktur ("Enfâl Suresi", 2025, 8:60), sonradan yazan kişi eklemiştir. Kuran'ın indirildiği dönemde savaş atları üzerinde kılıçlar ile savaşanların vereceği zarar daha hedef odaklı olabilirken, bir bombanın etkisi hedef olmayan insanları da öldürebilecek niteliktedir. Dolayısıyla burada, örgütün şiddet eylemlerini rasyonel bir zemine oturtabilme ihtiyacının neticesinde ayetin günümüze uyarlanmış ve örgütün eylemlerini meşrulaştırabilecek nitelikteki bir yorum seçilmiştir. Buradaki doğrulama yanlılığı ise, mektuplarda bahsedilen ayetlerin seçilerek konulmasıdır. Mektuplar incelendiğinde de örnek gösterilen ayetlerin kendi eylemlerini destekleyen ayetler olduğu ve sivillerin öldürülmemesi üzerine olan ayetlere yer verilmediği, yer verildiğinde ise sadece İslam'a inanan insanların öldürülmemesi üzerine ayetlere yer verildiği görülmüştür. Örneğin "kim, bir cana kıymayan veya yeryüzünde bozgunculuk çıkarmayan bir nefsi öldürürse, bütün insanları öldürmüş gibi olur" ("Mâide Sûresi", 2025, 32:120) şeklinde geçen ayette masum insanların öldürülmemesi gerektiği belirtilmektedir, ancak mektuplarda bu ayet gibi olan cümlelerden bahsedilmemiştir. Buradaki doğrulama yanlılığının işlevinin, örgüt üyelerinin düşünceleri ve eylemleri arasında uyumsuzluğun engellenmesi olduğu ve rasyonelleştirme çabasının ise ortaya çıkabilecek uyumsuzluğun azaltılması yönündeki ihtiyaçtan kaynaklandığı söylenebilir.

3.1.6. Estetik İhtiyaçlar

Maslow (1970), estetik ihtiyaçlar doğrultusunda güzellik arayışının yanı sıra düzen, simetri ve sistem ihtiyacı gibi durumları sıralayarak bu ihtiyaçların sadece fiziksel değil bilişsel olduğunu da belirtmiştir. Bu yüzden estetik ihtiyaçları somut ve soyut olarak tanımlamak mümkündür. Bu doğrultuda örgüt dokümanlarından estetik ihtiyacının göstergeleri olarak "cennet güzellemeleri" ve yapay olana duyulan nefret yani "doğallık arayışı" örnek verilebilir. El-Kaide'nin Afganistan gibi savaşın ve iç karışıklıkların olduğu dolayısıyla da düzensizliğin hâkim sürdüğü bir yerde örgütlenebilmesi yapılan cennet güzellemelerin de etkisinin olduğunu gösterebilir. Çünkü estetik ihtiyacının ortaya çıkardığı güzellik arayışı ve güzel olana ulaşma isteği önemli bir motivasyon olabilmektedir. Örneğin, 11 Eylül saldırılarını düzenleyen El-Kaide teröristlerinden birisi olan Muhammed Atta'nın bavulundan çıkan ve düzenlenecek eylem için motivasyon söylemleri bulunan mektupta geçen "cennet bahçelerinin tüm

güzellikleriyle sizi beklediğini bilin" ("Last Words of a Terrorist", 2001) söylemi, güzele ulaşma ihtiyacının bir bireyi intihar saldırılarına kadar götürebileceğini göstermektedir. Örgütün mektuplarında geçen "cennet ne güzeldir, ona yakın olmak ne güzeldir, tatlıdır" (*Second letter to Muslim brothers in Iraq*, t.y., s. 9) anlatısı, kişilerde estetik ihtiyacının getirdiği arayışın neticesinde oluşabilecek motivasyon ile örgüt eylemlerine ikna etme çabası olarak ifade edilebilir.

Estetik ihtiyacından doğan bir diğer arayış ise "doğallık" olarak ifade edilebilir. Örgütün mektuplarında "yapay" olarak tanımlanarak düşmanlaştırılan aktörler ve kavramlar hem nefret söylemlerini meşrulaştırma hem de doğal olana ulaşma arzusundan kaynaklandığı söylenebilir. Örneğin, Şiilerin gerçek İslam'ı temsil etmediğini, kendilerince farklı bir din oluşturduklarını söyleyerek (*Draft Speech About Iran and America with Mahmud's Comments*, t.y., s. 5) düşman olarak gördükleri grupların dinlerini "yapay" yani insan eliyle oluşturulmuş bir din olduğunu belirtmeleri, kendi dinlerinin "doğal" olduğunu düşündüklerini göstermektedir. Doğal olanın güzel olduğu anlayışı çerçevesinde kendi dinlerinin güzel olduğunu ve diğerlerinin dinlerinin yapay ve hoş olmadığını düşünerek ötekileştirmeye başvurulduğu söylenebilir. Buna diğer bir örnek ise El-Kaide'ye bağlı olan Eş-Şebab yapılanmasının lider yardımcısının söylediği "demokrasi, Müslüman olmayanların dini…demokrasi insanların seçimi. Bizim inandığımız ise kanunlar Allah'tandır." (Channel 4 News, 2022) söylemi demokrasiden nefret etme nedenlerinden birisi olarak insanların seçimi yani "yapay" bir oluşum olması olduğu ve kendi desteklediklerini sistemin Allah'tan geldiği yani "doğal" olduğu inancında olmalarıdır. Burada yapılan "bizim ve onların" ayrımının meşrulaştırılmasının "doğal ve güzel olanı takip etme" ihtiyacı üzerinden yapıldığı söylenebilir.

3.1.7. Kendini Gerçekleştirme İhtiyacı

Kendini gerçekleştirme, insanın potansiyellere ulaşma ve kim olduğunu bulma ihtiyacı ile oluşan bir süreçtir (Maslow, 1943). Burada bahsedilen durum, insanın kendini ve kimliğini bulabilme ihtiyacıdır. Bireyin kimliğinin oluşmasında içinde bulunduğu grubun dinamikleri de önemlidir. Mektuplardan birinde geçen "mücahit inşa etmek" (*Letter to our honorable Shaykh*, t.y., s. 2) kavramı üzerinden oluşturulan farklı kimlikler vardır. Örgütün cihat ideolojisi uğruna savaşanlar için kullandığı "mücahit" kimliği

ile bağdaştırılan diğer kimlikler, "silah" ve "din" üzerine kurularak bir bütün olacak şekilde örgüt kimliği oluşturulmuştur. "Silahlarımızı terk etmek tamamen kabul edilemez çünkü bu varlığımızın ve tarihimizin bir parçasıdır ve hayatımızı korumak için ona güveniyoruz. Bir adam silahsız eksiktir ve silahlarını bırakan insanlar artık değersizdir" (*Letter Addressed to Atiyah*, t.y., s. 3) ve "silahlar, hayatta kalanlarımızın ve tarihimizin bir parçasıdır. Silahsız adamlar eksiktir ve silahlarını bırakan adamlar başkaları tarafından saygı görmez" (*Letter to Abu Basir*, t.y., s. 3) şeklinde ifade edilen söylemlerde silaha ve dolayısıyla da şiddete atfedilen anlam, grubun varlığı ve kimliği ile bir tutulmasıdır. Bu yüzden de silahı bırakırlarsa saygı görmeyeceklerini ve değersizleşeceklerini, bu yüzden de dünya üzerindeki mevcudiyetlerinin zedeleneceğini düşünmektedirler. Bunlara ek olarak, "din öğretisini kafirlere sadakate ve boyun eğmeye uygun hale getiren…dinin kaybı, değerlerin yokluğu ve kimliğin kaybıdır" (*Letter to the Muslim Nation on Eid al-Adha*, t.y., s. 3) şeklinde ifade edilen bu durumda, dinin olmamasının kimliğin yokluğuna yol açacağını düşündüklerinin; din ve kendi kimliklerini özdeşleştirdiklerinin göstergesidir. Bu kimliği korumak için şiddet yöntemine başvurulması, bu yöntemin meşrulaştırılması anlamını taşımaktadır. Buraya kadar bahsedilen örgüt kimliği olgusu mücahit, silah ve din kavramları üzerinden ifade edilmektedir. Dolayısıyla kendini gerçekleştirme çabasındaki bir insanın kim olduğunu keşfederek bir kimlik kazanma ihtiyacı, örgüt kimliğini kendi kimliği üzerine inşa ederek özdeşleştirmeye itebilecek bir faktör olduğu söylenebilir.

3.1.8. Kendini Aşma İhtiyacı

Kendini aşma ihtiyacı, geniş ve soyut bir tanımlamaya sahip olmakla beraber "manevi doyum" ve "zirve deneyimler" ile açıklanmaktadır (Maslow, 1976). İnsanın kendi potansiyelini gerçekleştirmesi ile oluşturduğu kimlik üzerine inşa ederek manevi doyuma ulaşma ihtiyacı olarak ifade edilebilir. "Zirve deneyimlerinde, geçici de olsa, korku, kaygı, engelleme, savunma ve kontrol, şaşkınlık, karışıklık, çatışma, gecikme ve kısıtlama kaybı yaşanma eğilimi vardır. Parçalanma, delilik, ölüm korkusunun hepsi bir anlığına ortadan kalkma eğilimindedir. Belki de bu, korkunun ortadan kalktığını söylemek anlamına gelir" (Maslow, 1976, s. 71) şeklinde ifade edilen duruma ihtiyaç duyma hali El-Kaide bağlamında "şehitlik operasyonları" olarak ifade edilen örgüt jargonu üzerinden açıklanabilir. "Daha fazla fedakarlığa, daha fazla gerilla savaşına ve şehitlik operasyonlarına ihtiyaç duyuyor, çünkü bunlar Allah'a itaati kanıtlayan ve

sizi O'na yaklaştıran en iyi amellerdendir" (*Second letter to Muslim brothers in Iraq*, t.y., s. 2) şeklinde ifade edilen durum, ölüm gibi gündelik korkuların aşılmasını ve zirve deneyimleri yaşama ihtiyacını motive eden söylemlerdir. "Allah'a yaklaşma" olarak ifade edilen aşkınlık durumunun, örgütün "şehitlik operasyonları" dediği intihar saldırıları ile olabileceğinin söylenmesi, kendini aşma ihtiyacındaki birisi için şiddeti ve ölümü meşrulaştıran bir durum olduğu söylenebilir. Bunun için kullanılan bir diğer kavram ise "cennet" kavramıdır. "[11 Eylül sonrası] aynı yolu aramaya hevesli milyonlarca [Cihat] kardeşleri var…ölümü ve kargaşayı taşıyıp cenneti arayan" (*Message for all Muslims following US State of the Union Address*, t.y., ss. 4-5) şeklinde ifade edilen "cenneti arama durumu", gündelik ihtiyaçların karşılanması sonrası kişinin potansiyeli üstünde manevi doyuma ve aşkın bir gerçekliğe ulaşma ihtiyacı olarak ifade edilebilir. Bir El-Kaide üyesinin söylediği "Cihatı bir arınma ve bir keşif yolculuğu olarak görüyorsun" (Channel 4 News, 2018) cümlesindeki "arınma" ve "keşif yolculuğu" gibi kavramlar ile ifade edilebilecek kendini aşma ihtiyacının, örgütün cihat ideolojisi çerçevesinde algılanması, bu ihtiyacı karşılayabilmek için ideoloji ile bağlantılı olarak kullanılacak şiddet yöntemlerinin örgüt üyeleri tarafından içselleştirilmesine olanak sağlayabilir.

3.2. Mezo Düzey: El-Kaide'de Sosyolojik Faktörler

Terörizm ve radikalleşmenin sosyolojik dinamikleri ile ilgili olarak 3N yaklaşımı, "anlatılar" ve "grup dinamikleri (network)" kavramlarından bahsetmektedir (Webber ve Kruglanski, 2017). Bu doğrultuda söylem analizi yöntemiyle incelenen El-Kaide ile ilgili kaynaklardan elde edilen veriler neticesinde ulaşılan bulgular, bu kısımda değerlendirilmiştir.

3.2.1 Anlatılar

Anlatılar, şiddeti meşrulaştırmak için başvurulan bir yöntemdir. Bu doğrultuda, diğerlerini (düşmanı) tanımlamak, şiddetin uygun bir cevap olduğunu göstermek ve şiddetin amaca ulaşmada yüksek başarı sağlayacağı algısı oluşturmak terörizmi meşrulaştırma sürecindeki aşamalar olarak ifade edilmiştir (Webber ve Kruglanski, 2017). İlk olarak "diğerlerini" tanımlamak, grup için tehdit olan aktörleri somutlaştırmaktır (s. 40). Bu noktada, El-Kaide çerçevesinde bakıldığında gerçek suçlu olarak atfedilen aktörler, onların topraklarını işgal etmekte olduğunu söyledikleri Amerika ve müttefiklerinin hükümetleridir. Ancak bu hükümetlerin suçluluğunu somutlaştırmak için günah keçisi olarak belirledikleri ve saldırdıkları kişiler

bu ülkelerin vatandaşlarıdır. Mektuplar incelendiğinde örgüt üyelerinin "biz" diye bahsettikleri kişiler olan "Müslümanlar" içerisinde de ötekileştirme yaptıkları gözlenmektedir. Müslümanlar içerisinde de "biz ve onlar" ayrımı yaparak, Sünnileri kendilerinden ve Şiilik gibi İslam'ın diğer mezheplerinden olanları "diğerleri" olarak tanımlamaktadırlar. Buna ek olarak "biz" olarak bahsettikleri Sünnileri de kendi içlerinde ayırmaktadırlar: El-Kaide üyeleri/destekçileri ve örgüte destek olmayan "düşmana" yardım eden diğerleri. Dolayısıyla, "onlar ve diğerleri" olarak bahsedilen kişilerin Müslüman olmayan ve Müslüman olsa da örgütün ideolojisini desteklemeyen kişiler olduğu görülmektedir. Örgütün kendisini tanımladığı anlatılar üzerinden düşman tanımı yapılmaktadır. "Aşağılanma ve onur kırıcı bir hayat yaşıyorlar, çocukları hapse atılıyor, büyüklerine kötü muamele ediliyor, topraklarından sürülüyorlar ve tüm hakları ellerinden alınıyor" (Al-Qar'awi, 2010, s. 2) şeklinde geçen cümlede ve mektupların genelinde "kendilerini" tanımlamak için kullandıkları "aşağılanmış", "hapsedilmiş", "kötü muameleye maruz kalmış" ve "yerlerinden edilmiş" gibi kavramlar ile "ezilenler" (*Message for general Islamic nation*, t.y., s. 5) olduklarına dair anlatılar yapmaları; ve bu anlatılar ile inşa edilen "mağdur kimliği" üzerinden bu mağduriyete yol açan olarak gördükleri "diğerlerini" tanımlamanın söz konusu olduğu söylenebilir.

Şiddeti meşrulaştırma sürecindeki bir diğer aşama, şiddetin uygun cevap olduğuna dair anlatılardır. Bunun için seçilmiş travmaları hatırlatma, Kur'an'a atıf ve insanlıktan çıkarma (*dehumanization*) örgütün kullandığı yöntemlerdir. Seçilmiş travma "bir grubun diğer bir grup tarafından kendini çaresiz ve mağdur edilmiş durumda hissetmesine neden olan bir olaydır" (Volkan, 1993, s. 13). El-Kaide bu travmaları mektuplarında sık sık hatırlatarak anlatılarını oluşturmuştur. Örneğin; ABD'nin Irak'ı işgalini anlatırken "halkı ezdiler ve köyleri bombaladılar…barut patlamaları ölüm saçtı" (Bin Ladin, 2006, s. 4) diyerek tarihi travmaları örgüt üyelerine hatırlatarak intikam duygusunu canlı tutma ve mağdur psikolojisini devam ettirme çabasında olduğu söylenebilir. Seçilmiş travmalar üzerinden yapılan anlatılar ile adaletsizlik ve mağduriyet yaşadıkları hatırlatılarak şiddet eylemleri meşrulaştırılmaya çalışılmaktadır. Şiddete başvurma yolundaki bu meşrulaştırmayı Kur'an ve hadisler üzerinden de yapmaktadırlar. "Adaletsizlikten ve haksızlıktan kurtulmak ve adaletsiz yöneticiden kurtulmak ve insanlara adalet getirmek için bunu ancak zorla yapabilirsiniz…eğer zorlamadan başka bir yöntem olsaydı onu Kur'an'da

bulurduk" (Al-Qar'awi, 2010, s. 5) şeklinde belirterek şiddetin tek yöntem olduğu algısını Kur'an üzerinden kanıtlamak istemişlerdir. Bunlara ek olarak, insanlıktan çıkarma veya insandışılaştırma yönteminin de kullanıldığı görülmektedir. "İnsan altı Amerikalılar" (Al-Somali, t.y., s. 4) şeklinde betimleyerek düşman olarak atfettikleri kişilerin insandan aşağı olduğuna dair bir ötekileştirme yapmaktadırlar. "Amerikan ve Avrupa vatandaşları, bu kalpsiz, lanetli Siyonist haçlı seferi makinesini, kötülük ve açgözlülüğü kapatacak anahtardır" (Al-Somali, t.y., s. 4) diyerek kalpsiz ve lanetli diyerek aşağılama söz konusudur. "Hristiyanlar, Şiiler ve diğer saçaklar [kenarlar]" (Al-Qar'awi, 2010, s. 3) şeklinde marjinalleştirme yapılarak aşağılama ve ötekileştirme yapılmaktadır. "Yargınız, kardeşlerinizmiş gibi görünen şeytan tarafından etkilenmemelidir; onların eylemlerinin, sizin pahasına olsa bile, kendi kişisel çıkarları için olduğunu görmezsiniz" (Al-Qar'awi, 2010, s. 2). Burada mektubun bağlamıyla değerlendirildiğinde, şeytan diyerek düşmanlarını insan dışı bir varlıkla özdeşleştirmektedirler. Ayrıca 11 Eylül saldırıları öncesi örgüt üyesi olan Muhammed Atta'nın mektubunda "kesim esnasında bıçağınızı keskin tutmalı ve hayvanınızı rahatsız etmemelisiniz" ("Last Words of a Terrorist", 2001) şeklinde saldırı için "kurban kesme" metaforu kullanılmış ve bu şekilde uçaktaki yolcular insandışılaştırılarak gerçekleştirilecek şiddet eylemi meşrulaştırılmaya çalışılmıştır.

Şiddeti meşrulaştırmadaki bir diğer aşama, şiddeti kullanarak hedefe ulaşma ihtimalinin yüksek olduğu algısının yaratılmasıdır. Bunun için, örgüt üyeleri seçilmiş zaferleri anlatılarında kullanarak "görünür olma" amacına ulaşmanın şiddet ile başarılabileceği algısını tarihi olaylara atıf yaparak anlatmaktadır. Seçilmiş zafer, "başarılı olma ve başka grup üzerinde zafer kazanma duygusu yaratan olaylar" (Volkan, 1993, s. 14) olarak tanımlanmaktadır. Sovyetler Birliği'nin Afganistan'dan çekilmesi ve 11 Eylül saldırıları gibi olaylar zafer olarak anlatılmaktadır. "Amerikalılar buna yanıt vermezse, onların kaderi, askeri yenilgi, siyasi parçalanma, ideolojik çöküş ve ekonomik iflasla başa çıkmak için Afganistan'dan kaçan Sovyetlerin kaderi olacak" (Bin Ladin, 2002a) diyerek tehdit ile korku yaymanın yanı sıra Sovyetler Birliği'nin Afganistan'dan çıkarılmasını kendi zaferleri olarak anlatmaktadırlar. "Amerika'nın birini bastırmak istemesi halinde bunun sadece 24 saat süreceğini söylerlerdi, ve işte savaşın onuncu yılındayız ve Amerika ve müttefikleri hala bir serabın peşinde, sahili olmayan denizde kaybolmuş durumda" (*To the Islamic Community in*

General, t.y., s. 1) şeklinde yapılan bu anlatıda düşman olarak gördükleri ülkenin, örgütü yıllardır bitiremediğini vurgulayarak bunun üzerinden zafer inşa edilmiştir. Bütün bunlara ek olarak, 11 Eylül için "New York ve Washington savaşı" (*Letter to Abd al Rahman,* t.y., s. 1) ve "11 Eylül'ün mübarek işgalleri/saldırıları" (*Letter to the Muslim Nation on Eid al-Adha*, t.y., s. 4) şeklindeki anlatım ile savaş olarak gördükleri bir durumdan zafer ile ayrıldıklarını anlatmaktadırlar. Dolayısıyla bu zafer anlatıları, şiddeti kullanarak hedeflerine ulaşmanın mümkün olduğu düşüncesini içselleştirmek için kullanılmaktadır.

3.2.2 Grup Dinamikleri

Anlatılara ek olarak bağlantılar/grup dinamikleri de terörizmde grup süreçlerini etkileyen sosyal faktörlerdendir. Bu noktada örgütün yapısı ve sistematikliği de hem örgüte çeken bir faktör olarak hem de örgüt üyelerinin grup içinde devamlılığında etkilidir. Örneğin; mektuplardan birisi iklim değişikliği hakkında yapılması gerekenler; kalkınma projeleri, tarım gibi konular hakkında ve evlerini su basanlar, kıtlıkla boğuşanlar için planlamaları içermekte (*Letter Implications of Climate Change*, t.y.) ve diğer bir mektup örgüt yöneticilerinin görevleri; aileleri ziyaret etmek, ihtiyacı olana maddi destek sağlamak, ev onarımları, inşaat gibi konularda yapılan düzenlemeleri içermektedir (*Duties of administrators,* t.y.). Bir devlet gibi sistematik bir şekilde yapılan bu düzenlemeler, alternatif bir sistem arayışında olan insanları çekebilecek bir konudur. Özellikle Afganistan, Yemen, Sudan, Filistin, Somali gibi iç karışıklıkların olduğu dolayısıyla insanların temel ihtiyaçlarının karşılanamadığı ülkelerde yaşayan insanları El-Kaide gibi örgütlü yapılara çeken bir özelliktir. Böyle ülkelerde düzensizlik içinde yaşayan insanlar, terör örgütü olsa dahi içerisindeki planlamalar ve belirli kurallar ile alternatif bir düzen oluşturmuş bir yapıya katılma ihtiyacı hissedebilirler; oluşturulmuş bu sistematik yapı örgütte devamlılığı sağlayabilen bir özellik haline de gelebilir. Aynı zamanda yöneticilerin ailelere ziyarete gitmesi ve maddi destek sağlaması gibi planlamalar, yoksunluk içinde yaşayan ve değer görmediğini hissedenlerin ihtiyaçlarının karşılanması ve görünür olmalarını sağlama noktasında kişileri örgüte çekebilir.

Fikir birliğini sürdürmek ve grup kimliği ile bütünleşme süreçleri grup dinamikleri açısından önemlidir (Webber ve Kruglanski, 2017, ss. 41-42). Bu doğrultuda örgüt mektuplarında bahsedilen konulardan birisi de fikir

birliğinin önemidir. "Emir'in çabalamak için seçtiği konulara gelince…bunlara uyulması zorunludur…uyum, grubun ortak malıdır ve anlaşmazlık onun bozguncusudur" (*Recommendations for the Mujahidin Entering Afghanistan*, t.y.) ve "her mücahit, anlaşmazlık ve ayrılıklara yol açan küçük meseleler üzerinde değil, uyum ve fikir birliği temelinde hareket eder" (*Recommendations for the Mujahidin Entering Afghanistan*, t.y.). Burada ortak bir grup düşüncesinin önemine ve grup içi uyuma vurgu yapılarak anlaşmazlıkların hoş karşılanmadığı söylenmektedir. Dolayısıyla örgütün ortak fikirlerini sorgulayan kişiler uyumu bozan kişiler olarak görülmektedir. "Tartışmalardan ve çatışmalardan kaçınmak size cennette bir yer garanti edecektir" (al-Libi, 2010, s. 6) şeklinde bir söylemin olması ve bunun "ikiyüzlülükten kaçanlara cennette bir yer garanti ediyorum" (al-Libi, 2010, ss. 6-7) hadisi ile desteklenmesi farklı düşüncelere iyi gözle bakılmadığı hatta ikiyüzlülükle bir tutulduğu; örgütün kurallarının sorgusuz sualsiz kabul edilmesi gerektiği ve üyeler sonradan sorgulamaya başlarlarsa da iki yüzlü olarak suçlanacakları mesajının verildiği söylenebilir.

Bireysel kimliğin grup kimliği ile bütünleşmesi, grup hedeflerine uygun hareket ederken örgüt üyelerinin kendi hedefleri adına da hareket ettikleri düşüncesinin oluşmasını ve grup ile arasındaki bağın aile bağları gibi algılanmaya başlaması üzerine üyelerin grubu korumak için kendilerini feda etmeye daha istekli olmasını sağlar (Webber ve Kruglanski, 2017, s. 42). El-Kaide ise İslam'ın cihat anlayışı çerçevesinde oluşturduğu kimliğini örgüt mensuplarının bireysel kimlikleri üzerine inşa ederek örgüt ve kişi kimliklerinin özdeşleşmesini sağlamaktadır. Örgütün mektuplarda birbirlerinden "Müslüman kardeşler" olarak bahsetmesi üyelerin birbirlerini bir aile gördüğünü göstermektedir. Bu durum, örgütü korumak için bireyleri fedakârlık yapmaya iten nedenlerden birisi olarak gösterilebilir. Kimlik bütünleşmesi konusunda örgüt liderinin de önemli bir rolü vardır. Örneğin, bir mensup, Bin Ladin'i "cihadın özü" (LADbible Stories, 2021) olarak betimlemiştir. Aynı şekilde Zevahiri'nin Bin Ladin için "onun cihat yolundan" (BBC News, 2011) yürüyeceğini söylemesi cihatçı kimliğin lider kimliği ile bir tutulduğunu göstermektedir. Öte yandan, Bin Ladin'in Amerikalılara seslendiği mektubunda (Bin Ladin, 2002a), "biz" diliyle konuştuğu görülmüştür. Ben ve biz sözcüklerinin frekanslarına bakıldığında, "ben/beni/benim" sözcükleri üç kez geçmektedir ve bunlardan ikisi Kur'an'da geçen cümlelerden yapılan alıntılarda kullanılmıştır. "Biz/bize/bizim" sözcükleri ise toplamda 54 kere kullanılmıştır. Burada

birinci çoğul kişi anlatımını kullanarak grubun adına konuşması, grubu kendisiyle ve dolayısıyla da örgüt için oluşturduğu cihatçı kimliği ile bir bütün olarak gördüğü söylenebilir.

Bunlara ek olarak örgütün, intihar bombacılarının eylemlerinin anlamını "Allah'ın sözünü savunmak ve dini ve hayattaki her şeyi bozan kafir düşmanı püskürtmek için dinin adını güçlendirmek için kendilerini feda etmek" (*Dear Muslim brothers and sisters,* t.y., s. 4) olarak ifade etmesi, İslam kimliği ile örgüt kimliğini bir gördüklerini, bu yüzden dini korumak ve güçlendirmek için örgütün yöntemlerini kullanma noktasında bireylerin istekli olduğu söylenebilir. "Bu milleti kurtarmak ve dininin görkemini yeniden tesis etmek görevi mücahitlere aittir" (Bin Ladin, t.y., s. 1) şeklinde yapılan görev tanımlaması, dini kimlik ile örgüt kimliğinin bir tutularak El-Kaide'nin ve üyelerinin İslam dininin temsilcisi olarak kendilerini konumlandırdığını ifade etmektedir. Bu şekilde yapılan kimlik tanımlaması, üyelerin örgütü koruyarak dini de koruduğunu düşünmesine neden olarak fedakârlık yapmaya iten bir sebep olarak gösterilebilir.

SONUÇ

Sonuç olarak, terörizm olgusunda şiddetle radikalleşme sürecinde bireysel/psikolojik ve sosyolojik dinamikler etkili olmaktadır. El-Kaide üzerinden yapılan içerik incelemesi neticesinde tespit edilen bulgular, ihtiyaçlar hiyerarşisi ve 3N teorisi üzerinden yorumlanmıştır. İhtiyaçlar hiyerarşisindeki ilk basamak olan fizyolojik ihtiyaçların karşılanabilmesi noktasında, savaş ve çatışma bölgelerinde yaşayan ve ekonomik statünün düşük olduğu Afganistan, Irak gibi ülkelerde örgütün eleman bulabildiği söylenebilmektedir. Güvenlik ihtiyacı hem güvenli ortam hem de psikolojik olarak güvende hissetme arayışı içinde olan bireyleri radikalleşme sürecine itebilmektedir. Özellikle tehdit algısının yüksek olması, fiziksel bir güvenlik sorunu olmasa da kişinin güvende hissetmemesine neden olabilmektedir. El-Kaide, dinin aşağılandığını düşündüğü durumları işgal olarak algılamakta ve bu durumu düzeltebilmek için güvenlik arayışına girmektedir. Sevgi ve ait olma ihtiyacındaki bir birey için örgütün kardeş vurgusu ve benzer düşüncelere sahip insanların bir arada bulunmasının getirdiği ait olma hissi radikalleşmeye itebilecek bir unsurdur. Saygınlık, başarı ve özgürlük gibi öz saygı ihtiyaçları ve diğerlerinden saygı görme ihtiyacının getirdiği 3N yaklaşımında ifade edilen önem arayışı olarak iki kategoride incelenmiştir. Önem kaybı konusunda, El-Kaide için bireyselden çok grubun dini

kimliğinin aşağılanması sonucu oluşan adaletsizlik ve mağduriyet duygusunun giderilme ihtiyacı ile önem arayışına girildiği; önem kaybı ihtimali hususunda ise yapılan eylemin başarısız olma ihtimalinin getireceği utanç duygusunun önemli olduğu ve önem kazanma ihtiyacı için şehitlik ve kahramanlık gibi unsurların etkili olduğu tespit edilmiştir. Bilişsel ihtiyaç kategorisinde ise yorumlama ve anlamlandırma ihtiyacının ön planda olduğu, çünkü kişisel düşüncelerin ve şiddet eylemlerinin çelişmesi sonucu oluşabilecek bilişsel uyumsuzluk halinin giderilmesi için kavramların yeniden yorumlanarak eylemlerin meşrulaştırılmasının ve düşüncelerin rasyonelleştirilmesinin söz konusu olduğu tespit edilmiştir. Estetik ihtiyaç konusunda cennet kavramı üzerinden güzellemelerin yapıldığı ve doğallığın vurgulandığı görülmüştür. Kendini gerçekleştirme ihtiyacının kişinin kimliğinin oluşturulması ile yakından alakalı olduğu, örgütte mücahit kimliğinin oluşturulmasında dinin ve silahın önemli olduğu tespit edilmiştir. Hiyerarşideki son aşama olan kendini aşma ihtiyacı için ise örgütün şehitlik operasyonları olarak adlandırdığı eylemler sonucu Allah'a yaklaşma ve cenneti arama isteğinin söz konusu olduğu görülmüştür.

Terörizm olgusunu şekillendiren şiddetle radikalleşme sürecinde sosyolojik unsurlar çerçevesinde ise 3N teorisindeki diğer iki kavram olan anlatılar ve grup dinamikleri üzerinden inceleme yapılmıştır. Anlatıların şiddet eylemlerini meşrulaştırmada üç aşamadan oluştuğu belirtilmiştir. İlk olarak, örgütün "biz ve diğerleri" ayrımını, örgütü destekleyen Sünni Müslümanlar olarak "kendileri" ve başta Amerika olmak üzere örgütü desteklemeyen "diğerleri" olarak ifade ettikleri tespit edilmiştir. İkinci olarak, şiddetin uygun cevap olduğuna dair seçilmiş travmaların anlatılması, dini kitaba atıf ve insanlıktan çıkarma yöntemlerinin kullanıldığı görülmüştür. Son olarak ise şiddeti kullanarak amaca ulaşma ihtimalinin yüksek olduğu algısının oluşturulması için seçilmiş zaferlere vurgu yapıldığı değerlendirilmiştir. Grup dinamikleri incelendiğinde ise örgütlü yapının etkisi, fikir birliğine teşvik ve grup kimliği ile birleşerek kendini feda etme isteğinin önemli olduğu tespit edilmiştir.

Sonuç olarak, literatürde bahsedilen radikalleşme süreçlerinden hareketle, dini motivasyonlu radikal terör örgütlerinde; ait olma ihtiyacı, önem kazanma arayışı, anlatılar yoluyla örgüte ve şiddet eylemlerine meşruluk kazandırma çabası gibi birçok psiko-sosyal etmenin ortak özellikler olduğu tespit edilmiştir. Ayrıca, yapılan bu araştırmada da görüldüğü üzere kullanılan "ihtiyaçlar hiyerarşisi" ve "3N yaklaşımı" teorileri terörizm

olgusuna psiko-sosyal bir yaklaşım sunmaktadır. Dolayısıyla bu teoriler kullanılarak El-Kaide terör örgütünün belgeleri üzerinden yapılan söylem analizi neticesinde ulaşılan sonuçlar, gelecek araştırmalarda terörizmin ve radikalleşmenin nedenlerinin incelenmesinde hem psikoloji ve sosyoloji alanlarından hem de diğer alanlardan çeşitli yaklaşımların bir bütün olarak farklı örgütler üzerinden de değerlendirilmesinin mümkün olabileceğini göstermektedir.

KAYNAKÇA

Abbasi, I., Khatwani, M. K., & Soomro, H. A. (2017). A review of psycho-social theories of terrorism. *Grassroots*, *51*(2), 319-333. https://www.researchgate.net/publication/322896417_A_REVIEW_OF_PSYCHO-SOCIAL_THEORIES_OF_TERRORISM

Afghani Opportunity. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Afghani%20Opportunity.pdf

Al-Attar, Z. (2019). *Extremism, radicalisation & mental health: Handbook for practitioners*. RAN H&SC.

al-Libi, A. Y. (t.y.). *Do not ignore the plank and look for the speck*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Do%20not%20ignore%20the%20plank%20and%20look%20for%20the%20speck.pdf

al-Libi, A. Y. (2010). *Some advice for the Mujahidin.* Erişim Tarihi: 7 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Some%20Advice%20for%20the%20Mujahidin.pdf

al-Qurashi, A.-D. (t.y.). *Verbally Released doc for Naseer trial*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Verbally%20Released%20doc%20for%20Naseer%20trial.pdf

al-Zawahiri, A. (2003). *Letter from Al-Zawahiri dtd August 2003*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Letter%20from%20Al-Zawahiri%20dtd%20August%202003.pdf

Al-Qar'awi, S. A. (2010). *A Letter to the Sunnah people in Syria*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/A%20Letter%20to%20the%20Sunnah%20people%20in%20Syria.pdf

Al-Somali. (t.y.). *Terror Franchise*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Terror%20Franchise.pdf

Bandura, A. (1977). *Social learning theory*. Prentice Hall.

BBC News. (2011, Haziran 16). *Ayman al-Zawahiri appointed as al-Qaeda leader*. Erişim Tarihi: 3 Nisan 2025. https://www.bbc.com/news/world-middle-east-13788594

Bin Ladin, O. (t.y.). *Letter from UBL to Atiyah*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Letter%20from%20UBL%20to%20Atiyah.pdf

Bin Ladin, U. (2002a). *Full text: Bin Laden's "Letter to America"*. The Observer. Erişim Tarihi: 3 Nisan 2025. https://web.archive.org/web/20040615081002/http:/observer.guardian.co.uk/worldview/story/0,11581,845725,00.html

Bin Ladin, U. (2002b). *Letter to the American people*. Erişim Tarihi: 3 Nisan 2025. https://www.dni.gov/files/documents/ubl/english/Letter%20to%20the%20American%20people.pdf

Bin Ladin, U. (2006). *The Eulogy of the Nation's Martyr 30 June 2006*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/The%20Eulogy%20of%20the%20Nation's%20Martyr%2030%20June%202006.pdf

Blommaert, J. (2005). *Discourse: A critical introduction*. Cambridge University Press.

Borum, R. (2011a). Radicalization into violent extremism I: A review of social science theories. *Journal of Strategic Security*, *4*(4), 7-36. https://doi.org/10.5038/1944-0472.4.4.1

Borum, R. (2011b). Radicalization into violent extremism II: A review of conceptual models and empirical research. *Journal of Strategic Security*, *4*(4), 37-62. https://doi.org/10.5038/1944-0472.4.4.2

Channel 4 News (Direktör). (2018, Haziran 5). *I was an MI6 spy inside Al-Qaeda* [Video recording]. https://www.youtube.com/watch?v=CGc08LI2WlQ

Channel 4 News (Direktör). (2022, Haziran 15). *Inside Al Shabaab: The extremist group trying to seize Somalia* [Video recording]. https://www.youtube.com/watch?v=KVSw0E9Y1RI

Chulov, M. (2018, Ağustos 2). My son, Osama: The al-Qaida leader's mother speaks for the first time. Erişim Tarihi: 3 Nisan 2025. *The Guardian.* https://www.theguardian.com/world/2018/aug/03/osama-bin-laden-mother-speaks-out-family-interview

Cook, G. (1989). *Discourse*. Oxford University Press.

Crayton, J. W. (1983). Terrorism and the psychology of the self. İçinde L. Z. Freedman & Y. Alexander (Ed.), *Perspectives on terrorism* (ss. 33-41). Scholarly Resources.

Crenshaw, M. (1981). The causes of terrorism. *Comparative Politics, 13*(4), 379. https://doi.org/10.2307/421717

Dagher, M., Kaltenthaler, K., Gelfand, M. J., Kruglanksi, A., & McCulloh, I. (2023). *ISIS in Iraq: The social and psychological foundations of terror* (1. bs). Oxford University PressNew York. https://doi.org/10.1093/oso/9780197524756.001.0001

Dear Muslim brothers and sisters. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Dear%20Muslim%20brothers%20and%20sisters.pdf

Draft Speech About Iran and America with Mahmud's Comments. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Draft%20Speech%20About%20Iran%20and%20America%20With%20Mahmud's%20Comments.pdf

Duties of administrators. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2017/english/Duties%20of%20administrators.pdf

Elliott, M. (2002, Şubat 16). *The Shoe Bomber's World*. Time World. Erişim Tarihi: 3 Nisan 2025. https://web.archive.org/web/20130827143428/http:/www.time.com/time/world/article/0,8599,203478,00.html

Enfâl Suresi. (2025). Erişim Tarihi: 21 Mayıs 2025. İçinde Kur'an. https://www.kuranmeali.com/AyetKarsilastirma.php?sure=8&ayet=60

European Commission. (2024). *The root causes of violent extremism*. European Union. https://home-affairs.ec.europa.eu/document/download/63770ad9-8c0b-44c4-a568-254bb22a8009_en?filename=ran_root_causes_of_violent_extremism_ran storp_meines_july_2024.pdf&prefLang=de

European Commission's Expert Group on Violent Radicalisation. (2008). *Radicalisation processes leading to acts of terrorism*. https://www.clingendael.org/sites/default/files/pdfs/20080500_cscp_report_vries.pdf

Festinger, L. (1957). *A theory of cognitive dissonance*. Stanford University Press.

Hudson, R. A. (1999). *The sociology and psychology of terrorism: Who becomes terrorist and why*. Federal Research Division, Libray of Congress. https://www.aclu.org/sites/default/files/field_document/ACLURM054164.pdf

Kaşıkcı, T., & Bülbül, G. D. (2023). Selefi-cihadi örgütlerin karşılaştırmalı analizi: El Kaide ve IŞİD örneği. *Türkiye Ortadoğu Çalışmaları Dergisi*, *9*(2), 89-134. https://doi.org/10.26513/tocd.1148920

Kerküklü, Ö. (2023). Psikolojik perspektiften Ortadoğu'da terör yapılanmaları; reaksiyon ve istismar (El Kaide ve IŞİD örneği). *Akademi Sosyal Bilimler Dergisi*, *10*(28), 85-97. https://doi.org/10.34189/asbd.10.28.006

Kizilhan, J. I., & Steger, F. (2021). The socialpsychology of Islamist terror – interdisciplinary perspectives on violence and ISIS totalitarian structures. *Global Security: Health, Science and Policy*, *6*(1), 26-37. https://doi.org/10.1080/23779497.2021.1927796

Koltko-Rivera, M. E. (2006). Rediscovering the later version of Maslow's hierarchy of needs: Self-transcendence and opportunities for theory, research, and unification. *Review of General Psychology*, *10*(4), 302-317. https://doi.org/10.1037/1089-2680.10.4.302

Kurt, S., & DemiRat, V. (2024). Dinin bir referans nesnesi olarak güvenlikleştirilmesi: El-Kaide örneği. *Ortadoğu Etütleri*, *15*(4), 293-322. https://doi.org/10.47932/ortetut.1397497

LADbible Stories (Direktör). (2021, Şubat 14). *Life As A Spy Inside Al-Qaeda | Minutes With | UNILAD* [Video recording]. https://www.youtube.com/watch?v=Pxij_nd3BAA

Last words of a terrorist. (2001). Erişim Tarihi: 3 Nisan 2025. *The Guardian.* https://www.theguardian.com/world/2001/sep/30/terrorism.september113

Letter Addressed to Atiyah. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Letter%20Addressed%20to%20Atiyah.pdf

Letter Implications of Climate Change. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Letter%20Implications%20of%20Climate%20Change.pdf

Letter to Abd al Rahman. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english2/Letter%20to%20Abd%20al%20Rahman.pdf

Letter to Abu Basir. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Letter%20to%20Abu%20Basir.pdf

Letter to aunt. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2017/english/Letter%20to%20aunt.pdf

Letter to our honorable Shaykh. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Letter%20to%20our%20honorable%20Shaykh.pdf

Letter to the Muslim Nation on Eid al-Adha. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Letter%20to%20the%20Muslim%20Nation%20on%20Eid%20al-Adha.pdf

Letter to Uthman. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Letter%20to%20Uthman.pdf

Mâide Sûresi. (2025). Erişim Tarihi: 3 Nisan 2025. İçinde *Kur'an*. https://www.kuranvemeali.com/maide-suresi/32-ayeti-meali

Maslow, A. H. (1943). A theory of human motivation. *Psychological Review*, *50*(4), 370-396. https://doi.org/10.1037/h0054346

Maslow, A. H. (1970). *Motivation and personality*. Harper & Row. https://www.holybooks.com/wp-content/uploads/Motivation-and-Personality-Maslow.pdf

Maslow, A. H. (1976). *Religions, values, and peak experiences*. Penguin.

McDermott, T. (2005). *Perfect Soldiers: The 9/11 Hijackers: Who They Were, Why They Did It*. Harper Collins.

Message for all Muslims following US State of the Union Address. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Message%20for%20all%20Muslims%20following%20US%20State%20of%20the%20Union%20Address.pdf

Message for general Islamic nation. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl/english/Message%20for%20general%20Islamic%20nation.pdf

Moghaddam, F. M. (2005). The staircase to terrorism: A psychological exploration. *American Psychologist*, *60*(2), 161-169. https://doi.org/10.1037/0003-066X.60.2.161

Morf, C. C., & Rhodewalt, F. (2001). Unraveling the paradoxes of narcissism: A dynamic self-regulatory processing model. *Psychological Inquiry*, *12*(4), 177-196. https://doi.org/10.1207/S15327965PLI1204_1

National Geographic (Direktör). (2008, Şubat 14). *Bin Laden's Beginnings | Inside the Taliban* [Video recording]. https://www.youtube.com/watch?v=D_aENuLFBn8

Nickerson, R. S. (1998). Confirmation Bias: A Ubiquitous Phenomenon in Many Guises. *Review of General Psychology*, *2*(2), 175-220. https://doi.org/10.1037/1089-2680.2.2.175

Office of the Director of National Intelligence. (2015, Mayıs 20). *Bin Laden's bookshelf*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/index.php/features/bin-laden-s-bookshelf?start=3

Office of the Director of National Intelligence. (2016, Mart 1). *Bin Laden's bookshelf*. Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/index.php/features/bin-laden-s-bookshelf?start=2

Oots, K. L., & Wiegele, T. C. (1986). Terrorist and victim: Psychiatric and physiological approaches from a social science perspective. *Terrorism*, *8*(1), 1-32. https://doi.org/10.1080/10576108608435592

Önenli Güven, M. (2022). Radikalleşme süreçleri: PKK örneği. *Journal of Terrorism and Radicalization Studies*, *1*(1), 130-152. https://doi.org/10.29228/trad.5

Özyılmaz Kiraz, B. (2016). A social psychological approach to the conduct of Al-Qaeda terrorism. *TESAM Akademi Dergisi*, *3*(1), 81-97.

Recommendations for the Mujahidin Entering Afghanistan. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Recommendations%20for%20the%20Mujahidin%20Entering%20Afghanistan.pdf

Ross, J. I. (1993). Structural causes of oppositional political terrorism: Towards a causal model. *Journal of Peace Research, 30*(3), 317-329. https://www.jstor.org/stable/424809

Schmid, A. (2013). Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. *Terrorism and Counter-Terrorism Studies*. https://doi.org/10.19165/2013.1.02

Schmid, A. P., & Jongman, A. J. (1988). *Political terrorism: A new guide to actors, authors, concepts, data bases, theories, and literature*. Routledge.

Second letter to Muslim brothers in Iraq. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/Second%20letter%20to%20%20Muslim%20brothers%20in%20Iraq.pdf

The Infographics Show (Direktör). (2023, Ocak 4). *Why Osama bin Laden Attacked the US* [Video recording]. https://www.youtube.com/watch?v=HHPX_QdI804

Thomas, C. (2024). Al Qaeda: Background, Current Status, and U.S. Policy. *Congressional Research Service*. https://crsreports.congress.gov/product/pdf/IF/IF11854

To the Islamic Community in General. (t.y.). Erişim Tarihi: 3 Nisan 2025. https://www.odni.gov/files/documents/ubl2016/english/To%20the%20Islamic%20Community%20in%20General.pdf

Volkan, V. D. (1993). *Etnik Terörizmin Psikolojisi* (C. 1). Politik Psikoloji Yayınları.

Webber, D., & Kruglanski, A. W. (2017). Psychological Factors in Radicalization: A "3 N" Approach. Içinde G. LaFree & J. D. Freilich (Ed.), *The Handbook of the Criminology of Terrorism* (1. bs, ss. 33-46). Wiley. https://doi.org/10.1002/9781118923986.ch2

Terörizm ve Radikalleşme Araştırmaları Dergisi-TRAD, 2025, 4(2) : 223-265 Araştırma Makalesi
Journal of Terrorism and Radicalization Studies-TRAD, 2025, 4(2): 223-265 Research Article
DOI: 10.61314/traddergi.1618580

CYBERSECURITY IN CRITICAL INFRASTRUCTURES AND CYBER TERRORISM: A STRATEGIC ANALYSIS ON TÜRKİYE

Seçkin AKÖZ[*], Hatice SÜRURİ[**]

ABSTRACT

Cyber-attacks that may pose a threat to critical infrastructures (CI) have the potential to cause wide-ranging negative effects ranging from economic losses to service interruptions and social chaos. Türkiye is in a high-risk group against cyber-attacks due to its strategic geographical location and rapidly digitalizing infrastructures. Denial of service attacks on energy grids, ransomware threats in health infrastructures and data breaches on banking systems are concrete examples of the cyber security vulnerabilities that Türkiye faces. The study addresses the global dimension of cyber threats by taking into account large-scale cyber-attacks experienced internationally and examines the local effects of these threats with examples specific to Türkiye. The study evaluates Türkiye's current policies, legal regulations and defense strategies against threats. In the fight against cyber threats, the development of domestic and national technologies, strengthening cooperation at global, regional, national, international and institutional levels, international information sharing and the establishment of proactive response mechanisms against cyber threats are among the prominent strategic measures. In this context, cyber security is not only a technical issue; it is a necessity in terms of national security, economic sustainability and social stability.

Keywords: *Critical Infrastructures, Cybersecurity, Cyberterrorism, Türkiye, National Strategy, National Security*

KRİTİK ALTYAPILARDA SİBER GÜVENLİK VE SİBER TERÖRİZM: TÜRKİYE ÜZERİNE STRATEJİK BİR İNCELEME

ÖZET

Kritik altyapılara yönelik tehdit unsuru oluşturabilecek siber saldırılar, ekonomik kayıplardan, hizmet kesintilerine ve toplumsal kaosa kadar geniş kapsamlı olumsuz etkilere yol açabilecek potansiyeli barındırmaktadır. Türkiye, stratejik coğrafi konumu ve hızla dijitalleşen altyapıları nedeniyle siber saldırılara karşı yüksek risk grubunda yer almaktadır. Enerji şebekelerine yönelik hizmet reddi saldırıları, sağlık altyapılarındaki fidye yazılım tehditleri ve bankacılık sistemlerine yönelik veri ihlalleri, Türkiye'nin karşı karşıya olduğu siber güvenlik zafiyetlerinin somut örnekleridir. Çalışma, uluslararası düzeyde yaşanan büyük çaplı siber saldırılardan yola çıkarak, siber tehditlerin küresel boyutunu ele almakta ve Türkiye özelindeki örneklerle bu tehditlerin yerel etkilerini incelemektedir. Çalışmada tehditlere karşı Türkiye'nin mevcut politikaları, yasal düzenlemeleri ve savunma stratejileri değerlendirilmektedir. Siber tehditlerle mücadelede, yerli ve milli teknolojilerin geliştirilmesi, küresel, bölgesel, ulusal, uluslararası ve kurumsal düzeyde işbirliklerinin güçlendirilmesi, uluslararası bilgi paylaşımı ve siber tehditlere yönelik proaktif müdahale mekanizmalarının oluşturulması öne çıkan stratejik önlemler arasında yer almaktadır. Bu kapsamda, siber güvenlik, yalnızca teknik bir mesele değil; ulusal güvenlik, ekonomik sürdürülebilirlik ve toplumsal istikrar açısından bir zorunluluktur.

Anahtar Kelimeler: *Kritik Altyapılar, Siber Güvenlik, Siber Terörizm, Türkiye, Ulusal Strateji, Ulusal Güvenlik*

[*] Bağımsız Araştırmacı, Güvenlik Bilimleri Uzmanı, akzseckin@gmail.com. ORCID: 0000-0003-3233-1552.

[**] Dr. Gebze Teknik Üniversitesi Teknopark, haticesururi@gmail.com, ORCID: 0000-0003-0717-3230.

INTRODUCTION

As digitalization accelerates, critical infrastructures (CI) have become the building blocks of national security and social order. While the digitalization of vital systems such as energy, health, finance and transportation has increased the efficiency and accessibility of these infrastructures, it has also brought new security risks. This study aims to evaluate the cyber threats inherent in digitalized infrastructures and to reveal strategic approaches that can be developed against these threats, especially in Türkiye. As an inevitable consequence of digitalization, cybersecurity has become not only a technological issue but also a threat to the political and economic stability and national security of countries. Digital attacks on critical infrastructures can lead to a wide range of negative effects, from service interruptions to data theft, from economic losses to social chaos (Lewis, 2019, p.21). In this context, it is inevitable that cybersecurity will become a priority issue in digitalizing infrastructures. Any disruption to the functioning of critical infrastructures affects not only the individuals using these systems, but also other sectors due to interdependence between systems. Therefore, it is imperative for states to implement holistic cybersecurity policies in order to maintain national security and political stability.

Cyber terrorism threatens the security of individuals, societies and states through the malicious use of information technologies, targets critical infrastructures and aims to create fear and panic in society. Within the scope of this study, the multi-layered risks posed by cyber terrorism, both physically and digitally, are analyzed and the destructive effects of these risks on critical infrastructures are evaluated. In the information ecosystem where the physical world and the virtual world intersect, the primary targets of cyber terrorism include vital areas such as energy grids, health systems, air traffic control systems, telecommunications and financial infrastructures (Collin, 1997, p.15). The scale of these threats is not only limited to damaging individual infrastructures, but also has the potential to create instability by changing interstate dynamics in international relations and undermining global peace (Dubyna et al. 2024, p. 6952). In this framework, cyber threats are complex, destructive and challenging for states. To combat malicious cyber threats, international organizations such as the European Union (EU), the Organization for Security and Cooperation in Europe (OSCE), the United Nations (UN) and NATO (North Atlantic Treaty

Organization) focus on strategies to detect, prevent and respond to cyber-attacks (NATO, 2024). In this context, in 2016, NATO declared cyberspace as an area of operation against possible ultimate threats and developed cyber defense policies based on deterrence, defense, crisis prevention, management and cooperation to combat cyber threats (NATO, 2024).

It is observed that the effects of cyber terrorism and attacks are not only limited to short-term disruptions, but also damage public confidence and the sustainability of strategic sectors. Türkiye's focus on technological innovations, legal regulations and international cooperation in combating these threats is of vital importance for the management of these risks. Türkiye is in position more vulnerable to these threats due to its strategic location and rapidly developing digital infrastructures. As an important energy transit point on both national and regional scales, Türkiye is becoming one of the primary targets of cyber terrorism due to its geopolitical importance. This situation necessitates Türkiye to adopt a more comprehensive and holistic approach in its cyber security strategies. This article discusses the vulnerability of critical infrastructures in the face of digital threats, strategically analyzes Türkiye's current situation, and proposes concrete solutions to improve cybersecurity.

1. THE IMPORTANCE OF CRITICAL INFRASTRUCTURES IN INTERNATIONAL SECURITY IN A DIGITALIZING WORLD

The digital transformation of the 21st century has radically changed not only technology but also the understanding of international security. Access to information has become significantly easier, and the boundlessness of communication has reached alarming proportions. This situation has reshaped the security priorities of states. Wars are no longer confined to the battlefield; they now occur in energy lines, data centers, satellites, and even hospital systems. As a result, protecting critical infrastructure has ceased to be merely a technical task and has become a political, economic, and strategic necessity.

Globalization and the developments that accompany it demonstrate that today, a country's security is measured not only by its military power but also by the robustness of its water resources, energy systems, and financial infrastructure. In today's global security structure, states must be prepared not only for traditional threats but also for new risks brought about by the

digital age. Threats such as cyberattacks, infrastructure sabotage, and AI-driven information manipulation have reached a borderless, complex, and often unpredictable dimension. Therefore, the protection of critical infrastructure lies at the heart of not only national security policies but also international cooperation and strategic partnerships. While digitalization has made security more complex, it has also exposed vulnerabilities more quickly. For this reason, developing a layered, comprehensive, and proactive security approach for infrastructure now forms the foundation of modern security understanding.

1.1. International Security and Critical Infrastructures in the Digitalizing World

Critical infrastructures are the physical and virtual systems necessary to ensure the continuity of the basic functions of societies and have a central role in the functioning of societies. Any failure or attack on critical infrastructure systems has the potential to directly threaten national security Critical infrastructures consist of "systems, assets and networks, whether physical or virtual" (NATO, 2021). These systems, which provide essential services such as energy, transportation, health and finance, have become smarter, more connected and more efficient as digitalization has accelerated.

However, this transformation has increased the vulnerability of critical infrastructures to cyber threats by expanding the attack surface. In this context, especially energy grids and telecommunication infrastructures are becoming targets due to the widespread use of digital control systems (Ercan, 2015, p. 4). Since critical infrastructures generate and store data on a large scale, the security of this data creates domino effects that can affect not only the organizations that provide services, but also society as a whole. Therefore, it is inevitable that the digitalization process should be addressed together with security.

The protection of critical infrastructures is not only a technical problem, but also a strategic priority in terms of national security and social order. In the process shaped by the digital transformation of society, the dependence on digital infrastructure is increasing exponentially, and the proliferation of information and communication technologies in critical infrastructures makes these systems more complex and dynamic (KAS & EDAM, 2022, p. 10). In this context, the development of national and international

cybersecurity strategies, technology-oriented solutions and the integrated operation of legal regulations play a critical role in protecting critical infrastructures against cyber threats.

New security paradigms are needed to manage these threats brought about by digitalization and to increase the resilience and durability of infrastructure systems. As cyber threats are expected to become more complex in the future, strengthening these infrastructures within the framework of cyber security has become a common responsibility at both national and international levels. With the change in the dynamics of security understanding in the global framework and digitalization, a large number of threats have dominated the international arena. With the existence of new threats, non-traditional asymmetric threats have framed national and international competition and opened a space where the resilience of states and political powers is tested. These asymmetric threats are considered to be the products of the new world order in the field of defense. With modernity, the concept of total war has brought the speed of instant communication to the forefront with the changes in information and machine technologies.

In this new field of competition, cyber threats to critical infrastructures have been explicitly recognized as a significant threat element in NATO's 2022 Strategic Concept (NATO, 2024). This explicit recognition is particularly important for the academic and strategic literature, as NATO's strategic doctrines serve as normative frameworks that influence the cybersecurity and defense postures of member states (NATO, 2024).

NATO's framing of cyber threats as collective security issues provides not only a policy direction but also a theoretical foundation for understanding cyber conflict in international relations. NATO emphasizes operational strategies for defense, resilience, and the stability of the alliance by developing systems integrated with artificial intelligence strategies against external interventions targeting the protection of critical infrastructures. This integration of emerging technologies into strategic defense frameworks marks a paradigm shift in cybersecurity governance and has been highlighted in literature as a move toward anticipatory security models (Bellanova et al., 2022, p. 337). In this framework, international organizations such as NATO (North Atlantic Treaty Organization), OSCE, UN, and EU (European Union) are developing measures to increase resilience by improving national defense capacities, ensuring secure access

to critical infrastructures, and providing alternative defense perspectives in times of crisis (NATO, 2024). Such coordinated institutional efforts reflect what Deibert (2019) terms the "securitization of cyberspace," where cyber resilience becomes a shared transnational responsibility rather than a solely national concern. In this context, the concept of cyber resilience comes to the forefront as a critical solution within cyber security strategies due to the increasing complexity and frequency of cyber threats. As Carrapico and Barrinha (2018) emphasize, the inclusion of cyber resilience in NATO doctrine signals a growing recognition of the need for adaptive, multi-layered defense structures in the face of persistent and asymmetric threats. Therefore, NATO's approach not only informs operational practices but also contributes Therefore, NATO's approach not only informs operational practices but also makes a significant contribution to the academic literature on collective" defense, digital sovereignty and strategic adaptation in the era of hybrid warfare.

1.2. Converging Threats in International Security

In the digital age, the line between cybercrime and cyber terrorism has increasingly blurred, giving rise to converging threats that pose significant risks to national and international security. As Lewis (2019) argues, cyber capabilities now allow both state and non-state actors to target critical infrastructures with disruptive, and at times, destructive intent. Particularly in geopolitically exposed countries like Türkiye, the convergence of cyberattacks with broader terror strategies has made cyberterrorism a tool not just for disruption, but for political signaling and psychological impact.

The growing sophistication of attacks on energy grids, financial networks, and public institutions demonstrates that these threats are no longer hypothetical but operational realities (Radziwill, 2018). The 2023 and 2024 ransomware attacks on Turkish public institutions and the 2020 assault on gas distribution networks are stark examples of how intertwined cyber and physical security domains have become (Kriter Dergi, 2023; Kandır, 2025). As threats evolve in complexity and attribution becomes increasingly difficult, national cyber defense strategies must adapt by integrating intelligence, infrastructure resilience, and international cooperation mechanisms (Rid & Buchanan, 2015). Thus, cyber security and cyber terrorism should no longer be treated as separate policy domains, but rather as intersecting dimensions of a comprehensive national security paradigm.

1.2.1. Cyber Security and Cyber Terrorism

Cyber security and cyber-attacks in cyberspace have become one of the most important security issues and threats of the digital age. Cyberspace, as a strategic area beyond mere technological infrastructures, represents a multi-dimensional battlefield where security, sovereignty and power dynamics come together (Kello, 2013).The concept of cyberspace encompasses not only Internet-based systems but also unmanned aerial vehicles, airplanes, radio systems and all information systems (Libicki, 2009, p.12). Unlike traditional security paradigms where physical barriers define territorial control, cyberspace blurs these boundaries, creating an asymmetric and decentralized threat environment (Rid, 2011). In cyberspace, which is defined as an "interdependent network", attackers resort to DDoS (Distributed Denial of Service) attacks to damage the availability of internet systems, and more recently to the more effective and alarming ransomware. In this context, cyber threats are deliberate attacks aimed at disrupting, disrupting or completely destroying the computer systems and critical infrastructures of the target audience (Lin, 2010, p.63). In cyberspace, where information becomes a target for attacks, all strategies designed within the framework of establishing information security have built the concept of cyber security.

Cyber terrorism is characterized by terrorist groups' efforts to damage critical infrastructures, create social fear and achieve political goals by using digital tools. DDoS attacks are among the methods frequently used by sub-state terrorist groups. DDoS attacks overload target systems with excessive data, disabling their functions and disrupting infrastructure services (Bayrakçı & Koçman, 2023, p. 188). DDoS attacks are usually carried out by networks called botnets, which consist of a group of computers hijacked with malicious software. These attacks can cause serious operational damage to states by making the targeted systems vulnerable and they are also highly attractive due to the attackers' ability to conceal their identities. Such tactics highlight how cyberspace provides an opportunity for asymmetric warfare, in which non-state actors can challenge state authority without engaging in conventional military conflicts (Arquilla & Ronfeldt, 1996; p.4).

Cyber terrorism has the potential to cause large-scale economic and social damage at both individual and institutional levels. For example, an attack on energy grids can not only affect the national economy, but also

other infrastructures such as health systems (Yılmaz & Sağıroğlu, 2013). The vulnerability of critical infrastructures to such attacks makes it imperative for countries to give greater priority to cyber security policies in their national security strategies. In this context, the securitization of cyberspace has led to a paradigm shift, where digital assets are now treated as critical components of national security and necessitating coordinated international responses (Dunn Cavelty, 2008). In the future, cyber-attacks supported by the Internet of Things and artificial intelligence are expected to increase. In this context, adopting an approach supported not only by technological solutions but also by legal regulations and international cooperation will be inevitable in the fight against cyber terrorism. Moreover, cooperation with international organizations (NATO, UN and EU, etc.) are among the factors that can play a key role in managing these threats. For example, NATO has accepted cyberspace as an operational domain by integrating cyber resilience into its collective defense strategy (NATO, 2021). In countries like Türkiye that are rapidly developing their digital infrastructures, it is critical to include individuals in the digital security chain through education and awareness activities.

In cyber security, it is inevitable to develop resilient defense mechanisms against cyber threats. Early warning systems and threat analysis tools that will create resilience against cyber threats ensure that attacks are detected early and damages are minimized (Şeker, 2020, p.114). In addition, information sharing and coordination among international organizations can also form an effective defense mechanism against cyber threats (NATO, 2021, p.12). National policies to mitigate the effects of cyber threats need to cover not only technical but also economic and social dimensions. In order to fully address the geopolitical impacts of cyber threats, state actors need to go beyond traditional deterrence models and adopt multidimensional security strategies that include cyber intelligence, digital diplomacy and cross-Dectoral cooperation (Tikk & Kerttunen, 2020). In particular, to prevent economic losses, the resilience and resilience of critical infrastructures should be increased and regular stress tests should be implemented. Consequently, governance of cyberspace requires a hybrid approach that combines technological resilience, legal frameworks, and strategic alliances to counter the evolving nature of cyber threats.

1.2.1.1. Cyber Risks and Threats Affecting Critical Infrastructure

With the acceleration of digitalization, critical infrastructures have increasingly become targets of cyber threats. Vital sectors such as energy, water, transportation, and finance are subjected to attacks carried out by state-sponsored groups and organized crime syndicates. For example, in 2023, Chinese hacker groups infiltrated ports, energy grids, and telecommunications networks in the United States, demonstrating their capability to disable these infrastructures at will (The Wall Street Journal, 2025, p. 1). Similarly, in 2023, the Russia-linked group APT28 exploited a vulnerability in Microsoft Outlook to target the defense and technology sectors in Germany (The Guardian, 2024, p. 2).

The impact of cyberattacks is not limited to state-sponsored actors; financially motivated groups also target critical infrastructures. In 2023, a vulnerability in the MOVEit file transfer software was exploited by the ransomware group Cl0p, compromising the data of over 2,700 organizations worldwide (Robinson, 2025). This attack caused serious disruptions in sectors such as healthcare, finance, and public services.

Türkiye has also faced similar threats. In 2023, it ranked among the countries most affected by cyberattacks on a global scale. Iran-backed MuddyWater and Russia-linked groups targeted Türkiye's energy and telecommunications infrastructures (Kriter Dergi, 2023, p. 4). These attacks have once again underscored the importance of enhancing the country's cybersecurity capacity and protecting its critical infrastructures.

2. CYBER SECURITY AND CRITICAL INFRASTRUCTURES

In terms of cybersecurity, critical infrastructures has two dimensions: defense and offense. The rapid development in network technologies has led to decisions to manage critical infrastructure, which is vital for a state's national security and public functioning, through operating systems that rely heavily on internet technologies. Therefore, states engaged in power struggles within the international system can damage each other's critical infrastructure sectors and consider them as military targets. In this context, it is imperative for states to protect their critical infrastructure against cyber-attacks by investing in the defense capacity of these systems and trying to provide security for them. The other dimension is cyber-attack capacity. A state may seek to fully or partially damage an adversary state's critical infrastructure by seeking opportunities, developing capabilities in this

capacity, and conducting covert operations. These infrastructures not only cause economic losses if their functionality is disrupted, but also pose serious threats to national security and social order (Afyonluoğlu, 2020, p. 11). As part of a complex, interconnected ecosystem, their failure and destruction, whether physical or virtual, has the potential to weaken states in terms of national security, national public health and economic security (NIST, 2016).

Digitalization poses significant risk areas for states due to the potential for increased exposure to cyber-attacks and cybersecurity incidents, jeopardizing energy supply security, supply chains, public safety and the confidentiality of critical data for states. With the increase in cyber threats, the protection of these infrastructures has become a fundamental element of national security policies. Today, digitalization necessitates the implementation of not only physical security measures but also cyber security strategies in the defense of critical infrastructures. International organizations such as the EU and NATO create roadmaps and strategies at the level of awareness and preparedness to protect critical infrastructures within the scope of cyber security policies (EU, 2024). In this framework, the EU published the EU Security Union Strategy in 2020, aiming to ensure European security in both physical and digital areas covering the whole society at national level. While the focus of the strategy concept is on the energy sector, the strategy defined operational solution phases that can make critical infrastructures resilient against physical, cyber and hybrid threats. In strategically important countries such as Türkiye, the strategy focuses on international cooperation and local technology production for the protection of critical infrastructures, and establishes action and response plans with effective planning, monitoring and crisis management, prioritizing common minimum requirements.

2.1. Definition and Scope of Critical Infrastructure

Critical infrastructures are systems that are vital for a country's economic, social and national security. While sectors such as energy, health, transportation, communication and finance stand out in the definitions made by the European Union, new security risks arise with the integration of these systems (Karabacak, 2011, p. 2). The US Department of Homeland Security considers water supply, financial systems and communication infrastructures as critical infrastructures (Lee & Conway, 2022, p. 5). Critical

infrastructures are essential services that support society and serve as the backbone for its security (NIST, 2016). According to the US National Council for the Improvement of Public Service (1990), "critical infrastructure" is defined as facilities with long economic life, economic development, high fixed costs, and a tradition of public sector involvement (CRS, 2004, p.6). In this context, critical infrastructures are the structures that build the foundations of a strong economy and national security, including airports, water and energy resources.

The concept of critical infrastructure, which has been prominent in the EU and its member states since the early 2000s (Pursuianen, 2009, p.721), has also been discussed in a multidisciplinary manner in the literature. Russia has defined its critical infrastructure strategy within the framework of national security. In this context, in its approach focused on civil defense, emergencies and national security, critical infrastructures are based on human security within the framework of a comprehensive security approach. From a state-centered national security perspective, critical infrastructures are seen as a necessity to protect society and the state from internal and external threats, to protect systems that will guarantee the implementation of constitutional rights and freedoms, independence and sustainable economic development (Pursuianen, 2021, p.22)

AFAD's (Disaster and Emergency Management Presidency) definition of critical infrastructure is; "It is the whole of networks, assets, systems and temples that may pose serious threats to citizens, health, security and economy as a result of the negative impact on the environment, social order and public services when they do not fulfill their function partially or completely" (AFAD, 2014). In Türkiye, critical infrastructures include the energy, transportation, health and finance sectors, but communication infrastructures and digital systems are also becoming increasingly important (Demirci, 2021, p.54). However, a comprehensive national strategy and standards need to be developed for these infrastructures. In particular, energy infrastructures are one of the sectors that need to be protected as a priority due to Türkiye's geopolitical position. The scope of critical infrastructures is expanding with advancing technology and digitalization. In this context, Türkiye needs to make regulations in line with international standards and focus on local solutions to ensure the security of its infrastructures. In this context, in the event of cyber-attacks on critical infrastructures, states should

shape their cyber security strategies based on military, economic, civilian, social and psychological defense, as well as implement a resilience-based crisis management cycle. Resilience is the ability of a system to withstand and resist stress (Pursuianen, 2021, p.26). When faced with processes where service interruptions become difficult to prevent, it is inevitable to develop strategies that build redundancy and adaptive capabilities.

2.2. Importance of Cyber Security for Critical Infrastructures

Cyber security plays a key role in protecting critical infrastructures. Cyber security covers all activities carried out to ensure security in cyberspace. In this context, it is the existence of systems that can ensure confidentiality, integrity and accessibility criteria for cyber security (Ardielli & Ardielli, 2017, p.43). Violation of these three criteria in cyberspace means that there may be an existing threat. Especially when sectors such as energy, transportation and health systems are exposed to cyber-attacks and terrorist attacks, large-scale service interruptions and economic losses can occur. For example, the Black Energy (BE) cyber-attack on the Ukrainian energy infrastructure on December 23, 2015, has caused hundreds of thousands of people to experience unplanned power outages and demonstrated the vulnerability of critical infrastructures to cyber threats (Lee, Assante, & Conway, 2014, p.6). This attack demonstrated that remote access to energy grids can be used to take control of systems and cause large-scale damage and disruption. States' energy infrastructures are highly interdependent through transit gas pipelines or electricity transmission networks. In this context, the protection and resilience of the relevant infrastructure element will prevent system disruption (Zoli et al., 2018, p.4). Terrorist organizations and non-state actors also target critical infrastructures, especially where interdependence exists, to expand the sphere of influence of their mass actions. The academic draft approach to understanding the interdependencies of countries came to the forefront in the 2001s. The interconnected nature of critical infrastructures makes it important to identify the problems that may arise in each infrastructure in order to manage the related interdependencies. The problem is that when critical systems are considered holistically, the failure or damage that may occur in a single element of the system may be reflected in the whole system due to interdependencies. Therefore, an attack on systemically critical infrastructures may pose a risky threat that could disrupt the entire operation.

In Türkiye, when we evaluate critical infrastructures holistically, energy grids and healthcare systems are among the most vulnerable areas. Health infrastructures are particularly exposed to attacks such as ransomware. By encrypting patient data, attackers disrupt healthcare services and put patient safety at risk (Lewis, 2006, p.1). For example, the ransomware attacks against many hospitals in Europe and Türkiye in 2020 have once again highlighted the inadequacies in protecting these infrastructures.

Cyber security strategies should not be limited to technological solutions. Early warning systems and artificial intelligence-supported threat detection systems are at a level that will allow such such attacks to be detected in advance. In addition, the resilience of infrastructures should be increased by strengthening corporate collaborations. Türkiye's development of local software solutions in this area will reduce foreign dependency and increase its cyber defense capacity.

3. CYBER TERRORISM AND CRITICAL INFRASTRUCTURES

Cyber terrorism is a form of terrorism that targets society through attacks in the digital environment, usually aimed at creating fear and panic through cyber-attacks on states or critical infrastructures. This type of terrorism is considered a digital extension of traditional terrorism and is an expanding global threat in which individuals, institutions and states can be targeted. Considering cyber terrorism as an integral element of the digital domain, national security and intelligence-based digital surveillance has become an essential element of surveillance for states in the fight against cyber terrorism. In addition to the measures taken at the national level, the expansion of defensive practices by states against threats that may come with virtual surveillance has led to a decrease in risks in the context of national and international security.

The main purpose of cyber terrorism is to throw societies into economic and social chaos and to strain the capacity of states in crisis management (Singer & Friedman, 2014, p. 29). Such attacks are usually carried out by cyber criminals, hacker groups or terrorist organizations. Since cyber terrorism can be effectively carried out in the digital environment, its targets often cover a wider area compared to traditional terrorism. Especially the digital infrastructures of developed countries offer great opportunities for attackers. This situation shows that not only economic but also social and

psychological effects can be created cyber attacks. Critical infrastructures can be targeted by cyber terrorists and cause widespread effects that can stop the functioning of states or societies (Sağıroğlu & Alkan, 2018, p. 9). For example; In the Russia-Ukraine war, cyber attacks targeting Ukraine's critical infrastructures has been a cyber terror act linked to hacktivist groups designed by Russia.

According to intelligence sources, threats to critical infrastructures are increasingly being carried out by cybercriminal organizations and states carrying out "covert" actions. Cyber terrorism can directly affect societies through attacks on these critical infrastructures. The magnitude of the impact area of the related attacks is of a nature that can have long-term consequences not only economically but also socially and psychologically (Kurum, Bilgiç, & Çardak, 2022, p. 443). In this context, cyber security measures and strategies require not only technical solutions but also global coordination and more effective information sharing. Increasing inter-country solidarity will enable for a stronger fight against cyber threats.

From a policy perspective, states are planning cyber terrorism and terrorism as a growing threat in cyberspace and developing national security policy mechanisms using an "all-hazards awareness and preparedness model" based on risk and resilience, where multiple risk factors are addressed simultaneously. Terrorist organizations and sub-state groups also build critical infrastructures or aim to seize critical infrastructures in order to target critical points and carry out their actions (Asal et al., 2015, p.5). These emerging terrorist groups are pushing the boundaries and possibilities of critical infrastructures to serve the mass purposes of the organizations all for the sole purpose of action and expanding and their area and, to get one man closer to their course.

Cyber terrorism and the protection of critical infrastructures are of increasing importance for states. In this context, resistance against cyber threats should be increased by developing national security strategies, cyber security measures, international cooperation and cyber defense policies (Atasever, Özçelik & Sağıroğlu, 2019, p.239)**.** Protecting critical infrastructures against cyber-attacks is a policy necessity for states due to the destructive effects of digital technologies. In this context, cyber terrorism is a public responsibility for states to combat and prevent due to the limitlessness of the area it covers (Weiss & Biermann, 2021, p.1). The

rapidly evolving structure of technology requires continuous updating of cyber defense systems. This will enable states to prepared to identify, control and manage cyber-attacks and risks that may arise with a stronger and more flexible infrastructure.

3.1. Definition and Scope of Cyber Terrorism

Information systems and the digital space are considered as a vulnerable area and are placed in the target of terrorists. There for using information systems to determine a target area and plan an attack is one of the important stages of cyber terrorism activity (Jormakka and Mölsa, 2005). Parks and Duggan (2011) defined cyber terrorism as an extension of conventional terrorism and a new approach in which terrorist organizations take action in cyberspace to achieve their goals. Cyber terrorism refers to terrorist activities carried out in the digital environment and generally aims to create fear and panic in society through attacks on critical infrastructures. According to Pollitt, cyber terrorism is defined as "premeditated, ideologically motivated attacks on computer systems, non-combatant targets, computer programs and data by sub-national organizations and covert intelligence agents" (Pollitt, 1998). According to Evan Kohlmann (2008), cyber terrorism is defined as "any act of terrorism that takes place on the Internet". In this context, cyber terrorism is the use of the tools of the virtual world by terrorist organizations in cyberspace in attacks targeting online computers, networks and the information stored on them for communication, recruitment, coordination, fundraising on behalf of organizations, action planning and intelligence gathering (Kohlmann et al., 2008). Such attacks are carried out by non-state actors or state-sponsored groups and are considered the digital extension of traditional terrorism. The main objectives of cyber terrorism include threatening public security, targeting economic infrastructure and undermining public faith in state security (Singer & Friedman, 2014, p. 29). This reveals the complex nature and wide-ranging effects of cyberterrorism, as cyberattacks have a wider reach, with attacks taking place digitally rather than through physical violence (Sağıroğlu & Alkan, 2018, p. 37). According to Robert S. Mueller, cyber terrorists focus on combining physical attacks with cyber-attacks by recruiting from outside while training their members to carry out their actions in cyberspace (Nakashima, 2010). In this context, the fight against cyber-terrorism will not only be specific to states, but individual, society and state-related methods of struggle will be decisive.

Cyber terrorism also has the potential to surpass traditional terrorism with its social and psychological effects. Such attacks can create iimediate social fear and panic, while in the long run they can undermine confidence in the security and stability of the state (Kurum, Bilgiç, & Çardak, 2022, p. 458). While cyber security is becoming more important with each passing day, the complexity and impact of attacks are also increasing. This is because the global interconnectedness of digital systems allows an attack to spread rapidly over a wide area (Atasever, Özçelik, & Sağıroğlu, 2019, p. 238).

3.2. Differences between Cyber Terrorism and Traditional Terrorism

One of the main differences between cyber terrorism and traditional terrorism is the means used. While traditional terrorism uses physical violence and explosive devices to cause massive damage to targeted locations, cyber terrorism is more often a digital attack. Cyber terrorists often use digital tools such as computer viruses, ransomware and denial of service attacks (DDoS) to bring down the systems of targeted organizations or states (RAND Corporation, 2015, p. 21). In this context, traditional terrorism involves physical violence, geographical limitations, and visibility and high risk factors. Cyber terrorism, on the other hand, is a wide-area terrorism method in which attacks are carried out using digital tools such as computers, networks and software, and systems around the world can be targeted. Cyber terrorism is operationally covert, operationally low-risk and high-cost attacks.

These differences also make the impact of cyber terrorism more widespread because a cyber-attack can spread around the world in a few seconds and cause chaos on a global scale (Kurum, Bilgiç, & Çardak, 2022, p. 460). Attacks carried out in the digital environment leave fewer traces, it becomes much more difficult to track. This increases the impossibilities that attackers have to hide their identities and that states or organizations face when taking security measures (Atasever, Özçelik, & Sağıroğlu, 2019, p. 239).

3.3. Examples of Cyber Terrorism against Critical Infrastructure

3.3.1. International Cases

3.3.1.1. Estonia DDoS (Distributed Denial of Service) 2007 Attacks

The cyber-attacks on Estonia in 2007 are one of the most prominent examples of cyber-terrorism. Estonia was subjected to one of the most coordinated and comprehensive cyber-attacks against a single country to that date. The attacks took the form of Distributed Denial of Service Attacks (DDoS) on the websites of public organizations and the banking system. These attacks posed a serious threat to Estonia's digital infrastructure and led the country to take comprehensive measures in the field of cyber security (Sağıroğlu & Kanca, 2022, p. 70; Tikk & Kaska, 2010, p. 288). Estonia's rapid response to these attacks has been an important lesson on how to develop cyber defense strategies worldwide. The Estonian attacks not only affect inter-state relations, but also threaten the security of a nation's digital infrastructure. These attacks have demonstrated how critical the cyber defense capacities of states are and this highlights the importance of international cooperation in the field of cybersecurity (Singer & Friedman, 2014, p. 72).

3.3.1.2. Natanz Nuclear Facility Attack

The 2010 cyber-attack on Iran's Natanz Nuclear Facility was an example of cyber warfare as a real national security threat in the international arena. This attack was carried out with the use of a computer worm called Stuxnet and caused serious damage to Iran's nuclear program. Stuxnet is considered to be the most sophisticated and targeted computer virus (worm) ever discovered. It specifically targets industrial control systems and is designed to sabotage centrifuges used in Iran's nuclear facilities. After infiltrating the nuclear facility's networks, the Stuxnet worm manipulated the systems that control the speed of centrifuges (984 centrifuges), causing them to spin at excessive speeds and thus causing damage (Holloway, 2015; Kesler, 2011). The focus of the Stuxnet attack was the ability of the virus to penetrate deeply into targeted systems. The virus used various techniques to bypass the facility's firewall and remained undetected for a long time. The attack on the Natanz facilities opened a new dimension in international relations. It signaled that cyber threats, in addition to conventional warfare methods, could also affect international relations and even lead to conflicts. The attack increased international tension and antagonism between Iran and the other countries, causing states to take measures to increase their capacities in the cyber domain and invest more in defense systems.

4. CURRENT STATUS OF CRITICAL INFRASTRUCTURES IN TÜRKİYE

In the digital domain, where cyber-attacks have become prominent and are also used by sub-state groups, state-sponsored organizations and terrorist organizations, the protection of critical infrastructures has entered the agenda of national and international security. However, the threat posed by cyber-attacks has paved the way for states to focus on developing collective capabilities and capacities to respond to cyber-attacks, and to implement regulatory legal arrangements and strategic roadmaps between public and private institutions. Although there is disagreement in the literature on which factors should be included in the critical infrastructure classification, communication infrastructures, financial sector, commercial facilities, defense industry, emergency services, energy grids and nuclear facilities, transportation and information technology systems are considered critical infrastructures (Lewis, 2019). However, some of these sectors can be subject to attacks that can pose serious problems independent of cyberspace. The European Union (2022), has defined the sectors where a cyber threat is believed to have potentially catastrophic consequences as high critical infrastructures sectors. Accordingly, high criticality critical infrastructures are defined as transportation, energy, banking and financial infrastructures, health, drinking water, wastewater, digital infrastructures, information and communication technologies, public spaces and space (EU, 2022).

4.1. Energy Infrastructure

Türkiye is strategically located on energy transit routes, making energy infrastructures more critical for national security. Besides having national distribution lines in Türkiye's existing energy infrastructure, there are also international oil and natural gas pipelines (Baku-Tbilisi-Ceyhan Pipeline, TANAP, Turkish Stream Gas Pipeline, Kerkük-Yumurtalık Crude Oil Pipeline, etc.) is also in the transit corridor.

In energy grids and electrical systems in the energy infrastructure include all connections that allow the transmission of electricity from suppliers to consumers. They consist of power plants, storage facilities, transmission lines, distribution lines, transformers and power switches. Attacks on international power lines are focused on managing and protecting critical infrastructures that cannot be guaranteed. In cyberattacks on energy

infrastructure, smart grid systems are needed to protect infrastructures (Gündüz & Daş, 2020, p.971). The goals of smart grids are to increase efficiency and reliability by using automatic control and high-power smart converters. DDoS attacks on electricity grids leave the energy sector vulnerable and negatively affect other sectors with knock-on effects (Libicki, 2009, p.66). For example, a cyber-attack on energy infrastructures in Türkiye in 2016 temporarily disabled the functionality of electricity distribution systems, clearly demonstrating the vulnerability of these infrastructures (NTV, 2016). The security of energy infrastructures can be enhanced through regular stress tests and threat detection systems. Furthermore, to build cyber resilience in the energy sector, investments should be made in domestic solutions and international standards should be harmonized. In this context, cooperation with NATO and the European Union can play a critical role in the defense of energy infrastructures.

4.2. Health Systems

The healthcare sector is particularly vulnerable to cyber threats such as ransomware and data breaches. Health infrastructures in Türkiye have faced security vulnerabilities with the digitalization process. There has been a significant increase in ransomware attacks on healthcare systems, especially during the COVID-19 pandemic. These attacks disrupted the operations of healthcare organizations and jeopardized the treatment processes of patients (KAS & EDAM, 2022, p. 12). The use of AI-powered security solutions and encryption technologies is critical to protect healthcare infrastructures. In addition, awareness should be raised by providing regular cyber security trainings for healthcare professionals, and their capacity to respond quickly to attacks should be strengthened (Booker & Musman, 2020, p.1). Measures to be taken within this framework are;

- "Identify and prepare for potential threats and risks that may occur,

- Taking measures to reduce the security vulnerabilities of critical infrastructures, systems and networks identified in connection with internal-external and interdependencies in critical sectors in the health sector,

- Mitigating the potential threatening effects of critical infrastructures during or as a result of emergencies that may occur and ensuring that the relevant failure is eliminated after damage detection,

- Regardless of the causal factors, it will be decisive to establish systems that are resilient to interruptions caused by emergencies and systems that can adapt to changing conditions in order to quickly recover from damages that may occur, as well as preventive response systems that prevent systematic and operational attacks across the sector" (EU, 2024).

4.3. Financial Systems

Banking and financial infrastructures are one of the most frequently targeted sectors by cybercriminals. Ransomware and data theft attacks on banking systems in Türkiye have caused serious disruptions in the financial sector (Yeşilyurt, 2015, p.101). For example, in 2020, an attack on a banking institution in Türkiye resulted in the leakage of customer information and millions of liras in losses. This situation shows the necessity of continuous monitoring and rapid response teams in protecting financial systems. Another cyber-attack that took place in 2015 was a large-scale DDoS attack against *Türk Telekom and the Information and Communication Technologies Authority* (BTK). The attacks caused internet services to be interrupted, and along with the speed disruption, there were disruptions or even complete stoppages in digital and sometimes physical internet-based activities across the country.

Blockchain-based solutions and artificial intelligence-supported software should be used to protect financial infrastructures (Goeva et al., 2024, p.1). In addition, comprehensive training programs should be implemented to raise individuals' financial security awareness and regulatory bodies should strengthen cybersecurity protocols.

5. TÜRKİYE'S GEOSTRATEGIC POSITION AND INCREASING RISKS AND THREATS TO CRITICAL INFRASTRUCTURE

21. century, traditional geopolitical concepts such as land-based borders, maritime control or air superiority are no longer sufficient to explain strategic power. Instead, cyberspace has emerged as a distinct and dynamic space in which national interests are discussed and redefined. Rather than analyzing Türkiye's position through classical geopolitical lenses, its geostrategic importance must now be included in the developing cyberspace logic, which is an area shaped by digital infrastructures, information flows and cyber sovereignty. In this new environment, power is not solely determined by physical control, but also by a state's ability to protect,

disrupt, or govern the virtual architectures that sustain both civilian life and national security (Castells, 2009; Nye, 2010; Rid, 2020). These attacks in cyberspace not only cause infrastructural damage, but also target a state's strategic capacity, international reputation and social integrity.

In this multi-layered threat environment, Türkiye's geostrategic location makes it not only a physical bridge but also a "digital transit corridor". Türkiye is both a target and a transit route for attacks that may occur in cyberspace, as it is the crossroads of digital data flows connecting Europe, Asia and the Middle East. This situation necessitates Türkiye to address its cybersecurity policies not only from a defense perspective but also as a geopolitical priority.

Türkiye stands out as an important actor on both regional and global scales due to its geopolitical position. As an energy transit hub between Europe, Asia and the Middle East, Türkiye plays a strategic role in energy security with projects such as TANAP (Trans Anatolian Natural Gas Pipeline) and Baku-Tbilisi-Ceyhan. However within the context of cyberspace, these infrastructures represent not just physical assets but also critical digital terrains- vulnerable to cyberterrorism and state-sponsored attacks. These infrastructures are increasingly becoming high-value targets for adversial actors employing asymmetric methods such as ransomware, malware, or sabotage. Such attacks not only compromise operational continuity but also trigger cascading disruptions across financial markets, trade routes, and diplomatic engagements.

The strategic logic of cyberspace significantly undermines the basic assumptions of classical deterrence and war theories. The frequent targeting of Türkiye's financial, communication and defense infrastructures concretizes the geopolitical risk this new area poses. Indeed, ransomware attacks targeting the banking sector in recent years have clearly revealed the digital vulnerabilities and structural weaknesses of these infrastructures (Aydın, Barışkan & Çetinkaya, 2021, p. 156). The perpetrators of cyberattacks are often unidentifiable, and unlike classical security threats, the threshold for attack is often unclear; conflicts begin before they are officially declared and progress in a hybrid form (Rid, 2020). For this reason, cyberspace stands out as a strategic area of competition that disrupts traditional military power balances and enables asymmetric actions. As Joseph Nye (2010, p.1) stated, cyberpower is not only technical capacity, but

also the ability to manage perception, manipulate information and disrupt the opposing party's decision-making mechanisms.

As Joseph Nye (2010) points out, cyber power is inherently asymmetric; it privileges those who can move flexibly within open, decentralized networks. For Türkiye, this requires a strategic shift: national cyber security cannot be considered solely as a defensive posture, but must also include active deterrence, digital diplomacy, and network resilience. Manuel Castells (2009) emphasizes that power in the information age flows through networks; not only military alliances, but also data infrastructures and software ecosystems. In this sense, Türkiye's integration into transnational cyber defense networks (e.g. NATO's CCDCOE) becomes a way to strengthen not only protection but also digital sovereignty.

Moreover, cyberspace challenges the Westphalian paradigm by shifting the locus of sovereignty from territory to information. In such an environment, strategic depth is measured not in kilometers but in milliseconds of response time, degrees of system redundancy, and real-time threat detection capabilities. Türkiye's increasing participation in NATO's cyber doctrines (especially those emphasizing resilience and multilayered defense) reflects this transition (NATO, 2023). Moreover, cyberterrorism, which blurs the lines between political violence and digital sabotage, highlights the urgency of rethinking national security beyond traditional borders.

The convergence of cybersecurity and cyberterrorism highlights the need to reconceptualize geostrategy through the lens of cyberspace. As the boundaries between state and non-state actors, war and crime, and public and private sectors continue to erode, cyber resilience is becoming not only a technical requirement but also a geopolitical imperative. For a state like Türkiye, at the crossroads of continents, alliances, and conflicts, digital sovereignty and strategic adaptability in cyberspace are now essential components of national power On the other and increasing complexty of cyber threats requies coordination not only national level but also at the regional level. Türkiye should develop its own cyber policy doctrine against freely evolving threats, taking into account all this inclusiveness.

5.1. Threats Specific to Türkiye

Türkiye's geostrategic position and rapid digitalization have significantly increased its exposure to cyber threats, particularly targeting critical infrastructure sectors such as energy, finance, and public services. Among these, the energy sector has become a primary target due to its strategic importance and technological vulnerability.

These developments reveal that digital and physical security areas can no longer be addressed separately. It is clear that Türkiye needs an integrated security strategy to protect its critical infrastructures. This strategy should encompass not only technological solutions but also institutional coordination, crisis management capacity and public-private sector collaboration.

Cyberattacks targeting Türkiye's energy infrastructure have escalated both in frequency and complexity. According to Kaspersky's 2022 report, the percentage of industrial control system (ICS) computers in Türkiye's energy sector that encountered malicious objects reached 43.2% in the second half of the year—an increase of 1.8 percentage points compared to the first half (Kaspersky, 2023). These attacks aimed to infiltrate and disrupt industrial systems that manage energy generation and distribution, highlighting a critical vulnerability in the nation's cyber defense posture. This upward trend in cyber threats demonstrates the urgent need for Türkiye to reassess its national energy security paradigm—not only in terms of physical resilience but also through comprehensive cyber defense strategies. Given the cross-border and non-attributable nature of cyberattacks, enhanced collaboration with international cybersecurity frameworks, including NATO, is essential to mitigate such evolving threats.

In 2023, several banks in Türkiye were targeted by DDoS attacks on their digital platforms, resulting in significant disruptions to internet banking services. These attacks prevented users from accessing their accounts and caused considerable delays in financial transactions (Kriter Dergi, 2023). In the same year, ransomware attacks were carried out against the digital infrastructures of various public institutions, leading to the temporary suspension of municipal services. As a result, citizens experienced interruptions in accessing essential public services, and the security of public data was severely compromised (Kriter Dergi, 2023). In recent years, Türkiye has increasingly become a target of both cyber and physical security threats. This trend underscores the necessity of a comprehensive and

multidimensional security approach, particularly for the protection of critical sectors such as public institutions, the energy sector, and healthcare infrastructure.

In 2015, large-scale DDoS attacks targeted DNS servers with the ".tr" extension; access to thousands of websites was temporarily cut off. These attacks revealed the vulnerabilities in Türkiye's digital infrastructure and the lack of resilience of public information systems (Kandır, 2025). In 2020, a ransomware attack on an energy company that distributes natural gas in major cities halted the company's operations and revealed the infrastructure's vulnerability to cyber threats (Kandır, 2025). In the same year, the websites of various government ministries were subjected to simultaneous cyber attacks; Access to many institutions, including the Presidency's of the Republic of Türkiye Directorate of Communications, has been temporarily cut off (DGRNET, 2024, p. 4).

A cyber attack on the Ministry of Health in 2021 targeted personal health data. This incident has once again shown how sensitive health systems are in terms of cybersecurity, especially during the pandemic (DGRNET, 2024, p. 2). In addition to cyber threats, security risks related to the physical domain and intelligence have also come to the forefront. The terrorist attacks targeting the Ministry of Interior in October 2023 and the TUSAŞ facilities in 2024 have demonstrated that national security concerns are not limited to the digital sphere, but also encompass the physical domain and intelligence dimensions (Ceylan, 2024, p. 6).

These developments show that digital and physical security areas can no longer be considered separately. It is clear that Türkiye needs an integrated security strategy to protect its critical infrastructures. This strategy; in addition to technological solutions, it should also include elements such as institutional coordination, crisis management capacity and public-private sector cooperation

6. CYBER SECURITY AND THE FIGHT AGAINST CYBER TERRORISM IN TÜRKİYE

Türkiye is taking important steps in the field of cyber security against the increasing cyber threats on a global scale and developing various strategies to combat cyber terrorism. Within the framework of national security strategies, cyber security is seen as the guarantee of both the state's

understanding of security and economic and social security. In recent years, Türkiye has been trying to overcome its deficiencies in this field with the policies and strategies it has developed in the field of cyber security and has been conducting a more effective fight against cyber terrorism. In this context, cyber resilience, proactive cyber defense and deterrence, people-oriented cyber security approach, safe use of technology, domestic and national technologies in combating cyber threats, as well as the activities carried out by the Digital Transformation Office, ICTA and TÜBİTAK are effective.

6.1. National Cyber Security Policies and Strategies

Türkiye published its first National Cyber Security Strategy in 2013 and updated it in 2019. The National Cyber Security Strategy aims to protect critical infrastructures, detect cyber-attacks and develop effective response methods. While strengthening Türkiye's digital security infrastructure, the strategy also emphasizes the development of domestic cyber security products (Sağıroğlu & Alkan, 2018, p. 51). With its cyber security strategy, Türkiye aims to combat cyber threats not only at the national level but also at the global level.

The success of cyber security strategies depends on the strong cooperation of both the state and the private sector. Türkiye's cybersecurity strategy emphasizes the need to spread cybersecurity awareness in the public and private sectors. In particular, it is stated that institutions should have the capacity to detect threats in advance and take precautions. At this point, including the private sector in these strategies will be an important step in protecting critical infrastructures (Kurum, Bilgiç, & Çardak, 2022, p. 461). In addition, Türkiye's indigenous technologies developed in the field of cyber security have great potential for increasing its cyber defense capacity. Indigenous software and hardware reduce foreign dependency, while at the same time increasing the international competitiveness of domestic producers in this field. However, the rapidly changing nature of cyber threats requires continuous updating of cyber security policies. Within the framework of these policies, the "Cyber Security Presidency" was established with the decree published in the Official Gazette dated January 8, 2025. The Presidency will develop action plans and strategies to develop policies and objectives to ensure cyber security.

6.2. Legal and Regulatory Framework

The legal and regulatory framework in Türkiye plays an important role in combating cybercrime and ensuring cybersecurity. Law No. 5651 provides an important legal basis for combating cybercrime and crimes committed in the digital environment. This law defines offenses such as defamation, slander, and violation of personal data committed over the internet and imposes criminal sanctions (Acay, 2021, p.87). In addition, the Law on the Protection of Personal Data adopted in 2016 introduced important regulations for the protection of personal data in the digital environment. However, only legal regulations are not sufficient for cyber security. The effective implementation of these regulations requires strengthened oversight mechanisms and more training. Furthermore, active support from the private sector should be sought in the fight against cybercrime.

Türkiye's success in combating cybercrime relies on the effectiveness of both legal and administrative structures. From a national security perspective, broader cooperation is needed to combat a threat as complex and transnational as cyber terrorism. In order to combat global threats, Türkiye's cybersecurity laws should be continuously updated in parallel with international developments (Sağıroğlu & Alkan, 2018, p. 36). In this context, the National Cyber Security Law No. 7545, which entered into force in March 2025, has been a transformative step in Türkiye's cyber governance. This comprehensive legislation has brought significant reforms. Some of these reforms include mandatory periodic cyber risk assessment reports for critical infrastructure sectors (such as energy, finance, telecommunications), the establishment of the National Cyber Threat Intelligence Center, and gradual sanction mechanisms for non-compliance. The law also clarified the obligations of public and private sector actors regarding incident reporting processes, expanded the authorities of the National Cyber Incident Response Center (USOM), and institutionalized international cybersecurity cooperation. One of the most striking aspects of Law No. 7545 is that it has brought Türkiye's cyber resilience planning more in line with EU and NATO standards by placing public-private sector cooperation on a legal basis (Resmi Gazete, 2025).

Developing cybersecurity laws within the framework of international cooperation will play a critical role in mitigating the effects of cybercrime and cyberterrorism not only in Türkiye but also worldwide. Therefore,

Türkiye's harmonization with global cybersecurity regulations is important in terms of consolidating international cooperation.

6.3. Current Situation in the Protection of Critical Infrastructures

In Türkiye, critical infrastructures in the energy, healthcare and finance sectors can be vulnerable to cyber threats. Especially in the energy sector, cyber-attacks can cause major damage by targeting critical systems. Therefore, more effective cyber security measures are needed to protect energy infrastructures (Kurum, Bilgiç, & Çardak, 2022, p. 460). Türkiye's energy sector should be harmonized with cybersecurity standards and the resilience of systems against cyber threats should be increased. However, infrastructures in the healthcare sector are also highly vulnerable to cyber threats. Cyberattacks on the energy and manufacturing sectors in Türkiye are on the rise. According to Kaspersky's 2022 data, 41.9% of Industrial Control System (ICS) computers in Türkiye faced cyber threats. The energy sector is among the most attacked sectors (Kaspersky, 2023).

Critical data such as digital health records, patient information and medication management can be targeted by cyber-attacks, which can not only breach personal data but also harm public health (Singer & Friedman, 2014, p. 75). Protecting digital systems in the healthcare sector is critical to preventing cyberattacks that threaten public health. Healthcare organizations need to invest more in cybersecurity and strengthen their infrastructure. Financial systems are one of Türkiye's most vulnerable sectors and should have the highest standards of cybersecurity. Türkiye should adopt a more integrated and comprehensive security approach for continuous monitoring and protection of digital infrastructures in the financial sector (Tikk & Kaska, 2010, p. 293). Cyber-attacks targeting financial systems can cause huge economic losses and seriously undermine public confidence. Therefore, closing vulnerabilities in financial systems is an important part of cybersecurity policy.

7. DEFENSE AND PREVENTION STRATEGIES

Cyber security plays a critical role in ensuring national security, economic stability and social trust in today's digitalized world. In particular, cyber terrorism and cybercrime pose significant threats to states and the private sector. An effective fight against these threats is not only possible through technology-based solutions, but also requires the development of

strong defense and prevention strategies. These strategies are necessary not only to defend against cyber-attacks, but also to anticipate the effects of these attacks and minimize risks through early response and rapid recovery mechanisms. In this framework, it will be decisive to take prevention and response steps to detect and prevent cyber-attacks in advance and to create deterrent mechanisms (NATO, 2024).

Defense and prevention strategies are generally shaped around domestic and national technologies, public-private partnerships, international cooperation and proactive response approaches (Aksu Ereker, 2019). These strategies include key elements such as strengthening cyber security infrastructure, early detection of threats and rapid response to attacks. In addition, increasing information sharing among countries and establishing common defense mechanisms are also of great importance in the fight against cyber terrorism. Türkiye's cyber security strategies are shaped in this direction and include many important steps, from the development of indigenous solutions to the strengthening of international cooperation.

7.1. Domestic and National Technological Solutions

Domestic and national technological solutions play a critical role in Türkiye's cyber security strategies. In recent years, the development of indigenous cyber security software and hardware has enabled Türkiye to take important steps towards reducing its dependence on foreign sources. These solutions both reinforce national security and make Türkiye more resilient against cyber threats. Domestic software and hardware increase Türkiye's security power not only in the local scale but also in the international arena (Sağıroğlu & Alkan, 2018, p. 167).

Türkiye's success in this field shows that in addition to domestic production solutions, innovative strategies in cyber security should also be developed. The state's cyber security strategies become more effective through collaborations with the private sector. Public and private sectors acting together not only strengthen the cybersecurity infrastructure, but also increase Türkiye's technology production capacity in this field (Kurum, Bilgiç, & Çardak, 2022, p. 446). Since externally dependent systems may lose their effectiveness, especially in times of crisis, local solutions will also help to respond more quickly and effectively to cyber threats. Developing indigenous solutions is of great importance not only for national security but

also for economic development. In this context, the development of indigenous technologies will increase Türkiye's technology exports as well as its goal of becoming an independent country in the field of cyber security. Türkiye's investments in indigenous solutions in cyber security will also provide a significant advantage in its competition with other countries.

7.2. Public-Private Sector Cooperation Models

Public-private partnerships are especially important in combating threats to critical infrastructures. The effectiveness of cybersecurity strategies in Türkiye relies on cooperation between the governments's regulatory and oversight role and the private sector's innovative solutions. This collaboration enables faster and more efficient implementation of cybersecurity strategies. Especially in critical sectors such as financial and energy infrastructures, a stronger cybersecurity infrastructure can be created when the private sector's capacity to produce technology and the public sector's regulatory role are combined (Kurum, Bilgiç & Çardak, 2022, p. 461). However, cooperation between the public and private sectors should not be limited to joint projects. A stronger interaction between these two sectors should also be ensured in information sharing and training processes. This approach is critical not only for cyber security but also for the security of all digital infrastructures (Hekim & Başıbüyük, 2013, p. 137). Cyber security infrastructures developed through public-private partnerships will create a more secure environment in the digital environment and enable faster reactions to cyber threats. Moreover, the development of these collaborations may lead to more research and development (R&D) activities in the field of cyber security. These R&D activities will increase the effectiveness of Türkiye's cybersecurity strategies, not only for the country's internal security, but also on a global level. Strong collaborations between the public and private sectors can make Türkiye a more independent and powerful actor in cybersecurity. Cyber security should not be limited to technical measures; it should also include education, awareness, and international cooperation. For example, institutions such as CISA in the USA cooperate with the private sector in protecting critical infrastructures. In addition, international norms adopted under the leadership of the United Nations require states to act responsibly in the cyberspace and avoid attacks on critical infrastructures (Kesan, Hayes, & Bashar, 2021).

7.3. International Cooperation and NATO Integration

Since cyber security is a threat that transcends national borders, international cooperation against this threat is of great importance. Within the framework of its NATO membership, Türkiye is strengthening international cooperation in cyber security and developing a collective defense mechanism against cyber terrorism. NATO aims to develop a common strategy against cyber security threats among member states and Türkiye plays an important role as a part of these strategies (Singer & Friedman, 2014, p. 78).

By strengthening its cyber defense capacity with NATO, Türkiye is establishing a common line of defense against global cyber threats. This cooperation creates a strong solidarity against cyber threats not only for Türkiye but also for all NATO member states. Sharing cyber security knowledge and experience at the international level will play a key role in eliminating vulnerabilities in this area (Polat, 2020, p. 149). Information sharing with NATO and other international organizations will not only enable early detection of cyber-attacks, but will also help establish an international standard in cyber security. Türkiye's NATO integration will enable a more effective response to global cyber threats and strengthen international cooperation.

7.4. Proactive and Reactive Response Mechanisms

The effectiveness of cyber security strategies relies on both proactive and reactive response mechanisms. Proactive intervention involves detecting threats in advance and taking necessary measures against them. Such interventions are made possible by early warning systems and continuous monitoring (Tikk & Kaska, 2010, p. 294). Türkiye is working on developing such proactive systems to detect threats to its critical infrastructures in advance.

Reactive response, on the other hand, ensures a fast and effective response when a cyber-attack occurs. These responses help limit the impact of cyber-attacks and allow infrastructures to return to normal quickly. By strengthening these response mechanisms, Türkiye is becoming more resilient against cyber-attacks (Çahmutoğlu, 2020, p. 68). Proactive response means detecting attacks before they occur and being prepared for these threats. Reactive response, on the other hand, requires effective crisis management to minimize the damage caused by attacks. Türkiye's strategies

combining these two approaches play a key role in ensuring strong protection against cyber threats to critical infrastructures.

8. STRATEGIC RECOMMENDATIONS FOR TÜRKİYE

8.1. Roadmap for Countering Cyber Terrorism in Critical Infrastructure

Türkiye is developing strong cyber security strategies against cyber threats to critical infrastructures. The relevant strategies cover both cybersecurity and cyberterrorism dimensions in line with national security policies. Türkiye's National Cybersecurity Strategy, published in 2019, provides a guiding framework on how to approach cyberattacks to critical infrastructures (Tüzün, 2022). This strategy aims to detect cyber threats in advance, respond quickly to potential attacks, and take the necessary precautions. Within this framework, cyberattacks deepening with connectivity are important and the "cyber resilience" strategy is important for continuity in the cyber world (Demhack, 2011, p.76). The 2024-2028 National Cybersecurity Strategy and Action Plan was prepared based on the themes of "Human", "Defense", "Deterrence" and "Cooperation" and focused on the transformation of relevant themes into action within a concrete framework (UAB, 2024).

In the event of attacks on critical infrastructures, states are trying to resolve the issue with a paradigm shift from "protection to resilience". In the 2000s, the European Union launched the European Critical Infrastructure Program (EPCIP) to combat cyber threats. The focus of the EPCIP program is to offer solutions with a conventional approach to protect critical infrastructures. Since the conventional approach carries the risk of not being sufficient to prevent all threats, it will not be possible to protect all critical infrastructures. In this context, strategies such as robustness, stress resistance and resilience of critical infrastructures against possible crises have been focused on (Liu & Song, 2020). The term resilience is derived from the Latin word "*resiliere*", which means "bounce back". In this context, resilience refers to the capacity to adapt to changing conditions, withstand disruptions caused by emergencies and recover quickly. The focus is on resilience "against a variety of expected and unexpected events and risks". These risks are systemic due to their operational dimensions, their ability to be realized

through virtual or physical means, and the uncertainty and complexity of the threats.

The first step to prevent cyber threats to critical infrastructures should be to continuously update national security policies. The rapidly changing nature of technology requires cyber security strategies to be in constant evolution. Türkiye should consider not only current threats but also potential future cyberattacks and be prepared for them (Polat, 2020, p. 136). Within the scope of this strategy, developing domestic technologies, reducing foreign dependence and using domestic cyber security products have an important place. In Türkiye's cyber security strategy, a structure supported by innovative solutions from the private sector and academic research should be established. In this way, knowledge accumulation and technology development processes in the field of cyber security will become faster and more effective. Moreover, public-private sector cooperation will ensure more successful implementation of these strategies.

8.2. The Role of Academia and the Private Sector

Collaboration between academia and the private sector is crucial for success in cyber security. Academic research enables a better understanding of cyber threats and the development of new security technologies. Universities and research institutions in Türkiye (e.g. TÜBİTAK BİLGEM, BTK) play an important role in cybersecurity knowledge production (Hekim & Başıbüyük, 2013, p. 155). These institutions work to develop next-generation cyber security solutions and take precautions against potential cyber-attacks.

The private sector is a critical stakeholder in cyber security with its innovative solutions and technology development capacity. In particular, Türkiye's leading technology companies are developing indigenous cyber security solutions and implementing these solutions in cooperation with the government. These collaborations between the public and private sectors will enable Türkiye to fight more effectively against cyber threats (Sağıroğlu & Alkan, 2018, p. 36). A strong collaboration between the academic world and the private sector will ensure that research in the field of cyber security is transformed into viable solutions. These collaborations also allow for a stronger preventive mechanism against future cyber threats. Universities

and the private sector in Türkiye can build a more robust digital infrastructure by developing joint projects in cybersecurity.

8.3. Strengthening International Information Sharing and Cooperation

As cyber security has become a global threat, strengthening international cooperation is of utmost importance. In this context, Türkiye needs to increase its cooperation with NATO and other international organizations. NATO's strategies in the field of cyber security enable member states to act in a common language (Polat, 2020, p. 145). By strengthening its integration with NATO, Türkiye can create a more effective defense mechanism against global cyber threats. Such cooperation enables not only information sharing but also the coordinated development of cyber defense strategies.

International cooperation will contribute to enhancing Türkiye's cybersecurity capacity and enable the creation of a broader cybersecurity network. Increasing information sharing between countries on a global scale allows for a faster and more effective response to cyber threats (Çahmutoğlu, 2020, p. 69). Türkiye's strengthening international cooperation in cybersecurity will contribute significantly to both the prevention of cybercrime and the fight against cyberterrorism. International information sharing provides not only defense in cybersecurity but also global solidarity against cyber threats. Türkiye's cooperation with NATO is an example of global information sharing in this area. As cyber-attacks increase on a global scale, Türkiye's strengthening of such cooperation will help ensure not only national security but also worldwide security.

CONCLUSION

This article has aimed to comprehensively examine the cybersecurity risks faced by Türkiye's critical infrastructures and the strategic approaches required to combat cyber terrorism. In today's rapidly digitizing world, critical infrastructures are not only technological systems but also fundamental pillars of national security and social stability. Infrastructures serving sectors such as energy, healthcare, and transportation have become integral components directly affecting the daily functioning of society. However, with increasing digitization, these systems are increasingly exposed to cyber threats, which in turn makes defense requirements more complex. Due to both its strategic location and the rapid development of its

digital infrastructure, Türkiye finds itself in a particularly vulnerable position against threats like cyber terrorism.

The study has addressed Türkiye's current cybersecurity policies, their practical implementations, and potential strategic steps to counter emerging threats. Prioritizing domestic and national technologies, strengthening public-private sector cooperation, enhancing international information sharing, and developing proactive intervention systems are of critical importance for increasing Türkiye's resilience against cyber threats. These elements should be considered not only on a technical level but also as part of a holistic approach involving governance and strategic development. Moreover, constructive collaborations with international institutions will not only assist in neutralizing external threats but also bolster Türkiye's competitiveness on the global cybersecurity stage.

Progress in cybersecurity cannot be achieved solely through technical and institutional measures. Raising awareness across all segments of society is essential to ensuring the long-term effectiveness of security policies. Cybersecurity should not be regarded solely as a matter for the state or certain institutions, but as a shared responsibility encompassing a wide range of actors—from individuals and private sector entities to public institutions and academic circles. In this context, educational policies must be restructured around digital literacy and cybersecurity awareness. Encouraging younger generations to engage with this field from an early age is a strategic investment not only to address current threats but also to build the cybersecurity architecture of the future. This approach could contribute to Türkiye becoming a regional hub for cybersecurity in the long run.

Looking ahead, it is of great importance for Türkiye to invest in AI-supported defense systems, increase its pool of qualified human resources, and implement sector-specific risk analyses in order to further strengthen its capacity in this domain. In the coming years, it will be essential not only to build mechanisms that can defend against existing threats, but also to develop an effective deterrence capacity. In this regard, forming more integrated and functional partnerships with international structures such as NATO will play a key role in elevating Türkiye's cybersecurity ecosystem to global standards. In conclusion, the findings of this study demonstrate that while Türkiye has made significant strides in enhancing the security of its critical infrastructure and building resilience against cyber threats, this

process can only be rendered sustainable through a continuous, strategic, and multidimensional approach. Combatting cyber terrorism requires a comprehensive will that extends beyond technical solutions and encompasses political, economic, and social dimensions.

REFERENCES

Acay, F. (2021). Sosyal Medya Aracılığıyla Hakaret Suçu ve Suçun Tespitine Ilişkin Uygulamalar. *İstanbul Aydın University Faculty of Law Journal, 7*(1), 71-140. Accessed: November 12, 2024.

AFAD (2014). AFAD Critical Infrastructure Protection Roadmap Document. Accessed: November 20, 2024. https://www.afad.gov.tr/kurumlar/afad.gov.tr/3906/xfiles/teknolojik-afetler-son.pdf.

Afyonluoğlu, M. (2020). *Siber Güvenlik ve Kamu Politikaları*, Teknoloji ve Kamu Politikaları Kitabı, ss. 379-411, (Editör: Mete Yıldız-Cenay Babaoğlu), Gazi Kitabevi, Ankara, 2020.

Aksu Ereker, F. (2019). "NATO's Security Understanding and Strategic Concepts". Security Articles Series, No.23, October 2019. Accessed: December 12, 2024. https://trguvenlikportali.com/wp-content/uploads/2019/11/NATOStratejikKonseptleri_FulyaAksuEreker_v.1.pdf. https://doi.org/ 10.13140/RG.2.2.12855.47527.

Ardielli, E. & Ardielli, J. (2017). Cyber Security In Public Administration of the Czech Republic. *Social & Economic Review*, *15*(4). https://fsev.tnuni.sk/revue/papers/147.pdf.

Arquilla, J. & Rondfeldt, D. (1996). *The Advent of Netwar*. Published Rand Corporation, ISBN: 0-8330-2414-0, National Defence Research Institute. Accessed: March 30, 2025. https://www.rand.org/content/dam/rand/pubs/monograph_reports/MR789/RAND_MR789.pdf.

Asal, V. H., Park, H. H., Rethemeyer, R. K., & Ackerman, G. (2015). With Friends Like These Why Terrorist Organizations Ally. *International Public Management Journal*, 19(1), 1–30. https://doi.org/10.1080/10967494.2015.1027431.

Atasever, A., Özçelik, A. & Sağıroğlu, Ş. (2019). *Cyber Terrorism and DDoS.* Süleyman Demirel University Journal of Natural and Applied Sciences Volume 23, Issue 1, 238-244, 2019. DOI: 10.19113/sdufenbed.507948.

Aydın, H., Barışkan, M. A., & Çetinkaya, A. (2021). *Siber Güvenlik Kapsamında Enerji Sistemleri Güvenliğinin Değerlendirilmesi*. *Güvenlik Bilimleri Dergisi*, *10*(1), 151-174.

Bayrakçı, E. & Koçman, M. A. (2023). *Bilgi Güvenliği ve Elektronik Harp. Necmettin Erbakan Üniversitesi Siyasal Bilgiler Fakültesi Dergisi, 5(Özel Sayı), 184-206.*

Booker, L. B., & Musman, S. A. (2020). A Model-based, Decision-theoretic Perspective on Automated Cyber Response. *arXiv preprint arXiv:2002.08957*. Accessed: December 12, 2024. https://doi.org/10.48550/arXiv.2002.08957.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/Sovereignty and European Security Integration: an Introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887.

Carrapico, H. & Barrinha, A. (2018). European Union Cyber Security as an Emerging Research and Policy Field. *European Politics and Society*, *19*(3), 299–303. https://doi.org/10.1080/23745118.2018.1430712.

Castells, M. (2009). The Rise of the Network Society. Oxford: Blackwell Publishing. ISBN: 978-1-405-19686-4.

Ceylan, F. (2024). "'Kritik Altyapının Korunması ve Dayanıklılık", Çevrimiçi Yayın, 1 Kasım 2024. https://www.uikpanorama.com/blog/2024/11/01/tusas-saldiri-altyapi-fc.

CISA (2009). Critical Infrastructure Security and Resilience. Accessed: December, 10 2024. https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience.

Collin, B. (1997). The Future of Cyberterrorism: Where the Physical and Virtual Worlds Converge. *Crime and Justice International*, *13*(2), 15-18. Accessed: 28.12.2024 https://www.ojp.gov/ncjrs/virtual-library/abstracts/future-cyberterrorism-physical-and-virtual-worlds-converge.

CRS (2004). Critical Infrastructure and Key Assets: Definition and Identification. CRS Report for Congress Received through the CRS Web. https://apps.dtic.mil/sti/pdfs/ADA454016.pdf.

Çahmutoğlu, E. (2020). Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi. Analytical Politics, 1(1), 63-79.

DGRNET (2024). Türkiye'nin Maruz Kaldığı Şimdiye Kadarki En Büyük 5 Siber Saldırı. https://www.dgrnet.com.tr/2024/08/turkiyenin-maruz-kaldigi-simdiye-kadarki-en-buyuk-5-siber-saldiri/.

Deibert, R.J. (2019). The Road to Digital Unfreedom: Three Painful Truths About Social Media. *Journal of Democracy 30*(1), 25-39. https://dx.doi.org/10.1353/jod.2019.0002.

Demchak, C. C. (2011). *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security*. University of Georgia Press, Athens and London.

Demirci, K. (2021). Kritik Altyapılarda Siber Güvenlik ve AFAD Üzerinden Bir Değerlendirme. *Nazilli İktisadi ve İdari Bilimler Fakültesi Dergisi*, *2*(2), 54-64.

Denning, D. E. (2017). Cyberterrorism: The Logic Bomb Versus the Truck Bomb. *In Cyberspace Crime*, pp. 217-225, Routledge.

Dubyna, M., Shchur, R., Shyshkına, O., Sadchykova, I., Panchenko, O., & Bazılınska, O. (2024). The Role of Artificial Intelligence in the Cybersecurity System of Banking Instıtutıons in the Conditions of Instability. *Journal of Theoretical and Applied Information Technology*, *102*(19), 6950-6965. E-ISSN: 1817-3195.

Dunn Cavelty, M. (2008). Cyber-Security and Threat Politics: US Efforts to Secure the Information Age (1st ed.). Routledge. https://doi.org/10.4324/9780203937419.

Ercan, M. (2015). *Kritik Altyapıların Korunmasına İlişkin Belirlenen Siber Güvenlik Stratejileri* (Master's Thesis, Gebze Teknik Üniversitesi, Sosyal Bilimler Enstitüsü).

EU (2024). Critical Infrastructure and Cybersecurity. Accessed: December, 20 2024. https://energy.ec.europa.eu/topics/energy-security/critical-infrastructure-and-cybersecurity_en

Govea, J., Gaibor-Naranjo, W. & Villegas-Ch, W. (2024). Securing Critical Infrastructure with Blockchain Technology: An Approach to Cyber-Resilience. *Computers*, *13*(5), 122. Accessed: November 30, 2024. https://doi.org/10.3390/computers13050122.

Gündüz, M. Z. & Daş, R. (2020). Akıllı Şebekelerde İletişim Altyapısı ve Siber Güvenlik. *Journal of the Institute of Science and Technology*, *10*(2), 970-984. Accessed: December 20, 2024. https://doi.org/10.21597/jist.655990.

Hekim, H. & Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi*, *4* (2), 135-158.

Holloway, M. (2015). Stuxnet Worm Attack on Iranian Nuclear Facilities. *Retrieved: April 13*, 2017, Standford University. Accessed: November, 22 2024. http://large.stanford.edu/courses/2015/ph241/holloway1/.

Jormakka, J. & Mölsä, J. V. E. (2005). Modelling Information Warfare as a Game. *Journal of Information Warfare*, *4*(2), 12–25. https://www.jstor.org/stable/26504060.

Kandır, M.O. (2025). Kritik Altyapılarda Siber Güvenlik. Yayın Tarihi: 06 Nisan 2025. Erişim Tarihi: 10 Nisan 2025. https://www.hukukvebilisimdergisi.com/kritik-altyapilarda-siber-guvenlik/.

Karabacak, B. (2011). Kritik Altyapılara Yönelik Siber Tehditler ve Türkiye İçin Siber Güvenlik Önerileri. *Siber Güvenlik Çalıştayı, Bilgi Güvenliği Derneği, Ankara*, *29*, 1-11.

KAS & EDAM (2022). *Türkiye'de Kritik Altyapı ve Siber Güvenlik. Konrad-Adenauer-Stiftung Türkiye*, 1–32. Erişim Tarihi: 10 Aralık 2024. https://edam.org.tr/wp-content/uploads/2022/08/NATO-Uluslararasi-Guvenlik-ve-Siber-Raporu.docx.pdf -2022.

Kaspersky (2023). Enerjide Var "Türkiye'de En Çok Saldırıya Uğrayan Sektörler"- Yeni Rapor!. https://www.enerjiekonomisi.com/enerjide-var-turkiye-de-en-cok-saldiriya-ugrayan-sektorler-yeni-rapor/26690/

Kaspersky (2023). *Türkiye'de Enerji ve Üretim Sektörlerine Yönelik Siber Saldırılar Arttı*. 15 Mart 2023. Erişim Tarihi: 10 Kasım 2024. https://www.kaspersky.com.tr/about/press-releases/turkiyede-enerji-ve-uretim-sektorlerine-yonelik-siber-saldirilar-artti?utm_source=chatgpt.com.

Kello, L. (2013). The Meaning of the Cyber Revolution: Perils to Theory and Statecraft. *International Security* 2013; 38 (2): 7–40. https://doi.org/10.1162/ISEC_a_00138.

Kesan, J. P. Hayes, C. M. & Bashir, M. N. (2016) "A Comprehensive Empirical Study of Data Privacy, Trust, and Consumer Autonomy," *Indiana Law Journal*: Vol. 91: Iss. 2, Article 3. Available at: https://www.repository.law.indiana.edu/ilj/vol91/iss2/3.

Kesler, B. (2011). The Vulnerability of Nuclear Facilities to Cyber Attack; Strategic Insights: Spring 2010. Calhoun: The NPS Institutional Archive. Accessed: December, 20 2024. https://core.ac.uk/download/pdf/36718376.pdf.

Kohlmann, E. F. (2006). The Real Online Terrorist Threat. *Foreign Affairs, 85*(5), 115–124. https://doi.org/10.2307/20032074.

Kriter Dergi. (2023). Askersiz Savaş Çağı Başladı. Türkiye'nin Siber Kalkanı Güçlendiriliyor. *Kriter Dergi*. Erişim Tarihi: 20 Mart 2025. https://kriterdergi.com/dis-politika/askersiz-savas-cagi-basladi-turkiyenin-siber-kalkani-guclendiriliyor.

Kriter Dergi (2023). Türkiye'de Siber Güvenlik Gelişmeleri. Kriter Dergi, 7(84)

Kurum, M., Bilgiç, A., & Çardak, B. (2022). *Siber Alanda Radikalleşme ve İnternetin Panoptik Gözetimi*. Güvenlik Bilimleri Dergisi, 11(2), 441-470, Accessed: 12.12.2024. https://doi.org/10.28956/gbd.1092120.

Lee, R. M., Assante, M. J., & Conway, T. (2014). German Steel Mill Cyber-Attack. *Industrial Control Systems*, *30*(62), 1-15, *Accessed*: *December 10, 2024*.

Lee, R. M. & Conway, T. (2022). The Five ICS Cybersecurity Critical Controls. *Available from.* A*ccessed: December 10, 2024*.

Lewis, J. (2006). *Cybersecurity and Critical Infrastructure Protection*. Center for Strategic and International Studies, 1-12.

Lewis, T. G. (2019). *Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation*. John Wiley & Sons.

Libicki, M. C. (2009). Cyber Deterrence and Cyberwar. Published by 2009 *RAND Corporation*. ISBN: 978-0-8330-4734-2.

Lin, H. S. (2010). Offensive Cyber Operations and the Use of Force. *Journal of National Security Law & Policy, Vol.4, No.63. 2010.*

Liu, W. & Song, Z. (2020) Review of Studies on the Resillience of Urban Critical Infrastructure Networks. Reliability Engineering & System Safety, Volume 193, 2020, 106617, ISSN 0951-8320, https://doi.org/10.1016/j.ress.2019.106617**.**

Mueller, R. S. (2010) By Ellen Nakashima, "FBI Dırector Warns of Rapidly Expanding Cyberterrorism Threat". The Washington Post. 4 March 2010. Accessed: November 20, 2024. https://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html.

Nakashima, E. (2010). "FBI Dırector Warns of Rapidly Expanding Cyberterrorism Threat". The Washington Post. 4 March 2010. Accessed: 20.11.2024. https://www.washingtonpost.com/wp-dyn/content/article/2010/03/04/AR2010030405066.html.

NATO (2021). *NATO Siber Güvenlik Politikaları ve Uluslararası İşbirliği. NATO Siber Savunma Raporu*, 12.

NATO (2021). *NATO Cyber Defence Pledge. April 16, 2021.* Accessed: January 29, 2025. https://ccdcoe.org/news/2021/public-side-event-of-the-nato-cyber-defence-pledge-conference-2021-on-16-april/.

NATO (2022). *2022 NATO Strategic Concept*. Accessed: December 20, 2024. 290622-strategic-concept.pdf.

NATO (2024). *Resilience, Civil Preparedness and Article 3.* Accessed: November 29, 2024. https://www.nato.int/cps/bu/natohq/topics_132722.htm#vulnerabilities.

NATO (2024). *Cyber Defence*. July 30, 2024. Accessed December 12, 2024. https://www.nato.int/cps/de/natohq/topics_78170.htm.

NIST (2016). National Institute of Standards and Technology. Elaine Barker William C. Barker. Accessed: 25.11.2024. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf.

NTV (2016). Elektrik Hatlarına Siber Saldırı Girişimi. Yayın Tarihi: 31.12.2016. https://www.ntv.com.tr/turkiye/elektrik-hatlarina-siber-saldiri-girisimi,-ez-gYJG70Oqr5F-imHELg.

Nye, J. S. (2010). Cyber Power. Belfer Center for Science and International Affairs. Cambridge: Harvard Kennedy School, pp. 1-24. May 2010.

Parks, R. C. & Duggan, D. P. (2011). "Principles of Cyberwarfare," in IEEE Security & Privacy, Vol. 9, No. 5, pp. 30-35, Sept.-Oct. 2011, https://doi: 10.1109/MSP.2011.138.

Polat. D. (2020). *NATO'nun Yeni Operasyon Alanı: Siber Uzay*. Güvenlik Bilimleri Dergisi, Özel Sayı (International Security Congress Special Issue), 135-138. Accessed: December 20, 2024. https://doi.org/10.28956/gbd.695973

Pursiainen, C. (2009). The Challenges for European Critical Infrastructure Protection. *Journal of European Integration*, *31*(6), 721–739, Accessed: December 17, 2024. https://doi.org/10.1080/07036330903199846.

Pursiainen, C. (2021). Russia's Critical Infrastructure Policy: What do we Know About it?. *European Journal for Security Research*, 6(1), 21–38 (2021). https://doi.org/10.1007/s41125-020-00070-0.

Pollitt, M. M (1998). Cyberterrorism Fact or Fancy? Computer Fraud & Security, Volume 1998, Issue 2, 1998, Pages 8-10, ISSN 1361-3723, https://doi.org/10.1016/S1361-3723(00)87009-8.

RAND Corporation (2015). *Cyberterrorism: The Risks and Consequences of Digital Attacks on Critical İnfrastructure. RAND Corporation Report*, 21. Accessed: 15 December 2024. https://www.rand.org/content/dam/rand/pubs/research_reports/RRA2300/RRA2397-2/RAND_RRA2397-2.pdf.

Resmi Gazete (2025). Siber Güvenlik Kanunu. Kanun No: 7545, 12 Mart 2025, Sayı: 32846. https://www.resmigazete.gov.tr/eskiler/2025/03/20250319-1.htm

Rid, T. (2011). Cyber War Will Not Take Place. *Journal of Strategic Studies*, *35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939.

Rid, T. (2020). *Active Measures: The Secret History of Disinformation and Political Warfare*. Profile Books.

Rid, T. & Buchanan, B. (2014). Attributing Cyber Attacks. *Journal of Strategic Studies*, *38*(1–2), 4–37. https://doi.org/10.1080/01402390.2014.977382.

Robinson, P. (2025). The MOVEit Attack Explained. Erişim Tarihi: February, 16 2025. https://www.lepide.com/blog/the-moveit-attack-explained/

Saltzer, J. H., & Schroeder, M. D. (1975). "The protection of information in computer systems," in *Proceedings of the IEEE*, vol. 63, no. 9, pp. 1278-1308, Sept. 1975, doi: 10.1109/PROC.1975.9939.

Sağıroğlu, Ş. & Alkan, M. (2018). *Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık. Ankara: Grafiker Yayınları*, 52–67.

Sağıroğlu, Ş. & Kanca, A. M. (2022). İç Siber Güvenlik Tehdit Bilgisi Paylaşımı. *Siber Güvenlik ve Savunma Kitap Serisi 6: Siber Güvenlik Ontolojisi, Tehditler ve Çözümler*, *6*, 67.

Singer, P. W. & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know* (New York, 2014; online edn. http://dx.doi.org/10.1093/wentk/9780199918096.001.0001, Accessed: January 04, 2025.

Zoli, C., Steinberg, L. J., Grabowski, M., & Hermann, M. (2018). Terrorist critical infrastructures, organizational capacity and security risk, Safety Science, Volume 110, Part C, 2018, Pages 121-130, ISSN 0925-7535, https://doi.org/10.1016/j.ssci.2018.05.021.

Şeker, E. (2020). Yapay Zekâ Tekniklerinin/Uygulamalarının Siber Savunmada Kullanımı. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *6*(2), 108-115.

The Guardian. (2024). Germany Summons Russian Envoy Over 2023 Cyber-attacks. *The Guardian.* https://www.theguardian.com/world/article/may/03/germany-says-russians-behind-intolerable-cyber-attack-last-year.

The Wall Street Journal. (2025). How Chinese Hackers Graduated From Clumsy Corporate Thieves to Military Weapons. *The Wall Street Journal*. https://www.wsj.com/tech/cybersecurity/typhoon-china-hackers-military-weapons-97d4ef95.

Tikk, E. & Kaska, K. (2010). Legal Cooperation to Investigate Cyber Incidents: Estonian Case Study and Lessons. 9th European Conference on Information Warfare and Security, Thessaloniki, Greece, 01-02 July. Reading: Academic Publishing Limited, pp 288-294.

Tikk, E. & Kerttunen, M. (Eds.). (2020). *Routledge handbook of international cybersecurity*. The Cyber Dimension of Geopolitical Competition: Strategic Challanges in Cyperspace, London: Routledge.

Tüzün, F. (2022). *Siber Savaşın Yeni Cephesi: Kritik Altyapılar- İstihbarat ve Güvenlik Araştırmaları Merkezi*. Accessed December 28, 2024.https://igam.org.tr/siber-savasin-yeni-cephesi-kritik-altyapilar/.

UAB (2024). Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2024-2028. https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf.

Weiss, M. & Biermann, F. (2021). Cyberspace and the Protection of Critical National Infrastructure. *Journal of Economic Policy Reform*, *26*(3), 250–267. Accessed: December 30, 2024. https://doi.org/10.1080/17487870.2021.1905530.

Yeşilyurt, H. (2015). Finansal Hizmet Sektöründe Siber Güvenlik Riskleri ve Çözüm Yolları: Ödeme Sistemleri ve Tedarik Zinciri Bütünlüğü. *Celal Bayar University Journal of Social Sciences/ Celal Bayar Üniversitesi Sosyal Bilimler Dergisi.* Cilt: 13, Sayı: 2, 97-120. Haziran 2015. Doi Number: 10.18026/cbusos.40441.

Yılmaz, S. & Sağıroğlu, Ş. (2013). Siber Saldırı Hedefleri ve Türkiye'de Siber Güvenlik Stratejisi. 6. *Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı. Ankara: ISC,* 323-331.

Terörizm ve Radikalleşme Araştırmaları Dergisi-TRAD, 2025, 4(2) :266-287 Araştırma Makalesi
Journal of Terrorism and Radicalization Studies-TRAD, 2025, 4(2): 266-287 Research Article
DOI: 10.61314/traddergi.1691794

THE PREDICTIVE TACTICAL ADVANTAGES AND DISADVANTAGES OF ARTIFICIAL INTELLIGENCE IN THE FIELD OF COUNTERTERRORISM

Hatice VAROL DAĞDELEN*

ABSTRACT

The study examines the evolving predictive tactical approaches of states to counter terrorism by utilizing emerging artificial intelligence technologies in a multidimensional manner. The subject under scrutiny in the present study is the development of artificial intelligence in general, and which methods are most prominent in the field of counterterrorism. In this context, firstly the concept of artificial intelligence is discussed, and then the historical development of the concept is focused upon. In the following discussion, the subset of artificial intelligence that is applicable to counterterrorism is analyzed, and the predictive tactical advantages of these subsets are explained. The study delineates a predictive tactical approach to the terrorism threat, accompanied by illustrative applications of technology. The methodological approach employed is qualitative and interpretive. The findings obtained at the conclusion of the study indicate that, despite the success achieved in the field of security by artificial intelligence technologies, there is a necessity for a strict control mechanism with regard to ethical and moral responsibility. It is imperative that the effective and beneficial use of artificial intelligence in the field of security is predicated on the establishment of moral and legal use, transparency, accountability, and systems determined by national and international standards.

Keywords: *Artificial intelligence, Terrorism, Counterterrorism, Machine Learning, Predictive Detection*

TERÖRİZMLE MÜCADELE ALANINDA YAPAY ZEKANIN ÖNGÖRÜCÜ TAKTİK AVANTAJLARI VE DEZAVANTAJLARI

ÖZET

Çalışma, devletlerin gelişen yapay zekâ teknolojilerini kullanarak terörizmle mücadeleye yönelik değişen öngörüsel *(predictive)* taktik yaklaşımlarını çok boyutlu bir şekilde ele almaktadır. Çalışmada incelenen konu genel olarak yapay zekanın gelişimi ve terörizmle mücadele alanında en çok hangi yöntemlerinin öne çıktığıdır. Bu kapsamda öncelikle yapay zekâ kavramı ele alınmış ardından kavramın tarihsel gelişimine odaklanılmıştır. Sonrasında yapay zekanın terörizmle mücadele için kullanılabilecek alt kümelerine yer verilmekte ve bu alt kümelerin öngörüsel taktik avantajları anlatılmıştır. Çalışmada anlatılan terörizm tehdidine yönelik öngörüsel taktik yaklaşım teknolojinin kullanıldığı örnek uygulamalar yer almaktadır. Kullanılan yöntem niteliksel ve yorumlayıcı analizdir. Çalışma sonunda elde edilen bulgular yapay zekâ teknolojileri sayesinde güvenlik alanında başarı elde edilmesine karşın etik ve ahlaki sorumluluğun sıkı bir kontrol mekanizmasına muhtaç olduğu yönündedir. Sonuç olarak yapay zekanın güvenlik alanında etkin ve faydalı kullanımı için gerekli olan şeyler ahlaki ve hukuki kullanım, şeffaflık, hesap verilebilir, ulusal ve uluslararası standartlarda belirlenmiş sistemler kurulmasıyla mümkündür.

Anahtar Kelimeler: *Yapay Zekâ, Terörizm, Terörizmle Mücadele, Makine Öğrenimi, Öngörüsel Tespit.*

* PhD Candidate, TERAM Researcher, hvarol28@gmail.com, ORCID: 0000-0002-3668-3048

INTRODUCTION

The contemporary world is witnessing profound shifts in the security landscape, precipitated by the rapid evolution of threat concepts, technological advancements, and the proliferation of hybrid actors. The field of terrorism is one in which this shift is particularly pronounced. Terrorism is becoming increasingly dispersed, virtual, and unpredictable. These changes in the realm of terrorism have consequently precipitated alterations in this field, particularly due to the inadequacy of the security measures implemented in the period preceding September 11. In a globalized and digitalized world, security measures taken against terrorism have started to be carried out not only in the military field but also in the technological field. Simon, 2011, pp. 47-50: As posited by Ballard et al. (2002, pp. 2-7).

Despite the integration of technology into the security sector having occurred in parallel with weapon technologies, it is the advent of artificial intelligence (AI) and deep learning methods, developed in conjunction with AI, that has primarily driven the advancement of technology in the field of security. AI is defined as a set of systems that can systematically analyze scattered and complex data sets to produce logical results, identify certain patterns, make predictions for tomorrow with yesterday's data, and detect things that are wrong or different from normal (Kaplan, 2019, p. 2).Thanks to its wide usage area and capacity to process big data quickly, AI is not only a post-incident tool for the security field, but also contributes to the development of proactive and preventive strategies with profiling, patterning, face recognition methods and word analysis on social media. For instance, the United States' Defense Advanced Research Projects Agency (DARPA) and the Israeli Internal Security Organization (Shin Bet, Shabak, or Shin Bet) are institutions that utilize AI tools to predict terrorist activities. The operational capabilities of AI are revealed by the features. As Weimann (2016, pp. 1-5) and Russell & Norvig (2016, pp. 1-3) argue.

It is evident that there are numerous technical and tactical advantages inherent in the utilization of artificial intelligence within the domain of security. However, it is imperative to acknowledge that the implementation of this technology transcends the confines of the technical and tactical dimensions. Furthermore, while the operational characteristics of AI are beneficial, there are also ethical, social, cultural and legal debates concerning the development and utilization of the technology system based on AI. In her

seminal work, Shoshana Zuboff conceptualizes the term "surveillance capitalism", as employed in her book The Age of Surveillance Capitalism (2019), as a system in which the use of individual data is of paramount importance in the emerging capitalist system (pp. 203-213). Concerns regarding invasion of privacy, including unauthorized use of personal data, distrust of institutions, and technological biases, have led to questions regarding the use of AI.

Nevertheless, the threat posed by the use of this technology by terrorist organisations is indisputable. It is evident that organisations have the capacity to utilise this technology for a variety of purposes, including the recruitment of new members, the concealment of existing members' identities, the destruction of reputations, and the deceit of security forces through the presentation of false images of their activities. It is imperative to acknowledge that all of these threats have the potential to engender significant security concerns.

The main question of this study is how countries use artificial intelligence technologies in the fight against terrorism. The primary objective of this study is to provide a comprehensive, overarching review of the utilization of artificial intelligence as a method for the early detection of terrorism. The objective of the present study is twofold: firstly, to discuss the challenges currently being faced in this field, and secondly, to provide a perspective on future opportunities for those who are committed to the detection of terrorism using AI. The objective of the present study is to investigate the tactical advantages and disadvantages of AI-enabled technology in the prediction and early detection of terrorist threats. The assumption that is being made in the context of this question is that AI technologies have ethical and social risks as well as tactical advantages by transforming traditional intelligence. The present study offers suggestions for the ethical and social aspects of AI in the fight against terrorism. These suggestions are based on an analysis of the tactical usage of AI in this context. While preparing the recommendations, disadvantageous situations caused by AI are first identified. After the identification of these situations, recommendations are presented for each topic. The primary objective of these recommendations is to enhance the efficacy of AI utilization in the counterterrorism effort.

1. CONCEPTUAL FRAMEWORK AND HISTORICAL DEVELOPMENT

AI is open to diverse interpretations. Russell and Norvig (2016) posit that AI can be defined as a set of systems that are capable of perceiving their environment, making goal-oriented decisions, and undergoing constant development (p. 233). Michael Haenlein and Andreas Kaplan (2019) define AI as a field that encompasses a multitude of processes for the analysis of complex data, with the capability to sub-analyze its constituent elements, and to extend itself to autonomous decision-making processes (p. 2). According to Cole Stryker (2024), the concept refers to the comprehension of human learning by computers, the realization of problem solutions, and the development of creative and autonomous simulations. According to Kathleen McKendrick (2019), the primary objective of AI is not the emulation of the human brain, but rather its transcendence (p. 6). In the NATO terminology dictionary, created by NATO, AI is defined as the field of computer science that enables the analysis of large data sets to perform functions similar to human intelligence, such as reasoning or learning (NATO Term, 2005). In summary, the term 'AI' is a general designation for cognitive programs that possess the capacity for both deep learning and analysis.

Despite the pervasiveness of the notion of AI in contemporary discourse over the past decade, the field traces its origins and definitions to the previous century. It is important to acknowledge that AI has undergone various phases throughout its extensive history, from its inception to the present day. These stages are referred to as the spring, summer, fall and winter of AI (Haenlein & Kaplan, 2019, pp. 2-4).

The genesis of AI can be traced back to the 1940s, a period which bore witness to seminal contributions from both Alan Turing, with his formulation of the Turing Test, and Isaac Asimov, with his robotics stories. The concept transitioned from the domain of science fiction to that of academia in 1956. The initial conceptualization of the notion was undertaken by Marvin Minsky and John McCarthy in 1955. McCarthy, Marvin Minsky, Claude Shannon and Nathaniel Rochester were responsible for the preparation of a working paper for an eight-week congress at Dartmouth College about machine learning. The paper's underlying assumption is that machines should be designed to simulate human learning and intelligence

processes. Consequently, the resultant product will comprise not only a programming language but also a machine language, thereby elucidating the fundamental principles of intelligence. However, it is evident that the existing computers were not deemed adequate for these predictions. Notwithstanding the successful resolution of the hardware issue, it is imperative to consider the absence of efficacious software programs to facilitate the initiation of the project. Consequently, the primary recommendation of the authors of this paper is to comprehend and formulate methodologies for the development of machine learning processes. As demonstrated on pages 12 to 14.

The "Logic Theorist" (LT), developed by Allen Newell and Herbert Simon between 1955 and 1956, was conceived as the inaugural instance of AI. It is evident that, because of LT, machines have now been developed which are capable of emulating human problem-solving skills. In 1961, the pair developed a new program known as "General Problem Solver" (GPS). The GPS system was designed to address more complex objectives than LT, but this process was interrupted due to an incident (Neapolitan & Jiang, 2018, p. 1). The summer period utilized by AI was of a relatively limited duration.

In the late 1970s, the British mathematician James Lighthill published a report on the subject. In his report, Lighthill expressed a negative perspective on the prevailing positive outlook towards AI, characterizing machines as amateurs who have gained experience. According to the author, machines will never be able to compete with human intelligence (Haenlein & Kaplan, 2019, pp. 2-4). The seminal report by Lighthill initiated the winter period of AI technology.

After the five-year winter period of AI, a decline, or stagnation period, ensued until the 1990s. The initial programming that fostered the field, coupled with the critiques directed towards AI, prompted investors to withhold their financial support. Furthermore, the fact that data could not be entered automatically in the initial examples rendered analysis particularly challenging. The manual preparation of data sets has been identified as a contributing factor to the challenges encountered in determining the duration of the studies to be implemented (Haenlein and Kaplan, 2019, pp. 2-4).

In 1997, the world chess championship was won by IBM's Deep Blue, a supercomputer, over the then-current world champion, Kasparov. This event led to a resurgence of interest in the field of AI studies (IBM). After this, the development of Google Translate, search engines and other AI-supported technologies commenced. In the early 2000s, methods such as "decision tree" (DT) for AI classification gained popularity.

The rapid development of AI technology since the 2000s has led to its integration into various fields, including economics, informatics, and security strategies employed by states. The analysis of large data sets, the utilization of decision support systems, the capacity for linguistic analysis and the ability to process information in real-time, all of which are enabled by artificial intelligence (AI)-supported technologies, have collectively created the conditions for the emergence of anticipatory and predictive approaches within the domain of security. The methods employed in the domain of traditional security comprise post-incident intervention techniques. However, with the advent of AI, a change in thinking has occurred, allowing for the prediction of such events in advance.

The utilization of AI technology in the domain of security was initiated by institutions such as DARPA and IARPA, which were established in the USA in 1958. While the benefits provided by these institutions were limited in the early periods, their effectiveness increased with the development of AI technology. As demonstrated in the seminal works of Waibel (2019, pp. 1-12) and DARPA (2023).

The integration of AI technology, which is now prevalent across diverse sectors, into the realm of terrorism prevention signifies a paradigm shift towards a more comprehensive and nuanced approach to security assurance. The implementation of pattern recognition and anomaly detection tasks on large and complex data sets is facilitated by artificial intelligence (AI)-supported applications, which offer high processing power and rapid execution.

2. PREDICTING TERRORISM WITH AI

Terrorism is an area of study which, like any other discipline, is characterized by its low level of predictability. This is because it is a subject which depends on the human factor. The strategic stealth techniques and

self-development capacities of terrorist organizations or radicalized individuals pose a significant security threat that is challenging to analyze.

The application of classical intelligence methods for the early detection of terrorism, which is difficult to analyze, has not always yielded the desired results. In a world that is undergoing rapid change and becoming increasingly virtualized, there is a growing imperative to utilize cutting-edge technologies that are predicated on the analysis of digital traces for the purpose of detecting terrorism in its early stages. The utilization of artificial intelligence facilitates the processing of information derived from disparate and voluminous data layers, culminating in the classification of threats. Within the framework of categorized threats, states establish a prioritized ranking system for their own nations.

It is evident that there are various subsets of AI, with distinct application methods, including DT and random forest (RF). The primary categories encompass supervised learning, unsupervised learning, reinforcement learning, discriminative, generative, narrow or strong AI. Despite the heterogeneity of AI subsets, the process known as deep learning or machine learning occupies a central role in the classification, prediction, clustering, pattern recognition and decision-making stages that it applies to data. Machine learning employs deep neural networks (DNNs), which emulate the complex processes of the human brain.

DNNs are a system of interconnected artificial neurons that have the capacity to learn complex patterns from large data sets (Paris and Donovan, 2019, p. 12). DNNs are composed of multiple layers of artificial neural networks. The multiplicity of these layers is commensurate with the complexity of the data. Each layer processes the data it receives through a series of elementary calculations and then passes it on to the next layer. In order to reduce the error rate of the final version of the data, processes known as back propagation between layers are repeated, thereby characterizing the repetition of the process. Through repetition or back propagation, the network improves over time and increases in accuracy (Zhang et al., 2016, pp. 1-4). It is evident that this learning and development process has enabled the execution of functions such as classification, prediction, clustering, pattern recognition and decision making on a wide variety of data sources.

The utilization of AI classification models, such as DT and RF, is of paramount importance in the realm of terrorism prevention, given their capacity to facilitate both classification and prediction. DT and RF facilitate the identification of terrorist threats, the classification of suspicious behavior and the calculation of risk scores in large and multivariate data sets. As asserted by Lamptey et al. (2023, pp. 1-2). The DT method employs a branching model of the data, analogous to the branching structure of a tree. After each node, the conditions under scrutiny are catalogued in succession. The DT method facilitates the meaningful classification of data, including social media posts, IP mobility, digital footprints, and geographical locations of individuals with whom a suspicious person interacts. The merits of this approach are twofold: firstly, it is comprehensible and secondly, it lends itself to straightforward interpretation. However, DT, which is known to produce clearer results in small data sets, is unable to reach a sufficient level in complex data. As posited by Ali et al. (2012, p. 272), the RF method may be delineated as a forest version of the DT method, which is fundamentally designed as a single tree. In the RF method, each tree is trained using a random subset of the data set, thus creating a model that allows generalization. This method has been demonstrated to produce more reliable and accurate results in comparison with DT. However, the utilization of RF is considerably more challenging than that of DT about processing power and training level (Fratello and Tagliaferri, 2018, p. 374).

The classification structure of AI technologies is generally multidimensional, and is divided into areas such as machine learning, image recognition and processing, deep learning, and language processing. The accuracy rates of these systems, which are derived from supervised and unsupervised learning types, are quite high (Russell & Norvig, 2020, pp. 5). These technologies, which offer innovations in many fields from education to health, have also found a place in the field of security. In the context of counter-terrorism efforts, states employ artificial intelligence (AI) to collect extensive data concerning the interactions of digital content users with each other, their preferences, and other relevant information. However, the digital realm is not solely a medium for ordinary individuals to socialize; it is also a space in which malevolent ideologies are propagated. Weimann (2016) posits that a considerable proportion of radicalization occurs within the digital domain. It is imperative to comprehend, analyze and interpret the language employed in this domain. Digital communication strategies, social

media and online forums, especially popularized by DAESH and used extensively by terrorist organizations, have rendered these areas part and parcel of radicalization, propaganda, organization and intelligence gathering activities. The process of identifying radicalized individuals within social media or digital environments by means of reverse engineering is facilitated by the utilization of AI-supported technology.

To comprehend radicalization in so-called online environments, deep learning-based natural language processing (NLP) techniques are imperative in detecting the ideological language patterns of terrorist organizations. The utilization of NLP facilitates the categorization of social media articles as positive, neutral, or negative, thereby enabling the discernment of the public's stance on the subject matter. The utilisation of NLP facilitates the classification of tweets concerning a particular subject as either "positive", "neutral", or "negative". The objective is to ascertain public sentiment regarding the specified topic. This method is widely used in the commercial sector, for example, The effectiveness of marketing campaigns can be measured by monitoring brand mentions on social media. NLP is a branch of AI that uses machine learning methods to analyse and comprehend natural language. Its utilisation is pervasive, encompassing domains such as marketing, finance, and healthcare. NLP employs machine learning methodologies to analyse the natural language found on social media. The tool is a potent instrument for comprehending and analysing textual material, as well as for formulating decisions based on that comprehension. (Bural, 2021, p. 116).

One of the most significant features of AI technologies in the field of terrorism is the capacity for prediction of behavior. Behavior prediction is predicated on an examination of an individual's past actions, which allows for the prediction of how they will behave in the future. This method facilitates the identification of individuals who sympathize with terrorism or consume radical content, thereby enabling the early prevention of future criminal activity (Pfaff, 2025, p.5). As Helbing et al. (2017) emphasizes the ability of AI to analyze complex data sets quickly and in real time is of paramount importance. It is asserted that the utilization of AI technology will ensure the identification of any details or errors that may be overlooked by human workers.

AI-based image processing systems are utilized for the analysis of images obtained from security cameras or satellite images. In particular, facial recognition technologies have great importance in detecting suspicious individuals in crowds, monitoring illegal crossings and locating wanted persons. These systems have the capacity to be integrated with biometric data, thereby becoming real-time threat detection systems (Garcia-Sanchez et al., 2018). In addition to the aforementioned, data from security cameras employed in the targeting systems of autonomous aircraft is also analyzed by computers that possess deep learning capabilities.

In summary, the advantages of this system can be encapsulated as follows: classification and clustering of data, creation of ideological language patterns through data, behavioral predictions, creation of patterns, fast and real-time analysis of complex and large data, detection of fugitive or criminal individuals, and the capacity to recognize images obtained from autonomous vehicles (see Table 1). The advent of AI-enabled technologies has rendered the analysis of terrorism's logistical sources, individual or organizational connections, radicalization methods, smuggling activities and ideological language patterns a relatively straightforward task.

Table 1. Predictive Tactical Advantages of Artificial Intelligence in Terrorism

Classification and forecasting of big data
Creating ideological language patterns
Behavior prediction
Pattern recognition
Fast and real-time prediction of complex datasets
Recognition of illegal crossings or criminal individuals
Detection of threat elements by analyzing the images obtained by autonomous technology

3. THE DARK SIDE OF PREDICTIVE AI

Although it is recognized that artificial intelligence (AI) offers numerous advantages in numerous domains, there are approaches within the

counterterrorism literature that demonstrate a degree of caution about these technologies, and in some cases, even express criticism. The utilization of AI is not merely a technical concern; it is also a legal, human, social and moral issue. In this section, the primary challenges arising from the utilization of AI in the security sector are examined through the lens of five distinct categories. The categories encompass technical errors, privacy violations, algorithmic bias, democratic oversight and economic problems (see Table 2).

Table 2. Predictive Tactical Disadvantages of Artificial Intelligence in Terrorism

Vulnerability to technical errors
Privacy violations and ethical concerns
Algorithmic biases
Lack of democratic control
Economic problems

It is evident that technical criticisms of AI technologies are derived from the inherent characteristics of AI itself. The technology in question is predicated on the utilization of computers and cyber systems. While analyzing data, there is a possibility of integrating with various applications. In such circumstances, AI itself will be vulnerable to cyber-attacks. Of particular concern is the vulnerability of national security domains, such as the counterterrorism efforts, to potential threats. (PFAFF, 2025, p.10) One of the potential technical errors that can occur is the prediction of future behavior based on past data. Nevertheless, it should be noted that the accuracy of this prediction is questionable in dynamic and non-patterned fields, such as the social sciences.

In instances of so-called 'false positives', systems have the capacity to erroneously identify innocent individuals as suspects, a process which they subsequently deem to be of risk according to their proprietary algorithms. This phenomenon has the potential to not only compromise an individual's reputation but also hinder the apprehension of genuine lawbreakers (Wagner, 2018). Ethical concerns have been identified as a significant critique of AI (see Pfaff, 2025, p. 10; Pauwels, 2020, p. 16). Zuboff (2019) contends that AI surveillance systems have the potential to compromise privacy, autonomy

and freedom. He emphasizes that there is a risk of these systems falling into the hands of authoritarian governments and leading to social insecurity.

Another salient issue in relation to ethical concerns pertains to the equilibrium between security and freedom. The development of AI technologies for the early detection of terrorism has the potential to identify individuals deemed to be at risk. However, this process may also infringe upon individuals' rights and freedoms. It is emphasized that AI technology may become a part of preemptive security practices, which may result in a conflict with liberal legal norms (Amoore, 2013).

The training of artificial intelligence systems is contingent upon the data sets on which they are based. The algorithms may be influenced by historical, cultural or social biases inherent in the datasets. For instance, certain ethnic, religious or regional groups that have been associated with more terrorist links in the past may be classified as high-risk by the systems. This suggests that the automation of discriminatory practices is being encouraged, thereby reinforcing systemic bias (Noble, 2018).

The concept of constant surveillance, as depicted by George Orwell in his renowned work 1984 and as described by Michel Foucault as the metaphor of the panopticon[2], can be considered a form of self-censorship that leads to the internalization of specific behaviors. This state of affairs, particularly within democratic societies, gives rise to significant debates concerning the security-freedom balance. The development of AI technologies for the early prevention of terrorism has the potential to identify individuals deemed to be at risk. However, this identification process may also result in the infringement of individuals' rights and freedoms. It is emphasized that AI technology may become a part of preemptive security practices, which may result in a conflict with liberal legal norms (Amoore, 2013).

Most AI technologies associated with security and terrorism are characterized as 'black boxes'. In the context of a black box system, the general public is unable to ascertain the mechanisms by which processes

[2] The panopticon, invented in the 1700s by Jeremy Bentham. It is a design of a prison building with cells arranged in a circle around a central guard tower. This way, the inmates would never know when the guard was looking their way, and would have to behave as if they were being watched at all times. (Bentham, 2012, pp.13-15)

operate or the rationale underpinning the decisions that are made. Consequently, the system is perceived to be deficient in terms of transparency and accountability. One of the aspects of AI that has been the subject of considerable criticism is the paucity of information, particularly in the realm of trust-based areas such as security. (Pauwels, 2020, p. 19)

Another criticism level in the field is the replacement of systems based on human intelligence with those reliant on artificial intelligence (AI) technologies. Individuals who are no longer required are compelled to face economic instability and unemployment. The threat of unemployment will not only have economic consequences. Individuals facing challenges in meeting their fundamental needs may potentially engender novel security concerns if they are unable to address these needs through legitimate channels. (Pfaff, 2025, p.10)

In conclusion, the disadvantages of predictive tactics offered by AI technologies in the field of terrorism are manifold. However, it should be noted that only the technical and algorithmic elements of these disadvantages pertain to the nature of AI. The remaining aspects are associated with legal, social and ethical domains. Consequently, an inclusive perspective should underpin the beneficial use of this technology.

4. FORECASTING TERRORISM: AI IN ACTION

The utilization of AI in the prevention and combating of terrorism is a prevalent phenomenon. The cases under discussion in this study are drawn from a range of geographical locations. The case studies under consideration herein describe the practices of the United States of America (USA), Israel, China and the European Union, respectively. The units/institutions under discussion are analyzed in only the most general terms.

DARPA was established in 1958 by the United States government with the objective of developing military technology to counter the Soviet Union. It is evident that DARPA has a pioneering and innovative role in AI-enabled threat analysis. The institution has developed programs such as "Total Information Awareness" and "Insight", with the objective of identifying potential threats in advance by analyzing the behavioral patterns of individuals with data taken from the digital environment. It is evident that the areas of work undertaken by DARPA, in addition to those pertaining to artificial intelligence, encompass a range of disciplines including

autonomous systems, cybersecurity, quantum information systems, biotechnology and the advanced weapons industry. As demonstrated in the seminal works of Waibel (2019, pp. 1-12) and DARPA (2023),

The Intelligence Advanced Research Projects Activity (IARPA) was established in 2006. This organization operates in conditions that are more challenging than those faced by DARPA. However, IARPA has developed systems that enable it to analyze radicalization trends on social media. Quantum computing and natural language processing are two examples of AI techniques utilized by IARPA. It is evident that IARPA's notable domains of operation extend beyond the realm of artificial intelligence, encompassing such disciplines as crypto analysis, cyber intelligence, behavior prediction, open-source intelligence, and quantum computing. As demonstrated in the research by Bonvillian (2018, pp. 14–15) and IARPA (2023),

The Israel Internal Security Agency (Shin Bet or Shabak) is an institution that was established in the aftermath of the establishment of the State of Israel. The primary responsibilities of the organisation include the identification and prevention of internal threats, the gathering of intelligence from the region (primarily from Palestine), the protection of high-ranking bureaucrats, and the assurance of the security of critical infrastructure.

The Shin Bet utilizes AI in two primary domains: intelligence collection from Palestine (Gross, 2020; Goldman and Jamieson, 2017) and airport security (Wrobel, 2025; Leichman, 2024). The agency is also engaged in the development of algorithms for the analysis of content shared on social media, with a view to the prevention of potential threats.

The Social Credit System (SCS) of the People's Republic of China is a rating application that evaluates the behavior of individuals, institutions and companies. The evaluation process is informed by "trustworthiness scores." The overarching objective of this system is to enhance national allegiance, curtail criminal activity, and oversee economic management. To illustrate this point, it is noteworthy that individuals who violate traffic regulations experience a decline in their credit scores. Conversely, those who receive social assistance have been observed to see an increase in their credit scores. Furthermore, individuals engaging in protest activities against the state have been documented to face blacklisting, while debtors have been reported to be

subjected to bans from utilizing public transportation. As demonstrated in Creemers (2018, pp. 1-29) and Carbone (2019),

Another system utilized in China is known as Facial Recognition (FR). The development of this system has been primarily focused on leveraging technological advancements that facilitate the identification of individuals through biometric means. It is vital to emphasize that FR is of paramount importance to public safety in China. The system encompasses a broad spectrum of locations, including educational institutions, metropolitan transportation networks, urban centers, and dining establishments. The system has been developed to facilitate the identification of criminal elements by law enforcement agencies.

The utilization of FR technology in the Xinjiang Uyghur Autonomous Region has been the subject of considerable criticism. According to a report by Human Rights Watch (2019), the reverse engineering of a mobile application that enables the use of FR technology in the aforementioned region revealed that Chinese law enforcement agencies were collecting personal data on individuals, targeting them, and sending those arrested to political education camps or other facilities.

The European Police Office (Europol), an organization operating within the European Union (EU), has described AI technologies as an area that will completely transform police institutions in its 2024 report titled "AI and Policing." Europol, an organization which has integrated AI technologies, states that it has made progress in the areas of big data analysis and the identification of potential criminals (Reuters, 2025).

The European Internet Referral Unit (EU IRU) is responsible for the identification and removal of terrorist content in the digital environment. Following the identification of radical content circulating in the digital environment, the EU IRU reports it to the relevant platforms (Aunion, 2025).

5. AI AND THE FUTURE OF TERRORISM PREDICTION

The utilization of AI for the early detection of terrorism, or for counterterrorism purposes, gives rise to a number of changes. These changes are not only operational in nature, but also legal, ethical, social, and institutional. The efficacy of these changes is evident in the positive outcomes observed in state applications. Nevertheless, the pivotal element in guaranteeing the perpetuation of these favorable advancements is the

efficacious and commensurate utilization of AI governance. This section delineates a series of anticipations for the enhancement of the predictive capabilities of AI technologies in the future.

The visions to be developed in the field of AI have the potential to enhance the future applications of existing AI technologies. It is imperative that the vision presented encompasses not only application strategies but also normative elements. This will assist states in ensuring their security while protecting the rights of individuals.

The disadvantages of using AI in the field of terrorism have been discussed in detail in the previous sections of this study. The initial disadvantage pertains to technical errors. Even though AI technology can perform activities that exceed human capacity in many areas, it is essentially a machine learning process. To circumvent technical malfunctions during this process, it is projected that human-supported hybrid AI units will be developed. In contrast to a system that is entirely devoid of human involvement, structures founded upon human-machine collaboration are likely to demonstrate a high degree of success and a low probability of error as the control process unfolds. The system has been designed to transform disadvantages caused by technical errors into advantages.

It is an irrefutable fact that AI technologies are vulnerable to cyberattacks. There are established methods that can be applied to counteract this disadvantage. To illustrate, the following measures may be adopted in order to mitigate the risk of cyber-attacks: firstly, the number of individuals granted access to the system should be limited; secondly, multiple approval processes should be required for team members to gain access to the system; and thirdly, robust firewalls should be constructed.

The second disadvantage that has been discussed in the literature is that of privacy violations. The utilization of democratic control methodologies has been demonstrated to be advantageous in the resolution of privacy violations. Another recommendation is that judicial processes should be maintained to allow for the possibility of injustice, even in circumstances where all security data is not disclosed to individuals. Furthermore, it is imperative that teams utilizing AI technologies in the analysis of data be subject to rigorous oversight and control mechanisms. Access to data will be permitted only in situations where a high level of risk is identified, and

assessments will be conducted within the parameters of the identified risk. The imposition of severe penalties on individuals or institutions responsible for crimes in cases where risk-independent data is used can be considered a factor that increases trust in AI technologies.

As evidenced by the examples of SCS and FR applications supported by AI in China, AI technologies have the potential to be used for malicious purposes in societies where democracy is not fully established. In order to circumvent this issue, it is incumbent upon states to act in accordance with ethical principles, to maintain a balance between security and freedom, and to prefer to preserve their legitimacy in the eyes of the public by conducting transparent processes, thereby increasing their chances of achieving more positive results.

However, it is important to note that the utilization of AI technologies by states should be subject to general rules in international legal circles. The resolution of the aforementioned problem is predicated on the assumption that each state will regulate its AI security units in accordance with international standards and, if necessary, submit annual reports to an international organization to be established. Examples of work conducted in this area include the European Commission's Ethical Guidelines on High-Risk AI Applications (AI HLEG, 2019) and the European Union's Artificial Intelligence Act (AI Act). Despite the pioneering nature of these documents, their scope is somewhat restricted. It is anticipated that in the future, more comprehensive documents will be prepared, and that compliance with these documents by states will have a positive impact on ensuring security.

Another expectation is that institutional capacity will be increased to facilitate the storage and processing of large data sets so that AI technologies can be used more effectively in the future. This will facilitate the sustainable and reusable storage of data. It is imperative that capacity increases be realized at both the technical and institutional levels. Furthermore, it is imperative that personnel engaged in data management undergo periodic training to ensure proficiency and maintain data integrity. This will enable them to learn about ethical concerns, understand the limitations of algorithms, become experts in crisis management, and develop critical approaches to decision support units. About the training of personnel, the relevant security units of each state should prepare modular training programmers in accordance with the AI curriculum. The training provided

here should focus on legal, ethical, sociological, cultural, language skills, and technical issues.

It is important to note that not all data obtained in the field of intelligence is of the same quality. To facilitate the analysis of data with AI-supported technologies, it is essential that the data sets utilized are contemporary, precise, varied, and meticulously prepared with a emphasis on outcomes. It is imperative that the algorithms employed are secure. Furthermore, it is imperative that a uniform standard is adhered to by all institutions involved in the transfer and sharing of data. In order to ensure effective cooperation in the fight against terrorism, the establishment of national and international data pools is imperative. The transfer of data to these pools should be subject to regular monitoring by independent organizations.

In a manner analogous to Asimov's three laws of robotics, which stipulate that robots must not harm humans, the following eight principles can be enumerated. The disadvantages caused by AI technologies may, in the future, be transmuted into advantages. The following steps are recommended to facilitate the enhancement of AI technologies:

- The utilization of human-robot hybrid methodologies is imperative in contemporary research endeavors.
- The utilization of multi-security approval systems is imperative for the access of data.
- The implementation of data collection and analysis processes is to be conducted in a transparent manner.
- It is imperative that national and international legal regulations are revised in order to ensure compatibility with contemporary technological advancements.
- It is imperative to ensure an increase in institutional capacity.
- The preparation of regular and comprehensive training programmers for responsible personnel is of paramount importance.
- The enhancement of data quality is of paramount importance.
- The establishment of national and international data pools is contingent upon effective cooperation.

CONCLUSION

The evolving technological landscape is precipitating profound changes and transformations within the domain of security. In particular, the rapid

advancements in AI technologies, which have been increasing exponentially in recent years and are expanding their areas of application on a daily basis, are bringing about profound changes. AI technologies are being used in a variety of fields. These include the creation of large data clusters in the digital realm that can be understood by humans. They also include tracking and prevention of radicalization processes. In addition, they are used for the identification of fugitives or criminals through biometric identification. They are also used for the detection of abnormal behaviors, the making of behavior predictions and the creation of language patterns.. AI technologies can analyze past events and utilizing behavior prediction and pattern recognition methods to predict crimes that are likely to occur. It is evident that these features underpin a proactive and preventive paradigm shift in the field of terrorism, as represented by AI technologies.

However, as with any innovation, this technological advancement gives rise to controversial issues. Even though AI technologies are planned to reach or even surpass human intelligence, these systems have the potential to make technical errors. Furthermore, individuals have ethical concerns regarding the collection and analysis of data. These ethical concerns, termed privacy violations, are substantiated by the example of China.

It is impossible to predict the analyses produced by AI technologies due to the openness of their learning processes to intervention. This is one of the factors that could lead to individuals being discriminated against or suffering unjust loss of reputation. The absence of democratic oversight in data collection and analysis processes gives rise to concerns regarding the reliability of the system. While it is reasonable that data should not be disclosed to the public due to its confidentiality, it is important that the institutional system to be established is subject to regular monitoring. Another problem posed by AI technologies is the unemployment problem seen in every technological innovation. The utilization of AI in data analysis can facilitate the preparation of data sets that would otherwise require months of analysis to complete within a matter of hours.

In conclusion, it is evident that AI is a powerful and transformative tool for the early detection and prevention of terrorism. Nevertheless, it is imperative that this power is utilized in a more proactive manner, with a view to generating social benefits. The cornerstone of this transformation is the balance between freedom and security. It is imperative that the security

environment provided by technology does not impede personal freedoms. In this context, the utilization of artificial intelligence within the domain of security should be regarded as a political decision and an issue of values, as opposed to a mere technical advancement. Consequently, governance models should be constructed in accordance with this perspective.

REFERENCES

Aldrich, D. P. (2021). *Black wave: The Saudi-Iran wars on terror*. Oxford University Press.

Ali, J., Khan, R., Ahmad, N., & Maqsood, I. (2012). Random forests and decision trees. *International Journal of Computer Science Issues (IJCSI), 9*(5), 272.

Aunion, J. A. (February 28, 2025). *Aunque la víctima sea artificial, el crimen es real: 25 detenidos en una operación internacional contra la pornografía infantil creada con IA.* El País. Access date: 25.04.2025. https://elpais.com/sociedad/2025-02-28/aunque-la-victima-sea-artificial-el-crimen-es-real-25-detenidos-en-una-operacion-internacional-contra-la-pornografia-infantil-creada-con-ia.html

Ballard, J. D., Hornik, J. G., & McKenzie, D. (2002). Technological facilitation of terrorism: Definitional, legal, and policy issues. *American Behavioral Scientist, 45*(6), 989-1016.

Bentham, J. (2012). The Panopticon. In *Offenders or Citizens?* Antony Duff (Ed.) (pp. 13-15). Routledge.

Bural, E. B. (2021). *Sosyal Medya İstihbaratı*. Yeditepe Akademi Yayınları

Bonvillian, W. B. (2018). DARPA and its ARPA-E and IARPA clones: A unique innovation organization model. *Industrial and Corporate Change, 27*(5): 897–914.

Carbone, C. (February 22, 2019). *China bans 23 million from traveling as part of citizen report card system*. Fox News. Access date: 24.04.2025. https://www.foxnews.com/world/china-bans-23-million-from-buying-travel-tickets-as-part-of-social-credit-scoring-system

Creemers, R. (2018). *China's social credit system: An evolving practice of control*. SSRN.

DARPA. (2023). *Defense Advanced Research Projects Agency*. Access date: 30.03.2025. https://www.darpa.mil

Fratello, M., & Tagliaferri, R. (2018). Decision trees and random forests. In *Encyclopedia of bioinformatics and computational biology: ABC of bioinformatics* 1: 374.

Goldman, P., & Jamieson, A. (January 30, 2017). *Hamas used fake social media accounts to hack Israeli soldiers' phones: IDF*. NBC News. Access date: 20.03.2025. https://www.nbcnews.com/news/world/hamas-used-fake-social-media-accounts-hack-israeli-soldiers-phones-n706036

Gross, J. A. (February 17, 2020). *IDF: Hamas again tries to 'catfish' soldiers with fake women on social media.* Times of Israel. Access date: 20.03.2025. https://www.timesofisrael.com/idf-hamas-again-tries-to-catfish-soldiers-with-fake-women-on-social-media/

Haenlein, M., & Kaplan, A. (2019). A brief history of artificial intelligence: On the past, present, and future of artificial intelligence. *California Management Review*, *61*(4): 5–14.

Human Rights Watch. (May 1, 2019). *China's algorithms of repression: Reverse engineering a Xinjiang police mass surveillance app*. Access date: 20.03.2025. https://www.hrw.org/report/2019/05/01/chinas-algorithms-repression/reverse-engineering-xinjiang-police-mass

IARPA. (2023). *Intelligence advanced research projects activity*. Access date:10.03.2025. https://www.iarpa.gov

IBM. (n.d.). *Deep blue*. Access date: 25.04.2025. https://www.ibm.com/history/deep-blue

Lamptey, O., Gegov, A., Ouelhadj, D., Hopgood, A., & Da Deppo, S. (2023, June). Neural Network Based Identification of Terrorist Groups Using Explainable Artificial Intelligence. In *2023 IEEE Conference on Artificial Intelligence (CAI)* (pp. 191-192). IEEE.

McKendrick, K. (2019). *Artificial intelligence prediction and counterterrorism*. Chatham House.

NATOTerm. (n.d.). NATO Terminology Database. Access date: 10.03.2025. https://nso.nato.int/natoterm/Web.mvc

Paris, B., & Donovan, J. (2019). *Deepfakes and cheap fakes: The manipulation of audio and visual evidence.* Data & Society Research Institute, 12.

Reuters. (18 Mart 2025). Europol warns of AI-driven crime threats. Access date: 13.04.2025. https://www.reuters.com/world/europe/europol-warns-ai-driven-crime-threats-2025-03-18/

Russell, S., & Norvig, P. (2016). *Artificial intelligence: A modern approach* (3rd ed.). Pearson Education.

Simon, J. D. (2011). Technological and lone operator terrorism: Prospects for a fifth wave of global terrorism. In *Terrorism, identity and legitimacy: The four waves theory and political violence*. Jean E. Rosenfeld (Ed.). (pp.44-66) Routledge.

Wagner, B. (2018). Ethics as an escape from regulation: From ethics-washing to ethics-shopping? In *Being profiling*. Amsterdam University Press.

Waibel, A. (2019). *What is DARPA? How to design successful technology disruption.* Access date: 13.04.2025. https://isl.iar.kit.edu/downloads/WhatIsDarpa.Waibel.pdf

Weimann, G. (2016). *Terrorism in cyberspace: The next generation*. Columbia University Press.

Wirtz, B. W., & Müller, W. M. (2019). Artificial intelligence and the public sector—Applications and challenges. *International Journal of Public Administration*, *42*(7): 596–615.

Zhang, J., Zheng, Y., Qi, D., Li, R., & Yi, X. (November 2016). DNN-based prediction model for spatio-temporal data. In *Proceedings of the 24th ACM SIGSPATIAL International Conference on Advances in Geographic Information Systems*. 1–4.

Zuboff, S. (2019). The age of surveillance capitalism. In *Social theory re-wired*. Longhofer, W., & Winchester, D. (Ed.) (pp.203-213) Routledge.

Terörizm ve Radikalleşme Araştırmaları Dergisi-TRAD, 2025, 4(2) : 288-297 Kitap İncelemesi
Journal of Terrorism and Radicalization Studies-TRAD, 2025, 4(2): 288-297 Book Review
DOI: 10.61314/traddergi.1702252

UNDERSTANDING THE PKK TERRORIST ORGANISATION: CAPABILITIES, PROPAGANDA, AND SYSTEM

Özdemir AKBAL[*]

Erkmen, Serhat A., and Burak Güneş, eds. *Anatomy of a Terrorist Organisation: The Kurdistan Workers' Party*. Cambridge Scholars Publishing, 2025. 507 pp. ISBN 9781036444884.

Published in 2025 by Cambridge Scholars Publishing and edited by Dr. Serhat Erkmen and Dr. Burak Güneş, *Anatomy of a Terrorist Organisation: The Kurdistan Workers' Party* offers an interdisciplinary perspective on the historical development, ideological transformation, and operational strategies of the separatist terrorist organization PKK. This edited volume serves as a comprehensive reference work for scholars in the fields of security studies, international relations, political science, sociology, and psychology. In addition, it offers valuable insights for policymakers, members of the security bureaucracy, and postgraduate students interested in terrorism and insurgent movements. By integrating multiple disciplinary lenses, the book provides an in-depth examination of the PKK's historical evolution, ideological shifts, and operational strategies, making it a significant contribution to both the academic literature and policy-relevant debates on terrorism.

Over the past five decades, the organizational activities of the PKK have resulted in significant civilian casualties, affecting individuals from various professional and social backgrounds, including children, educators, and technical personnel. Beyond the widespread civilian casualties, the PKK's activities have placed a substantial economic strain on Türkiye's national budget, particularly in terms of security expenditures and lost economic productivity. The inclusion of fallen soldiers, law enforcement officers, and local security personnel further underscores the magnitude of Türkiye's human losses in the context of its counterterrorism efforts. Given the scope

[*] Dr., Trakya Üniversitesi, ozdemirakbal@gmail.com, ORCID: 0000-0001-7030-7946.

and persistence of the PKK-related conflict, the literature dedicated exclusively to this organization has expanded to such an extent that it now represents a standalone domain within the broader field of terrorism and security studies. What sets this study apart from earlier works is its integrative approach, which synthesizes diverse analytical perspectives within a political science framework to offer a more comprehensive understanding of the subject.

Comprising a total of 19 chapters, the volume features contributions from academics who have conducted long-standing research on the specific topics addressed in each section. Thus, the volume emerges as a work capable of addressing the operational dynamics of a terrorist organization from a wide range of disciplinary and analytical perspectives, offering insights regardless of the lens through which the subject is approached. Accordingly, the book offers a wide-ranging analytical framework through which readers can explore the actions, organizational structure, and strategic objectives of the separatist terrorist organisation PKK, spanning fields from political psychology and political economy to theories and strategies of international politics.

Authored by the book's editors, Dr. Serhat A. Erkmen and Dr. Burak Güneş, the introductory chapter highlights that the PKK should not be understood merely as a terrorist entity, but as an organization sustained by a broad financial infrastructure, including narcotics trafficking and human smuggling. Furthermore, the introduction is notable for its detailed examination of the PKK's international organizational network and the support it has received from various state actors.

Building upon the foundational themes set out in the introduction, the first chapter, *Describing the PKK: The Anatomy of a Terrorist Organisation in Terms of Organisation, Ideology and Leadership*, is co-authored by Dr. Serhat A. Erkmen and PhD candidate Hatice Varol. Serving as the conceptual cornerstone of the volume, this chapter explores the ideological evolution, structural configuration, and leadership model of the PKK. In doing so, it reveals how the group's pragmatic orientation over time has enabled it to function as a useful proxy for external state actors.

While the first chapter provides a general overview of the PKK—tracing its ideological transformations and pragmatic foundations to form a conceptual baseline for the reader—the second chapter, titled *Terror, Fear of*

Partition and the Sacred Homeland: Re-Membering Collective Trauma Through PKK Actions, authored by Dr. Akif Bahadır Kaynak and Dr. Deniz Ülke Kaynak, delves into the politico-psychological motivations, origins, and objectives underlying the group's actions. The chapter argues that the PKK's objectives extend beyond conventional military and civilian attacks, aiming also to erode the foundational principles of the Turkish state. Framed through the lens of political psychology, it provides a thought-provoking analysis of how a terrorist organization can evolve into a functional instrument within the systemic dynamics of international politics.

Building on the preceding chapter grounded in political psychology, the third chapter, *Continuity and Change in the PKK: An Examination of Evolutionary Dynamics from Foundation to Present*, written by PhD candidate Arman Sert, explores the processes of continuity and transformation in the PKK's trajectory, contextualized through key events from its inception to the contemporary period. Approaching the PKK as a separatist terrorist organization, PhD candidate Sert contends that in the context of the geopolitical power shift from the Soviet Union to U.S., the group has undergone a significant ideological transformation—shifting from its Marxist-Leninist foundations toward a model more aligned with libertarian socialism. Thus, the chapter demonstrates that the transformation initiated in the 1990s reshaped the PKK's understanding of organizational structure, evolving from a rigid Leninist vanguard model toward a framework of democratic confederalism—a shift that is evident in the group's internal configuration and the nature of its actions.

Authored by Dr. Merve Önenli Güven, the fourth chapter—*Radicalization and Indoctrination Processes in the PKK*—focuses on the mechanisms through which the organization fosters radicalization and ideological conditioning. Dr. Önenli Güven contends that the PKK employs a multifaceted indoctrination strategy, grounded in mechanisms that promote the radicalization of individuals within a structurally complex framework. The analysis presented in the chapter draws first on the PKK's official congress resolutions and further substantiates its claims through Abdullah Öcalan's book *Militant Personality in People's War*, which articulates the ideological foundations of militant identity within the organization. After exploring the processes and techniques of radicalization, the chapter shifts its focus to the drivers of recruitment into the PKK, using these motivations as a basis to further analyze the organization's indoctrination strategies.

Building on the preceding analysis of recruitment processes within the context of radicalization, Dr. Muhittin Imıl's fifth chapter, *An Analysis of a Religiousness Without a Kibla: PKK and Religion*, offers a critical examination of the PKK's engagement with religion, framing it as a strategically adaptive element shaped by the organization's evolving ideological and pragmatic orientations. Dr. Imıl's analysis, grounded in the concepts of identity and religious belief, maps out the key dynamics that have shaped the trajectory of Kurdish political life. Building upon this conceptual foundation, the chapter offers an analysis of historical uprisings, interpreting them in terms of identity-based and religious motivations. Following this conceptualization, Dr. Imıl explores the PKK's phases marked by religious ambiguity or secularism, and outlines the internal discursive and ideological mechanisms by which Zoroastrianism has been constructed as a folk religion within the organization.

The sixth chapter marks a departure from the primarily psychopolitical and sociopolitical focus of the earlier sections, directing attention instead to the assessment of the PKK's operational behavior and its capacity for action, analyzed through the lens of organizational effectiveness. The result is the chapter entitled *Analysis of the Transformation in PKK's Actions from the Perspective of Learning Organisations: Drone Attacks*, in which Dr. Selim Kurt critically examines how technological developments have shaped the PKK's operational patterns, framing this transformation within the theory of learning organizations. Although drone warfare has gained considerable attention in contemporary security literature, examining the PKK's use of this strategy from the perspective of organizational learning offers a novel and insightful analytical framework.

Having explored the PKK's drone tactics through the lens of organizational learning in the previous chapter, the reader is next presented with Dr. Gökhan İbrahim Öğünç's analysis, which engages with the argument that organizational survival depends on environmental adaptation—using this framework to assess the PKK's evolving operational similarities with ISIL. In his chapter, *The Effects of ISIS Terrorist Organisation on the Action Strategy of PKK/PYD Terrorist Organisation in Tactical and Technical Aspects*, Dr. Öğünç argues that the tactical and technical similarities between the PKK and ISIL can be explained by the erosion of state authority in Syria and Iraq, which enabled non-state actors to seize control of military capabilities formerly monopolized by state armed

forces. Such cross-organizational fluidity is enabled by militants who act as conduits for the transfer of tactical knowledge and technological capabilities. Dr. Öğünç thus introduces a distinctive perspective by conceptualizing technology transfer as a mechanism that enables the formation of inter-organizational networks, facilitating knowledge exchange and mutual enhancement among terrorist groups.

In the eighth chapter, *PKK Terrorist Organisation's Propaganda Activities (1984–2024)*, Bora İyiat provides a detailed analysis of the propaganda strategies utilized by the PKK over a forty-year period. Advancing the argument that the PKK's propaganda methods mirror Western models—especially those outlined in NATO manuals—İyiat observes that the organization has shown a consistent preference for radio as a primary tool within the realm of conventional media. İyiat highlights that while the PKK has relied on conventional media, especially television broadcasting, to sustain militant morale, it has simultaneously turned to websites and social media networks as tools for expanding its recruitment base and attracting sympathizers.

Authored by Erol Başaran Bural, the ninth chapter—*PKK Terrorist Organisation's Social Media Propaganda*—focuses on the organization's evolving use of social media as a strategic propaganda tool. Building on the general overview of propaganda strategies presented in the previous chapter, the ninth chapter provides a more focused examination of the PKK's use of social media, enabling readers to gain a deeper understanding of both the organization's overarching propaganda logic and its digital execution. Bural begins his chapter with a reference to Dr. Tahir Tamer Kumkale, underscoring the intrinsic connection between propaganda and the tactical methods employed in terrorism. By outlining the PKK's conventional propaganda methods, the chapter maintains a cohesive narrative that complements and builds upon the discussions presented in the two preceding chapters. Bural identifies the intended uses of social media and argues that its widespread adoption for propaganda by terrorist organizations—especially the PKK—can be attributed to the low cost and ease of access associated with these digital platforms. Furthermore, by asserting that social media facilitates the PKK's access to emerging technologies, Bural presents a cohesive analysis that complements previous chapters focusing on the group's technological adaptability and operational evolution. Building on his previous observations, Bural focuses specifically on the PKK's strategic use

of Twitter, emphasizing the platform's affordability, ease of access, and its effectiveness in mobilizing targeted social groups.

Authored by Dr. Fatma Anıl Öztop, the tenth chapter—*Female Militants in PKK*—examines the role and significance of female participation within the organization. Dr. Öztop explores how female militants have moved beyond conventional roles within the organization, adopting what is described as a more innovative and proactive pattern of engagement in terrorist activities. Dr. Öztop argues that women's motivations for joining the organization are shaped initially by socio-economic hardship, perceived persecution and discrimination, and gender-based inequality. These are subsequently reinforced by ideological aspirations such as the pursuit of liberation, shared grievances, familial loyalty, and a strong sense of mission and heroism. The chapter highlights the multifaceted involvement of female militants, emphasizing their roles that span from fundraising activities to active participation in public protests and demonstrations. Furthermore, Dr. Öztop emphasizes that women have assumed a prominent role in the organization's suicide operations, accounting for 71% of such attacks since 1996. Identifying increased social recognition as one of the primary motives behind the PKK's recruitment of female militants, Dr. Öztop underscores the critical role that women play not only in operational activities but also in the organization's broader membership and image-building strategies.

In the eleventh chapter, titled *Child Abuse by PKK Terrorist Organisation*, Dr. Begüm Çardak builds upon the preceding discussion of female militants by presenting a significant study on another inhumane practice of the PKK: the exploitation and abuse of children. The chapter opens with a conceptual discussion of child abuse, outlining its historical development and evolution as a recognized phenomenon. Building on the initial conceptual framework, the chapter traces the emergence of the child abuse concept in international discourse and analyzes the involvement of children in the context of armed conflicts. Building upon her analysis of how terrorist organizations utilize children, Dr. Çardak specifically investigates the PKK's use of child recruits between 1987 and 1991 through its so-called youth organization, detailing the roles children played both in urban operations and in the group's rural (mountain) units. Highlighting that the PKK—partially inspired by the Intifada—attaches strategic importance to child exploitation as a means of acquiring legitimacy and social approval, the chapter, together with the preceding one, provides readers with a

comprehensive and nuanced perspective on the instrumentalization of women and children in terrorist organizations.

Chapter twelve focuses on the often-overlooked economic impact of terrorism. Dr. Necmettin Çelik, in his chapter *The Effects of PKK Terrorism on the Turkish Economy*, brings attention to a largely overlooked dimension of terrorism by examining the long-term economic repercussions of the PKK's activities over the past fifty years. Dr. Çelik highlights that beyond the immediate effects, the indirect consequences of terrorism have significantly undermined economic activity, leading to broader disturbances in macroeconomic equilibrium. By presenting the direct economic impacts of PKK-related violence in a detailed table, Dr. Çelik demonstrates that the financial losses incurred amount to several hundred billion dollars. The chapter underscores that the PKK's operations have not only targeted military objectives but have also produced significant indirect economic consequences. Dr. Çelik highlights that the organization's secondary objective appears to be economic destabilization, as illustrated by the decline in tourism revenues and the negative effects on private sector activity between 2014 and 2018.

Authored by PhD candidate Yasin Yıldız, the thirteenth chapter—*The Relationship Between the PKK and Radical Leftist Organisations in Türkiye: Continuity or Rupture?* —examines the historical and ideological connections between the PKK and radical leftist movements in Türkiye. PhD candidate Yıldız analyzes the ties between radical leftist movements and the PKK through the lens of radicalism, situating the processes of ideological alignment and rupture among terrorist organizations within a broader historical context. Based on this analytical framework, PhD candidate Yıldız asserts that the PKK gradually distanced itself from its leftist ideological roots and transitioned toward a discourse increasingly shaped by nationalist themes. Yıldız argues that during the Cold War, the groups that formed the nucleus of the PKK were closely aligned with leftist movements, and he critically examines the ideological roots of Kurdish nationalist formations within this leftist tradition. The chapter analyzes how the disintegration of the Soviet Union and the subsequent erosion of ideological legitimacy among leftist structures in the post–Cold War era contributed to the PKK's ideological shift. PhD candidate Yıldız introduces the concept of "Türkiyefication" to describe the PKK's shift toward a more localized ideological orientation during this period, effectively linking his analysis to

the broader arguments developed in earlier chapters of the volume. In addition, the chapter examines how the post-9/11 global security environment and the dynamics of the Syrian Civil War have influenced the PKK's ideological trajectory, culminating in a contemporary reassessment of the organization's ideological positioning.

In the fourteenth chapter, *Analysis of PKK/KCK Terrorist Organisation Youth Structures*, Dr. Alper Güneş highlights the organization's strategic attempt to influence social groups as part of a broader revolutionary agenda targeting the transformation of the current socio-political order—an approach that mirrors patterns observed in comparable terrorist organizations. Dr. Güneş argues that from the earliest stages of its formation, the PKK has strategically prioritized youth mobilization as a dual-purpose mechanism—serving both as a recruitment reservoir and a critical tool for ideological propagation. The chapter employs a chronological framework, beginning with an analysis of the Kurdistan Revolutionaries—a group active prior to the official founding of the PKK—as an early precursor to the organization's youth mobilization efforts. After detailing the operations of the Kurdistan Student Association—identified as a major recruitment base for the PKK, especially across Europe—the chapter proceeds to explore additional youth organizations and their strategic role in supporting the Civil Defence Units. Moreover, Dr. Güneş elaborates on the PKK's youth organization by examining its functions through youth camps, street-level propaganda, involvement in public events, and on-the-ground activities, presenting a framework that complements the insights offered in the chapters on female militancy and child exploitation.

Authored by Dr. Emre Çıtak, the fifteenth chapter—*PKK/KCK's Shadow and Shadowing in Syria: The Establishment and Evolution of the PYD-YPG*—examines the formation and development of the PYD-YPG within the context of the PKK/KCK network in Syria. Beginning with its founding, the chapter offers an extensive analysis of the PYD-YPG's operations within Syria, presenting a thorough and illustrative account. Following a description of the PYD-YPG's origins and fundamental characteristics, the chapter offers an in-depth examination of the group's pivotal involvement in the Syrian Civil War. Highlighting the PYD-YPG's acquisition of substantial legitimacy through its anti-ISIL operations, Dr. Çıtak then details the changes brought about by Türkiye's subsequent military actions against the organization. In addition to examining the global implications of these

military campaigns, Dr. Çıtak predicts that the group will pursue strategic alliances and assert influence within Syria's shifting power dynamics.

In the sixteenth chapter, Dr. Mehmet Çağatay Abuşoğlu offers an analysis of the PKK's organizational framework in Iran, contributing to the volume with his study titled *PKK's Organisation in Iran*. Following a broad historical introduction, Dr. Abuşoğlu situates his study within the context of Iran's political landscape starting from the era of the Mossadegh government. Emphasizing the post-9/11 era, Dr. Abuşoğlu assesses PJAK's operations within Iran, revealing the significant degree of U.S. backing that the group has received. After outlining the extent of U.S. backing, Dr. Abuşoğlu examines PJAK's involvement in the Syrian Civil War, including a detailed account of the organization's early operations originating from Iran and targeting Türkiye. In his chapter, Dr. Abuşoğlu demonstrates the convergence of U.S. and Iranian interests via their respective backing of proxy groups associated with the terrorist organization.

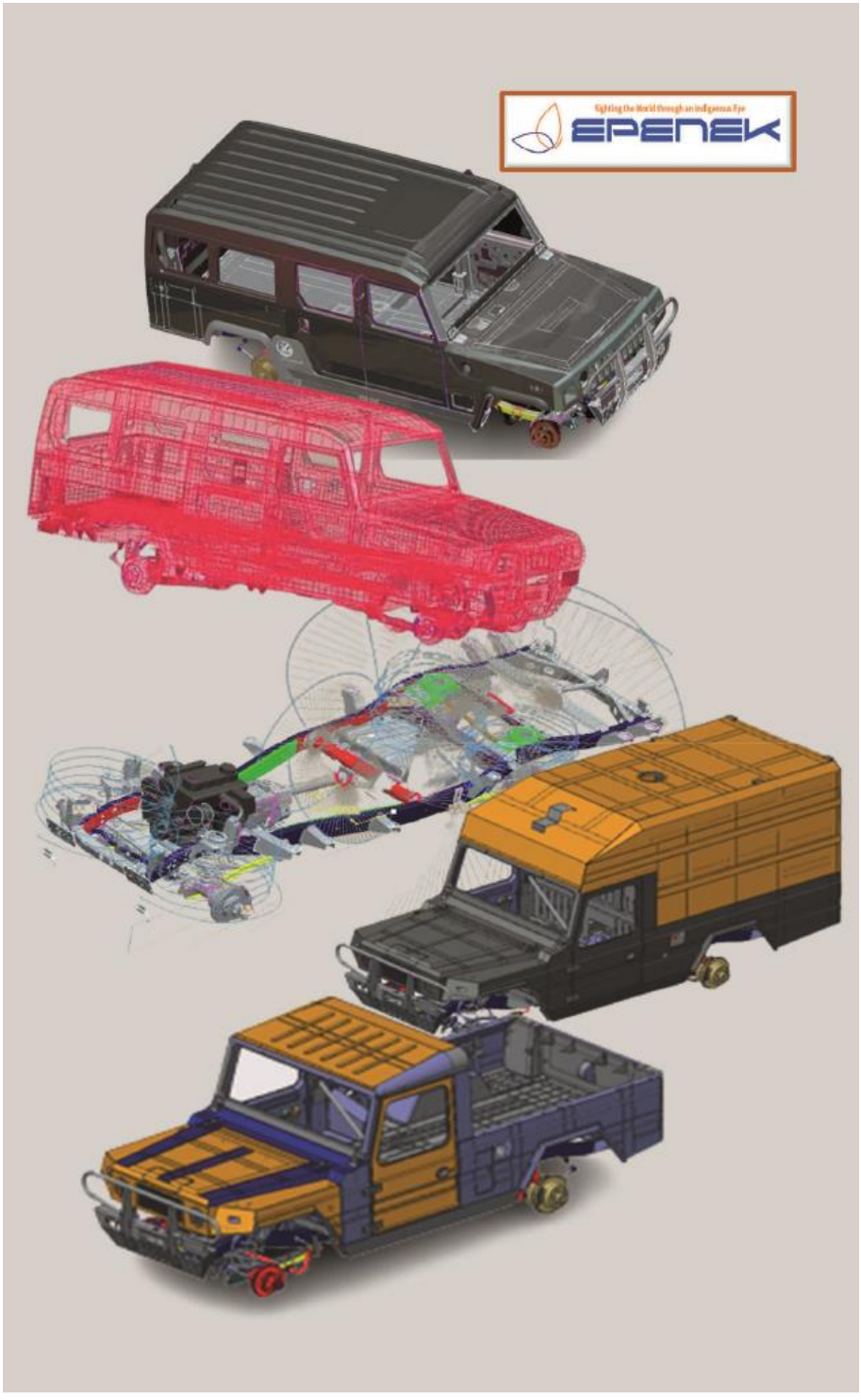
Authored by Dr. Özdemir Akbal, the seventeenth chapter examines how U.S. and the Russian Federation formulate foreign policy strategies by supporting terrorist groups, with a particular focus on the PKK and its Syrian affiliate, the PYD. In his study, which adopts a structural realist perspective, Dr. Akbal elucidates how alliances formed between primary actors—states—and secondary actors such as terrorist organizations function to maintain the status quo. Observing that both U.S. and Russia endorse the PYD in pursuit of their strategic objectives, Dr. Akbal emphasizes how the organization has leveraged this support to enhance its legitimacy.

Building on the discussion of global powers, the eighteenth chapter—*Russia's PKK/PYD/YPG Policy*—authored by Dr. Sabir Askeroğlu, provides an in-depth and nuanced analysis specifically centered on Russia's approach to the PKK and its Syrian affiliates. By revealing the direct nature of Russia's backing for the separatist terrorist group, Dr. Askeroğlu exposes the gap in analyses that typically consider such support exclusively within the context of U.S. policy. Starting with the historical roots of Russia's support, the chapter offers an in-depth analysis of relevant actions from late Tsarist Russia through the Soviet era, followed by a comprehensive overview of the backing provided to separatist terrorist groups in the post-Soviet context. Addressing the conflicts between Türkiye and Russia within the context of the Syrian crisis, Dr. Askeroğlu contends that the Russian Federation backs

the PYD as a strategic proxy to sustain its influence and control in the region.

The final and nineteenth chapter, titled *The US Grand Strategies' Consequences for the Evolving PKK Threat to Türkiye*, is authored by Dr. Özgür Uğurdan. Dr. Uğurdan's chapter complements Dr. Akbal's analysis of the major powers and, subsequently, Dr. Askeroğlu's study of Russia, thereby completing the volume's examination of great power dynamics. Building upon the works of academics like Mackinder and Spykman, Dr. Uğurdan's chapter offers an in-depth examination of the Heartland theory as it applies to the geopolitical dynamics of the Middle East. Drawing on the strategic importance derived from the region's geography, Dr. Uğurdan illustrates how, beginning with World War II, Washington has actively backed separatist movements to advance its interests in the Middle East. The chapter clearly addresses how this U.S. policy became even more pronounced in the post–Cold War period. Focusing on the Bush and Obama eras, the chapter offers an in-depth analysis of separatist movements, highlighting the PKK's historical presence in Syria and the extent of U.S. backing with clarity and detail.

Beyond offering a multifaceted analysis of the PKK's organizational complexity, the book extensively explores the group's developmental trajectory, its involvement in human rights abuses—including the exploitation of women and children—and its relationships with key international stakeholders. The study's integration of distinct disciplinary approaches is particularly valuable. Through this nineteen-chapter volume, readers are provided with a comprehensive resource capable of addressing a wide array of inquiries within the field, effectively consolidating essential knowledge into a single edition. The deliberate organization of closely related perspectives throughout the volume underscores the careful and thorough editorial effort behind the work. This characteristic further establishes the volume as a standout reader within the discipline of terrorism studies.


Sighting the World through an Indigenous Eye
EPENEK

Terörizm ve Radikalleşme Araştırmaları Dergisi
Journal of Terrorism and Radicalization Studies
Cilt/Volume:4 Sayı/Issue:2 Yıl/Year: 2025 Haziran/June
ISSN 2792-0518 (Basılı- Print)
ISSN 2822-2334 (Çevrimiçi- Online)

T
R
A
D

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği
Research Center for Defense Against Terrorism and Radicalization Association

Adres / Address: Beytepe Mah. Kanuni Sultan Süleyman Bulvarı
5387. Cadde No:15A D:58 06800
Çankaya/Ankara
Telefon/Telephone: +90 312 441 11 50
www.tradergisi.com
e-posta/e-mail: editortrad@teram.org