ISSN 2822-3349

İSTİHBARAT ÇALIŞMALARI VE ARAŞTIRMALARI DERGİSİ

Terörizm ve Radikalleşme ile Mücadele
Araştırma Merkezi Derneği
Ankara 2024

İ

Journal of Intelligence Research and Studies

Ç

Cilt/Volume: 3
Sayı/Issue: 2
Yıl/Year: 2024
Haziran/June

A

www.icadergisi.com

D

editor@icadergisi.com

İstihbarat Çalışmaları ve Araştırmaları Dergisi

İÇAD

Journal of Intelligence Research and Studies

ISSN 2822-3349 (Basılı/Print)

ISSN 2822-3357 (Çevrimiçi/Online)

Cilt / Volume: 3 Sayı / Issue: 2 Yıl / Year: 2024

Haziran / June

İSTİHBARAT ÇALIŞMALARI VE ARAŞTIRMALARI DERGİSİ

İÇAD

KÜNYE

ISSN 2822-3349 (Basılı) ISSN 2822-3357 (Çevrimiçi)

İMTİYAZ SAHİBİ

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi (TERAM) Derneği Adına,

Ediz EKİNCİ

SORUMLU YAZI İŞLERİ MÜDÜRÜ

Soner ALAN

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.icadergisi.com

e-posta: editor@icadergisi.com

BASKI

Vadi Grafik Tasarım Reklam Ltd.Şti.

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

Tel: 0312 395 85 71

İÇAD halen "Directory of Research Journals Indexing (DRJI)", "Directory of Open Access Scholarly Resources (ROAD)", "Academic Resource Index", "EuroPub", "Idealonline", "International Institute of Organized Research (I2OR)" ve "Advanced Sciences Index (ASI)" bünyesinde taranmaktadır.

ISSN 2822-3349 (Print) **ISSN 2822-3357 (Online)**

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.icadergisi.com

e-mail: editor@icadergisi.com

PRINTED BY

Vadi Grafik Tasarım Reklam Ltd.Şti.

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

Tel: 0312 395 85 71

İÇAD is indexed in the "Directory of Research Journals Indexing (DRJI)", "Directory of Open Access Scholarly Resources (ROAD)", "Academic Resource Index", "EuroPub", "Idealonline", "International Institute of Organized Research (I2OR)"and "Advanced Sciences Index (ASI)" indexes.

İÇİNDEKİLER / TABLE OF CONTENTS

EDİTÖR'DEN

Merhabalar…

İstihbarat Araştırmaları ve Çalışmaları Dergisi -İÇAD üçüncü Yılına giriyor. İstihbarat Çalışmalarını akademik alanda geliştirmeyi amaçlarken özellikle Türkiye'de bu konuda bir farkındalık oluşturmayı hedefleyen dergimiz tüm zorluklara rağmen yoluna istikrarlı bir biçimde devam etmektedir. Bu çerçevede yeni çalışmalarla karşınızdayız.

Her sayımızda olduğu gibi bu sayımızda da öncelikle akademik bir mülakata yer verdik. Bu sayımızdaki mülakat konuğumuz Doçent Dr. Erik J. Dahl oldu. ABD Ordusunda uzun yıllar görev yaptıktan sonra "İstihbarat Çalışmaları" alanına akademik olarak katkıda bulunmaya başlayan Dahl son yıllarda özellikle "İstihbarat Başarısızlığı" kavramı üzerine önemli eserler vermiştir. 2023 yılında istihbarat servisleri açısından güçlü olduğu düşünülen ülkelerin yaşadıkları istihbarat başarısızlıkları Dahl'ın bu konuda yazdıklarının önemini göstermiştir. İÇAD olarak Eric Dahl ile akademik alanda istihbarat çalışması yapmanın zorlukları, akademi ve uygulayıcılar arasındaki etkileşim, istihbarat başarısızlığının nedenleri ve terörizm ile istihbarat arasındaki ilişki konularında bir mülakat gerçekleştirdik.

Dergimizde, mülakatın yanısıra üç makale yer almaktadır. Bu makalelerden ilki Pınar Demirci tarafından hazırlanan "Siber Güvenlikte Siber Gözetim: Pegasus Projesi"dir. İsrail kökenli bir şirketin geliştirdiği Pegasus isimli casus yazılımın istihbarat alanındaki etkilerinin tartışıldığı makale siber güvenlik, istihbarat faaliyetleri ve hükümetler arasındaki ilişkiyi ele almaktadır.

Bu sayımızdaki ikinci makalemiz literatürde pek fazla işlenmeyen konulardan birisiyle ilişkilidir. İbrahim Rasulov ve Murat Jane tarafından hazırlanan "Stratejik İstihbarat ve Örtülü Operasyonların Dış Politikada Önemi: İran'ın Balkanlar Politikası (Bosna Hersek ve Arnavutluk Örneği) başlıklı makalede İran'ın Balkanlar'da uygulamış olduğu politika, Bosna Hersek ve Arnavutluk üzerinden stratejik istihbaratın uzun vadeli planlaması ve örtülü operasyonlar kapsamında incelenmiştir.

Son çalışmamız ise Mücahit Dizman tarafından hazırlanmıştır. Dizman'ın "Egmont Grubu Stratejik Planı (2022-2027) Kapsamında Terörizmin Finansmanı İle Mali İstihbarat İlişkisi" adlı makalesinde uluslararası mali istihbarat kuruluşu olan Egmont Grubu'nun Stratejik Planı

(2022-2027) incelenerek terörizmin finansmanıyla mücadelede istihbarat araçlarının etkin şekilde kullanılması süreci incelenmektedir.

Gelecek sayımızda görüşmek üzere…

İÇAD Editörü

Prof.Dr.Serhat ERKMEN

INTERVIEW WITH ASSOC. PROF. ERIK J. DAHL: INTELLIGENCE OFTEN FAILS TO "CONNECT THE DOTS"

ABSTRACT

Journal of Intelligence Research and Studies (İÇAD) is pleased to host an interview with Associate Professor Erik J. Dahl. Dahl was a pre-doctoral research fellow from 2006 to 2008 at the Belfer Center for Science and International Affairs at Harvard's Kennedy School of Government. He received his Ph.D. from the Fletcher School of Tufts University, from which he also received a Master of Arts in Law and Diplomacy. In addition, he holds master's degrees from the Naval War College and the London School of Economics, and a bachelor's degree from Harvard. His research focuses on intelligence, terrorism, homeland defence, and homeland security. His book, "Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond" was published by Georgetown University Press in 2013. His latest book is "The COVID-19 Intelligence Failure: Why Warning Was Not Enough", was published by Georgetown in 2023. Dahl's work has been published in Political Science Quarterly, Studies in Conflict and Terrorism, Intelligence and National Security, The International Journal of Intelligence and Counterintelligence, Strategic Studies Quarterly, Homeland Security Affairs, The Journal of Strategic Studies, Defense Studies, The Journal of Policing, Intelligence and Counter Terrorism, and The Naval War College Review among others. Dahl retired from the U.S. Navy in 2002 after serving 21 years as an intelligence officer. From 1999 to 2002, he served on the faculty of the Naval War College in Newport, Rhode Island. He is a former Chair of the Intelligence Studies Section of the International Studies Association. Erik Dahl joined the faculty of the Department of National Security Affairs in September 2008, and he is currently an Associate Professor of National Security Affairs. He is also on the faculty of the Center for Homeland Defense and Security at Naval Postgraduate School.

Keywords: *Intelligence Studies, Intelligence Failure, Intelligence Against Terrorism, Surprise, Future of Secret Intelligence.*

İÇAD: First of all, thank you for accepting the interview request from the Journal of Intelligence Research and Studies (İÇAD). Sir, you served for the U.S. Navy for 21 years as an intelligence officer. And you are also working on secret intelligence in academic field. Therefore you have experience in both practice of intelligence and studying it. In this context our first question is about intelligence studies. Are there any difficulties in studying intelligence in the academic field? What should be the purpose of intelligence studies in the academic field? What issues should intelligence researchers focus on to increase the intelligence capabilities of the states? What are the main gaps in the literature?

Assoc.Prof. Erik Dahl: Thank you very much for interviewing me. It is a pleasure to speak with you. The field of intelligence studies has existed for many years, but it has become especially popular since the 9/11 attacks. There are many challenges in studying intelligence, such as that so much of what our governments do in terms of intelligence is secret. But I think it is important to study intelligence despite these challenges, because we see every day that intelligence is becoming more important around the world, and there are more kinds of intelligence and intelligence organizations being developed today, such as private organizations and new types of open source intelligence.

I think the academic study of intelligence is important for two main reasons. First, because it is a very good way for young people and others interested in the field of intelligence to learn about it. And second, because it is important for all of us to understand intelligence better. I think some of the most exciting areas of study concern new technologies such as artificial intelligence, and how we can use these tools to understand our world better.

İÇAD: Our second question is more related to the interaction between the academia and practitioners. How do practitioners perceive the intelligence scholars and their works? In the last few decades, dozens of books and hundreds of articles have released all around the world. Do you believe that these academic pieces affect scope and implementation of intelligence works?

Assoc.Prof. Erik Dahl: I have to say that during my career as a military intelligence officer I didn't read much academic work on intelligence. I was too busy with my job, and I didn't understand the value that can come from the many articles and books written on intelligence. But now that I have the experience of working both as an intelligence practitioner and intelligence scholar, I can see that these two worlds are closely related. For example, the CIA has a very well-known intelligence studies journal, Studies in Intelligence, with many articles available on the internet. And many serving intelligence officers take time from their careers to study intelligence, often getting a master's degree, which they can later use in their regular work.

İÇAD: As a part of the intelligence studies, there is still an ongoing debate about the intelligence failure. You also have many studies on intelligence failure. You have a book named, "Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond". In order to keep up to

date, I would like to ask you a question about the Israel-Hamas conflict. Do you think that Hamas's attack was an Israeli intelligence failure or not? Why and how?

Assoc.Prof. Erik Dahl: The Hamas attack on Israel on October 7, 2023, was clearly a major intelligence failure for Israel. This failure has been acknowledged by Israeli intelligence leaders, and the director of military intelligence resigned because of it. Although we may not know the full story for several years, after an official Israeli investigation is conducted, it is clear that there had been many different kinds of warnings that Israeli leaders either missed or failed to pay attention to. For example, there are reports that Israeli intelligence got a copy of Hamas's attack plan well before October 7, but leaders didn't believe it. And there were other, more tactical types of warning of increased Hamas activity in the days before the attack, but those warnings, too, seem to have been disregarded.

It is hard to believe that such an advanced intelligence system such as Israel's could have been so completely surprised by an enemy they were watching so closely. And the threat came from the Gaza Strip, right next to Israel. The intelligence failure appears to be as significant as the failure of the Yom Kippur War in 1973, which had come almost exactly 50 years before the October 7 attack. In the case of the Yom Kippur surprise, Israeli leaders were blinded by their belief—what was called "the conception"—that Egypt was not prepared to attack and would not attack for several years. That problem also seems to have occurred in the Hamas attack, as Israeli leaders appear to have been convinced that Hamas would not attempt and could not carry out such a major, coordinated attack.

But there also seem to have been other reasons for the failure, such as that Hamas carried out a very successful deception campaign to convince Israel that it was not planning anything. And we also understand that some of the last-minute tactical warnings came from female border surveillance troops, who were not listened to by their male superiors.

İÇAD: Sir, let's continue our interview on the subject of intelligence failure. As you have discussed in your previous book, "Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond", intelligence failures and surprise effect is in your area of interest. States attach importance to intelligence efforts in order to predict important events that may occur in the future and protect themselves against threats by

producing strategic warnings. I think we all agree that intelligence is the most effective tool used by states to minimize the surprise effect. Although states attach great importance to intelligence and produce huge amounts of intelligence to protect themselves, why are surprise attacks by both conventional threats and terrorist organizations often successful? How it is possible? Does the intelligence community failed to "connect the dots" to create the big picture? Why does intelligence fail, and how can it succeed? And what should the states do to prevent surprise attacks?

Assoc.Prof. Erik Dahl: I think most people would expect that intelligence agencies today would be getting better at anticipating the future. After all, intelligence organizations have increasingly effective tools available to them, including monitoring social media and internet use that can help them track all of our activities. And in many countries, including the United States, the budgets for intelligence agencies are going up every year. But we continue to see that governments and all of us are surprised by new threats and events, including not only the Hamas attack on Israel, but the attack on the U.S. Capitol Building in Washington in 2021, and even the outbreak of the coronavirus in 2020.

How can we explain the continuing problem of surprise and intelligence failure? We often hear that intelligence fails to "connect the dots," and this was one of the common beliefs about what happened before the 9/11 attacks. This suggests that intelligence agencies usually have collected the right information and intelligence—they have "collected the dots." But they haven't analysed that intelligence properly—they haven't connected the dots well enough. Many intelligence experts do not like the "connect the dots" idea, because it seems to make the job of intelligence too simple. All you have to do is connect the dots! But I think there is an important point here, because after almost every major failure we do find that there had been many warnings available—there had been dots, if only someone could have connected them.

But my study of intelligence and surprise shows that too often those warnings that had been collected were not the right kind of warnings. They are usually big-picture, long-term warnings, which we usually call strategic warnings. But for intelligence to be used and to prevent surprise attacks, it needs to be very precise—what we call tactical intelligence. And that's not all: there also needs to be a close, trusting relationship between intelligence

agencies and the policymakers they support. I call this "receptivity"—leaders must be educated about what intelligence can do, and they need to work closely enough with their intelligence advisors that they will listen to the warnings they receive.

İÇAD: In your article titled "Warning of Terror: Explaining the Failure of Intelligence Against Terrorism", you argue that the older literature on intelligence failure should be integrated with the threat of terrorism and that "our understanding of intelligence failure against surprise terrorist attacks should be revised" in the age of terrorism. In this context, could you tell us something about the role and importance of intelligence in the fight against terrorism? Also, as you discussed in your article in 2005, do you think that today our understanding of intelligence failure is being revised and reconstructed within the scope of the threat of terrorism? Do you think we use intelligence effectively in the fight against terrorism? What more can we do in terms of intelligence to protect states against terrorism threats?

Assoc.Prof. Erik Dahl: Here in the United States much of the focus for intelligence and national security has moved away from terrorism toward great power competition, and the threat to peace and security posed by states such as Russia and China. But we know that the threat of terrorism has not gone away, either in the United States, in Turkey, or in other countries around the world. This means we must expect even more from our intelligence agencies and professionals. And I think some of the most difficult challenges for intelligence come in the area of domestic terrorism—terrorism that may not come from international organizations such as al Qaeda and ISIS, but from our own citizens who are radicalized and choose violence for many different reasons. This is difficult because it means that intelligence agencies must monitor our own citizens, and they must respect our civil liberties while still keeping us safe. This is a difficult trade off, but it is important that we have open and frank discussions about this trade off in each of our countries. How many of our civil liberties are we willing to give up in exchange for what may be increased security? I think each of us will have a different answer to that question, but the important thing is that we have that conversation.

İÇAD: Especially after surprise attacks occur in a country, intelligence failure often comes into question. However, it may also be possible that the intelligence services informed the decision makers about the incident, but the

decision makers ignored this warning. In this context, is it possible to encounter problems of intelligence not being understood by policy makers or intelligence not being presented to policy makers by appropriate methods? What might be the reasons why decision makers do not take into account the intelligence presented to them? What should be done to ensure that decision makers take intelligence into account?

Assoc.Prof. Erik Dahl: This is problem of receptivity. As in the case of Israel, how can it be that leaders are not receptive to the intelligence they receive? I think the biggest problem is that often leaders do not understand the warnings they are given, or they do not trust the intelligence professionals who support them. The best way to avoid that problem is for leaders and intelligence professionals to work together regularly, and to develop a close relationship. In the U.S. military, for example, our leaders have often spent time in training courses or in school together with intelligence officers, so that when they serve together in the field later, they already know and trust one another.

But I believe that intelligence professionals also need to work harder to help policymakers understand the information they are giving them. And they should not be afraid to push back once in a while, if they believe that leaders—or any other customers—are not understanding how important a piece of intelligence is. It is not the job of intelligence officers to make policy or tell leaders what to do; but it should be their job to do the best they can to help leaders understand the importance of what they are telling them.

İÇAD: Another question from the recent past is about the Chinese balloon seen in the skies of the USA last year. Was the purpose of this balloon, in a way, to test the intelligence failure or success of the USA? What was the main aim of this spy balloon for you? Does China really need to use a balloon to spy on USA?

Assoc.Prof. Erik Dahl: That Chinese balloon episode was another example of how even the best intelligence systems can be surprised. Although China denies it, this seems clearly to have been a surveillance effort, and our intelligence and warning systems weren't calibrated to detect something that small, and moving that slowly. This shows that even in today's high-tech world, old-fashioned technologies are still important.

İÇAD: As you stated in your article titled "The Plots that Failed: Intelligence Lessons Learned from Unsuccessful Terrorist Attacks Against

the United States", which you wrote in 2011, it seems possible to determine what kind of intelligence and security measures contributed to the prevention of terrorist acts as a result of examining the unsuccessful terrorist attacks. In this context, why some terrorist attacks succeed while the others fail? What kinds of intelligence and security efforts are most useful in preventing terrorist attacks?

Assoc.Prof. Erik Dahl: Because terrorist attacks are tactical-level operations—even if they are able to achieve larger strategic effects—they can best be prevented through the collection and analysis of very specific, tactical-level intelligence. And in addition, my study of unsuccessful terrorist attacks has shown that most plots and attacks are foiled through basic police work, or through tips and reports from neighbours or from other people who see something that worries them. This is good news, because it means that most terrorist plots can be prevented, if we are all watchful. This also means that the more complicated plots are most likely to be prevented, because they involve more people, more time, and more planning—all of which give police and security forces the opportunity to disrupt the plot. But the bad news is that smaller-scale attacks, such as those carried out by lone individuals, can be very difficult to prevent.

İÇAD: In your latest book titled "The COVID-19 Intelligence Failure: Why Warning Was Not Enough" you examined in depth the issues of how medical intelligence is collected and why the intelligence collected on this subject failed. What was the main reason that motivated you to write this book? Could you please tell more about your book?

Assoc.Prof. Erik Dahl: Early on in the pandemic I realized that we were all living through a global intelligence failure—a failure of traditional intelligence agencies, but even more a failure of medical and public health agencies to be able to anticipate and warn us about this new disease before it was able to spread around the world and kill millions of people. And I was struck by how similar this intelligence failure was to past cases such as 9/11, because even though there had been warnings, somehow leaders around the world failed to pay enough attention. I wrote the book for two reasons. First, I wanted to understand what role intelligence and warning played in the pandemic. But even more important, I wanted to find out what we need to do in order to do a better job next time, when the next pandemic or other global health threat arises. I believe we have made important changes in the

areas of disease surveillance, but there is still a lot of work we need to do. We are not yet prepared for the next pandemic.

İÇAD: Prof. Dahl, our last question is about the future of secret intelligence. What will the future of intelligence look like? What will be the threats, challenges, and opportunities for the states in the context of secret intelligence?

Assoc.Prof. Erik Dahl: That is a great question! There are many challenges for intelligence agencies today, but I think there are three that are most important. First, in terms of secret intelligence—spying, or what is technically called espionage—all intelligence services are challenged by the spread of technologies such as facial recognition that are making it harder for people to travel and operate in secret. Second, intelligence agencies are struggling with how to use the many kinds of open source intelligence that are now available. For example, in the United States some experts believe we need to set up a new open source intelligence agency, while others believe that the current system, in which each agency uses open source intelligence in its own say, is best. And the third and I think the biggest challenge will concern technologies such as artificial intelligence. On the one hand, will AI help intelligence agencies do a better job of anticipating future threats? Or on the other hand, will these technologies themselves become threats, as many experts warn?

I don't think anyone knows the answers to these challenges, but I think it is safe to say that the future of intelligence will be a fascinating one, and this means that it is a great time to be studying and thinking about intelligence.

İÇAD: Thank you for answering our questions. Is there anything you would like to add?

Assoc.Prof. Erik Dahl: Thank you very much for all of your questions. I have enjoyed our interview!

DOÇ. DR. ERIK J. DAHL İLE SÖYLEŞİ: İSTİHBARAT GENELLİKLE "NOKTALARI BİRLEŞTİRMEKTE" BAŞARISIZ OLUYOR

ÖZET

İstihbarat Araştırmaları ve Çalışmaları Dergisi (İÇAD) Doçent Dr. Erik J. Dahl ile bir söyleşiye ev sahipliği yapmaktan büyük memnuniyet duymaktadır. Dahl 2006-2008 yılları arasında Harvard Kennedy School of Government'a bağlı Belfer Center for Science and International Affairs'de doktora öncesi araştırma görevlisi olarak çalışmıştır. Doktorasını Tufts Üniversitesi Fletcher School'dan almış ve aynı okuldan Hukuk ve Diplomasi alanında yüksek lisans derecesi almıştır. Ayrıca Deniz Harp Okulu ve London School of Economics'ten yüksek lisans ve Harvard'dan lisans derecelerine sahiptir. Araştırmaları istihbarat, terörizm ve iç güvenlik konularına odaklanmaktadır. "Intelligence and Surprise Attack: Failure and Success from Pearl Harbor to 9/11 and Beyond" adlı kitabı 2013 yılında Georgetown University Press tarafından yayımlanmıştır. Son kitabı olan "The COVID-19 Intelligence Failure: Why Warning Was Not Enough" ise Georgetown tarafından 2023 yılında yayımlanmıştır. Dahl'ın çalışmaları "Political Science Quarterly", "Studies in Conflict and Terrorism", "Intelligence and National Security", "The International Journal of Intelligence and Counterintelligence", "Strategic Studies Quarterly", "Homeland Security Affairs", "The Journal of Strategic Studies", "Defense Studies", "The Journal of Policing", "Intelligence and Counter Terrorism" ve "The Naval War College Review" adlı dergilerde yayımlanmıştır. Dahl, 21 yıl istihbarat subayı olarak görev yaptıktan sonra 2002 yılında ABD Donanmasından emekli olmuştur. 1999'dan 2002'ye kadar Newport, Rhode Island'daki Deniz Harp Akademisi'nde öğretim üyesi olarak görev yapmıştır. Uluslararası Çalışmalar Derneği İstihbarat Çalışmaları Bölümü'nün eski başkanıdır. Erik Dahl, Eylül 2008'de Ulusal Güvenlik Bölümünün öğretim kadrosuna katılmıştır ve halen Ulusal Güvenlik Doçenti olarak görev yapmaktadır. Dahl aynı zamanda Naval Postgraduate School'da İç Güvenlik Merkezi'nin öğretim üyesidir.

Anahtar Kelimeler: *İstihbarat Çalışmaları, İstihbarat Başarısızlığı, Terörizmle Mücadelede İstihbarat, Sürpriz, Gizli İstihbaratın Geleceği.*

İÇAD: Öncelikle İstihbarat Araştırmaları ve Çalışmaları Dergisi'nin (İÇAD) söyleşi talebini kabul ettiğiniz için teşekkür ederiz. Sayın Dahl, 21 yıl ABD Deniz Kuvvetleri'nde istihbarat subayı olarak görev yaptınız. Aynı zamanda akademik alanda istihbarat üzerine çalışıyorsunuz. Dolayısıyla hem istihbarat pratiği hem de istihbarat çalışmaları konusunda deneyim sahibisiniz. Bu bağlamda ilk sorumuz istihbarat çalışmaları hakkında olacak. Akademik alanda istihbarat çalışması yapmanın zorlukları var mı? Akademik alanda istihbarat çalışmalarının amacı ne olmalıdır? Devletlerin istihbarat yeteneklerini artırmak için istihbarat araştırmacıları hangi konulara odaklanmalıdır? Literatürdeki temel boşluklar nelerdir?

Doç.Dr. **Erik Dahl:** Benimle söyleşi yaptığınız için çok teşekkür ederim. İstihbarat çalışmaları uzun yıllardır var olan bir alan, ancak özellikle 11

Eylül saldırılarından sonra popüler hale geldi. İstihbarat alanında çalışmanın pek çok zorluğu var, örneğin hükümetlerimizin istihbarat alanında yaptıklarının büyük bir kısmı gizli. Ancak bu zorluklara rağmen istihbarat üzerine çalışmanın önemli olduğunu düşünüyorum, çünkü her geçen gün istihbaratın dünya çapında daha önemli hale geldiğini görüyoruz. Günümüzde özel kuruluşlar ve yeni açık kaynak istihbaratı gibi daha fazla istihbarat türü ve istihbarat örgütü geliştiriliyor.

İstihbaratın akademik olarak incelenmesinin iki ana nedenden dolayı önemli olduğunu düşünüyorum. Birincisi, gençlerin ve istihbarat alanına ilgi duyan diğer kişilerin bu konuda bilgi edinmeleri için çok iyi bir yol olması. İkincisi ise, istihbaratı daha iyi anlamanın hepimiz için önemli olması. Bence en heyecan verici çalışma alanlarından bazıları yapay zekâ gibi yeni teknolojiler ve bu araçları dünyamızı daha iyi anlamak için nasıl kullanabileceğimizle ilgili.

İÇAD: İkinci sorumuz daha çok akademi ve uygulayıcılar arasındaki etkileşimle ilgili. Uygulayıcılar istihbarat akademisyenlerini ve onların çalışmalarını nasıl algılıyor? Son yıllarda tüm dünyada düzinelerce kitap ve yüzlerce makale yayımlandı. Bu akademik eserlerin istihbarat çalışmalarının kapsamını ve uygulamasını etkilediğine inanıyor musunuz?

Doç.Dr. **Erik Dahl:** Askeri istihbarat subayı olarak kariyerim boyunca istihbarat üzerine çok fazla akademik çalışma okumadığımı söylemeliyim. İşimle çok meşguldüm ve istihbarat üzerine yazılmış birçok makale ve kitaptan elde edilebilecek değeri anlayamadım. Ancak şimdi hem istihbarat uygulayıcısı hem de istihbarat akademisyeni olarak çalışma deneyimine sahip olduğum için bu iki dünyanın birbiriyle yakından ilişkili olduğunu görebiliyorum. Örneğin, Amerika Birleşik Devletleri (ABD) Merkezi Haberalma Teşkilatı'nın (*Central Intelligence Agency – CIA*) çok iyi bilinen bir istihbarat çalışmaları dergisi var, (*Studies in Intelligence*) ve internette pek çok makale mevcut. Görevdeki pek çok istihbarat görevlisi kariyerlerinden zaman ayırarak istihbarat üzerine çalışmakta, genellikle daha sonra normal işlerinde kullanabilecekleri bir yüksek lisans derecesi almaktadırlar.

İÇAD: İstihbarat çalışmalarının bir parçası olarak istihbarat başarısızlığı konusunda hala devam eden bir tartışma var. Sizin de istihbarat zafiyeti üzerine birçok çalışmanız var. "İstihbarat ve Sürpriz Saldırı: Pearl Harbor'dan 11 Eylül ve Ötesine Başarısızlık ve Başarı" isimli bir kitabınız

var. Güncelliği yakalamak adına size İsrail-Hamas çatışmasıyla ilgili bir soru sormak istiyorum. Sizce Hamas'ın saldırısı İsrail istihbaratının bir hatası mıydı, değil miydi? Sizce neden ve nasıl?

Doç.Dr. **Erik Dahl:** Hamas'ın 7 Ekim 2023'te İsrail'e düzenlediği saldırı, İsrail için açıkça büyük bir istihbarat başarısızlığıydı. Bu başarısızlık İsrail istihbarat liderleri tarafından da kabul edilmiş ve askeri istihbarat direktörü bu nedenle istifa etmiştir. Hikâyenin tamamını birkaç yıl boyunca öğrenemeyecek olsak da, resmi bir İsrail soruşturması yürütüldükten sonra, İsrailli liderlerin gözden kaçırdığı ya da dikkat etmediği birçok farklı türde uyarı olduğu açıktır. Örneğin, İsrail istihbaratının Hamas'ın saldırı planının bir kopyasını 7 Ekim'den çok önce aldığı ancak liderlerin buna inanmadığı yönünde haberler var. Saldırıdan önceki günlerde Hamas'ın faaliyetlerinin arttığına dair taktik uyarılar da vardı ancak bu uyarılar da göz ardı edilmiş gibi görünüyor.

İsrail gibi gelişmiş bir istihbarat sisteminin, yakından izlediği bir "düşman" karşısında bu kadar şaşırmış olabileceğine inanmak zor. Üstelik tehdit İsrail'in hemen yanı başındaki Gazze Şeridi'nden geliyordu. İstihbarat başarısızlığı, 7 Ekim saldırısından neredeyse tam 50 yıl önce gerçekleşen 1973'teki Yom Kippur Savaşı'nın başarısızlığı kadar önemli görünüyor. Yom Kippur sürprizinde İsrailli liderler, Mısır'ın saldırmaya hazır olmadığı ve birkaç yıl boyunca saldırmayacağı yönündeki inançları -ki buna "anlayış" deniyordu- nedeniyle kör olmuşlardı. Bu sorun Hamas saldırısında da yaşanmış gibi görünüyor çünkü İsrailli liderler Hamas'ın böylesine büyük ve koordineli bir saldırıya kalkışmayacağına ve bunu gerçekleştiremeyeceğine ikna olmuş görünüyor.

Ancak başarısızlığın başka nedenleri de var gibi görünüyor; örneğin Hamas, İsrail'i bir şey planlamadığına ikna etmek için çok başarılı bir aldatma kampanyası yürüttü. Ayrıca son dakika taktik uyarılarından bazılarının, erkek üstleri tarafından dinlenmeyen kadın sınır gözetleme birliklerinden geldiğini de anlıyoruz.

İÇAD: Dr.Dahl, söyleşimize istihbarat zafiyeti konusuyla devam edelim. "İstihbarat ve Sürpriz Saldırı: Pearl Harbor'dan 11 Eylül ve Ötesine Başarısızlık ve Başarı" adlı kitabınızda da bahsettiğiniz gibi istihbarat başarısızlıkları ve sürpriz etkisi sizin ilgi alanınıza giriyor. Devletler gelecekte meydana gelebilecek önemli olayları önceden tahmin edebilmek ve stratejik uyarılar üreterek kendilerini tehditlere karşı koruyabilmek için

istihbarat çalışmalarına önem verirler. Sürpriz etkisini en aza indirmek için devletlerin kullandığı en etkili aracın istihbarat olduğu konusunda sanırım hepimiz hemfikiriz. Devletler istihbarata büyük önem vermelerine ve kendilerini korumak için çok büyük miktarda istihbarat üretmelerine rağmen neden hem konvansiyonel tehditler hem de terör örgütleri tarafından yapılan sürpriz saldırılar çoğu zaman başarılı olmaktadır? Bu nasıl mümkün olabiliyor? İstihbarat topluluğu büyük resmi oluşturmak için "noktaları birleştirmekte" başarısız mı oluyor? İstihbarat neden başarısız oluyor ve nasıl başarılı olabilir? Devletler sürpriz saldırıları önlemek için ne yapmalıdır?

Doç.Dr. Erik Dahl: Sanırım çoğu insan bugün istihbarat teşkilatlarının geleceği tahmin etme konusunda daha iyi olmasını bekler. Ne de olsa istihbarat örgütleri, tüm faaliyetlerimizi takip etmelerine yardımcı olabilecek sosyal medya ve internet kullanımını izlemek de dâhil olmak üzere giderek daha etkili araçlara sahip oluyorlar. ABD de dâhil olmak üzere pek çok ülkede istihbarat kurumlarının bütçeleri her yıl artıyor. Ancak, sadece Hamas'ın İsrail'e saldırısı değil, 2021'de Washington'daki ABD Kongre Binası'na yapılan saldırı ve hatta 2020'de Koronavirüs salgını da dahil olmak üzere, hükümetlerin ve hepimizin yeni tehditler ve olaylar karşısında şaşırdığını görmeye devam ediyoruz.

Sürpriz ve istihbarat başarısızlığı sorunlarının devam etmesini nasıl açıklayabiliriz? İstihbaratın "noktaları birleştirmekte" başarısız olduğunu sık sık duyarız ve bu konu 11 Eylül saldırılarından önce olanlarla ilgili yaygın inançlardan biriydi. Bu, istihbarat teşkilatlarının genellikle doğru bilgi ve istihbaratı topladıklarını, yani "noktaları topladıklarını" göstermektedir. Ancak bu istihbaratı düzgün bir şekilde analiz etmemişlerdir - noktaları yeterince iyi birleştirmemişlerdir. Pek çok istihbarat uzmanı "noktaları birleştirme" fikrinden hoşlanmıyor çünkü bu fikir istihbarat işini çok basitleştiriyor gibi görünüyor. Tek yapmanız gereken noktaları birleştirmek! Ancak bence burada önemli bir nokta var, çünkü neredeyse her büyük başarısızlıktan sonra birçok uyarının mevcut olduğunu görüyoruz - noktalar vardı, keşke birileri onları birleştirebilseydi.

Ancak istihbarat ve sürpriz üzerine yaptığım çalışma, toplanan bu uyarıların çoğu zaman doğru türden uyarılar olmadığını gösteriyor. Bunlar genellikle stratejik uyarılar olarak adlandırdığımız büyük resimli, uzun vadeli uyarılardı. Ancak istihbaratın kullanılabilmesi ve sürpriz saldırıları önleyebilmesi için çok kesin olması gerekir ki biz buna "taktik istihbarat"

diyoruz. Hepsi bu kadar da değil: istihbarat kurumları ile destekledikleri politika yapıcılar arasında yakın ve güvene dayalı bir ilişki olması da gerekiyor. Ben buna "kavrayış" diyorum -liderler istihbaratın neler yapabileceği konusunda eğitilmeli ve aldıkları uyarıları dinleyecek kadar istihbarat danışmanlarıyla yakın çalışmalıdırlar.

İÇAD: "Terör Uyarısı: Terörizme Karşı İstihbarat Başarısızlığını Açıklamak" başlıklı makalenizde, istihbarat başarısızlığına ilişkin eski literatürün terörizm tehdidiyle bütünleştirilmesi gerektiğini ve terörizm çağında "sürpriz terörist saldırılara karşı istihbarat başarısızlığı anlayışımızın gözden geçirilmesi gerektiğini" savunuyorsunuz. Bu bağlamda bize terörle mücadelede istihbaratın rolü ve önemi hakkında bir şeyler söyleyebilir misiniz? Ayrıca, 2005 yılındaki makalenizde ele aldığınız gibi, bugün istihbarat başarısızlığı anlayışımızın terörizm tehdidi kapsamında gözden geçirildiğini ve yeniden yapılandırıldığını düşünüyor musunuz? Terörle mücadelede istihbaratı etkin bir şekilde kullandığımızı düşünüyor musunuz? Devletleri terörizm tehdidine karşı korumak için istihbarat anlamında daha fazla ne yapabiliriz?

Doç.Dr. **Erik Dahl:** ABD'de istihbarat ve ulusal güvenliğin odak noktası terörizmden uzaklaşarak büyük güç rekabetine, Rusya ve Çin gibi devletlerin barış ve güvenliğe yönelik tehditlerine odaklanmıştır. Ancak ne ABD'de ne Türkiye'de ne de dünyanın diğer ülkelerinde terörizm tehdidinin ortadan kalkmadığını biliyoruz. Bu da istihbarat teşkilatlarımızdan ve profesyonellerimizden daha fazlasını beklememiz gerektiği anlamına geliyor. Bence istihbarat için en zorlayıcı konulardan bazıları iç terörizm - El Kaide ve Irak ve Şam İslam Devleti (IŞİD) gibi uluslararası örgütlerden değil, radikalleşen ve farklı nedenlerle şiddeti seçen kendi vatandaşlarımızdan kaynaklanan terörizm - alanında karşımıza çıkmaktadır. Bu oldukça zordur, zira istihbarat kurumlarının kendi vatandaşlarımızı izlemesi ve bizi güvende tutarken sivil özgürlüklerimize saygı göstermesi gerektiği anlamına gelir. Bu zor bir konudur, ancak ülkelerimizin her birinde bu konu hakkında açık ve dürüst tartışmalar yapmamız önemlidir. Artan güvenlik karşılığında sivil özgürlüklerimizin ne kadarından vazgeçmeye hazırız? Sanırım her birimizin bu soruya farklı bir cevabı olacaktır, ancak önemli olan bu konuyu konuşabilmemizdir.

İÇAD: Özellikle bir ülkede sürpriz saldırılar gerçekleştikten sonra genellikle istihbarat zafiyeti gündeme gelir. Ancak istihbarat servislerinin karar vericileri olay hakkında bilgilendirmiş olması ve karar vericilerin bu uyarıyı

dikkate almamış olması da mümkün olabilir. Bu bağlamda, istihbaratın karar alıcılar tarafından anlaşılamaması ya da istihbaratın karar alıcılara uygun yöntemlerle sunulamaması gibi sorunlarla karşılaşmak mümkün müdür? Karar alıcıların kendilerine sunulan istihbaratı dikkate almamalarının nedenleri neler olabilir? Karar alıcıların istihbaratı dikkate almalarını sağlamak için neler yapılmalıdır?

Doç.Dr. Erik Dahl: Bu bir kavrayış sorunudur. İsrail örneğinde olduğu gibi, liderler nasıl oluyor da aldıkları istihbarata karşı duyarlı olmuyorlar? Bence en büyük sorun liderlerin kendilerine verilen uyarıları anlamamaları ya da kendilerini destekleyen istihbarat uzmanlarına güvenmemeleridir. Bu sorundan kaçınmanın en iyi yolu liderlerin ve istihbarat uzmanlarının düzenli olarak birlikte çalışmaları ve yakın bir ilişki geliştirmeleridir. Örneğin ABD ordusunda liderlerimiz genellikle eğitim kurslarında ya da okulda istihbarat görevlileriyle birlikte zaman geçirirler, böylece daha sonra sahada birlikte görev yaptıklarında birbirlerini zaten tanır ve güvenir durumda oluyorlar.

Ancak istihbarat uzmanlarının aynı zamanda politika yapıcıların kendilerine verdikleri bilgileri anlamalarına yardımcı olmak için daha fazla çalışmaları gerektiğine inanıyorum. Ve eğer liderlerin - ya da diğer müşterilerin - bir istihbaratın ne kadar önemli olduğunu anlamadıklarına inanıyorlarsa, arada bir geri adım atmaktan korkmamalılar. İstihbarat görevlilerinin işi politika belirlemek ya da liderlere ne yapmaları gerektiğini söylemek değildir; ancak liderlerin kendilerine söylediklerinin önemini anlamalarına yardımcı olmak için ellerinden gelenin en iyisini yapmak onların işi olmalıdır.

İÇAD: Yakın geçmişten bir başka soru da geçen yıl ABD semalarında görülen Çin balonuyla ilgili. Bu balonun amacı bir bakıma ABD'nin istihbarat başarısızlığını ya da başarısını test etmek miydi? Sizin için bu casus balonun asıl amacı neydi? Çin'in ABD'yi gözetlemek için gerçekten bir balon kullanmaya ihtiyacı var mı?

Doç.Dr. Erik Dahl: Çin'in balon olayı, en iyi istihbarat sistemlerinin bile nasıl şaşırabileceğinin bir başka örneğiydi. Çin inkâr etse de, bunun bir gözetleme çabası olduğu açıktır ve istihbarat ve uyarı sistemlerimiz bu kadar küçük ve bu kadar yavaş hareket eden bir şeyi tespit etmek için dizayn edilmemiştir. Bu da günümüzün yüksek teknoloji dünyasında bile eski moda teknolojilerin hala önemli olduğunu göstermektedir.

İÇAD: "Başarısız Eylemler: ABD'ye Yönelik Başarısız Terörist Saldırılardan Öğrenilen İstihbarat Dersleri" başlıklı makalenizde de belirttiğiniz gibi başarısız terör saldırılarının incelenmesi sonucunda ne tür istihbarat ve güvenlik önlemlerinin terör eylemlerinin önlenmesine katkı sağladığını tespit etmek mümkün görünüyor. Bu bağlamda, neden bazı terör saldırıları başarılı olurken diğerleri başarısız oluyor? Size göre ne tür istihbarat ve güvenlik gayretleri terör saldırılarını önlemede en yararlı olanıdır?

Doç.Dr. **Erik Dahl:** Terör eylemleri taktik düzeydeki operasyonlar olduğundan -daha büyük stratejik etkiler yaratabilseler bile- taktik düzeydeki istihbaratın toplanması ve analiz edilmesiyle önlenebilirler. Buna ek olarak, başarısız terör eylemleri üzerine yaptığım çalışmalar, çoğu eylemin basit polisiye tedbirlerle ya da komşulardan veya kendilerini endişelendiren bir şey gören diğer insanlardan gelen ihbar ve raporlarla engellendiğini göstermiştir. Bu iyi bir haber, çünkü hepimiz dikkatli olursak çoğu terör eyleminin önlenebileceği anlamına geliyor. Bu aynı zamanda daha karmaşık planların engellenme olasılığının daha yüksek olduğu anlamına gelmektedir, çünkü bu planlar daha fazla insan, daha fazla zaman ve daha fazla planlama içermektedir. Tüm bunlar polis ve güvenlik güçlerine planı bozma fırsatı vermektedir. Ancak kötü haber şu ki, yalnız bireyler tarafından gerçekleştirilenler gibi daha küçük ölçekli saldırıları önlemek çok zor olabilir.

İÇAD: "COVID-19 İstihbarat Başarısızlığı: Uyarı Neden Yeterli Değildi" isimli son kitabınızda tıbbi istihbaratın nasıl toplandığı ve bu konuda toplanan istihbaratın neden başarısız olduğu konularını derinlemesine incelediniz. Sizi bu kitabı yazmaya iten ana neden neydi? Kitabınız hakkında daha fazla bilgi verebilir misiniz?

Doç.Dr. **Erik Dahl:** Pandeminin başlarında hepimizin küresel bir istihbarat başarısızlığı yaşadığımızı fark ettim - geleneksel istihbarat kurumlarının başarısızlığı, ancak daha da önemlisi tıp ve halk sağlığı kurumlarının bu yeni hastalığı dünyaya yayılmadan ve milyonlarca insanı öldürmeden önce tahmin edip bizi uyarma konusundaki başarısızlığı. Bu istihbarat başarısızlığının 11 Eylül gibi geçmiş vakalara ne kadar benzediği konusu beni çok etkiledi, çünkü uyarılar olmasına rağmen, bir şekilde dünyanın dört bir yanındaki liderler yeterince bu hususa dikkat etmediler. Bu kitabı iki nedenden dolayı yazdım. Birincisi, istihbarat ve uyarıların pandemide nasıl bir rol oynadığını anlamak istedim. Ancak daha da önemlisi, bir sonraki

pandemi veya diğer küresel sağlık tehdidi ortaya çıktığında daha iyi bir iş çıkarmak için ne yapmamız gerektiğini öğrenmek istedim. Hastalık gözetimi alanında önemli değişiklikler yaptığımıza inanıyorum, ancak hala yapmamız gereken çok iş var. Bir sonraki pandemi için henüz hazır değiliz.

İÇAD: Dr. Dahl, son sorumuz istihbaratın geleceği ile ilgili. İstihbaratın geleceği neye benzeyecek? Gizli istihbarat bağlamında devletler için tehditler, zorluklar ve fırsatlar neler olacak?

Doç.Dr. **Erik Dahl:** Bu harika bir soru! Günümüzde istihbarat teşkilatlarının karşılaştığı pek çok zorluk var ama bence en önemli üçü şu şekilde. Birincisi, gizli istihbarat - casusluk ya da teknik adıyla casusluk - açısından tüm istihbarat servisleri, yüz tanıma gibi teknolojilerin yaygınlaşmasıyla insanların gizlice seyahat etmesini ve faaliyet göstermesini zorlaştırıyor. İkinci olarak, istihbarat teşkilatları şu anda mevcut olan pek çok açık kaynak istihbaratını nasıl kullanacakları konusunda mücadele ediyorlar. Örneğin, ABD'de bazı uzmanlar yeni bir açık kaynak istihbarat ajansı kurmamız gerektiğine inanırken, diğerleri her ajansın kendi sözleriyle açık kaynak istihbaratını kullandığı mevcut sistemin en iyisi olduğuna inanıyor. Üçüncü ve bence en büyük zorluk ise yapay zekâ gibi teknolojilerle ilgili olacak. Bir yandan, "Yapay zekâ istihbarat kurumlarının gelecekteki tehditleri öngörme konusunda daha iyi bir iş çıkarmalarına yardımcı olacak mı?" diğer yandan, "Birçok uzmanın uyardığı gibi, bu teknolojilerin kendileri birer tehdit haline mi gelecek?" soruları aklımızı kurcalıyor.

Kimsenin bu zorlukların cevabını bildiğini sanmıyorum, ancak istihbaratın geleceğinin büyüleyici olacağını ve bunun da istihbarat üzerine çalışmak ve düşünmek için harika bir zaman olduğu anlamına geldiğini söylemenin önemli olduğunu düşünüyorum.

İÇAD: Sayın Dahl, Sorularımızı yanıtladığınız için teşekkür ederiz. Eklemek istediğiniz bir şey var mı?

Doç.Dr. **Erik Dahl:** Tüm sorularınız için çok teşekkür ederim. Söyleşimizden büyük keyif aldım.

İstihbarat Çalışmaları ve Araştırmaları Dergisi-İÇAD, 2024, 3(2) : 175-211 Araştırma Makalesi
Journal of Intelligence Research and Studies-İÇAD, 2024, 3(2) : 175-211 Research Article
DOI: 10.61314/icad.1468290

SİBER GÜVENLİKTE SİBER GÖZETİM: PEGASUS PROJESİ

Pınar DEMİRCİ*

ÖZET

İsrail Hükümeti'nin siber ihracatta özel sektör üzerinde tam kontrol gücüne sahip olması kamu-özel sektör iş birliğinin kötüye kullanılmasına neden olmaktadır. Makalede 2021 yılında ortaya çıkan İsrailli NSO şirketinin Pegasus casus yazılımını satın alan hükümetlerin neden olduğu insan hakları ihlallerini içeren Pegasus Projesi vakası ele alınacaktır. Araştırma nitel bir çalışmadır. Nitel araştırma yöntemlerinden dokümantasyon incelemesi yapılacaktır. Makalenin amacı, siber güvenlik alanında kamu-özel sektör iş birliğinde İsrail Hükümeti'nin siber ihracatta özel sektör üzerinde tam kontrol gücüne sahip olmasıyla iş birliğinin kötüye kullanılmasını Pegasus Projesi üzerinden göstermektir. Bu amaç doğrultusundan makalede şu sorulara yanıt aranmıştır: Pegasus projesi kapsamında İsrail Hükümeti'nin sorumluluğu nedir? İsrail Hükümeti'nin İsrailli siber ürünlerin ihracatındaki yetkisi nedir? Söz konusu yetkiyi hangi amaçlar için kullanmaktadır? Çalışmada, NSO şirketinin tarihine, Pegasus Projesinin ortaya çıkarılışı ve sonrasındaki yaşanan sürece ve proje kapsamında İsrail Hükümeti'nin sorumluluğuna yer verilmiştir. İsrail güvenlik şirketleri tarafından üretilen casus yazılımların ülkelere satılmasında onay yetkisine sahip İsrail Hükümeti, diplomatik ilişkiler geliştirmek ve siyasi kazanımlar elde etmek için baskıcı hükümetlere casus yazılımların satılmasına izin vermektedir.

Anahtar Kelimeler: *İsrail, NSO, Siber Güvenlik, Casus Yazılım, Pegasus Projesi*

Cyber Surveıllance In Cyber Securıty: The Pegasus Project

ABSTRACT

The Israeli government's full control over the private sector in the export of cyber products causes the abuse of the cooperation between the public and private sectors. The article will discuss the case of the Pegasus Project emerging in 2021 and involving human rights violations caused by oppressive governments that purchased the Pegasus spyware of the Israeli NSO company. The research is a qualitative study. Document analysis, one of the qualitative research methods, will be conducted. The aim of the article is to show the abuse of public-private sector cooperation in cyber security as the Israeli government has full control over the private sector in the export of cyber products through the Pegasus Project. For this purpose, answers to the following questions were sought in the article. What is the responsibility of the Israeli Government within the scope of the Pegasus Project? What is the Israeli Government's authority on the export of Israeli cyber products? For what purposes does she use this authority? In the study, the history of the NSO Company, the process of revealing the Pegasus Project and its aftermath, and the responsibility of the Israeli

* Yüksek Lisans Mezunu, Milli Savunma Üniversitesi, ORCID: 0000-0003-2980-4857.

Makale Başvuru Tarihi / Application Date: 15 Nisan 2024 / 15 April 2024

Makale Kabul Tarihi / Acceptance Date: 03 Haziran 2024 / 03 June 2024

Government within the scope of the project are included. The Israeli government, which has the authority to approve the sale of spyware such as Pegasus produced by Israeli security companies to other countries, allows the sale of spyware to oppressive governments with an aim to develop diplomatic relations and attain political gains.

Keywords: *Israel, NSO, Cyber Security, Spyware, Pegasus Project*

GİRİŞ

Günümüzde, İsrail'in siber gözetim ve casus yazılım endüstrisi, İsrail Savunma Kuvvetleri'nin (Israel Defense Forces – IDF) teknik bilgi birikiminden yararlanmaktadır. IDF'in siber birim mezunları ve gazileri, kurdukları siber şirketlerle askeri teknolojik deneyimlerini ve bilgilerini özel sektöre aktarmakta, siber gözetim ve casus yazılım endüstrisinin büyümesini ve gelişimini sağlamaktadır. Birçok İsrailli casus yazılım şirketinin kurucuları ve çalışanları, IDF'in elit siber birimlerinde tecrübe kazanmıştır. Ürettiği Pegasus adlı casus yazılımla ön plana çıkan İsrailli ünlü casus yazılım şirketi NSO Grup'un üç kurucusu Omri Lavie, Shalev Hulio ve Niv Karmi, Birim 8200[1] gazileridir (Levy, 2017; Melman, 2021). Ayrıca casus yazılım şirketinin araştırma ekibinin tamamı ve çalışanlarının çoğu, başta Birim 8200 olmak üzere IDF siber birimlerinde görev aldığı medyada rapor edilmektedir (Bergman ve Mazzetti, 2022). 2014 yılında kurulan diğer bir İsrailli gözetim şirketi Candiru'nun kurucuları Eran Shorer ve Yaakov Weizman da Birim 8200'de görev almıştır (Megiddo, 2021). Siber gözetleme şirketi Intellexa'nın kurucusu Tal Dilian da, IDF'in özel harekât birimleri ve diğer savunma teşkilatları için istihbarat araçları geliştirmekten sorumlu başka bir siber birim olan Birim 81'de görev almıştır (Sadeh, 2020).

NSO başta olmak üzere İsrailli siber gözetim şirketleri, son yıllarda siber teknolojilerini birçok otoriter rejime ihraç etmektedir. Başta Pegasus olmak üzere İsrailli siber gözetleme şirketleri tarafından üretilen casus yazılımların satın alınan ülkeler tarafından farklı muhalif gruplara karşı kullanıldığı ve satılan ülkelerde başta mahremiyet ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlaline neden olduğu raporlarda yer almaktadır (Uluslararası Af Örgütü, 2021a; Kaldani ve Prokopets, 2022,

[1] Birim 8200 olarak bilinen Merkezi Toplama Birimi ya da diğer adıyla İsrail Sinyal İstihbaratı Ulusal Birimi, IDF bünyesindeki Askeri İstihbarat Müdürlüğü (AMAN)'ne bağlı askeri siber uzay operasyonlarını koordine etmek ve yönlendirmekle görevli bir siber karargâhtır. Bkz. Oren, A. (2010, Ocak). The IDF's New Battlefield Is Found In Computer Networks. *Haaretz*. Erişim Tarihi: 24 Mayıs 2023, http://www.haaretz.co.il/misc/1.1182490

ss.19-20; Goodfriend, 2021). Uluslararası Af Örgütü'nün teknik desteğiyle 17 küresel medya kuruluşunun iş birliğinde ortaya çıkarılan Pegasus Projesi skandalı kapsamında, Pegasus yazılımını satın alan müşteriler için potansiyel hedef olduğu düşünülen telefon numaralarının olduğu NSO şirketine ait bir kayıt listesi ele geçirilmiştir. Proje kapsamında ortaya çıkarılan listede, 50'den fazla ülkeden devlet başkanları, politikacılar, diplomatlar, insan hakları savunucuları, akademisyenler, iş adamları, avukatlar, doktorlar, sendika liderleri ve gazetecilerin numaralarının olduğu belirlenmiştir (Uluslararası Af Örgütü, 2021a). Uluslararası Af Örgütü Güvenlik Laboratuvarı'nın teknik analizine göre, gazetecilerden insan hakları savunucularına birçok kişi casus yazılım tarafından hedef alınmış; hukuka aykırı şekilde casus yazılımla takip edilmiştir (Uluslararası Af Örgütü, 2021b, s.6). Mahremiyet, ifade özgürlüğü ve basın özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlali 17 medya kuruluşu tarafından rapor edilmiştir (Richard, 2021).

Silah sistemlerinin ihracatında olduğu gibi, İsrailli şirketler tarafından üretilen Pegasus gibi casus yazılımların yurt dışına ihracatlarının İsrail Savunma Bakanlığı tarafından onaylanması gerekmektedir (İsrail Savunma Bakanlığı, 2023a). 2007 tarihli İsrail yasası uyarınca, siber güvenlik ürünleri satmak isteyen şirketler, Wassenaar Düzenlemesi'ne dayalı olarak Savunma Bakanlığı'nın Savunma İhracat Kontrolleri Dairesi'nden ihracat lisansları almaktadır (İsrail Savunma Bakanlığı, 2007, s.7; Wassenaar Düzenlemesi, 2023a; Silahlı Kontrol Derneği, 2022). İsrail Savunma Bakanlığı, siber ürünlerin ihracatına yönelik kararlarda Wassenaar Düzenlemesi'ne bağlılığını ifade ederken İsrailli casus yazılımların neden olduğu insan hakları ve temel özgürlüklerin ihlali, İsrail tarafından Wassenaar Düzenlemesi'ne uyulmadığını göstermektedir.

Bu makalede günümüzde uzun dönemli siber güvenlik politikalarının geliştirilmesi ve uygulanmasında kamu-özel sektör iş birliğinin arz ettiği önem İsrail örneği üzerinden ele alınmaktadır. Gelişen teknolojiyle birlikte günümüzde siber tehdit unsurlarının niceliği ve çeşitliliği artarken tehditlerin etkisi ve yıkıcılığı da ciddi boyutlara ulaşmaktadır. Siber saldırılar devletlerin siber uzayda faaliyet gösteren sağlık hizmetleri sistemlerinden bankacılık hizmetlerine, iletişim sistemlerinden enerji tesislerine kadar tüm altyapı sistemlerinin faaliyetlerinin felce uğramasına veya sistemlerin tamamen işlevsiz kalmasına neden olmaktadır. Bu bağlamda, siber saldırılar devletler için öncelikli ulusal güvenlik sorunları olurken daha kapsamlı ve

etkili siber güvenlik politikaları yürütülmesi için farklı siber aktörlerle iş birliği yapmaktadır.

Bu çalışmada günümüzde uzun dönemli siber güvenlik politikalarının geliştirilmesi ve uygulamasında kamu-özel sektör iş birliğinin arz ettiği önem kapsamlı ve detaylı bir şekilde İsrail örneği üzerinden ele alınmaktadır. Makalede 2021 yılında, Uluslararası Af Örgütü Güvenlik Laboratuvarı'nın teknik destek sağladığı, 17 küresel medya kuruluşu tarafından ortaya çıkarılan İsrailli NSO şirketinin Pegasus casus yazılımını satın alan hükümetlerin neden olduğu hak ihlallerini içeren Pegasus Projesi vakası ele alınmaktadır (Uluslararası Af Örgütü, 2021, s.6). İsrail güvenlik şirketleri tarafından üretilen Pegasus gibi casus yazılımların ülkelere satılmasında onay yetkisine sahip İsrail Hükümeti, diplomatik ilişkiler geliştirmek ve siyasi kazanımlar elde etmek için insan hakları ihlalleri yapan otoriter rejimlere yazılımların satılmasına izin vermektedir. 2021 yılında 11 milyar dolar ile tarihindeki en yüksek siber ihracat rakamına ulaşan İsrail, küresel siber güvenlik yatırımlarının yaklaşık %40'ını çekerek 8,8 milyar dolar yatırıma sahip olmuş; dünyada en çok siber yatırım çeken ülke olmuştur (İsrail Ulusal Siber Müdürlüğü, 2022). Diğer yandan, siber güvenlik alanında kamu-özel sektör iş birliğinde küresel alanda en çok yatırım çeken endüstriye sahip olan İsrail'de siber ihracatta hükümetin özel sektör üzerinde tam kontrol gücüne sahip olması, iş birliğinin kötüye kullanılmasına neden olmaktadır.

Araştırma nitel bir çalışmadır. Nitel araştırma yöntemlerinden dokümantasyon incelemesi yapılmıştır. Makalenin amacı, siber güvenlik alanında kamu-özel sektör iş birliğinde İsrail Hükümeti'nin siber ihracatta özel sektör üzerinde tam kontrol gücüne sahip olmasıyla iş birliğinin kötüye kullanılmasını Pegasus Projesi üzerinden göstermektir. Bu amaç doğrultusundan makalede şu sorulara yanıt aranmıştır:

- Pegasus Projesi kapsamında İsrail Hükümeti'nin sorumluluğu nedir?
- İsrail Hükümeti'nin İsrailli siber ürünlerin ihracatındaki yetkisi nedir? Söz konusu yetkiyi hangi amaçlar için kullanmaktadır?

1. LİTERATÜR TARAMASI

2022 yılında yayınlanan "*Misenformasyon & Pegasus Projesi: Hindistan Örneği*" adlı tez, ana akım Hint medyasının Pegasus Projesi sızıntısına ve bunun Twitter'daki konuşmaları yönlendirmedeki etkisine nasıl tepki verdiğini analiz etmektedir (Khurana, 2022, s.8). Tez, Hint medyasının devlete yakın bölgelerdeki yanlış bilgilerin yayılmasındaki kalıpları ortaya çıkarmayı amaçlamaktadır (Khurana, 2022, s.8). Analiz edilen medya kuruluşlarının tamamı, değişen derecelerde de olsa, haberlerinde yanlış bilgilerin kurbanı olmuştur. Tezde, ulusal medya kuruluşlarının kamuoyunu yanlış bilgiye maruz bırakmada önemli bir rol oynadığı ve kendilerinin de yanlış bilgiye yatkın olduğu sonucuna varılmaktadır (Khurana, 2022, s.67). Çalışma, nüfusun önemli bir kısmının Pegasus casus yazılımlarıyla ilgili önemli yanlış bilgilerin farkında olduğunu ortaya koymaktadır. Ancak bu anlayış medya kuruluşlarının sosyal medya (Twitter) üzerinden eylem çağrısına dönüşmemiştir. Hint medya raporları ile sosyal medya arasındaki zayıf korelasyon, incelenen Hint medya kuruluşlarının izleyiciler tarafından yapılan haberlerine güven eksikliğini göstermektedir (Khurana, 2022, s.67-69).

2022 yılında Avrupa Konseyi için hazırlanan "*Pegasus Casus Yazılım ve İnsan Hakları Üzerindeki Etkileri*" adlı rapor, Pegasus casus yazılımlarının başta mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlükler üzerindeki etkisini analiz etmektedir (Kaldani ve Prokopets, 2022, s.5). Rapor, Pegasus casus yazılımlar gibi müdahaleci gözetim teknolojilerinin, yalnızca mahremiyet hakkı ve ifade özgürlüğü üzerinde değil, onur hakkı, toplanma özgürlüğü, din özgürlüğü ve hatta bireyin fiziksel ve psikolojik bütünlüğü de dahil olmak üzere diğer insan hakları ve temel özgürlükler üzerinde yarattığı veya potansiyel olarak yaratabileceği caydırıcı etkinin altını çizmektedir (Kaldani ve Prokopets, 2022, s.19-20). Raporda ayrıca yalnızca Pegasus'a değil aynı zamanda diğer kötü amaçlı saldırılara maruz kalma olasılığını en aza indirmek amacıyla daha iyi koruma için temel kurallar da sunulmaktadır (Kaldani ve Prokopets, 2022, s.15-20).

"*Pegasus Casus Yazılım: Vataşların Gizlilik Hakkının Destekleme*" adıyla 2023 yılından yayınlanan makalenin amacı, gözetim araçlarına ilişkin şeffaflığı ve hesap verebilirliği belirlemek ve Pegasus casus yazılımları aracılığıyla verilerin korunmasına ilişkin mahkemelerin gözlemlerini analiz

etmektir (Sneha, 2023, s.453). Birçok davada Hindistan mahkemesi, mahremiyet hakkının insan haklarının inkar edilemeyecek önemli yönlerinden biri olduğuna karar vermiştir. Elektronik delilleri sırasıyla birincil veya ikincil delil olarak göstermenin tek alternatifi, aslını, kopyasını veya 1872 tarihli Hindistan Delil Yasası'nın 65B Bölümü uyarınca bir sertifikayla bağlantılı muadilini ibraz etmektir. Elektronik kayıtların kabul edilebilirliği ve hukuk, ceza ve diğer hukuki prosedürlerde delil olarak kullanışlılığı, Yüksek Mahkeme tarafından birçok önemli kararla açıkça ortaya konmuştur. Elektronik cihazlar soruşturma için değeri Hindistan Kanıt Yasası kurallarına uyup uymadıklarına bağlıdır (Sneha, 2023, s.467)

2023 yılında "*Pegasus Casus Yazılımı: Gizlilik Hakkının İhlali ve Hindistan'da Gözetim Yasalarına Tehdit*" adıyla yayınlanan makalenin amacı, Pegasus casus yazılımlarının gizlilik hakkı üzerindeki çeşitli sorunlarını ve etkilerini özetlemek ve Hindistan Anayasası'nın özel hayatın gizliliğine ilişkin hükümlerini ve gözetim ile ilgili çeşitli yasaları incelemek ve analiz etmektir (D'Souza, 2023, s.425). Makalede, casus yazılımın bireylerin mahremiyetini ve güvenliğini etkili ve kesin bir şekilde tehlikeye attığı vurgulanmaktadır (D'Souza, 2023, s.436). Hindistan'daki 2000 Bilişim Yasası ve kuralları veri korumasına ilişkin hükümler içermesine rağmen yetersiz görünmektedir (D'Souza, 2023, s.436). Zayıf yasa ve mevzuatlar mahremiyet hakkını etkilemekte ve dolayısıyla kolay gözetime olanak tanımaktadır. Müdahale türleri, ele geçirilebilecek bilgilerin ayrıntı düzeyi ve hizmet sağlayıcıların işbirliği düzeyi, yasanın çiğnenmesini kolaylaştırmakta ve devletin izlemesini desteklemektedir (D'Souza, 2023, s.433).

2023 yılında yayınlanan "*Görünmez Casusun Düzenlenmesi – Pegasus Casus Yazılımına İlişkin Gözetim Teknolojisini İnceleyen Örnek Olay İncelemesi*" adlı tezde, Pegasus casus yazılımlarına ilişkin gözetim teknolojilerinin yarattığı zorluklara teknoloji düzenleyici kurumların ulusal anayasaları, bölgesel anlaşmaları, evrensel hak ve özgürlükleri dikkate alarak ne ölçüde yanıt verdiği ele alınmıştır (Dieterle, 2023, s.4). Çalışma düzenleyici kurumların Pegasus ve benzeri casus yazılımların kötüye kullanılmasına çözüm bulma ihtiyacını kabul ettiğini ve mevcut düzenleyici çerçevelerdeki boşlukları tespit ettiğini ortaya koymuştur (Dieterle, 2023, s.34). Sivil toplum üyelerinin çalışmaları nedeniyle gözetim düzenlemesine ilişkin sorunlar küresel gündeme taşınmış ve uluslararası, bölgesel, ulusal ve özel paydaşlar sorunlara yanıt vermeye zorlanmıştır. Bu da onların bir

kontrol mekanizması, başka bir deyişle bekçi köpeği rolünü üstlenmelerini sağlamıştır. Kamu ve özel sektör paydaşları sorunlara farklı şekillerde yanıt vermişlerdir. AB gibi bölgesel paydaşlar, düzenleyici çerçevelerdeki boşlukları doldurmaya çalışarak soruşturmalar yürütürken, BM gibi uluslararası paydaşlar, evrensel haklara uyum garanti altına alınıncaya kadar gözetim teknolojisinin satışı, transferi ve kullanımı konusunda küresel bir moratoryum ilan edilmesini tavsiye etmiştir. Her iki yanıt da gözetim teknolojisine ilişkin parçalı yasal çerçeveyi ve daha fazla insan hakları ihlalini önlemek için mevcut boşlukların doldurulması ihtiyacını vurgulamaktadır (Dieterle, 2023, s.34).

2024 yılında yayınlanan "*Pegasus Casus Yazılımlarının Kapsamlı Analizi ve Dijital Gizlilik ve Güvenlik Açısından Etkileri*" adlı makale, Pegasus casus yazılımını ve bunun dijital gizlilik ve güvenlik üzerindeki etkilerini kapsamlı bir şekilde analiz etmektedir. Çalışmanın amacı, yasal, etik ve politika konularını derinlemesine inceleyerek Pegasus ve benzeri casus yazılım araçlarının yarattığı zorluklara ilişkin bütünsel bir anlayış sunmaktır. Çalışma, tehditleri azaltmaya ve kullanıcıları istilacı gözetim tekniklerinden korumaya yönelik potansiyel çözümler sunmaktadır (Kareem, 2024, s.1360). Pegasus gibi gelişmiş casus yazılımların varlığı ve yaygınlaşması, dijital teknolojilere olan güvenin erozyona uğramasına, gözetlemenin normalleşmesine ve siber güvenlikteki açıkların açığa çıkmasına neden olmuştur (Kareem, 2024, s.1366-1367). Bu zorluklar, yenilikçi çözümler geliştirmek, yasal ve düzenleyici çerçeveleri güçlendirmek ve dijital çağda sorumlu davranışı teşvik etmek için hükümetlerin, endüstrinin, akademi ve sivil toplumun ortak çabalarını gerektirmektedir (Kareem, 2024, s.1370). Pegasus ve benzeri casus yazılımların oluşturduğu tehditleri azaltmak için önerilen çözümler arasında şifreleme ve güvenli iletişim teknolojilerinin güçlendirilmesi, kamuoyunun farkındalığının artırılması ve dijital okuryazarlığın teşvik edilmesi, mahremiyet artırıcı teknolojilerin geliştirilmesi, yasal ve düzenleyici çerçevelerin revize edilmesi ve ortak norm ve kuralların geliştirilmesi için uluslararası iş birliğinin teşvik edilmesi yer almaktadır (Kareem, 2024, s.1371).

2. NSO ŞİRKETİ

NSO şirketi, 2010 yılında İsrailli üç girişimci Niv Carmi, Shalev Hulio ve Omri Lavie tarafından Tel Aviv yakınlarındaki Herzliya şehrinde kurulmuştur. Şirket adını kurucuları Niv, Shalev ve Omri'nin baş harflerinden almaktadır (Bergman ve Mazzetti, 2022). Daha önce, IDF bünyesindeki Askeri İstihbarat Müdürlüğü (AMAN)'ne bağlı siber istihbarat birimi Birim 8200'de çalışan çocukluk arkadaşları Shalev Hulio ve Omrie Lavie, 2007 yılında ilk ortak girişimlerini gerçekleştirmişlerdir. İzleyicilerin ekranda görünen ürünleri bulmasına ve satın almasına yardımcı olan ilk girişimleri olan video pazarlama şirketi MediAnd şirketini kurmuşlardır. Hulio ve Lavie'nin ilk ortak girişimi MediAnd, Eddie Shalev'in kurucusu olduğu İsrailli Genesis Partners adlı risk sermayesi şirketi tarafından fonlanmıştır (Yablonko, 2019).

2008 yılında ise Hulio ve Lavie, ikinci girişimleri olan müşterilerinin mobil telefonlarına uzaktan erişim sağlayarak teknik destek sunan mobil müşteri hizmetleri şirketi CommuniTake şirketini kurmuşlardır. CommuniTake şirketi müşterilerine mobil cihazlar için uzaktan destek sağlayarak mobil servis noktalarını ziyaret etme ihtiyacını ortadan kaldıran bir hizmet sunmuştur. İkili, diğer ortaklarla yaşanan anlaşmazlıklar nedeniyle şirketten ayrılmışlardır (Fischer ve Levy, 2016).

CommuniTech'in mobil cihazları uzaktan kontrol yeteneği, Lavie ve Hulio için mobil cihazları izinsiz olarak uzaktan kontrol edebilecekleri bir yazılım geliştirme fikrini ortaya çıkarmıştır. CommuniTake şirketinin ardından 2010 yılında Hulio ve Lavie ikilisi, Birim 8200'de ve İsrail Dış İstihbarat Servisi MOSSAD'da görev yapmış Niv Karmi ile birlikte üçüncü girişimleri olan NSO şirketini kurmuşlardır (Bergman ve Mazzetti, 2022). NSO şirketinin 1,5 milyon dolarlık ilk finansman desteği MediAnd şirketinde olduğu gibi Genesis Partners şirketi tarafından sağlanmıştır (Lipson, 2017). Kurucu ortaklardan Niv Carmi'nin şirketin kuruluşundan kısa bir süre sonra şirketten ayrıldığı medyada yer almıştır (Shahaf, 2018).

NSO şirketinin kurulmasından bir yıl sonra 2011 yılında NSO mühendisleri, ilk casus yazılımlarının ilk versiyonunun kodlamasını tamamlamıştır (Bergman ve Mazzetti, 2022). NSO kurucuları, casus yazılımlarına Pegasus[2] adını vermiştir. Pegasus, Apple ve Android mobil

[2] Pegasus, Yunan mitolojisinde dişi canavar Medusa'nın kanından doğduğuna ve kutsal yerleri koruduğuna inanılan kanatlı bir attır. Bkz. Theoi Project. (2023). *Pegasos*. https://www.theoi.com/Ther/HipposPegasos.html

işletim sistemlerindeki sıfır gün kusurlarından yararlanarak hedef cihazlara bulaşan bir yazılımdır (Bergman ve Mazzetti, 2022). Bu casus yazılım kullanıcının herhangi bir etkileşimini gerektirmeden, herhangi bir dosya ya da mobil uygulama indirmesine gerek duymadan telefona yüklenebilmektedir. Hedeflenen kişinin telefonuna, tabletine veya bilgisayarına yüklenebilmesi için kişiyi, güvenliği ihlal edilmiş bir bağlantıya veya dosyaya tıklamaya ikna etmeye dayanan geleneksel casus yazılımların aksine sıfır tıklama saldırısında casus yazılım, herhangi bir bağlantıya tıklanmadan cihazlara yüklenebilmektedir (Kaspersky, 2023). Yazılım yüklendiği telefonlardaki tüm bilgilere ulaşılabilmekte, telefon dinlenmesi yapabilmektedir. Sıfır tıklama saldırısı, mobil cihazlardaki boşluklardan yararlanarak hedeflenen sisteme girmek için veri doğrulama boşluğunu kullanmaktadır. Saldırının işleyişi, hedeflenen sistemlere gönderilen verilerin, sistem henüz verilerin güvenilir olup olmadığını kontrol edemeden harekete geçmesini sağlamaktır.[3]

Sıfır tıklamayla bulaşmada casus yazılım, hedef cihaza tam erişim sağlayabilmekte ve kullanıcı kötü amaçlı bir bağlantıya tıklamadan tüm verileri indirebilmektedir. Sıfır tıklamada sadece telefon numarasına sahip olunarak hangi cep telefonu şirketinin kullanıldığına bakılmaksızın mobil cihazlardaki tüm belgelere erişilmesine, cihazların gizlice dinlenmesine, telefon görüşmelerinin kaydedilmesine, hedefin bulunduğu yerin takip edilmesine ve tüm çağrıların, mesajların, e-postaların ve sosyal ağlardaki hareketlerin görüntülenmesine olanak sağlamaktadır (Shezaf ve Jacobson, 2018). Bu durum, mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlaline neden olmaktadır (Kaldani ve Prokopets, 2022, s.19-20).

Şirket kısa bir süre içerisinde genişleyerek farklı ülkelerde ofisler açmış; Herzliya'da bulunan genel merkezinde ve ofislerinde 700'den fazla kişiyi istihdam etmiştir. NSO şirketinde istihdam edilen araştırma üyelerinin ve personellerin büyük çoğunluğu, başta Birim 8200 olmak üzere AMAN'ın elit birimlerinde görev almış kişilerden seçilmiştir (Bergman ve Mazzetti, 2022).

[3] Detaylı bilgi için bkz. BilgiGüvende. (2020, 13 Mayıs). *Siber Güvenlik Dünyasında Bir Başka Gizli Tehdit: Zero-Click Saldırısı.* Erişim Tarihi: 29 Ağustos 2023, https://bilgiguvende.com/siber-guvenlik-dunyasinda-bir-baska-gizli-tehdit-zero-click-saldirisi/

NSO resmi web sitesinde telekomünikasyon ve istihbarat uzmanları tarafından üretilen Pegasus yazılımı, terörizm, uyuşturucu kaçakçılığı ve diğer büyük suçlarla mücadele aracı olarak tanıtılmıştır. Yazılımın, devlet kurumlarına, istihbarat teşkilatlarına ve kolluk kuvvetlerine terör saldırılarını önlemede ve suç şebekelerini dağıtmada şifrelemenin zorluklarını ortadan kaldırmak için satılan bir araç olduğu belirtilmiştir. Terörizmin ve diğer büyük suçların önlenmesinin yanı sıra yazılımın kayıp kişilerin bulunmasına ve arama kurtarma faaliyetlerine yardımcı olduğu vurgulanmıştır (NSO Grup, 2023).

NSO teknoloji şirketinin Pegasus yazılımını ilk sattığı ülke Meksika olmuştur. 2012 yılında Meksika hükümeti NSO ile Pegasus yazılımının satışı için 20 milyon dolarlık bir sözleşme imzaladığını bildirmiştir (Hirschauge ve Orpaz, 2014). NSO yetkilileri, El Chapo lakabıyla tanınan Meksikalı uyuşturucu baronu Joaquín Archivaldo Guzmán Loera'nın 2016 yılında yakalanmasında Pegasus casus yazılımının kullanıldığını ifade etmiştir (Yaron, 2020; Bergman, 2019). Aynı yıl NSO'nun, Pegasus yazılımını Panama Hükümeti'ne sattığı medyada yer almıştır (News Room Panama, 2021).

NSO şirketinin tek ürünü olan Pegasus casus yazılımının birçok yabancı hükümet tarafından ilgi gördüğü ve bundan dolayı NSO şirketinin yazılım için hükümetlerden yüksek fiyatlar talep ettiği medyada yer almıştır (Dogani, 2016). Amerika Birleşik Devletleri (ABD) merkezli New York Times gazetesinin NSO şirketinin satış sözleşmelerine dayandırdığı haberinde NSO şirketinin geleneksel yazılım şirketlerine benzer olarak gözetim araçlarını hedef sayısına göre fiyatlandırdığı ve fiyatların 500 bin dolarlık sabit bir kurulum ücretinden başladığı yer almıştır. Haberde, sabit kurulum ücretine ek olarak, NSO'nun, 10 iPhone kullanıcısını gözetlemek için devlet kurumlarından 650 bin dolar, 10 Android kullanıcısı için 650 bin dolar, 5 BlackBerry kullanıcısı için 500 bin dolar ve 5 Symbian kullanıcısı için 300 bin dolar talep ettiği belirtilmiştir. Haberde, NSO şirketinin, 100 ekstra hedef için 800 bin dolar, 50 ekstra hedef için 500 bin dolar, 20 ekstra hedef için 250 bin dolar ve 10 ekstra hedef için 150 bin dolar talep ettiği ifade edilmiştir. Ayrıca, şirketin her yıl toplam satış ücretinin yüzde 17'si kadar yıllık sistem bakım ücreti talep ettiği de haberde yer almıştır (Perltroth, 2016).

2014 yılında Hulio ve Lavie, NSO şirketinin %70 hissesini, 120 ile 130 milyon dolar arasında bir ücrete 1999 yılında kurulan Kaliforniya merkezli bir özel sermaye şirketi olan Francisco Partners şirketine satmıştır (Yablonko, 2019). Francisco Partners, NSO şirketinden önce de Kudüs merkezli Ex Libris ve Tel Aviv merkezli Dmatek teknoloji şirketlerini satın almıştır (Shezaf ve Jacobson, 2018). NSO şirketinin satın alınmasından bir yıl sonra Francisco Partners şirketinin, NSO'dan 75 milyon dolar kar elde ettiği medyada yer almıştır (Stone ve Roumeliotis, 2015).

Francisco Partners şirketi, 2017 yılında NSO'nun hisselerini resmi olarak 1 milyar dolardan fazla bir bedelle satışa çıkarmıştır (O'neill, 2017). 14 Şubat 2019'da ise Francisco Partners, NSO şirketinin sahip olduğu hisselerini tekrardan NSO'nun kurucu ortakları Hulio ve Lavie'ye satmıştır. NSO şirketinin hisselerinin 1 milyar dolara yakın bir paraya satıldığı medyada yer almıştır. NSO şirketi tarafından yapılan açıklamada Hulio ve Lavie'nin NSO şirketini Londra merkezli özel sermaye şirketi Novalpina Capital ile ortak satın aldığı, eski kurucuların ve Novalpina Capital şirketinin ayrı ayrı olarak %50'şer hisseye sahip olduğu belirtilmiştir (Solomon, 2019).

Günümüzde, sıfır tıklama teknolojili Pegasus casus yazılımı dünyadaki en gelişmiş casus yazılım araçlarından biri olarak görülmektedir (Mazzetti, Bergman ve Stevis-Gridneff, 2022). Küresel yazılım endüstrisinde adını duyuran Pegasus gibi casus yazılımları üreten İsrail siber casusluk endüstrisi, gözetleme araçları ve iletişim dinleme alanında küresel ticaretin öncüleri arasında yer almıştır. 2021 yılında 11 milyar dolar ile tarihindeki en yüksek siber ihracat rakamına ulaşan İsrail, küresel siber güvenlik yatırımlarının yaklaşık %40'ını çekerek 8,8 milyar dolar yatırıma sahip olmuş; dünyada en çok siber yatırım çeken ülke olmuştur (İsrail Ulusal Siber Müdürlüğü, 2022). Günümüzde değeri 1 milyar doların üzerinde olan NSO şirketi, faaliyetlerini halen kurucu üyeleri Hulio ve Lavie başkanlığında yürütmektedir (Brewster, 2021).

3. PEGASUS PROJESİ

18 Temmuz 2021'de, Paris merkezli Fransız kâr amacı gütmeyen medya kuruluşu olan Forbidden Stories, Uluslararası Af Örgütü'nün teknik desteğiyle NSO şirketine ait Pegasus casus yazılımının satın alan müşteriler tarafından kötüye kullandığını ortaya çıkaran bir soruşturma başlatmıştır (Forbidden Stories, 2021). Uluslararası Af Örgütü'nün Güvenlik

Laboratuvarı tarafından elde edilen veriler, Forbidden Stories medya kuruluşu tarafından 10 ülkeden 16 küresel medya kuruluşuyla paylaşılmıştır. Soruşturmanın analizleri 17 medya kuruluşunun ortak çalışmasıyla tamamlanmış; soruşturma Pegasus Projesi adını almıştır (Uluslararası Af Örgütü, 2021b, s.6). Forbidden Stories tarafından verilerin paylaşıldığı medya kuruluşları arasında ABD merkezli Organize Suç ve Yolsuzluk Raporlama Merkezi (OCCRP), Washington Post ve PBS Frontline, İngiliz gazetesi Guardian, Fransız Le Monde ve Radio France, İsrail gazetesi Haaretz, Alman Süddeutsche Zeitung ve Die Zeit, Meksika merkezli Proceso ve Aristegui Noticias, Belçika merkezli Le Soir ve Knack, Hindistan merkezli Wire, Macaristan merkezli Direkt36 ve Suriye merkezli Daraj yer almaktadır (Forbidden Stories, 2021). 17 medya kuruluşundan 80'den fazla gazeteci telefon numaralarından oluşan bu kayıtları analiz ve rapor etmiştir (Richard, 2021).

Uluslararası Af Örgütü'nün Güvenlik Laboratuvarı, listede kayıtlı telefon numaralarının kullanıldığı telefonlara yönelik adli analizler gerçekleştirmiştir. Güvenlik Laboratuvarı listede kayıtlı telefon numaralarının kullanıldığı 67 iphone telefona ulaşarak telefonları analiz etmiştir. Adli analizler sonucunda listede kayıtlı 67 telefon numarasının 37'sinde Pegasus casus yazılımına ait izler olduğu tespit edilmiştir. Yazılımın saldırılarına maruz kalan telefon numaraları Azerbaycan, Fransa, Macaristan, Hindistan ve Meksika ülkelerine ait olduğu belirlenmiştir (Pfenniger, 2023). Ayrıca, Pegasus casus yazılımının izlerinin tespit edildiği 37 telefon numarasından bazılarına çok yakın tarihlerde, Apple'ın iOS mobil işletim sistemindeki güvenlik açıklarından yararlanılarak Pegasus yazılımının bulaştığı rapor edilmiştir (Schwartz, 2021). İncelenen 67 telefonun yarısından fazlasında Pegasus casus yazılımına ait izlerin olduğunun doğrulanması, Uluslararası Af Örgütü ve Forbidden Stories tarafından ortaya çıkarılan NSO şirketine ait 50.000'den fazla telefon numarasının bulunduğu listenin Pegasus casus yazılımı için bir hedef listesi olduğu düşüncesini desteklemektedir (Pfenniger, 2023).

Forbidden Stories ve Uluslararası Af Örgütü, Kanada'daki Toronto Üniversitesi bünyesindeki Munk Küresel İlişkiler ve Kamu Siyaseti Okulu'nda disiplinlerarası bir laboratuvar olarak faaliyet gösteren Vatandaş Laboratuvarı (Citizen Lab)'ndan Uluslararası Af Örgütü Güvenlik Laboratuvarı tarafından incelenen telefon numarası örneklerinin ve ortaya çıkarılan adli metodolojinin bağımsız bir şekilde incelenmesini talep etmiştir

(Marczak, Scott-Railton, Anstis ve Deibert, 2021). Vatandaş Laboratuvarı yaptığı adli incelemeler sonucunda, Uluslararası Af Örgütü'nün adli tıp metodolojisinin, Pegasus saldırılarını doğru şekilde tespit ettiğini doğrulamıştır (Marczak, Scott-Railton, Anstis ve Deibert, 2021). Bu bağlamda, iki farklı bağımsız kuruluşunun da incelenen telefon numaralarında Pegasus yazılımına ait izlere ulaşması, erişilen NSO'ya ait listenin casus yazılım için bir hedef listesi olduğu tezinin güvenirliliğini artırdığı değerlendirilmektedir (Pfenniger, 2023).

3.1. Pegasus Projesi Kapsamında Hedef Profilleri

Uluslararası Af Örgütü Güvenlik Laboratuvarı'nın teknik desteğiyle, 17 medya kuruluşunun Pegasus yazılımı için potansiyel hedef olduğu düşünülen telefon numaralarına yönelik inceleme ve analizlerinin sonuçları, 18 Temmuz 2021'de kamuoyuyla paylaşılmıştır (Kirchgaessner vd., 2021). Soruşturma sonucunda, 2016 yılından beri Pegasus yazılımını satın alan müşteriler tarafından potansiyel hedef olarak seçildiği düşünülen telefon numaralarının kayıtlarının olduğu listede 50'den fazla ülkeden devlet başkanları, politikacılar, diplomatlar, insan hakları savunucuları, akademisyenler, iş adamları, avukatlar, doktorlar, sendika liderleri ve gazetecilerin numaralarının olduğu belirlenmiştir (Richard, 2021). 17 medya kuruluşunun ortak soruşturmasında, NSO'ya ait listeye telefon numaraları giren ve NSO'nun müşterisi olduğu düşünülen 11 hükümet tespit edilmiştir. Listeye telefon numaraları giren hükümetler arasında Meksika, Suudi Arabistan, Birleşik Arap Emirlikleri (BAE), Hindistan, Macaristan, Azerbaycan, Bahreyn, Kazakistan, Fas, Ruanda ve Togo hükümetleri yer almaktadır (Uluslararası Af Örgütü, 2021a).

Medya kuruluşlarının incelemesine göre, 15.000'den fazla telefon numarasıyla listeye en çok telefon numarası giren ülke, farklı devlet kurumlarının Pegasus yazılımını kullandığı bilinen Meksika olmuştur. Meksika'nın ardından NSO'ya ait listeye 10.000'den fazla numara giren ülkeler BAE ve Fas gelmektedir. NSO müşterileri tarafından Avrupa Birliği (AB) ülkelerine ait 1.000'den fazla telefon numarası listeye eklenmiştir (Kirchgaessner vd., 2021). Medya kuruluşlarının incelemesine göre, 34 ülkeden 600'den fazla hükümet yetkilisi ve politikacının potansiyel hedef olarak seçildiği tespit edilmiştir (Uluslararası Af Örgütü Birleşik Krallık, 2021). Kayıtlı listede aralarında Fransa Cumhurbaşkanı Emmanuel Macron, Güney Afrika Devlet Başkanı Cryil Ramaphosa, Fas kralı 6. Muhammed el-

Sadis bin el-Hasan, Mısır Başbakanı Mustafa Kemal Madbuli, Irak eski Cumhurbaşkanı Berham Ahmed Salih, eski Belçika Başbakanı Charles Michel, eski Fransa Başbakanı Edouard Philippe, eski Lübnan Başbakanı Saad Hariri, eski Kazakistan Başbakanı Bakıtcan Abdirulı Sağıntayev, eski Fas Başbakanı Saadeddin Osmani, eski Uganda Başbakanı Ruhakana Rugunda, eski Pakistan Başbakanı İmran Khan, eski Cezayir Başbakanı Nureddin Bedevi ve Yemen Başbakanı Ahmed bin Dağr'ın olduğu 14 ülke liderinin telefon numaralarının yer aldığı tespit edilmiştir (Timberg, Birnbaum, Harwell ve Sabbagh, 2021).

Erişim sağlanan listede Fransa, Hindistan, Meksika, Macaristan ve Fas'ın aralarında bulunduğu 20 ülkeden yaklaşık 200 gazetecinin telefon numarası kaydının olduğu tespit edilmiştir (Richard, 2021). Listede, Financial Times, CNN, New York Times, France 24, Economist ve Associated Press ve Reuters gibi küresel medya kuruluşlarından yöneticilerin, muhabirlerin ve editörlerin telefon numaralarının yer aldığı tespit edilmiştir (Kirchgaessner vd., 2021). Soruşturmada, Suudi gazeteci Cemal Kaşıkçı'nın aile üyelerinin 2 Ekim 2018'de İstanbul'da yaşanan Kaşıkçı cinayeti[4] öncesinde ve sonrasında Pegasus yazılımıyla hedef alındığına dair kanıtlar ortaya çıkmıştır. İncelemeye göre, Cemal Kaşıkçı'nın aile üyelerinin numaraları cinayetin öncesi ve sonrasında Suudi Arabistan tarafından listeye eklenmiştir (Uluslararası Af Örgütü, 2021a). Cemal Kaşıkçı cinayetinden 6 ay sonra Mart 2019'da ABD merkezli CBS televizyon kanalında yayınlanan 60 dakika programına katılan NSO şirketinin kurucusu Shalev Hulio, cinayetle ilgilerinin olduğu, gazeteciyi ve ailesini hedef almak için Pegasus casus yazılımının kullanıldığına dair iddiaları reddetmiştir (CBS News, 2019). NSO şirketinin cinayetle ilgililerinin olduğuna dair iddiaları daha öncesinde reddetmesine karşın

[4] Washington Post gazetesi yazarı Suudi Arabistan vatandaşı Cemal Kaşıkçı 2 Ekim 2018'de, Suudi Arabistan'ın İstanbul'daki Başkonsolosluğu'na Türk nişanlısı Hatice Cengiz ile evlenmek için gereken belgeleri almak için geldiği sırada Suudi bir tim tarafından öldürülmüştür. Gazeteci Kaşıkçı ölmeden önce Washington Post gazetesinde Suudi yönetimini ve Suudi Veliaht Prens Muhammed bin Salman el-Suud'un politikalarını eleştiren yazılar yazmıştır. Suudi Arabistan Dışişleri Bakanlığı tarafından 19 Ekim'de yapılan açıklamada, savcılar tarafından yürütülen ön soruşturmaya göre Kaşıkçı'nın Başkonsoloslukta karıştığı kavga sonucunda öldüğü bilgisine yer verilmiştir. Ocak 2019'da Kaşıkçı cinayetiyle ilgili olarak Suudi Arabistan Riyad Ceza Mahkemesi'nde adı açıklanmayan 11 kişi yargılanmıştır. Aralık 2019'da mahkeme beş kişiyi cinayeti işledikleri gerekçesiyle idam cezasına çarptırmış; üç kişiye suçu örtbas etmekten 24 yıl hapis cezası vermiştir. Diğer üç kişi suçsuz bulunmuştur. Bkz. BBC. (2021, 24 Şubat). *Jamal Khashoggi: All You Need To Know About Saudi Journalist's Death*. Erişim Tarihi: 8 Eylül 2023, https://www.bbc.com/news/world-europe-45812399

Uluslararası Af Örgütü Güvenlik Laboratuvarı, Suudi Arabistan ve BAE'de yaşayan Kaşıkçı'nın oğlu Abdullah Kaşıkçı, Kaşıkçı'nın eski eşi Hanan Elatr ve diğer aile üyelerinin mobil cihazlarının Eylül 2017 ile Nisan 2018 arasında defalarca casus yazılımın saldırısına uğradığını tespit etmiştir. Güvenlik Laboratuvarı'nın adli analizinde, Pegasus casus yazılımının, Kaşıkçı'nın nişanlısı Hatice Cengiz'in telefonuna cinayetten dört gün sonra yüklendiği kanıtlanmıştır (Uluslararası Af Örgütü, 2021a). Adli tıp sonuçlarına göre, Kaşıkçı cinayetinden sonra, Cemal Kaşıkçı'nın yakın arkadaşı El Cezire kanalının eski yöneticisi Vaddah Hanfar'ın telefonu da Pegasus yazılımının saldırısına uğramıştır (Priest, Mekhennet ve Bouvart, 2021).

Meksika'da ise gazeteci Cecilio Pineda'nın telefonunun, 2017 yılında öldürülmesinden sadece birkaç hafta önce listeye eklendiği belirlenmiştir. Gazeteci Pineda kendi sosyal medya hesabında düzenli olarak Meksika'nın organize suç gruplarının savaş alanı olan Tierra Caliente bölgesindeki yerel yetkililer ile uyuşturucu kaçakçıları arasında bağlantı olduğunu iddia eden yayınlar yapmıştır. 2 Mart 2017'de gazeteci Pineda, Tierra Caliente bölgesindeki Ciudad Altamirano kasabasında vurularak öldürülmüştür. Soruşturmada, Pineda'nın ölüm tehditleri aldığı sıralarda telefon numarasının NSO'nun kayıt listesine Meksikalı bir müşteri tarafından eklendiği tespit edilmiştir (Lakhani, 2021). Soruşturmaya göre, 2016 ile 2017 yılları arasında en az 26 Meksikalı gazetecinin telefon numaraları potansiyel hedef olarak listeye eklenmiştir (Uluslararası Af Örgütü, 2021a).

Soruşturmaya göre, Hindistan'da 2017 ile 2021 yılları arasında büyük medya kuruluşlarından 40'tan fazla gazeteci hedef olarak listeye eklenmiştir (Uluslararası Af Örgütü, 2021b). Uluslararası Af Örgütü Güvenlik Laboratuvarı'nın adli tıp testleriyle Hindistan'ın bağımsız medya kuruluşu The Wire'ın kurucusu Siddharth Varadarajan'ın telefonuna Nisan 2018'de Pegasus casus yazılımın bulaştığı kanıtlanmıştır (Forbidden Stories, 2021a). Güvenlik Laboratuvarı, medya kuruluşu The Wire gazetesinin diğer kurucu ortağı MK Venu'nun telefonuna ise Haziran 2021'de Pegasus casus yazılımı bulaştığını ortaya çıkarmıştır (Forbidden Stoeies, 2021b). Pegasus casus yazılımıyla yaklaşık 200 gazetecinin hedef seçilmesi, basın özgürlüğü ve gazetecilerin ifade özgürlüğünün ihlal edilmesine neden olmaktadır (Kaldani ve Prokopets, 2022, s.5).

NSO'ya ait telefon numaralarının olduğu kayıt listesinde insan hakları savunucularının ve avukatların telefon numaraları da yer almaktadır. Soruşturmada, Suudi kadın hakları savunucusu Luceyn el-Hezlul'un telefon numarasının 2018 yılında BAE'den Suudi Arabistan'a zorla geri gönderilmesinden birkaç hafta önce hedef olarak listeye eklendiği tespit edilmiştir. El-Hezlul, Suudi Arabistan yönetiminin kadınlara yönelik yasaklarının eleştiren kampanyalar yürütmüştür (Walker, Kirchgaessner, Lakhani ve Safi, 2021). Soruşturmada, birçok insan hakları davasında yer alan İngiliz avukat Rodney Dixon'un telefon numarasının da 2019 yılında hedef olarak seçildiği tespit edilmiştir. Güvenlik Laboratuvarı'nın adli tıp analizleriyle, Dixon'un telefonunun Pegasus yazılımı tarafından hedef alındığı ortaya çıkarılmıştır. İngiliz avukat Dixon'ın müvekkilleri arasında öldürülen Suudi gazeteci Cemal Kaşıkçı'nın nişanlısı Hatice Cengiz de yer almaktadır (Sabbagh, Pegg, Lewis ve Kirchgaessener, 2012). İnsan hakları davaları yürüten Fransız avukat Joseph Breham'ın telefon numarasının da Fas tarafından 2019 yılında listeye kaydedildiği tespit edilmiştir. Adli tıp analizleri sonucunda Breham'ın telefonunun casus yazılım tarafından saldırıya uğradığı ortaya çıkarılmıştır (Benjakob, 2022).

NSO'nun kullanım amaçlarını açıkladığı üzere Pegasus yazılımının terörizm, uyuşturucu kaçakçılığı ve diğer büyük suçlarla mücadelede devletlerin istihbarat teşkilatlarına ve kolluk kuvvetlerine yardımcı olmaktır (NSO Grup, 2023). Yazılımın satın alan hükümetler tarafından muhalif grupları takip etmek, yerlerini tespit etmek, faaliyetlerini gözetlemek ve üzerlerinde baskı kurmak amacıyla kullanılması, yazılımın üretim amaçlarından uzaklaştırarak yazılımı hükümetler için rakiplerine veya muhalif gruplara karşı kullandıkları bir baskı aracına dönüştürmüş; başta mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlal edilmesine neden olmuştur.

3.2. Pegasus Projesi Sonrası Yaşananlar

18 Temmuz 2021'de Pegasus Projesi soruşturmasının sonuçlarının yayınlamasının ardından NSO şirketi, avukatları aracılığıyla soruşturmayla ile ilgili kamuoyuna yaptığı açıklamada Pegasus Projesi kapsamında öne sürülen tüm iddiaları kesin olarak reddettiklerini, iddiaların Pegasus veya diğer NSO ürünlerini kullanan müşterilerin hedef listesiyle hiçbir ilgisi olmayan, HLR arama hizmetleri gibi, erişilebilir ve açık temel bilgilerden sızdırılan verilerin yanıltıcı bir şekilde yorumlanmasına dayandığını ifade

etmiştir (Guardian, 2021). Açıklamada, sözleşme koşulları ve ulusal güvenlik hususları nedeniyle NSO şirketinin, hükümet müşterilerinin isimlerini açıklamayacağı ifade edilmiştir (Kirchgaessner vd., 2021). Açıklamada, Meksika'daki bir NSO müşterisinin 2017 yılında öldürülmeden önce Meksikalı gazeteci Cecilio Pineda'yı hedeflediği haberinin doğru olsa bile NSO müşterisinin veya NSO yazılımı tarafından toplanan verilerin gazetecinin öldürülmesiyle bağlantısı olduğu anlamına gelmeyeceği ifade edilmiştir. Ayrıca, yazılımın ABD'de siber gözetim gerçekleştirmek için kullanılamayacağı ve hiçbir yabancı müşterinin ABD numaralarına sahip telefonlara erişemeyecekleri ifade edilmiştir. Şirketin, tüm kötüye kullanım iddialarını araştıracağı ve araştırmaların sonuçlarına göre, 2021 Haziran'da şirketin yayınladığı Şeffaflık ve Sorumluluk Raporu'nda belirtildiği gibi kötüye kullanım durumlarında müşterilerin sistemlerini kapatmak gibi uygun önlemleri alınacağı vurgulanmıştır (Guardian, 2021). Haziran 2021'de yayınlanan şirketin ilk Şeffaflık ve Sorumluluk Raporu'nda, insan hakları inceleme süreçlerinin bir sonucu olarak 300 milyon dolarının üzerinde satış fırsatının NSO tarafından reddedildiği; Pegasus casus yazılımının insan hakları endişeleri nedeniyle bazı ülkelere satışına izin verilmediği ifade edilmiştir (NSO Grup, 2021, s.4)

19 Temmuz 2021'de, Uluslararası Af Örgütü'nün, NSO şirketinin gözetleme faaliyetleri için ABD merkezli bulut bilişim platformu Amazon Web Services'in altyapısını kullandığını açıklamasının ardından Amazon Web Services şirketi, NSO şirketine bağlı bulut hesaplarını devre dışı bıraktığını açıklamıştır (Fung, 2021). 21 Temmuz'da Fransa Cumhurbaşkanı Macron, kendisinin, eski Fransa Başbakanı Édouard Philippe'in ve 14 Fransız Bakan'ın telefon numaralarının listede hedef olarak yer aldığının ortaya çıkmasının ardından casus yazılımla ilgili soruşturma talimatı vermiştir. Güvenlik Laboratuvarı'nın adli analiziyle eski Fransa Çevre Bakanı François de Rugby'in telefonunda casus yazılıma ait izlerin olduğu kanıtlanmıştır (Chrisafis, 2021).

24 Temmuz'da ABD merkezli anlık mesajlaşma uygulaması WhatsApp Messenger'ın Genel Müdürü Will Cathcart yaptığı açıklamada, 2019 yılında 1400 WhatsApp kullanıcısına yönelik düzenlenen saldırıların Pegasus casus yazılımıyla gerçekleştiğini ve 2019 yılındaki WhatsApp kullanıcılarına yönelik saldırı ile Pegasus Projesi kapsamında ortaya çıkarılan verilerin örtüştüğünü ifade etmiştir (Kirchgaessner, 2021). 2019 yılının Nisan ile Mayıs ayları arasında 20 farklı ülkeden aralarında üst düzey

hükümet yetkililerinin, politikacıların, gazetecilerin ve insan hakları savunucularının olduğu 1.400 WhatsApp kullanıcısının telefonlarına saldırı gerçekleşmiştir. 29 Ekim 2019'da WhatsApp şirketi, NSO şirketine WhatsApp mesajlaşma uygulamasındaki bir hatadan yararlanarak 1.400 kişinin gözetlenmesine neden olan casus yazılımı yüklemekle suçlayan bir dava açmıştır (Hopkins ve Kirchgaessner, 2019). Mahkeme belgelerinde NSO, müşterilerinin devlet müşterileri olması nedeniyle kendisine devlet dokunulmazlığı verilmesi gerektiğini savunduğu medyada yer almıştır. 9 Ocak 2023'te, ABD Yüksek Mahkemesi, NSO şirketinin daha önceki itirazını reddederek WhatsApp'ın NSO şirketine yönelik dava açmasına izin vermiştir (Reuters, 2023).

29 Ekim 2021'de İrlanda merkezli sivil toplum kuruluşu Front Line Defenders, Filistin merkezli insan hakları örgütü Al Haq kuruluşunun 6 Filistinli çalışanının telefonlarında Pegasus casus yazılımına ait izler tespit etmiştir (Front Line Defenders, 2021). Front Line Defenders kuruluşunun 6 Filistinlinin telefonlarına yönelik adli analizi, Vatandaş Laboratuvarı ve Uluslararası Af Örgütü'nün Güvenlik Laboratuvarı'nın adli analizleriyle doğrulanmıştır (Citizen Lab, 2021; Uluslararası Af Örgütü, 2021c).

3 Kasım 2021'de ABD'de Joe Biden yönetimi, NSO şirketinin ABD'nin dış politikasına ve ulusal güvenlik çıkarlarına aykırı davrandığını belirlediği NSO şirketini ve bir başka İsrail gözetim şirketi olan Candiru şirketini ABD'nin varlık listesine eklemiştir. Federal bir kara liste olan varlık listesinde yer alan şirketlerin, Amerikan şirketleriyle ticareti yasaklanmaktadır (Harwell, Nakashima ve Timberg, 2021a). ABD Ticaret Bakanlığı yaptığı açıklamada, NSO Grup ve Candiru şirketinin casus yazılımlarının, yabancı hükümetlerin ulus ötesi baskı yürütmesine ve otoriter rejimlerin muhalefeti susturmak için kendi egemenlik sınırları dışındaki muhalif politikacıları, gazetecileri ve aktivistleri hedef almasına neden olduğu; şirketlerin kara listeye alınmasının baskı için kullanılan dijital araçların yayılmasını durdurmak da dâhil olmak üzere insan haklarını, ABD dış politikasının merkezine koyma çabalarının bir parçası olduğu belirtilmiştir (Harwell, Nakashima ve Timberg, 2021a).

Candiru şirketi 2014 yılında Birim 8200 mezunu ve eski NSO çalışanları olan Eran Shorer ve Yaakov Weizman tarafından Tel Aviv'de kurulmuştur. Candiru şirketi kurulduktan kısa bir süre sonra NSO şirketinin eski yönetim kurulu üyesi Isaac Zack şirketin en büyük yatırımcısı olmuştur

(Megiddo, 2021). Temmuz 2021'de Toronto Üniversitesi bünyesindeki Vatandaş Laboratuvarı ve Microsoft Tehdit İstihbarat Merkezi'nin adli analizleri sonucunda, 10 ülkeden 100'den fazla politikacı, gazeteci ve aktivistin Candiru tarafından üretilen casus yazılımların hedefi olduğu ortaya çıkarılmıştır. Vatandaş Laboratuvarı'nın yayınladığı raporda, Candiru şirketinin casus yazılımının saldırdığı hedefler arasında Filistin, Lübnan, Türkiye, İran, İsrail, Yemen, İngiltere, Ermenistan ve Singapur yer almaktadır (Marczak, Scott-Railton, Berdan, Abdul Razzak ve Deibert, 2021, s.1).

23 Kasım 2021'de ABD merkezli teknoloji şirketi Apple, NSO şirketine Pegasus yazılımıyla kullanıcılarını gözetlemek ve hedeflemekle suçlayan bir dava açmıştır. Apple şirketi, kullanıcılarının daha fazla suiistimal edilmesini ve zarar görmesini önlemek amacıyla, mahkemeye NSO şirketinin herhangi bir Apple yazılımını, hizmetini veya cihazını kullanmasını yasaklayan kalıcı bir ihtiyati tedbir talebinde de bulunmuştur (Apple, 2021). Apple'ın yasal şikâyeti, Pegasus Projesi skandalının sonuçlarının ve Apple cihazlara sızmak için güvenlik açığından yararlanan NSO şirketinin FORCEDENTRY yazılımının Vatandaş Laboratuvarı tarafından tespit edilmesinin ardından gelmiştir (Marzczak vd., 2021a, s.1).

13 Eylül 2021'de Vatandaş Laboratuvarı, Pegasus casus yazılımının bulaştığı bir Suudi insan hakları savunucusunun telefonunun analizinde, Apple tarafından geliştirilen anlık mesajlaşma uygulaması iMessage platformunda sıfır tıklama açığı keşfetmiştir. Güvenlik Laboratuvarı tarafından FORCEDENTRY adını alan güvenlik açığı, laboratuvarın raporuna göre Apple'ın görsel işleme kütüphanesini hedef almakta ve Apple iOS, MacOS ve WatchOS cihazlarında etkili olmaktadır. Güvenlik açığının Apple şirketine bildirilmesinin ardından 13 Eylül'de Apple yeni bir güncelleme yayınlamıştır (Marczak vd., 2021a, s.1). 3 Aralık'ta ise Apple, 11 ABD Büyükelçiliği çalışanının iPhone telefonlarının Pegasus casus yazılımı tarafından saldırıya uğradığını bildirmiştir (Harwell, Nakashima ve Timberg, 2021b). 21 Aralık'ta ise Güvenlik Laboratuvarı'nda çalışan Bill Marczak, Cemal Kaşıkçı'nın eşi Hana Elatr'ın iki telefonunda da Kaşıkçı cinayetinden önce BAE tarafından hedeflenen Pegasus casus yazılımın izlerini tespit etmiştir (Priest, 2021).

Pegasus Projesinin sonuçlarının açıklanmasının ardından Vatandaş Laboratuvarı'nın yeni Pegasus casus yazılım saldırıları tespit etmesi,

WhatsApp ve Apple şirketlerinin casus yazılım saldırıları için NSO şirketini dava etmesi ve NSO şirketinin ABD'nin ticari kara listesi olan varlık listesine eklenmesi şirket için tüm dünyada olumsuz bir hava yaratmıştır. 21 Ağustos 2022'de NSO şirketi, yaptığı açıklamada şirketin kurucusu ve CEO'su Shalev Hulio'nun görevinden istifa ettiğini duyurmuş; yeniden yapılanma sürecinin bir parçası olarak 100 çalışanın da işten çıkarıldığı ifade edilmiştir (Berger, 2022). İşten çıkarılan 100 çalışanla birlikte şirketin çalışanlarının yaklaşık %13'ünü kaybettiği medyada yer almıştır. Şirket açıklamasında, yeniden yapılanmayla NATO üyesi ülkelere odaklanılarak NSO şirketinin önde gelen yüksek teknoloji siber istihbarat şirketlerinden biri olarak kalmasının sağlanmaya çalışılacağı ifade edilmiştir (Obel ve AP, 2022).

18 Temmuz 2023'te ise ABD Ticaret Bakanlığı, NSO ve Candiru'nun yanı sıra iki İsrailli siber casus yazılım şirketini daha ticari kara listesine eklediğini açıklamıştır. İsrail dışında faaliyet gösteren Yunanistan merkezli Intellexa ve Kuzey Makedonya merkezli Cytrox şirketleri, ABD'nin varlık listesinde yer almıştır (Benjakob ve Reuters, 2023). Cytrox şirketi, 2017 yılında İsrail Havacılık ve Uzay Sanayisi'nden sağlanan finansmanla Rotem Farkash tarafından Kuzey Makedonya'nın Üsküp kentinde kurulmuştur (Benjakob ve Reuters, 2023). 2019 yılında şirket, İsrail'in siber elit birimi Birim 81'in eski komutanı Tal Dillian'ın başkanlığını yaptığı Yunanistan'da faaliyet gösteren Intellexa şirketi tarafından satın alınmıştır. Cytrox şirketi hedef alınan kişinin gönderilen bağlantıya tıklamasıyla mobil cihazdaki tüm verilere ulaşan Predator casus yazılımını geliştirmiştir (Haaretz, 2023). Mart 2022'de, Vatandaş Laboratuvarı, Yunan gazeteci Thanasis Koukakis'in telefonunda Predator casus yazılımının izlerini bulmuştur (Telloglou ve Triantafillou, 2022). Temmuz 2022'de ise Avrupa Parlamentosu Laboratuvarı, Yunanistan'ın Panhelenik Sosyalist Hareket Partisi lideri Nikos Androulakis'in mobil cihazında Predator casus yazılımının yüklenmesi için gönderilen bir mesaj bulmuştur (Mildebrath, 2022). Yunan muhalif lider Androulakis ve Yunan gazeteci Koukasis'in casus yazılımla hedef alınmasını kapsayan 2022 Yunanistan dinleme skandalının ardından ABD, Intellexa ve Cytrox şirketlerini varlık listesine eklemiştir (Benjakob ve Reuters, 2023).

Birçok hükümete ülkelerinde veya egemenlik sınırları dışında muhalif grupları hedef almalarına ve muhalif gruplar üzerinde baskı oluşturmalarına neden olan casus yazılımı satmakla suçlanan NSO şirketine yönelik davalar

ve soruşturmalar günümüzde devam etmektedir. ABD'nin kara listesi olarak adlandırılan varlık listesinde bulunan şirket, ABD şirketleriyle de olası iş fırsatlarını kaybetmektedir. Nitekim casus yazılımı satın almak için NSO şirketi ile görüşmelerde bulunan Amerikalı savunma yüklenicisi L3 Harris Teknolojileri şirketi, ABD yönetiminin olası herhangi bir anlaşmanın ABD hükümeti için ciddi karşı istihbarat ve güvenlik kaygıları yaratacağına dair uyarısının ardından satın alma görüşmelerine son vermiştir (Kirchgaessner, 2022a). Mart 2023'te de ABD Hükümeti, ABD kamu kurumlarının ve departmanlarının ulusal güvenlik riskleri oluşturabilecek veya küresel olarak insan haklarını tehlikeye atacak şekilde kötüye kullanılabilecek ticari casus yazılımlar kullanmasını yasaklamıştır (ABD Beyaz Saray, 2023). Bu bağlamda, ABD kamu kurumlarının ve departmanlarının, ticari kara listesinde bulunan Pegasus casus yazılımı satın alması engellenmiştir.

3.3. İsrail Hükümeti'nin Pegasus Projesi Kapsamında Sorumluluğu

İsrail ihracat kontrolü uygulamaları, 2007 tarihli Savunma İhracatı Kontrol Kanunu'na ve takip eden resmi düzenlemelere dayanmaktadır. İsrail resmi olarak Wassenaar Düzenlemesi'nin bir üyesi değildir. Ancak, Savunma İhracatı Kontrol Kanunu, konvansiyonel silahların ve çift kullanımlı mal ve teknolojilerin transferinde şeffaflığı ve daha fazla sorumluluğu teşvik eden uluslararası Wassenaar Düzenlemesi'nin çift kullanımlı ürünler ve teknolojiler listesine atıfta bulunmaktadır (İsrail Savunma Bakanlığı, 2007, s.7; (Wassenaar Düzenlemesi, 2023a; Silahlı Kontrol Derneği, 2022). İsrail'de savunma ürünlerinin ihracat lisanslarının verilmesinden sorumlu DECA, siber gözetim ve casus yazılım ürünlerini de kapsayan çift kullanımlı ürünler ve teknolojiler için Wassenaar Düzenlemesi'ne uygun şekilde lisans vermektedir (İsrail Savunma Bakanlığı, 2007, s.7; Gross, 2021). DECA, Wassenaar Düzenlemesi'ne uymayan İsrailli siber güvenlik şirketlerinin ürünlerinin lisanslanmasını kısıtlayabilmektedir. Ayrıca, DECA, İsrailli şirketlere ait casus yazılım ürünlerini satın almak isteyen ülkelerin insan hakları kayıtları için kendi incelemesini yürütebilmektedir (Harris ve Mekhennet, 2021). Bu bağlamda, İsrail Savunma Bakanlığı, casus yazılımların yurt dışına satılmasında gözetim ve kontrol rolü üstlenmekte ve İsrailli gözetleme şirketlerinin müşteri seçimlerinde son karar yetkisine sahip olmaktadır.

Pegasus Projesi skandalının ardından 6 Aralık 2021'de DECA, siber sistemlerin ihracatına ilişkin düzenlemeyi sıkılaştırdığını duyurmuştur.

DECA, Pegasus casus yazılımı gibi siber saldırı teknolojilerini satın almak isteyen ülkelerin imzalaması gereken Nihai Müşteri Beyannamesi'nin yeni bir versiyonunu yayınlamıştır. Yeni beyannamenin şartlarına göre ülkeler, teknolojiyi yalnızca terör ve ciddi suçları önlemek için kullanacağını taahhüt etmek zorundadır. Beyannamede belirtilen yükümlülüklere uyulmaması durumunda siber sistemin kullanımının kısıtlanması veya kapatılması dâhil olası yaptırımlar açıkça belirtilmektedir (İsrail Dışişleri Bakanlığı, 2021).

Günümüzde, Pegasus ve Candiru casus yazılımlarıyla hükümet yetkililerinden avukatlara birçok kişinin hedef alınarak kişiler üzerinde hukuka aykırı gözetim yapılması, kişilerin özel hayat ve mahremiyetinin çiğnenmesi, ifade özgürlüğü basın özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlal edilmesi Wassenaar Düzenlemesi'nin bölgesel ve uluslararası güvenlik ve istikrara katkıda bulunma ve terörle mücadele gibi amaçlarıyla uyuşmamaktadır. Casus yazılımların sebep olduğu insan hakları ve temel özgürlüklerin ihlalinden casus yazılımları baskı araçları olarak kullanan hükümetlerle birlikte casus ürünleri satın almak isteyen ülkelerin insan hakları kayıtları için kendi incelemesini yürütebildiği halde yazılımların bu otoritelere satışına onay veren İsrail Savunma Bakanlığı ve İsrail Hükümeti de sorumlu olmaktadır.

Pegasus Projesinin sonuçlarının yayınlanmasının hemen ardından Haaretz gazetesi tarafından yayınlanan araştırmada, Pegasus Projesi skandalı kapsamında casus yazılımı satın aldığı ortaya çıkan aralarında Suudi Arabistan, Macaristan, Azerbaycan, Birleşik Arap Emirlikleri, Ruanda, Hindistan ve Meksika'nın yer aldığı ülkelerle İsrail'in son yıllarda önemli diplomatik ilişkiler geliştirdiği ifade edilmiştir (Ziv, 2021). Nitekim bu ülkelerden biri olan Suudi Arabistan ile Cemal Kaşıkçı cinayetinde Pegasus yazılımının kullanıldığı suçlamaları üzerine NSO şirketinin aynı yıl sözleşmesini feshettiği; ancak 2019 ortalarında NSO şirketi tekrardan Suudi Arabistan'a sistemlerini açtığı medyada yer almıştır. New York Times gazetesinin İsrailli yetkililere dayandırdığı haberinde, İsrail Hükümeti'nin NSO şirketine Suudi Arabistan ile tekrardan çalışması için baskı yaptığı ve baskı sonucu NSO şirketi yazılım sistemlerini tekrardan Suudi Arabistan'a açtığı ifade edilmiştir (Bergman ve Mazzetti, 2021b). Bu bağlamda Pegasus casus yazılımının ülkelere satışına izin veren DECA'nın İsrail'in dış politikasıyla uyumlu kararlar aldığı, İsrail'in ilişkilerini geliştirdiği ülkelere Pegasus yazılımının satışına onay verdiği değerlendirilmektedir. İsrail Hükümeti'nin Pegasus casus yazılımından diplomasi alanında kullanılabilir

bir araç olarak fayda sağlamak amacıyla ulusal çıkarları için yaşanan insan hakları ihlallerini göz ardı ederek baskıcı rejimlerin yazılımı kullanmasına onay vermesi, yazılımı üretim amacından uzaklaştırmaktadır.

SONUÇ

İsrailli siber casusluk şirketi NSO'nun son yıllarda Pegasus casus yazılımını birçok otoriter rejime ihraç ettiği ve ürünlerin devlet başkanlarından gazetecilere kadar binlerce insan üzerinde kullanıldığı Pegasus Projesi soruşturması kapsamında medyada yer almıştır (Uluslararası Af Örgütü, 2021a). Proje kapsamında listede telefon numarası yer alan politikacılardan gazetecilere birçok kişinin casus yazılım tarafından hedef alındığı, kişiler üzerinde hukuka aykırı gözetim yapıldığı, kişilerin özel hayat ve mahremiyetinin çiğnendiği, yazılımın basın özgürlüğü ve ifade özgürlüğü olmak üzere diğer insan hakları ihlallerine neden olduğu ortaya çıkmıştır (Kaldani ve Prokopets, 2022, s.19-20; Richard, 2021). Uluslararası Af Örgütü'nün Güvenlik Laboratuvarı tarafından listede kayıtlı telefon numaralarının kullanıldığı 67 telefona ulaşarak yapılan adli analizlerde, 67 telefonun yarısından fazlasında Pegasus casus yazılımına ait izlerinin olduğunun ortaya çıkarılmış, Uluslarararası Af Örgütü'nün ulaştığı sonuçlar bağımsız bir kuruluş olan Vatandaş laboratuvarı tarafından da doğrulanmıştır (Marczak, Scott-Railton, Anstis ve Deibert, 2021). İki kuruluş tarafından 67 telefonun yarısından fazlasında Pegasus casus yazılımının bulaştığının doğrulanması, Uluslararası Af Örgütü ve Forbidden Stories tarafından ortaya çıkarılan listesinin Pegasus casus yazılımı için bir hedef listesi olduğu düşüncesini güçlendirmiştir (Pfenniger, 2023).

Casus yazılımların sebep olduğu insan hakları ve temel özgürlüklerin ihlalleri doğrudan satın alan hükümetler tarafından kaynaklansa da casus ürünleri satın almak isteyen ülkelerin insan hakları kayıtları için kendi incelemesini yürütebildiği halde casus yazılımların satın alan hükümetler tarafından muhalifler üzerinde kullanılmasına izin veren İsrail Hükümeti de bu ihlallerden sorumlu olmaktadır. Casus yazılımın neden olduğu insan hakları ve temel özgürlüklerin ihlalini ortaya çıkaran Pegasus Projesi skandalı, İsrail'de kamunun siber ihracatta özel sektör üzerinde tam kontrol gücüne sahip olmasıyla kamu-özel sektör iş birliğinin kötüye kullanıldığını gösteren önemli bir örnek olmaktadır. Başta Pegasus olmak üzere casus yazılımlarla muhalif grupların hedef alınması, kişilerin hukuka aykırı takip

edilmesi, özel hayat ve mahremiyetinin ihlal edilmesi, ifade özgürlüğü ve basın özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin engellenmesi, İsrail'in Savunma Bakanlığı'nın bağlı olduğunu ifade ettiği Wassenaar Düzenlemesi'nin bölgesel ve uluslararası güvenlik ve istikrara katkıda bulunma ve terörle mücadele gibi amaçlarıyla uyuşmamaktadır.

İsrailli siber casus yazılımların devletlere satışında lisans verme yetkisine sahip olan İsrail, yazılımların satışını ulusal çıkarları için diplomatik bir araç olarak kullanabilmekte ve insan haklarını göz ardı ederek İsrail casus yazılımlarını muhalif gruplar üzerinde baskı aracı olarak kullanan otoriter rejimlere satabilmektedir. Nitekim, Haaretz gazetesi tarafından, Pegasus Projesi skandalı kapsamında casus yazılımı satın aldığı ortaya çıkan Suudi Arabistan ve BAE gibi ülkelerle İsrail'in son yıllarda önemli diplomatik ilişkiler geliştirdiği ifade edilmiştir (Ziv, 2021). İsrail Hükümeti'nin NSO şirketinin Cemal Kaşıkçı cinayetinin ardından Suudi Arabistan ile sözleşmeyi feshettiği ancak İsrail Hükümeti'nin baskısıyla yazılım sistemlerini tekrardan Suudi Arabistan'a açtığı iddiası medyada yer almıştır (Bergman ve Mazzetti, 2021b). İsrail Hükümeti'nin Pegasus casus yazılımından diplomasi alanında kullanılabilir bir araç olarak fayda sağlamak amacıyla ulusal çıkarları için mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlalini göz ardı ettiği görülmektedir.

Pegasus casus yazılım skandalın ortaya çıkmasının ardından şirket birçok olumsuz durumla karşılaşmıştır. Amazon Web Services şirketi, NSO şirketine bağlı bulut hesaplarını devre dışı bırakmış; WhatsApp ve Apple şirketlerinin casus yazılım saldırıları için NSO şirketini dava etmiştir (Fung, 2021). NSO şirketi ABD Hükümeti tarafından ABD'nin ticari kara listesi olan varlık listesine eklenirken ABD Merkezli önde gelen savunma şirketi L3 Harris Teknolojileri ABD Hükümeti'nin baskısıyla casus yazılımının satın alam işlemlerine son vermiştir (Harwell, Nakashima ve Timberg, 2021a; Kirchgaessner, 2022a). Şirket yeniden yapılanma adı altında 100 çalışanını işten çıkarırken şirketin kurucusu Shalev Hulio başkanlık görevinden istifa etmiştir. Şirket yeniden yapılanmayla hedef pazar olarak NATO üyesi ülkelere odaklandığını açıklamıştır (Obel ve AP, 2022). Pegasus Projesi skandalının ardından şirketin kendine yönelik dava, soruşturma ve ambargolardan dolayı maddi kayıplar yaşadığı görülmektedir. Şirketin yeniden yapılanmayla birlikte NATO üyesi ülkelere odaklanma stratejisiyle hem daha çok Avrupalı müşteriler kazanmak hem de yazılımları

baskı aracı olarak kullanan hükümetlere casus yazılım sattığına yönelik eleştirileri ortadan kaldırmak istediği düşünülebilir.

Pegasus Projesi skandalının ardından İsrailli yazılımlarının yurt dışına satışında onay makamı DECA, siber sistemlerin ihracatına ilişkin düzenlemeyi sıkılaştırdığını duyurmuş; yeni müşteri beyannamesinde müşteri ülkelerin teknolojini yalnızca terör ve ciddi suçları önlemek için kullanacağını taahhüt etmek zorunda olduğu belirtilmiştir (İsrail Dışişleri Bakanlığı, 2021). Bu bağlamda, Pegasus başta olmak üzere İsrailli siber gözetim yazılımlarının satın almak isteyen ülkelerin Pegasus gibi siber yazılımları muhalif gruplar üzerinde kullanılmasının önüne geçilmek istendiği görülmektedir. İsrail Hükümeti'nin siber sistemlerin ihracatına ilişkin düzenlemeyi sıkılaştırmasıyla İsrail'in kendisine yönelik Pegasus casus yazılımının neden olduğu insan hakları ve temel özgürlüklerin ihlaline göz yumduğu suçlamalarını ortadan kaldırmayı ve küresel kamuoyu baskısını azaltmayı amaçladığı düşünülebilir.

Günümüzde baskıcı otoriteler tarafından Pegasus yazılımı kullanılarak neden olunan mahremiyet hakkı ve ifade özgürlüğü olmak üzere insan hakları ve temel özgürlüklerin ihlali, NSO şirketine yönelik devam eden davalar ve yazılımın Kaşıkçı ve Pineda cinayetleriyle ilişkilendirilmesi, Pegasus'un kötü bir ünle anılmasına neden olmaktadır. İsrail'in İsrailli casus yazılımların baskıcı rejimlere satılmasına izin veren politikasını sürdürmesi, İsrailli siber gözetim şirketlerinin ABD örneğinde olduğu gibi daha fazla ülke tarafından kara listeye eklenmesine, Amerikalı L3 Harris Teknoloji şirketiyle yaşananlar gibi küresel şirketlerle olası iş birliği fırsatlarının kaybedilmesi ve mali kayıpların yaşanmasına, İsrail siber endüstrisine yönelik yatırımların azalmasına ve endüstrinin dünyada en çok siber yatırım çeken endüstri pozisyonunu da kaybetmesine neden olabilir. Sonuç olarak, İsrail'de siber güvenlik alanında kamu-özel sektör iş birliğinde siber ihracatta kamunun özel sektör üzerinde tam yetkiye sahip olması, iş birliğinin kötüye kullanılmasına ve insan hakları ihlallerinin yaşanmasına neden olmaktadır.

Bu makalede, siber güvenlik alanında kamu-özel sektör ve akademi iş birliği modeli, İsrail örneği üzerinden incelenmiş ve iş birliğinde İsrail Hükümeti'nin siber ürünlerin ihracatında özel sektör üzerinde tam kontrol gücüne sahip olmasının neden olduğu kötüye kullanım Pegasus Projesi kapsamında ele alınmıştır. Çalışmada günümüz güvenlik ortamının en

önemli konularından biri olan siber güvenlik konusu özel sektör iş birliği boyutuyla incelenerek literatüre katkı sağlanması amaçlanmaktadır. Çalışma ülkemizin siber güvenlik politikalarının şekillendirilmesi konusundaki fayda sağlayabileceği ve siber güvenlik alanına yapılacak yatırımlar için ülkemize yol gösterici olabileceği gibi, benzer yazılımlara karşı güvenlik eksenli oluşturacağı farkındalık da önem taşımaktadır. Çalışmanın Türkçe literatüre kazandırılmasının akademinin yol gösterici olarak yapacağı ileri çalışmalara katkı sağlayacağı değerlendirilmektedir.

KAYNAKÇA

ABD Beyaz Saray. (2023). *Fact Sheet: President Biden Signs Executive Order To Prohibit U.S. Government Use of Commercial Spyware That Poses Risks To National Security*. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/

ABD Fas Büyükelçiliği. (2020). *December 22, 2020 a Historic Day For Morocco, Israel, and the United States*. https://ma.usembassy.gov/white-house-senior-advisor-to-the-president-jared-kushner-visit/

Apple (2021). *Apple Sues NSO Group To Curb The Abuse of State-Sponsored Spyware*. https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/

BBC. (2017, 4 Temmuz). *Narendra Modi Becomes First Indian PM To Visit Israel*. Erişim Tarihi: 12 Eylül 2023, https://www.bbc.com/news/world-asia-india-40489746

BBC. (2021, 24 Şubat). *Jamal Khashoggi: All You Need To Know About Saudi Journalist's Death*. Erişim Tarihi: 8 Eylül 2023, https://www.bbc.com/news/world-europe-45812399

Benjakob, O. (2022, 5 Nisan). The NSO File: A Complete (Updating) List of Individuals Targeted With Pegasus Spyware. *Haaretz*. Erişim Tarihi: 6 Eylül 2023, http://www.haaretz.com/israel-news/tech-news/2022-04-05/ty-article-magazine/nso-pegasus-spyware-file-complete-list-of-individuals-targeted/0000017f-ed7a-d3be-ad7f-ff7b5a600000

Benjakob, O. & Reuters. (2023, 18 Temmuz). U.S. Blacklists Israeli-owned Cyber Arms Firms. *Haaretz*. Erişim Tarihi: 11 Eylül 2023, https://www.haaretz.com/israel-news/security-aviation/2023-07-18/ty-

article/.premium/intellexa-cytrox-tal-dilian-u-s-blacklists-israeli-owned-cyber-arms-firms/00000189-6927-dc94-a78d-f9ef48d10000

Berger. M. (2022, 22 Ağustos). CEO of Israeli NSO Spyware Company Steps Down Amid Shakeup. *The Washington Post*. Erişim Tarihi: 11 Eylül 2023, https://www.washingtonpost.com/world/2022/08/22/nso-pegasus-ceo-shalev-hulio-israel/

Bergman, R. (2019, 1 Ekim). Exclusive: How Mexican Drug Baron El Chapo Was Brought Down By Technology Made In Israel. *Ynetnews*. Erişim Tarihi: 31 Ağustos 2023, https://www.ynetnews.com/articles/0,7340,L-5444330,00.html [Erişim Tarihi: 31.8.2023].

Bergman R. & Mazzetti M. (2021, 17 Temmuz). Israeli Companies Aided Saudi Spying Despite Khashoggi Killing. *New York Times*. Erişim Tarihi: 13 Eylül 2023, https://www.nytimes.com/2021/07/17/world/middleeast/israel-saudi-khashoggi-hacking-nso.html

Bergman, R. & Mazzetti, M. (2022, 28 Ocak). The Battle for the World's Most Powerful Cyberweapon. *New York Times Magazine*. Erişim Tarihi: 17 Ağustos 2023, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html [Erişim Tarihi:17.8.2023].

BilgiGüvende. (2020, 13 Mayıs). *Siber Güvenlik Dünyasında Bir Başka Gizli Tehdit: Zero-Click Saldırısı.* Erişim Tarihi: 29 Ağustos 2023, https://bilgiguvende.com/siber-guvenlik-dunyasinda-bir-baska-gizli-tehdit-zero-click-saldirisi/

Brewster, T. (2021, 22 Temmuz). 'If You're Not A Criminal, Don't Be Afraid'—NSO CEO On 'Insane' Hacking Allegations Facing $1 Billion Spyware Business". *Forbes*. Erişim Tarihi: 5 Eylül 2023, https://www.forbes.com/sites/thomasbrewster/2021/07/22/nso-group-ceo-defends-1-billion-spyware-company-against-pegasus-project-hacking-allegations/?sh=54db5cc4472d

CBS News. (2019, 24 Mart). *CEO of Israeli Spyware-Maker NSO On Fighting Terror, Khashoggi Murder, and Saudi Arabia.* Erişim Tarihi: 8 Eylül 2023, https://www.cbsnews.com/news/interview-with-ceo-of-nso-group-israeli-spyware-maker-on-fighting-terror-khashoggi-murder-and-saudi-arabia-60-minutes/

Chrisafis, A. (2021, 21 Temmuz). Macron Orders Multiple Inquiries Into Leaked Pegasus Project Data. *Guardian.* Erişim Tarihi: 9 Eylül 2023, https://www.theguardian.com/news/2021/jul/21/macron-orders-multiple-inquiries-into-leaked-pegasus-project-data

Chrisafis, A., Sabbagh, D., Kirchgaessner S., Safi M. (2021, 20 Temmuz). Emmanuel Macron Identified In Leaked Pegasus Project Data. *Guardian.* Erişim Tarihi: 7 Eylül 2023, https://www.theguardian.com/world/2021/jul/20/emmanuel-macron-identified-in-leaked-pegasus-project-data

Citizen Lab. (2021). *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware.* https://citizenlab.ca/2021/11/palestinian-human-rights-defenders-hacked-nso-groups-pegasus-spyware/

D'Souza, J. (2023). *Pegasus Spyware: A Violation of Right to Privacy and a Threat to Surveillance Laws in India*. Journal of Legal Studies & Research, Cilt: 9, Sayı:6, ss. 424-438.

Dieterle, L. C. (2023). "Regulating The Invisible Spy – A Case Study of the Pegasus Spyware examining Surveillance Technology Regulation". University of Twente, ss.1-47.

Dogani, R. (2016, 4 Eylül). NSO charges $650,000 to hack 10 iPhones – report. *Globes*. Erişim Tarihi: 6 Eylül 2023, https://en.globes.co.il/en/article-nso-group-charges-650000-to-hack-ten-iphones-report-1001149988

Euronews. (2021, 18 Mayıs). *Hungary Only Nation Against EU Call For Israel-Hamas Ceasefire*. Erişim Tarihi: 13 Eylül 2023, https://www.euronews.com/2021/05/18/eu-fms-due-to-discuss-political-solutions-to-end-israel-gaza-conflict-as-violence-surges-o

Feldstein, S. & Kot, B. (2023). Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. *Carnegie Uluslararası Barış Vakfı.* 1-35.

Fischer, Y. & Levy, R. (2016, 29 Ağustos). The Israelis Behind History's 'Most Sophisticated Tracker Program' That Wormed Into Apple. *Haaretz*. Erişim Tarihi: 28 Ağustos 2023, https://www.haaretz.com/israel-news/business/2016-08-29/ty-article/.premium/the-most-sophisticated-tracking-program/0000017f-f70f-ddde-abff-ff6f051d0000

Forbidden Stories. (2021). *Pegasus Project – All the Articles*". Erişim Tarihi: 6 Eylül 2023, https://forbiddenstories.org/pegasus-project-articles/

Front Line Defenders. (2021, 8 Kasım). *Six Palestinian human rights defenders hacked with NSO Group's Pegasus Spyware.* Erişim Tarihi: 13 Eylül 2023, https://www.frontlinedefenders.org/en/statement-report/statement-targeting-palestinian-hrds-pegasus

Fung, B. (2021, 19 Temmuz). Amazon Web Services Disables Cloud Accounts Linked To NSO Group. *CNN Business*. Erişim Tarihi: 10 Eylül 2023, https://edition.cnn.com/2021/07/19/tech/amazon-nso-group-pegasus-cloud-accounts/index.html

Goodfriend, S. (2021, 23 Kasım). "We Violated People's Privacy For A Living": How Israel's Cyber Army Went Corporate. *+972Magazine*. Erişim Tarihi: 25 Ağustos 2023, https://www.972mag.com/nso-surveillance-companies-israel-army/

Gross, J. A. (2021, 19 Temmuz). Israel: If NSO Group Violated Export Permits, 'Appropriate Action' Will Be Taken. *The Times of Israel*. Erişim Tarihi: 15 Ağustos 2023, https://www.timesofisrael.com/israel-if-nso-group-violated-export-permits-appropriate-action-will-be-taken/

Guardian. (2021, 20 Temmuz). *Response From NSO and Governments*. Erişim Tarihi: 30 Ağustos 2023, https://www.theguardian.com/news/2021/jul/18/response-from-nso-and-governments

Haaretz. (2023, 13 Temmuz). *Report: Israeli Spyware Firm, Ex-security Boss, Advised on Secret Greek Spy Agency Deal*. Erişim Tarihi: 11 Eylül 2023, https://www.haaretz.com/israel-news/security-aviation/2023-07-13/ty-article/report-israeli-spyware-firm-ex-security-boss-advised-on-secret-greek-spy-agency-deal/00000189-4e9a-da08-a5ef-defa40b20000

Harris, S. & Mekhennet, S. (2021, 20 Temmuz). U.S. And E.U. Security Officials Wary of NSO Links To Israeli Intelligence. *The Washington Post*. Erişim Tarihi: 12 Eylül 2023, https://www.washingtonpost.com/national-security/2021/07/20/nso-israel-intelligence/

Harwell, D., Nakashima, E., Timberg, C. (2021a, 3 Kasım). Biden Administration Blacklists NSO Group Over Pegasus Spyware. *The Washington Post*, Erişim Tarihi: 10 Eylül 2023, https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/

Harwell, D., Nakashima, E., Timberg, C. (2021b, 3 Aralık). Pegasus Spyware Used To Hack U.S. Diplomats Working Abroad. *The Washington Post*. Erişim Tarihi: 10 Eylül 2023, https://www.washingtonpost.com/technology/2021/12/03/israel-nso-pegasus-hack-us-diplomats/

Hirschauge, O. & Orpaz, I. (2014, 17 Şubat). U.S. Fund to Buy NSO and Its Smartphone-snooping Software. *Haaretz*. Erişim Tarihi: 30 Ağustos

2023, https://www.haaretz.com/israel-news/business/2014-02-17/ty-article/u-s-fund-to-buy-snooping-software/0000017f-f010-d223-a97f-fdddda30000

Holmes, O. (2020, 23 Kasım). Netanyahu Holds Secret Meeting With Saudi Crown Prince. *Guardian*. Erişim Tarihi: 12 Eylül 2023, https://www.theguardian.com/world/2020/nov/23/benjamin-netanyahu-secret-meeting-saudi-crown-prince-mohammed-bin-salman

Hopkins, N. & Kirchgaessner, S. (2019, 20 Ekim). Whatsapp Sues Israeli Firm, Accusing It of Hacking Activists' Phones. *Guardian*. Erişim Tarihi: 9 Eylül 2023, https://www.theguardian.com/technology/2019/oct/29/whatsapp-sues-israeli-firm-accusing-it-of-hacking-activists-phones

İsrail Dışişleri Bakanlığı. (2021). *Israel Mod Tightens Control of Cyber Exports*. https://www.gov.il/en/departments/news/mod-tightens-control-of-cyber-exports-6-december-2021

İsrail Ekonomi ve Sanayii Bakanlığı. (2023). *Export Control Agency, Ministry of Economy and Industry*. https://www.gov.il/en/Departments/General/duexportcontrol-info

İsrail Savunma Bakanlığı. (2007). *Defense Export Control Law, 5766-2007*. 1-32.

İsrail Savunma Bakanlığı. (2023a). *Defense Exports Control Agency (DECA)*. ,https://english.mod.gov.il/Departments/Pages/DefenseExportsControlAgency.aspx

İsrail Savunma Bakanlığı. (2023b). *Message From Director*. https://exportctrl.mod.gov.il/English/Pages/Message-from-Director.aspx

İsrail Ulusal Siber Müdürlüğü, "Israeli Cyber Security Industry Continues Growth In 2021", 20 Ocak 2022, https://www.gov.il/en/departments/general/israeli-cyber-security-industry-continues-growth-20-jan-2022 [Erişim Tarihi: 13.06.2023].

İsrail Ulusal Siber Müdürlüğü. (2022). *Israeli Cyber Security Industry Continues Growth In 2021*. Erişim Tarihi: 13 Haziran 2023, https://www.gov.il/en/departments/general/israeli-cyber-security-industry-continues-growth-20-jan-2022

Kaldani, T. & Prokopets, Z. (2022). "Pegasus Spyware And Its Impacts On Human Rights". Council of Europe, s.1-23.

Kareem, K. M. (2024). "A Comprehensive Analysis of Pegasus Spyware and Its Implications for Digital Privacy and Security", International Journal of Intelligent Systems and Applications In Engineering, ss.1360-1373, Mart 2024.

Kaspersky. (2023). *Sıfır Tıklama Kötü Amaçlı Yazılımı Nedir ve Sıfır Tıklama Saldırıları Nasıl Gerçekleştirilir?.* Erişim Tarihi: 28 Ağustos 2023, https://www.kaspersky.com.tr/resource-center/definitions/what-is-zero-click-malware

Khurana. A. (2022). "*Misinformation & Pegasus Project: Case study of India*". Univerzita Karlova, Fakulta sociálních věd, Katedra bezpečnostních studií.

Kirchgaessner, S. (2021, 24 Temmuz). Officials Who Are US Allies Among Targets of NSO Malware, Says Whatsapp Chief. *Guardian.* Erişim Tarihi: 9 Eylül 2023, https://www.theguardian.com/technology/2021/jul/24/officials-who-are-us-allies-among-targets-of-nso-malware-says-whatsapp-chief

Kirchgaessner, S. (2022b, 23 Mart). Israel Blocked Ukraine From Buying Pegasus Spyware, Fearing Russia's Anger. *Guardian*. Erişim Tarihi: 13 Eylül 2023, https://www.theguardian.com/world/2022/mar/23/israel-ukraine-pegasus-spyware-russia

Kirchgaessner, S. (2022a, 10 Temmuz). US Defence Firm Ends Talks To Buy NSO Group's Surveillance Technology. *Guardian*. Erişim Tarihi: 10 Eylül 2023, https://www.theguardian.com/us-news/2022/jul/10/us-defence-firm-ends-talks-to-buy-nso-groups-surveillance-technology

Kirchgaessner, S., Lewis, P., Pegg, D., Cutler, S., Lakhani, N., Safi, M. (2021, 18 Temmuz). Revealed: Leak Uncovers Global Abuse of Cyber-Surveillance Weapon. *The Guardian.* Erişim Tarihi: 7 Eylül 2023, https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus

Lakhani, N. (2021, 18 Temmuz). Revealed: Murdered Journalist's Number Selected By Mexican NSO Client. *The Guardian*. Erişim Tarihi: 8 Eylül 2023, https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto

Landau, N. (2020, 15 Eylül). Full Text: The Israel-UAE-Bahrain Abraham Accords Peace Agreement. *Haaretz*. Erişim Tarihi: 13 Eylül 2023, https://www.haaretz.com/middle-east-news/.premium-full-text-the-israel-uae-bahrain-abraham-accords-declaration-1.9159509

Landau, N. & Khoury, J. (2018, 27 Ekim). Netanyahu Visits Oman, Which Has No Diplomatic Ties With Israel. *Haaretz*. Erişim Tarihi: 12 Eylül 2023, https://www.haaretz.com/middle-east-news/2018-10-27/ty-article/netanyahu-secretly-visits-oman-which-has-no-diplomatic-ties-with-israel/0000017f-dc28-d3a5-af7f-feae05340000

Levy, R. (2017, 21 Nisan). Who Makes Millions Off Israel's Top Cyber Spy Agency?, *Haaretz*. Erişim Tarihi: 21 Ağustos 2023, https://www.haaretz.com/israel-news/business/2017-04-21/ty-article/who-makes-millions-off-israels-top-cyber-spy-agency/0000017f-db2e-d3a5-af7f-fbae453c0000

Lior, I. (2017, 20 Kaım). Israel to Pay Rwanda $5,000 for Every Deported Asylum Seeker It Takes In. *Haaretz*. Erişim Tarihi: 14 Eylül 2023, https://www.haaretz.com/israel-news/2017-11-20/ty-article/israel-to-pay-rwanda-5-000-for-every-asylum-seeker-deported-there/0000017f-e9cc-da9b-a1ff-edefea800000

Lipson, N. (2017, 27 Ekim). Goodbye Uzi, Hello Big Brother: The Israelis Arming the World With Sophisticated Cyber-weapons. *Haaretz*. Erişim Tarihi: 1 Eylül 2023, https://www.haaretz.com/israel-news/2017-10-27/ty-article/the-new-face-of-israels-arms-exporters/0000017f-db9c-db22-a17f-ffbd474f0000

Marczak, B., Scott-Railton, J., Anstis S., Deibert, R. (2021, Temmuz). Independent Peer Review of Amnesty International's Forensic Methods for Identifying Pegasus Spyware. *The Citizen Lab*. Toronto Üniversitesi. https://citizenlab.ca/2021/07/amnesty-peer-review/

Marczak, B., Scott-Railton, J., Berdan, K., Abdul Razzak, B., Deibert, R. (2021, Temmuz). Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus. *Citizen Lab Araştırma Raporu* No.139, Toronto Üniversitesi. 1-14.

Marczak, B., Scott-Railton, J., Abdul Razzak, B., Al-Jizawi, N., Anstis, S., Berdan, K., Deibert, R. (2021a, Eylül). Forcedentry: NSO Group iMessage Zero-Click Exploit Captured in the Wild. *Citizen Lab Araştırma Raporu* No:143, Toronto Üniversitesi. 1-4.

Marczak, B., Scott-Railton, J., Abdul Razzak, B., Al-Jizawi, N., Anstis, S., Berdan, K., Deibert, R. (2021b, Aralık). Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware. *Citizen Lab*. Toronto Üniversitesi. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/

Mazzetti, M., Bergman R., Stevis-Gridneff, M. (2022, 8 Aralık). How the Global Spyware Industry Spiraled Out of Control. *The New York*

Times. Erişim Tarihi: 4 Eylül 2023, https://www.nytimes.com/2022/12/08/us/politics/spyware-nso-pegasus-paragon.html

Megiddo, G. (2021, 17 Aralık). "We're on the U.S. Blacklist Because of You": The Dirty Clash Between Israeli Cyberarms Makers. *Haaretz*. Erişim Tarihi: 18 Ağusots 2023, https://www.haaretz.com/israel-news/2021-12-17/ty-article-magazine/.highlight/were-on-the-u-s-blacklist-because-of-you-the-clash-of-israeli-cyberarms-firms/0000017f-f195-dc28-a17f-fdb72e9a0000

Melman, Y. (2021, 21 Temmuz). Pegasus Scandal Turns Spotlight on Israel's Controversial Military Tech Sector. *Middle East Eye*. Erişim Tarihi: 18 Ağustos 2023, https://www.middleeasteye.net/news/pegasus-israel-scandal-military-tech-sector-spotlight

Mildebrath, H. (2022, Eylül). Greece's Predatorgate: The Latest Chapter In Europe's Spyware Scandal?. *Avrupa Parlamentosu Araştırma Servisi*. https://www.europarl.europa.eu/RegData/etudes/ATAG/2022/733637/EPRS_ATA(2022)733637_EN.pdf

News Room Panama. (2021, 26 Temmuz). *'Disappeared' Pegasus Spyware Used In Panama In 2012*. Erişim Tarihi: 1 Eylül 2023, https://www.newsroompanama.com/news/disappeared-pegasus-spyware-used-in-panama-in-2012

NSO Grup. (2021). *Transparency and Responsibility Report 2021*. 1-32.

NSO Grup. (2023). *About Us*. Erişim Tarihi: 1 Eylül 2023, https://www.nsogroup.com/about-us/

Obel, A. & AP (2022, 21 Ağustos). NSO Group's Hulio Steps Down As CEO Of Spyware Firm, 100 Employees Let Go. *Haaretz*. Erişim Tarihi: 10 Eylül 2023, https://www.timesofisrael.com/nso-groups-hulio-steps-down-as-ceo-of-spyware-firm-100-employees-let-go/

O'neill, P. H. (2017, 12 Haziran). Israeli Hacking Company NSO Group Is On Sale For More Than $1 Billion. *CyberScoop*. Erişim Tarihi: 1 Eylül 2023, https://cyberscoop.com/nso-group-for-sale-1-billion-pegasus-malware/ [Erişim Tarihi: 1.9.2023].

Oren, A. (2010, Ocak). The IDF's New Battlefield Is Found In Computer Networks. Erişim Tarihi: 24 Mayıs 2023, http://www.haaretz.co.il/misc/1.1182490

Perltroth, N. (2016, 2 Eylül). How Spy Tech Firms Let Governments See Everything on a Smartphone. *The New York Times*. Erişim Tarihi: 1 Eylül 2023, https://www.nytimes.com/2016/09/03/technology/nso-

group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html

Pfenniger, K. (2023, 17 Temmuz). Pegasus Project: What Has Happened Since The Revelations?. Forbidden Stories. Erişim Tarihi: 9 Eylül 2023, https://forbiddenstories.org/pegasus-project-impacts-map/

Priest, D. (2021, 21 Aralık). A UAE Agency Put Pegasus Spyware On Phone of Jamal Khashoggi's Wife Months Before His Murder, New Forensics Show. *The Washington Post*. Erişim Tarihi: 12 Eylül 2023, https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/

Priest, D., Mekhennet, S., Bouvart, A. (2021, 18 Temmuz). Jamal Khashoggi's Wife Targeted With Spyware Before His Death. *The Washington Post*. Erişim Tarihi: 8 Eylül 2023, https://www.washingtonpost.com/investigations/interactive/2021/jamal-khashoggi-wife-fiancee-cellphone-hack/

Reuters. (2023, 9 Ocak). *U.S. Supreme Court Lets Meta's WhatsApp Pursue 'Pegasus' Spyware Suit,* Erişim Tarihi: 10 Eylül 2023, https://www.reuters.com/legal/us-supreme-court-lets-metas-whatsapp-pursue-pegasus-spyware-suit-2023-01-09/

Richard, L. (2021, Temmuz 18). The Pegasus Project: A Worldwide Collaboration to Counter A Global Crime". *Forbidden Stories*. Erişim Tarihi: 7 Eylül 2023, https://forbiddenstories.org/the-pegasus-project-a-worldwide-collaboration-to-counter-a-global-crime/

Sabbagh, D., Pegg, D., Lewis P., Kirchgaessner, S. (2021, 21 Temmuz). UAE linked to listing of hundreds of UK phones in Pegasus project leak. *Guardian.* Erişim Tarihi: 7 Eylül 2023, https://www.theguardian.com/world/2021/jul/21/uae-linked-to-listing-of-hundreds-of-uk-phones-in-pegasus-project-leak

Sadeh, S. (2020, 31 Aralık). A Shady Israel Intel Genius, His Cyber-spy Van and Million Dolar Deals. *Haaretz*. Erişim Tarihi: 19 Ağustos 2023, https://www.haaretz.com/israel-news/tech-news/2020-12-31/ty-article-magazine/.highlight/a-shady-israeli-intel-genius-his-cyber-spy-van-and-million-dollar-deals/0000017f-f21e-d497-a1ff-f29ed7c30000

Schwartz, M. J. (2021, 19 Temmuz). Leak of 50,000 Contact Details Tied to Spyware Targeting. *Bank of Security*. Erişim Tarihi: 7 Eylül 2023, https://www.bankinfosecurity.com/leak-50000-contact-details-tied-to-spyware-targeting-a-17097

Shahaf, T. (2018, 5 Temmuz). Verint Was Reportedly About to Buy NSO At A $1 Billion Valuation. *Globes*. Erişim Tarihi: 1 Eylül 2023,

https://en.globes.co.il/en/article-nso-cyber-weapon-co-sale-to-verint-in-jeopardy-1001244757

Shahaf, T. (2019, 11 Nisan). Technology. *Ynetnews*. Erişim Tarihi: 11 Eylül 2023, https://www.ynetnews.com/articles/0,7340,L-5618901,00.html

Shezaf, H. & Jacobson, J. (2018, 20 Ekim). Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays. *Haaretz*. Erişim Tarihi: 15 Ağustos 2023, 20 Ekim 2018, https://www.haaretz.com/israel-news/2018-10-20/ty-article-magazine/.premium/israels-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays/0000017f-e9a9-dc91-a17f-fdadde240000

Arms Control Association. (2022). *The Wassenaar Arrangement at A Glance*. https://www.armscontrol.org/factsheets/wassenaar

Sneha. (2023, Nisan). "The Pegasus Spyware: Endorsing The Citizens' Right To Privacy". Journal of Legal Research and Juridical Sciences. Vol:2, Sayı:3, s.451-468, ISSN (O): 2583-0066.

Solomon, S. (2019, 14 Şubat). NSO Founders, Management Buy Stake In Firm From Francisco Partners. *The Times of Israel*. Erişim Tarihi: 5 Eylül 2023, https://www.timesofisrael.com/nso-founders-management-buy-stake-in-firm-from-francisco-partners/

Stone M. & Roumeliotis, G. (2015, 3 Kasım). Secretive Cyber Warfare Firm NSO Group Explores Sale: Sources. *Reuters*. Erişim Tarihi: 1 Eylül 2023, https://www.reuters.com/article/us-nsogroup-m-a-idUSKCN0SR2JF20151103

Telloglou, T., Triantafillou, E. (2022, 11 Nisan). Ποιος παρακολουθούσε το κινητό του δημοσιογράφου Θανάση Κουκάκη. *Inside Story*. Erişim Tarihi: 11 Eylül 2023, https://insidestory.gr/article/poios-parakoloythoyse-kinito-toy-dimosiografoy-thanasi-koykaki

Theoi Project. *Pegasos*. Erişim Tarihi: 30 Ağustos 2023, https://www.theoi.com/Ther/HipposPegasos.html

Timberg, C., Birnbaum, M., Harwell, D., Sabbagh, D. (2021, 20 Temmuz). On The List: Ten Prime Ministers, Three Presidents And A King. *The Washington Post*. Erişim Tarihi: 16 Eylül 2023, http://www.washingtonpost.com/world/2021/07/20/heads-of-state-pegasus-spyware/

Timberg, C., Kirchgaessner, S., Mekhennet, S., Nakashima, E., Harris, S. (2022, 23 Mart). Israel Blocked Ukraine From Getting Potent Pegasus Spyware. *The Washington Post*. Erişim Tarihi: 13 Eylül 2023, https://www.washingtonpost.com/technology/2022/03/23/urkraine-spyware-pegasus-russia/

Uluslararası Af Örgütü. (2021a). *Massive Data Leak Reveals Israeli NSO Group's Spyware Used to Target Activists, Journalists, and Political Leaders Globally*. https://www.amnesty.org/en/latest/press-release/2021/07/the-pegasus-project/

Uluslararası Af Örgütü. (2021b). *Forensic Methodology Report: How To Catch NSO Group's Pegasus*. 1-81. DOC 10/4487/2021.

Uluslararası Af Örgütü. (2021c). *Devices of Palestinian Human Rights Defenders Hacked with NSO Group's Pegasus Spyware.* https://www.amnesty.org/en/latest/research/2021/11/devices-of-palestinian-human-rights-defenders-hacked-with-nso-groups-pegasus-spyware-2/

Ulusal Af Örgütü Birleşik Krallık. (2021). *Pegasus Project: Macron Among World Leaders Selected As Potential Targets of NSO Spyware*". https://www.amnesty.org.uk/press-releases/pegasus-project-macron-among-world-leaders-selected-potential-targets-nso-spyware

Walker, S., Kirchgaessner, S., Lakhani, N., Safi, M. (2021, 19 Temmuz). Pegasus Project: Spyware Leak Suggests Lawyers and Activists at Risk Across Globe. *The Guardian*. Erişim Tarihi: 9 Eylül 2023, https://www.theguardian.com/news/2021/jul/19/spyware-leak-suggests-lawyers-and-activists-at-risk-across-globe

Wassenaar Düzenlemesi. (2023a). *About Us*, https://www.wassenaar.org/about-us/#faq

Wassenaar Düzenlemesi. (2023b). *Overview*. https://www.wassenaar.org/about-us/#faq

Yablonko, Y. (2019, 14 Şubat). Novalpina Capital and Founders Buy NSO At $1b Co Value. *Globes*. Erişim Tarihi: 1 Eylül 2023, https://en.globes.co.il/en/article-novalpina-capital-and-founders-buy-nso-for-1b-1001273312

Yaron, O. (2020, 30 Kasım). The Secret of NSO's Success in Mexico. *Haaretz*. Erişim Tarihi: 30 Ağustos 2023, https://www.haaretz.com/israel-news/tech-news/2020-11-30/ty-article/.highlight/the-secret-of-nsos-success-in-mexico/0000017f-e0f5-d568-ad7f-f3ff5cff0000

Ziv, A. (2021, 20 Temmuz). The Pegasus Project | Where Netanyahu Went, NSO Followed: How Israel Pushed Cyberweapon Sales. *Haaretz*. Erişim Tarihi: 12 Eylül 2023, https://www.haaretz.com/israel-news/tech-news/2021-07-20/ty-article/.highlight/where-bibi-went-nso-followed-how-israel-pushed-cyberweapons-sales/0000017f-e388-d7b2-a77f-e38fd45a0000

İstihbarat Çalışmaları ve Araştırmaları Dergisi-İÇAD, 2024, 3(2) : 212-242 Araştırma Makalesi
Journal of Intelligence Research and Studies-İÇAD, 2024, 3(2) : 212-242 Research Article
DOI: 10.61314/icad.1491465

STRATEJİK İSTİHBARAT VE ÖRTÜLÜ OPERASYONLARIN DIŞ POLİTİKADA ÖNEMİ: İRAN'IN BALKANLAR POLİTİKASI (BOSNA HERSEK VE ARNAVUTLUK ÖRNEĞİ)

İbrahim RASULOV[*], Murat JANE[**]

ÖZET

Devletler, herhangi bir istihbari faaliyete veya örtülü/açık operasyona geçmeden önce kendilerine bir yol çizmek için hedef ülke ile ilgili bazı bilgiler edinmek zorundadırlar. Bu bilgiler, devletler tarafından stratejik istihbaratın ortaya koyduğu başlıklar altında toplanır. Stratejik istihbarat kapsamında toplanmış bilgiler geniş çevrede değerlaendirilir. Uzun dönemleri kapsayan planlar stratejik istihbaratın özelliklerinden biridir. Devletler, bazen çıkarları için hedef aldıkları devletlerde farklı faaliyetlerde bulunurlar. Bazen bu faaliyetler göz önünde, bazense gizli olarak, niyetlerini belirtmeden gerçekleştirirler. Böyle gizli faaliyetler literatürde örtülü operasyonlar olarak tanımlanmaktadır. Buradan anlaşıldığı üzere stratejik istihbarat, örtülü operasyonların yapılması için hazırlık aşaması olarak da kabul edilebilir. Bu çalışmada, İran'ın Balkanlar'da uygulamış olduğu politika, Bosna Hersek ve Arnavutluk üzerinden stratejik istihbaratın uzun vadeli planlaması ve örtülü operasyonlar kapsamında değerlendirilmektedir. İran, Balkanlar'da politikalarını gerçekleştirebilmenin öncelikli koşulunun din faktörü olduğunu belirlemiştir. Ayrıca, İran bu ülkelerde politik faaliyetleri sürdürebilmek için ideolojik motif faktörünü devamlı olarak kullanmaktadır. İran, istihbari yöntem olarak, yumuşak güç kullanmayı ve bununla halkın dikkatini çekilmeyi benimsemektedir. İran, bölgeye gönderdiği din adamları aracılığıyla Şii ideolojiyi yaymakta, açtığı ilm merkezleri vasıtasıyla ise, bölgedeki ilm adamları ile bağlantılar kurarak kültürel ve ilmi projeler yürütmek istemektedir. Bu çalışmada İranın yumuşak ve bazen sert güç unsurlarını (stratejik istihbarat ve örtülü operasyonlar kapsamında) kullanarak, bölgede politik ağırlık inşa etmeyi amaç edindiği belirtilmektedir.

Anahtar Kelimeler: *Dış Politika, Stratejik İstihbarat, Örtülü Operasyonlar, İran, Balkanlar*

THE IMPORTANCE OF STRATEGIC INTELLIGENCE AND COVERT OPERATIONS IN FOREIGN POLICY: IRAN'S POLICY IN THE BALKANS (THE EXAMPLE OF BOSNIA AND HERZEGOVINA AND ALBANIA)

ABSTRACT

Before embarking on any intelligence activity or covert/overt operation, states need to obtain some information about the target country in order to draw a path for themselves. This information is collected by states under the headings of strategic intelligence. Information

[*] Yüksek Lisans Öğrencisi, İstanbul Aydın Üniversitesi, Uluslararası İlişkiler ve Terörizm Araştırmaları Bölümü, ibrahimrasulov@stu.aydin.edu.tr, ORCID: 0009-0007-2357-6378
[**] Dr. Öğr. Üyesi, İstanbul Aydın Üniversitesi Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, muratjane@aydin.edu.tr, 0000-0002-2409-131X

Makale Başvuru Tarihi / Application Date: 28 Mayıs 2024 / 28 May 2024

Makale Kabul Tarihi / Acceptance Date: 09 Haziran 2024 / 09 June 2024

gathered within the scope of strategic intelligence is evaluated in a wide environment. Long-term plans are one of the characteristics of strategic intelligence. States sometimes engage in different operations in the states they target for their interests. Sometimes these operations are carried out openly, sometimes covertly, without stating their intentions. Such covert operations are defined as covert actions in the literature. As understood from this point, strategic intelligence can also be considered as the preparatory stage for covert operations. In this study, Iran's policy in the Balkans is evaluated through Bosnia and Herzegovina and Albania in the context of long-term strategic intelligence planning and covert operations. Iran has determined that the primary condition for realizing its policies in the Balkans is the religious factor. Moreover, Iran constantly uses the factor of ideological motives to sustain its political activities in these countries. As an intelligence method, Iran adopts the use of soft power to attract the attention of the public. Iran spreads Shiite ideology through the clerics it sends to the region, and through the scientific centers it opens, it wants to carry out cultural and scientific projects by establishing connections with the scholars in the region. This study argues that Iran aims to build political weight in the region by using soft and sometimes hard power elements (within the scope of strategic intelligence and covert operations).

Key Words: *Foreign Policy, Strategic Intelligence, Covert Actions, Iran, Balkans*

GİRİŞ

"Stratejik İstihbarat ve Örtülü Operasyonların Dış Politikada Önemi: İran'ın Balkanlar Politikası" başlıklı bu araştırma, dış politika açısından kritik bir unsuru ele alarak, stratejik istihbaratın ve örtülü operasyonların önemini vurgulamayı amaçlamaktadır. Balkanlar, jeopolitik önemi ve stratejik konumu nedeniyle küresel güç mücadelesinin yoğunlaştığı bir bölgedir. İran, bu bölgede stratejik istihbarat ve örtülü operasyonlar kullanarak etkisini artırmayı ve bölgedeki Batılı nüfuzu dengelemeyi hedeflemektedir. İran'ın bölgesel ve küresel düzeyde jeopolitik konumu, enerji kaynakları, askeri ve nükleer programı, bölgesel etkisi, uluslararası ilişkileri, kültürel ve tarihi bakımdan bir öneme sahip olması nedeniyle bu çalışma, stratejik istihbaratın dış politika oluşturmada kilit rolünü anlamamıza yardımcı olacaktır. Bu makale, İran'ın Balkanlar'daki nüfuz stratejilerini ve bu stratejilerin ardındaki istihbarat faaliyetlerini kapsamlı bir şekilde ele alarak, bölgedeki siyasi, ekonomik ve kültürel dinamiklere dair detaylı analizler sunmaktadır. İran'ın bölgesel hedeflerine ulaşmak için kullandığı örtülü operasyonlar ve istihbarat yöntemleri, bu makalede titizlikle incelenmekte ve İran'ın Balkanlar'daki etkisinin ne derece derin ve geniş kapsamlı olduğunu ortaya koymaktadır. Mevcut literatürde, İran'ın Balkanlar'daki faaliyetleri hususunda çalışmalar bulunsa da bu çalışmaların istihbarat boyutu oldukça zayıftır. Bu çalışma, literatüre, İran'ın

Balkanlar'daki dış politika stratejilerini ve araçlarını daha derinlemesine analiz ederek, bölgedeki jeopolitik dinamiklere ve İran'ın bölgesel stratejilerine dair yeni bir bakış açısı kazandırmaktadır.

Bu araştırma, stratejik istihbaratın ve örtülü operasyonların dış politika belirlemedeki etkisini, İran'ın özelinde analiz ederek, bölgesel güvenlik dinamiklerini anlamamıza katkı sağlamayı hedeflemektedir. İran'ın bölgedeki politik, askeri ve ekonomik etkisi, bu ülkenin stratejik önemini artırmaktadır. Dolayısıyla, İran'ın Balkanlar politikası örneği üzerinden stratejik istihbaratın ve örtülü operasyonların dış politika oluşturmada rolünün derinlemesine anlaşılması, uluslararası ilişkilerde daha geniş bir bağlamı anlamamıza ve stratejik öngörülerde bulunmamıza yardımcı olacaktır.

İran İslam Cumhuriyeti, 1979 İslam Devrimi sonrasında kendi kimliğini öncelikle dini değerler üzerinden tanımlamıştır. Bu durum, İran'ın çıkarlarını ve tehdit algılayışını belirlemiştir. Tahran, Şii yayılmacılığı olarak adlandırılan bir stratejiyi benimsemiş, bu çerçevede Şii grupları desteklemekte ve diğer inanç gruplarından olanları Şiileştirmeye çalışmaktadır. İran, Balkanlar politikasında etkin bir kamu diplomasisi kullanarak bölgedeki sufiler üzerinden nüfuz sağlamaya çalışmaktadır. Ayrıca Tahran, bu hedeflere ulaşmak için zaman zaman stratejik ve örtülü istihbarat operasyonları gibi sert güç unsurlarını da kullanabilmektedir. İran'ın Balkanlar politikası, ülkeden ülkeye farklılık göstererek Müslüman nüfusun yoğunluğuna bağlı olarak şekillenmektedir.

Bu çalışmada, İran'ın Balkanlara neden önem verdiği ve hangi kazanımlar elde etdiği, nasıl politika izlediği, araştırma soruları sorulmaktadır. Bu araştırmada ana hipotez olarak, "İran dış politikasının oluşturulmasında stratejik istihbarat ve örtülü operasyonlar kritik önem taşımaktadır" fikri ortaya konulmuştur. Amaç ise, stratejik istihbarat ve örtülü istihbarat operasyonları ele alınarak, İstihbarat kapsamında İran İslam Cumhuriyeti'nin Balkanlar'da faaliyetlerinin araştırılmasıdır.

1. YÖNTEM

Literatür Taraması: Araştırmanın ilk adımı olarak, stratejik istihbarat, örtülü operasyonlar ve İran'ın dış politikası konularında mevcut literatür taranmıştır. Bu sayede, konuya ilişkin teorik çerçeve oluşturulmuş ve mevcut bilgi birikimi değerlendirilmiştir.

Vaka Analizi: İran'ın Balkanlar'da uyguladığı politikaların analizi için vaka çalışması yöntemi kullanılmıştır. Bu kapsamda, İran'ın Bosna-Hersek, Sırbistan, Arnavutluk gibi ülkelerdeki faaliyetleri incelenmiştir. Bu faaliyetlerin nasıl organize edildiği, hangi stratejik amaçlara hizmet ettiği ve sonuçları detaylı bir şekilde ele alınmıştır.

Stratejik İstihbarat Analizi: İran'ın Balkanlar'da yürüttüğü istihbarat faaliyetleri, stratejik istihbarat çerçevesinde analiz edilmiştir. Bu analiz, İran'ın bölgedeki istihbarat toplama yöntemleri, kullandığı araçlar ve uyguladığı stratejilerin değerlendirilmesini içermektedir.

Örtülü Operasyonların İncelenmesi: Çalışmada, İran'ın örtülü operasyonları detaylı bir şekilde ele alınmıştır. Bu kapsamda, İran'ın bölgedeki dini ve ideolojik faaliyetleri, yerel halk üzerindeki etkileri ve bu operasyonların dış politika üzerindeki yansımaları incelenmiştir.

İdeolojik ve Kültürel Bağlantılar: İran'ın Balkanlar'da kurduğu ideolojik ve kültürel bağlar da çalışmanın önemli bir parçasını oluşturmaktadır. İran'ın Şii ideolojisini yayma çabaları, dini liderler aracılığıyla yürüttüğü faaliyetler ve açtığı ilm merkezleri üzerinden gerçekleştirdiği projeler analiz edilmiştir.

Bu yöntemler sayesinde, İran'ın Balkanlar'da stratejik istihbarat ve örtülü operasyonlar kapsamında yürüttüğü faaliyetlerin dış politika üzerindeki etkileri kapsamlı bir şekilde ortaya konulmuştur

2. STRATEJİK İSTİHBARAT ve ÖRTÜLÜ OPERASYON KAVRAMI

Bu çalışmada stratejik istihbarat kavramına geçmeden önce istihbaratın ne olduğunun açıklanması gerekmektedir. Türk Dil Kurumu'na göre güncel haliyle istihbarat "yeni öğrenilen bilgiler, haberler, duyumlar" ve "bilgi toplama, haber alma" şeklinde tanımlanmıştır (TDK, 2023). İstihbarat kelimesi Türk diline Arapçadan gelme olup "istihbar", "haber" ve "bilgi alma" kelimesinin çoğuludur. Türk kültüründe "bilginin toplanması" yeterli görüldüğü için "istihbarat" bu faaliyeti tanımlamaya yeterli gelmektedir. Oysa istihbarat kelimesinin İngilizcede karşılığı olan "*intelligence*" ise akıl, zekâ, anlayış anlamına gelmektedir. Bu kültürde "bilginin değerlendirmesine" ağırlık verildiği için "*intelligence*" sözcüğü kullanılmaktadır. Bu iki yaklaşımı basit bir etimolojik farklılık olarak görmek mümkün değildir (Özdağ, 2017, s.29).

İstihbarat, ulaşılabilen bütün açık, yarı açık ve/veya gizli kaynaklardan her türlü aracın kullanılması sonucunda elde edilen her türlü veri, malûmat ve bilginin ulusal genel veya ulusal özel planda politikaların gerçekleştirilmesi ve ulusal politikalara zarar verilmesinin engellenmesi amacı ile toplandıktan sonra önemine ve doğruluğuna göre sınıflandırılması, karşılaştırılması, analiz edilerek değerlendirilmesi süreci sonucunda ulaşılan bilgidir (Özdağ, 2017, s.31). Milli İstihbarat Teşkilatı'nın tanımlamasına göre stratejik istihbarat, ülkeler ve diğer unsurlarda hareketlerin tamamını takip ve analiz ederek öngörüsü yüksek sonuçlar ele alınan bilgileri karar alıcılara sunma süreçlerini içeren bir faaliyettir (MİT, t.y). İstihbaratın içeriğinin açılması gerekirse, bir milletin karşı karşıya olduğu fırsat ve tehlikeleri önceden görebilmesi için stratejik, operasyonel ve taktik düzeyde olaylarla, gelişmelerle, kişiliklerle, kurumlarla ilgili olarak bilgi toplama karşılaştırma, değerlendirme, analiz, birleştirme ve yorumlama faaliyeti şeklinde ifade edilebilir

Stratejik istihbarat, bir devlet için gelecekte ortaya çıkabilecek fırsatları, tehditleri araştırıp tespit ederek ve öngörerek, karar alıcıların önüne olabilecekler ile ilgili seçenekler koyarak onların siyaset üretme sürecini daha doğru bir zemine çekmek amacı ile yapılan istihbarat türüdür. Hasım devletin milli gücünü ortaya çıkarmaya, kuvvetli ve zayıf taraflarını tespit etmeye yöneliktir. Bir devletin milli gücü insan gücü, coğrafi güç, psiko-sosyal güç, teknolojik güç, politik ve idari güç, ekonomik güç, askeri güç olarak tanımlanmaktadır (Koca, 2019, s.2190). Bu bağlamda stratejik istihbarat çalışmaları coğrafi, ulaşım ve iletişim, sosyal, politik, ekonomik, bilimsel ve teknolojik, askeri ve biografik istihbarat konularında ele alınmaktadır (Gül, 2014, ss.86-87). Aşağıda stratejik istihbarat çalışmalarının hepsi ayrı ayrı incelenmektedir.

Coğrafi İstihbarat**,** Bir ülkenin coğrafyası, yani dünyanın hangi bölgesine ve nasıl yerleşmiş olduğu, büyüklüğü, topoğrafya ve bitki örtüsü ülkenin kaderini belirleyen temel unsurlardan biridir. (Seren, 2023, s.291). Bir ülke için coğrafi istihbarat coğrafi mevki (dünya üzerindeki yeri, yüzölçümü, hudutları ve özellikleri, ülkenin fiziki şekli vb.), arazi şekilleri (topografik, yükseklik ve drenaj, harekât için uygun bölgeler), iklim ve hava şartları (iklim faktörleri, meteorolojik ölçümler vb.), başlıca nehir ve göller (nehirler, göller, denizler, plajlar, iç suyolları vb.), bitki örtüsü (kategorisi, sahaları, engelleme durumu, elverişlilik derecesi, tesirleri vb.), ovalar ve

dağlar (ovalar, platolar, dağ silsileleri), coğrafyanın askeri harekâta olumlu/olumsuz etkileri başlıkları altında değerlendirilir (Koca, 2019, s.2193). Coğrafya, orada yaşayan millet için fırsatlar yaratabileceği gibi en büyük talihsizliklere de neden olabilir.

Ulaştırma ve Muhabere İstihbaratı**,** Ulaştırma ve muhabere istihbaratı bir ülkenin lojistik sistemlerinin imkân ve kabiliyetleri ile haberleşme ağı altyapısının askeri harekâta etkilerini inceler. Demiryolu ağının coğrafi güzergâhı, uzunluğu ve etkinliği ulusal ekonomi ve askeri potansiyelin önemli bir ölçüsüdür. Demiryolu yolcu ve yük taşıma kapasitesi (hat sayısı, vagon ve lokomotif sayısı ve eski/yeni durumu, bakım faaliyetleri ve kapasitesi, demiryolu ağının kalitesi vb.) barışta, gerginlik ve savaş döneminde personel ve malzeme intikali potansiyelinin tahmin edilmesinde önemli bir yer tutar (Seren, 2023, ss.296-298). Demiryollarının birleşim yerleri (düğümler), tüneller ve istasyonlar sistemin hassas noktalarıdır. Bir ülke için ulaştırma ve muhabere istihbaratı; genel ulaştırma sistemi ve politikası, demiryolu ulaştırması, karayolu ulaştırması, iç suyolu ulaştırması, denizyolu ulaştırması, petrol ve doğal gaz boru hatları, havayolu ulaştırması, muhabere/haberleşme, ulaştırma ve muhaberenin askeri harekâta etkileri başlıkları altında değerlendirilir. Bu istihbarat türü, düşmanın planlarını, niyetlerini ve faaliyetlerini belirleme amacıyla askeri strateji ve operasyonlarda önemli bir rol oynar. Ayrıca, düşmanın savunma sistemleri, askeri hareketleri ve lojistik yapıları hakkında bilgi sağlamak için de kullanılır.

Sosyal İstihbarat, Toplumlar, aralarında duygu, düşünce, davranış biçimi, ırk, din, dil ve menfaat gibi hususlarda benzerlik ve beraberlik bulunan insanların bir araya gelmesiyle oluşur. Toplumlar gelenek ve göreneklerinden anayasaya kadar uzanan hukuk kurallarına birlikte uyar ve onlara göre organize olursa millet olma aşamasına erişirler. Devletin gerçek gücü her şeyden önce vatandaşlarının bir toplum olarak bütünleşmeleri ve bir millet olarak organize olabilmelerinin etkinliğine bağlıdır. Bu bağların kuvvetli ve zayıf taraflarını bulmak, bu zayıflıklar üzerine gidecek şekilde planlamalar yapmak başarıyı getirecektir (Özdağ, 2017: 97-98). Ulusun sayısı, türdeşliği, eğitim yapısı, yaş dağılımı ulusal nüfusun değerini stratejik faktör olarak belirleyen özelliklerdir. Nüfusun büyüklüğü tek başına belirleyici değildir. Bazı uluslar karşılaştırıldığında nitelik/nicelik kavramları farklı sonuçlar verir. Ülkelerin yerleşim merkezleri ve büyüme oranları,

nüfus artışı, nüfus politikası, yaş ve cinsiyet dağılımı, iş gücü kalitesi, köylerden kentlere göç vb. refah seviyesine ilişkin bilgi verecektir. Nüfusun demografik yapısı, azınlıklar, azınlık politikaları, azınlık politikasına bağlı göç durumları toplumsal barışın seviyesini ve toplumun hassasiyetlerini ortaya koyacaktır. Kültürel yapı ve ilişkiler, eğitim ve öğretim kalitesi, basın-yayın takip edilirliği, basının toplum üzerindeki kamuoyu oluşturma etkisi, genel kamuoyu eğilimleri, çevre sorunları psikolojik harekât açısından önemli bilgiler verecektir (Seren, 2023, s.285). Bu kapsamda bir ülkenin sosyal istihbaratı nüfus ve nüfus hareketleri, azınlıklar, halkın sosyal durumu, din, eğitim ve öğretim, kamuoyu, basın-yayın, kültürel yapı ve kültürel ilişkiler, sağlık ve sosyal hizmetler, çevre sorunları, iş gücü, başlıkları altında değerlendirilir.

Siyasi İstihbarat**,** Siyasi istihbarat, diplomatik personel (büyükelçi, askeri ataşe, konsolos, büyükelçilik/konsolosluk çalışanı) veya saha elemanı tarafından açık veya kapalı espiyonaj faaliyetleri, teknik istihbarat vasıtaları, resmi beyanatlar, basın, kamuoyu, iş adamları, akademik çalışmalardan elde edilir. Siyasi güç, en basit tanımıyla, bir devletin milli hedeflerine erişmek, erişilenleri koruyup geliştirmek ve milli menfaatleri sağlamak amacıyla kullandığı siyasi kuvvetlerin toplam verimidir (Girgin, 2003, ss.68-72). Siyasi güç, genel olarak bir devletin iç politikasının bünyesine, milletin özelliklerine ve çağın isteklerine uygunluğu; diplomatik faaliyet ve ilişkilerini, üyesi bulunduğu uluslararası antlaşma, ittifak ve kuruluşları ve bunlar içindeki mevkiini, diplomatik alanda hareket serbestisini, uluslararası itibarını, devlet teşkilat yapısı ve devlet kurumlarını, devlet yönetim biçimi ve etkinliğini, politik liderliği, her aşamada kanunların ve/veya hukuki mevzuatın yeterlilik ve etkinliğini kapsar. Siyasi istihbarat bir ülkenin siyasi gücünü mercek altına alarak tarihçe, devletin kuruluşu, yasama organları, yürütme organları, yargı sistemi, idari teşkilat, seçim sistemi, siyasi partiler ve genel eğilim, istihbarat teşkilatı, milli politika, bağlı olduğu askeri paktlarla münasebetleri, ülkenin genel politik hedefleri, ikili ilişkiler başlıkları altında değerlendirir (Özdağ, 2017, ss.66-67). Genel olarak siyasi istihbarat, devletlerin, uluslararası örgütlerin veya diğer politik grupların siyasi faaliyetleri, karar alma süreçleri, niyetleri ve politik durumları hakkında bilgi toplama ve analiz etme sürecidir. Siyasi istihbarat, genellikle devletlerin iç politikalarını ve dış ilişkilerini anlama, politik stratejiler geliştirme, güvenlik değerlendirmeleri yapma ve ulusal çıkarları koruma amacıyla kullanılır.

Ekonomik İstihbarat**,** Bir ülkenin tehdit değerlendirmesinde ekonomik gücünün askeri harekâtı destekleme durumu son derece önemlidir. Hasım ülkelerin ekonomisi değerlendirilirken neyi ürettiği, üretebileceği, dışa bağımlılığı ve yetersizliklerinin bilinmesi gereklidir (Güldiken, 2006, ss.172-175). Bir ülkenin ekonomik istihbaratı devletin ekonomik durumu ve politikası, ekonomik hedefler, son ekonomik durum ve muhtemel geleceği, tarım, sanayi, enerji, ticaret, madencilik, turizm, ekonomik sorunlar, bütçe, ülke ekonomisinin kuvvetli ve zayıf tarafları başlıkları altında değerlendirilir (Özdağ, 2017, s.93). Bu tür istihbarat, devletlerin ve örgütlerin ekonomik çıkarlarını korumak, ekonomik politikalarını belirlemek, ticaret ilişkilerini yönetmek ve gelecekteki ekonomik gelişmelere yönelik stratejiler oluşturmak için kullanılır. Ekonomik istihbarat, açık kaynaklardan (örneğin, ekonomik raporlar, ticaret anlaşmaları, finansal raporlar), gizli kaynaklardan (örneğin, casusluk faaliyetleri, bilgi sızıntıları) ve teknik istihbarattan (örneğin, finansal verilerin analizi, ticaret ağlarının izlenmesi) elde edilen bilgileri içerebilir. Bu bilgiler, ekonomik politika yapıcılarına, ticaret müzakerelerine katılanlara ve diğer ilgili aktörlere stratejik avantaj sağlama amacıyla kullanılır.

İlmi ve Teknolojik İstihbarat**,** Bir ülkenin bilimsel ve teknik olanağı, bilimsel eğitimin kalite ve yaygınlığına, AR-GE finansmanına ve bilim insanlarının niteliklerine bağlıdır. Konuya askeri açıdan bakıldığında, hasım ülkenin elindeki mevcut teknolojik seviyenin, AR-GE faaliyetleri ile ulaşmak istediği teknolojik seviye veya ikili ilişkiler sonucu yapacağı teknoloji transferlerinin savunma sanayisine yansımaları, silah sistemlerinde elde edilecek yeni imkân ve kabiliyetler ilmi ve teknolojik istihbaratın önemini ortaya koymaktadır. Bir ülkenin ilmi ve teknolojik istihbaratı ilmi ve teknolojik temel yapısı, teknolojik gelişmeler ve yatırımlar, teknoloji transfer durumu, teknolojik gelişmelerin askeri neticeleri, başlıkları altında değerlendirilir (Seren, 2023 ss.299-301). Bu tür istihbarat, bilimsel gelişmeler, teknolojik yenilikler, savunma sanayii çalışmaları ve benzeri konulara odaklanarak stratejik avantaj sağlamak amacıyla kullanılır. Genellikle açık kaynaklardan (bilimsel makaleler, patentler, teknik raporlar), gizli kaynaklardan (casusluk faaliyetleri, içeriden bilgi sızdırma) ve teknik istihbarattan (siber güvenlik analizleri, teknik verilerin değerlendirilmesi) elde edilen bilgileri içerir. İlmi ve teknolojik istihbarat, ülkelerin rekabet avantajlarını sürdürmelerine, savunma yeteneklerini güçlendirmelerine ve ekonomik kalkınmalarını desteklemelerine yardımcı olabilir.

Silahlı Kuvvetler İstihbaratı**,** Bir devletin askeri gücü, politikasını uygularken gerektiğinde kullanabileceği güçtür. En önemli nokta bir ülkenin politik amaçlarına ulaşmak için askeri güç kullanma arzu istekliliği konusundaki temayülüdür. Bir ülke için genel askeri istihbarat silahlı kuvvetler, kara kuvvetleri, deniz kuvvetleri, hava kuvvetleri, jandarma kuvvetleri, yarı askeri kuvvetler başlıkları altında değerlendirilir (Özdağ, 2017, s.81). Silahlı Kuvvetler İstihbaratı, genellikle çok gizli ve özel bir karaktere sahiptir. Bu tür istihbarat faaliyetleri, devletin güvenliği ve savunması açısından kritik öneme sahiptir. Silahlı Kuvvetler İstihbaratı, genellikle askeri operasyonların planlanması, stratejik kararlar alınması ve güvenlik tehditlerine karşı önlem alınması gibi amaçlar doğrultusunda çalışır.

Biyografik İstihbarat**,** üst düzey yöneticiler ve komutanlar ile potansiyel öneme sahip şahsiyetler üzerine yoğunlaşır. Biyografik istihbarat adı, soyadı, eşkâli (fiziki özellikleri), unvanı/rütbesi, baba adı/anne adı, doğum yeri ve tarihi, medeni hali, çocukları, eğitim, bildiği diller, en son göreve başlama tarihi, sırasıyla ifa ettiği görevler, siyasi eğilimi (askeri, sosyal, ekonomik ve diğer konulardaki fikirleri), idarecilik/liderlik/komutanlık vasfı, aile hayatı, sağlık durumu, karakteri gibi başlıklarda toplanır (McDowell, 2008). Ayrıca bu tür istihbarat, genellikle güvenlik, istihbarat, kolluk kuvvetleri veya istihdam süreçlerinde kullanılır. Biyografik istihbarat, bir kişinin güvenlik riski olup olmadığını değerlendirmek, suçları ortaya çıkarmak, terörle mücadele etmek veya belirli pozisyonlara uygunluğu değerlendirmek gibi amaçlar için kullanılabilir.

Örtülü operasyon faaliyetleri, istihbaratın sadece karşı tarafın niyet ve kapasitelerini değil, aynı zamanda karşı tarafın eylemlerinin yönünü belirlemeye odaklanan, daha ileri düzeyde bir istihbarat çabasını ifade eder. Bu tür çalışmalar, psikolojik savaşın bir parçası olarak kabul edilebilir. Gizli müdahale faaliyetleri öyle planlanır ve icra edilir ki, destekleyen taraf gerektiğinde inandırıcı bir şekilde reddedebilir (Özdağ, 2017, s. 274). Eski CIA direktörü olan Stransfield Turner, örtülü operasyonları, hedef ülkedeki gelişmelerin seyrini rolümüz açığa çıkmadan kendi ülkemizin çıkarıarına göre etkilemek için gösterdiğimiz çaba olarak tanımlamıştır. Buna ek olarak örtülü operasyonlarda, arkasında istihbarat servisinin olduğunu belli etmeden propaganda faaliyetleri, politik eylemler ve gizli paramiliter destekler gibi görevlerin olduğunu belirtmiştir (Ataç, 2019, ss.6-8). Bazı İstihbarat

literatüründe örtülü operasyonların tatbik edilen bir politika olduğu savunulmaktadır. Bu tür faaliyetler İngiliz istihbarat literatüründe, "özel politik operasyonlar", Rus istihbarat literatüründe ise, "etkin önlem" olarak adlandırılmaktadır. Örtülü operasyonlar hedef ülkede kültürel faaliyetlerden ülke içinde düzenlenen sabotaj ve suikastlere kadar geniş bir alanı kapsamaktadır (Özdağ, 2017, s. 274). Örtülü operasyonlar, askeri ve politik seçeneklerden sonra gelen üçüncü bir seçenektir. Bu yöntem hedef veya rakip ülke ile ilan edilmemiş bir savaşı kapsayan örtülü ve gizli bir yöntemdir. Böylece doğrudan bir savaşa girmeksizin ve ulusal gücü topyekûn bir mücadeleye sokmadan asimetrik hale getirilmiş bir savaş ile sonuç almak söz konusudur (Kaynak, 2009, Karaağaç, 2021, s.84). Örtülü operasyonlar genellikle 4 temel tipten oluşmaktadır: politik operasyonlar, propaganda ve yanlı bilgilendirme, ekonomik savaş, yarı askeri operasyonlar (Seren ve Yıldız, 2023). İstihbarat örgütlerinin ve işbirliği yapılan kurumların örtülü operasyon gücü ülke politikalarının uygulanmasında politikacılara hareket kabiliyeti sağlar. Örtülü operasyonlar, dış politika ve ulusal güvenlik hedeflerinin gerçekleştirilmesinde istihbarat sisteminin entegre bir parçasıdır.

3. STRATEJİK İSTİHBARAT VE ÖRTÜLÜ OPERASYONLARIN DIŞ POLİTİKADA KULLANILMASI

İstihbaratın evrim süreci, istihbaratın ve örtülü operasyonların, dış politika ile ilişkisini anlamak için önemli bir bağlam sunar. İnsanlık tarihinde, istihbarat çalışmalarının uzun bir geçmişi vardır. Ancak, bu çalışmaların dış politika oluşturulmasında etkili bir rol oynaması, 17. yüzyıldan itibaren kademeli olarak artmıştır. Ulus devletlerin oluşumundan İkinci Dünya Savaşı'na kadar olan dönemde, istihbarat çalışmaları genellikle askeri istihbarat alanında ve savaş zamanlarında gerçekleştirildiği için dış politika üzerinde sınırlı bir etki bırakmıştır(Özgüven, 2011 s.36-38). Bu süreçte gerçekleştirilen istihbarat çalışmaları genellikle taktiksel istihbarat olarak nitelendirilmiştir.

3.1 Stratejik İstihbarat ve Dış Politika

Sherman Kent, 1940'lı yıllarda stratejik istihbarat terimini tanımlayarak ve bu alanda yeni bir disiplin oluşturarak önemli bir kavram ortaya koymuştur. Bu nedenle, 1940'lı yıllardan önce gerçekleştirilen istihbarat çalışmalarının genellikle güvenlik politikaları alanında etkileri

vardır. Stratejik istihbarat kavramının ortaya çıkmasından günümüze kadar geçen süreçte ise istihbarat çalışmalarının dış politika oluşturulmasında kullanımı artmıştır (Beşe ve Seren, 2011, ss.127-129).

Stratejik istihbarat, devletler için hayati öneme sahip bir faaliyet olmaktadır. Bu durum, istihbarat çalışmalarının devletlerin oluşumundan önceki dönemlere dayanmasının nedenini açıklamaktadır. İstihbaratın etkin bir şekilde kullanılması, egemen güçlerin toprak ve nüfus kontrolü için mücadele etmeye karar verdikleri tarihlerle doğrudan ilişkilidir (Treverton ve Jones, 2006, ss.2-3). Ulus-devletleşme sürecinden sonra, Stratejik istihbarat devletlerin güvenlik ve dış politika oluşturma süreçlerinde, yani uluslararası sistemdeki pozisyonlarını belirleme ve davranışlarını yönlendirme süreçlerinde kritik bir rol oynamaktadır. İstihbarat, olası bir çatışma öncesinde devletlere pozisyonlarını belirleme, fırsatları ve müdahale noktalarını önceden tespit etme fırsatı tanır. Bu nedenle, istihbarat devletlere, daha avantajlı bir pozisyon elde etme, ülke sınırları ve vatandaşlarının güvenliğini artırma, kaynakları etkili bir şekilde kullanma ve çıkarlarını artırma imkanı sağlar (Treverton ve Jones, 2006, s.8).

Bir hükümet işlevi olarak istihbarat süreci ve ürünü normalde gizlilikle örtülüdür. Entelektüel bir girişim olarak stratejik dış istihbaratın misyonu geçmiş olayları anlamayı, mevcut koşulları doğru yorumlamayı ve geleceği tahmin etmeyi içerir. Bu tür entelektüel çabaların ürünü ya da sonucu dış politika kararlarının alınmasında etkili bir faktör olabilir. İstihbarat tekniklerinin, analistlerin ihtiyaç duyduğu gizli verileri toplamak amacıyla casusluktan yabancı seçimlere müdahaleye, aldatma ve sabotaj yoluyla siyasi suikast ve paramiliter girişimlere kadar uzanan geniş ve farklı dış politika işlevleri için savaşta ve barışta kullanılmış olması konunun karmaşıklığını arttırmaktadır (Ransom, 1974, ss. 138-143). İstihbaratın çok boyutlu olması, görünmeyen nedenleri anlama ve politika yapıcılara yön verme yeteneği açısından önemlidir. İstihbarat, problem çözmeye yönelik, ortaklık ve gelişmeye açık bir model oluşturmalıdır. Ayrıca, politik karar alıcıların belirsizlikle başa çıkabilmelerini sağlar ve devletlerin sürprizlere karşı önlem almasına yardımcı olmayı amaçlar. Uluslararası arenada aktörler, etkilerini artırmak için diğer devletlerin siyasi sistemlerini ve sosyokültürel yapılarını anlamalı ve stratejilerini buna göre geliştirmelidir. Bu bilgiler, istihbarat çalışmaları aracılığıyla elde edilir ve devletler dış politika oluştururken kullanılır.

Stratejik istihbaratın dış politikada kullanılmasına yönelik akademik çalışmalar ve tartışmaların olması bu süreç içerisinde farklı ekollerin oluşması ile sonuçlanmıştır (Ateş, 2013, ss.22-23). Bu çalışmalardan akademik çevrelerce en çok kabul gören, Sherman kent ekolü olarak bilinen, Sherman Kent'in öncülüğünü yaptığı Geleneksel Amerikan Misyonu ve ortaya konulan "stratejik istihbarat" kavramıdır. Bu aynı zamanda Kent'e bu sebeple istihbarat biliminin kurucusu da denmektedir.

Sherman Kent, "Stratejik İstihbarat" adlı eserinde dış politika oluşturulmasında kullanılan istihbaratı "Üst Düzey Yapıcı Dış İstihbarat" olarak tanımlamış ve bu segmentin istihbaratın en kritik bileşeni olduğunu öne sürmüştür. Pozitif dış istihbarat, iç politika oluşturma konusuna odaklanmaz ve yürütülen çalışmaların temel amacı uluslararası sistemdeki diğer devletlerdir. Kent'e göre devletler, Ulusal Politika ve Ulusal Güvenlik Politikası olmak üzere iki tür politika oluşturmalıdır. Bu politikaların başarıyla uygulanabilmesi için ise istihbarat çalışmalarının desteklenmesi gerekmektedir (Kent, 2002, s.12). Kent'e göre stratejik istihbarat, sistemin diğer devletlerinin mevcut dinamikleri, potansiyeli ve gelecekteki niyet ve davranışlarının analizi ile elde edilen bilgi üzerine inşa edilir. Devletlerin uluslararası sistemdeki dış politika tercihlerini belirleme sürecinde stratejik istihbarata dayalı olarak hareket etmeleri gerektiğini savunmaktadır. Kent'e göre stratejik istihbaratın iki temel kullanımı bulunmaktadır: ilk olarak, diğer devletlerin yıkıcı ve ya negativ faaliyetlerini engellemek, ikincisi, devletin çıkarlarını ve stratejilerinin oluşumunda ve maksimize etmekte katkıda bulunmaktır. Kent'e göre istihbaratın politika oluşturma sürecindeki başlıca görevleri şunlardır: Politika belirlenmesini gerektiren durumun kapsamlı ve detaylı bir şekilde incelenmesi, karşılaşılan problem karşısında politikanın sunduğu çözümlerin nesnel bir biçimde değerlendirilmesi (Kent, 2002, s.12).

Sherman Kent, istihbarat üreticileri ile politik karar alıcılar arasındaki ilişkinin optimal düzeyde olması gerektiğini vurgulamıştır. Ona göre, istihbarat politika, planlama ve operasyonlara en büyük yardımı sağlamak için yakın olmalıdır, ancak bu yakınlık nesnelliği ve yargı bütünlüğünü tehlikeye atacak düzeyde olmamalıdır (Özdağ, 2017, s.420). Nesnellik ve yargı bütünlüğü, istihbarat üreticilerinin çalışmalarının iç politika etkilerinden bağımsız olarak tarafsız bir şekilde yapılması anlamına gelmektedir. Bu bağlamda, istihbaratın oluşturulmasında devletin diğer ilgili

kurumlarının istihbarat birimleri ile koordineli bir şekilde çalışması gerektiğini savunmaktadır (Kent, 2002, s.12).

Sherman Kent'in stratejik istihbaratı kurumsallaştırma konseptine göre, stratejik istihbarat süreci yedi temel aşamadan oluşmaktadır (Biçer, 2017):

1. Sorunun Oluşumu: İlk aşama, bir sorunun ortaya çıkması veya belirlenmesidir.

2. Sorunun Ülke İçin Önemli Aşamalarının Tespiti İçin Analiz ve Hipotez Geliştirme: Bu aşama, sorunun ülke için ne kadar önemli olduğunun analiz edilmesini ve hipotezlerin geliştirilmesini içerir.

3. Hipoteze Yönelik Bilgi Toplama: Üçüncü aşama, belirlenen hipotezleri test etmek için gerekli bilgilerin toplanmasını içerir.

4. Toplanan Bilgilerin Sınıflandırılması ve Hipotezin Test Edilmesi: Dördüncü aşama, toplanan bilgilerin sınıflandırılması ve hipotezin doğruluğunun veya yanlışlığının test edilmesini içerir.

5. Hipoteze Yönelik Toplanan Bilgilerin Özünün Tespiti İçin Yeniden Değerlendirilmesi: Beşinci aşama, hipoteze yönelik toplanan bilgilerin özünün tespit edilmesi için bir yeniden değerlendirme sürecidir.

6. Hipotezin Doğrulanması veya Yanlışlanması İçin Sona Gidiş: Altıncı aşama, hipotezin kesin olarak doğrulanması veya yanlışlanması için sona giden bir süreci içerir.

7. Son Hipotezin Belirlenmesi: Yedinci aşama, stratejik istihbaratın sonucunu oluşturan ve sorunun çözümüne ulaşılmasını sağlayan son hipotezin belirlenmesini içerir.

Bu aşamalardan stratejik istihbaratın ülkenin dış politika oluşumundakı kritik önemi açıkca görülmektedir.

Kent, stratejik istihbaratın nesnel olması gerektiğini vurgulamış ve bu nesnel istihbaratın dış politikada rasyonellik sağlayacağını savunmuştur. Oluşturulacak nesnel istihbarat sistemi ile birlikte, bu rasyonalitenin devam edeceğini öngörmüştür. Kent'e göre, nesnel istihbarat sistemi sayesinde elde edilen bilgilerin düzenli bir yapı içinde olması, örtülü operasyonların azalmasına ve dış politikada kullanılan istihbaratın profesyonelleşmesine katkı sağlayacaktır (Ateş, 2019: 24-25). Özetle, Sherman Kent, oluşturduğu

ekol ile istihbaratı akademik bir perspektifle ele alarak stratejik istihbaratın gerekliliklerini, istihbarat-dış politika sürecini ve istihbarat üreticileri ile politik karar alıcılar arasındaki ilişkiyi ele almıştır.

3.2 Örtülü Operasyonlar ve Dış Politika

Johnson'ın örtülü operasyon türlerini dört ana başlık altında sıralamasının yanı sıra, John D. Stembel "Örtülü Operasyonlar ve Diplomasi" adlı eserinde, bu operasyonları "propaganda", "siyasal eylemler", "paramiliter" ve "ekonomik faaliyetler" olarak tanımlamıştır. Rory Cormac'ın "Bozmak ve İnkâr Etmek" isimli kitabında ise örtülü operasyonların "politik", "ekonomik" ve "özel operasyonlar" olarak üç ana kategoride bulunduğu belirtilmiş, ayrıca "propaganda"nın hem bağımsız bir araç olarak kullanılabildiği hem de bu operasyonları destekleyici bir rol üstlenebileceği ifade edilmiştir. Bir diğer eser olan "Yönetici Sırları: Örtülü Operasyonlar ve Başkanlık" adlı kitapta ise Daugherty, örtülü operasyonları "propaganda", "siyasal eylemler" ve "paramiliter operasyonlar" olarak tanımlayarak "üç geleneksel metodoloji" olduğunu aktarmıştır (Seren ve Yıldız, 2023 ss.192).

Politik örtülü operasyonlar, politik süreçlere, karar alımlarına ve kurumlara doğrudan etki etmeye yönelik faaliyetlerdir. Önemli birey ve kuruluşlara (siyasi figürler/partiler, güvenlik güçleri, medya, ticaret odaları, sendikalar, akademik araştırmacılar, düşünce kuruluşları vb.) maddi destek/rüşvet yanında eğitim desteği sağlanması veya çeşitli kaynaklarla ulusal/uluslararası alanda tanınırlıklarını artırmaya yönelik faaliyetleri içermektedir. Kamuya açık olmayan ödemeler, "hizmet bedeli", "bağış" veya "iyi niyet göstergesi" gibi terimlerle örtülü bir şekilde sunularak, ödeme yapan tarafın siyasi çıkarlarını desteklemesi ve en azından olumlu bir atmosfer yaratması veya karşı tarafın desteğini kazanması hedeflenir. Para dışında, değerli teknoloji temelli yardımlar (silah/teçhizat, teknolojik destek) ve bireylere yönelik dokunulmazlık veya siyasi sığınma hakları gibi argümanlar da kullanılabilir (Stempel, 2007, ss.126-127). Politik örtülü operasyonların uygulandığı diğer alanlar, kalkınma ve diyalog projelerini içerir. Kalkınma projelerinde genellikle geri kalmış ülkeler hedef alınır. Destek verilen ülkede, sivil toplum kuruluşları aracılığıyla kaynak transferleri sağlanır ve sadece göz alıcı ancak sınırlı faaliyetlerde bulunulur. Hükümetle kurulan sağlam ilişkiler sayesinde, ülkenin eğitim ve teknoloji eksikliğinden kaynaklanan potansiyel kaynaklar sömürülür. Diyalog

projelerinde ise hedef ülkede yeni kurulan organizasyonlar veya mevcut kuruluşlar, toplumu oluşturan farklı kültür, ırk, din veya mezhep grupları üzerinden gerçekte olmayan sorunlar yaratmak amacıyla kullanılır (Özdağ, 2017, s.247). Sosyolojik ve akademik çalışmalarla bu gruplara yönelik sözde olumsuzluklar çözülmeye çalışılır ve bu grupların düşüncelerini şekillendirmek adına devlet veya diğer gruplar tarafından sosyal ayrıcalıklar tanınır. Sonuç olarak, federal bir yapı veya özerkleşme talepleri oluşturularak ülkelerin bölünmesi hedeflenir.

Ekonomik örtülü operasyonlar, girişilen bazı faaliyetler sonucu hedef ülke veya kişinin ekonomik çöküşünü gerçekleştirmek amacıyla gerçekleştirilir. Bu faaliyetin nihai amacı üç farklı sonuca ulaşmaya neden olabilir. Bunlar, karşı tarafın ekonomik kaynaklarını asıl amaçları doğrultusunda kullanmasını engellemek, dış borç ve diğer yöntemlerle fakirleştirmek ve kötüleşen ekonomik şartlar yaratmak suretiyle hedef ülke içinde halk ayaklanması veya darbe ile hükümet değişimidir. İyi kurgulanan dış borç tuzağı; borçlarını ödeyemeyen ülkelerin ekonomi ve güvenliğinin kontrol altına alınmasını hedeflemektedir. Yüksek faizli ve kısa vadeli kredi, iç piyasalardan karlı tahvil ve hisse senetleri alınması, özelleştirmenin teşvik edilmesi gibi yöntemler dış borç tuzağının kapanıdır. Dış borcun sonuçları, ulus egemenliğinin sınırlanması, ekonomi ve iç dengelere müdahale, siyasi baskılara bağımlılık, ulusal kaynakların kaybıdır . Sermaye veya finans piyasası oyunları ulusal güvenliğe yönelik en önemli tehditlerden biri haline gelmiştir. Merkez bankalarının yönlendirilmesi, borsa işlemleri ile ani para transferleri, ulusal paranın değerinin yitirilmesi, ülkenin sürekli borçlanması hedeflenmektedir. Gelişmekte olan ülkeler genellikle euro/dolar olarak borçlanması sebebiyle alacaklıların geri ödemede zorlanma yaşanacağını hissetmesi halinde ani sermaye çıkışları yaşatarak döviz kurları karşısında ülke para biriminin değersizleşmesi, ithalat fiyatlarının artışı ve enflasyon ortamı yaşatılmaktadır (Johnson, 1989, ss.80-85). Ekonomik örtülü operasyona maruz kalan bir ülkenin içine düşeceği maddi sıkıntı o kadar büyük olabilir ki verilen borçların geri ödemesinde yetersiz kalan ülke bu borcunu BM'de rızası dışında oy kullanma, topraklarında yabancı ülke askeri üslerinin kurulmasına müsaade etme, değerli doğal kaynaklarına el konulması/yabancılara işletme hakkı verilmesi şeklinde ödeyebilir (Özdağ, 2017: 149).

Yarı askeri örtülü operasyonlar, hedef ülkede doğrudan savaşacak güçlerin oluşturulmasından, mevcut devlet karşıtı güçlere silah, eğitim, askeri destek veya danışmanlık sağlanmasına kadar geniş bir yelpazede gerçekleştirilen faaliyetlerdir. Bu operasyonlarda, devletin doğrudan rol almak yerine özel yapılanmalar olarak adlandırılabilecek aracı kurumlar tercih edilmektedir. Yarı askeri örtülü operasyonların uygulanacağı bölgedeki güçlerle koordinasyon ve sahada icra görevi, özel operasyon birlikleri ve istihbarat teşkilatının dış operasyon birimlerine aittir. Bu operasyonlar, kişilere yönelik suikasttan stratejik hedeflere sabotaja kadar geniş bir yelpazede icra edilmektedir (Johnson, 1989, s.86).

İstihbarat örgütlerinin ve işbirliği yapılan kurumların örtülü operasyon gücü, ülke politikalarının uygulanmasında politika uygulayıcılara büyük bir hareket kabiliyeti sağlar. Örtülü operasyonların yukarıda belirtilen türlerini ayrı ayrı incelediğimiz zaman, tümünün dış politika oluşturmak için yapıldığı kanaatine gelebiliriz.

4. STRATEJİK İSTİHBARAT VE ÖRTÜLÜ OPERASYONLAR KAPSAMINDA İRAN'IN BALKANLAR'DAKİ FAALİYETLERİ

Savaşın ardından ve daha yakın dönemde, Balkan ülkeleri, Avrupa ekonomisine entegre olma çabası içinde bulundular. Bazıları zaten AB üyeliğine sahip olan Bulgaristan ve Hırvatistan gibi, diğerleri, Arnavutluk, Kosova, Bosna-Hersek ve Sırbistan gibi, AB üyeliği için çaba gösteriyor. Bu bağlamda İran İslam Cumhuriyeti, Avrupa'ya olan ihracatını artırmak amacıyla Balkanları potansiyel bir fırsat olarak değerlendirmektedir (Dinçel, 2023, s.421).

İran'ın Balkanlar politikasındaki temel amaç, Yugoslavya'nın ve Sovyetler Birliği'nin dağılmasının ardından artan ABD ve Batı etkisini sınırlamaktır. Tahran yönetimi, bölgenin gelecekte kendi aleyhine kullanılacak bir üs haline gelmesinden endişe duymaktadır, bu nedenle Balkanlar'da etkin bir rol oynamaya çabalamaktadır (Progonati, 2017, s.202). Bu bölgede ABD ve Batı etkisinin sınırlanması İran'a, Avrupa'nın güneydoğusunda, yani Batı'nın yakın çevresinde, Devrim Muhafızları Ordusu ve Hizbullah gibi organizasyonların var olması fırsatlarını da içermektedir. Dolayısıyla İran, Balkanlar'daki varlığı aracılığıyla Avrupa'da açık ve örtülü operasyonlar yapma kapasitesini artırmayı hedeflemektedir (Başaran ve Kaya, 2023 s.3). Ayrıca İran'ın bu stratejisinin bir parçası

olarak, İsrail'le mücadele etme amacı da bulunmaktadır. Bu bağlamda Tahran, çeşitli dönemlerde Hizbullah gibi örgütler aracılığıyla İsrail'e yönelik çeşitli saldırılar düzenlemeğe çaba gösterebilir. Örneğin, 2012 yılında Bulgaristan'ın Burgaz kentinde İsrailli sivillere yönelik düzenlenen saldırıda altı kişi hayatını kaybetmiş ve bu saldırının Hizbullah tarafından gerçekleştirildiği iddia edilmiştir (Başaran ve Emrah, 2023, ss.2-4).

İran ve vekillerinin Balkanlar'daki Batı çıkarları için oluşturduğu tehdit, Bosna, Kosova, Makedonya ve Karadağ ile Sırbistan sınırındaki dağlık Sancak bölgesinde Vahhabi hareketlerin büyümesiyle katlanıyor. Balkanlar'daki ücra, izole köylerde Vahhabi gruplar, son yirmi yılda dünyanın dört bir yanından gelen cihatçılar için güvenli bir sığınak ve asker toplama alanı haline gelen, bölge dışı, şeriatla yönetilen yerleşim bölgelerinden oluşan bir ağ geliştirdiler. Son yıllarda İslamcı radikaller "gençlik kampları" adı altında gençleri sistematik olarak milli parklara ya da yerel tepelere ve ormanlara götürerek eski mücahitler tarafından askeri eğitim almalarını sağladılar. Bu kamplar kasıtlı olarak geçicidir, her yıl farklı yerlerde ve farklı himayeler altında yeniden kurulur, böylece güvenlik görevlilerinin onları takip etmesi daha zor hale gelir, ancak geçici doğalarına rağmen aşırılık yanlısı gençlerin yaratılması için gereken ilişkilerin geliştirilmesinde etkili olmuşlardır (Bardos, 2013, s.60).

İran'ın ikinci önemli hedefi, Balkan coğrafyasının İran'a karşı olan muhalifleri için güvenli bir sığınak olmaktan çıkarılmasıdır. Özellikle İran'daki en etkili muhalif örgüt olan ve rejim karşıtı faaliyetleriyle öne çıkan Halkın Mücahitleri Örgütü'nün merkezi Arnavutluk'ta bulunmaktadır. Bu durum, İran'ın bölgedeki ilgisini daha da artırmaktadır. Arnavutluk, özellikle Tahran'ın terörle mücadele politikasının bir parçası olarak ele alınmaktadır (Başaran ve Emrah, 2023, s.5). Örneğin, 20 Haziran 2023 yılında Hallın Mücahitleri Örgütü üyeleri Tiran'da bazı protesto eylemlerinde bulundular (Radio Liberty, 2023). Bosna savaşı sırasında 'Müslüman kardeşleri' desteklemek için Orta Doğu'dan Balkanlar'a yapılan göç, Müslüman nüfusun çoğunluğunun tarihsel olarak Sünniliğe bağlı olduğu bir bölgede radikal İslam'ı tanıttı. Özellikle Arnavutluk'ta Komünizmin çöküşünden sonra Arap köktendinciler cami inşaatlarına büyük yatırımlar yapmış ve komşu Kuzey Makedonya'ya da taşınmışlardır. İranlılar, Suudilerin rakibi olarak ortaya çıktılar ancak Araplardan daha az etkiye sahiptiler (Progonati 2017, s.178). Ancak Araplardan ziyade, İran'ın

Balkanlar politikasını etkileyen faktörlerden biri, Türkiye'nin rolüdür. Ankara, Osmanlı mirasına dayanarak Balkan coğrafyasında etkin olma çabasındadır. Bu durum, Tahran'ı endişelendirmektedir, çünkü Türkiye'nin İslamiyet ile demokrasinin bir arada varlığını sürdürebilen laik yapısı, sadece Balkan Müslümanlarına değil, aynı zamanda Ortadoğu halklarına da örnek teşkil edebilir ve bir model olarak algılanabilir. Balkanlar gibi Ortadoğu coğrafyasında da Osmanlı İmparatorluğu'nun izleri bulunmaktadır ve her iki bölge de Türkiye'nin gönül coğrafyasında yer almaktadır (Battir ve Davut, 2013, s.36). Bu nedenle, Ankara'nın Balkanlardaki Müslüman gruplar üzerindeki etkisinin artması, Türkiye'nin Orta Doğu'da bir rol model olarak algılanmasına neden olabilir. Bu durum, İran'ın antiemperyalizm ve antisiyonizm vurgusuyla Şii yayılmacılığı aracılığıyla elde ettiği kazanımları riske atabilir. Bu bağlamda İran'ın Balkanlardaki hedeflerinden biri, Türkiye'nin bölge politikasını etkisizleştirmektir.

İran'ın Balkanlar politikasını belirleyen dördüncü amaç, Suudi Arabistan tarafından desteklenen Selefileşmenin engellenmesidir. Bu durum, İran'ın İslam Dünyası liderliğine dair iddiası bağlamında geleneksel rakibi olan Suudi Arabistan'ın, Balkanlar üzerinden olası bir tehdit algısına yol açabilir. Özellikle Tahran, Riyad'ın Balkan Yarımadası'nda başarılı olması halinde, bu durumun bir domino etkisi yaratarak Ortadoğu'da İran'a karşı bir üstünlük sağlayabileceği endişesindedir (Başaran ve Kaya, 2023, s.6). Vehhabilik büyük miktarda Arap parasıyla desteklenerek bölgeye girerken, Sufi mirasını yayan İranlılar etkilerini kültür merkezleri, yayınlar ve seminerler aracılığıyla genişletmeye çalışmış ve bu şekilde etkilerini daha az sayıda bir kitleyle sınırlandırmıştır. Aslında, İslam devriminden sonra İran liderliği, jeopolitik etkiler için dinin cazibesini sunmanın daha sofistike yollarını geliştirmiştir (Mandaville ve Hamid 2018, s.15). Bektaşi tarikatı geleneksel olarak Arnavut nüfusu arasında (özellikle Orta ve Güney Arnavutluk'ta) çok güçlüydü ve Sünni çoğunluk içinde Şii bir azınlık olarak nitelendirilebilir. İran, Bosna, Arnavutluk, Kosova, Kuzey Makedonya ve Sırbistan'daki Sancak bölgesinde Vahhabi hareketlerin büyümesinde çok etkili olmuştur. Buna ek olarak, Bosna Savaşı sırasında Bosnalı Müslüman Hükümet üzerindeki etkisiyle çok önemli bir rol oynamıştır (Bardos 2013). İran 1992-95 yılları boyunca Bosnalılara silah, mühimmat ve para sağlamayı başarmıştır. Binlerce yabancı mücahit Bosna tarafında savaşırken, 1993'ten itibaren Körfez ülkelerinin mali desteği de çok önemliydi. Ancak İran da çok

sayıda Devrim Muhafızı gönderdi ve özel kuvvet birimlerini eğitmeyi teklif etti (Koppa, 2021, s.7).

İran'ın Balkanlar politikasındaki son hedefi, bölgedeki Müslümanların Şiileştirilmesi ve İran'ın Dini Rehberi'nin taklit mercii olarak kabul edilmesidir. Bu durumun gerçekleşmesi, Tahran'ın Balkanlar'da önemli bir siyasi etki elde ettiği anlamına gelecektir. Zaten İran, dünyanın farklı bölgelerinde yaşayan Şiilerin İran İslam Cumhuriyeti Dini Rehberi'ni taklit mercii olarak benimsemelerini teşvik etmeye çalışmaktadır. Bu şekilde, Tahran, Şii dünyasının siyasi ve dini referans noktası olacağına inanmaktadır (Berkoli, 2021, a,b,c). Tahran yönetimi, Bu bağlamda, sufi tarikatlar ve Bektaşi grupların, İran'ın Şiileştirme politikasında temel aktörler olarak kullanıldığı ve Tahran'ın bu gruplarla çeşitli araçlar aracılığıyla temas kurduğu belirtilebilir. Ayrıca, İran, bölgede ücretsiz Kur'an-ı Kerim ve dini kitaplar dağıtarak, yerel halka İslam'ın Şii inancını ve bu inanç doğrultusunda Kum merkezli olarak İran'ın İslami yorumunu aktarmaktadır (Başaran ve Kaya, 2023, s.19).

İran'ın Balkanlardaki hedeflerine ulaşmak için başvurduğu stratejilerden biri, Fars kültürünü tanıtmak ve Farsça dil kursları açarak bölgede Farsça öğrenimini teşvik etmektir. Ayrıca, Fars kültüründen önemli şahsiyetleri tanıtarak İran, bölgede kendisine yönelik sempatiyi artırmayı hedeflemektedir. Ancak İran'ın Balkanlardaki amaçlarına ulaşmak için kullanılan yöntemler sadece yumuşak güç kullanımıyla sınırlı değildir. İran, bölgede etkili olmak için özellikle Devrim Muhafızları Ordusu ve onun desteklediği paramiliter yapılar aracılığıyla, özellikle Hizbullah vasıtasıyla, açık ve örtülü istihbarat operasyonları gerçekleştirmektedir. Bu operasyonlardan aşağıda bahs edilmiştir (Berkoli, 2021a).

Boşnak topluluğu, 1960'lı yıllardan itibaren ulusal bir kimlik arayışına girdi. İslam Devrimi'nden etkilenen Bosnalı lider Alija İzetbegoviç, 1979 yılında İran'da hapis yattığı sırada uluslararası bir hareketin parçası olarak kendisini hissetmeye başladı. İzetbegoviç'in o dönemdeki yakın çalışma arkadaşları, 1982'de İran'daki İslam Cumhuriyeti'nin kuruluş yıldönümü kutlamalarına ve Sünni ve Şii İslam'ın birleşmesini amaçlayan bir kongreye gizlice katıldı (Domazeti, 2017 s.17). Bu dönemden itibaren, İran, Balkanlar'da etkisini güçlendirmeye başladı. Bosna Savaşı sırasında, İran'ın Şii mezhebine mensup olması, Sünni kökenli Bosna Müslümanlarını desteklemesi, İran'ın bu bölgedeki nüfuzunu artırmak istediğini gösteren bir

belirleyici faktördür. İran, Bosna Savaşı'nda yoğun bir şekilde silah yardımı sağlayan uluslararası bir aktör olarak öne çıktı. İran'ın katkıları sadece silah yardımı ile sınırlı kalmadı, aynı zamanda İran Devrim Muhafızları Ordusu, Bosna Hersek Ordusu'nun askeri eğitimine de önemli bir katkıda bulundu (Progonati, 2017, s.203). Ayetullah Ahmed, Boşnaklara yardımı koordine etti ve bu müdahaleyi İslam Cumhuriyeti'nin Filistin'den Güney Afrika'ya kadar dünyanın dört bir yanındaki ezilenleri savunma konseptine uygun olarak gerekçelendirdi.

Avrupalı hükümetler BM'nin Bosna Hersek'e uyguladığı silah ambargosuna uyarken, İran ağır silahlı düşmanlarına karşı mücadele eden Boşnaklara askeri eğitmenler, istihbarat görevlileri, gıda, para ve insani yardım göndererek bu boşluğu doldurdu. İran Kızılayı üniforması giymiş yardım görevlileri kılığında İslam Devrim Muhafızları Ordusu güçleri BH'ye ulaştı. Her ne kadar gizli olsa da bu katkı etkili oldu (Bardos, 2013, s.63). Bosnalı bir siyasi analist olan Harun Karcic'e göre "İran silahları kuşatılmış Bosna yönetimi için çok önemliydi ve Devrim Muhafızları eğitmenleri çatışmanın ilk aşamalarında ayak takımı Bosnalı savaşçıların eğitiminde çok önemli bir rol oynadı (Califero, t.y)." 10 Eylül 1992'de Batılı yetkililer Hırvat meslektaşlarının İran silahları ve personeliyle Zagreb'e uçan bir İran Boeing 747'sini yakaladıklarını ve bunun Tahran'ın Boşnaklara verdiği maddi desteğin belgelenmiş ilk örneği olduğunu belirttiler. Uçağın görevinin Bosna Hersek'e yardım malzemesi sağlamak olduğu belirtilmişti, ancak Hırvat yetkililer "4.000 silah, bir milyondan fazla mermi ve arkada toplanmış 20 ila 40 İranlı keşfetti." (Califero, t.y). Uygulanan silah ambargosuna rağmen İran, Bosna Hersek'e silah, istihbarat ve lojistik desteği sağlamıştır. İran, bu dönemde Bosna Hersek'te istihbarat ağını genişletmiştir. Savaşın sona ermesinden sonra da Saraybosna, Mostar, Zenica, Bihac ve Visoko gibi bölgelerde İran, "hayır kurumları" vasıtasıyla nüfuzunu artırmayı sürdürmüştür.

Bu dönemden sonra İran yanlısı gruplar çok sayıda kurumun içine derinlemesine yerleşmişlerdi. Amerikalı gazeteci James Risen'a açıklanan bir CIA raporuna göre, İzetbegoviç'in doğrudan İran'dan mali destek aldığı ve tek bir seferde İranlı ajanlardan 500.000 dolar gibi önemli bir miktarda nakit para aldığı bildirildi. Özellikle İran'ın Bosna Büyükelçisi, 1996'daki seçim kampanyası sırasında İzetbegoviç'e eşlik eden tek yabancı diplomattı (Bardos, 2013 s.63). 1997 yılına gelindiğinde CIA raporlarına göre, İran'ın

çeşitli Bosna kurumlarına yaklaşık iki yüz ajan yerleştirdiği tahmin ediliyordu. Özel hedeflerinden biri, Müslüman-Hırvat Federasyon Ordusu için ABD destekli "silahlandır ve eğit" programıydı. İzetbegoviç rejimi içindeki kilit müttefiklerin desteğiyle İran istihbarat servisleri, İzetbegoviç'in güvenlik servisi içindeki İran yanlısı hizip tarafından özenle seçilen şoförleri, çevirmenleri ve idari personeli programa başarıyla sızdırdı. Örneğin, "silahlandır ve eğit" programının koordinasyonu için ABD Savunma Bakanlığı ile baş irtibat görevlisi olan General Dzemal Merdan, aynı zamanda İzetbegoviç'in İran Devrim Muhafızları ile ilişkilerinden sorumlu subayı olarak görev yapıyordu. Ayrıca, mücahit güçleri Bosna'ya entegre eden "7. Müslüman Tugayı"nın kurucu üyelerinden biriydi. İran, çeşitli hayır kurumlarına, medya kuruluşlarına ve hatta Saraybosna'daki bir hazır yiyecek zincirine yerleştirdiği ajanlarla Bosna'daki erişim alanını genişletti. Eş zamanlı olarak Bosna hükümeti de İran'a askeri personel gönderiyordu (Bardos, 2013, ss. 63-64).

Saraybosna'daki İran Kültür Merkezi, İran Büyükelçiliği'nin bir parçası olarak faaliyet gösteriyor. Araştırmalardan malum olduğu üzere bu merkezin özellikle İran ve Şiilik konularında kültürel etkinliklere ev sahipliği yaptığı görülmektedir. Bu merkezin çatısı altında bilimsel Beharistan dergisi yayın yapmaktadır. Dergi yılda iki kez yayınlanıyor ve edebi, felsefi, dilbilimsel ve kültürel konuları içeren zengin bir içeriğe sahiptir. Bu dergi, Bosnalı profesör ve entelektüeller tarafından yönetiliyor ve yayın kurulunda İranlı uzmanlar da bulunuyor. Saraybosna başta olmak üzere Bosna'nın diğer şehirlerindeki üniversitelerle, bilim, kültür ve dini çevrelerle işbirliği yaparak dağıtımını gerçekleştiriyor. Beharistan dergisindeki makalelerin yarısı İranlı yazarlar tarafından yazılıyor ve daha sonra Boşnakça'ya çevriliyor. İran Kültür Merkezi ayrıca siyaset, Şiilik ve Fars edebiyatı gibi konularda bir dizi kitap yayınlamıştır (Berkolli, 2021a). Dünya İslam Bilimleri Merkezi, Yurtdışı Eğitim Kurumu, İslam Kültürü ve İlişkiler Organizasyonu, Uluslararası el-Mustafa Üniversitesi gibi kurumlar, Şii İslam anlatısı ve İslamcı ideolojik söylemi yayma hedefiyle faaliyet göstermiştir (Berkolli, 2021d).

Batılı güçlerin Boşnak yetkililerinden İran'ın silahlı birliklerinin ülkeden çekilmesini talep etmesinden kısa bir süre sonra, 1996 yılında Saraybosna'da kurulmuş Ibn-i Sina Enstitüsü, İran İslam Cumhuriyeti'nin Balkan bölgesindeki varlığını inceleyen herkesin kolayca ulaşabileceği bir

kurumdur. Enstitünün faaliyet alanı ve etkisi, Bosna Hersek ve Balkan bölgesindeki kültür uzmanlarının yazılarında ve kendileriyle gerçekleştirilen görüşmelerde açıkça görülmektedir. Beşeri bilimlerde çalışma ve araştırma yapma, İranlı ve Boşnak alimlerle iş birliğini geliştirmek, kültür-bilim enstitüleri arasında bilim, araştırma ve kültür alanlarında iş birliğini desteklemek gibi faaliyetler, kurumun odaklandığı alanları oluşturuyor (Berkolli, 2021b).

Bunlardan başka 2003 yılında kurulan Molla Sadra Enstitüsü Saraybosna'da faaliyet göstermektedir, yine İran'ın etkili kültürel stratejilerinden birini yansıtan önemli bir kurumdur. Bu enstitü, Balkan devletlerinde Ayetullah Humeyni'nin temsilcisi olarak bilinen Şii din adamı Akbar Eydi tarafından yönetilmektedir. Kurumun hedefleri arasında, "üniversite hocaları, önde gelen şahsiyetler, bilim ve kültür merkezleri, öğrenciler ve sosyal gruplarla iş birliği yaparak özellikle Bosna-Hersek İslam Birliği ile uyum ve koordinasyon sağlamak" gibi amaçlar da bulunmaktadır (Berkolli, 2021a).

İran'ın etkinlikleri, kültürel etkisini genişletmek amacıyla enstitü ve okul benzeri kuruluşlar kurma gibi stratejiler içermektedir. Balkan bölgesinde faaliyet gösteren İran'a bağlı kültür merkezleri, toplum içinde etkilerini artırmak için çeşitli stratejiler uygulamışlardır. İran Büyükelçiliği, bu kuruluşlar aracılığıyla birçok Boşnak entelektüel ve akademisyenle sıkı ilişkiler kurmayı başarmış ve İran'da eğitim görmüş Boşnak öğrencilerle birlikte çalışarak birçok projede yer almıştır. İran, bu faaliyetleri ele alarak Balkanlarda dini ve siyasi propaganda yapabilme fırsatına sahiptir.

İran ve Arnavutluk arasındaki ilişkiler, Arnavutluk'ta komünist rejimin çöküşünden sonra değişti. 1990'lı yılların ardından İran, kültürel faaliyetlerini sürdürmek amacıyla Tiran'da Büyükelçilik açtı. İran'ın Tiran'daki ilk kültür merkezi olan Sa'di-i Şirazi Kültür Kurumu, 1995 yılında kuruldu (Berkoli, 2021). Kurumun amacı, "İran-Arnavutluk arasındaki kültürel bağları canlandırmak, İran medeniyetinin geleneklerini Arnavutluk'ta tanınır hale getirmek ve iki kadim halkın dostluğuna hizmet etmek"ti. Sa'di-i Şirazi Kültür Kurumu, İslam Kültürü ve İletişim Örgütü'nün Arnavutluk'taki bir temsilcisi olarak faaliyet göstererek Arnavutluk'un entelektüelleri, bilim insanları ve akademisyenleri ile geniş bir iş birliği geliştirdi (Berkoli, 2021c). Kurum bünyesinde yer alan Perla isimli bilim-kültür dergisi, ülkenin önde gelen bilimsel dergilerinden biri

haline geldi. İran Büyükelçiliği ve Sa'di-i Şirazi Kültür Kurumu, bu dergi aracılığıyla Arnavutluk'taki birçok kültür ve eğitim kurumu yanı sıra Profesör Jorgo Bulo, Profesör Shaban Sinani, Profesör Muzafer Korkuti ve Profesör Emil Lafe gibi önemli Arnavut alimlerle de iş birliği geliştirmeyi başardı.

İran, 2000 yılı öncesinde Yurt Dışı Okullar Kurumu ve ardından el-Mustafa Üniversitesi aracılığıyla Tiran'da Kur'an Kurumu'nu kurdu (Berkoli, 2021b). Ancak Arnavut halkının muhalefeti ve kaydedilen yavaş ilerleme, İran'ı faaliyetlerini yerel teşkilatlar altında sürdürmeye zorladı. Bu nedenle İranlılar, 2005 yılında Kur'an Kurumu'nu kapatıp, Beyrut'ta eğitim almış Şii ilahiyatçı Sheikh Vullnet Merja'nın başkanlığını yaptığı Nesim (Flladi/Breeze) Kültür ve Din Kurumu'nu açtı (Berkolli, 2021c). 2007 yılında İran tarafından Arnavutluk'ta Rumi Vakfı kuruldu. Bu vakfın temel amaçlarından biri, İslam'ı felsefi bir şekilde yorumlayan eserleri yayınlamaktı. Vakıf, ilk zamanlarda felsefi eserleri tercüme etme amacına uygun hareket etti. Ancak daha sonra vakıf bünyesinde, radikal İranlı dini liderlerin kitapları da basıldı (Berkolli, 2021c). İran'ın Balkanlardaki kültürel yatırımlarından biri de Bektaşiliği, Şiiliğin bir parçası olarak tanıtmasıdır. İran, Arnavutluk'taki Bektaşilerin liderleri ile diyalog kanallarını geliştirmiştir. Ancak Arnavutça yazılan eski Bektaşi metinlerinde veya Bektaşi mezhebinin klasik sayılabilecek eserlerinde, Bektaşiliğin Şiiliğin bir parçası olduğuna dair hiçbir kanıt bulunmamaktadır. İran, Balkanlar'daki Sufi geleneğe, Şii bakış açısı çerçevesinde yaklaşmaktadır ve Balkanlar'daki tekke ve tarikatlar ile ilişki geliştirerek, buralarda var olan ritüel ve kaideleri Şii perspektifi üzerinden yorumlamaktadır (Berkolli, 2021d).

İran, bu bölgelerde kültür kullanarak, Şii mezhebinin prensiplerini Balkan Müslümanları arasında yaymaya çaba göstermektedir. Ancak Balkan Müslümanları arasında Şiiliğin pek yaygın olmadığı gözlemlenmektedir. İran'ın stratejik istihbarat faaliyetlerini sadece askeri veya politik unsurlarla sınırlı tutmadığı söylenebilir. İran, diplomasi ve kültürel konularda da etkin olmaya çalışarak, uzun vadeli perspektifte Balkanlar'da politika izlemeye çalışmaktadır (Başaran ve Emrah, 2023, s.24-25). Bu bölgelerde yaşayan ve İran etkisinde kalan Müslümanların, düşüncelerinde, tarihe bakışlarında veya kıyafetlerinde birçok konuda farklılıklar yaranmıştır.

Balkanlarda geniş etki alanları olan Rusya ve Çin gibi, İran da etkili ama daha az görünür bir rol oynamaktadır. İran bölgede, kültürel konularda faaliyet yürütmekle birlikte, özellikle kitlesel manipülasyon konusunda güçlüdür. İran'ın Balkan coğrafyasına odaklanmasının sebepleri arasında, bu bölgenin küresel istihbarat teşkilatları için ikincil öneme sahip olması, güvenliğin bu coğrafyada daha esnek olması ve kurumların köklü olmaması gibi faktörler bulunmaktadır (Dinçel, 2023, s.423). İran, Orta ve Batı Avrupa'da, faaliyet yürütebilmek için Balkanlar'ı bir geçiş noktası olarak değerlendirmektedir. İran'ın Avrupa'da yaşanan saldırılara müdahil olduğu bilinmektedir. Örneğin, Fransa'da 2018 yılında muhalif İranlılara yönelik bombalı bir saldırı gerçekleşmiştir. İranlı diplomat Asadullah Asadi, saldırının planlayıcısı olduğu gerekçesiyle 20 yıl hapis cezasına çarptırılmıştır. Fransa, Asadi'nin İran istihbaratı adına görev yaptığını iddia etmiştir (Başaran ve Emrah, 2023 s.27). Tahran yönetimi, Balkanlar bölgesinde düşük profilli ancak etkili faaliyetlerde bulunmaktadır. Bosna Savaşı'ndan sonra İran, siyasi yerel aktörlerle iş birliğini sürdürmeye çaba göstermiştir. Bosna Müslümanlarının Sünni mezhebine mensup olması, İran için bir engel teşkil etmemektedir. İran, Balkanlar'ı stratejik bir konum olarak görmektedir ve bu nedenle mezhepsel farklılıkları göz ardı etmektedir (Avramov ve Trad, 2018). İran, Balkan coğrafyasında etkili olabilmek için siyasi ve diplomatik araçları etkili bir şekilde kullanmanın önemine inanmaktadır. Politik çıkarların daha baskın olduğu bir ortamda, bölgede etkili olma çabalarında sadece ideolojik araçları kullanma yaklaşımından vazgeçilmiştir.

Bosna Savaşı sonrası, İran bölgedeki istihbarat elemanları ve casusları vasıtasıyla Bosna-Hersek'teki faaliyetlerini sürdürmüştür. Bu unsurların ana görevi, bilgi toplamak ve Batılı devletlerin Bosna'daki etkinliklerini engellemeye çalışmaktı. İran ajanlarının, Bosna-Hersek İstihbarat Servisi'nde bir grup ile yakın ilişkiler içinde olduğu öne sürülmüştür. O dönemde, Batılı ülkelerin en büyük kaygısı, İran adına çalışan ajanlar tarafından Batılı devletlere yönelik saldırı düzenlenmesi olasılığıydı (Dinçel, 2023, s.423). İran, bölgeye yayılmak ve halkın ilgisini çekmek için çaba göstererek sempati kazanmayı hedeflemiştir. İran, samimi ilişkiler kurarak bölgedeki etkisini artırmaya çalışmıştır. Ayrıca, yüzlerce Boşnak, İranlı yetkililer tarafından askeri eğitimden geçirilmiştir (Tokgöz, 2015, s. 142).

Batılı ve Bosnalı yetkililere göre, İran istihbarat ajanları Bosna'da geniş çaplı operasyonlar düzenliyor ve Bosna Ordusu'nu eğiten Amerikan programına sızmış durumda. Yetkililere göre, Bosnalı Müslüman siyasi ve sosyal çevrelere sessizce ve sistemli bir şekilde sızdıklarına inanılan 200'den fazla İranlı ajan tespit edilmiş durumda. Hedeflerinin hem bilgi toplamak hem de Bosna'daki Batı çıkarlarını engellemek olduğu anlaşılıyor. Yetkililer, Amerikan destekli askeri eğitim programının yıkıcılık için kilit bir hedef olduğunu belirtiyorlar. Çünkü Müslüman ve Hırvat güçlerin ortak bir komuta altında birleşerek entegre bir Bosna ordusu kurmayı amaçladığını ve bu durumun ülkede siyasi istikrarı yeniden tesis etmek ve NATO liderliğindeki güçlerin çekilmesine izin vermek için önemli bir unsur olduğunu ifade ediyorlar. Yetkililere göre, İranlı ajanlar Bosna istihbarat servisi içindeki İran yanlısı bir grupla yakın işbirliği içinde bulunuyor. Bosna'daki istihbarat teşkilatının mevcut ve eski altı yetkilisi ayrı ayrı verdikleri mülakatlarda, teşkilat içinde İran ile daha yakın ilişkiler kurup kurmama konusunda bir mücadele yaşandığını anlattılar (Dinçel, 2023, s.423). İran, ilişkilerini samimi kurmakla, bölgede etkinliğini artırmağa gayret göstermektedir. Bunun yanısıra yüzlerce Boşnaklı İran tarafından görevlendirilenlerin gözetimi altında askeri eğitimlere tabi tutulmaktaydı.

İran, Devrim Muhafızları Ordusu, İran İstihbarat Bakanlığı ve İslam Kültürel İlişkiler Organizasyonu aracılığıyla bölgede etkinlik göstermeye başlamıştır. Arnavutluk hükümetinin DMO veya İran istihbaratının faaliyetlerine izin vermeyeceği bilindiğinden, Tahran yönetimi çeşitli kültürel örgütler kurmuştur. Arnavutluk'taki Bektaşi toplulukları, İran'dan para teklifleri aldıklarını, ancak bu teklifleri reddettiklerini ifade etmektedir. Ülkenin eski Cumhurbaşkanı Sali Berisha da İran'ı eleştiren açıklamalar yapmıştır (Prognati, 2017, ss.187-188).

İran ayrıca NATO üyeleri olan Arnavutluk, Hırvatistan ve Bulgaristan gibi Balkan ülkeleriyle de yakından ilgilenmektedir. Arnavutluk, İran tarafından yönlendirilen ajanların kendi topraklarında faaliyet göstermesini bir tehdit olarak değerlendirmektedir. Arnavutluk'taki İran yanlısı unsurlar, Tahran yönetiminin bölgedeki ekonomik faaliyetlerini destekleme potansiyeline sahiptir (Progonati, 2017, s.190). Ancak, Arnavutluk'ta İran tarafından terör örgütü olarak tanımlanan bir oluşum bulunmaktadır. İran yetkilileri, rejim karşıtı "Halkın Mücahitleri Örgütü" mensuplarının Arnavutluk'ta yargılanması gerektiğini ifade etmektedirler. Arnavutluk'un,

örgütün 2800 üyesine sığınma hakkı tanıması, Tahran ile Tiran arasındaki diplomatik ilişkileri olumsuz etkilemiştir (Independent Türkçe, 23 Haziran, 2023). İran, Temmuz 2022'de Arnavutluk'un dijital altyapısına yapılan siber saldırının ardından, Eylül 2022'de iki ülke arasındaki diplomatik ilişkileri kestiğini duyurmuştur (Cuka, 2022). Halkın Mücahitleri Örgütü, ilk kez 2013'te ABD'nin etkisiyle Arnavutluk'a yerleşmiştir. Örgüt mensupları, Dıraç'taki "Ashraf 3" adlı kampta yaşamlarını sürdürmektedir. Arnavutluk'taki güvenlik güçleri, 20 Haziran 2023'te bu kampa baskın düzenlemiştir ve çıkan çatışmada bir örgüt mensubu hayatını kaybetmiştir (Balkannews, 20 Haziran, 2023). Bu bağlamda, İran'ın bu gelişmelerden memnun olduğu söylenebilir.

İran'ın Balkanlardaki etkinliği, Bektaşilik ve benzeri yaklaşımlar üzerinden stratejik istihbarat yöntemlerini başarılı bir şekilde kullanmasını göstermektedir. İran, uzun vadeli hedef olarak bu bölgede politik açıdan, diğer güçlerle (Suudi Arabistan ve Türkiye) karşı karşıya daha güçlü bir konuma gelmeyi amaçlamaktadır. İran'ın Doğu Avrupa'da istihbarat faaliyetlerini artırma isteği, Balkanlar'ı istihbarat savaşlarının yaşandığı bir ortam haline getirmektedir. İran, Doğu Avrupa ve Balkanlar'da istihbarat faaliyetlerini sürdürürken sadece yumuşak güç unsurlarını değil, taktik ve operasyonel istihbaratın unsurlarını da kullanmaktadır. Avrupa'da muhaliflere yönelik saldırıların artması, İran'ın Balkanlar'da etkili bir politika izlemesinin bir sonucudur. İran'ın Bosna Hersek'ten ayrılmaması ve istihbarat gücünü artırması, uzun vadeli planlamalara önem verdiğini göstermektedir. İran, stratejik istihbarat unsurlarını etkili bir şekilde kullanarak ulusal çıkarlarına uygun enstrümanları sahada kullanmaktan kaçınmamıştır.

SONUÇ

Balkanlar, İran için ekonomik ve diğer alanlarda kazanımlar elde edebileceği önemli bir bölge konumundadır. Bu sebepten İran Balkanlarda aktif bir rol almak için stratejik istihbarat faaliyetleri ve istihbarat operasyonu unsuru olan örtülü operasyonlar kapsamında yumuşak güç kullanmaya özen gösterdiğini görmekteyiz. Bosna Savaşı'nın ardından Bosna Hersek başta olmak üzere İran'ın, Balkan devletleri üzerinde etkili olma çabası başlamıştır. İran'ın, bu bölgede etkili olma isteğinin altında, Avrupalı muhaliflere karşı baskı ve saldırını güçlendirme, İran taraftarlarını

bu bölgelerde artırma ve bu yolla bu bölgenin İran için Avrupa'ya açılan kapı konumuna getirme amacı yatmaktadır.

Bosna Hersek Savaşı sırasında İran agresif bir istihbarat yöntemi kullanmış, Bosna Hersek'in kurumlarına sızmaya çalışarak, savaş sonrası kazanımlarını artırmayı hedef olarak belirlemiştir. Savaşın ardında günümüze kadar İran, bu bölgede daha çok diplomatik ve kültürel faaliyetlerde bulunarak sessiz bir dış politika izlemiş ve bu faaliyetler üzerinden örtülü operasyonlar ve stratejik istihbarat anlayışlarının geliştirdiği görülmektedir. 30 yıla yaklaşık bir süreçte, bu bölgede güven oluşturma çabası sarf eden ve bu doğrultuda faaliyetler sürdüren İran İslam Cumhuriyeti'nin, uzun vadeli planları ile stratejik istihbaratın enstrümanlarını uygulama ve örtülü operasyonlar yapma konusunda başarılı olduğu görülmektedir.

İran, kültür merkezleri aracılığıyla Şiiliği yaymakta, toplumda İran taraftarlarını artırmakta ve bu bölgedeki ilim adamlarıyla bağlantılar kurarak projeler kurmaktadır. Bu bilgileri ele alarak İran'ın Balkanlar'daki istihbarat faaliyetlerini, yalnızca askeri veya politik araçları kullanarak hareket etmediği söylenebilir. Diplomasi ve kültürel alanlarda da etkili olmaya çalışarak, Balkanlarda uzun vadeli politika yürütmesi dikkat çekmektedir.

KAYNAKÇA

Ataç, K. K. (2019). İstihbarat, casusluk, karşı casusluk, örtülü operasyonlar ve güvenlik. *Güvenlik Yazıları Serisi, 45*, 1-10.

Ateş, A. (2013). *Stratejik istihbarat ve Türk dış politikasına etkisi*, Yayımlanmamış Yüksek Lisans Tezi, Adnan Menderes Üniversitesi.

Avramov, K., Trad, R. (2018, October 12). Under the radar: Iran's 'stealth' presence on the Balkans. Erişim tarihi: 05 Aralık 2024, https://theglobepost.com/2018/12/10/iran-stealth-presence-balkans/

Balkannews. (2023, Haziran 20). Arnavutluk'ta Halkın Mücahitleri Örgütü'nün kampına baskın, Erişim tarihi: 05 Aralık 2024, https://www.balkannews.com.tr/arnavutluk/arnavutluk-ta-halkin-mucahitleri-orgutu-nun-kampina-h7106.html

Bardos, G. N. (2013). Iran in the Balkans: A history and a forecast. *World Affairs*, 175(5), 59-66.

Başaran, D., ve Emrah, K. (2023). İran İslam Cumhuriyeti'nin Balkanlar Politikası: Bosna-Hersek ve Arnavutluk Örnekleri. *Balkan Araştırma Enstitüsü Dergisi*, *12*(1), 1-35.

Battir, O., ve Davut, A. (2013). Türkiye bölgesel hegemonya arayışında mı? *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, (29), 31-44. s. 36.

Berkolli, L. (2021). *Bosna Hersek: İran'ın Balkanlar'daki kültürel etkisinin zirvesi*. Erişim tarihi: 30 Aralık 2023, https://iramcenter.org/bosna-hersek-iranin-balkanlardaki-kulturel-etkisinin- zirvesi/

Berkolli, L. (2021). *Iran's cultural activities in Albania (Western Balkan).* Erişim tarihi: 30 Aralık 2023, https://iramcenter.org/en/irans-cultural-activities-in-albania-western-balkan-453

Berkolli, L. (2021). *İran'ın Balkan ülkelerinde kültürel hâkimiyetini genişletme stratejileri*. Erişim tarihi: 30 Aralık 2023, https://iramcenter.org/iranin-balkan-ulkelerinde-kulturel-h%C3%A2kimiyetini-genisletme-stratejileri-556

Berkolli, L. (2021). *İran'ın Bosna-Hersek'teki kültürel varliği*. Erişim tarihi: 30 Aralık 2023, https:// iramcenter.org/iranin-bosna-hersekteki-kulturel-varligi/

Berkolli, L. (2021). *İran'ın Bosna-Hersek'teki kültürel varliği*. Erişim tarihi: 30 Aralık 2023, https:// iramcenter.org/iranin-bosna-hersekteki-kulturel-varligi/

Beşe, E., ve Seren, M. (2011). Stratejik istihbarat olgusunun teorik çerçevesi, unsurları ve terörle mücadele politikalari açisindan rolü ve önemi. *Turkish Journal of Police Studies/Polis Bilimleri Dergisi*, *13*(3).

Biçer, S. (2017). Ulusal güvenlik ve istihbarat sisteminde geleneksel anlayıştan modern ve değişen ihtiyaçlar dönemine geçiş. *Karadeniz Sosyal Bilimler Dergisi*, *9*(2), 435-464.

Cafiero, G. (2022, September 5). In the rearview mirror: The case of Iranian influence in Bosnia. Erişim tarihi: 25 Aralık 2023, https:// gulfif.org/in-the-rearview-mirror-the-case-of-iranian-influence-in-bosnia/

Califero, G. (t.y.) *In the rearview mirror: The Case of Iranian Influence in Bosnia*. Erişim tarihi: 25 Aralık 2023, https://gulfif.org/in-the-rearview-mirror-the-case-of-iranian-influence-in-bosnia/

Cuka, F. (2022, September 7). *Arnavutluk, İran ile diplomatik ilişkilerin kesilmesine karar verdi*. Erişim tarihi: 28 Aralık 2023, https://www.aa.com.tr/tr/dunya/arnavutluk-iran-ile-diplomatik-iliskilerin-kesilmesine-karar-verdi/2678926

Dinçel, Y. (2023). Stratejik İstihbarat Kapsamında Suudi Arabistan'ın ve İran'ın Batı Balkanlar'daki Faaliyetleri. *Marmara Üniversitesi Siyasal Bilimler Dergisi*, *11*(2), 412-429.

Domazeti, R. (2017). Suudi Arabistan'ın Balkan politikaları. *Ortadoğu ve Afrika Araştırmacıları Derneği (ORDAF)*. Rapor 17.

Girgin, K. (2003). *Uluslararası ilişkiler, modern istihbarat ve Türkiye*. Okumuş Adam Yayıncılık.

Gül, Z. (2014). İstihbarat Çeşitleri ve Stratejik İstihbarat. İçinde: Harmancı, F. M.; Gözübenli, M. ve Zengin, C. (Ed.), Güvenlik Sektöründe Temel Stratejiler (ss. 83-98). Nobel Yayınevi.

Güldiken, N. (2006). Bilginin elde edilmesi ve korunmasinda ekonomik istihbarat sistemlerinin rolü. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi*, *7*(2), 169-182.

Güzel Özgüven, N. (2011). *Soğuk Savaş dönemi sonrasi özel askeri şirketler yoluyla yürütülen istihbarat faaliyetlerinin incelenmesi* (Yayınlanmamış Yüksek Lisans Tezi). İstanbul, T.C. Genelkurmay Başkanlığı Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü Müdürlüğü.

Independent Türkçe. (2023, Haziran 23). Tahran Halkın Mücahitleri örgütü hakkında Arnavutluk'u uyardı. Erişim tarihi: 25 Aralık 2023, https://www.indyturk.com/node/642401/d%C3%BCnya/tahran-halk%C4%B1n-m%C3%BCcahitleri-%C3%B6rg%C3%BCt%C3%BC-hakk%C4%B1nda-arnavutluku-uyard%C4%B1

Johnson, L. K. (1989). Covert action and accountability: Decision-making for America's secret foreign policy. *International Studies Quarterly*, *33*(1), 81-109.

Johnson, L. K. (2022). *The third option: Covert action and american foreign policy*, Oxford University Press

Karaağaç, Y. (2021). Gizli servislerde örtülü operasyon faaliyetleri. *Academic Review of Humanities and Social Sciences*, *4*(1), 79-97.

Kaynak, M. (2009). *İstihbaratta yeni stratejiler: örtülü operasyonlar*. Truva Yayınları.

Kent, S. (2002). *Stratejik istihbarat.* ASAM Yayınları.

Koca, H. İ. (2019). Stratejik istihbarat. *Akademik Tarih ve Düşünce Dergisi*, *6*(4), 2187-2198.

Koppa, M. E. (2021). Turkey, Gulf States and Iran in the Western Balkans: more than the Islamic factor?. *Journal of Contemporary European Studies*, *29*(2), 251-263

Mandaville, P., ve Hamid, S. (2018). *Islam as statecraft: How governments use religion in foreign policy*. Washington, DC: New Geopolitics, Foreign Policy at Brookings.

McDowell, D. (2008). *Strategic intelligence: a handbook for practitioners, managers, and users* (Vol. 5). Scarecrow Press.

MİT (t.y.). İstihbarat sözlüğü, Erişim tarihi: 25 Aralık 2023, https://www.mit.gov.tr/sozluk.html#A

Özdağ, Ü. (2017). *İstihbarat Teorisi*. Kripto Yayınları.

Progonati, E. (2017). The Balkan region as a new target for the Iranıan-Israeli political rivalry. *Bölgesel Araştırmalar Dergisi*, *1*(2), 199-219.

Radio Free Europe/Radio Liberty. (2023, June 20). Albania expels Iranian diplomats over 'terrorist threat'. Radio Free Europe/Radio Liberty. Retrieved from https://www.rferl.org/a/albania-iran-peoples-mujahedin-organization/32467998.html

Ransom, H. H. (1974). Review: strategic intelligence and foreign policy. *World Politics*, 27(1), 131-146.

Seren Yeşiltaş, M., (2021). Türkiye'nin stratejik istihbarat anlayişı: zihinsel ve kurumsal dönüşüm. *Uluslararası Güvenlik Kongresi: İstihbarat ve Güvenlik* (pp.196-198). Ankara, Turkey

Seren, M. (2023). *Stratejik istihbarat ve ulusal güvenlik.* Kadim Yayınları.

Seren, M., ve Yıldız, N. K. (2023). Bir diş politika araci olarak örtülü operasyonlar: ABD'nin Sovyet-Afgan savaşina müdahalesi (1979-89). *İstihbarat Çalişmaları ve Araştırmaları Dergisi*, *2*(2), 178-220

Stempel, J. D. (2007). Covert action and diplomacy. *International Journal of Intelligence and Counterintelligence*, *20*(1), 122-135.

Tokgöz, B. (2015). *Cihadın Mahrem Hikâyesi*. Ark Kitapları.

Treverton, G. F., Jones, S. G., Boraz, S., ve Lipscy, P. (2006). Toward a theory of intelligence: Workshop report. *Washington, DC*.

Türkçe sözlük (2023), Erişim tarihi: 25 Aralık 2023, htt'ps://sozluk.gov.tr/

İstihbarat Çalışmaları ve Araştırmaları Dergisi-İÇAD, 2024, 3(2):243-263 Araştırma Makalesi
Journal of Intelligence Research and Studies-İÇAD, 2024, 3(2): 243-263 Research Article
DOI: 10.61314/icad.1493890

EGMONT GRUBU STRATEJİK PLANI (2022-2027) KAPSAMINDA TERÖRİZMİN FİNANSMANI İLE MALİ İSTİHBARAT İLİŞKİSİ

Mücahit DİZMAN[*]

ÖZET

Terörizm, çağın en büyük tehditlerinden birisidir. Terörizmle mücadelede finansal kaynakların kati şekilde kesilmesi önemli bir hususdur. Ancak teknoloji ve insan zekâsının ulaştığı nokta, finansal kaynakların engellenmesine yönelik çalışmalarda kapsamlı bir mücadelenin ortaya konulmasını zorunlu kılmaktadır. Yapılan bu çalışmada, terörizmin finansmanıyla mücadelede mali istihbaratın önemi ve rolü değerlendirilmektedir. Bu kapsamda uluslararası mali istihbarat kuruluşu olan Egmont Grubu'nun Stratejik Planı (2022-2027) incelenerek Türkiye'ye yönelik birtakım tespit ve öneriler ortaya konulmaktadır. Nitel araştırma tekniklerinin kullanıldığı çalışma, temel olarak stratejik planda yer alan hedeflerin doküman analizi tekniğiyle incelenmesi yoluyla şekillenmiştir. Bulgulara göre Egmont Grubu'nun, terörizmin finansmanını önlemek amacıyla hazırladığı tematik alan ve stratejik hedeflerde, paydaşların iş birliği ile uyum içinde hareket etmesini kolaylaştırma, bilgi paylaşımında erişilebilirliği sağlama ve mali istihbarat araçlarının kullanımında teknolojiyi kolaylaştırıcı olarak işe koşma çabası önemlidir. Türkiye, terörizmin finansmanıyla mücadelede, istihbarat araçlarını etkin şekilde kullanmak için çabalamaktadır. Ancak etkinlik seviyesini artırmak için Egmont Grubu'nun vizyonu dikkatle ele almalıdır. Sonuç olarak Stratejik Plan, terörizmin finansmanıyla mücadelede mali istihbarat konusuna bütüncül bir yaklaşım sergilenmesi hususunda önemli ipuçları barındırmaktadır.

Anahtar Kelimeler: *Terör, Terörizmin Finansmanı, Terörizmin Finansmanıyla Mücadele, Mali İstihbarat, Egmont Grubu.*

RELATIONSHIP BETWEEN TERRORISM FINANCE AND FINANCIAL INTELLIGENCE WITHIN THE SCOPE OF EGMONT GROUP STRATEGIC PLAN (2022-2027)

ABSTRACT

Terrorism is one of the greatest threats of our age. Strict cutting of financial resources is an important issue in the fight against terrorism. However, the current state of technology and human intelligence necessitates a comprehensive struggle to prevent financial resources. In this study, the importance and role of financial intelligence in the fight against the financing of terrorism is evaluated. In this context, the Strategic Plan (2022-2027) of the Egmont Group, an international financial intelligence organization, is examined and some findings and

[*] Dr. Adayı, Polis Akademisi Başkanlığı Güvenlik Bilimleri Enstitüsü, Uluslararası Güvenlik Bölümü, mucahitdizman@gmail.com, ORC-ID: 0000- 0003-4600-8078.

Makale Başvuru Tarihi / Application Date: 02 Haziran 2024 / 02 June 2024

Makale Kabul Tarihi / Acceptance Date: 25 Haziran 2024 / 25 June 2024

suggestions for Türkiye are put forward. The study, in which qualitative research techniques were used, was basically shaped by examining the objectives in the strategic plan using the document analysis technique. According to the findings, the Egmont Group's efforts to facilitate the cooperation and harmony of stakeholders, ensure accessibility in information sharing, and use technology as a facilitator in the use of financial intelligence tools are important in the thematic areas and strategic objectives prepared to prevent the financing of terrorism. Türkiye strives to use intelligence tools effectively in the fight against the financing of terrorism. However, to increase the level of effectiveness, the Egmont Group's vision must carefully considered. As a result, the Strategic Plan contains important clues about taking a holistic approach to financial intelligence in the fight against the financing of terrorism.

Keywords: *Terrorism, Financing of Terrorism, Combating the Financing of Terrorism, Financial Intelligence, Egmont Group.*

GİRİŞ

Her ülkenin karşı karşıya kaldığı çeşitli iç ve dış tehditler mevcuttur. Böylesi durumlar, vatandaşları endişeye sevk etmesinin yanı sıra ekonomik refahına yönelik ciddi zararlara yol açmaktadır. Bu tehdit ve tehlikeler arasında küresel bir sorun olan terör, uzun yıllardır mücadele edilen önemli bir sorundur. Terörün varlığını sürdürmesi için en önemli unsurların başında finansal kaynak akışının sağlanması gelmektedir (Altun, 2015: ss.2-5). Bu bakımdan finansal akışın sağlanması için çeşitli suçlar açığa çıkmakta olup finansal suçların ulusal ve uluslararası sahada etki alanının genişlemesi karşısında, ülkelerin iş birliği içinde hareket etmesi zorunlu hale gelmektedir (Bural, 2022).

Terörizmin finansmanı devam ettiği sürece terör örgütlerinin eylem ve faaliyetleri de kesilmeden devam etmektedir. Bu bağlamda terör örgütleri için finansal kaynaklar, yaşamsal öneme sahip olup bu örgütler yasal ve yasadışı yollardan finansman sağlamaya devam etmektedir. Dolayısıyla terörün finansmanını önleme noktasında kara para aklama başta olmak üzere suç gelirlerini önlemek için mali istihbarat ön plana çıkmaktadır (Altun, 2015, s.3; Köksal, 2023). Mali istihbarat çalışmalarının denetlenmesi ve sorumlular arasında bilgi paylaşımının sağlanması noktasında ulusal düzeyde birimler kurulmuş ve çeşitli yetkilerle donatılmıştır. Bu kurumlar mali istihbaratın elde edilmesi, denetlenmesi ve analizi sonrası gerekli mercilere iletilmesinde başat rol oynamaktadır (Ikbal vd., 2020, s.82). Bu durum istihbaratın kaynaktan elde edilerek yerelden merkeze kadar iletimini kapsamaktadır. Bir toplumun güven içinde yaşamasını sağlayan farklı

unsurlar söz konusudur. Bu unsurlardan en önemli olanları çeşitli amaçlarla kurularak örgütlenmiş kurum ve kuruluşlardır. Örneğin ulusal düzeyde Mali Suçları Araştırma Kurulu (MASAK) ile uluslararası alanda ise Mali Eylem Görev Gücü (Financial Action Task Force - FAFT) ve Egmont Grubu, finansal suçlara karşı organize bir şekilde çalışmaktadır (Yüce ve Akkaya, 2020, s.41; İrdem, 2022). Başlangıçta suç gelirlerini (kara para) aklamayı önlemek ve şüpheli işlem bildirimlerini almak maksadıyla oluşturulan, günden güne terörizmin finansmanını önlemede de rol alan mali istihbarat birimleri dünya çapında gelişme göstermektedir. Özellikle mali bilgilerin elde edilip analiz edilmesiyle mali istihbarat birimleri önemli hale gelmiştir (Çelik vd., 2000, ss.10-46). Mali istihbarat birimlerinin etkin bir şekilde çalışması ve uluslararası iş birliğinin sağlanması için 9 Haziran 1995'te, 24 ülke ve 8 uluslararası kuruluşun katılımıyla Brüksel'de yer alan Egmont Sarayında uluslararası finansal suçlarla mücadeleyi merkezine alan Egmont Grubu kurulmuştur. Türkiye bu kuruluşa, 29 Haziran 1998'de üye olmuştur. Egmont Grubu, suç gelirlerinin aklanmasının önlenmesi ve terörizmin finansmanıyla mücadele (Anti-Money Laundering-AML/Combating The Financing Terrorism-CFT) amacıyla, üyeleri arasında mali istihbarat alışverişi sağlamaya yönelik teknolojik bir platform sunmaktadır (Egmont Grubu, 2020).

Terör örgütlerinin finansman kaynaklarının ve para aklama yöntemlerinin belirlenmesinde işe koşulan metodolojileri anlamak kritiktir (Turan ve Gemici, 2020, s.265). Bu hususta terörizmin finansmanı ile mücadele eden kurum, kuruluş ve grupların çalışmaları ile önerileri dikkate değerdir. Sınırları aşan ve uluslararası düzeyde büyük etkiye sahip olan terörizm unsurlarını engellemek için mali istihbarattan faydalanılması gerektiği düşüncesiyle hazırlanan bu çalışmada mali istihbarat konusunda uluslararası koordinasyonu ve teknik altyapıyı sağlayan Egmont Grubu'nun ileriye dönük (2022-2027) vizyonunu belirleyen Stratejik Planı incelenmektedir. Stratejik Planda yer alan tematik alan ve hedefler analiz edilerek Türkiye'nin mali istihbarat konusunda gelişmesine katkı sağlayabileceği varsayımı üzerinden hazırlanan çalışmada, buna yönelik beklentiler değerlendirilmiştir.

Nitel araştırma yöntemlerinin kullanıldığı çalışmada, Egmont Grubu'nun ortaya koyduğu Stratejik Plan ile Egmont Grubu, FATF ve MASAK'ın web sitesinde yer alan rapor ve diğer dokümanlar birincil

kaynaklar olarak ele alınmıştır. Literatürde yer alan güncel nitelikteki bilimsel çalışmalar ve konuyla ilgili kitaplar ikincil kaynakları oluşturmaktadır. Terörizmin finansmanıyla mücadelede mali istihbarat altyapısının güçlendirilmesinin önemli olduğu varsayımından yola çıkılarak hazırlanan çalışma, doküman analizine dayalı şekilde tasarlanmış betimsel araştırma ve analiz niteliğinde olup stratejik plandaki hedeflerin mevcut ilerlemeleri, gerçekleştirilebilme olasılıkları ve Türkiye'nin mali istihbarat konusunda ileriye dönük hedeflerine katkı sağlaması noktalarında analiz edilmiştir. Elde edilen bulgulara göre Türkiye, mali istihbarat konusunda ilerleme sağlamak istiyorsa uluslararası boyutta konuyla ilişkili kuruluşları yakından takip etmelidir. Bu kapsamda Egmont Grubu'nun Stratejik Planında yer alan teknolojik araçların mali istihbarat kullanımında etkinliğinin artırılması hususu, önemli bir yol gösterici olarak görünmektedir.

1. FİNANSAL İSTİHBARAT

Mali istihbarat kavramının tarihsel süreci yakın bir zamana dayanmaktadır. Kavram, ilk olarak 1989 yılında G7 ülkelerinin Paris Zirvesi toplantısında ortaya atılmıştır (Rudner, 2006, s.34). Mali istihbarat, *"kesin bir analitik titizlikle işlenmiş mali bilgi"* olarak tanımlanırken (Sathye ve Patel, 2007, s.392) mali suçlar ile mücadelede temel yöntemler arasında bulunmaktadır. Mali istihbaratın elde edilerek işlenmesinde, disiplinler arası bir alt yapıya sahip şekilde analitik ve esnek düşünme, raporlama, ekip çalışması ve iş birliği gibi birçok beceriye gereksinim duyulmaktadır (Ünal ve Altun, 2021, ss.575-579).

Egmont Grubu, Mali İstihbarat Birimi (Financial Action Task Force - FIU) hakkında ilk tanımını 1996'da Roma'daki Egmont Genel Kurulunda yapmıştır (Demirtaş, 2011, s.5). Burada yapılan tanımlama, yalnızca suç gelirlerinin aklanmasına odaklanmaktadır. Ancak 2004'te Guernsey Adasındaki toplantıda yapılan Kurul Toplantısında bu tanıma, terörizmin finansmanı kavramı eklenmiştir. Son yapılan FIU tanımına göre; suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadelede, suç gelirleri ile terörizme aktarılma ihtimali olan finansal bilgiler ve yasal düzenlemeler gereği, bildirilmesi zorunlu verileri almak, istemek, derlemek, analiz etmek ve elde edilen bulgularla sonuçları yetkili mercilerle paylaşmakla görevli ulusal düzeyde kurulmuş birimlerdir (MASAK, 2024a).

Bahsedilen tanım, çeviri farklılıkları dikkate alınmaksızın aynı minvalde anlam içerecek şekilde FATF Tavsiyeleri ve mevcut Metodolojilerinde, Avrupa Konseyi'nin 198 sayılı Sözleşmesinin 1/f maddesinde, Avrupa Birliği'nin 3'ncü Direktifinin 21'nci maddesinde ve Palermo Konvansiyonu'nun 7/1-b maddesinde yer almaktadır. Ayrıca bu metinlerde FIU'ya sahip olunmasının zorunluluk olduğuna dair ifadeler mevcuttur (Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü, 2024). Türkiye, 1998 yılında üyeliğe kabul edilmiş olup Hazine ve Maliye Bakanlığı bünyesinde yer alan MASAK, 5549 sayılı Kanun'un 19/1'nci maddesinin m bendinde yer alan düzenlemeler dolayısıyla yabancı ülkelerdeki eşdeğer kurumlarla bilgi ve belge değişiminde yetkilendirilmiştir (MASAK, 2024a).

Finansal sistemlerde her geçen gün ortaya çıkan gelişmeler pek çok finansal aracın ortaya çıkmasını sağlarken finansal suç işleyenler için de yeni teknikler geliştirmelerine olanak sağlamaktadır (Kiremitçi, 2023, s.108). Bununla beraber finansal sistemde işlenen suçların araştırılması yeni ve farklı seviyelerde mali istihbarat araç ve yöntemlerinin kullanılmasını ortaya çıkarmaktadır. Aynı zamanda finansal suçlara yönelik olarak resmi tedbirler alabilmek için yasal araçlar kullanılmaktadır. Bunlar arasında suç gelirlerinin aklanması, terörizmin finansmanı ve yolsuzluğu önlemeye yönelik kanunlar ile FATF Tavsiyeleri gibi yasal düzenlemeler mevcuttur (Sathye ve Patel, 2007, s.393).

Öte yandan suçtan sağlanan gelirlerin, ulusal ve uluslararası alanda meydana getirdiği zararlardan ötürü ülkeler, fiili olarak bazı önlemler almaya yönelmiştir. Bilhassa Soğuk Savaş sonrası uluslararası terör örgütleriyle organize suç örgütleri arasındaki karşılıklı ilişki artarken bunlara yönelik olarak finans kaynaklarının yok edilmesi önemli hale gelmiştir (Üstün, 2008, s.20). Bu kapsamda BM ve eşdeğer düzeydeki uluslararası otoritelerin tavsiyeleriyle devlet yapıları içinde mali istihbarat birimleri kurulmuş ve hâlihazırda, mali istihbaratın işleyişi, içeriği ve araçları gibi konuların gelişmesi ve daha etkili hale getirilmesi için çalışılmaktadır.

2. FİNANSAL İSTİHBARATIN TERÖRİZMİN FİNANSMANIYLA MÜCADELEDEKİ ROLÜ

Terörizmle mücadele ederken birçok yönteme ihtiyaç duyulmaktadır. Bu bakımdan terörizmin finansmanının önlenmesinde etkili bir politika oluşturulması gerekmektedir. Dolayısıyla terörizmin finansmanının

önlenmesinde *"baskılayıcı"* ve *"önleyici"* tedbirler birlikte kullanılmalıdır. Buna göre istihbarat, terörizmin önlenmesinde önleyici bir yöntem olarak bilinmektedir. İstihbarat, terörle mücadele eden ülkelerin ilk savunma hattını oluşturmakta ve adeta bir kılavuz vazifesi görmektedir (Flavius-Cristian ve Andreea, 2023, s.5). Terörizmin finansmanının önlenmesinde mali istihbarat, adli ve kolluk güçlerinin fiili müdahalelerinde yol gösterici niteliğiyle mühim bir yere sahip olup farklı istihbarat dallarıyla birleşerek terörizmin finansmanıyla mücadeleye önemli katkılar sunmaktadır (Pitteloud, 2003, ss.107-108).

Finansal incelemeler neticesinde terör örgütlerinin finansman hareketleri takip edilmekte olup böylelikle örgüt tarafından organize edilen saldırılar ve saldırıların failleri tespit edilebilmektedir (Şen, 2011). Finansal sistemlerde yetkin elemanların istihdam edilmesi, tecrübenin etkin kullanılması ve yapay zekâ teknolojilerinin entegrasyonu mali istihbarat sağlayıcılarının etkinliğiyle bağlantılıdır. Öte taraftan, terörizmin globalleşen doğası, terörle mücadele ve finansmanın önlenmesi süreçlerinde devletler arası istihbarat faaliyetlerinin uluslararası alanda iş birliğini elzem hale getirmektedir (Lutz ve Lutz, 2017, ss.275-278). Söz konusu iş birliği, hâkim devletler arasında, uluslararası kuruluşlar ve ulus-üstü yapılar ve tek tek egemen devletler arasında sağlanabilmektedir (Koncagül, 2022). Buna göre terörizmin finansmanının önlenmesinde; Birleşmiş Milletler (BM), Birleşmiş Milletler Güvenlik Konseyi (BMGK), Avrupa Birliği (AB), Avrupa Konseyi (AK), FATF, Egmont Grubu, Wolfsberg Grubu, Interpol, Europol, Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT), Dünya Bankası (WB) ve Uluslararası Para Fonu (IMF) önde gelmektedir (Altun, 2015, s.15). Belirtildiği üzere terörizmin finansmanının önlenmesinde birçok kurum, kuruluş, grup ve organizasyon bulunmakta olup bu araştırma kapsamında, terörizmin finansmanının önlenmesinde Egmont Grubu'nun stratejik planı ele alınmaktadır. Bu bölümde mali istihbaratın ulusal ve uluslararası alandaki rolleri üzerinde durulmaktadır.

2.1. Ulusal Alandaki Rolü

Türkiye, terörizmin finansmanının önlenmesi noktasında idari ve adli tedbirler almanın yanı sıra 2001 yılında, *"Terörizmin Finansmanının Önlenmesine Dair Uluslararası Sözleşme"*yi imzalayarak konuyu önemsediği ortaya koymuştur. Terörizmin finansmanıyla mücadele noktasında ise uluslararası alandaki uygulamaları takip etmekte olup ilk

olarak kara paranın önlenmesine yönelik çalışmalara odaklandığı görülmektedir. Bu doğrultuda 1997 yılında, 4208 sayılı Kanunla, doğrudan Hazine ve Maliye Bakanlığı'na bağlı olarak çalışan MASAK Başkanlığı kurulmuştur. Öte yandan terörizmin finansmanının önlenmesine ilişkin yeni koşullara göre kanuni düzenlemeler yapılmaya devam etmiş ve 11 Ekim 2006 tarihinde 5549 sayılı *"Suç Gelirlerinin Aklanmasının Önlenmesi Hakkında Kanun"* kabul edilmiştir (MASAK, 2018).

Türkiye'de mali suçlarla mücadelede uluslararası iş birliği, stratejik kararların ve yönlendirmelerin belirlenmesinde Mali Suçları Araştırma Koordinasyon Kurulu yetkilidir. MASAK, AML/CFT ve kitle imha silahlarının yayılmasının finansmanının önlenmesi meseleleri ile görevlendirilmiştir. MASAK'ın yetkilendirilmedeki tarihsel süreci FATF'a benzemektedir. Kuruluşunda AML'ye odaklanan kuruluş, zaman içerisinde yaşanan mihenk taşı olabilecek olaylar sonrasında terörizmin finansmanıyla mücadele ve son olarak kitle imha silahlarının yayılmasının finansmanının önlenmesi ile görevlendirilmiştir. Bu noktada kuruluşun misyonunun, dönemsel gerçekleşen konjonktürel olaylara göre geliştirildiğini söylemek mümkündür. MASAK, terörizmin finansmanı ile mücadele ederken finansal verilerin elde edilmesi, takip edilmesi, incelenmesi, analiz edilmesi ve gerekli hallerde yetkili mercilere iletilmesi ile görevlendirilmiştir. Ayrıca Türkiye'nin Egmont Grubu ile bağlantılı ve muhtıra imzalama yetkisine haiz tek mali istihbarat birimidir (MASAK, 2024b).

MASAK, 1 No'lu Cumhurbaşkanlığı Kararnamesi'nin 231'inci maddesinin tanıdığı yetki ve misyon çerçevesinde görevlerini yerine getirmektedir. Bu noktada yasal düzenlemeler ışığında görevlerini ifa etmektedir. Yapılan yasal düzenlemeler, mali suç doğuran herhangi bir eylemin terörist bireyler ile bağlantılı olması, bilinçli şekilde terör yapılarına destek sağlanması veya bilmeyerek dolaylı şekilde terörizm odaklarına destek olunması durumlarında cezalandırıcı, denetleyici ve düzenleyici normları oluşturmaktadır. Ayrıca MASAK, yasal düzenlemelerin yanı sıra rehberler, kitap, kamu spotu, broşür ve bilimsel makaleler ışığında çeşitli rolleri yerine getirmektedir (Dizman, 2024; MASAK, 2024b).

Mali istihbaratın katkıları bağlamında ulaşılan bilgiler doğrultusunda, terör örgütlerinin üyeleri ya da destekleyicileri hakkında birçok hukuki işlem yapılabildiği söylenebilmektedir. Bunlardan ilki, terörizme finans sağlayan ya da onu destekleyen kişi ya da şirketlerin malvarlıklarını dondurma

yetkisidir (Yıldırım, 2010, ss.2-8). 6415 sayılı Kanun'un 2'nci maddesine göre malvarlığının dondurulması; *"Malvarlığının ortadan kaldırılmasının, tüketilmesinin, dönüştürülmesinin, transferinin, devir ve temlik edilmesinin ve sair tasarrufi işlemlerin önlenmesi amacıyla, malvarlığı üzerindeki tasarruf yetkisinin kaldırılması veya kısıtlanmasını"* ifade etmektedir. Bu bağlamda mal varlığının dondurulmasıyla, terörizmin finansmanının önlenmesi amaçlanmakta, istihbarat bilgileri ışığında idari önlemler alınmaktadır. Yine adli makamlar tarafından alınan bir karar olan *"elkoyma"*, 5549 sayılı Kanun'un 17'nci maddesinde yer almaktadır. Bu karar, terörün finansmanı suçunun işlendiğine yönelik güçlü deliller bulunduğunda teröristlerin veya terör yapılarının malvarlıklarına elkonulmasına olanak sağlamaktadır.

Günümüzde birçok ülkede faaliyet sahasına sahip FIU'ların öncelikli görevi suç gelirlerinin aklanmasının önlenmesidir (Reznik vd., 2023, ss.95-100). Ancak yapılan yasal düzenlemeler ışığında dolaylı yoldan terörizmin finansmanının önlenmesine de katkı sağlamaktadır. Türkiye'de mali istihbarat görevini MASAK Başkanlığı yürütmektedir. MASAK'ın temel görev alanı; AML/CFT'ye yönelik suçun ortaya çıkarılması ve suçun önlenmesine yönelik özel yöntemlerin geliştirilmesi ile sektörler arası çalışmalar yapmaktır. Ayrıca her türlü mali veriyi toplamak-analiz etmek-değerlendirmek, derinlemesine mali araştırmalar yapmak ve bütün bunlar ışığında biriktirdiği büyük veri analizinde yer alanlardan elde edilen sonuçları ilgili/yetkili mercilerle paylaşmaktır. Bu faaliyetleri yürütürken politika oluşturabilme ve uygulama stratejileri geliştirebilme kabiliyetine sahip olan Başkanlık, belirli çerçevede yasal düzenlemeler (kanun-yönetmelik taslakları ve uygulamaya ilişkin idari düzenlemeler) hazırlayarak kurum ve kuruluşlar arası koordinasyonu sağlama suretiyle bilgi paylaşımı gerçekleştirmektedir. Ayrıca MASAK, ekonominin etkinliği ve toplumdaki suç oranlarının düşüşüne katkı sağlamak için teknolojiden en üst seviyede yararlanarak son dönemde mücadele kabiliyetini kayda değer düzeyde artırmıştır (MASAK, 2024b).

Terörizmin finansmanının önlenmesinde Türkiye'de MASAK Başkanlığı (2022), ulusal ve uluslararası alanda ilgili kurum ve kuruluşlarla iş birliği içerisindedir. Nitekim Türkiye'nin bulunduğu jeostratejik ve jeopolitik konum göz önüne alındığında somut adımlar ve önlemlerin alınması kaçınılmaz görülmektedir. Türkiye mali istihbarat alanında Egmont

Grubu'nun liderliğinde gerçekleştirilen çalışmalara yüksek oranda uyum göstermiştir. Egmont Grubu, pratik ve sistemli bilgi paylaşımı amacıyla ESW adıyla bilgisayar tabanlı veri paylaşım ve paydaşlar arası bilgi entegrasyon altyapısı kurmuştur. 1997 yılında faaliyete geçirilen sistem, sadece üyelerine açık olup Türkiye 1998 yılında üyeliğe kabul edilmiştir. Türkiye'nin 2001 yılında dâhil olduğu ESW altyapısında birçok ülkenin tipolojileri oluşturulmakla birlikte paydaşlarına da hızlı ve güvenilir bir gizli haberleşme altyapısı sunmaktadır (Dışişleri Bakanlığı, 2024). Egmont Grubu'nun üyeliği Mutabakat Muhtıraları ile sağlanmakta olup hâlihazırda 167'den fazla üyesi vardır. Anlaşma niteliğinde olmayan Mutabakat Muhtırası imzalanabilmesi için Türkiye'de MASAK Başkanlığı 5549 sayılı Kanun'un 19'ncu maddesi ile yetkilendirilmiştir. Bu kapsamda MASAK Başkanlığı, ilk muhtırasını Kuzey Kıbrıs Türk Cumhuriyeti (KKTC) ile imzalamıştır.

Türkiye'nin Egmont Grubu ile ilişkilerini yeni bir seviyeye çıkardığı dönem 2016 yılıdır. Bu yıl Egmont Grubu, 2016 Yıllık Olağan Genel Kurul Toplantısını Türkiye'de gerçekleştirmiştir. Toplantı öncesi Türkiye'nin o güne kadar *"48 ülkeyle mali istihbarat birimleri arası mutabakat muhtıraları imzaladığı ve bu konuda birçok ülkeyle görüşmelerin devam ettiği"* bizzat Hazine ve Maliye Bakanı Mehmet Şimşek tarafından vurgulanarak toplantıdan elde edilecek kazanımların önemli olduğu ifade edilmiştir (Demir, 2016). Bu toplantı Türkiye'nin uluslararası alanda finansal konulardaki hassasiyetini ortaya koymasının yanı sıra tanınırlığı konusunda da önemli çıktılar elde etmesini sağlamıştır. Bunun yanı sıra MASAK, 2021 yılında Malta, 2022 yılında Birleşik Arap Emirlikleri ve aynı yıl Çin Halk Cumhuriyeti Hong Kong Özel İdare Bölgesi İstihbarat Birimi ile *"Kara Para Aklama, Bağlantılı Öncül Suçlar ve Terörizmin Finansmanı ile İlgili Finansal İstihbarat Değişiminde İşbirliğine Dair Mutabakat Muhtırası"* imzalamıştır.

2.2. Uluslararası Alandaki Rolü

Terörizm ve organize suç örgütlerinin gelir elde etme teknikleriyle farklı yöntemlerle mücadele eden ülkeler, bilhassa 11 Eylül terör olaylarının yaşanmasından sonra terörizmin finansmanıyla mücadele politikalarında ortak yöntemler belirlemeye başlamıştır. Bu kapsamda, terörizmin finansmanıyla mücadele ederken mali istihbarat birimlerinin görev ve yetki alanlarının kapsamlı şekilde düzenlenmesi gerekmiştir. Örneğin, Amerika

Birleşik Devletleri, İngiltere ve Fransa, 11 Eylül saldırılarından sonra terörizmle mücadele politikasında revizyona gitmiş, güvenlik ve istihbarat stratejilerinde birtakım köklü ve kurumsal değişiklikler yapmıştır. Türkiye ise MASAK'ın yetkilerini değerlendirerek uluslararası sisteme ayak uyduracak şekilde yeniden yapılandırmıştır (Yamaç, 2009, s.156).

Reddington (2011, ss.2-6) tarafından Brezilya, Çin Halk Cumhuriyeti, Mısır, Endonezya, Meksika, Suudi Arabistan, Güney Afrika ve Birleşik Arap Emirlikleri olmak üzere birçok ülke örneğiyle yapılan çalışmada, ülkelerin terörizmin finansmanı ile mücadeleyi önemsediklerinde denetim mekanizmalarının etkin bir şekilde işlediği sonucuna ulaşılmıştır. Neticede her ülkenin, kendi devlet yapısı içinde terörizmle mücadele yöntemleri farklılık göstermekle birlikte genel olarak Ekonomik Kalkınma ve İşbirliği Örgütü (OECD) bünyesinde faaliyet gösteren FATF'ın tavsiyelerine uyulmaktadır (Marcus, 2022). Finansal İstihbarat Birimlerine küresel olarak bakıldığında üyeliği, FATF tarafından tavsiye edilen Egmont Grubu'ndan bahsetmek önemlidir (Brewczyńska, 2021, ss.3-6). Egmont Grubu mali istihbarat birimleri arasında bilgi değişimi ve akışını sağlamayı amaç edinmiş oluşum olarak terörizmin finansmanının önlenmesine yönelik stratejiler geliştirmektedir (Egmont Grubu, 2024). Bu bağlamda terörizmin finansmanının önlenmesinde ulusal düzeyde ve uluslararası alanda da ortak bir anlayış oluşturmaya çalışılmakta, yasal dayanaklarla ve öncü kuruluşların tavsiyeleri ile tedbirler almaya çalışılmakta ve mali istihbaratla elde edilen bilgiler ışığında hareket etmektedir.

Egmont Grubu, başlangıçta şüpheli işlem bildirimlerinin uluslararası koordinasyonu ve bu sistemin teknik altyapısının kurulmasına odaklanmaktaydı. Bu noktada ulusal FIU'ların kurulmasına öncülük eden kuruluşlar arasında yer almaktadır. Sonraki süreçte sadece teknik altyapı değil personel eğitimi ve tecrübe bilgisinin aktarımına yönelik de önemli eğitim ve konferanslar yürütmüştür. Bu çalışmalar, genellikle üye ülkelerin yetkili ve temsilcilerinin katılımıyla gerçekleştirilmiş olup suç gelirleri ve terörizmin finansmanıyla mücadele literatürüne önemli katkı sunmaktadır. Bahsedilen faydalar elde edilirken birçok teknik uygulanmakta olup bunlar arasında 5 adet *"çalışma grubu"* oluşturulması yöntemi en etkili olanıdır. Bu yöntemle, mevzuat, bilgi işlem ve benzeri stratejik alanlar ayrı çalışma gruplarına ayrılmıştır. Bu çalışma gruplarının temel perspektifinde mali istihbaratın etkinliği ve konu içerisindeki bulunduğu nokta temel

alınmaktadır. Bu gruplar Egmont Grubu'nun yürütme organı görevindedir (MASAK, 2024a).

Egmont Grubu'nun hizmet odağına yönelik birçok çalışma, teknik altyapıya odaklıdır. Egmont Grubu, FIU'lar arasındaki bilgi paylaşımını sağlayan teknolojik ağı, kapsamlı ve sistemli şekilde geliştirmekte ve çağa ayak uydurması adına güncellemektedir. Bu kapsamda iki önemli gelişme mevcuttur. İlki, 1997 yılında faaliyete geçirilen ve Egmont Güvenlik Ağı (Egmont Secure Web-ESW) olarak bahsedilen FIU'lar arasındaki bilgi değişimini güvenlik ve hız olarak üst seviyeye taşıyan bir bilgisayar ağıdır. Diğeri ise sistemli bilgi akışını ve değişimini sağlamaya odaklı Mutabakat (Memorandum of Understanding-MOU)'tır (MASAK, 2024a).

3. EGMONT GRUBU STRATEJİK PLANI (2022-2027)

Egmont Grubu (2022) tarafından hazırlanan ve 2022-2027 yıllarını kapsayan Stratejik Plan, kilit paydaşların bir araya gelerek kapsamlı bir istişare süreci neticesinde geliştirilen Kurumun gelecek vizyonunu ve misyonunu belirleyen nihai strateji belgesidir. Bu Stratejik Plan, önceki sürümlere ve Egmont Grubu'nun değişmeden kalan temel misyonuna dayanmaktadır. Stratejik Plan beş yıllık bir dönemi kapsamakta fakat gerekli görüldüğü takdirde güncellenip yenilenebilmektedir. Stratejik Planda, Egmont Grubu faaliyetlerinin önümüzdeki beş yıl boyunca koordine edileceği çerçeveyi sağlayan *"Dört Tematik Eylem Alanı"* dikkat çekmektedir. Bunlar şöyledir (Egmont Grubu, 2022):

a. FIU'lar arasında etkili bilgi alışverişi için genel çerçeveyi geliştirmek,
b. Uluslararası paydaşlar ve ortaklık sağlanan yapılarla iş birliğini güçlendirmek,
c. Yeni veya gelişmekte olan AML/CFT yöntemleri ve trendleri hakkında bilgi geliştirmek ve teşvik etmek,
ç. Grup üyelerine ve aday FIU'lara yönelik desteği artırmak.

Egmont Grubu, finansal kuruluşlar arasında bilgi alışverişine adanmış bir platform olarak küresel ölçekte FIU'lar arasında doğrudan operasyonel ve stratejik öngörü ile istihbarat alışverişini kolaylaştıran ulus üstü bir organizasyondur. Üye ülkelerin birbiriyle yakın çalışması, iş birliğinden yola çıkması ve iş birliğine doğru yönelmesi/ilerlemesi oldukça mühimdir. Bu bağlamda Egmont Grubu, 2022-2027 Stratejik Planı çerçevesinde bazı

stratejik hedefler belirlemiştir. Bu hedefleri aşağıda yer verildiği gibi açıklamak mümkündür. Stratejik hedefler şöyledir:

a. Mevcut stratejik ortaklıkların güçlendirilmesi, büyütülmesi ve diğer kilit paydaşlarla yeni ortaklıkların oluşturulmasına ilişkin çalışılmaların yapılması,

b. Artan veri toplama, bilgi paylaşımı ve operasyonel bilgi alışverişini sağlayan yeni ortaklıkların geliştirilmesi yoluyla FIU üyelerinin faydalı bilgi ve istihbarata erişiminin artırılması,

c. Grubun FATF ile olan ilişkilerinin derinleştirilerek ortak çalışma alanların çeşitlendirilmesi,

ç. Özel sektör, akademi, teknoloji ve konunun uzmanları dâhil olmak üzere geleneksel olmayan ortaklarla belirli konular ve projeler hakkında ilişki kurulması ve bu ilişki ağının genişletilmesine yönelik çalışmaların yapılması,

d. Gelecekteki güvenlik açıkları ve tehditleri belirleme ile mücadele yeteneğinin güçlendirilmesine yönelik çalışmalarının yapılması,

e. Terörizmin finansmanı ile mücadelede iyi uygulamalar geliştirilerek tüm paydaşların teşvik edilmesi,

f. Çeşitli ortak kuruluşlar arasında iyi uygulamaların yaygınlaştırılması,

g. Gelecek beş yıl boyunca üyelere her konuda etkin destek sağlanması ve karapara aklama, terörizmin finansmanı gibi ciddi suçların kapsamlı bir şekilde ele alınması,

ğ. Finansal kuruluşlar arasında etkili bilgi alışverişi için çerçevenin geliştirilmesi,

h. Uluslararası kuruluşlarla iş birliğinin teşvik edilmesi ve ortaklıklara daha hedefli bir yaklaşımın ortaya konulması,

ı. Operasyonel sonuçlara daha fazla odaklanılması,

i. Karşılıklı değerlendirme sonuçları ile dış tehditlerden ve eğilimlerden belirlenen konularla ilgili iyi uygulamaların geliştirilmesi ve teşvik edilmesi,

j. Grubun operasyonel bir şekilde iş birliği ve bilgi paylaşımını kolaylaştırılıp Kamu-Kamu İşbirliği ve Kamu-Özel Ortaklıkları ile nasıl ilişki kurabileceği ve iş birliği yapabileceğinin anlaşılması,

k. Üyelerin ve Grubun, kritik, yüksek riskli, yeni ve ortaya çıkan eğilimler ile tehditler üzerinde çalışmasına, plan ve projeleri bunlara göre değiştirmesine izin vermek için yeterli alan sağlanması,

l. Yeni ortaya çıkan trendleriyle başa çıkmak ve bunları keşfetmek için uygun teknolojinin elde edilmesiyle üyelere bu teknolojilerden mümkün olduğunca yararlanmaları ve haberdar olmaları için destek sağlanması.

Stratejik Plan aracılığıyla Egmont Grubu kendisini daha verimli ve etkili bir küresel karapara aklamayla mücadele ve terörizmin finansmanıyla mücadele ekosisteminin merkezinde konumlandırmayı amaçladığı gibi önümüzdeki beş yıl boyunca güvenilir, çeşitliliğe sahip ve kapsayıcı bir kuruluş olmaya kendini adamıştır. Neticede 2018-2021 Stratejik Planı, arzu edilen düzeyde etkinlik için geniş bir çerçeve sağlarken, 2022-2027 Stratejik Planı, stratejik yönlendirme, hedefleri sonuçlara dönüştürme ve sonuçta küresel ölçekteki rolünü güçlendirme yoluyla önceki planın girişimlerine dayanmaktadır (Egmont Grubu, 2024).

4. TARTIŞMA

Alanyazın incelendiğinde terörün ve terörizmin global ölçekli bir sorun olduğu anlaşılmaktadır. Terörle mücadele söz konusu olduğu zaman terörün finansmanıyla mücadele, temel girişim olarak görülmektedir. Araştırmacılar terörizmin finansmanının önlemesine yönelik olarak uygulamada hala çok eksik olduğunu belirtmekle birlikte etkin ve verimli bir mücadele için özerk, esnek ve proaktif yaklaşım sergileyebilecek istihbarat birimlerine ihtiyaç olduğunu vurgulamaktadır (Ünal ve Altun, 2021, s.573). Bu hususta ulusal ve uluslararası alanda koordineli çalışmanın ne denli mühim olduğu tahmin edilebilmektedir.

Günümüzde istihbarat, terörle mücadelenin pratik ve teorik yönünün merkezine yerleşmiştir (Marcus, 2022). Teknolojiyle birlikte insanların bilgiye ulaşmasının ve karmaşık bilgileri algılamasının kolaylaşmış olması, kompleks ortamların artmasına ve terörle mücadele ortamının genişlemesine sebep olmuştur. Bu durum mücadeleyi zorlaştırmasının yanı sıra mücadele alanının genişlemesini sağlamıştır. Haliyle, pratik ve teorik uygulamalardaki mücadele yöntemlerinin gelişmesine sebep olduğu gibi istihbaratı da önemli

bir konuma yükseltmiştir. Nihayetinde mali istihbaratın toplanması, elde edilmesi ve analiz edilmesi konuları terörle mücadelede başat rol oynar hale gelmiştir.

İstihbarat üzerine yapılan çalışmalar terörizmin finansmanının önlenmesine dair kayda değer gelişmeler ortaya çıktığını göstermektedir. İstihbarat kurumlarının faaliyetleri sayesinde önleyici müdahalelerle terörizmle mücadelede önemli ilerlemeler kaydedilmektedir (Olgunsoy, 2022, ss.43-55). Terörizmle mücadelede işe koşulan askeri yöntemlerle birlikte mali istihbaratın ön plana çıkarılması terörle mücadelede terörizmin finansmanının önlenmesine önemli faydalar sağlamaktadır (Ergin, 2019, s.1).

Mali istihbarat birimlerine yönelik yapılan değerlendirmeler, bu birimlerin çeşitli kaynaklardan toplanan finansal bilgileri işleyerek kara para aklama ve diğer öncül suçları (NE DEMEK OLDUĞUNU AÇIKLA) tespit etmek ve veri değişimini sağlamak için bir platform sağladığı yönündedir. Aynı zamanda mali istihbarat birimlerinin çerçevesi, finansal kurumların yanında finansal olmayan kuruluşlardan sağlanan bilgileri de işleme konusunda kapsamlı hale getirilmiştir (Akkaya ve Yüce, 2023, s.265). Buna göre terörizmin finansmanında her türlü enformasyon göz önünde bulundurularak etkin bir yaklaşım sergilenmektedir. Diğer bir deyişle terörizmin finansmanı ile mücadele ederken hukuki, mali, adli ve idari birimlerin yanında enformasyon sağlayacak tüm kaynak ve verilerin değerlendirilerek terör faaliyetlerine ilişkin açıklar bırakılmaması gerekmektedir.

Yapılan araştırmalar incelendiğinde mali istihbarat birimlerinin üç temel hedefi yerine getirmesi, suçla mücadelede büyük önem taşımaktadır (Bulut vd., 2015, ss.94-101; Karatay ve Kapusızoğlu, 2011, s.116). Bu ilkeler şu şekildedir:

a. Yurt içinde ve yurt dışındaki FIU ve benzeri diğer kurum ve kolluk kuvvetleri ile bilgi alışverişinde Egmont Grubu, ilkeleri ve FATF Tavsiyeleri doğrultusunda hareket etmelidir.

b. Finansal suçlarla ilgili eğilim ve kalıpların belirlenmesine yönelik olarak FATF standartları ve metodolojisine uygun olarak stratejik analiz doğrultusunda hareket edilmelidir. Bu sayede gerçekleştirilenler raporlanarak ölçülebilir hale getirilmelidir.

c. Teşebbüs de dâhil olmak üzere suç teşkil eden davranışlara ait karapara aklama, terörizmin finansmanı ve kitle imha silahlarının yayılması dâhil istihbarat toplanarak yetkili mercilerle paylaşılmalıdır.

Bu maddeler dikkatle incelendiğinde terörizmin finansmanının önlenmesinde sınır ötesi girişim ve çabaların, sürdürülebilir, gerçekçi ve sonuçlarının kontrol edilebilir olması gerektiği anlaşılmaktadır. Dolayısıyla mali istihbarat birimleri, FATF ve Egmont Grubu'nun çalışmalarını izleyerek stratejilerini belirlemelidir.

SONUÇ

Terörizmle mücadele, bir ülkenin maddi ve manevi kaynakları üzerinde birçok değişime yol açmaktadır. Bir toplumun huzur ve güven içinde yaşaması ile maddi kaynaklarının korunmasının sağlanması noktasında, terörizm tehdidi söz konusu olduğunda herkesin sorumluluk alması gereken bir durum ortaya çıkmaktadır. Terörizmle mücadele politikalarından sonuç alınması için ise finansman kaynaklarının öncelikli olarak engellenmesi gerekmektedir. Bu kapsamda devletler genellikle "mali suçlarla mücadele" misyonu altında suç gelirlerinin aklanması ve terörizmin finansmanıyla mücadele yürütmektedir. Dolayısıyla hedeflerine ulaşabilmek için mevcut araçların kullanılması ve geliştirilmesini önemsemektedirler. Mali istihbarat sağlanması da bunlardan birisidir. Mali istihbarat sayesinde devletler organize suç şebekelerinin ve terör örgütlerinin finansman kaynaklarına yönelik önlemler alabilir veya saldırılar düzenleyerek ket vurabilir. Bu kapsamda devletlerin mali istihbarat politikalarının mevcut konjonktürü yakalaması ve uluslararası bağlamda fayda sağlayabilmesi için belirli bir vizyonun oluşturulması ya da mevcut olanların takip edilmesi önemlidir. Çalışma kapsamında mali istihbarat konusunda uluslararası koordinasyonu sağlayan ve teknolojik altyapı sunarak etkin mücadelenin vizyonunu belirleyen Egmont Grubu'nun gelecek perspektifini ortaya koyan Stratejik Planı analiz edilmiştir.

Mali istihbarat, genellikle kolluk kuvvetlerinin faaliyetleri kapsamında değerlendirilmektedir. Mali istihbarat terimi ilk olarak vergi kaçakçılığı ve kara para aklama suçları kapsamında kullanılmıştır. Ancak OECD, FATF ve Egmont Grubu'nun koordineli çalışmaları sonucunda mali istihbaratın önemli ortaya çıkarılmış olup etkinlik seviyesinin artırılmasına yönelik politikaların oluşturulmasında Egmont Grubu'na destek olunmaktadır.

Egmont Grubu ise mali istihbaratı, birincil araç olarak kullanmakta olup uluslararası düzeyde etkinliğini artırmak için kendi vizyonuna ve üye devletlere katkı sağlayacak planlar belirlemiştir. Bu planlardan anlaşıldığı üzere ilerleyen süreçte mali istihbaratın önemi daha fazla anlaşılacak olup Egmont Grubu, uluslararası düzeyde mali istihbaratın etkin ve hızlı şekilde sağlanabilmesinde önemli roller üstlenecektir. Küresel bilgi ağı altyapısını oluşturarak, genişleterek ve koordine ederek tüm Dünyadan veri erişimine sahip olan Egmont Grubu'nun önemi, üyeliğine dâhil olan FIU'ların koordinasyonunu sağlamasıyla ortaya çıkmıştır.

Egmont Grubu belirlediği Stratejik Planlarla vizyonunu geliştirerek misyonunu güçlendirmeye çalışmaktadır. Bu amaçla en son yayınladığı 2022-2027 yıllarını kapsayan Stratejik Plan önemli bir yere sahiptir. Çalışma kapsamında analiz edilen Stratejik Planda belirlenen dört temel anahtar nokta dikkat çekmektedir. Bu anahtar noktaların ilkinde, FIU'ların varlıklarını daha fazla hissettirerek etkinlik düzeylerini yükseltmesi hedeflenirken bunu yaparken ikili ve çok taraflı bilgi paylaşımını kolaylaştırıcı projeler ortaya çıkarmaları beklenmektedir. Bu durumun önemli örneğini Amerika Birleşik Devletleri (ABD), 2022 yılında sentetik veri paylaşımı başlığı altında oluşturduğu projeyle deneyimlemiştir. ABD, bu projeyle bilgi paylaşımındaki en uygun zemini yakalamayı hedeflemiştir. İkinci olarak, uluslararası paydaşlarla ilişkilerin güçlendirilmesi hususunun mali istihbaratta önemli yere sahip olduğu değerlendirmesinden yola çıkarak FIU'ların elde ettiği bilgilerin önemine daha fazla dikkat çekilmesinin gerekliliği vurgulanmaktadır. Bu madde kapsamında Egmont Grubu, FATF ile olan ilişkilerinin daha fazla geliştirilmesine yönelik çalıştaylar düzenleyerek ilişkilerin geliştirilmesine yönelik düzenleyici kuruluşları, ülkelerin ilgili kurumlarını, akademisyenleri ve özel sektörün öncülerini toplantılara davet ederek etkileşim içerisindeki aracıları çoğaltmanın yolunu aramaktadır. Üçüncüsü, güncel AML/CFT metotlarını uygulamaya yönelik iyi uygulama örneklerinin ortaya çıkarılması için çalışmalar yapılmasıdır. Bu kapsamda Egmont Grubu, 2023 yılında FATF ve üyelerinin katıldığı bir dizi toplantı düzenlemiş olup henüz somut sonuçlarının yer aldığı bir rapor sunmamıştır. Egmont Grubu burada uzun vadeli hedefler belirlediği için kısa vadede sonuçların ortaya konulması beklenmemektedir. Son olarak dördüncü anahtarda, FIU'ların AML/CFT noktasında küresel erişim genişliklerinin artırılmasına yönelik adımların atılmasıdır. Bu noktada FIU'lara büyük görev düşmekte olup birinci hedefteki gibi kendilerine ait yetki alanlarını

genişletmekte ve etki düzeylerini güçlendirmekte proaktif bir yaklaşım benimsemeleri gerekmektedir. Stratejik plana göre Egmont Grubu, bu tarz atılımların arkasında duracağını vurgulamaktadır. Ayrıca bu hedef kapsamında Egmont Grubu, Afrika ve Asya'daki FIU'ların girişimlerini yakından takip edeceğini de hedefleri arasına eklemiş olup Erik Kennes ve Ninan Wilen gibi önemli Afrika uzmanı akademisyenlerin *"Afrika Özeti"* başlıklı yazı serilerini yayınlamaya başlamıştır.

Terörizmle mücadele oldukça karmaşık bir süreç olup esnek bir yapı içinde bulunmak yapılan çalışmaların hayata geçirilmesini kolay hale getirecektir. Bu noktada mali istihbarat, diğer istihbarat faaliyetlerini tamamlayıcı niteliktedir. Aynı zamanda terör örgütlerinin niteliği de nasıl bir mücadele planı oluşturulacağını ve strateji izleneceğini belirlemektedir. Türkiye, terörizmin finansmanı ile mücadele ederken uluslararası alandaki düzenlemeler ve uygulamalardan yararlanmakta ve kendine özgü bir sistem geliştirme yolunda ilerlemektedir. Fakat Türkiye'de mali istihbarat alanında yapılan çalışanların nicelik ve nitelik yönünden hala geliştirilmesi gerektiği anlaşılmaktadır. Bu noktada yapılan araştırmalardan elde edilen sonuçlar, ulusal FIU olan MASAK'ın, terörizmin finansmanıyla mücadele çerçevesinde veri toplaması, değerlendirmesi, raporlar hazırlaması ve bunları dağıtması konularında rol alması, başka roller almaması gibi görüşlerin mevcut olduğunu ortaya koyulmaktadır. Öte yandan bu görevi ifa ederken gereksinim duyduğu finansal bilgilere erişim sağlanması için mali istihbarattan yararlanması gerektiği şeklindedir.

Sonuçta terörizmin finansmanının önlenmesi noktasında pek çok argüman mevcut olup bunların etkin bir şekilde ve kalıcı olarak hayata geçirilmesi önemlidir. Bu noktada MASAK'ın mali istihbarat konusunda daha fazla proaktif bir yaklaşımı gündemine alarak daha güçlü alternatifler geliştirmeye yönelik çalışmalar gerçekleştirmelidir. Nitekim MASAK'ın 2022 Yılı Faaliyet Raporu incelendiğinde; 6'ncı sayfada mali istihbarat faaliyetlerine yaklaşımda geniş bir perspektif benimsenerek bu faaliyetlerin yanı sıra düzenleyici, denetleyici ve eğitici rolünün olduğu vurgulanmıştır. Ancak raporun genelinde yer alan temel hedeflere bakıldığında, MASAK'ın istihbarat birimi olarak daha güçlü olması gerektiği ve bu kapsamda yeniden yapılandırılması hususu vurgulanmaktadır. Hedeflerin Egmont Grubu'nun stratejik hedefleriyle zamanlama ve menzil olarak kesişmesinden kaynaklı stratejik plandaki dört temel temada belirlenen destekleyici hükümlerden

faydalanmaktan da kaçınılmayarak uluslararası entegrasyon konusunda etkili bir adım atılmalıdır.

KAYNAKÇA

Akkaya, Hüseyin ve Yüce, M. (2023). Mali suçlarla mücadelede mali istihbaratın rolünün değerlendirilmesi. *Bilgi Sosyal Bilimler Dergisi*, *25*(2), 262-285.

Altun, M. Ö. (2015). *Terörizmin finansmanı ile mücadelede finansal istihbaratın rolü.* (Yayınlanmamış Doktora Tezi). Kütahya Dumlupınar Üniversitesi Sosyal Bilimler Enstitüsü.

Brewczyńska, M. (2021). Financial ıntelligence units: reflections on the applicable data protection legal framework. *Computer Law and Security Review,* (43), 1-14, https://doi.org/10.1016/j.clsr.2021.105612.

Bulut, S., Özkan, H. ve Çimi, M. (2015). FATF ve egmont grubu özelinde türkiye'nin karapara serüveninde güncel değerlendirmeler. *Vergi Sorunları Dergisi, 38*(323), 92-103.

Bural, E. B. (2022). "Türkiye'de Terörizm ve Radikalleşme Literatürü Üzerine Bir İnceleme: Akademik Makaleler". Terörizm ve Radikalleşme Araştırmaları Dergisi, 1(1), 67-101.

Çelik, K., Koçağa, I. ve Güler, K. (2000). *Kara para aklama tanımı, aşamaları, yöntemleri ve ilgili uluslararası çalışmalar.* MASAK Yayınları.

Demir, R. (2016). *Mali istihbaratçılar Türkiye'ye geliyor*. Erişim tarihi: 4 Mayıs 2024. https://www.aa.com.tr/tr/ekonomi/mali-istihbaratcilar-turkiyeye-geliyor/77620.

Demirtaş, İ. (2011). *FATF üyesi bazı ülke mali istihbarat birimlerinin yapısı, fonksiyonları ve MASAK ile mukayesesi*. MASAK Yayınları

Dış İlişkiler ve Avrupa Birliği Genel Müdürlüğü. (2024). *Sözleşmeler*. Erişim tarihi: 15 Nisan 2024. https://diabgm.adalet.gov.tr/arsiv/sozlesmeler/sozlesmeler.html.

Dışişleri Bakanlığı. (2024). *Kara paranın aklanmasıyla mücadele konusundaki temel uluslararası metinler ve oluşumlar*. Erişim tarihi: 3 Nisan 2024. https://www.mfa.gov.tr/default.tr.mfa.

Dizman, M. (2024). "Terör Örgütlerinin Finansman İhtiyacı". GÜ İslahiye İİBF Uluslararası E-Dergi, 7(7), 13-34.

Egmont Grubu. (2020). *About*. Erişim tarihi: 24 Nisan 2024. https://www.Egmontgroup.org/en/content/about.

Egmont Grubu. (2022). *Egmont group strategic plan 2022-2027*. Erişim tarihi: 13 Mayıs 2024. https://egmontgroup.org/wp-content/uploads/2022/08/33.-Egmont-Group-Strategic-Plan-2022-2027-1.pdf.

Egmont Grubu. (2024). *The 2022-2027 Egmont Group Strategic Plan is now available – turning aspirations into outcomes*. Erişim tarihi: 11 Ocak 2024. https://Egmontgroup.org/news/turning-aspirations-into-outcomes-the-2022-2027-Egmont-group-strategic-plan-is-no.

Ergin, A.D. (2019). *Terörizmin finansmanının önlenmesinde malvarlıklarının dondurulması.* (Yayınlanmamış Doktora Tezi). Ankara Üniversitesi Siyasal Bilimler Fakültesi.

Flavius-Cristian, M. ve Andreea, C. M. (2013). The role of ıntelligence in the fight against terror. *European Scientific Journal, 9*(2), 1-11.

Ikbal, M., Irwansyah, I., Paminto, A., Ulfah, Y. ve Dio C. D. (2020). Financial ıntelligence: financial statement fraud in Indonesia. *Journal of Intelligence Studies in Business, 10* (3), 80-95.

İrdem, İ. (2022). Terrorist organizations exploiting religion within the scope of hybrid warfare: the case of FETO and DAESH. Security Issues in the Context of Political Violence and Terrorism of The 21st Century. Acar, H., & Deniş, H.E. (Ed). UK: Cambridge Scholars Publishing.Karatay, Ö. ve Kapusızoğlu, M. (2011). Mali ve ekonomik suçların terörün finansmanı bağlamında değerlendirilmesi. *Ekonomi Bilimleri Dergisi, 3*(1), 115-121.

Kiremitçi, O. (2023). Karşılaştırmalı hukukta şüpheli işlem bildirimi ve mali istihbarat birimleri. *Yıldırım Beyazıt Hukuk Dergisi*, (1): 107-163.

Köksal, T. D. (2023), *Terörizmin finansmanı ile mücadele konulu koordinasyon toplantılarına ilişkin nihai birleşik rapor.* Erişim tarihi: 13 Nisan 2024. www.coe.int/tr/web/ankara.

Lutz, J.M. ve Lutz, B.J. (2017). Terörizm, Çağdaş güvenlik çalışmaları içinde (Ed. Allan Collins). *Uluslararası İlişkiler Kütüphanesi*. 273-288.

Marcus, A. (2022). *Financial ıntelligence units (FIUs): Effective İnstitutional design, mandate and powers*. Erişim tarihi: 23 Mayıs 2024. https://knowledgehub.transparency.org/assets/uploads/helpdesk/FinancialIntelligence-Units_Design-Mandate-Powers_2019_PR.pdf.

MASAK. (2018). *Uluslararası mücadele*. Erişim tarihi: 21 Ocak 2024. https://masak.hmb.gov.tr/uluslararasi-mucadeletf.

MASAK. (2022). *Finansal kuruluşlara yönelik terörizmin finansmanıyla mücadele rehberi.* Erişim tarihi: 13 Mayıs 2024 https://masak.hmb.gov.tr/duyuru/finansal-kuruluslara-yonelik-terorizmin-finansmaniyla-mucadele-rehberi-26-11-2022-tarihinde-yayimlandi.

MASAK. (2023). *2022 yılı Faaliyet Raporu*. Erişim tarihi: 1 Şubat 2024. https://ms.hmb.gov.tr/uploads/sites/12/2023/04/2022-Faaliyet-Raporu.pdf.

MASAK. (2024a). *Egmont Grubu*. Erişim tarihi: 7 Nisan 2024. https://masak.hmb.gov.tr/egmont-grubu.

MASAK. (2024b). *Sunuş*. Erişim tarihi: 9 Mayıs 2024. https://masak.hmb.gov.tr/sunus.

Olgunsoy, F. (2022). *Terörle mücadelede istihbarat faaliyetlerinin özgürlükler rejimine etkisi: Türkiye, Birleşik Krallık, Amerika Birleşik Devletleri.* (Yayınlanmamış Doktora Tezi). İstanbul Üniversitesi Sosyal Bilimler Enstitüsü.

Pitteloud, J. (2003). The role of ıntelligence in coordinationg the fight against terrorist financing. *Combating the financing of terrorism within the EAPC/PFP framework, CiSP proceedings, swiss EAPC/PfP workshop on combating the financing of terrorism.* 27-28 Kasım 2003. 107-108.

Reddington, B. J. (2011). *Assessing the true effectiveness of AML/CFT controls in developing countries.* (Yayınlanmamış Yüksek Lisans Tezi). Georgetown University, Washington, ABD.

Reznik, O., Utkina, M. ve Bondarenko, O. (2023). Financial intelligence (monitoring) as an effective way in the field of combating money laundering. *Journal of Money Laundering Control*. *26*(1), 94-105.

Rudner, M. (2006). Using financial ıntelligence against the funding of terrorism. *International Journal of Intelligence and Counter Intelligence*. *19*(1), 32-58.

Sathye, M. ve Patel, C. (2007). Developing financial intelligence: an assessment of the FIUs in Australia and India. *Journal of Money Laundering Control*. *10*(4), 391-405.

Turan, D. ve Gemici, E. (2020). Terörizmin finansman kaynakları ve kara para aklamanın terörizmin finansmanındaki rolü. *Anadolu Üniversitesi Sosyal Bilimler Dergis., 20*(2): 257-278.

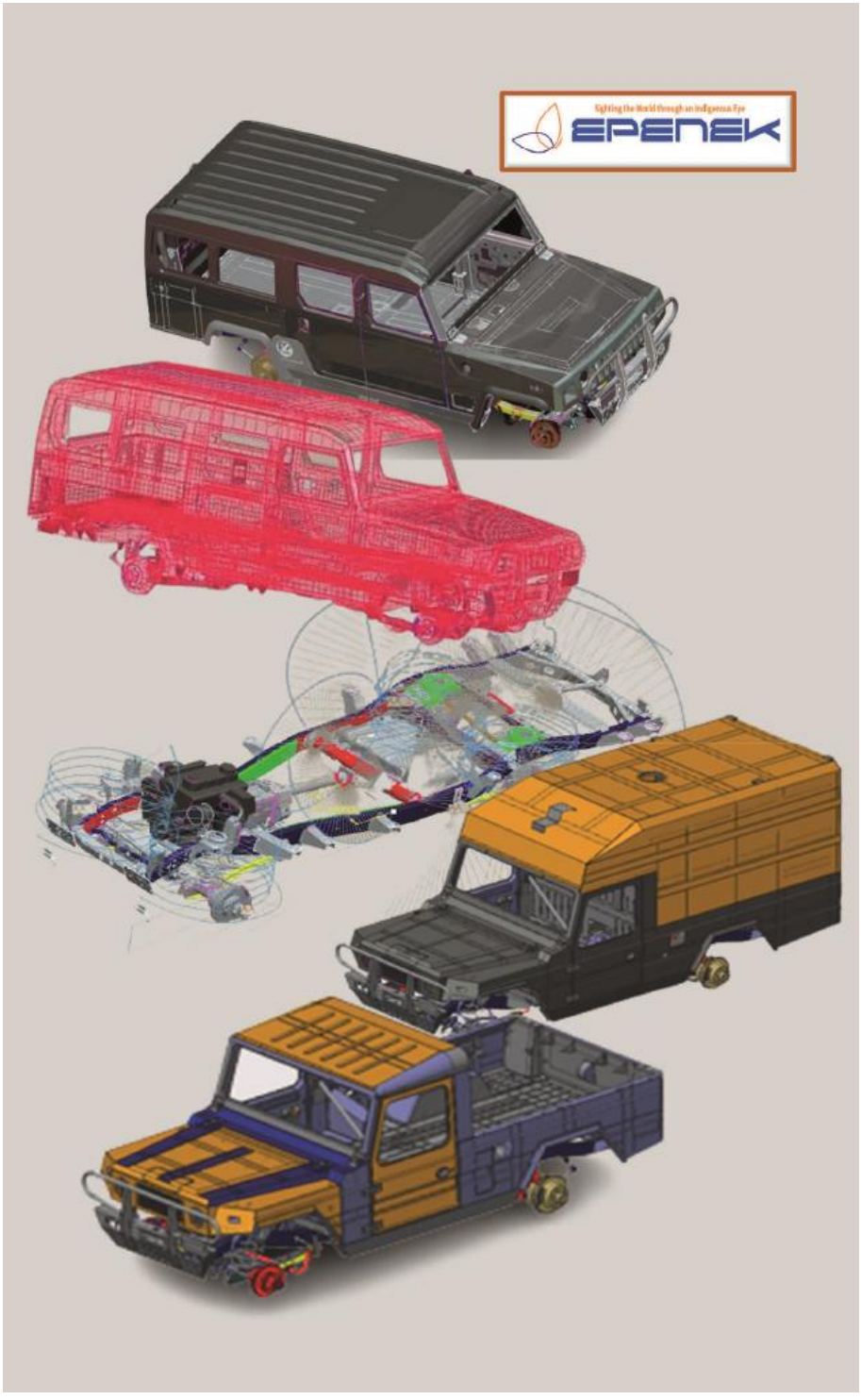
Ünal, S. ve Altun, Ö. M. (2021). The role of financial ıntelligence in combating the financing of terrorism. *Journal of Money Laundering Control. 24*(3), 571-583.

Üstün, O. (2008). Karapara aklama ve terörün finansmanı ile mücadelede uluslararası girişimler ve araçlara toplu bakış. *Bankacılar Dergisi. 65*, 19-36.

Yamaç, F. (2009). Terörle mücadele politikalarında yeni stratejiler: fransa örneği, uzakdoğu'dan yeni kıtaya terörle mücadele. *Uluslararası Stratejik Araştırmalar Kurumu*. 155-172.

Yıldırım, Z. (2010). *Hukuksal açıdan terörizmin finansmanının önlenmesi ve vergisel boyutu.* (Yayınlanmamış Doktora Tezi). İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü.

Yüce, M. ve Akkaya, H. (2020). Mali suçlarla kurumsal mücadele ve bazı ülke örnekleri. *Uygulamalı Bilimler Fakültesi Dergisi. 2*(2): 40-61.


Sighting the World through an Indigenous Eye
EPENEK

İstihbarat Çalışmaları ve Araştırmaları Dergisi
Journal of Intelligence Research and Studies
Cilt/Volume:3 Sayı/Issue:2 Yıl/Year: 2024 Haziran/June
ISSN 2822-3349 (Basılı- Print) ISSN 2822-3357 (Çevrimiçi- Online)

İ

Ç

A

D

Söyleşi / Interview

Araştırma Makaleleri

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.icadergisi.com
e-posta/e-mail: editor@icadergisi.com