

ISSN 2822-3349

Ana Tema:  
İstihbarat Analizi

İSTİHBARAT  
ÇALIŞMALARI VE  
ARAŞTIRMALARI  
DERGİSİ

Terörizm ve Radikalleşme ile Mücadele  
Araştırma Merkezi Derneği  
Ankara 2023

i

Journal of Intelligence  
Research and Studies

Ç

Cilt/Volume: 2  
Sayı/Issue: 1  
Yıl/Year: 2023  
Ocak / January

A

[www.icadergisi.com](http://www.icadergisi.com)

D

[editor@icadergisi.com](mailto: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: 2 Sayı / Issue: 1 Yıl / Year: 2023

Ocak / January

**İSTİHBARAT ÇALIŞMALARI VE ARAŞTIRMALARI DERGİSİ**

**İÇAD**

**KÜNYE**

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

**İMTİYAZ SAHİBİ**

Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği Adına,  
Ediz EKİNCİ

**SORUMLU YAZI İŞLERİ MÜDÜRÜ**

Soner ALAN

**BAŞ EDITÖR**

Mehmet DAYSAL, Emekli Korgeneral

**EDİTÖR**

Serhat Ahmet ERKMEN, Altınbaş Üniversitesi

**EDİTÖRLER KURULU**

Tarık OĞUZLU, İstanbul Aydın Üniversitesi

Bariş ÖZDAL, Uludağ Üniversitesi

Ali Burak DARICILI, Bursa Teknik Üniversitesi

Mehmet Emin ERENDOR, Kırgızistan Türkiye Manas Üniversitesi

Tarık AK, Jandarma ve Sahil Güvenlik Akademisi

Çağla Gül YESEVİ, İstanbul Kültür Üniversitesi

**YABANCI DİL EDITÖRÜ**

Burak GÜNEŞ, Ahi Evran Üniversitesi

**DANIŞMA KURULU**

Mustafa SAĞSAN, Uluslararası Kıbrıs Üniversitesi

M.Sadık AKYAR, Girne Amerikan Üniversitesi

Hakan ARIDEMİR, Kütahya Dumlupınar Üniversitesi

Emre ÇITAK, Hitit Üniversitesi

Merve SEREN, Yıldırım Beyazıt Üniversitesi

Yavuz ÇİLLİLER, İstanbul Gelişim Üniversitesi

Selim KURT, Giresun Üniversitesi

Tolga ÖKTEN, Milli Savunma Üniversitesi

**YAYIN KOORDİNATÖRÜ**

Sami ÖZTÜRK

Her hakkı saklıdır. İstihbarat Çalışmaları ve Araştırmaları Dergisi (İÇAD) Ocak ve Haziran aylarında yılda iki defa yayımlanan; yayın prensipleri, bağımsız, ön yargısız ve çift-kör hakemlik ilkelerine dayanan ulusal hakemli bir dergidir. Makalelerdeki görüş, sav, tez ve düşünceler yazarların kendi kişisel görüşleri olup, hiçbir şekilde Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneğinin (TERAM) veya İstihbarat Çalışmaları ve Araştırmaları Dergisi (İÇAD) görüşlerini ifade etmez. Makaleler, İstihbarat Çalışmaları ve Araştırmaları Dergisi (İÇAD) referans verilerek akademik çalışmalarda kullanılabilir. İstihbarat Çalışmaları ve Araştırmaları Dergisi'ne gönderilen makaleler iade edilmez. Dergimiz "Açık erişimli" olup yayınlanan eserlerin tam metinlerine erişim ücretsiz, yazı dili Türkçe ve İngilizcedir.

## **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  
Telefon: +90 312 441 11 50  
web sayfası: [www.icadergisi.com](http://www.icadergisi.com)  
e-posta: [editor@icadergisi.com](mailto: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

### **DİZİNLER**

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.

**EDITORIAL BOARD**  
**JOURNAL OF INTELLIGENCE RESEARCH AND STUDIES**

**İÇAD**

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

**LICENSEE**

In the name of Research Center for Defense Against Terrorism and  
Radicalization Association, Ediz EKİNCİ

**MANAGING EDITOR**

Soner ALAN

**EDITOR IN CHIEF**

Mehmet DAYSAL, (Ret.) Lieutenant General

**EDITOR**

Serhat Ahmet ERKMEN, Altınbaş University

**EDITORIAL BOARD**

Tarık OĞUZLU, İstanbul Aydın University

Barış ÖZDAL, Uludağ University

Ali Burak DARICILI, Bursa Technical University

Mehmet Emin ERENDOR, Kyrgyz-Turkish Manas University

Tarık AK, Gendarmerie and Coast Guard Academy

Çağla Gül YESEVİ, İstanbul Kültür University

**EDITOR FOR ENGLISH**

Burak GÜNEŞ, Ahi Evran University

**ADVISORY BOARD**

Mustafa SAĞSAN, Cyprus International University

M.Sadık AKYAR, Girne American University

Hakan ARIDEMİR, Kütahya Dumlupınar University

Emre ÇITAK, Hitit University

Merve SEREN, Yıldırım Beyazıt University

Yavuz ÇİLLİLER, İstanbul Gelişim University

Selim KURT, Giresun University

Tolga ÖKTEN, Turkish National Defense University

**PUBLICATION COORDINATOR**

Sami ÖZTÜRK

All rights reserved. The Journal of Intelligence Research and Studies – İÇAD published twice a year, in January and June; is a nationally peer-reviewed journal based on the principles of publishing, independent, unprejudiced and double-blind arbitration. In its published articles, the Editorial Board observes the highest ethical and scientific standards in relation to the issue and the requirement not to bear commercial concern. The opinions, arguments, thesis and thoughts within the articles are reflections of the authors and do not, in anyway, represent those of the Research Center for Defense Against Terrorism and Radicalization Association (TERAM). Articles can be used for academic purposes with reference to The Journal of Intelligence Research and Studies – İÇAD. Articles sent to the Journal of Intelligence Research and Studies – İÇAD will not be sent back. Our journal is "Open Access" and access to full texts of the published works is free and the literary language is Turkish and English.

### **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

Telephone: +90 312 441 11 50

web page: [www.icadergisi.com](http://www.icadergisi.com)

e-mail: [editor@icadergisi.com](mailto: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

### **INDEXES**

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

Editör'den / *Editor's Note* .....I-III

**Serhat Ahmet ERKMEN**

### **Araştırma Makaleleri / Research Articles**

Stratejik İstihbarat Analizini Anlamak: Bilimsel Araştırma ile Benzerlikleri ve Farkları / *Understanding Strategic Intelligence Analysis: Similarities and Differences with Scientific Research*.....1

**Müberra HUDOĞLU**

21'nci Yüzyılda Açık Kaynak İstihbaratı / *Open Source Intelligence in The 21<sup>th</sup> Century*.....17

**Tolga ÖKTEN**

Dijital Çağda İstihbarat Analizi / *Intelligence Analysis in The Digital Era*.....39

**M. Hayati TABAN ve Emre AYDİLEK**

Sinyal İstihbaratı Analizi Bağlamında Bir Değerlendirme: Rubicon Operasyonu ve Türkiye / *An Evaluation in the Context of Signal Intelligence Analysis: Operation Rubicon and Türkiye*.....68

**Semih SEVİNÇ**

### **İnceleme Makaleleri / Review Articles**

Psikolojik Harekât İstihbaratında Bir Analiz Yöntemi: Hedef Kitle Analizi / *An Analysis Method in Psychological Operations Intelligence: Target Audience Analysis*.....82

**Ediz EKİNCİ**

## EDİTÖR'DEN

İlk sayımız kısa sürede önemli bir ilgi gördü. Bu ilgi Türkiye'de istihbarat çalışmalarına artan alakanın ne kadar yoğun olduğunu anlamak açısından son derece memnuniyet vericidir. Ancak hala atılması gereken birçok adım, alınması gereken uzun bir yol bulunmaktadır. Bununla birlikte, dergimiz, istihbarat çalışmalarının Türkçede literatüre kazandırılması konusundaki temel amacı doğrultusunda yoluna inanca devam etmektedir. Nitekim, okuyacağınız ikinci sayı, istihbarat çalışmalarının en tartışmalı ve önemli boyutlarından birisi olan istihbarat analizi konusunda değerli eserleri içermektedir.

İstihbaratın tanımına ilişkin farklı görüşlerin üzerinde birleştiği ortak noktaların başında istihbaratın işlenmiş bir bilgi olduğu gelmektedir. Bu işleme süreci sadece bilginin toplanması, sevk ve idare edilmesi aşamasını içermez. Aslında işleme sürecinin en hassas kısmı, elde edilen verinin anlamlı bir bilgi örüntüsüne çevrilmesi kısmıdır. Bu kısım genellikle analiz olarak adlandırılmaktadır. Bu nedenle, elde edilen herhangi bir veri parçasının bir istihbarat çalışması için anlamlı bir istihbarata dönüşebilmesi için gerekli olan analiz gün geçtikçe daha fazla önem kazanmaktadır.

Güncel bir sorunun tanımlanmasından gelecekteki potansiyel tehditlerin belirlenmesine, hızlı dönüşüm süreçlerindeki fırsatların anlaşılmasından bu fırsatlardan yararlanılabilmesi için gerekli hazırlıkların yapılabilmesine kadar geniş bir bilgi dağarcığının oluşturulabilmesi bilginin analizinin doğru biçimde yapılabilmesine bağlıdır. Nitekim, istihbarat çalışmaları dünyasında gün geçtikçe artan bir biçimde istihbarat çalışmalarının sosyal bilimlerin farklı alanlarından daha çok şey öğrenmesi gereği tartışılmaktadır. 20 yıl kadar önce başlayan bu tartışmanın günümüzde geldiği nokta, istihbarat çalışmalarının özellikle analize ilişkin kısımlarının tarihselci bakış açısını bir yana bırakıp sosyoloji, psikoloji, siyaset bilimi ve uluslararası ilişkiler gibi bilim ve disiplinlerin metodolojisinden faydalanması gerektiği yönündedir. Bu nedenle son yıllarda istihbarat analizi sadece stratejik, taktik, operasyonel gibi ayrımlar üzerinden verilen eserleri aşmıştır.

Günümüzde istihbarat analizine ilişkin yeni eserlerin ortak noktası hangi konuları içermesi gerektiğinden ziyade istihbarat analizinin hangi metotlarla yapılması gerektiğini ele almasıdır. Elbette, tarihsel örneklerden yola çıkma, geçmiş tecrübelerden faydalanma ve karşılaştırma yapma



istihbarat faaliyetlerinin organizasyonu kadar analiz sürecinde de uygulanabilecek yaklaşımlardır. Bununla birlikte sosyal bilimlerin istihbarat çalışmaları üzerindeki etkisi arttıkça ve istihbarat çalışanları kadar sivil alandan gelen akademisyenlerin istihbarat çalışmaları alanında verdiği eserler çoğaldıkça sosyal bilimlerde kullanılan nitel araştırma yöntemlerinin istihbarat çalışmaları içindeki önemi de artacaktır. Nitekim, istihbarat çalışmalarının bilimsel yöntemlerle yapılması tartışmasının özü de burada yatmaktadır. Analiz süreci, geçmişten gelen mesleki edinimlerin ötesinde yeni sosyal bilim yöntemlerini de içerecek şekilde genişledikçe istihbarat analizi daha da güçlenecektir.

Elinizdeki bu sayımız tam da bu mantık ve öngörü doğrultusunda hazırlanmaya çalışılmıştır. Dergimizin bu sayısının ana teması olan istihbarat analizine ilişkin hazırlanan çalışmalar içerik olarak yukarıdaki tartışmayı geniş bir biçimde içerecek şekilde planlanmıştır.

Bu çerçevede ilk makalemiz Müberra HUDOĞLU tarafından “Stratejik İstihbarat Analizini Anlamak: Bilimsel Araştırma ile Benzerlikleri ve Farkları” başlığıyla hazırlanmıştır. Hudoğlu, çalışmasında istihbarat analizini konu ve yöntem bakımından bilimsel çalışmalarla karşılaştırmıştır. İstihbarat çalışmalarının hedeflerinin ve içeriğinin, bilimsel araştırmalarla benzer ve farklı yanlarını ortaya koyan bu çalışma, istihbarat çalışmalarına başlangıç seviyesinde ilgi duyan araştırmacılar için iyi bir giriş yapma olanağı sunmaktadır.

Dergimizin ikinci çalışması açık kaynak istihbaratı üzerinedir. Konuya ilişkin en yetkin isimlerden Tolga ÖKTEN tarafından hazırlanan “21’nci Yüzyılda Açık Kaynak İstihbaratı” adlı makale bir başvuru eseri niteliğinde sayılabilir. Halihazırda yapılan istihbarat analizlerinin temel kaynağı durumunda olan açık kaynak istihbaratının nasıl yapılması gerektiği kadar, açık kaynak istihbaratının potansiyellerinin ve sınırlarının tartışıldığı makale 21. Yüzyıldaki dijital gelişmelerin açık kaynaktan bilgi toplama üzerindeki etkisini de detaylı olarak ortaya koymaktadır.

Dijitalleşme diye söze devam ederken üçüncü makalemizin “Dijital Çağda İstihbarat Analizi” olduğunu söylemeliyiz. M.Hayati TABAN ve Emre AYDİLEK tarafından hazırlanan çalışmada modern çağın en önemli olgularından birisi olan dijitalleşmenin istihbarat analizi üzerindeki etkisi detaylı bir biçimde tartışılmıştır. Büyük veri ve yapay zekâ gibi artık aşına olunmaya başlanan konuları içeren çalışmanın en orijinal katkısı “Intellepedia” veri tabanının incelenmesi ve katkılarının sorgulanmasıdır.

Bu sayıdaki dördüncü makalemiz ise sinyal istihbaratı üzerindedir. Semih SEVİNÇ tarafından kaleme alınan “Sinyal İstihbaratı Analizi Bağlamında Bir Değerlendirme: Rubicon Operasyonu ve Türkiye” çalışmada sadece sinyal istihbaratının önemi ele alınmamaktadır. Ülkemizde az bilinen Rubicon Operasyonu ve bu operasyonun Türkiye üzerindeki etkileri de tartışılmıştır.

Son makalemiz ise benzerine az rastlanan türden bir birleşimin ürünüdür. Ediz EKİNCİ tarafından yazılan çalışma hem tecrübenin hem akademik çalışmanın birleşimi olarak ortaya çıkmıştır. Bu çerçevede EKİNCİ, “Psikolojik Harekât İstihbaratında Bir Analiz Yöntemi: Hedef Kitle Analizi” Psikolojik harekatta hedef kitle analizinin önemini ortaya koymaktadır. Bu çalışmanın çok dikkatle okunmasını tavsiye ederim. Birçok ülkedeki toplumsal olayların ve bu olaylara verilen tepkilerin anlaşılmasında anahtar niteliğinde bilgiler sunan eserin Türk okuyucular açısından önemli bir başvuru kaynağı olacağını umut ediyorum.

Türkiye’de istihbarat gibi hassas bir konuda akademik dergi çıkarmak gerçekten zor ve emek yoğun bir süreci gerektiriyor. İkinci sayımızı da yüz akıyla tamamladığımıza inanıyoruz. Bu çabanın devam edebilmesi için katkılarınızı bekliyoruz. Üçüncü sayımızda görüşmek üzere...

Prof.Dr. Serhat Ahmet ERKMEN

İÇAD Editorü

## STRATEJİK İSTİHBARAT ANALİZİNİ ANLAMAK: BİLİMSEL ARAŞTIRMA İLE BENZERLİKLERİ VE FARKLARI

Müberra HUDOĞLU\*

### ÖZET

Bilimsel araştırmalarda olduğu gibi stratejik istihbarat araştırmasında analist, belli fenomenleri açıklamak ve gerçek dünyadaki sorunları incelemek adına metodolojik yaklaşımlar ile hipotezler ortaya koyar ve bunları test eder. Neticede bilgi üretmenin yolları sınırlıdır, bilimsel yöntem de bunlardan en önemlisidir. Öte yandan stratejik istihbaratın araştırma konuları, büyük ölçüde sosyal bilimlerin kapsamına girer. Öyleyse bilimsel araştırma ile stratejik istihbarat analizini birbirinden ayıran ne olabilir? Bu çalışma, stratejik istihbarat analizinin bilimsel araştırma ile benzerliklerini ve farklarını ortaya koyarak, bilim dünyası için stratejik istihbarat analizini daha anlaşılır hale getirmeyi amaçlamaktadır.

**Anahtar Kelimeler:** *İstihbarat, Stratejik İstihbarat, İstihbarat Analizi Süreci, Stratejik İstihbarat Analizi, Bilimsel Araştırma.*

## UNDERSTANDING STRATEGIC INTELLIGENCE ANALYSIS: SIMILARITIES AND DIFFERENCES WITH SCIENTIFIC RESEARCH

### ABSTRACT

In strategic intelligence research, as in scientific research, the analyst puts forward and tests hypotheses through methodological approaches to explain certain phenomena and examine real-world problems. After all, the ways of producing knowledge are limited, and the scientific method is the most important of them. So what could separate scientific research from strategic intelligence analysis? This study aims to make strategic intelligence analysis more understandable for the scientific world by revealing the similarities and differences between strategic intelligence analysis and scientific research.

**Keywords:** *Intelligence, Strategic Intelligence, Intelligence Analysis Process, Strategic Intelligence Analysis, Scientific Research.*

---

\* İstihbarat Bilim Uzmanı, İş Analisti, [muberrahudoglu@gmail.com](mailto:muberrahudoglu@gmail.com), ORCID: 0000-0002-8577-8588.  
Makale Başvuru Tarihi / Application Date: 28 Kasım 2022 / 28 November 2022  
Makale Kabul Tarihi / Acceptance Date: 19 Aralık 2022 / 19 December 2022

## GİRİŞ

Dünyanın herhangi bir yerinde ani gelişen bir olay karşısında, karar alıcının yapacağı ilk şey istihbarat servislerinden konu hakkında bilgi talep etmektir. Yeni gelişen olay karşısında istihbarat analistinin bir anlayış geliştirmesi için birkaç saatten fazlası yoktur. Bu yüzden halihazırda analistin, öncesinde olayın gelişme sürecini takip etmiş olması, derinlemesine araştırıp istikameti hakkında fikir edinmiş olması gerekir (Hedley, 2007, s.40). Zira bir ülkenin dış politikası, stratejik istihbarat üzerinden şekillenir. Hedefin veya ülkenin güçlü ve zayıf yönleri, amaçları, kaynakları, kabiliyetinin tespiti ile analiz, ileriye dönük politikalarda karar alıcıya destek olur. Analist, olası stratejik sürprizleri takip eder ve öngörülerde bulunur. Gelişmeleri tanımlar, süreci yönlendiren etmenleri belirler, sürecin nereye evrileceğini görmeye çalışır, hangi işaretlerin yörünge değişikliğine neden olabileceğini belirleyip karar alıcıya sunar.

Bilimsel araştırmalarda olduğu gibi istihbarat araştırmasında da analist, başlangıçta belli fenomenleri açıklamak ve gerçek dünyadaki sorunları incelemek adına metodolojik yaklaşımlar ile hipotezler ortaya koyar. Dolayısıyla analist, bir bakıma bilimsel yöntemin uyarlanmış bir biçimini kullanır. Nihayetinde bilgiyi üretmenin sınırlı yolu vardır, analist ister istemez bilimsel disipline ihtiyaç duyar ve bunu araştırmasına yansıtır. Halihazırda stratejik istihbarat, istihbarat türleri arasında bilimsel disiplin olarak ortaya çıkar. Konu olarak ise “dış istihbarattır” ve ulusal güvenlik faaliyetleri ile ilgilenmektedir. Nihayetinde analistin, araştırdığı ve anlayış geliştirdiği konular, büyük ölçüde sosyal bilimlerin araştırma konuları kapsamına girmektedir.

İstihbarat görevlisinin ve sosyal bilimcinin temel görevi, gerçekleri anlamlı kalıplara oturtmak, böylece onların alaka düzeyini ve eldeki sorunla ilişkisini kurmaktır. İstihbarat analizi toplama ve yorumlama tekniklerine göre nicel sosyal bilim araştırmalarından ziyade kendi bağlamında yorumlayıcı incelemeler yapan nitel araştırmalara daha yakındır. Bu sebeple özellikle uluslararası ilişkiler araştırmaları ile stratejik istihbarat analizi araştırmaları benzerlik gösterebilir. Her ikisi geçmiş ve bugün arasında sağlam bir anlayış kurarak en başta olayları anlamaya ve açıklamaya çalışır. O halde stratejik istihbarat analizini bir uluslararası ilişkiler araştırmasından ayıran ne olabilir? Bu çalışma, akademik araştırma ile stratejik istihbarat analizinin benzerliğini ve farklarını ortaya koyarak, bilim dünyası için stratejik istihbarat analizini daha anlaşılır hale getirmeyi amaçlamaktadır.

## **1. STRATEJİK İSTİHBARAT ve STRATEJİK İSİTHBARAT ANALİZİ**

Hükümetler, ulusal karar alma düzeyinde fırsatları ve tehditleri ortaya çıkarmak amacıyla bilgi arayışı içerisine girerler. Bu bilgi arayışı çabası, istihbarat faaliyetini ortaya çıkarır (Johnson, 2008, s.33). İstihbarat her ne kadar basit manada “haber alma” olarak tanımlansa da istihbarat faaliyeti bundan fazlasıdır. Shulsky’e (2002, s.116) göre istihbarat, “her türlü politik, ekonomik, sosyal ve askeri meseleyi anlamayı ve nihayetinde öngörmeyi amaçlayan evrensel bir sosyal bilimdir”.

İstihbaratın kendisi hem süreçtir hem de sürecin sonunda elde edilen üründür (Warner, 2002). Elde edilen bilginin yanında, sürecin kendisi de “istihbarat” olarak ifade edilir. Bu süreç, diğer deyişle istihbarat faaliyeti, karar alıcının sorusuna binaen ihtiyaç duyulan bilgilerin toplanması, belli bir sistematığe göre işlenmesi ve kararı destekleyecek biçimde karar alıcıya sunulmasını içerir. Stratejik sürprizlere karşı hazırlıklı olunmasını sağlar; belirsizliği azaltmak amacıyla fırsatları ve tehditleri tanımlar. Netice itibarıyla istihbarat, karar alıcının “daha iyi” karar alınmasını hedefleyen bir karar destek aracıdır (Warner, 2008, s.16).

İstihbarat taktik, operasyonel ve stratejik olmak üzere üç ölçekte incelenir. Stratejik istihbarat, operasyonel ve taktik istihbarat ihtiyaçlarının ötesinde ulusal ve uluslararası düzeydeki stratejik hedeflere hizmet eder (McDowell, 2009, s.21). Millî İstihbarat Teşkilâtı, stratejik istihbaratı “ülkeler ve diğer yapılanmalardaki gelişmelerin tamamını takip ve analiz ederek öngörüsü yüksek sonuçlara ulaşılan bilgileri karar alıcılara sunma süreçlerini içeren bir faaliyettir” şeklinde tanımlar (Göktaş, 2018, s.21).

Nihayetinde stratejik istihbarat bir “dış istihbarattır” ve ulusal güvenlik faaliyetleri ile ilgilenir. Bir ülkenin dış politikası, stratejik istihbarat üzerinden şekillenir (McDowell, 2009, s.53). Kent’e (2015, s.3) göre stratejik istihbarat, bilginin en önemli bölümüdür. Onun tanımına göre stratejik istihbaratın konusunun kapsamı; operasyonel, taktik ve muharebe istihbaratı dışında kalan her şeyi içermektedir.

Pruncun’a (2010, ss.6-7) göre istihbaratın yüksek bir biçimi olarak kabul edilen stratejik istihbarat; (i) bir hedef veya faaliyetin kapsamlı bir görünümünü sağlar, (ii) gelecekteki olasılıklar hakkında yorum yapar veya potansiyel sorunları tanımlar, (iii) tehditler, riskler ve güvenlik açıkları

hakkında tavsiyelerde bulunur ve (iv) planlama ve politika geliştirme için seçenekler sunar.

Siyasal karar alıcılar, eldeki verileri nesnel bir biçimde değerlendirerek genel çerçeveyi ortaya koyabilen, belirsizlikle başa çıkarak en olası tahminleri, karar alıcının anlayabileceği şekilde sunarak kararı destekleyecek analistlere ihtiyaç duyar. İstihbarat analistleri, karar alıcıların bu ihtiyaçlarına binaen politika belirlemede destek sağlar. Bunlar:

- Ülkenin veya hedef ülkenin çıkarları için mevcut olan fırsatları ve tehditleri, beklenmeyen gelişmeleri öngörme,
- Hasım ve hasım olması muhtemel aktörlerin ve müttefiklerin hedefleri, güçlü ve zayıf yönleri ve amaçlarını belirleme,
- Ülkenin veya hedef ülkenin politik gücü, dış politikadaki doğrudan veya dolaylı kaynaklarını belirleme
- Ülkenin veya hedef ülkedeki amaçları ve hedeflerin engellenmesine yönelik faaliyetleri tespit etme ve engel olma,
- Stratejik sürprizlere karşı ön uyarı sağlama,
- İleri dönük planlamalar yapma ve belirlenen politika hedeflerine ulaşmak üzere aşamalar kaydetme adına alternatifler oluşturma, şeklindedir (Karabacak, 2002 s.22).

Stratejik istihbaratın omurgasını oluşturan şey ise geleceğe yönelik olmasıdır. Analistler, geçmişten geleceğe doğru bir anlamlandırma faaliyeti sürdürürler (Göktaş, 2018, s.22). Neticede stratejik istihbarat analizi “gelecekte ne olabilir?” sorusunu, mevcuttan yola çıkarak temellendirilmiş yargılar oluşturup sistematik bir süreç sonucunda alternatif gelecekler oluşturarak yanıtlamaya çalışır (Kuosa, 2014, s.17).

Analistin amacı burada incelediği olgu ile ilgili (i) gelişmelerin gidişatlarını tanımlama, (ii) süreci yönlendiren etmenleri belirleme, (iii) sürecin nereye gittiğini görmeye çalışma, (iv) hangi işaretlerin yörünge değişikliği gösterebileceğini belirlemeye çalışma şeklindedir (Fingar, 2022, s.53).

Bu sebeple analist, bazı özellikler taşımalıdır. Bruce ve George’a (2008 s.3) göre ise istihbarat analistinde olması gereken özellikler şöyledir: (i) araştırma konusuna ve ilgili ülkenin politikalarına hakim olmak, (ii) verileri düzenlemek ve değerlendirmek için araştırma yöntemlerini anlamış olmak, (iii) hipotezlerin test edilme kabiliyetinin yanı sıra hayal gücü ve bilimsel titizliğe sahip olmak, (iv) istihbarat toplama yöntemlerini anlamak,

(v) analizde yanlış çıkarımlara sebep olan “bilişsel önyargılara” ve başka etmenlere karşı farkındalığa sahip olmak, (vi) zıt görüşlere veya alternatif modellere karşı açık fikirli olmak, (vii) analitik hataları kabul etmek ve hatalardan ders çıkarmaya karşı özgüvenli olmak. Onlara göre ilk üç özellik, aslında genel manada akademik uzmanların sahip olduğu özelliklerdir; istihbarat analistini ayırt eden şey son dört özelliktir.

İstihbarat analizini anlatmak için pek çok yerde “noktaları birleştirme” benzetmesi yapılır. Ancak bu analogi, sürecin karmaşıklığını basit bir yapıya indirger. Esasen istihbarat analizi hipotezleri geliştirme ve yanlışlama ile başlayan, mantıksal akıl yürütmelerin farklı derecelerde kullanımı dahil olmak üzere bilimsel yöntemin uyarlanmış bir biçimini içermektedir (Marrin, 2012a, s.81).

Stratejik istihbarat analizine metodolojik bir bağlam kazandırarak bilimsel bir disiplin olmasına öncü olan isim Sherman Kent'tir. Kent, stratejik istihbaratın bir sosyal bilim olarak ortaya çıkmasını sağlayan “Strategic Intelligence for American World Policy” adlı kitabı kaleme almıştır (CIA, 2010). Ona göre istihbarat toplama teknikleri ve teknoloji, bilginin yorumlanmasında yetersiz kalmaktaydı. Klasik istihbarat raporlarının büyük bir çoğunluğu iddia ettiği yargıları destekleyecek argümanları içermiyor ve mantık hataları bulunduyordu (Tuzcu, 2013, s.36). Kent, mantıksal ve bilimsel metodolojiyi birleştirebilen analistler yetiştirerek mesleki beceriler kazandırmanın önemli olduğunu vurgulamaktaydı (Seren, 2017, s.340). Bu nedenle hipotezlerin oluşturulup test edildiği ve bilimsel araştırma yöntemlerine benzer bir üretim süreci içeren modern istihbaratta, Kent'in atılımına binaen bilimsellik ve akademik konsept ön plana çıkmış oldu (Yılmaz, 2019, s.385). Dolayısıyla stratejik istihbarat, geleneksel istihbaratın aksine bilimsel bir disiplin rolü üslendi (Beşe ve Seren, 2011, s.133).

## **2. BİLİMSEL ARAŞTIRMA İLE BENZERLİKLERİ VE FARKLARI**

Kent'e göre (2015, s.175) stratejik istihbaratın çalıştığı konular büyük ölçüde sosyal bilimler alanına girmektedir. Stratejik istihbarat, bir ülkenin güvenliği için sağlık, eğitim, sosyal yapısı, karşı karşıya kaldığı sosyal ve siyasal sorunlar, yasal problemler, gıda üretim-tüketim ve dağıtım kabiliyeti, dünyadaki kaynaklar (içme suyu, petrol vb.), politik ilişkiler, uluslararası ticaret ilişkileri, göç ilişkileri, etnik ve kültürel değişim ve dönüşümler, küresel para düzeni, teknolojik gelişmeler, nükleer meseleler,

silah üretimi ve kabiliyeti, savunma sanayi tesisleri, askeri yetenekleri vs. gibi (Prunckun, 2010, ss.12-13) geniş bir alanda, aslında sosyal bilimlerin araştırma konusu olan meseleler hakkında bilgiye ihtiyaç duymaktadır.

Bilim temelde; evren, doğa ve toplumda meydana gelen hadiselerin ve fenomenlerin işleyiş ilişkilerini mantıksal tutarlılık içerisinde açıklama misyonu güder. Dolayısıyla her araştırmacı gibi istihbarat analisti de gerçek dünyaya ait sorunları ile alakalı içgörü sağlamak adına metodolojik bir araştırma süreci yürütmeye ihtiyaç duyar (Prunckun, 2010, s.44). Zira belli noktalarda farklılaşma oluşsa da bilgilerin toplanması ve analitik sürece tabi tutulması temelde benzer metodolojiyi gerektirir. Carter'a göre bu noktada bilim, bu sürece yol gösteren bir "düşünme biçimi"dir (Marrin, 2012b, s.531). Marrin'e (2012a, s.87) göre bilimsel yöntem de istihbarat analizi gibi tanımlama ve açıklama içerir:

"...bilimsel yöntemin uygulandığı tüm alanlarda, metodolojistler uygulayıcılara güvenilir olan iyi verileri kullanmalarını ve mümkünse doğrulamalarını söyler. Nesnelerin özelliklerini tanımlarken, kategorilerin nominal mı, ordinal mi, aralık (interval) mı yoksa oran (ratio) mı olduğuna karar verir ve buna göre çıkarımlar yapar. Açıklarken, mümkün olduğu kadar çok sayıda bağımsız değişkeni hesaba katar; bağımlı değişkeni ne kadar etkilediklerine göre sıralar. Bağımlı değişkendeki en büyük değişikliği hangisinin açıkladığını bulmak için nedensellik hakkındaki alternatif hipotezleri birbirine karşı test eder. Ve saire."

Bilimsel bilgiye ulaşmada temel kaide hipotez oluşturmak ve bu hipotezleri bilimsel yöntemler ile test etmektir (Ben-Israel, 1989, s.693). Bilimsel araştırmalarda olduğu gibi istihbarat araştırmasında da analist, metodolojik yaklaşımlar ile hipotezler ortaya koyar. Bu sebeple bilimsel araştırmada olduğu gibi problem formülasyonu, literatür taraması, verilerin toplanması vs. gibi bilimsel araştırma süreci ile benzer bir süreç izler. Zira analist, verileri toplamada ve yorumlamadaki bu nesnel yaklaşıma ihtiyaç duymaktadır (Prunckun, 2010, s.44). Bu sebeple bilimsel araştırma süreci ile istihbarat analiz süreci benzerlik göstermektedir (Tablo 1).



Tablo 1. İstihbarat Analiz Süreci ile Bilimsel Araştırma Süreci Karşılaştırması.  
(Kaynak: Yazar tarafından oluşturulmuştur)

<b>İstihbarat Analiz Süreci</b>	<b>Bilimsel Araştırma Süreci</b>
Karar alıcı tarafından istihbarat sorusu verilir.	Araştırmacı tarafından problem tanımlanır.
İstihbarat kaynaklarından veriler toplanır. (Açık, kapalı, yarı açık kaynaklar ve istihbaratçı bilgi bankası)	Literatür taraması yapılır.
Bilgiler bir araya getirilir ve tasnif edilir. (Doğruluğu, güvenilirliği ve alaka düzeyi değerlendirilir)	
Bir araya getirilmiş bilgilerle mantıksal hipotezler oluşturulur. (Yapılandırılmış analitik teknikler <sup>1</sup> kullanılabilir.)	Hipotezler ve varsayımlar oluşturulur.
Hipotezler test edilir (Yapılandırılmış analitik teknikler kullanılabilir) ve uygun çıkarımlar ortaya konur.	Araştırma yöntemi belirlenir ve veriler analiz edilir.
İstihbarat raporu sunulur.	Sonuçlar yayınlanır.

İstihbarat görevlisinin ve sosyal bilimcinin temel görevi, gerçekleri anlamlı kalıplara oturtmak, böylece onların alaka düzeyini ve eldeki sorunla ilişkisini kurmaktır (Marrin, 2012a, s.90). Dolayısıyla akademik çalışma ile istihbarat analizi arasında benzerlik oluşmaktadır. Her ikisi geçmiş ve bugün arasında sağlam bir anlayış kurarak en başta olayları anlamaya ve açıklamaya çalışır (Heuer, 2019). Keza “bilgi üretmenin” sınırlı sayıda yolu bulunur. Bu her disiplinde olduğu gibi istihbarat için de geçerlidir (Bruce, 2008, s.172). Gün sonunda, istihbarat analistleri ham istihbarata gömülü gerçeklerden anlam çıkarmak için bilginin güvenilirliğini ve geçerliliğini

<sup>1</sup> Yapılandırılmış analitik teknikler (structured analytic techniques), analizi ve karar vermeyi geliştirmeyi, sezgi kullanımına bağlı hataları ve bilişsel önyargıları olabildiğince indirgeyebilmeyi amaçlayan yöntemlerdir. Yapılandırılmış analitik teknikler ile ilgili detaylı bilgi için bkz. Pherson, R. H., & Heuer Jr, R. J. (2020). Structured analytic techniques for intelligence analysis. Cq Press.

değerlendirirken, hipotezler oluşturup mantıksal bir çıkarım yaparken, problem çözerken, sosyal bilimlerden türetilen bir bilimsel yaklaşım kullanmaktadır (Marrin, 2012b, s.531).

Tablo 2. Stratejik İstihbarat Analizi ile Akademik Araştırmanın karşılaştırılması (Kaynak: Yazar tarafından oluşturulmuştur)

	<b>Stratejik İstihbarat Analizi</b>	<b>Akademik Araştırma</b>
<b>Araştırma sorusunun verilişi</b>	Karar alıcı tarafından verilir.	Araştırmacının kendisi oluşturur.
<b>Araştırılan olayın farkı</b>	Olay yeni gerçekleşmiştir, veri azdır.	Olayın üzerinden zaman geçmiş, yeterli veri mevcuttur.
<b>Amaç olarak farkı</b>	Belirsiz olaylarla ilgilenir, bilgi karar alıcı içindir.	Kalıplar ve genel bilgilerle ilgilenir, bilgi bilgi içindir.
<b>Belirsizlik</b>	Belirsiz ortamlardaki belirsizliği azaltmaya çalışır.	Mevcudu tanımlar.
<b>Öngörüler</b>	Öngörülerde bulunmaya çalışır.	Öngörü temel misyon değildir.
<b>Çıktının farkı</b>	Güvenilir sonuca ulaşmaya çalışır.	Nesnel sonuca ulaşmaya çalışır.
<b>Kaynaklar</b>	İstihbarata özgü gizli ve açık kaynaklar kullanılır.	Açık kaynaklar kullanılır.
<b>Gizlilik epistemolojisi</b>	Gizlidir, karar alıcıya sunulur.	Kamuoyuna açıktır.
<b>Aldatma unsuru</b>	“Hedef” analisti aldatmaya çalışır.	Bilgi, araştırmacıyı kandırmaya çalışmaz.
<b>Zaman kısıtlılığı</b>	Sonuca hızlı ulaşmalıdır.	Zaman sınırlaması genellikle yoktur.
<b>Analiste bağlı olması</b>	Analistin zihninde şekillenen bir sonuca ulaşılır.	Araştırmacının sonuç üzerinde etkisi sınırlıdır.
<b>Sezgi unsuru</b>	Sezgi, analizi yönlendirebilir.	Sezginin kullanımı sınırlıdır, araştırma sorusu oluşturulurken kullanılabilir.

Anlaşılabacağı üzere istihbarat analizi toplama ve yorumlama tekniklerine göre nicel sosyal bilim araştırmalarından ziyade kendi bağlamında yorumlayıcı incelemeler yapan nitel araştırmalara daha yakındır (Marrin, 2012a, s.81).

Bilimsel araştırma ile istihbarat analizi olayları anlama, açıklama ve yorumlama konusunda benzer bir model izliyor olsa da bilimsel araştırma ile istihbarat analizi arasında, araştırmacının yürütülmesindeki amaç, araştırılan olay ve araştırma süreci sonunda oluşan çıktı başta olmak üzere belli noktalarda farklılaşmalar oluşur. Bilimsel araştırma ile stratejik istihbarat analizi arasındaki fark Tablo 2'deki şekilde sınıflandırılmıştır. Açıklaması ise devam eden metinde sunulmuştur.

*Araştırma sorusunun verilmesi.* Bilimsel araştırmada, araştırma sorusu araştırmacının inisiyatifindedir, istihbarat analizinde ise istihbarat sorusu büyük ölçüde müşteri tarafından verilmektedir (Clark, 2013, s.29). Tabii bu analistlerin bağımsız araştırma yapmalarını engellemez. Analistler kendi teorilerini oluşturmak adına kendi araştırma sorularını da oluşturabilirler (Prunckun, 2010, s.23).

*Araştırılan olayın farkı.* Sosyal bilimciler olaylar arkasındaki itici güçleri ve nedenselliği açıklamaya çalıştıklarında çoğunlukla olay gerçekleşmiştir, sonuç biliniyor durumdadır ve analiz için yeterli veri artık mevcuttur (Phythian, 2017, s.602). Ancak istihbarat analizinde, karar alıcının ihtiyaç duyacağı içgörüler genellikle yeni problemleri kapsar. Bu tip konularda veriler daha azdır, konu genellikle karmaşık, yeterince anlaşılmamış, çok değişkenli ilişkiler içerir (Heuer, 2019). Analist bu az verili, belirsiz ve çelişkili ortamdan anlam çıkarmaya çalışır.

*Amaç olarak farkı.* İstihbarat analisti olaylardaki teorik kalıplarla ve genellemelerle ilgilenmez. Genellikle incelediği olay benzersizdir ve bu olaylar ile ilgili açıklamalarda ve tahminlerde bulunmaya çalışır. Bu açıklamaları yaparken teoriden faydalanabilir. Ancak teorik önermelerin geliştirilmesi veya kanıtlanmaya çalışması ile ilgilenmez. Bu akademinin işidir (Heuer, 2019). Sosyal bilimci ise güvenilir sebep-sonuç ilişkileri kurarak, incelediği durumu şekillendiren kritik faktörleri belirler. Analistin aksine bir durumun unsurlarını ortaya koymakla ilgilendiği kadar, aynı durum hakkında inandırmak veya tahminde bulunmakla ilgilenmez. Bu fark, kalıpları araştıran ve genel bilgilerle ilgilenen araştırmacı ile, bireysel

olaylara odaklanan analist arasında bir perspektif farkı da meydana getirmektedir (Platt, 1957, s.137).

Bilimsel araştırmada bilgi bilgi içindir, pratik bir amaç gütmaz. Araştırmada önemli olan araştırmanın “iyiliğidir”. Zaman zaman bulgular uygulamalı ortamda kullanılıyor olsa da araştırmanın nihai amacı uygulama değildir (Prunckun, 2010, s.8). İstihbarat analizinde ise temel amaç karar alıcının “iyiliğidir”; analist, karar alıcı için faydaya odaklanır (Marrin, 2012b, s.533). Dolayısıyla istihbarat bir “uygulamalı araştırma” olarak görülebilir: “Hedefe yönelik yapılır, geleceğe yöneliktir ve tahmin odaklıdır. Analiz sonucu karar alıcı harekete geçer (Clark, 2013, s.29). Amaç içgörü sağlama, belirsizliği azaltma, öngörülerde bulunma, kararı destekleme vb. şeklindedir (Prunckun, 2010, s.8).

*Belirsizlik* Bilimsel araştırmada araştırmacı belirsiz ortamlarda çalışmaz, daha ziyade mevcudu tanımlamaya çalışır, gerçekleşmiş, olan biten hadiselere odaklanır. İstihbarat analisti için ise durum farklıdır. Garst ve Gross’un (1997, ss. 48-49) belirtmesine göre, çalıştığı konu hakkında donanımlı bilgiye sahip olmasının yanında istihbarat kaynaklarından da bilgi yığını elde eden analist, genellikle belirsiz ortamlardaki parçalı, çelişkili ve aldatmaya açık bilgilerden anlam çıkarmaya çalışır. Dolayısıyla istihbarat analisti, en önemli görevlerinden biri olarak, belirsizlik dolu kanıtların arasından çıkarım yaparak belirsizliği azaltmak zorundadır (Betts, 2008, s.93). İstihbarat analisti belirsizlik içerisinde ortaya çıkan sürprizleri, sürpriz olmaktan çıkarılması amacıyla gerçekleşmesi olası durumların tanımlanmasını yapması gerekir. Böylelikle belirsiz ortamlardan doğacak tehlikelere karşı karar alıcının bir anlayış geliştirmesine yardımcı olmayı hedefler (Clauser, 2008, s.24).

*Öngörüler.* İstihbaratta öngörülerin en ehemmiyet teşkil ettiği alan stratejik düzeydir (Kuosa, 2014, s.17). Stratejik istihbarat analistinin temel görevlerinden biri öngörülerde bulunmaktır. Clauser’a (2008) göre basit bir istihbaratın amacı bile aslında öngörüdür. ABD resmi olarak, stratejik istihbarat raporları için “tahminler” (estimates) ifadesini kullanır (Prunckun, 2010, s.22). Analist, belirsiz ortamlar için gelecek öngörüsünde bulunarak karar alıcıya olası alternatifleri sunar. Akademik araştırma ise daha çok çözümlenmeye odaklanır, öngörülerde bulunmayı temel misyonu olarak görmez.

*Çıktının farkı.* Bilimsel araştırmada araştırmacı, olabildiğince nesnel veriler ile nesnel sonuçlara ulaşmaya çalışır. Her ne kadar istihbarat analizi, nesnel bir yöntem ve sağlam teknikler ile hipotezleri test ediyor olsa da istihbarat analizi sonucu ortaya çıkan ürün, bilimsel bilgi nesnellüğünde olmaz. Zira istihbarat belirsizlikle ve gelecek öngörülerıyla ilgilenir, geleceğin öngörülemez doğası sebebiyle yüzde yüzlük bir tahmin ürününe ulaşmak nadiren mümkündür.<sup>2</sup> Dolayısıyla istihbarat analizi sonucu oluşan çıktı, kesin olmaktan ziyade güvenilirdir (Mathams, 1995, s.84).

*Kaynaklar.* Stratejik istihbarat analizi büyük ölçüde açık kaynak istihbaratına dayanır (Johnson, 2003, s.16). Bakıldığında pek çok akademik kurum veya bağımsız kuruluş, açık kaynakları kullanarak istihbarat kurumlarının hazırladığı analizlere eş değer analizler hazırlayabilirler. Öyleyse neden devletler istihbarat servislerine ihtiyaç duyar? İstihbarat örgütlerinin hazırladığı değerlendirmeler, akademinin aksine “açık” ve “gizli” kaynaklardan toplanan bilgilerin kombinasyonundan oluşur (Scott ve Jackson, 2004, s.142). Hükümetten başka hiçbir kuruluş, bu ikili kapasiteye sahip değildir. Dolayısıyla istihbarat örgütlerini özel kılan bu ikili kapasitenin harmanlanması ve müşterinin ihtiyaçlarına uygun cevapları içeren raporlama teknikleri ile sunulmasıdır.

En geniş haliyle istihbarata özgü toplama yöntemleri şöyledir; insan istihbaratı (HUMINT), sinyal istihbaratı (SIGINT), haberleşme istihbaratı (COMINT), elektronik istihbarat (ELINT), radar istihbaratı (RADINT), siber istihbarat (CYINT), fotoğraf istihbaratı (IMINT veya PHOTOINT), uydu ve hava sistemleri (GEOINT), sosyal medya istihbaratı (SOCMINT) ve açık kaynak istihbaratı (OSINT) (Yılmaz, 2019, ss.334-335).

*Gizlilik epistemolojisi.* İstihbaratı akademik araştırmadan ayıran diğer şey gizlilik epistemolojisidir. Bilimsel araştırma kamuoyuna açıktır, araştırmanın kendisi ve sonucu uzmanların eleştirisine ve tartışmasına sunulur. Buna kıyasla istihbarat kördür. İstihbaratın kapalı doğası, elde edilen sonuçların düzeltilmesini veya serbest rekabete tabi tutulmasını engellemektedir (Horn, 2003, s.66). Analitik ürünler, istihbarat kaynakları ve yöntemlerinin gizli tutulması amacıyla “gizli” veya “çok gizli” sınıflandırılması ile korunmaktadır (George ve Bruce, 2008, s.6). Dolayısıyla çalışmanın yönteminin ve bulgularının eleştirilememesi, istihbarat

---

<sup>2</sup> İstihbaratın öngörülebilirlik üzerine doğasını Kaos Teorisi ile açıklayan çalışma için bkz. Hudoğlu, M.& Ak, G. Stratejik istihbarat analizinde öngörülebilirliğin doğası: Kaos Teorisi ışığında yeni bir muhakeme denemesi. *Florya Chronicles of Political Economy*, 8(2), ss.23-40.

çalışmasının geliştirilmesi açısından bir dezavantajdır (Prunckun, 2010, s.44). Bilimsel araştırmanın kitlesi kamuoyu iken, istihbarat raporunun müşterisi karar alıcıdır.

*Aldatma unsuru.* İstihbarat analizinde “hedef”, analisti aldatmak ve yanlış sonuçlara ulaşmasını sağlamak adına özel bir mesai harcar. Bilimsel araştırmada araştırılan bilgi, araştırmacıyı kandırmaya çalışmaz (Ben-Israel, 1989, s.679).

*Zaman kısıtlılığı.* Akademisyenin aksine, analistin zamanı oldukça kısıtlıdır. Genellikle yeni gelişen olay karşısında kanaat geliştirme gayreti içerisinde analist, karar alıcının anlayışını derinleştirmek adına zamanla yarışarak hızlı bir sonuca varmak zorundadır (Johnson, 2003, s.648).

*Analiste bağlı olması.* Bilimsel araştırmada, araştırmacının kendisi araştırmayı yürüten bir rol üstlenir, öznel yargılarda bulunmaz, sonuç üzerindeki etkisinin sınırlı olması beklenir. Ortaya çıkan bilimsel bilgiden araştırmacı sorumlu değildir. Bilim insanı için kullanacağı yöntem, doğru toplama teknikleri, doğru kaynaklar, doğru metodoloji vb. unsurlar iyi bir bilimsel araştırma için yeterli olabilir. Keza bilim hata yaptığında denetime tabi tutulur. Ölçek, veri ve metodoloji bilgisi tekrar edilebilirlik sağlar. Dolayısıyla farklı grupların aynı sonuçlara ulaşması sağlanmış olur. Bu da test edilen hipotezlerden elde edilen sonuçlara güvenmeyi sağlar (Bruce, 2008, s.178).

İstihbarat analizinde ise aynı verileri inceleyen analistler farklı sonuçlara ulaşabilir veya farklı verilerden aynı sonuçlara ulaşabilirler (Marrin, 2012a, s.86). Nihayetinde elde edilen verilerin kalitesinin ölçümü, verilerin değerlendirmesi, verilerin doğruluğunun ölçümü daha çok analistin deneyimlerine ve muhakeme kabiliyetine bağlıdır (Mathams, 1995, s.84). İstihbarat analizinde teknikler yalnızca araçtır. Burada analistin donanımı, kullandığı metodolojiden çok daha önemlidir. Ne kadar bilimsel metodoloji kullanılmaya çalışırsa çalışırsın, nesnellığe yaklaşılmaya çalışılsın, istihbarat analizi nihayetinde analistin zihninde şekillenen bir sonuca ulaşır. Bilimsel araştırmanın aksine, analiz sonucu ortaya çıkan ve karar alıcıya sunulan bilgiden istihbarat servisi sorumludur.

*Sezgi unsurunun önemi.* Analist zamanının kısıtlı olması sebebiyle, az kanıtla olabildiğince doğru sonuçlara hızlı bir biçimde varmaya çalışır. Buradaki boşlukları ise, deneyimleri ve konu üzerindeki uzmanlığı ile doldurmaya çalışır (Mathams, 1995, s.87). Keynes’e (2013, s.76) göre, bu

bilgi boşlukları “sezgi” ile dolmaktadır. Folker (2000, s.5) sezgiyi, "... muhakeme süreçlerini kullanmayan ve analist tarafından mevcut kanıtlarla yeterince açıklanamayan bir duygu veya içgüdüdür" şeklinde tanımlar. Betts'e (2008, s.93) göre analist, bu zamansız ve belirsiz ortamda, bir sonuca ulaşmak adına sezgilerinin analizi yönlendirmesine izin vermek durumunda kalır. Sosyal bilimlerde de araştırma sorusunu tasarlarken araştırmacının yaratıcı sezgiye ihtiyacı vardır, ancak istihbarat analizinde bilgi boşlukları doldurulmalıdır, dolayısıyla yaratıcılık, hayal gücü ve spekülatif yorum istihbarat analizinde çok daha önemli bir rol oynar (Phythian, 2017, s.603). Bu noktada istihbarat literatüründe bir kısım, istihbarat analizinin büyük ölçüde sezgi, bilgi, eğitim ve tecrübe ile öğrenilebilecek usta-çırak ilişkisine dayanan bir sanat olduğunu vurgular. Diğer taraftan istihbaratın büyük ölçüde yapılandırılmış, sistematik analitik yöntemlere bağlı olan bir bilim olduğu iddiasında bulunanlar ile “istihbarat bir bilim mi yoksa sanat mı?” tartışması yapılmaktadır (Folker, 2000, s.6). Son zamanlarda, istihbaratın birbirine zıt olmayan bu iki unsuru da kullanan bir meslek olduğu vurgusu yapılmaktadır.<sup>3</sup>

## **SONUÇ**

İstihbarat analizi nesnel yöntemlerle ve nesnel bilgiler vasıtasıyla hedef ile ilgili kapsamlı bir durum tanımlaması yapar, fırsat ve tehditleri belirler, güçlü ve zayıf yönleri ortaya koyar, niyet tespiti yapmaya çalışır. Nihayetinde ise ön uyarı sağlamak ve öngörüsü yüksek sonuçlara ulaşmaya çalıştırarak karar alıcıya seçenekler sunar. Bilimsel araştırma ile istihbarat analizinin benzeştiği nokta analistin fenomenleri açıklamak ve sorunları incelemek üzere durum tanımlaması yaptığı noktadır. Bu noktada analist, verilerin toplanması, işlenmesi ve yorumlama sürecinde bilimsel metodoloji ve bilimsel disipline ihtiyaç duyar. Bu noktadan sonra incelenen olay, amaç ve çıktı başta olmak üzere farklılaşmalar başlar.

İstihbarat analisti, bir olayın tanımlanması için evveliyatına ihtiyaç duyuyor olsa da incelediği olay genellikle yeni gerçekleşmiş bir olaydır ve yeterli veri olmaz. Akademik araştırmalarda ise genellikle araştırmacı, üzerinden yeterli zaman geçmiş bir olay ve etkileri üzerine çalışmalar yapar. Dolayısıyla analist, belirsiz ortamlar üzerinde çalışıyor olur, karar alıcıya ise nihayetinde tahminler ve öngörüler barındıran bir rapor verir. Temel amaç

---

<sup>3</sup> Tartışma için bkz. Marrin, S. (2012b). Is intelligence analysis an art or a science?. International Journal of Intelligence and CounterIntelligence, 25(3), 529-545.

karar alıcının ihtiyaçlarına cevap vermektir. Araştırmacı ise araştırmasında teorik kalıplarla açıklamalarla ilgilenir ve bilimsel bilgiye hizmet eder. Neticesinde belirsiz bir ortam üzerinde çalışmadığı gibi öngöründe bulunma misyonu da gütmaz. Dolayısıyla istihbarat metodoloji olarak bilimsel konseptin bir türevini kullanıyor olsa da istihbarat sonucu elde edilen çıktı, bilimsel bilgi nesnellğinde olmayacaktır.

Farkların tümü genel olarak; araştırma sorusunun verilişi, araştırılan olayın farkı, amaç olarak farkı, belirsizlik, öngörüler, çıktının farkı, kaynaklar, gizlilik epistemolojisi, aldatma unsuru, zaman kısıtlılığı, araştırma sonucunun analiste bağılı olması ve sezgi unsurunun önemi, noktalarında sınıflandırılabilir.

## **KAYNAKÇA**

- Ben-Israel, I. (1989). Philosophy and methodology of intelligence: The logic of estimate process. *Intelligence and National Security*, 4(3), 660-718.
- Beşe, E., & Seren, M. (2011). Stratejik İstihbarat Olgusunun Teorik Çerçevesi, Unsurları ve Terörle Mücadele Politikaları Açısından Rolü ve Önemi. *Turkish Journal of Police Studies/Polis Bilimleri Dergisi*, (13)3, 123-145.
- Betts, R. K. (2008). Analysis, War, and Decision: Why intelligence failures are inevitable. *In Intelligence Theory* (ss. 101-125). Routledge.
- Bruce, J. B. (2008). Making analysis more reliable: Why epistemology matters to intelligence. *Analyzing intelligence: Origins, obstacles, and innovations* (ss.171-190). Georgetown University Press.
- CIA. (2010). A Look Back... Sherman Kent: The Father of Intelligence. *News and Information*. <https://www.cia.gov/news-information/featured-story-archive/2010-featured-story-archive/shermankent-the-father-of-intelligence.html> [Erişim Tarihi: 09.11.2020].
- Clark, R. M. (2013). *Intelligence analysis: a target-centric approach*. CQ press.
- Clauser, J. (2008). *An introduction to intelligence research and analysis*. Scarecrow Press.
- Fingar, T. (2011). *Reducing uncertainty: Intelligence analysis and national security*. Stanford University Press.



- Folker, R. D. (2000). *Intelligence analysis in theater joint intelligence centers: An experiment in applying structured methods*. Joint Military Intelligence College.
- Garst, R. D., & Gross, M. L. (1997). On becoming an intelligence analyst. *Defense Intelligence Journal*, 6(2), 47-59.
- George, R. Z., & Bruce, J. B. (Eds.). (2008). *Analyzing intelligence: Origins, obstacles, and innovations*. Georgetown University Press.
- Göktaş, O. (2018). Büyük veya Doğal Arnavutluk İdeali'nin Stratejik İstihbarat Analizi. Doktora Tezi. Polis Akademisi Güvenlik Bilimleri Enstitüsü.
- Hedley, J. H. (2007). Analysis for strategic intelligence. *In Handbook of intelligence studies* (ss. 229-244). Routledge.
- Heuer, R. J. (2019). Adapting Academic Methods and Models to Governmental Needs. *In Quantitative Approaches to Political Intelligence* (ss. 1-10). Routledge.
- Horn, E. (2003). Knowing the enemy: The epistemology of secret intelligence. *Grey Room*, (11), 58-85.
- Hudoğlu, M.& Ak, G. Stratejik istihbarat analizinde öngörülebilirliğin doğası: Kaos Teorisi ışığında yeni bir muhakeme denemesi. *Florya Chronicles of Political Economy*, 8(2), 23-40.
- Johnson, L. K. (2003). Preface to a theory of strategic intelligence. *International journal of intelligence and counterintelligence*, 16(4), 638-663.
- Johnson, L. K. (2008). Sketches for a theory of strategic intelligence. *In Intelligence Theory* (ss. 47-67). Routledge.
- Karabacak, T. (2002). İstihbarat Biriminin Çalışma Yöntemleri. *Avrasya Dosyası*, 8(2).
- Kent, S. (2015). *Strategic intelligence for American world policy*. Vol. 2377. Princeton University Press.
- Keynes, J. M. (2013). *A treatise on probability*. Courier Corporation.
- Kuosa, T. (2014). *Towards strategic intelligence: foresight, intelligence, and policy-making*. Dynamic Futures.
- Marrin, S. (2012a). *Improving intelligence analysis: Bridging the gap between scholarship and practice*. Routledge.
- Marrin, S. (2012b). Is intelligence analysis an art or a science?. *International Journal of Intelligence and CounterIntelligence*, 25(3), 529-545.

- Mathams, R. H. (1995). The Intelligence Analyst's Notebook. *Strategic Intelligence: Theory and Application* (ss.77-96). United States Army War College.
- McDowell, D. (2009). *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users*. The Scarecrow Press.
- Pherson, R. H., & Heuer Jr, R. J. (2020). *Structured analytic techniques for intelligence analysis*. Cq Press.
- Phythian, M. (2017). Intelligence analysis and social science methods: exploring the potential for and possible limits of mutual learning. *Intelligence and National Security*, 32(5), 600-612.
- Platt, W. (1957). *Strategic Intelligence production: basic principles*. FA Praeger.
- Prunckun, H. (2010). *Handbook of scientific methods of inquiry for intelligence analysis*. Scarecrow Press.
- Scott, L., & Jackson, P. (2004). The study of intelligence in theory and practice. *Intelligence & National Security*, 19(2), 139-169.
- Seren, M. (2017). *Stratejik istihbarat ve ulusal güvenlik*. Ankara: Orion Publishing.
- Shulsky, A. N., & Schmitt, G. J. (2002). *Silent warfare: understanding the world of intelligence*. Potomac Books, Inc.
- Tuzcu, M.E. (2013). İstihbarat Analizinde Belirsizlik Faktörü ile Çalışma Yöntemleri ve Bilimselliğin Önemi. Yüksek Lisans Tezi. Harp Akademileri Stratejik Araştırmalar Enstitüsü.
- Warner, M. (2002). Wanted: A Definition of "Intelligence" Understanding Out Craft. *Studies in Intelligence*. 46(3), 15-22.
- Warner, M. (2008). Intelligence as risk shifting. *In Intelligence Theory* (ss. 30-46). Routledge.
- Yılmaz, S. (2019). *Temel İstihbarat: Toplama, Analiz ve Operasyonlar*. Ankara: Kripto Kitaplar.

## 21'NCİ YÜZYILDA AÇIK KAYNAK İSTİHBARATI

Tolga ÖKTEN\*

### ÖZET

Açık kaynaklar, günümüz istihbarat çalışmalarında yoğun olarak tartışılan bir konu başlığıdır. Birçok profesyonel, istihbaratın mutlaka gizli haber toplama faaliyetlerine dayanması gerektiğini ve bilgiye ulaşmanın kolay ve kısa bir yolu olmayacağını savunmaktadır. Diğerleri içinse açık kaynak istihbaratı yeni bir dönemi işaret etmektedir. Bu makalede, istihbarat çalışmaları literatüründe genelde teknoloji özelde ise açık kaynak başlığı altında yer alan bazı temel konu başlıklarının okuyuculara tanıtılması ve tartışılması amaçlanmıştır. Ayrıca, Türkçe terminoloji oluşturma sürecine de katkı sağlamak istenmektedir. Tartışma başlıkları; istihbaratın demokratikleşmesi, toplama-analiz ikiliği, görev ve kadro tanımlarındaki dönüşüm, açık kaynakların önleyici istihbarattaki güçlü ve zayıf yanları ile istihbarat zafiyeti olarak belirlenmiştir. Bu başlıklar etrafında istihbaratın 21. yüzyıldaki dönüşümü ve yol haritası tartışılmıştır.

**Anahtar Kelimeler:** *Açık Kaynak, Teknoloji, Dönüşüm, Toplama, Analiz.*

## OPEN SOURCE INTELLIGENCE IN THE 21<sup>TH</sup> CENTURY

### ABSTRACT

Open sources are an important topic of discussion in contemporary intelligence studies. Many professionals argue that intelligence should be based on covert intelligence collection methods and there is no easy way or shortcut to access information. For others, open-source intelligence indicates a new era in intelligence. Accordingly, in this study, some of the primary debates in the intelligence studies literature under technology generally and open source specifically are introduced and examined. Besides, it intends to contribute to the efforts of forming Turkish terminology. The main discussion topics are the democratization of intelligence, collection-analysis duality, transformation in job descriptions, strengths and weaknesses of open sources in warning intelligence, and intelligence failure. Around these topics, the transformation and the road map of intelligence are discussed.

**Key Words:** *Open-Source, Technology, Transformation, Collection, Analysis.*

## GİRİŞ

İstihbarat, en basit tanımıyla sistemdeki aktörleri anlamak, etkilemek ve önlemek amacıyla yürütülen gizli faaliyetlerdir. Bunun başarılabilmesi

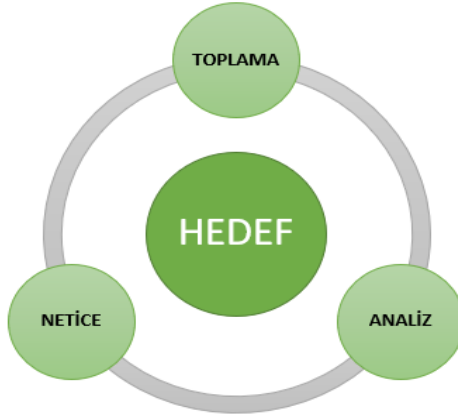
---

\* Öğretim Görevlisi Tolga ÖKTEN, Milli Savunma Üniversitesi, Atatürk Stratejik Araştırmalar Enstitüsü, [tolgaokten1982@gmail.com](mailto:tolgaokten1982@gmail.com), ORCID: 0000-0002-6102-7704  
Makale Başvuru Tarihi / Application Date: 09 Kasım 2022 / 09 November 2022  
Makale Kabul Tarihi / Acceptance Date: 05 Aralık 2022 / 05 December 2022

için siyasi ve bürokratik karar alıcılar tarafından belirlenen önceliklere yönelik olarak yürütülen toplama faaliyeti neticesinde elde edilen bilgilerin<sup>1</sup> analizi ve sürecin zamanında neticelendirilmesi gerekmektedir. İstihbarat çarkı olarak da tanımlanan bu süreç istihbarat mesleğini teorik bir zemine oturtmaktadır.

İstihbarat teşkilatı personelinin temel görevi, hedef öncelikleri çerçevesinde yeni kaynaklar yaratmak, mevcutları yönetmek ve toplanan bilgilerin doğruluğunu ve güvenilirliğini analiz ederek faaliyeti neticelendirmektedir (Şekil-1). Önceliklerin belirlenmesi ve neticelendirme aşaması istihbarat teşkilatlarının karar alıcılar ile arasındaki bağlantıyı oluşturur. Toplama ve analiz ise teşkilatın içine ayna tutar ve mesleğin özünü oluşturmaktadır. Her faaliyetin<sup>2</sup> kendi karakteri olmakla birlikte istihbarat mesleğinin doğası aynıdır ve süreç her birimde genellikle bu şekilde yürütülür.

Şekil 1: İstihbarat Çarkı (Kaynak: Yazar tarafından hazırlanmıştır)



Bilgi farklı kaynaklardan toplanmaktadır. Mesleğin kökeni espionaj faaliyeti olarak da adlandırılan insan istihbaratına,<sup>3</sup> diğer bir deyişle casuslara dayanmakla birlikte, teknoloji geliştikçe teknik istihbarat kaynakları da denkleme girmiş ve kaynak çeşitliliği sağlanmıştır. Özellikle

<sup>1</sup> Türk istihbarat literatüründe bilgiye haber de denilmektedir. Bu çalışmada iki terim birbiri yerine kullanılmıştır.

<sup>2</sup> Faaliyet; ülke, bölge, konu, görev vb. farklı başlıklar altında bölümlenebilir.

<sup>3</sup> İnsana dayalı istihbarat İngilizce literatürde Human Intelligence (HUMINT), Türkçe literatürde ise İNİS olarak kısaltılabilmektedir. Çalışmada kısaltma kullanılmamıştır.

internet teknolojisinde yaşanan gelişmeler, istihbaratın önemli bir parçası olan gizlilik boyutunu aşındırmaya başlamıştır. Günümüzde bilgisayar başından kalkmadan stratejik ve taktik istihbarat öncelikleri hakkında önemli bilgiler toplanabilmekte ve analiz edilebilmektedir. Açık kaynak<sup>1</sup> olarak adlandırılan bu veriler; askeri birliklerin konumlarının tespitinden, savaş suçlarının belgelenmesine, radikalleşme emarelerinin tespitinden, terör eylemlerinin soruşturulmasına kadar geniş bir yelpazede kullanılmaktadır. Ayrıca, stratejik öncelikleri oluşturan, örgüt içerisindeki hizipleşmeler, lider kadrolardaki değişiklikler, alınan siyasi kararlar, diplomatik gelişmeler ve dezenformasyon faaliyetleri de açık kaynaklar üzerinden takip edilerek yorumlanabilmektedir.

Bu çalışmanın amacı 21. yüzyıla damga vuran açık kaynak teknolojisinin istihbarat faaliyeti üzerindeki etkilerinin tartışılmasıdır. Bu kapsamda, istihbarat çalışmaları literatüründe genelde teknoloji özelde ise açık kaynak başlığı altında yer alan bazı temel konu başlıklarının okuyuculara tanıtılması ve tartışılması amaçlanmıştır. Açıklayıcı olması amacıyla, teorik çerçeve, örnek vakalar üzerinden detaylandırılmıştır. Çalışmanın bir diğer amacı da Türkçe terminoloji oluşturma sürecine katkı sağlamaktır.

Makalede öncelikle açık kaynak tanımı kavramsallaştırılmıştır. Sonrasında ortaya çıktığı değerlendirilen etkiler birkaç alt başlık üzerinden tartışılmıştır. Bu alt başlıklar hipotezler üzerinden formüle edilmiştir. Son bölümde ise bulgular özetlenmiştir.

*H-1: Açık kaynak teknolojisi istihbarat faaliyetini tabana yayarak alanı demokratikleştirmiştir.*

*H-2: Açık kaynaklar toplama-analiz ikiliğini analiz lehine azaltmıştır.*

*H-3: Açık kaynaklar istihbarat teşkilatlarının kadro ve görev tanımlarında dönüşümü tetiklemiştir.*

*H-4: Açık kaynakların zayıf yanı, proaktif olmaktan ziyade reaktif olması ve bu nedenle önleyici istihbarat faaliyetindeki etkisinin sınırlı kalmasıdır.*

*H-5: Açık kaynakların terör/güvenlik istihbaratında en fazla potansiyel vaat ettiği nokta siber alan hakimiyeti sağlanmasıdır.*

---

<sup>1</sup> Açık kaynak istihbaratı İngilizce literatürde Open-Source Intelligence (OSINT), Türkçe literatürde ise AKİS olarak kısaltılabilmektedir. Çalışmada kısaltma kullanılmamıştır.

*H-6: Açık kaynakların geriye yönelik çok güçlü bir araştırma yöntemi olması nedeniyle, istihbarat zaafiyeti başlığı altındaki öngörü yanlışları artmıştır.*

## **1. AÇIK KAYNAK İSTİHBARATININ KAVRAMSALLAŞTIRILMASI**

Teknik ve insana dayalı bilgi; açık, yarı açık ya da gizli kaynaklara dayanmaktadır. Gizli kaynaklar üzerinden yapılan haber toplama işlemi sadece bir imkân değil aynı zamanda bir yetki meselesidir. Yasa dışı bir faaliyetin içerisinde yer alan insanların para karşılığı çalıştırılması ya da bir hedefin dinlenmesi sürecinin sınırları yasal çerçeveler ile belirlenmektedir. Açık kaynaklar ise herkes tarafından kullanılabilir ve bu nedenle istihbarat mesleğinin görünür yüzüdür.

Açık kaynakların 20. yüzyıl öncesinde fiziki olarak elde edilen yazılı metinlerden oluştuğu görülmektedir. 20. yüzyılda buna elektronik dalgalar üzerinden yayılan radyo ve televizyonlar da eklenmiştir. Bu yüzyılda görüntü<sup>1</sup> ve sinyal istihbaratı<sup>2</sup> alanında çok büyük ilerlemeler yaşanmıştır. 21. yüzyılda ise mecra giderek siber alana doğru kaymıştır. Bu çerçevede günümüzde açık kaynak ile internette bulunan büyük verinin eşanlamlı olarak kullanılmaya başlandığı söylenebilecektir.

Bu noktada internette yer alan bütün bilgiler açık kaynak olarak kabul edilebilir mi sorusu ön plana çıkmaktadır. Bu soru çerçevesinde açık kaynaklar dar ve geniş olarak iki şekilde kavramsallaştırılabilecektir (Tablo-1). Dar anlamıyla, sahibi tarafından bilinçli olarak yüklenen bilgilerden oluşmaktadır (Steele, 2019). Bu tanıma üçüncü şahıslar tarafından çalınarak toplumun kullanımına sunulan bilgiler de eklenebilecektir.<sup>3</sup> Arama motorları üzerinden yasal olarak ulaşılabilecek olan; haber programları, uzman görüşlerini içeren röportaj, dergi, kitap ve raporlar, ticari uydu görüntüleri ile internet sitelerine ve sosyal paylaşım platformlarına yüklenen fotoğraf, video vb. yapılandırılmış ve yapılandırılmamış veriler bu tanıma girmektedir. Geniş tanım ise internette kullanıma bilinçli olarak açılmış verilerin yanı sıra, ağ üzerinde bulunan ancak çeşitli şifreleme yöntemleri ile korunan bilgileri de içermektedir. Resmi ve özel kurumlarda bulunan kişisel veriler,

---

<sup>1</sup> Görüntü istihbaratı İngilizce literatürde Imagery Intelligence (IMINT), Türkçe literatürde ise GÖRİS olarak kısaltılabilmektedir. Çalışmada kısaltma kullanılmamıştır.

<sup>2</sup> Sinyal istihbaratı İngilizce literatürde Signal Intelligence (SIGINT), Türkçe literatürde ise SİNİS olarak kısaltılabilmektedir. Çalışmada kısaltma kullanılmamıştır.

<sup>3</sup> İkinci duruma örnek olarak Wikileaks belgeleri verilebilir. Özü itibarıyla gizli bilgi olan diplomatik kriptolar Irak'ta görevli bir Amerikan ordu personeli olan Bradley Edward Manning tarafından sızdırılmış ve internette yayımlanmıştır.

banka hesap bilgileri, e-posta ve online konferanslar gibi internet görüşmeleri bu tanıma dahil edilebilecektir. Bu bilgiler yarı açık kaynak olarak da adlandırılabilir.<sup>1</sup> Bu bilgiler kişisel veri düzenlemeleri çerçevesinde korunan ve sadece ilgili kurum yetkililerin sorgulayabileceği bilgilerdir.<sup>2</sup> Geniş kavramsallaştırma açık kaynakların istihbarat faaliyetinde kapladığı yeri çok fazla genişletmiştir. 20. yüzyılda fiziki olarak güvenli binalarda ve kasalarda saklanması ve bu yüzden açık olmaması gereken birçok bilgiye günümüzde internet üzerinden ulaşılabilir. Günümüzde, veri bir kez ağa yüklendikten sonra bunlara ulaşılabilir ve manipüle edilebilir.

Tablo 1. Açık Kaynak Kavramsallaştırmaları (Kaynak: Yazar tarafından hazırlanmıştır)

DAR KAVRAMSALLAŞTIRMA	GENİŞ KAVRAMSALLAŞTIRMA
Haber programları Uzman görüşleri Dergi, kitap ve raporlar Ticari uydu görüntüleri Yüz tanıma, Flight Radar vb. internet uygulamaları İnternet sitelerine ve sosyal paylaşım platformlarına yüklenen medya	Şifreli sosyal medya hesapları Kamu kuruluşlarının veri tabanlarında bulunan bilgiler Kişisel Verileri Koruma Kanunu kapsamındaki diğer veriler

Bazı senaryolarda akıllı telefon uygulamaları vasıtasıyla, biyografik bilgilerin yanı sıra konum ve görüşme verileri gibi anlık bilgiler elde edilebilmekte ayrıca kişisel bilgisayarların harddiskinde bulunan verilere ulaşılabilir. Ancak bunlar için cihazlara teknik yerleşme yapılmalıdır. Bu faaliyet için ya kullanıcının ya da ikinci bir şahsın telefona virüs programı yüklemesi gerekir. Bilgisayarların harddiskinde, akıllı telefonlarda ya da şifreli hesaplarda bulunan verilere ulaşmak istihbarat teşkilatlarınca sıklıkla uygulanan bir taktiktir.<sup>3</sup> Mahkeme kararı ile yapılan iletişimin dinlenmesi faaliyeti gibi bu yöntem de gizli kaynak olarak kabul edilmektedir. Yetkili olmayan şahıslarca yapılması durumunda suç oluşturmaktadır.

<sup>1</sup> Yarı açık kaynaklar literatürde Proprietary Intelligence – PROPINT olarak da adlandırılmaktadır (Denécé, 2014, s.35)

<sup>2</sup> Türkiye’de bu veriler 6698 sayılı Kişisel Verilerin Korunma Kanunu ile korunmaktadır. (www.mevzuat.gov.tr, 2016)

<sup>3</sup> Pegasus yazılımının kullanılması bu duruma örnek olarak verilebilir. (www.europarl.europa.eu, 2022)

Her seviyedeki kullanıcının açık kaynak istihbaratının farklı tonlarında aktif olduğu söylenebilecektir. Amatör seviyedeki kullanıcılar firmaların sağladığı imkanları kullanırken<sup>1</sup>, teşkilatların ve diğer profesyonel kullanıcıların yarı açık kaynak olarak tanımlanan alanda daha aktif oldukları görülmektedir.

## 2. AÇIK KAYNAKLARIN İSTİHBARAT FAALİYETİ ÜZERİNDEKİ ETKİLERİ

Çalışmada açık kaynakların istihbarat üzerindeki etkileri çeşitli alt başlıklarda incelenmiştir. Bu alt başlıklar hipotezler şeklinde tartışılmıştır.

*H-1: Açık kaynak teknolojisi istihbarat faaliyetini tabana yayarak alanı demokratikleştirmiştir.*

Teknoloji bir işin nasıl yapılacağını ya da yapılmayacağını belirleyen en önemli değişkenlerden bir tanesidir. Bu nedenle sadece istihbaratta değil diğer alanlarda da oyunun kurallarını değiştiren bir etken olarak görülmüştür. İster savaş ister bankacılık olsun işlerin teknoloji sayesinde eskisinden çok daha farklı ve kolay bir şekilde yürütülebileceği görüşü yaygındır.

Açık kaynak teknolojisinin, yarattığı fırsatlar ile istihbarat faaliyetini tabana yayarak alanı demokratikleştirdiği ileri sürülmektedir (Wheaton, 2019). Aslında demokratikleşme, istihbaratın masa başı bir iş haline geldiği anlamına gelmektedir. Bu noktada, bütün bilgiler ulaşılabilir olduğuna göre açık kaynak analizi yapan siviller ve özel sektör bileşenlerinin post-modern istihbaratçılar haline geldiğini ve hedefe yaklaşarak risk almadan, bilgisayar başında istihbarat üretilebileceğini iddia edebilir miyiz sorusu ön plana çıkmaktadır. Konuyu bir metaforla açıklamak gerekirse, bu soru, bütün kaynaklara internette ulaştıktan sonra zahmet edip kütüphaneye gitmeye gerek var mıdır sorusudur.

Bu noktada, istihbarat analizinin büyük bölümünün açık kaynaklardan yararlanılarak hazırlandığı ve çok az bir kısmının gizli bilgi içerdiği görüşü ön plana çıkmaktadır (Johnson, 2009, s.42).<sup>2</sup> Açık kaynak bilgileri istihbarat mıdır sorusunu bir kenara bırakmak gerekirse bile, bu yanlış bir genelleme ve doğru bilinen bir yanlıştır. Dışa açık bir ülkenin makro ekonomik

---

<sup>1</sup> Örneğin Flight Radar ve Google Earth açık kaynak analizinde sıklıkla kullanılmaktadır.

<sup>2</sup> Buna karşı çıkan görüşe göre istihbarat faaliyeti mutlaka gizli bilgiye dayanmalıdır ve bilgiye ulaşmak ne kadar zorsa bilgi o kadar değerlidir. Lowenthal bu görüşü eleştirmektedir (Lowenthal, 2008, ss.182-185).



göstergeleri hakkında toplanan veriler açısından bu doğru olabilir ancak örgüt hücrelerine dair toplanan bilginin çok az bir bölümü açık kaynaktan toplanır. Özellikle teknolojinin kullanımının kısıtlı olduğu kırsal alana yönelik taktik istihbarat faaliyeti açısından kullanım alanı çok dardır.

Bu noktada istihbarat ürününün niteliği de önemlidir. Bir konu başlığında hazırlanan ülke analizi açık kaynaklar üzerinden ilerleyebilir ancak eylem ikaz istihbaratında durum karmaşılaşır. Özellikle önleyici faaliyetleri oluşturan istihbarata karşı koyma ve terörle mücadele konularında açık kaynak bilgileri çok sınırlıdır ve genellikle istihbarat değeri bulunmamaktadır. Bir tepenin ya da sokağın görüntüsüne Google Earth'den ulaşılabilir ancak hücre evinin ya da sığınacağın konumunu gösterecek olan birine ihtiyaç vardır. Benzer bir şekilde, bir telefon hattının kimin adına kayıtlı olduğu yarı açık kaynak bilgisidir, ancak hattı kimin kullandığı bilgisi saklanmaktadır ve tespit edilebilmesi için farklı yöntemlere başvurulması gerekir.

Konunun daha iyi anlaşılabilmesi için stratejik-taktik istihbarat önceliği ayrımı yapılması da gerekmektedir. Bir terör örgütünün herhangi bir ülkeyi hedef alacağını ilan etmesi o ülke açısından stratejik bir istihbarat önceliğidir. Diğer taraftan bu karar örgüt açısından da stratejik bir karar olduğu için kamuoyuna ve tabanına medya kanalları üzerinden açıklanmaktadır. Bu tarz bilgiler açık kaynak istihbaratı üzerinden toplanarak analiz edilebilir. Bunlar 5N1K'nın "ne" ve "neden" sorularıdır. Diğer taraftan, saldırının "kim" tarafından, "ne zaman", "nereye" ve "nasıl" yapılacağı taktik istihbarat boyutudur ve bu bilgiler çoğunlukla açık kaynaklarda yer almaz. Aslında, bu tartışma sadece açık kaynak teknolojisi için değil, uydu ve uçak gibi ileri teknoloji ürünü cihazlara dayanan teknik istihbarat faaliyeti için de geçerlidir. Örneğin, Soğuk Savaş boyunca uydu ve U-2'lerden gelen teknik istihbarata dayanılmasının, insan boyutunu ikinci plana atarak Sovyet nükleer silah kapasitesinin tespitinde hatalara yol açtığı belirtilmektedir (Freedman, 1977).

Diğer taraftan açık kaynak teknolojisi stratejik öncelikler açısından kamu ve özel sektör bileşenleri arasında önemli bir iş birliği potansiyeli sunmaktadır (Lahneman, 2016, ss.12-14). Daha önce belirtildiği üzere açık kaynaklar mesleğin görünen yüzüdür ve istihbarat teşkilatları ile sivil araştırmacılar arasındaki sınırı oluşturmaktadır. Bu sınır her geçen gün daha fazla geçirgen hale gelmektedir. Bu çerçevede özellikle stratejik istihbarat

önceliklerinde açık kaynakların rolü ve iş birliği fırsatları giderek artmaktadır. Kabul etmek gerekir ki, stratejik istihbarat analizi sürecinin en önemli aktörleri konu/bölge uzmanlarıdır. Yıllarca aynı konu/bölge üzerinde çalışmış, ilgili ülkelerde bulunmuş, büyük ihtimalle bölge diline, kültürüne ve siyasetine hâkim kişilerdir. Bu noktada istihbaratçılara göre çok daha uzmanlaşabilme potansiyelleri vardır (Johnson, 2009, s.42). Örneğin bir teşkilat mensubuna ekonomi öğretmektense bir ekonomiste analiz edeceği bilgileri vermek daha mantıklıdır. 20. yüzyılda gizli kalması gereken birçok bilgi ve belgeye günümüzde internetten kolaylıkla ulaşılabilmekte bu sayede konu hakkında uzmanlığı bulunan akademisyen ve diğer sivil uzmanların analiz sürecine katkı yapmaları çok daha kolaylaşmaktadır.

*H-2: Açık kaynaklar toplama-analiz ikiliğini analiz lehine azaltmıştır.*

İstihbarat çalışmaları literatüründe yer alan toplama-analiz ikiliği sadece masa başında yapılan felsefi bir tartışma değil, mesleğin her anında yaşanan bir olgudur. Her iki aşamanın da taraftarları, gelenekleri, teknikleri ve örgütleri vardır.

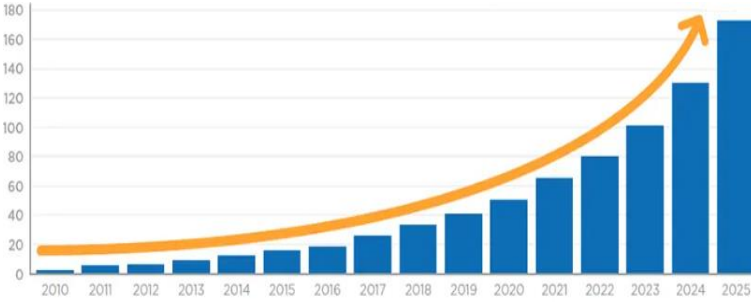
İlk bakışta açık kaynak istihbaratının bir toplama aracı olduğu düşünülebilecektir. Açık kaynak istihbaratını, insan istihbaratı ya da sinyal istihbaratı gibi ayrı bir toplama disiplini olarak kabul eden çalışmalar da bulunmaktadır (Field Manuel 2-0, s.I-30) (Lowenthal, 2008, s.187) (Johnson, 2014, s.9) (Wirtz ve Rosenwasser, 2010, s.726). Diğer taraftan açık kaynak istihbaratı özü itibariyle toplama değil bir analiz faaliyetidir.

Toplama ve analizin aşamalarının merkezinde teknoloji olmasına rağmen, analiz kapasitesi toplama kapasitesine oranla çok daha yavaş ilerlemektedir. Teknoloji veri toplama ve işleme kapasitesini arttırmıştır ancak üretilen istihbarat aynı hızla artmamıştır (Lowenthal, 2008, s.184). Yapay zekâ uygulamaları sayesinde veri madenciliği ve analiz teknikleri sürekli gelişmekte, ancak alınan kararlar eninde sonunda insan zihninin algılama kapasitesine dayanmaktadır. Sistemin toplam kapasitesini de belirleyen bu darboğazı, toplanan veri yığınına analiz edebilecek nitelikteki programlar ve personel oluşturmaktadır. Bu nedenle analiz aşamasının açık kaynak istihbaratının ağırlık merkezini oluşturduğunu söylemek yanlış olmayacaktır.

Analizin artan öneminin en önemli nedeni, açık kaynaklara dayalı toplamanın artık bir yetenekten ziyade standart haline gelmesidir. Gelişen bilgisayar teknolojisi sayesinde hedef ekosistemine yönelik olarak toplama

(*bulk collection*) rutin bir işlem haline gelmiştir (Gill ve Phythian, 2018, s.322). İnternet ve akıllı telefon teknolojisi ile birlikte bir haber patlaması yaşanmıştır ve toplanan veri her geçen gün çığ gibi büyümektedir. İnternetteki veri sayısı 2010-2018 arasında yaklaşık 30 kat artmıştır ve hızla artmaya devam etmektedir (Grafik-1). 2018'de 33 zetabayt olan verinin 2025'te 175 zetabayta ulaşması beklenmektedir (www.i-scoop.eu). Bu verinin yaklaşık yarısı gerçek zamanlı olarak paylaşılan veridir (www.statista.com). Bu çerçevede internetin istihbarat teşkilatları için bir süper arşiv haline geldiği söylenebilecektir. Teorik olarak internet üzerinden hemen her türlü bilgiye ulaşılabilir. Bu durum sadece istihbarat teşkilatları açısından değil sivil kullanıcılar açısından da geçerlidir. İnternete sahibi tarafından bilinçli şekilde yüklenen ya da başka taraflarca sızdırılan her türlü yapılandırılmış ya da yapılandırılmamış bilgi, bilgisayarı olan her bir kullanıcı için büyük bir veri havuzu oluşturmaktadır.

Grafik 1: İnternetteki Veri Miktarı (www.i-scoop.eu)



Analiz sürecinin amacı ise büyük veriyi yorumlayarak görselleştirmek ve operasyonel hale getirmektir. Bu aşamada da teknolojiye önemli görevler düşmektedir. Özellikle bilgi sistemleri teknolojileri (*Management Information Systems - MIS*), analizi geçmişten çok daha güçlü hale getirmiştir. 11 Eylül saldırıları bu anlamda milat olarak görülebilir. Daha önce üretim yönetimi, pazar ve müşteri analizi gibi alanlarda kullanılan bu sistemler 11 Eylül sonrasında istihbarat alanına hızlı bir giriş yapmıştır. Bu teknolojiler sayesinde; farklı istihbarat ve kolluk birimleri arasındaki bilgi paylaşımı hızlanmakta, arşiv bilgileri farklı kurumların veri tabanlarından çok daha hızlı bir şekilde çekilebilmekte, irtibat ağları ile eylem paternlerinin görselleştirilmesi ve haritalandırılması (*link analysis*) sağlanabilmekte, yarı açık kaynaklarda yer alan bilgiler tek bir ara yüzde toplanabilmektedir. Günümüzde analiz faaliyeti bu tarz kullanıcı dostu işletim sistemleri sayesinde mümkün olmaktadır. Bu kapsamda en önemli analiz araçlarından

bir tanesi sosyal ağ analizidir. Sistemin haritalandırılması ve nodların ve ilişki ağının çözülmesi açısından önemli bir kapasite sunmaktadır. Aslında sosyal ağ analizi yeni bir şey değildir ve henüz bilgisayarlar kullanılmazken bile mekanik olarak yürütülmüştür. Diğer taraftan analiz teknolojilerindeki ilerleme ve sosyal ağın giderek artan bir şekilde fiziki dünyadan açık kaynak olan sanal dünyaya kayması analizin karakterini değiştirmiştir. Diğer taraftan bu başlık altında vurgulandığı üzere analiz kapasitesi hala toplama kapasitesine yetişmekten uzaktır.

Açık kaynaklarda yaşanan bu genişleme ironik bir şekilde analistlerin iş yükünü arttırmıştır. Şu anda sistemde çok fazla uyarın vardır ve bu gürültü içerisinde sinyalleri tespit etmek çok zordur.<sup>1</sup> Her ne kadar algoritmalar vasıtasıyla filtrelenseler de çok fazla gereksiz bilgi akışı mevcuttur. Sıfır hata prensibi nedeniyle her bilgi eninde sonunda incelenmek zorundadır. Bilgisayar üzerinden mesajlar anlık olarak paylaşılmaktadır ancak bilgilerin analiz edilmesi zaman alan bir süreçtir ve analistlerin iş yükü her gün daha da artmaktadır.

20. yüzyıl istihbaratçılığında, haber toplama faaliyetinin istihbarat çarkının en meşakkatli kısmı olduğu görülmektedir. Bir şehrin detaylı haritası, silahın teknik özellikleri, askeri üssün fotoğrafı, siyasi liderlerin biyografilerine ulaşmak mesleğin önemli bir parçası olmuştur. Günümüzde bu bilgilere açık kaynaklardan ulaşmak mümkündür. Bu durum büyük bir bilgi bombardımanına neden olmaktadır. Analizcilerden, bilgisayar ekranından hızla akan mesajlara işlem yapması ve internette yer alan bilgilerin sürekli takip etmesi beklenmektedir. Steril hedef önceliklerine sahip olmak giderek zorlaşmakta ve sayı odaklı bir performans beklentisi yerleşmektedir.

*H-3: Açık kaynaklar istihbarat teşkilatlarının kadro ve görev tanımlarında dönüşümü tetiklemiştir.*

Geleneksel olarak toplama ile analiz arasında bir duvar bulunmaktadır (Herman, 1998, s.5). Analiz teknolojileri bu duvarı giderek şeffaflaştırmakta, istihbarat personelinin görev tanımları ve kadroları da bu durumdan etkilenmektedir. Bu tartışma 4. Nesil İstihbarat kavramını da gündeme getirmiştir. Bu teoriye göre, yeni dönemde dijital ve biyolojik analiz

---

<sup>1</sup> Wohlstetter sinyal (*signal*) ve gürültü (*noise*) kavramlarını kullanmaktadır (s.3).

yöntemlerinin iç içe geçmiş ve aradaki fark bulanıklaşmıştır (Younger, 2018).

Öncelikle analizciler giderek kendi toplayıcıları haline gelmektedir (Treverton, 2019, s.145). Gelişen bilgisayar teknolojisi, veri analiz sistemleri ve açık kaynaklar sayesinde günümüzde analizciler giderek daha fazla oranda ihtiyaç duydukları bilgileri kendileri toplayabilmektedir. Farklı kurumların veri tabanlarına tek bir arayüz üzerinden ulaşılabilmesi durumunda fiziki engeller ortadan kalkmakta ve herkes kendi toplayıcısı haline dönüşmektedir. Bu nedenle hedef ülkede maske kimliklerle yaşayan ya da servislere akredite olarak çalışan toplayıcılardan beklenen bilginin içeriği de değişmiştir. Toplayıcılar artık giderek daha fazla gizli bilgi peşinde koşmak zorundadır. İnternetin yetersiz kaldığı noktalara ulaşmak ve faaliyetin içerisinde yer alan gizli bilgiyi elde edecek kaynaklar bulmalıdır. Örnek vermek gerekirse hedef şahsın ikamet adresi ya da telefon numarası bilgisayar başından bulunabilir, ancak hedefe yönelik yürütülecek operasyonel çalışmalar halen toplayıcıların görevidir.

İkinci olarak geleneksel toplama ve analiz görevlerinin yanına farklı görev tanımlarının da eklendiği görülmektedir. İnternet her ne kadar herkese açık olsa da burada yer alan yapılandırılmamış ya da korunan bilginin toplanarak analiz edilebilecek formata getirilmesi ayrı bir meslektir (Shulsky ve Schmitt, 2002, s.41). Yapılandırılmamış verinin işlenmesi analizin ilk aşamasıdır. Bazen istihbarat çarkında tasnifleme olarak da adlandırılır. Bu aşama analizin en zor ve zaman alan aşaması haline geldiği savunulmaktadır (Johnson, 1994, s.19).<sup>1</sup> Öyle ki birçok veri bu aşamayı geçememekte süper arşivin tozlu raflarında kalarak hiçbir zaman kullanılmamaktadır. Bu bilginin işlenmesi analizin bir sonraki aşamasına geçilmesi için şarttır.

Bu çerçevede, teşkilatların konu/bölge uzmanından ziyade teknik analiz uzmanına ihtiyaç duyduğu ve analizin giderek bir teknik görev haline dönüştüğü yorumu da yapılmaktadır (Treverton ve Gabbard, 2008, s.35). 20. yüzyılın aksine günümüzde analiz daha matematiksel hale gelmiştir. Python ve R gibi uygulamalar büyük veri setleri, sosyal medya uygulamaları ve haber sitelerinde bulunan büyük verinin tasnif ve analiz edilmesinde büyük kolaylıklar sağlamaktadır. Açık kaynak istihbaratı artık bilgisayar okur yazarlığı ile yürütülecek bir iş olmayı çoktan aşmış ve farklı bir uzmanlık

---

<sup>1</sup> Johnson bu tespiti dönemin National Security Agency (NSA) Başkanı Mike McConnell'a dayandırmaktadır. NSA Amerikan istihbarat yapılanmasında sinyal istihbaratının toplanmasından sorumlu temel kurumdur.

alanı haline gelmiştir. Bu nedenle günümüzde teknik analiz, veri analizi gibi adlar altında farklı bir görev tanımları, kadrolar ve taktik yenilikler ortaya çıkmıştır. Geleneksel istihbaratçılık yeteneklerinden ziyade bilgisayar diline hâkim olmayı gerektirmektedir. Bu durum geleneksel olarak destek personeli olarak görülen teknik uzmanlar artık avcıya mı dönüşmekte ve istihbarat personeli kaçınılmaz olarak mühendisler arasından mı seçilmeye başlanacak gibi bazı soruları da beraberinde getirmektedir.

Üçüncüsü, teknoloji ve yapay zekâ uygulamaları bazı görev tanımlarını ortadan kaldıracak gibi gözükmektedir. Örneğin analiz sürecinin önemli bir parçası olan tercüme faaliyeti giderek ticari uygulamalar üzerinden gerçekleştirilebilir hale gelmiştir. Kritik dillerdeki çeviriler artık tek bir tuşla anlık olarak yapılabilmektedir. Benzer bir şekilde, sinyal istihbaratından elde edilen konuşmaları yazı formatında yapılandırarak uygulamalar sayesinde bu işle görevli çok sayıdaki personelin de yükü azalacaktır. Bu nedenle geleceğin istihbarat teşkilatlarında yeni görev tanımları ortaya çıktığı gibi bazı görevlerin ortadan kalkması da olasıdır.

*H-4: Açık kaynakların zayıf yanı, proaktif olmaktan ziyade reaktif olması ve bu nedenle önleyici istihbarat faaliyetindeki etkisinin sınırlı kalmasıdır.*

İstihbaratın kolluk görevinden ve gazetecilik mesleğinden farkı, işlenen bir suçu aydınlatmaktan ziyade suçu işlenmeden öngörmesidir. Geleceğe yönelik tahminde bulunmak istihbarat ile diğer meslekler arasındaki farkı oluşturmaktadır (Hulnick, 1999, s.46). Bu çerçevede açık kaynakların çoğunlukla proaktif değil reaktif olduğu söylenebilecektir. Bu nedenle açık kaynak analizinin belki de en zayıf yanı ileriye dönük değil geriye dönük bilgiler vermesidir.

Özellikle güvenlik/terör istihbaratının ana görevi önleyici istihbarattır. Elde edilecek eylem ikaz istihbaratı (*warning intelligence*) sayesinde eylemlerin planlama aşamasında tespit edilerek gerçekleştirilmeden önlenmesi amaçlanır. Bu süreçte, eylem kapasitesi ve niyeti bulunan hücrelerin tespit edilerek faaliyetin neticelendirilmesi gereklidir. İkaz istihbaratı eylemleri her zaman önleyemese bile, gerekli pasif güvenlik önlemlerin alınarak caydırıcılığın sağlanması ya da direnç (*resilience*) yaratarak yıkıcı etkilerinin azaltılmasını hedefler.

Sofistike eylemler, hücre üyelerinin hataları (Ör. hücre evinde patlama olması), çevredekilerin dikkatini çekmeleri<sup>1</sup> (Ör. yanıcı madde stoklanması) gibi nedenlerle hazırlık aşamasında önlenmektedir. Diğer taraftan bu senaryolar genellikle istisnadır ve eylemlerin önlenmesi için hücreye sızılması gereklidir. Bu aşamadan sonra bir operasyon kurulur ve süreç neticelendirilir (Woo, 2011, s.51). Yalnız aktörlerin aksine, gizli faaliyet gösteren hücrelerin saldırı planlarını internetten öğrenmek pek mümkün değildir. Sosyal gruplar ya da yalnız aktörler sohbet odalarında ya da sosyal medya hesaplarında eylem hazırlıklarına dair mesajlar paylaşılsa da profesyonel hücreler operasyonel güvenliğe riayet etmektedirler.

Bu noktada, ağ analizinin kendine has sınırlılıklarının bulunduğu anlaşılmaktadır. Ağ analizi sistemdeki farklı noktalar arasında içeriğinden bağımsız olarak bir ilişki şeması çıkarmayı amaçlar (Barnea, 2018, s.224). İltisak ağını haritalandırır ancak irtibatın içeriğine dair bir bilgi veremez. Durumun fotoğrafını çeker ancak operasyonel bir planlama için yeterli değildir. Faaliyetin neticelendirilebilmesi için sadece fotoğrafının değil röntgeninin çekilmesi gereklidir. Bu da sadece gizli kaynaklar kullanılarak başarılabilir. Bu nedenle açık kaynaklar hedefleme sürecinin önemli bir parçasıdır ancak mucizevi bir iksir olmaktan uzaktadır.

Bu çerçevede, açık kaynakların önleyici istihbarattan ziyade genellikle soruşturma aşamasında daha etkili olduğu görülmektedir (Krebs, 2016, s.49). Ortada çözülmesi gereken bir suç varsa ipuçlarını açık kaynaklarda ya da gri alanda kalan bilgileri analiz ederek bulmamız mümkündür. Bu durumda suça bir bulmaca olarak bakılır ve kanıt aranır. Henüz işlenmemiş bir suçun önlenmesi ise kaçınılmaz olarak bilinmezlik içerir.<sup>2</sup> Bu bilinmezliğin somutlaştırılabilmesi için hedefe yaklaşarak risk almak gerekir. Bu risk bazen genellikle istihbaratçılar ve onların yönettiği kaynaklar alır.

Diğer taraftan açık kaynak analizinden bahsederken sadece örgüt hücrelerine odaklanmak da doğru değildir. Özellikle istihbarata karşı koyma kapsamında maske kimliklerle faaliyet gösteren illegallerin<sup>3</sup> hareketlerinin takibi ve haber kanallarının ortaya çıkarılması gibi amaçlarla da kullanılabilir. Örneğin Bellingcat, açık ve yarı kaynak analizi

---

<sup>1</sup> Bu durum literatürde pasif mukavemet olarak adlandırılmaktadır.

<sup>2</sup> Bu konu istihbarat zafiyeti başlığı altında daha detaylı açıklanmıştır.

<sup>3</sup> "İllegal" terimi, derin bir maske hikaye ile hedef ülkede görev yapan istihbarat personelini tanımlamak için kullanılmaktadır. Bunlar teşkilat mensubu olabilecekleri gibi teşkilat personeli tarafından yönetilen elemanlar da olabilirler.

üzerinden çok önemli soruşturmalar yürüterek Rus istihbarat servislerinin yasa dışı faaliyetlerini ortaya çıkarmaktadır. Bu sayede Avrupa'da gerçekleştirilen çok sayıda suikast aydınlığa kavuşturulmuştur. Sergey Skripal'e yönelik suikast girişiminin şüphelileri olan GRU mensupları Anatoliy Chepiga ve Alexander Mishkin'in deşifre edilmesi bu duruma örnek olarak verilebilecektir (Bellingcat. 2018). Eylemciler görev öncesinde tespit edilemeseler de arkalarında çok sayıda dijital ayak izi bırakmışlardır. Kapalı devre kamera görüntüleri, araç plaka kayıtları, uçuş bilgileri ve geçmiş dönemde başkalarına ait sosyal medya hesaplarında yer alan özel fotoğrafları sayesinde tespit edilebilmişlerdir. Aslında Bellingcat'ın ulaştığı bilgilerin birçoğu dar anlamda açık kaynak bilgisi değildir. Plaka kayıtları, telefon arama ve baz istasyonu bilgiler, pasaport bilgileri, PNR verileri, kamera kayıtları gibi birçok bilgi dış kullanıma kapalıdır. Kurum bu bilgilerin kaynağı olarak yerel ortaklarını göstermektedir. Bu çerçevede yabancı istihbarat servisleri ve Rusya içindeki muhalif yapılarla da yakın temasta oldukları anlaşılmaktadır.

Bellingcat'ın açık kaynak analiz faaliyeti soruşturma odaklı olsa da ortaya çıkan bilgilerin önleyici istihbarat açısından bazı fırsatlar yarattığını da kabul etmemiz gerekmektedir. Bellingcat'ın Rus illegallerinin kullandıkları pasaport serilerini ifşa etmesi sayesinde hem geçmişe yönelik soruşturmalar yürütülebmiş hem de halen maske kimlikle faaliyet gösteren illegaller deşifre edilmiştir. Bu illegallerin bir kısmının görevlerini sona erdirerek Rusya'ya geri döndüğü bilinmektedir.<sup>1</sup>

*H-5: Açık kaynakların terör/güvenlik istihbaratında en fazla potansiyel vaat ettiği nokta siber alan hakimiyeti sağlanmasıdır.*

Bir önceki başlıkta görüldüğü üzere açık kaynakların güvenlik/terör istihbaratındaki rolü tartışmalı bir konudur. Genel kanı bu kaynakların sofistike terör eylemlerini engellemede başarılı olmadığıdır. Diğer taraftan, açık kaynak istihbaratının iddiası, potansiyel eylemcilerin radikalleşme süreçlerinin büyük veri üzerinden takip edilebileceği ve bazı senaryolarda eylemlerin önlenebileceğidir (Ball ve Webster, 2003, s.4).

Radikalleşme emarelerinin tespiti için potansiyel eylemcinin parçası olduğu ekosisteme yani ağa odaklanması gerekmektedir. Bu hem fiziki

---

<sup>1</sup> Maria Adela Kuhfeldt River kod adını kullanarak NATO personellerine yaklaşan bir GRU elemanı olduğu iddia edilen Olga Kolobova hakkındaki analiz bu duruma örnek verilebilir (www.bellingcat.com, 2022).



hem de elektronik bir ilişki ağıdır. Ağ üzerindeki noktalar (eylemci, milis, kurye, telefon, bilgisayar, internet sitesi, hücre evi, mağara, vb.) birbirleriyle iltisaklıdır (Arquilla ve Ronfeldt, 2001, s.II-7, Sparrow, 1991, s.257). Bu irtibat arkadaşlık, akrabalık, ideoloji, para, lojistik, irtibat ya da eylem amaçlı olabilir. Ağ üzerindeki bu noktalar arasındaki ilişki arkasında iz bırakmaktadır. Noktaların tespiti yeni hedefler yaratarak deşifre edilen ağı genişletmektedir.

Bir önceki başlıkta belirtildiği gibi ağ analizi sihirli bir çözüm sunmasa da analiz teknolojisinin örgüt ekosisteminin görselleştirilmesi açısından büyük kolaylıklar sağladığı kabul edilmelidir. Bu çerçevede açık kaynak analizinin en güçlü olduğu nokta belki de siber alan hakimiyetinin sağlanmasıdır. Asker ve polis birimlerinin fiziki alan hakimiyeti sağlaması gibi istihbarat teşkilatları da siber alanı örgütlere kapayarak hareketlerini yavaşlatmak ve engellemek zorundadır. Siber devriye<sup>1</sup> olarak da adlandırılan bu görev çerçevesinde sadece internet üzerinden islenen suçların tespiti değil örgütsel faaliyetlerin de kontrolü amaçlanmaktadır. Bu çerçevede örgütsel sitelerin sosyal medya uygulamalarının ve mesaj trafiğinin kontrol altında tutulması ve eylem ya da radikalleşme sinyallerinin tespit edilerek operasyona dönüştürülmesini öngörmektedir.

Radikalleşme emarelerinin tespiti için büyük veri toplanarak süzgeçten geçirilmektedir (Barnea, 2019, ss.440-441). Yapay zekâ uygulamaları bu süreçte büyü bir rol üslenmektedir. Davranış kalıplarını ve kilit söylemleri takip ederek, mekanik olarak takip edilemeyecek bir alanı kontrol altında tutmaktadır. Yapay zekâ uygulamaları ile; radikal söylemler, eylem öncesi hazırlık aşamasındaki sızıntı davranışları, bir konu ya da kişi hakkındaki takıntılı davranışlar ve başka saldırganlarla özdeşleşme çabaları takip edilmektedir (Brynielsson vd., 2013, ss.7-9).<sup>2</sup> Haritalandırma programları ve anahtar kelime sorgulamaları, olağan şüphelilerin takibi ve ikaz emarelerinin toplanması açısından önemli araçlardır.

Bu noktada, özellikle yalnız aktör eylemlerinin engellenmesinde önemli fırsatların söz konusu olduğu söylenebilecektir. Her ne kadar Reina saldırganı Masharipov ya da Paris saldırganı Abdelhamid Abaaoud eylemciler internet üzerinde aktif değillerse de özellikle yalnız aktörlerin

---

<sup>1</sup> Tanım için bkz. [www.egm.gov.tr](http://www.egm.gov.tr), 2020

<sup>2</sup> Özellikle aşırı sağ vasat içerisinde Anders Breivik ile özdeşleşme çabalarına sıklıkla rastlanılmaktadır. Breivik'in 22 Temmuz 2011'de Oslo ve Utoya'da gerçekleştirdiği saldırılarda 77 kişi hayatını kaybetmiştir.

eylem öncesinde güçlü sinyaller verdikleri bilinmektedir. Eyleme geçmeden önce ortaya çıkan bu emarelerin tespiti durumunda önleyici adımların atılması mümkündür. Bu kapsamda alan kaplama faaliyetinin nokta operasyona dönüşmesi de mümkündür. Mizansen operasyonlarla (*sting operations*) potansiyel saldırganın kontrollü bir şekilde eylem aşamasına geçirilerek suç üstüne gidilmesi özellikle Amerikan iç istihbarat kurumlarınca sıkça kullanılan bir uygulamadır. Benzer bir şekilde ağ üzerindeki kişilerin motivasyon unsurlarının tespit edilerek, angaje amacıyla kullanılabilirdiği görülmektedir. Çin'in LinkedIn gibi uygulamaları bu amaçla kullandığı bilinmektedir.

*H-6: Açık kaynakların geriye yönelik çok güçlü bir araştırma yöntemi olması nedeniyle, istihbarat zafiyeti başlığı altındaki öngörü yanlışlıkları artmıştır.*

Açık kaynak arşivinin bilgisayarı olan herkes tarafından geçmişe yönelik detaylı olarak sorgulanabilmesi, istihbarat zafiyeti (*intelligence failure*) kavramının sıklıkla gündeme gelmesine neden olmuştur. Teknolojinin analiz boyutunu ön plana çıkarması ile bağlantılı olarak, eylemlerin önlenmesindeki başarısızlıklarda oklar giderek daha fazla analiz aşamasına işaret etmeye başlamıştır (Treverton, 2009, s.106). Bunun nedeni bütün bilinmezliklerin cevabının internetin derinliklerinde bir yerde olduğu yanlışlığıdır (Treverton vd., 2006, s.14). Zaten eylemciler hakkındaki bilgilere açık kaynaklardan ulaşılabiliriyorsa, hata, bu bilgilerin doğru analiz edilememesi nedeniyle oluşmuştur. Özet olarak ortada bir istihbarat zafiyeti bulunmaktadır.

Açık kaynakların geçmişe yönelik sorgulama gücü, sonuç odaklı eleştirilere ve öngörü yanlışlıklarına (*hindsight bias*) yol açmaktadır. İstihbarat teşkilatları saldırganlar hakkında çok fazla bilgi bulunmasına rağmen saldırıyı engelleyememekle suçlanmaktadır. Çokça vurgulandığı üzere kimse polisın bütün cinayetleri engellemesini beklememekte ama istihbaratın bütün eylemleri önlemesini istemektedirler (Goldman, 2016). Öncelikle şunu belirtmek gerekir ki daha fazla bilgi daha fazla istihbarat anlamına gelmemektedir (Treverton vd., 2006, s.14). Veri toplama ve işleme kapasitesinde yaşanan büyüme hayali bir güvenlik algısı yaratmakta, ancak daha fazla veri daha fazla güvenlik anlamına gelmemektedir. Her ilave bilgi ile operasyonel etkinlik arasında doğrudan bir ilişki mevcut değildir. Bu çerçevede, aslında eylemciler hakkında internette çok fazla bilgi bulunduğu

görülmektedir. Örneğin, 11 Eylül saldırganlarının kendi adlarına kayıtlı adreslerine, ehliyetlerine, kredi kartı bilgilerine ve seyahat geçmişlerine rahatlıkla ulaşılabilmiştir. Bu bilgilere saldırıdan önce de ulaşmak mümkündür ancak nereye bakılması gerektiği bilinmediğinden saldırı öncesinde hiçbir işe yaramamıştır (Treverton, 2009, s.32). Belki de derinlerde bir yerde bütün eylemciler hakkında bilgi bulunmaktadır, ancak bu bilginin değerli olduğuna nasıl karar verileceği sorusu genellikle yanıtsız kalmaktadır.

Bu noktada, realizmin klasik tehdit formülasyonu açıklayıcı bir çerçeve sunmaktadır. Formüle göre, tehditler kapasite ve niyetin etkileşiminden oluşur. Açık kaynaklar kapasite hakkında genellikle doğru ve güvenilir bilgilere ulaşmamızı sağlar. Diğer taraftan niyetleri tespit etmek çok daha zor ve subjektif bir süreçtir (Treverton, 2009, s.138). Rusya nükleer silah kullanacak mı ya da varlığı bilinen bir radikal eylem kararı verecek mi soruları somut verilerin ötesine geçen bir durumdur. Benzer bir şekilde zaten kırsala katılmış kişilerden oluşan bir örgüt grubunun konumunun tespiti ile henüz fikir aşamasında olan bir eylemin önlenmesi farklı özellikteki faaliyetlerdir. Kapasitenin gözlemlenebilmesi gereklidir. Bir silah, ya da insan varlığı kapasitenin kanıtı olabilir. Ancak silahın nerede ve ne zaman kullanılacağı gözlemleyebilmek pek mümkün değildir.

Bu durum istihbarat çalışmaları literatüründe sıkça tartışılan bulmacası (puzzle-mystery) farklılığına işaret etmektedir. İlk duruma göre ortada çözülmesi gereken bir bulmaca vardır ve tek gereken şey doğru parçayı doğru yere yerleştirmektedir. Özellikle kapasite boyutunu oluşturan somut eşyalar bulunmayı bekler. Bunlar; eylem malzemesi olan patlayıcılar, bir hücre evi ya da kırsalda bir mağaradır. Aksi görüş ise eksik parçaların hala keşfedilmeyi beklediğidir. Örnek vermek gerekirse El Kaide liderlerinin Afganistan Pakistan sınırındaki sığınakları bir bulmacanın parçalarıdır. Ancak saldırıların kim tarafından, ne zaman, nereye ve nasıl gerçekleştireceği bir sırdır (Treverton, 2009, s.33-34). 11 Eylül saldırısının lideri Muhammed Atta'nın kimlik bilgilerini bulmak yapbozun parçalarını birleştirmeye benzetmektedir. Bu bilgilere açık kaynaklardan ulaşılabilir. Diğer taraftan eylem niyetini öngörebilmek ayrı bir mesleki yeterlilik gerektirmektedir.

Kapasite sorusunun genellikle bir cevabı vardır. Diğer taraftan niyetler konusunda ortada bir cevap değil sadece tahminler olabilir (Treverton, 2009,

s.147). Tahminler demokratik ülkelerde kanıt yerine geçmez. Örneğin 12 Haziran 2016 tarihinde Orlando'daki bir gece kulübüne gerçekleştirdiği saldırıda 49 kişiyi öldüren Omar Mateen gibi yalnız aktörlerin engellenememesi ABD'de geniş şekilde tartışılmıştır. Mateen, saldırı öncesinde, iş yerinde El Kaide ve IŞİD'in gerçekleştirdiği terör eylemlerini öven söylemlerde bulunması nedeniyle FBI tarafından kontrol altında tutulmuş ancak hakkında kanıt bulunamamıştır. Yetkililerce, Mateen gibi yalnız aktörlerin saldırı öncesinde yasalara aykırı hiçbir eyleminin bulunmadığı, Afganistan'a gitmenin ya da Osama bin Laden'i övmenin bir kişiyi istihbarat hedefi haline getireceği, ancak suçlanması ve tutuklanması için yeterli olmayacağı belirtilmiştir (Goldman, 2016). Dönemin FBI Başkanı Comey, teşkilatın yasal sınır olan on ay boyunca Mateen hakkında ön soruşturma yürüttüğünü, ancak herhangi bir eylem emaresine rastlanmadığını, geriye bakınca bu vakada eksik ya da yanlış olan ve farklı yapmaları gereken bir prosedürün bulunmadığını açıklamıştır (Goldman, 2016).

Güvenlik/terör istihbaratında yaşanan kapasite niyet sorunsalında tartışılan bir konu da alan hakimiyeti başlığında vurgulanan mizansen operasyonlardır. Kabul edileceği üzere, geleceği tahmin etmek kolay bir iş değildir. Bu nedenle istihbarat teşkilatlarına sadece geleceği tahmin etmek değil geleceği dizayn etmek gibi bir görev de verilmiştir. Bazı senaryolarda potansiyel eylemciye çözümü sunmak yoluna gidilmektedir. Mizansen operasyonlarda, niyeti hakkında şüphe bulunan potansiyel eylemciye gerekli kapasite sunulmakta ve suçüstü ile sürecin neticelendirilmesi yoluna gidilmektedir. Bu sayede aktör söylemden eylem aşamasına kontrollü bir şekilde geçirilmekte ve sistemden ayıklanmaktadır.

## SONUÇ

Bu çalışmada açık kaynak istihbaratı üzerinde istihbarat çalışmaları literatüründe yer alan bazı temel tartışmalara değinilmiştir. Bu tartışmalar; istihbaratın demokratikleşmesi, toplama-analiz ikiliği, görev ve kadro tanımlarındaki dönüşüm, açık kaynakların önleyici istihbarattaki güçlü ve zayıf yanları ile istihbarat zafiyeti başlıklarında incelenmiştir. Şaşırtıcı olmayacak şekilde birçok senaryoda gri alanların bulunduğu görülmüştür.

Öncelikle, insanların sosyal paylaşım platformlarında paylaştıkları görüntü ve mesajlar üzerinden "büyük sonuçlara ulaşmak" istihbaratçılık değildir. Özellikle taktik istihbarat boyutunda hala gizli haber toplama

yöntemleri kullanarak hedefe yaklaşmak gerekmektedir. Diğer taraftan stratejik analiz boyutunda önemli bir demokratikleşme fırsatı yakalandığı da söylenebilecektir. Özellikle dış politika ya da ekonomi gibi alanlarda uzman özel sektör bileşenleri her geçen gün daha fazla bilgiye ulaşabilmekte ve bu da stratejik analizi demokratikleştirmektedir.

İkincisi, açık kaynaklar her ne kadar toplama boyutuyla gündeme gelse de aslında bir analiz meselesidir. Bunun nedeni internet üzerinden yapılan toplama işleminin bir standart haline gelmekle birlikte, analizin halen bir yetenek olmasıdır. Toplanan her bilgi istihbarat anlamına gelmemekte ve analiz aşamasının üstüne ilave sorumluluk olarak binmektedir. Bu nedenle analiz aşamasının öneminin arttığı ve açık kaynakların toplama-analiz ikiliğinde sarkacı analiz boyutuna çevirdiği söylenebilecektir.

Üçüncü olarak açık kaynak teknolojisi istihbarat alanındaki kadroları ve görev tanımlarını da dönüştürmektedir. Teknoloji sayesinde toplama ve analiz arasındaki geçiş hızı artmış ve analizciler giderek kendi toplayıcıları haline gelmiştir. Bu nedenle toplayıcılardan giderek daha fazla gizli ve operasyona dönüştürülebilir bilgi talep edilmektedir. Ayrıca, özellikle analiz boyutunda teknoloji merkezli yeni görev tanımları ortaya çıkarken, tercümanlık gibi bazı kadrolar da önemini yitirmektedir.

Dördüncüsü, açık kaynaklar proaktif olmaktan ziyade reaktiftir. Bu nedenle özellikle güvenlik/terör istihbaratındaki önleyici gücü kısıtlıdır. Diğer taraftan geriye doğru işleyen tahkikat aşaması için çok güçlü bir kabiliyet sunmaktadır.

Beşincisi, önleyici istihbarat açısından birtakım potansiyeller de vaat etmektedir. Siber alan hakimiyeti üzerinden vasatın kontrol edilmesi ve radikalleşme emarelerinin tespiti bu açıdan değerlendirilebilir. Özellikle yalnız aktörlerin eylem öncesinde kapasite ve niyeti hakkında sosyal medyada önemli belirtiler verdikleri bilinmektedir.

Son olarak, açık kaynaklar istihbarat zafiyeti konusunun daha sık gündeme gelmesine neden olmuştur. Kuşkusuz ki eylem öncesinde hedef önceliklerinin belirlenmesi, toplama, analiz ya da neticelendirme aşamaları üzerinden hatalar yapılabilir. Diğer taraftan, açık kaynak teknolojisindeki ilerlemenin zafiyet başlığı altında yapılan yorumlardaki öngörü yanlışlarını arttırdığı görülmektedir.

## KAYNAKÇA

- Ball, K. Webster, F. (2003) The intensification of surveillance. Ball, K. Webster, F. (Ed.). The intensification of surveillance: crime, terrorism and warfare in the information içinde (ss.1-15). Pluto Press.
- Barnea, A. (2018). Challenging the “lone wolf” phenomenon in an era of informant. *International Journal of Intelligence and Counterintelligence*. 31(2). 217-234.
- Barnea, A. (2019) Big data and counterintelligence in western countries. *International Journal of Intelligence and counterintelligence*. 32(3). 433-447.
- Brynielsson, J. Horndahl, A. Johansson, F. Kaati, L. Mårtenson, C. ve Svenson, P. (2013) Harvesting and analysis of weak signals for detecting lone. *Security Informatics*. 2(11). 1-15.
- Denécé, E. (2014). The revolution in intelligence affairs: 1989–2003, *International Journal of Intelligence and Counterintelligence*. 27(1): 27-41.
- Field manuel 2-0 intelligence. (2007). United States Army Press.
- Freedman, L. (1977). U.S. Intelligence and the soviet strategic threat. Princeton University Press.
- Gill P. ve Phythian M. (2018). *Intelligence in an Insecure world*. Polity Press Cambridge.
- Goldman, A. (2016). Why didn't the F.B.I. stop the New York bombing? Erişim tarihi: 24 Ekim 2018. <https://www.nytimes.com/2016/09/22/us/fbi-terror-ahmad-khan-rahami.html>.
- Herman, M. (1998). Diplomacy and intelligence, *Diplomacy & Statecraft*, 9(2). 1-22.
- <https://www.bellingcat.com/news/uk-and-europe/2018/10/09/full-report-skripal-poisoning-suspect-dr-alexander-mishkin-hero-russia/> Erişim tarihi: 24 Ekim 2018.
- <https://www.bellingcat.com/news/2022/08/25/socialite-widow-jeweller-spy-how-a-gru-agent-charmed-her-way-into-nato-circles-in-italy/?s=03> Erişim tarihi: 24 Ekim 2022.
- <https://www.egm.gov.tr/02072020-tarihli-basin-aciklamasi> Erişim tarihi: 24 Ekim 2022.

- <https://www.europarl.europa.eu/news/en/press-room/20220412IPR27112/ep-inquiry-committee-for-pegasus-and-other-spyware-launched> Erişim tarihi: 20 Ekim 2022.
- <https://www.mevzuat.gov.tr/mevzuatmetin/1.5.6698.pdf> Erişim tarihi: 14 Ekim 2022.
- [https://www.i-scoop.eu/big-data-action-value-context/data-age-2025-datasphere/#:~:text=In%20the%20announcement%20of%20the,a%20yearly%20basis\)%%20by%202025](https://www.i-scoop.eu/big-data-action-value-context/data-age-2025-datasphere/#:~:text=In%20the%20announcement%20of%20the,a%20yearly%20basis)%%20by%202025). Erişim tarihi: 24 Ekim 2022.
- <https://www.statista.com/statistics/949144/worldwide-global-datasphere-real-time-data-annual-size/> Erişim tarihi: 24 Ekim 2022.
- Hulnick, A.S. (1999) Fixing the spy machine: Preparing American intelligence for the twenty-first century. Praeger.
- James J. Wirtz, ve Rosenwasser, J.J. (2010). From combined arms to combined intelligence: philosophy, doctrine and operations, *Intelligence and National Security*, 25(6). 725-743.
- Johnson, L.K. (2009). Sketches for a theory of strategic intelligence. Gill, P. Marrin,S. ve Phythian, M. (Ed). Intelligence theory key questions and debates içinde. (ss.33-53). Routledge.
- Johnson, L.K. (2010). National security intelligence. Johnson, K.L. (Ed). The oxford handbook of national security intelligence içinde. (ss.3-32). Oxford University Press.
- Johnson, L.K. (2014). The development of intelligence studies. Dover, R. Goodman, M. ve Hillebrand, C. (Ed). Routledge companion to intelligence studies içinde. (3-22). Routledge.
- Joint publication 3-25 countering threat networks. (2016). United States Army Press.
- Krebs, V.E. (2002). Mapping networks of terrorist cells. *Connections*. 24(3): 43-52.
- Lowenthal, M. (2008). Intelligence: From secrets to policy. CQ Press.
- Lahneman, W.J. (2006). The future of intelligence analysis volume I final report. University of Maryland.
- Shulsky, A.N. ve Schmitt G.J. (2002). Silent warfare: Understanding the world of intelligence. Potomac Books.
- Sparrow, M.K. (1991). Network vulnerabilities and strategic intelligence in law enforcement. *International Journal of Intelligence and counterintelligence*. 5(3). 255-274.

- Steele, R.D. (2007). Open source intelligence. Johnson, K.L. (Ed). Handbook of intelligence studies içinde. (ss.129-147). Routledge
- Treverton, G.F. Jones, S.G. Boraz, S. Lipsy, P. (2006). Toward a theory of intelligence. RAND Corporation.
- Treverton, G.F. C. Gabbard, B. (2008). Assessing the tradecraft of intelligence analysis. RAND Corporation.
- Treverton, G.F. (2009). Intelligence for an age of terror. RAND Corporation. Cambridge University Press.
- Williams, P. (2001). Transnational criminal networks. Phil Arquilla, J. Ronfeldt, D.F. (Ed). Networks and netwars: The future of terror, crime, and militancy içinde. (ss.61-98). RAND Corporation.
- Wheaton, K.J. (2019). How to teach 2500 years of intelligence history in about an hour. Erişim tarihi: 11 Ekim 2022. <https://sourcesandmethods.blogspot.com/2019/06/how-to-teach-2500-years-of-intelligence.html>.
- Wohlstetter, R. (1962). Pearl harbor warning and decision. Stanford University Press.
- Woo, G. (2011). Interdiction of plots with multiple operatives. Wiil, U.K. (Ed). Counterterrorism and open-source intelligence içinde. (ss.49-60) Springer-Verlag.
- Younger A. MI6 'C' speech on fourth generation espionage, Erişim tarihi: 11 Mayıs 2022. <https://www.gov.uk/government/speeches/mi6-c-speech-on-fourth-generation-espionage>.



## DİJİTAL ÇAĞDA İSTİHBARAT ANALİZİ

M. Hayati TABAN \* ve Emre AYDİLEK\*\*

### ÖZET

Değişen ve çeşitlenen tehdit iklimi, her alanda yaşanan teknolojik gelişmeler ve önemi gittikçe artan big data-algoritmalar-yapay zekâ vb. yeni analiz yöntemleri, günümüzde istihbarat alanının doğasının ve dönüşümünün dinamiklerindedir. Temel amacı devletlerin güvenliğine yönelik tehditlerin bertaraf edilmesine katkı sağlamak olan istihbarat toplulukları/kurumları, değişen koşullarda yeni risklerle/tehditlerle başa çıkmaya çalışmaktadır. İstihbarat döngüsünün en önemli aşamalarında olan istihbarat analizi de bu yeni konjonktüre göre yeniden şekillenmekte ve bu yeni ortama adapte olmaktadır. Bu noktadan hareketle çalışma, dijital çağ olarak adlandırabileceğimiz içinde bulunduğumuz dönemde istihbarat analizine odaklanmaktadır. İstihbarat analizinin dönüşümünde etkili olan dinamiklere ve tartışmalara ağırlıklı olarak yer verilen çalışmada, istihbarat analizinde mevcut ve gelecek perspektifler; veri madenciliğinde uzmanlaşma, algoritmalar geliştirme, insan unsurunun dijital yeniliklerle desteklenmesi gibi spesifik konular incelenmiştir.

**Anahtar Kelimeler:** *İstihbarat, İstihbarat Analizi, Açık Kaynak İstihbaratı, Dijitalleşme, İstihbaratın Değişimi.*

## INTELLIGENCE ANALYSIS IN THE DIGITAL ERA

### ABSTRACT

Today, the world has its own global characteristics due to the threat climate, the size of the data, the variety of actors and the speed of change. Intelligence communities/institutions, whose main purpose is to contribute to the elimination of threats to the security of states and to eliminate uncertainties, are trying to cope with the effects of these factors. As one of the most important stages of the intelligence cycle, intelligence analysis is also reshaped according to these factors. From this point of view, this study focuses on intelligence analysis in the digital age. In this age the importance of open-source intelligence has increased cyber space has created new threats. These factors are considered to be effective in the transformation of intelligence analysis. Thus, intelligence analysis has included algorithms by considering these factors and needs to adapt itself to this period by supporting the human element with digital innovations.

**Keywords:** *Intelligence, Intelligence Analysis, Open-Source Intelligence, Transformation of Intelligence, Digitization.*

---

\* Dr. Öğr. Üyesi, Milli Savunma Üniversitesi, Alparslan Savunma Bilimleri ve Milli Güvenlik Enstitüsü, mhtaban@kmo.msu.edu.tr, ORCID: 0000-0003-1785-9965.

\*\* Dr., Kastamonu Üniversitesi, BAP Koordinatörlüğü, eaydilek@kastamonu.edu.tr, ORCID: 0000-0002-4767-2424.

Makale Başvuru Tarihi / Application Date: 30 Kasım 2022 / 30 November 2022

Makale Kabul Tarihi / Acceptance Date: 19 Aralık 2022 / 19 December 2022

## GİRİŞ

Dijitalleşmenin doruk noktasına ulaştığı çağımızda ekonomik, politik, sosyal ve kültürel birçok alanda hem fırsatlar hem de zorluklar ve tehditler aynı anda bir arada bulunmaktadır. Güvenlik ve istihbarat açısından düşünüldüğünde küreselleşmenin artan hızı, uluslararası aktörlerin giderek çeşitlenmesi, gelişen teknoloji gibi olgular, küresel belirsizlikler, sistemik riskler ve daha az öngörülebilir bir gelecek yaratmakta. Bu ortamda istihbarat alanında kalıcı stratejik avantaj elde etmenin anahtarı, karmaşık zorlukları hızlı ve doğru bir şekilde tahmin etme ve bunlara uyum sağlama yeteneği olarak öne çıkmaktadır (Director of National Intelligence, 2015, s.4).

Özellikle siber alandaki gelişmeler, istihbari hedef belirlemeden devşirmeye, istihbarat toplamadan işlemeye ve gizli operasyonların yürütülmesine uzanan bir çerçevede istihbaratın her alanına etki etmiştir. Örneğin Soğuk Savaş döneminde ABD'nin ihtiyaç duyduğu istihbari bilgilerin %80'i gizli, %20'si açık kaynaklardan elde edilirken Soğuk Savaş sonrası dünyada bu durum tersine dönmüştür. Açık kaynak istihbaratının (AKİS veya OSINT) daha fazla kullanılabilirliği nedeniyle “sırları elde etmek” için oluşturulmuş istihbarat kurumları, bu yeni bilgi/veri toplama sürecinde (açık kaynaklı bilgileri kendi toplama sürecine entegre etmekte) güçlük çekmiştir (Lowenthal, 2020, s.140). Bu güçlükleri aşmak amacıyla çeşitli çalışmalar yürütülmektedir. Örneğin Birleşik Krallık'taki en eski düşünce kuruluşlarından olan Royal United Services Institute (RUSI) tarafından “Birleşik Krallık Ulusal Güvenliği için Açık Kaynak İstihbaratının Geleceği” başlıklı raporda söz konusu alanda daha geniş ve belirli standartları olan destek altyapısı oluşturulması önerilmektedir (Janjeva, Harris ve Byrne, 2022, s.44).

İstihbarat toplulukları, Soğuk Savaş döneminden çok farklı olan 21. yüzyılın konjunktürüne adapte olmaya çalışmaktadır. Bu öyle bir değişimdir ki; istihbaratın her alanında hissedilmiş ve ivme tek bir temel hedeften (düşman devlet gibi) çok çeşitli hedeflere; varoluşsal tehditlerden belirgin hedeflere yönelik saldırı tehditlerine; herhangi bir A ülkesinin B aktörüne sağladığı silah bilgisinden belirli bir gemi, uçak veya birey hakkında harekete geçirilebilir istihbarat taleplerine doğru gerçekleşmiştir. Sovyetler Birliği'nin nükleer silah ve tehdit kapasitesinin keşfedilmesi için gereken istihbarat kabiliyetiyle, bir terörist grubun bir şehirde, alışveriş merkezinde

veya okulda doğaçlama bombalı eylem planladığını keşfetmek için gerekenler çok farklıdır. Bu iki konu hakkında veri toplama, analiz etme kabiliyeti oldukça asimetriktir. Dünyadaki bu değişikliklerin her biri istihbarat analistlerinden neyi bilmesi beklendiği ve işlerini nasıl yaptıkları üzerinde kayda değer etkiye sahiptir (National Research Council, 2011, s.10).

20. yüzyılın ikinci yarısına hâkim olan Soğuk Savaş sırasında istihbarata ilişkin en önemli sıkıntı, genellikle çok az veriye sahip olmaktı. Fakat 21. yüzyıldaki en temel sorunlardan biri mevcut bilginin hacminin büyüklüğüdür. Ayrıca bilgi teknolojisindeki gelişmeler istihbarat analizinde çalışanlara hem yardımcı olmuş hem de yeni sorunlar ortaya çıkarmıştır. Haber servislerinden ve World Wide Web'den gelen açık kaynaklı bilgilerde yaşanan patlama, istihbarat analizinin hızını ve hacmini gözden geçirmeyi daha da zorlaştırmıştır. Veri baş döndürücü bir hızla çoğalırken analistler ayıklamaları, analiz etmeleri ve yorumlamaları gereken bilgi yığınıyla karşı karşıyadır (Hedley, 2007, s.128). Yukarıda belirtildiği üzere istihbarat alanındaki değişimlerin bir kolu da istihbarat analizinde yaşanmaktadır. Analistlerin çalışma biçiminin son dönemde önemli ölçüde değiştiği açıktır.

ABD Ulusal İstihbarat Konseyi (National Intelligence Council) tarafından 2021 yılında hazırlanan 'Küresel Eğilimler 2040' raporunda istihbarat alanındaki bu yapısal değişimlere dikkat çekilmektedir. Gelecek perspektiflerinin ele alındığı raporda, bilgi teknolojilerindeki gelişmeler vurgulanmaktadır. Devlet ya da devlet dışı aktörlerin bilgiyi nasıl elde ettikleri, yorumladıkları ve kullandıkları konusunda öngörülere yer verilen analizlerde; yapay zekâ, nesnelerin interneti ve diğer araçlardan yararlanma oranının artacağı paylaşımı yapılmaktadır. Bu öngörüler istihbarat toplama ve analizindeki değişimlere işaret etmektedir (National Intelligence Council, 2021, s.97).

Açık kaynaklı bilgilerin hacminin artması, hedeflerin çeşitlenmesi (devlet dışı aktörlerin çoğalması) ve özellikle siber alandaki tehditler günümüz istihbarat alanını zorlayan faktörlerdir. Son dönemlerde istihbarat analizi, insan veya diğer geleneksel bilgi toplama kaynaklı çizgisinden uzaklaşarak; insan ve algoritmaların birleşiminden oluşan yeni ve hibrit bir temelde gelişmektedir. Buradan hareketle bu çalışmada, dijital çağda istihbarat analizi konusu incelenmektedir. Bu çalışmanın iddiası; veri madenciliğini, yapay zekâları ve algoritmaları bir yandan aktif-etkin olarak

kullanmayı başararak çağa ayak uyduran, diğer yandan insan unsurunu dışlamadan en doğru biçimde dijital tabanlı analizle entegre bir model oluşturabilen ülkelerin, geleceğin istihbaratına yön vereceğidir.

Üç bölümden oluşan çalışma, öncelikle istihbaratın dönüşümü ve değişimine tarihsel olarak yaklaşmaktadır. İkinci olarak istihbarat analizi hakkında kısa ama öz bir bilgilendirme yapılmakta ardından üçüncü bölümde günümüzde istihbarat analizinin karşılaştığı sorunlar ve dönüşümü ele alınmaktadır. Çalışma dijitalleşmenin istihbarat analizindeki dönüşümlere etkisine odaklandığından, istihbarata ilişkin bazı temel konuları inceleme dışında bırakmaktadır.

## **1. İSTİHBARATIN DEĞİŞİMİ VE DÖNÜŞÜMÜ**

Klasik tanımıyla istihbarat, bilgilerin karar vericilere belirsizlikleri azaltmak veya kaldırmak amacıyla sağlanmasıdır (Johnson, 2010, s.5). Bu bağlamda bakıldığında istihbaratın amacı başka güçlerin bir devletin ulusal çıkarlarına zarar vermek üzere kurmakta oldukları kumpas plânlarına karşı devleti önceden ikaz etmesi bakımından koruma ya da savunma yararına ve o devletin dış politikası doğrultusunu ve yolunu hazırlaması anlamında da olumlu ve dışa yönelik bir faydaya hizmet eder (Kent, 2003, s.134). Bu nedenle stratejik sürprizlerden kaçınmak, uzun vadeli uzmanlık sağlamak, politika sürecini desteklemek ve bilgi, ihtiyaç ve yöntemlerin gizliliğini korumak, istihbarat kurumlarının var olma sebeplerini oluşturur (Lowenthal, 2020, s.3).

Öteden beri istihbaratın amacı, düşman veya rakiplerin ve bazen ortakların/müttefiklerin istekleri, niyetleri, yetenekleri ve eylemleri hakkındaki belirsizliği azaltmak olmuştur (Fingar, 2011, s.6). Bir toplumun güvenli bir biçimde yaşamını sürdürebilmesi için ilgili devletin dış ilişkiler, milli savunma ve diğer ulusal güvenlik politikalarının geliştirilmesi, koordine edilmesi ve icra edilmesi süreci hayati önem taşımaktadır (Biçer, 2017, s.435). Dolayısıyla istihbaratın amacı yalnızca bilgi toplamak değil karar vericilerin kendi kontrolleri dışındaki güçlerle başa çıkmada daha iyi seçimler yapmalarını sağlamaktır. Böylelikle istihbarat, kritik seçimler anında belirsizlik ve risk derecesinin azaltılmasına yardımcı olmaktadır (Director of National Intelligence, 2015, s.8).

Daha kapsamlı bakıldığında istihbarat bilgi, faaliyet/süreç ve kurum olarak farklı boyutları olan bir kavramdır. Bilgi anlamında istihbarat, bütün verileri kapsaması dahi oldukça geniş anlamda ve çeşitlilikte bir yığın

oluşturan enformasyondur. Burada dikkat edilmesi gereken nokta, bu bilginin güvenlik kapsamına giren bir araştırma sürecinin sonunda üretildiğidir. Bilgi, nasıl keşfedildiğine bakılmaksızın bilinebilen her şeydir. Bu açıdan istihbarat politika yapıcıların belirtilen ihtiyaçlarını karşılayan ve bu ihtiyaçları karşılamak için toplanmış, işlenmiş ve daraltılmış bilgileri ifade eder. Daha net ifade edilirse, istihbarat bilgiyi içerir ama her bilgi istihbarat değildir. İstihbarat ve onun tanımlandığı, elde edildiği ve analiz edildiği tüm süreç, politika yapıcıların ihtiyaçlarına cevap veren bir niteliktedir (Lowenthal, 2020, s.2). Kurum olarak istihbarat ulusal güvenlik ile ilgili olarak bilgi peşinde koşan kişilerden ve düzenlemelerden oluşan bir organizasyondur. Bu organizasyonun yerine getirdiği faaliyetler de istihbarat kavramına içkindir (Kent, 2003). Bir faaliyet olarak istihbarat ise ulusal güvenlik için önemli olan belirli bilgi türlerinin talep edildiği, toplandığı, analiz edildiği ve politika yapıcılara sağlandığı sürecini; bu sürecin sonunda ortaya çıkan ürünleri, bu süreçlerin ve bilgilerin karşı istihbarat faaliyetleriyle korunması ve yasal makamlar tarafından talep edilen işlemlerin gerçekleştirilmesi işlevlerini kapsar (Lowenthal, 2020, s.4). İstihbarat süreci, istihbarat çarkını oluşturan bir dizi prosedür veya adım sonucunda gerçekleşir. Süreç, bir soru soran veya tavsiye isteyen bir karar verici tarafından başlatılır. Buna istihbarat gereksinimi denir. İstihbarat gereksinimleri ilgili istihbarat birimine iletilir ve döngü başlar. İstihbarat çarkı (ilk beşi ham verileri tamamlanmış, odaklanmış istihbarata dönüştüren, son ikisi elde edilen bu istihbaratı işleyen) yedi adımdan oluşur: 1. problem formülasyonu ve planlama; 2. bilgi toplama; 3. veri harmanlama; 4. veri işleme; 5. veri analizi; 6. rapor yazma; 7. karar vericilere dağıtma ve geri dönüt (Prunckun, 2010, s.5, Lowenthal, 2020, s.160). McGlynn ve Garner benzer ama daha sade bir formülasyonla istihbarat çarkını birbiriyle ilişkili altı aşamaya ayırmıştır: Gereksinimler; planlama ve yönlendirme, toplama, işleme ve kullanım, analiz, üretim, yayma, istihbarat çarkının aşamalarıdır (McGlynn ve Garner, 2019, s.22).

İstihbarat kavramı birçok farklı türde tasnife konu olmuştur. Alanlarına, bilgiyi toplama çeşitlerine, coğrafi-görev alanı ve faaliyet biçimine göre kategorize edilen istihbarat kavramı bu tasniflerin en yaygın tezahürleridir. En geniş sınıflandırmalardan birini yapan Özdağ istihbaratı, alanlarına göre dokuz kategoride incelemiştir. Bunları; siyasi istihbarat, askeri istihbarat, ekonomik istihbarat, sosyal istihbarat, coğrafi istihbarat,

biyografik istihbarat, ulaşım ve iletişim istihbaratı, bilimsel ve teknik istihbarat, siber istihbarat olarak sıralamıştır (Özdağ, 2014, s.8).

Bir başka tasnife göre ise istihbarat bilgiyi toplama çeşitleri açısından üç türdür: Teknik istihbarat, insan istihbaratı ve açık kaynak istihbaratı. Teknik istihbarat kendi içinde; muhabere istihbaratı, haberleşme istihbaratı, telemetrik istihbarat, elektronik istihbarat, ölçüm ve işaret istihbaratı, radar istihbaratı, görüntü istihbaratı, fotografik istihbarat gibi alt uzmanlık alanlarından oluşmaktadır (Yılmaz, 2015, s.185). İnsan istihbaratı sahadaki eğitilmiş uzmanlardan elde edilen bilgilerden oluşmaktadır (Urhal, 2008, s.222). Açık kaynak istihbaratı ise kamuya açık tüm kaynakların sunduğu verilerin toplanması olarak ifade edilebilir. Bu bakımdan hükümetin resmi evrakları, yazılı, görsel ve işitsel medya kaynakları, bilimsel ve süreli yayınlar ile uluslararası kuruluşların raporları açık kaynak istihbaratın bilgi edinme yolları olabilmektedir. Günümüzde istihbaratın yüzde 80'inin açık kaynaklardan temin edildiği tahmin edilmektedir. Açık kaynaklardan istihbarat toplama yöntemi, özellikle internetin yaygınlaşmaya başlaması ve sosyal paylaşım sitelerinin artış göstermesi ile birlikte oldukça önem kazanmıştır. Her gün milyonlarca insanın katrilyonlarca bit veriyi ağ sistemine eklemesi ciddi miktarda ham bir bilgi yığını meydana getirmiştir. Sosyal paylaşım sitelerinin popülerlik kazanması ile birlikte insanlar birçok alanda her türlü bilgiyi gönüllü olarak paylaşmaktadır. Günümüzde istihbarat servislerinin özellikle "Facebook, Twitter, Instagram" gibi sosyal paylaşım sitelerinden faydalanarak hedeflerine yönelik çalışmalar yürüttükleri bilinmektedir (Yılmaz, 2015, ss.184-186). Bunların yanında, literatürde, coğrafi açıdan; iç ve dış istihbarat (Johnson, 2007, s.1), faaliyet açısından operasyonel, taktik ve stratejik istihbarat (Gül, 2014, s.88) gibi farklı terminolojik tasniflerine de rastlanmaktadır. Çalışma kapsam olarak istihbarat analizine odaklandığından, istihbaratın sınıflandırılmasına yönelik bu bilgilerle yetinmektedir.

Akademik açıdan henüz çok yeni (yaklaşık yarım asırdır) bir disiplin olan istihbarat (Kahn, 2008, s.4), profesyonel bir alan olarak, Birinci Dünya Savaşı'nın hemen öncesinde, ilk olarak Britanya'da ve kısa bir süre sonra diğer savaşan ülkelerde ortaya çıkmıştır (Warner, 2007, s.23-24). Uygulamada kurumsal olarak 17. yüzyılın başlarından İkinci Dünya Savaşı'nın hemen sonrasına kadar, Avrupa ülkeleri kapsamlı istihbarat sistemleri geliştirmeye başladılarsa da bugüne kıyasla büyük bir başarı elde edememiş, İkinci Dünya Savaşı'yla birlikte, askeri istihbarat servisleri

kapsam ve gelişmişlik açısından büyük ölçüde genişlemiş ve günümüzdeki çok yönlü ve uzmanlık temelli bir niteliğe bürünmüştür (Prunckun, 2010, s.15).

İlkel düzeyde istihbarat uygulamaların tarihi ise binlerce yıllık bir geçmişe sahiptir. Yeryüzündeki ilk savaşlardan Birinci Dünya Savaşı'nın başlangıcına kadar, neredeyse tüm istihbari bilgiler fiziksel kaynaklardan elde edilmiştir. Ancak bu yetersiz fiziksel istihbarat süreci, komutanların savaşları kazanmasına çoğu zaman yardımcı olacak düzeye erişememiştir. Modern dönemde ise daha önce önemsiz görülen faktörler değerli hale gelmiştir. Örneğin bir orta çağ kralı için düşmanın ne kadar kömür ve demir üretebileceği pek önemli değildi; oysa böyle bir bilgi modern devletlerin güvenlik kurumları için hayati önem taşımaktadır. Çünkü demiryolları büyük birliklerin hızlı seferber edilmesini, yoğunlaşmasını ve tedarik edilmesini mümkün kılmıştır. Dolayısıyla istihbarat artık, savaşlarda ilk göz önünde bulunması gereken önemli parametrelerden birine dönüşmüştür (Kahn, 2008, ss.5-6).

Son yüzyılda istihbaratın öneminin gittikçe arttığı, yalnızca savaşların kazanılmasında değil, devletlerin politika oluşturma sürecinde de göz önünde bulundurulması önemli bir faktöre dönüştüğünün tekrar vurgulanması yerinde olur. Özellikle İkinci Dünya Savaşı'nda ve takip eden Soğuk Savaş yıllarında istihbarat olgusunun modern devletler için önemini giderek artırmıştır. Bu da istihbarat örgütlenmesinin insan, araç-gereç ve mali kaynaklar açısından genişlemesi sonucu doğurmuştur.

Soğuk Savaş boyunca, ABD başta olmak üzere birçok Batılı devlet esas olarak Sovyetler Birliği ve komünist bloğa karşı istihbarat toplamaya odaklanmış, dünyanın geri kalan bölgelerine ve sorunlarına daha az ilgi göstermiştir. Terör gibi meseleler ilgilenecek istihbarat konuları listesinde yer alsada ancak 11 Eylül 2001'den itibaren istihbarat kurumlarının önceliği haline gelmiştir (Johnson, 2007, s.9).

Günümüzle kıyaslandığında Soğuk Savaş sırasında istihbarat toplama yöntemleri önceki dönemlere oranla giderek gelişmeye başladıysa da yine de yeterince kompleks değildi. Baskın uygulama biçimi, uydu keşifleri ve benzeri yöntemlerle elde edilen pahalı teknik istihbarattı (Walsh, 2011, s.11). Uyduların ve keşif uçaklarının (U-2'ler, SR-21'ler, İHA'lar) teknolojik yeteneklerine hayranlık duyan yetkililer, istihbarat bütçesinin çoğunu Sovyet tanklarını ve füze silolarını fotoğraflayabilen ve komünist başkentlerdeki

telefon konuşmalarını dinleyebilen gözetleme araçlarına kanalize etmişti (Johnson, 2007, s.8). Bunun yanında istihbarat toplulukları nükleer silahlar ile ilgili teknoloji transferi ve ticari istihbarata da yer yer önem vermişti. Ancak istihbarat alanında bu dönemde yüksek teknolojiye büyük paralar harcanırken zaman zaman verileri bir araya getirecek insanları (analistleri) unutmuş (Yılmaz, 2015, s.79) beşerî casus ağları ihmal edilmiştir (Johnson, 2007, s.8).

ABD ve Sovyetler Birliği'nin iki kutuplu güvenlik yapısının çöküşü, ulusal güvenlik istihbarat teşkilatlarının her zaman izlediği (ancak Soğuk Savaş'ın zirvesinde devlete varoluşsal tehdit olarak görülmeyen) uluslararası terörizm ve uyuşturucu kaçakçılığı gibi daha büyük bir tehdit çeşitliliği ortaya çıkarmıştır. Amerikan Merkezî Haberalma Teşkilatı (CIA) gibi kurumlar, varlıklarını tek bir büyük ve kalıcı hedeften (Sovyetler Birliği) çok sayıda daha küçük ve spesifik hedeflere ayarlamaya mecbur kalmıştır (Walsh, 2011, ss.14-15).

Takip eden yıllarda -özellikle 11 Eylül 2001'den sonra-, küresel bazda istihbarat örgütlerinin çalışmalarının çoğunun odağı, benzer biçimde ulus devletlerden devlet dışı aktörlere, özellikle de El Kaide gibi terör örgütlerine kaymaya başlamıştır. Ancak devlet dışı aktörleri izlemek, büyük ülkelerin konvansiyonel ve stratejik güçlerini izlemekten çok daha zor olmuştur (Fingar, 2011, s.8). Krizlerin ve çatışmaların doğası değişmiş ve bu kaçınılmaz olarak istihbarat alanına da yansımıştır.

Eski Amerikan Ulusal İstihbarat Direktörü Michael McConnell, konvansiyonel bir askeri tehditle başa çıkmanın, düşmanın kabiliyetini belirlemede nispeten daha kolay olduğunu kabul etmektedir. McConnell'a göre konvansiyonel bir düşman söz konusu olduğunda, düşmanın niyeti bir ölçüde bellidir ancak terörizm söz konusu olduğunda tehdidin doğası gereği muğlaklık ve belirsizlik baskın gelir. Bir başka ifadeyle, düşmanın zarar verme niyeti açıktır ama bu noktada istihbarat tarafından karşılaşılan zorluk düşmanın zarar verme kapasitesini öğrenmektir (McConnell, 2007). Dönemin CIA Direktörü Michael Hayden de istihbarat topluluğunun Soğuk Savaş'ta karşılaştığı sorunlarla bugün karşılaştığı sorunlar arasında bir başka farklılığa dikkat çekmektedir. Hayden'e göre Soğuk Savaş sırasında birlik oluşumları, tanklar ve balistik füze siloları gibi düşman kuvvetlerini bulmak görece kolaydı ama imhası zordu. Bugün ise durum tersine dönmüş ve artık



birincil düşmanın imhası kolay, bulunması ve fark edilmesi zordur (Hayden, 2007).

İstihbaratın dönüşümünü etkileyen en önemli bir diğer faktör teknolojik gelişmelerdir. Son yarım yüzyılda insan ve bilgisayar arasında gelişen bir ilişki olmuştur. Başlangıçta bilgisayarlar, insan problemlerini çözmeye ek veya yardımcı araçlar olarak hizmet etmişlerdir. İnternet/Web alanındaki yeni gelişmeler, bilgi-veri alanlarında insan-bilgisayar simbiyozu için yeni roller yaratmış, aslında dinamik problem çözmeye kurumsal kabiliyetleri artırmıştır. Web'in icadı ve en sıradan insan görevlerini bile etkilemeye başladığı olağanüstü hız kapasitesi hem dramatik hem de kafa karıştırıcı bir şekilde gerçekleşmiştir (Glassmann ve Kang, 2012, s.674). Bu da istihbarat kaynaklarının tamamıyla başka bir boyut almasına neden olmuştur. Açık kaynak istihbaratının, kamuya açık bilgilerden üretilen ve belirli bir istihbarat ihtiyacını karşılamak amacıyla toplanan, kullanılan ve zamanında uygun bir alıcıya dağıtılan niteliği göz önüne alındığında, internetin getirmiş olduğu değişim daha iyi anlaşılacaktır.

21. yüzyıldan başından itibaren istihbarat örgütlerinden tüm nükleer silahlı füzelerin yerini saptamak yerine bireysel teröristlerin, bireysel el yapımı patlayıcı cihazların ve bireysel nakliye konteynirlerinin yerini tam olarak belirleyebilmesi beklenmektedir. Odak bir avuç büyük ülkeden, neredeyse 200 ulus-devlette bulunan milyarlarca bireye genişlemiştir. Beklentilerin ve hassasiyet taleplerinin buna bağlı olarak artması, odağı değiştirmekten veya örgütsel birimlere birkaç analist eklemekten fazlasını gerektirmektedir. Küresel iklim değişikliği, bulaşıcı hastalıklar, siber güvenlik, insan kaçakçılığı, sahte ilaçlar ve uluslararası suç ağları gibi yeni sorunlara yönelen istihbarat örgütleri bu odak kaymasına ayak uydurmaya çalışmaktadır (Fingar, 2011, s.9). Bu süreçte istihbarat analizi ne oranda etkilenmektedir sorusunun cevabı için öncelikle istihbarat analizinin ne olduğundan bahsetmek gerekmektedir.

## **2. İSTİHBARAT ANALİZİ**

Analiz, istihbarat döngüsünün en temel aşamalarından biridir (McGlynn ve Garner, 2019, s.22). Toplanan ham istihbaratın işlenmesini ve bu işlenmiş materyalin anlamını deşifre ederek karar vericilere iletilmesini, analistler sağlar (Marrin, 2008, s.131). Bir bakıma raporlama aşaması biter bitmez istihbarat analizi başlar denilebilir. Dolayısıyla istihbarat analizi, bir karar vericiye güvenlik ortamı hakkında bir yorum üretmek amacıyla, bilgiyi

işlemeye ve değerlendirmeye yönelik hem bilişsel hem de metodolojik bir yaklaşımdır (Walsh, 2011, s.237). Özünde istihbarat analizinin amacı uyarı sağlamak, belirsizliği azaltmak ve fırsatları belirlemektir (Fingar, 2011, s.35).

İstihbarat analizi bir gizemi ya da jeopolitik bir bulmacayı çözmeye benzer. Ulusun güvenliğini etkileme potansiyeli olan durumların önceden bilinmeyen boyutlarını keşfetme zorluğu, titizlik gerektirmektedir (Fingar, 2011, s.5). Analiz bir olayı bildirmekten ötesidir; “bu ne anlama geliyor?” sorusuna odaklanmaktadır. Analiz sonucunda ortaya çıkan ürün, hızlı bir yorum, bir olayın yakın vadedeki olası sonuçlarının bir değerlendirmesi, uzun vadeli eğilimler ya da onların potansiyel sonuçları formunda olabilir. Her durumda istihbarat analistleri genellikle belirsiz, tutarsız, eksik ve bazen çelişkili verilerden anlam çıkarmaya çalışır (Hedley, 2007, s.123). Bunun da ötesinde analistler savunulabilir sonuçlara dayalı olarak karar vericilere çözümler veya seçenekler sunarlar. Bu noktada bu tür sonuçların mutlak olmadığı ve istihbarat bulgularını sunarken her zaman bir miktar olasılık veya belirsizlik olacağı kabul edilir (Prunckun, 2010, s.2).

İstihbarat analizi bir bakıma ihtiyaç duyulan problemin araştırılmasından nihai istihbarat ürünlerinin sağlanmasına kadar (örneğin, değerlendirmeler, görüntüler, sinyal raporlama) tüm faaliyetleri içeren bir süreçtir. Analizin en önemli ayaklarından biri olan problemi analiz ederken şu sorular sorulur: Problemin geçmişi nedir? Problemin nedenleri nelerdir? Problemin belirtileri nelerdir? Problemlerle başa çıkmak için mevcut hangi yöntemler var? Bu yöntemlerin sınırlamaları nelerdir? Böylece analiz alt birimler ve dış kuruluşlar tarafından sağlanan rafine, derlenmiş ve işlenmiş bilgi ve verileri kullanarak nihai istihbarat ürünlerini oluşturur (McGlynn ve Garner, 2019, ss.4-28).

Analiz süreci aslında istihbaratın toplanma safhasında başlar. Bir başka ifadeyle analiz açısından ayırt edici durum, istihbaratın toplanmasının analitik ihtiyaçlar için gereken yanıt çerçevesinde olmasıdır. Bu durum veri toplama ve analizi (ve karşı istihbaratı) stratejik bir düzeyde bir araya getiren ve daha sonra istihbarat topluluğuna nüfuz edecek olan ‘istihbarat entegrasyonunun’ da temelidir (Lowenthal, 2020, s.220).

Günümüzde istihbarat analizinin temeli, dijitalleşmenin doğurduğu bilgi yığınyından uygun gerçekleri ayırt etmek ve küresel ölçekteki gelişmeleri ele almak için karar vermesi ve doğrudan eyleme geçmesi

gerekenleri bilgilendirebilecek yargıları ve içgörülerini belirlemeye evrilmiştir. Kararları ve eylemleri olumlu bir fark yaratabilecek şekillerde etkilemek, yaklaşmakta olan krizler konusunda uyarıda bulunmak, tehditleri tanımlamak, sorunları aydınlatmak, bunlara örnek olarak verilebilir (Hedley, 2007, s.124).

Farklı gereksinimler için genellikle (tanımlama, açıklama ve tahmin olmak üzere) üç düzeyde istihbarat analiz yapılır. Tanımlama, mümkün olduğu kadar çok ilgili değişkeni hesaba katarak incelenen olgunun netleştirilmesidir. Açıklama, fenomenin içerdiği unsurların bütün üzerindeki önemini ve etkilerinin yorumlanmasıdır. Tahmin ise durum hakkında sentez ve sonuç çıkarımıdır (Krizan, 1999, s.29).

Analistler taktik (kısa vadeli veya sınırlı bir alanda), operasyonel (belirli bir eyleme göre uyarlanmış) veya stratejik (uzun vadeli veya daha kapsamlı alanda) istihbarat üretirler (Gill ve Phythian, 2018, s.174). İyi istihbaratın zamanında üretilmiş olması, hedefe yönelik düzenlenmiş olması, anlaşılır olması ve bilinen ile bilinmeyeni net bir şekilde gösterebiliyor olması gerekir. İstihbarat analizi yapılırken tüm bu kriterler göz önüne alınmalıdır (Lowenthal, 2020, s.260). Amerikan istihbarat topluluğu Rusya'nın 2016 ABD seçimlerine müdahale etmesine yönelik hazırladığı raporda istihbarat analizinin amacını, karar vericilere titiz, nesnel, zamanında, faydalı ve istihbarat standartlarına uygun değerlendirmeler sağlamak olarak belirtmiştir (U.S. Office of the Director of National Intelligence, 2017, s.1).

### **3. İSTİHBARAT ANALİZİNİN DEĞİŞİMİ VE KARŞILAŞAN SORUNLAR**

İstihbarat analizinin, sivil politika yapıcılara ve askeri uygulayıcılara, karşılaştıkları sorunlar ve almaları gereken kararlarla doğrudan ilgili bilgiler sağladığı (Lowenthal, 2020, s.220), çözüm önerileri ve tahminler sunduğu daha önce ifade edilmişti. Şu ana kadar oluşan literatür ve kavramsal altyapı sayesinde, çalışmanın kapsamıyla ilişkili yeni ve son bir tartışmaya ihtiyaç vardır: İstihbarat olgusunun niteliğinde, sürecinde, teorik yazınında ve pratik uygulamalarında yaşanan dönüşüm, istihbarat analizinde nasıl tezahür etmiştir?

İstihbarat faaliyetinin başarısı, analistlerin doğrudan değişimin faydasını görmelerini, yeni süreçlere ve uygulamalara uyum sağlamalarını, benimsemelerini ve değişimi içeriden yönlendiren bir dijital kültür geliştirip

benimsemelerine bağlıdır. Dijital dönüşüm, istihbarat faaliyetinin tüm yelpazesine avantaj sağlamaktadır. Analistlerin, tehditleri algılama sürecinde hızlı hareket edebilmesi ve içgörülerini karar vericilere iletebilmesi için, dijital dönüşümleri mümkün olduğunca erken benimsenmesi bir zorunluluktur (Ashwell, 2017, s.408).

Gittikçe dijitalleşen çağımızda -istihbaratla ilgili ya da değil- hem her konuda ciddi sayıda veri/data mevcuttur ve bu hem günden güne artmakta hem de bunlara ulaşmak kolaylaşmaktadır. Dolayısıyla istihbarat açısından incelenecek, değerlendirilecek çok sayıda materyal mevcuttur. Yine de salt bilgi toplamak, hızla değişen ve giderek daha fazla birbirine bağlı olan dünyamızı anlamak için gerekli ancak yeterli olmayan bir koşuldur. Terabaytlarca veri tek başına olayların gidişatını, onları neyin yönlendirdiğini, nereye doğru gittiklerini, neyin raydan çıkıp yönünü değiştirebileceğini veya onları nasıl saptırabileceğini ortaya çıkarmaya yetmez. Verileri anlamlandırmak ve karar vericilere yardımcı olacak bilgileri damıtmak (verileri içgörüye dönüştürmek) için analiz etmek ön koşuldur (Fingar, 2011, s.10).

Günümüzde istihbarat analizini gerçekleştiren ekibin, geniş ulusal güvenlik tehditleri yelpazesini anlaması, bunlara ilişkin yargılar geliştirmesi ve benzeri görülmemiş miktarda ve türde bilgiye erişimle başa çıkması beklenmektedir. Aşırı bilgi yüklemesi bu alanda büyük bir zorluk teşkil etmektedir. Bu zorluklar göz önüne alındığında, analiz topluluğunun kapasitelerini artırmak bir gereklilik olarak ortaya çıkmaktadır (Director of National Intelligence, 2015, s.13).

Son dönemlerde istihbarat analizi, iş birliği içinde çalışan bir ekip tarafından yapılan bir etkinliğe doğru sürekli olarak gelişmektedir. Bu değişimin, uluslararası sorunların gittikçe karmaşıklaşması; daha fazla bilgiyi daha hızlı paylaşmaya verilen önemin artması; analistler, toplayıcılar, operatörler ve karar vericiler arasındaki sınırların bulanıklaşması gibi nedenleri bulunmaktadır (Pherson ve Heuer, 2015, s.25).

Soğuk savaş sonrası istihbarat analizinin ayırt edici özelliklerinden biri açık kaynak istihbaratının (Open Source Intelligence, OSINT) artan kullanılabilirliğidir. Dijital OSINT patlaması, 2000 yıllarda üç şeyin bir araya gelmesiyle gerçekleşmiştir: 3G bağlantılı akıllı telefonların kullanımının artması; vatandaşların, ülkelerindeki olaylarla ilgili büyük miktarda içeriği paylaşmak için az sayıda uygulamaya yönelmesi; bu

verilerin ücretsiz ve dünyanın geri kalanının erişmesi ve analiz etmesi için açık olması (Colquhoun, 2016). Dijitalleşmeyle birlikte kapalı toplulukların ve erişilemez alanların sayısı önemli ölçüde azalmıştır. OSINT'in en büyük avantajı erişilebilirliğidir ancak yine de bu kaynakların analiz edilmesi gerekir. Örneğin, güvenilir olarak bilinen bir gazeteyi haber kaynağı olarak kullanan analistin, bu açık kaynak bilgisini karar alıcılara iletirken şüphe ve sorgulama içerisinde olması gerekir. Sahte haber, aldatıcı bilgi, tarafılık, ön yargı ya da manipülasyon riski her zaman mevcuttur. Analist bu ihtimallere karşı uyanık olmalıdır. Aynı risk sosyal medya istihbaratı için de geçerlidir. Sosyal medya içerik açısından görece manipülasyona ve dezenformasyona açıktır. Sosyal medyadan toplanan istihbaratın analizinde doğru/yararlı bilgiler ve kasıtlı/yanlış gönderilerin ayırt edilmesi önemlidir (Lowenthal, 2020, ss.165-174). Benzer bir risk olarak internetten veya kamuya açık raporlardan elde edilen açık kaynaklı istihbarat, rakipler/düşmanlar tarafından kasıtlı olarak yayınlanan yanlış ve yanıltıcı bilgiler içerebilir. Analistleri yanıltılmak ve istihbarat başarısızlığına yol açmak gibi amaçları içeren bu dezenformatik durumlara karşı, sorgulayıcı bir temelde yaklaşmak gerekir (Wu vd, 2022, s.452).

OSINT'in sağladığı verilerin büyüklüğü ve çeşitliliği bu yöntemle toplanan istihbaratın analizinde bilgisayar temelli farklı tekniklerin kullanılmasına yol açmıştır. Metinlerin analiz edilmesinde dilbilimel/metin tabanlı yöntemler, konum bilgileri ve kartografik bilgilerin analiz edilmesinde coğrafi bilgi sistemleri (GIS) ve uzaktan algılama, ilişkilerin, grupların ve ağların analizi için ağ bilimi ve son olarak da medya tabanlı verilerin analizinde görsel adli bilimler, OSINT ile elde edilen verilerin analizinde kullanılan tekniklerin başlıcalarıdır (Ünver, 2018, s.8). İnsan destekli olarak gerçekleştirilen bu analizlerin yönü artık makine öğrenmesinin de bu alanda uygulanması ile birlikte, artık sonuç odaklı çıkarım yapmanın otomasyona bağlanacağı bir sürece doğru evrilmektedir (Williams ve Blum, 2018, s.40). OSINT sayesinde bireyler, gruplar (şirketler, kurumlar, örgütler, ülkeler gibi), olaylar, coğrafi bilgiler, IT ile ilgili veriler (alan adları, yazılımlar gibi) ve nesnelere (resim ve video gibi) hakkında bilgiler daha kolay ve yoğun biçimde edinilebilmektedir (Böhm ve Lolagar, 2021, s.325).

Bu şartlar altında istihbarat analizinde bilgisayar tabanlı ağ analizi, profil oluşturma ve veri madenciliği gibi yeni yöntemlerin önemi artmıştır. Örneğin ağ analizi, bireylerden kurumlara çeşitli hedefleri hakkında veri

toplamak için hem suç hem de güvenlik istihbaratında yaygın olarak kullanılmaktadır. Ağdaki düğümler arasındaki temas miktarlarını ölçmek (örneğin, e-posta ve telefon görüşmelerinin meta verilerini kaydederek) görece basittir, ancak bu temaslar içinde yararlı istihbaratı ayıklamak çok daha zordur. Bir diğer örnek olan profil oluşturma ise, hedefleme kararları için temel olarak kullanılan olağandışı veya şüpheli davranış kalıpları için büyük veri kümelerinin incelenmesine dayanan tekniklerdendir. Bu amaçla potansiyel tehditler hakkında veriler yığın halinde biriktirilir ancak veri yığınlarının işlenmesinin aynı zamanda pek çok gereksiz bilgi içerdiği (profile uyan ancak hedef faaliyete dâhil olmayan insanlar gibi) unutulmamalıdır (Gill ve Phythian, 2018, s.175).

Büyük veri terimi, mobil İnternet, bulut depolama, sosyal ağlar ve ‘nesnelerin interneti’ gibi yeni bilgi teknolojileri (IT) tarafından yaratılan katlanarak artan miktarda dijital bilgi anlamına gelmektedir. Büyük veri, bilgide yalnızca niceliksel bir artışı değil aynı zamanda yeni bilgi yaratma ve dünyayı anlama biçimimizde niteliksel bir değişikliğe işaret etmektedir. Büyük verideki patlamanın çoğu, bilginin giderek daha fazla sosyal (birkaç büyük üretici yerine birçok kullanıcı tarafından üretilip iletilen), mobil (her yerde bulunan, internete bağlı mobil cihazlardaki sensörler tarafından toplanan) ve yerel (coğrafi olarak etiketlenen) olmasından kaynaklanmaktadır. Bu patlama sadece istihbaratın toplama alanını değil aynı zamanda işleme, analiz ve dağıtım süreçlerini de doğal olarak etkilemiştir. İstihbarat alanında büyük verinin en büyük vaadi, bilgileri bütünleştirme ve organize etme potansiyelidir. Verileri toplamak, taşımak, depolamak ve organize etmek için kullanılan yeni teknolojiler, tüm kaynaklardan analistlere daha fazla otomasyon ve üretkenlik ile çok daha fazla bilgiye erişim sağlayabilmekte ve böylece sınırlı bilişsel kapasitelerini en zor, en yüksek öncelikli sorunlara yoğunlaştırmalarına imkân vermektedir. Herhangi bir analist tarafından henüz işlenmemiş çok büyük miktarda veri depolanıp daha sonra gelecekteki veriler veya gereksinimler bağlamında işlemek veya ilişkilendirmeleri veya eğilimleri keşfetmek veya tanımak için kullanılabilir. Makine öğrenimi, tüm bu sürecin zamanla gelişmesini sağlar. Verilerin toplanması ve algoritmaların iyileştirilmesi, dinamik ve kademeli olarak daha doğru modellere veya daha sağlam ve uyarlanabilir modellerine imkân verir ve buna göre daha spesifik veya daha anlamlı anormalliklerin tespit edilmesini sağlar (Symon ve Tarapore, 2015, ss.4-6).

Her ne kadar internet ve sosyal medya büyük verinin varlığını mümkün kılan açık kaynaklar olsa da büyük veri internetten de iletişimden de daha fazlasıdır. Büyük veri kullanımı ile amaç normal şartlarda anlamlandıramadığımız veri kümesinden yeni çıkarımlar yapabilmektir. Böylece analistler araştırma konuları hakkında büyük miktarda bilgi toplayıp analiz ederek riskleri ve tehditleri tahmin etmeye yardımcı olabilecek trendler ararlar (Cukier ve Mayer-Schoenberger, 2013, ss.28-29).

Veri madenciliği büyük veri yığımındaki belirli örüntülerin ortaya çıkarılmasını sağlar. Veri madenciliği yoluyla tespit edilen modeller, bu süreçte farklı değişkenlerin bazılarının ilişkili olduğunu göstermekle birlikte nedenselliğe ulaşmakta yeterli değildir. Örneğin analistler, veriler arasındaki korelasyonlarla yalnızca bir kişi tarafından sergilenen belirli bir modelin bir teröristi işaret ettiğine ulaşabilir ancak tek başına bu çıkarım, bireyin tahmin edildiği gibi bir terörist olduğunu göstermez (Lahneman, 2016, s.710). Bunun yanında büyük veri analizi sınırlı soruları ele almak için tek veya çoklu toplama platformu şeklinde yapılandırılmış verileri kullanılarak kim, ne, nerede ve ne zaman sorularının analizinde işe yararken neden ve nasıl sorularının analizinde daha küçük bir rol oynar. Bu nedenle analiz sürecinde, istihbarat döngüsünü yönlendirilmesi ve verilerin kölesi olmak yerine, bu verilerin alıcının/karar vericinin gereksinimlerine hizmet ettiğinden (doğru soruları sorarak ve toplama ve analizi buna göre yönlendirerek) emin olunmalıdır (Symon ve Tarapore, 2015, s.8).

OSINT ürünlerini kullanmayla ilgili en önemli zorluklardan biri, halka açık olan bilgilerin hacmi ve bu bilgilerin doğasında bulunan güvenilirlik dereceleridir. Analiz alanında, verilerin artan hacmi, hızı ve çeşitliliği, ‘gürültü ile sinyali’ veya yığın verilerden yararlı bilgileri ayırt etmeyi zorlaştırmaktadır. Geleneksel beceriler, sistemler ve süreçler, çok fazla ‘sinyalin’ olduğu bir ortamda mücadele ettiğinden potansiyel ‘istihbarat başarısızlıklarının’ oluşmasına neden olabilmektedir. Modern bilgi işlem ve veri altyapısının geliştirilmesi ve sürdürülmesi, ticari sağlayıcıların, kullanıcılarının ihtiyaçlarına uyum sağlamak için önemli kaynaklara ve esnek bir yaklaşıma sahip olmasını gerektirmektedir (Janjeva, Harris ve Byrne, 2022, s.8).

Bu nedenle, güvenilir, ‘iyi’ istihbaratı ‘kötü’ istihbarattan ayırmak için, OSINT’ analizlerine adapte olacak yeni modellere ihtiyaç vardır. Analiz sürecinde bilginin toplanması, anlaşılması, sınıflandırılması ve aynı zamanda

farklı kullanıcılar, ihtiyaçlar, görevler, organizasyonlar, kurumlar ve yasaların göz önünde bulundurulması gerekmektedir. Ancak böylelikle nihai ürün, mevcut kaynakların rehberliğinde analitik ve iyi sonuçlar sağlayabilecektir (Williams ve Blum, 2018, s.17). Açık kaynak verilerinin ‘açık ve var’ olması erişimin mutlaka kolay olduğu anlamına gelmez. Araştırmayı ilerletmek için gerekli verilerin belirlenmesi, bu tür verileri elde etmek için en iyi kaynağın ve yöntemin hangisi olduğunu belirlemenin ilk adımıdır. Ayrıca, doğru verilere erişilmesi yetmez. Bu verilerin kullanılabilir bir formatta olması da gerekir. Bu gereklilik analiz sürecini önemli ölçüde yavaşlatma riski barındırdığından, verilerin dönüştürüleceği formatlar da analiz ve üretim sürecinde dikkate alınması gereken bir konudur (Gibson, 2016, s.73).

OSINT altında da sınıflandırılabilen ama sunduğu imkânlardan dolayı farklı bir istihbarat toplama disiplini olarak da kabul edilen dijital çağdaki bir diğer kaynak, sosyal medya istihbaratıdır. Literatüre SOCMINT olarak geçen (Omand, Barlett ve Miller, 2012) sosyal medya istihbaratı, sosyal medyanın çok geniş kitleler tarafından aktif olarak kullanılmasından ötürü, istihbarat açısından değerli bir kaynaktır. Dijital ortamda tartışan, konuşan, şakalaşan, kınayan ve alkışlayan milyonlarca insanın tutumunu ölçmek ve anlamak istihbarat açısından değerli bilgi potansiyeli taşımaktadır. Örneğin şüphelileri hakkında konum vb. bilgiler arayan istihbarat görevlileri için sosyal medya, günümüzde hayati bir kaynak haline gelmiştir. Diğer taraftan kendi amaçları için kamuoyunu ve duyarlılığını anlamaya ve gizlice etkilemeye çalışanlar için de sosyal medya giderek daha da önem kazanmaktadır<sup>1</sup>. Sosyal medyayı izleyerek toplanan istihbaratı ifade eden SOCMINT, dijital çağın önemli bir parametresine dönüşmüştür (Omand, 2017, s.369). SOCMINT kullanılarak olayların 'ne zaman' meydana geldiği, şu anda 'ne' olduğu, 'nerede' ve 'kim' ile ilgili olduğu anlaşılabilir. Gerçek zamanlı durumsal farkındalık sağlanabilir. Terörizmden sokak suçlarına kadar söz konusu faaliyetlerin ‘neden’ ve ‘nasıl’ olduğu gibi, gözlemlendikleri şekliyle olayların olası en iyi nedensel açıklamasını oluşturularak bu tür suç örgütlerine dair içgörüler elde edilebilir. Olaylara ve katılımcıların motivasyonlarına ilişkin yeterli açıklamalar elde edildiğinde, olayların nasıl gelişeceğine dair bir tahmin yürütülebilir. Sosyal medyadan

---

<sup>1</sup> Rusya'nın 2016 ABD başkanlık seçimlerindeki sosyal medya üzerinden yaptıkları için bkz. Robert S. Mueller Report On The Investigation Into Russian Interference In The 2016 Presidential Election, <https://www.justice.gov/archives/sco/file/1373816/download>



elde edilenler sayesinde politik ve operasyonel otoritelerin ‘sırada ne var’ ve ‘nerede’ gibi kaçınılmaz sorularını yanıtlamak kolaylaşabilmektedir (Omand, Barlett ve Miller, 2012, s.804; Omand, Barlett ve Miller, 2014, s.25).

Sosyal medyadan üretilen istihbaratın analizinde dikkat edilmesi gereken hususları örneklendirmek için bazı temel sorular sormak faydalı olabilir: Araştırılan istihbarata ilişkin sosyal medyada en etkili kişiler kimlerdir ve neden bu kadar etkililerdir? Cevap arama sürecinde, takipçi sayısı ve mesajlarının içeriğine bakılabilir. Ancak bu bizi bir başka soruya götürür: Diğer tüm veri toplama kaynakları gibi sosyal medya da aldatıcı içerikler barındırır. Araştırılan sosyal medya hesapları gerçek olmayan bir isimle açılmış olabilir ya da bireyler birden fazla hesaba sahip olabilir. Twitter gibi sosyal ağlarda, sahte takipçi satın alınabilmektedir (399 dolara 100.000 takipçi gibi). Ayrıca bu veriler belirli teknolojiler aracılığıyla elde edilebilmekle birlikte, örneğin Twitter akışlarının coğrafi konumu yanıltıcı olabilir. Bu gibi nedenlerden dolayı analistler büyük belirsizliklerle uğraşırlar. Dolayısıyla çoğu sosyal medya verisi ilk aşamada ham/güvenilmez istihbarattır ve önemli bir raporun temeli haline gelmeden önce -tıpkı diğer tüm istihbarat kaynakları gibi- analizi dikkatli yapılmalıdır (Lowenthal, 2020, s.184).

Analiz edilecek bilgi yığını her an arttığından analistlerin bu bilgi kaosunda anlamlı yorumlar getirme yeteneği, hizmet ettikleri topluluklarda kamu güvenliği ve yaşam kalitesi üzerinde büyük bir değere sahiptir. Öte yandan, analitik ve tahmine dayalı verilerden doğrudan operasyonel bir model oluşturma fırsatı, kamu güvenliği ve istihbarat uzmanlarına, rakiplerinin karar ve uygulama döngüleri içinde manevra yapma yeteneği verebilmektedir. Terörizme, uyuşturucuya veya diğer suçlara karşı savaşta, gelişmiş bilgi ve gelecekteki eylemleri tahmin etme yeteneği, ülkeler için hayati önemdedir (McCue, 2015, s.xxiv).

Ancak yığınlar halindeki âtıl/anlamsız veriler, istihbarat açısından bir anlam ifade etmez. Bu nedenle verilerin kullanılabilir olmaları için üzerinde çalışılması gerekir. Bu noktada algoritmalar önem kazanır. Algoritma seçimi, verilerin anlamlandırılmasını etkileyebilir. Farklı veri türlerini (salgın verileri, finansal veriler, sosyal medya verileri vb.) yorumlamak ve anlamlandırmak için farklı algoritmalar ve farklı uzmanlık türleri gereklidir. Ayrıca birbirleriyle uyumlu olmayan veri türlerini (heterojen veriler)

birleştirme ve anlamlı bir bütüne dönüştürme sorunu ile karşı karşıya kalabilme riski mevcuttur. Tıpkı diğer istihbarat kaynaklarının analistlere aktarılmadan önce işlenmesi ve ayıklanması gerektiği gibi, verileri anlam ifade edecek bir biçime veya içeriğe çevirmek, istihbarat analizi için zorunludur (Lowenthal, 2020, s.186).

İstihbarat topluluklarının sözü edilen zorluklara ayak uydurma çabaları biz dizi yeniliği beraberinde getirmiştir. Özellikle analiz sürecine yönelik gelişmeler bu açıdan dikkat çekicidir. Bunlardan biri CIA analistleri tarafından geliştirilen ve Wikipedia ile aynı yazılımı kullanan, kimin neyi eklediğine dair bir denetim izi sağlayan Intellipedia<sup>1</sup> platformudur. Bu platform, bilgileri mümkün olan en geniş kitleye ulaştırırken, üç sınıflandırma seviyesine (tasnif dışı, gizli ve çok gizli) göre bilgiyi kategorize eder. Resim 1 ve Resim 2’de örnekleri gösterilen Intellipedia platformu kullanılabilir istihbari verilerin yanı sıra çok sayıda yararlı makale ile analistlerin bakış açılarını genişletmelerine katkıda bulunmaktadır (Gill ve Phythian, 2018, s.178).

Resim 1. Edward Snowden’e ait Intellepedia Ekranı (Kaynak: The Black Vault, <http://documents.theblackvault.com/documents/intellipedia/Intellipedia-Snowden.pdf>)

**(U) Edward Snowden** 🔍 📄 🗑️ 📧

UNCLASSIFIED//~~FOUO~~

From Intellipedia

You have new messages (last change).

See the Wikipedia article  
*Edward Snowden*

**(U)** This article contains information about a **United States Person**, as defined by the Intelligence Oversight regulations. 🇺🇸

**(U)** The information herein falls under the provision(s) for: publicly available information.

(b) (3) -P.L. 86-36

**(U)** Placeholder page. Requires more substantive information. See discussion.

Retrieved from [redacted]  
Category: United States persons

UNCLASSIFIED//~~FOUO~~

(b) (3) -P.L. 86-36

- This page has been accessed 3,434 times.
- 1 [redacted] watching user
- This page was last modified 17:05, 31 December 2015 by [redacted] Most recent editors: [redacted] and [redacted]

<sup>1</sup> Intellipedia hakkında daha fazla bilgi için bkz. Emily Dreyfuss, "The Wikipedia for Spies—And Where It Goes From Here", <https://www.wired.com/2017/03/intellipedia-wikipedia-spies-much/>

Resim 2. Vatikan'a ait Intellopedia Ekranı (Kaynak:  
Muckrock,(https://www.muckrock.com/news/archives/2014/feb/17/needs-edit-  
intellipedia-nsas-own-wikipedia/)

## (U) Vatican City

From Intellopedia

(Redirected from Holy See)  
From Intellopedia

UNCLASSIFIED//~~FOUO~~

Location: Map | Coordinates | About

### Contents




- 1 Threats
- 2 See also
- 3 References
- 4 External Links

### Threats

(U) Al-Qaeda (AQ) has expressed a strong hatred for the Pope and the Roman Catholic Church in the last several years. The group has called them enemies and denounced attempts by the Holy See to reach out to Islam as part as a "crusader campaign."<sup>[1]</sup> AQ vowed to wage a *jihād* against Christians following controversial remarks made by Pope Benedict XVI.<sup>[2]</sup> It is likely any attack against Vatican City or senior officials of the Holy See in Italy would be perpetrated by AQ.

### See also

- Pope Benedict XVI US Visit

<i>Status Civitatis Vaticanae</i> (Latin) <i>Stato della Città del Vaticano</i> (Italian) State of the Vatican City	
	
Flag of Vatican City National Emblem of Vatican City	
Motto: none	
Anthem: <i>Inno e Marcia Pontificale</i>	
	
<b>Capital</b>	Vatican City <sup>1</sup> 41°54' N 12°27' E
<b>Largest city</b>	Vatican City <sup>1</sup>
<b>Official language(s)</b>	Latin <sup>2</sup>
<b>Government</b>	Ecclesiastical Pope Benedict XVI Secretary of State Tarcisio Cardinal Bertone
<b>Independence</b>	11 February 1929 Lateran Treaties
<b>Area</b>	
• Total	0.44 km <sup>2</sup> (194th) 108.7 acres or 0.17 mi <sup>2</sup>

Bunun yanında Amerikan istihbarat topluluğundaki tüm analistler için ortak bir çalışma alanı olan A-Space; iletişim bilgileri ve becerileri, uzmanlıkları ve deneyimleri hakkında ayrıntılar da dâhil olmak üzere Amerikan istihbarat topluluğundaki analistler hakkında bilgiler içeren bir veri tabanı olan Analitik Kaynaklar Kataloğu; dağıtılmış tüm istihbarat ürünlerinin entegre aramalarını, çapraz referanslarını sunan, tüm analistlerin belirli konulardaki raporları bulmasına olanak tanıyan Ulusal İstihbarat Kütüphanesi gibi bazı yeni platformlar, yeni dönemdeki zorluklarla daha kolay baş edebilmek için atılmış adımlara örnektir (National Research Council, 2011, s.11). İstihbarat analizinin platformlaştırılmasında bir diğer somut uygulama, zaman baskısı olan istihbarat değerlendirmelerinin üretiminde insanların, algoritmaların, yazılımların, araçların ve manuel çalışmanın entegrasyonunu geliştirerek istihbarat analistlerini güçlendirmek için tasarlanan Analitik Bileşen Sistemi (ACS) adı verilen bir hesaplama platformudur (Schmidt ve Vogel, 2020). Benzer şekilde hızla artan veri hacimlerini etkin bir şekilde yönetmek için gerekli araçları, analistleri ve

karar vericileri desteklemek için gerçekleştirilen çalışmalar, diğer ülkelerde de devam etmektedir. Örneğin Birleşik Krallık, analistlerin hem kamuya açık kaynaklar hem de dâhili hükümet raporları aracılığıyla bilgileri işlemesine yardımcı olacak (kullanıcıların açık kaynak materyali bulması, bağlaması ve tanıtması için ortak bir alan sunan) bir platform olan Bilgi ve Veri Alışverişi (INDEX) platformunu geliştirmiştir (Janjeva, Harris ve Byrne, 2022, s.10).

Dijital çağda istihbarat analistleri, artık geleneksel yöntemler yerine, otomatik arama, indeksleme, kategorilere ayırma ve yapılandırma süreçlerini takip ederek sürekli olarak bilgiyi (veya indekslerini) kurumsal bilgi tabanına aktarmaktadır. En alt seviyelerde, bu yapılanma söz dizimsel bir seviyede gerçekleştirilse de yakın gelecekte insanların, yerlerin, duyguların, hareketlerin, çağrışımların otomatik olarak tanımlanması gibi semantik veri yapılanmasının sunacağı fırsatlarla önemli ilerlemeler gerçekleşeceği öngörülmektedir. Bu alanda yapılacak çalışmalarla geleceğin analistinin bilgiyle etkileşiminin daha kolay ve işlevsel olacağı tahmin edilmektedir (Hare ve Coghill, 2016, s.9).

Günümüzde üretilen istihbarat, çok farklı formatlarda, bağlantısız veya erişilemeyen çok sayıda sistemde, standartlaştırılmış yapılar olmadan ve üzerinde anlaşmaya varılan kapsayıcı bir ontoloji olmadan üretilmektedir. Bu durum, bilgi toplama çabasının boşa gitmesi, zamanında istihbarat üretilmemesi, işaretlerin ve uyarıların gözden kaçırılması ve üretilen istihbaratın karar almayla ilgili olmaması risklerini taşımaktadır. Bu faktörler, istihbarat döngüsünün erken safhalarında ve toplama noktasına mümkün olduğunca yakın çok kaynaklı istihbarat oluşturmak için verilerin birleştirilememesine neden olabilir. Dolayısıyla, istihbarat analizi politika yapıcılara ve uygulayıcılara zamanında, ilgili analitik yargılar ve eyleme geçirilebilir istihbarat sağlamak için zor, külfetli ve üstesinden gelinmesi gereken engeller içeren bir faaliyet haline gelmiştir (Weinbaum ve Shanahan, 2018, s.5).

Veri ve dijital teknolojiler, insan faaliyetinin her sektörü üzerinde belirgin bir etkiye sahip olan hızlı ve devam eden bir dijital dönüşümün temelini oluşturmaktadır. Bu dönüşüme ayak uydurabilenler, rakipleri karşısında kritik bir karar alma avantajına sahip olabilecektir. Geleneksel istihbarat döngüsüne (yönlendirme, toplama, işleme ve dağıtım) dayanan istihbarat analistlerinin artık dijital dönüşümün etkisiyle veri, korelasyon, tahmin ve karar vermeden oluşan yeni bir modelden yararlanması

gerekmektedir. Büyük veri, yapay zekâ ve algoritma kültüründen, paylaşım ve füzyondan yararlanan, nedenlere değil korelasyonlara odaklanan ve geleneksel sınıflandırılmış metodolojilerin yanı sıra bulut, kitlesel ve sosyal medya kaynaklarını kullanan bir modelin, istihbarat analizinin geleceği olması muhtemeldir (Ashwell, 2017, s.405).

## SONUÇ

21. yüzyılda özellikle iletişim ve internet alanında yaşanan gelişmeler, bu çağın dijital/bilgi çağı gibi terminolojik ifadelerle adlandırılmasına neden olmuştur. Dijital çağdaki gelişmeler kaçınılmaz olarak istihbarat alanını etkilemiştir. Açık kaynak verilerindeki patlama, sosyal medya platformlarının yaygınlaşması ve veri analizinde yaşanan gelişmeler, istihbarat analizinin dönüşmesini gerektirmiştir.

İstihbarat analiz sürecinde, analistler uzun süre yeterli veri kaynağının olmamasının zorluklarını yaşamış ve yalnızca az miktarda veri yoluyla çıkarım yapabilmişlerdir. Bu da zaman zaman istihbarat başarısızlığının meydana gelmesine yol açmıştır. Sensör, internet ve diğer teknolojilerin hızla gelişmesiyle birlikte, açık kaynaklı istihbarat verileri, sinyal istihbarat verileri, uzaktan algılama görüntüleri gibi istihbarat veri kaynakları bugün bu zorlukları aşmak için ciddi fırsatlar sunmaktadır (Wu vd, 2022, s.451).

Birçok alan için geçerli olduğu gibi istihbarat analizi görevi de dönüşmektedir. Yeni teknikler ve teknolojiyle birleşen yeni bir dizi zorluk, istihbarat faaliyetinin doğasında yapısal bir değişime neden olmaktadır. İstihbarat analizindeki ilk büyük değişiklik, faaliyet alanının hacminin ve kapsamının artmasıdır. İstihbarat analizi artık her zamankinden daha fazla alanda gerçekleşmektedir. 10 yıl önce öyle önemsiz görünen sağlık, siber güvenlik ve iklim değişikliği gibi bağlamlar artık istihbarat analizi için büyük önem taşımaktadır. Bir diğer dönüşüm parametresi, istihbarat analistlerinin her zamankinden daha fazla bilgiyle uğraşmak, her zamankinden daha fazla bilgiyi sentezlemek ve anlamlandırmak zorunda kalmasıdır. Ayrıca istihbarat analizi, artık daha fazla iş birliği gerektirmektedir. Geleneksel istihbarat analizi bireyler tarafından yapılan tekil bir faaliyetken, bu alandaki ekip çalışmasının önemi ve faydası, problem alanının karmaşıklığı arttıkça anlaşılmaktadır (Cooke, 2015, s.132).

Dijital bir dönüşümün içinde bilgi çağı teknolojileri beklenmedik ve durmaksızın bir hızla gelişmeye devam etmektedir. Nesnelerin interneti ve büyük veri analitiği kavramları günlük yaşamın her alanına nüfuz etmiş

durumda. Dijital teknolojilerin etkisi ve internetin gelişimi kitlesel birbirine bağlılığı güçlendirerek tüm faaliyet alanlarındaki hızlı değişimin temelini oluşturmaktadır. Bu değişim istihbarat analizi kuruluşlarının ve kolluk kuvvetlerinin karşı karşıya kaldığı organize suç ve terörizm gibi meseleleri daha iyi anlama ve bunlarla mücadele etmek için süregelen dijital dönüşümden tam olarak yararlanma fırsatı sunmaktadır. Diğer taraftan tehditlere karşı koymak için veri ve bilgi teknolojilerinden yararlanacak analistlerin yetiştirilmesi büyük önem arz etmektedir. World Wide Web, sosyal medya ve artan küreselleşme gibi devlet-örgüt-insan faaliyetinin tüm yönlerini etkileyen olaylar veriye, bilgi teknolojilerine ve insana odaklanan etkin dijital dönüşüm, çağa ayak uydurabileceklere önemli bir rekabet avantajı sağlama potansiyeline sahiptir. Dijitalleşme, daha önce karmaşık olan süreçleri ve görevleri, analistlerin anlamasını ve kullanmasını kolaylaştırmaktadır. Giderek daha fazla otomatikleştirilen veri madenciliği ve analizi yeni ve heyecan verici içgörüler ve modeller sağlamaktadır. Verilerdeki algoritmalar ve korelasyonlar fırsatları ortaya çıkarmakta ve çeşitli faaliyetlerde potansiyel rekabet avantajı sağlayan karar verme sürecini iyileştirmektedir (Ashwell, 2017, ss.393-394).

Dijital dünyada istihbarat üretim sürecinin dönüşmesi kaçınılmazdır. Bu sürecin özü, daha fazla veri aramak ve bir analistin yapabileceğinden çok daha fazla hipotezi inşa etmek için algoritmalar ve istatistikler kullanan makinelerle yön vermeye dayanmaktadır. Beşerî analitik beceri ve deneyim makinelerin oluşturduğu korelasyon modellerini ve bilgileri elemek için hala çok fazla gerekli olsa da algoritmalar ve bilgisayar modelleri, analistleri, arama ve işleme yükünün çoğundan kurtarabilir ve analitik görevin kritik unsuruna, yani problem çözmeye odaklanması için daha fazla zaman sunar. Uygulamalar bilgiyi özümseme, anlamlandırma ve karar verme şeklimizi değiştirmektedir. Doğal olarak bilgi yığınlarına, karmaşık fikirlere ve teknolojilere uygun maliyetli erişime izin verir ve bunların kullanımını basitleştirirler (Ashwell, 2017, ss.399-400). Veri işleme teknolojileri, verilerden tam olarak yararlanma, tamamlayıcı entegrasyon ve kapsamlı araştırma/muhakeme gibi dijital yenilikler, istihbarat analizini iyileştirmenin anahtarlarıdır. Derin öğrenme gibi akıllı algoritmalar, istihbarat analistlerinin doğal dil anlama, konuşma tanıma, görüntü sınıflandırma, hedef tanıma gibi işlemleri hızlı bir şekilde gerçekleştirmesine, işleme verimliliğini artırmasına, dolayısıyla analistlerin yükünün azalmasına ve gizli korelasyon bilgilerinin keşfedilmesine yardımcı olan araçlardır. Büyük veri yığınlarının

işlenmesi için fayda sağlayan akıllı algoritmalar ve büyük verileri verimli bir şekilde depolayabilen bulut teknolojileri analiz sürecinde ek yükü azaltan gelişmelerdir (Wu vd, 2022, ss.451-454).

Özetle, dijitalleşme, algoritmalar, yapay zekâ gibi yeni istihbarat analizi modellerinin önemi yadsınamaz bir gerçeğe dönüşmüştür. Ancak sadece bu dijital yöntemler üzerinden istihbarat analizini gerçekleştirmek mümkün değildir. İnsan unsuru analiz sürecinin halen oldukça önemli bir parçasıdır. İstihbarat gizemleri salt bilgi toplanarak çözülemez. Bir gizemin derinlerine inmek, analiz ve muhakeme gerektirir. Veri tufanı çağında bu noktada istihbarat topluluklarının özellikle ekonomistlerden veri bilimcilere kadar uzmanların niceliksel ve niteliksel analitik yeteneklerinden daha fazla yararlanmaları gerekmektedir (Coyne, 2017).

Dijital olarak dönüşen istihbarat organizasyonlarında, insan sezgisinin eşsiz gücüne hâlâ ihtiyaç var. Makineler devasa verileri toplayıp işleyebilir ve birden çok hipotezi dikkate alarak ilgi alanları, modelleri ve aykırı değerleri üretebilirken, insanlar da arama sürecini yönlendiren üst akıl olarak konumlandırılmalı, makinelerin sunacağı pek çok seçenek arasından en değerli bilgi ve bilgi külçelerini hızla elemek ve seçmek için deneyim ve sezgilerini uygulamaya devam etmelidir. Özetle gerekli olan şey makinelerin giderek daha fazla veri işleme sürecini üstlendiği ve analistlere en zor sorun çözme görevine odaklanmaları için giderek daha fazla zaman tanıyan doğru koşullardır. Aynı şekilde analistlerin dijital çağ süreçlerini ve davranışlarını benimsemelerini teşvik eden veri ve teknolojilerle etkileşime girmelerine olanak sağlamak sürecin anahtarı olmaya devam edecektir (Ashwell, 2017, ss.394-407).

Son olarak, istihbarat analizinde dijitalleşmeye yönelik birtakım varoluşsal eleştirilerden bahsetmek gerekir. Wu ve arkadaşlarına (2022) göre akıllı algoritmaların uygulamalarında belirli sınırlamaları olduğu ve istihbarat analizlerinde tamamen insanın yerini alabilmeleri için daha kat edilmesi gereken çok yol var (Wu vd, 2022, s.452). Gilchrist'e (2017) göre ise veri kaynaklarındaki olağanüstü artış bunları işlemek için insan kaynaklarındaki artışla paralel olmamıştır. Doğası gereği insani ve belirsiz bir sorun olan savaşlar için makine çözümlerine ve kesinliğe sahip olacaklarına dair vaatler ve bilgi üstünlüğünün kutsallaştırılması orduları, savunmasız bırakmaktadır. Mevcut yazılımlar-algoritmalar karmaşık insan etkileşimlerini, iyi eğitilmiş bir analistin yapabileceği veya yapması gerektiği

şekilde veya aynı zaman duyarlılığıyla anlamlandıramaz. Öte yandan askeri analistler geleneksel olarak nicel becerilerden çok nitel becerilere güvenirlir. Başarıları büyük ölçüde zor kazanılmış deneyimlerden gelen sezgilere dayanmaktadır. Gelişmiş analitiği çalıştırmak için gereken beceri ve yetenek ise büyük ölçüde bunun tersidir. Analistler sosyal medya gönderilerinden, görüntü kayıtlarına ve tonla kâğıt parçasına kadar her şeyle ilgilenir. Veri standartlarını kontrol etmek hem inanılmaz derecede zordur hem de zaman alıcıdır. 'Veri girişi' zayıf olduğunda, 'veri çıkışı' yanlış olacaktır. Orduya pazarlanan analiz platformlarının birçoğu finans ve endüstri için geliştirildiğinden savaşın doğasında var olan kaosa düzen getirebilecek bir algoritma yazmak büyük ölçüde imkânsızdır (Gilchrist, 2017).

İstihbaratın tarihsel ve konjonktürel anlamda değişimi, güvenlik tehditlerinin bertaraf edilmesinde sürekli yeni zorluklar inşa eden bir diyalektiği doğurmaktadır. Bu durum, istihbarat çarkında en önemli aşamalardan biri olan istihbarat analizinin önemini artırmaktadır. İstihbarat toplulukları teknolojinin, ulaşımın ve iletişimin sürekli gelişiminin yanında artan küreselleşmenin yarattığı yeni koşullara ayak uydurma sorunuyla baş etmek zorundadır. Bu kapsamda istihbarat analizinde yeni yöntemlerin geliştirilmesine ek olarak mobilite ve hibritleşmeyi zorunlu kılan bir anlayışın analistlere yön vermesi gerekliliği ortaya çıkmaktadır.

İnternet ve dijitalleşmenin giderek yaygınlaşacağı aşıkârdır. Bunun doğal bir sonucu olarak algoritmalar istihbarat analizindeki süreçlerde ilk sıralarda olmaya devam edecektir. İlerleyen dönemlerde kapsamı ve içeriği artması muhtemel bilgi yığınlarından anlamlı analizler gerçekleştirebilecek analistlerin yetiştirilmesi, eğitilmesi ve uzmanlaştırılması<sup>1</sup>, ülkeler ve istihbarat toplulukları için hayati öneme sahip olacaktır. Bilgi güç demektir. Gelecekte bilgiyi yorumlamak, güvenliği sağlamak için temel kıstas olma potansiyeline sahiptir.

---

<sup>1</sup> 2008 yılında Amerikan Ulusal İstihbarat Direktörü, Ulusal Araştırma Konseyi'nden, analitik yöntemlerle ve bunların istihbarat alanındaki potansiyel uygulamalarıyla ilgili davranışsal ve sosyal bilimlerden elde edilen yöntemleri değerlendirmelerini talep etmiştir. Bu talebin ardından Konsey istihbarat alanında davranışsal ve sosyal bilimlerin özellikle analiz alanında kullanılmasını, bilimsel analitik yöntemlerinin analistlere öğretilmesini, bilimsel iş birliği yöntemlerinin uygulanmasını ve bilimsel iletişim yöntemlerine başvurulmasını önermiştir (National Research Council, 2011, s.xiii).



## KAYNAKÇA

- Ashwell, M.L. (2017). The digital transformation of intelligence analysis, *Journal of Financial Crime*, 24(3), ss. 393-411, doi: 10.1108/JFC-03-2017-0020
- Biçer, S. (2017). Ulusal güvenlik ve istihbarat sisteminde geleneksel anlayıştan modern ve değişen ihtiyaçlar dönemine geçiş. *Karadeniz Sosyal Bilimler Dergisi*, 9(2), ss. 435-464
- Böhm, I. ve Lolagar, S. 2021. “Open Source Intelligence: Introduction, Legal, and Ethical Considerations”. *International Cybersecurity Law Review*, 2(2), 317-37. doi: 10.1365/s43439-021-00042-7.
- Clark, R. M. (2016). *Intelligence analysis: a target-centric approach*. CQ Press.
- Colquhoun, C. (2016). A Brief History of Open Source Intelligence, <https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/>
- Cooke, N. J. (2015). The Changing Context And Dynamics Of Intelligence Analysis, *The Human Factors of Intelligence Analysis* içinde, Proceedings of the Human Factors and Ergonomics Society Annual Meeting, 59 (1), ss,130-134
- John Coyne, J. (2017). The future of intelligence analysis: computers versus the human brain? *The Strategist*, <https://www.aspistrategist.org.au/future-intelligence-analysis-computers-versus-human-brain/>
- Cukier, K. ve Mayer-Schoenberger, V. (2013). The rise of big data: How it's changing the way we think about the world. *Foreign Affairs*, 92 (3), ss. 28-40
- Director of National Intelligence (2015). *Vision 2015: A globally networked and integrated intelligence enterprise*. [https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Vision\\_2015.pdf](https://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Vision_2015.pdf)
- Fingar, T. (2011). *Reducing uncertainty: Intelligence analysis and national security*. Stanford University Press.
- Gibson, Helen. 2016. “Acquisition and Preparation of Data for OSINT Investigations”, ss. 69-93 içinde *Open source intelligence investigation: From Strategy to Implementation*, editör B. Akhgar, P. S. Bayerl, ve F. Sampson. New York, NY: Springer Berlin Heidelberg

- Mark Gilchrist, M. (2017). You can't write an algorithm for uncertainty: why advanced analytics may not be the solution to the military 'big data' challenge, *The Strategist*, <https://www.aspistrategist.org.au/cant-write-algorithm-uncertainty-advanced-analytics-may-not-solution-military-big-data-challenge/>
- Gill, P. ve Phythian, M. (2018). *Intelligence in an insecure world*. Polity Press
- Glassman, M., and Kang M.J. (2012). Intelligence in the Internet Age: The Emergence and Evolution of Open Source Intelligence (OSINT).” *Computers in Human Behavior* 28(2). 673–82. <https://doi.org/10.1016/j.chb.2011.11.014>.
- Global Trends 2040: A More Contested World*, Mart 2021, National Intelligence Council  
[https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends\\_2040.pdf](https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf)
- Gül, Z. (2014). İstihbarat çeşitleri ve stratejik istihbarat. Harmancı, F.M. v.d. (Ed.). *Güvenlik Sektöründe Temel Stratejiler* içinde. (ss.83-98). Nobel Yayınları.
- Hare, N. ve Coghill, P. (2016). The future of the intelligence analysis task, *Intelligence and National Security*, 31 (6), ss. 858-870
- Hayden, M. V. (2007). Remarks of central intelligence agency director at the council on foreign relations. New York.  
<https://irp.fas.org/cia/product/dcia090707.html>
- Hedley, J.H. (2007). The challenges of intelligence analysis. Johnson, L. K. (Ed.). *Strategic Intelligence: Understanding the hidden side of government* içinde. (ss.123-138). Praeger Security International.
- Janjeva, A., Harris, A., & Byrne, J. (2022). The Future of Open Source Intelligence for UK National Security. RUSI Occasional Paper, 7  
[https://static.rusi.org/330\\_OP\\_FutureOfOpenSourceIntelligence\\_FinalWeb0.pdf](https://static.rusi.org/330_OP_FutureOfOpenSourceIntelligence_FinalWeb0.pdf)
- Johnson, L.K (2007). Introduction. Johnson, L.K. (Ed.) *Handbook of Intelligence Studies* içinde. Routledge.
- Johnson, L.K (2010). National Security Intelligence. Johnson, L.K. (Ed.) *The Oxford Handbook of National Security Intelligence* içinde. Routledge, ss.3-32

- Kahn, D. (2008). An historical theory of intelligence. Gill, P., Marrin, S. ve Phythian, M. (Ed.). *Intelligence Theory Key Questions and Debates* içinde. Routledge.
- Kent, S. (2003). *Stratejik istihbarat* (Y. Özbek ve N. Şüküroğlu, Çev.) ASAM Yayınları.
- Krizan, L. (1999). *Intelligence essentials for everyone. occasional paper #6*, Joint Military Intelligence College. <https://apps.dtic.mil/sti/pdfs/ADA476726.pdf>
- Lahneman W. J. (2016). IC data mining in the post-Snowden era, *International Journal of Intelligence and Counter Intelligence*. 29 (4), ss.700-723.
- Lowenthal, M. M. (2020). *Intelligence: From secrets to policy*. CQ Press.
- Mangır, D. Ş. ve Küçükkırlı, S. N. (2019). Gelenekselden dijitale siber istihbarat ve Rus dış politikası. *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*. Özel Sayı, ssss. 296-308
- Marrin, S. (2008). Intelligence analysis and decisionmaking, Gill, P., Marrin, S. ve Phythian, M. (Ed.). *Intelligence Theory Key Questions and Debates* içinde. Routledge.
- McConnell, J. M. (2007). Remarks and Q&A by the director of national intelligence. Project on National Security Reform Conference (July 26), Washington, DC. [https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20070726\\_speech.pdf](https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20070726_speech.pdf)
- McCue, C. (2015). *Data mining and predictive analysis: Intelligence gathering and crime analysis*. Butterworth-Heinemann.
- McGlynn, P. ve Garner, G. (2019). *Intelligence analysis fundamentals*, CRC Press
- Millî İstihbarat Teşkilâtı (2002). *İstihbaratın Tanımı ve İstihbarat Çarkı*, Erişim Tarihi: 10.11.2022. <https://www.mit.gov.tr/tarihce/giris.html>
- Mueller R. S. (2019). Report On The Investigation Into Russian Interference In The 2016 Presidential Election, <https://www.justice.gov/archives/sco/file/1373816/download>
- National Research Council (2011). *Intelligence analysis for tomorrow: Advances from the behavioral and social sciences*. National Academies Press.
- Omand, D., Miller, C ve Bartlett, J. (2014). “Towards the Discipline of Social Media Intelligence”, ss.24-43 içinde *Open Source Intelligence*

- in the Twenty-First Century New Approaches and Opportunities*, editör C. Hobbs, M. Moran, ve D. Salisbury
- Omand, D. (2017). “Social media intelligence (SOCMINT)”. R. Dover, H. Dylan, ve M. S. Goodman (Eds.) Ss. 355-71 içinde *The Palgrave handbook of security, risk and intelligence* içinde, ss. 355-71, editör. London: Palgrave Macmillan
- Omand, David., Jamie Bartlett, J. ve Miller, C. (2012). “Introducing social media intelligence (SOCMINT)”. *Intelligence and National Security*, 27 (6), ss.: 801-23. doi: 10.1080/02684527.2012.716965 ss. 24-43
- Özdağ, Ü. (2014). *İstihbarat teorisi*, Kripto Kitaplar
- Pherson, R. H. ve Heuer, R. (2015). *Structured analytic techniques for intelligence analysis*. CQ Press
- Prunckun, H. (2010). *Handbook of scientific methods of inquiry for intelligence analysis*, The Scarecrow Press.
- Schmidt, M. ve Kathleen, M. V. (2020). “Algorithms that Empower? Platformization in U.S. Intelligence Analysis,” *2020 IEEE International Symposium on Technology and Society (ISTAS)* (12-15 November 2020), doi:10.1109/ISTAS50296.2020.
- Symon, P. B., ve Tarapore, A. (2015). Defense intelligence analysis in the age of big data. *Joint Force Quarterly*, 79 (4), ss.04-11.
- U.S. Office of the Director of National Intelligence (2017). Background to “Assessing Russian Activities and Intentions in Recent U.S. Elections”: The Analytic Process and Cyber Incident Attribution [and] Assessing Russian Activities and Intentions in Recent U.S. Elections. Intelligence Community Assessment. [https://www.dni.gov/files/documents/ICA\\_2017\\_01.pdf](https://www.dni.gov/files/documents/ICA_2017_01.pdf)
- Urhal, Ö. (2008). *Kamu güvenliği açısından istihbarat ve örgütlü suçlar*. Adalet Yayınları.
- Ünver, A. (2018). *Dijital Açık Kaynaklı İstihbarat ve Uluslararası Güvenlik*, EDAM. <https://edam.org.tr/dijital-acik-kaynakli-istihbarat-ve-uluslararasi-guvenlik/>
- Walsh, P. F. (2011). *Intelligence and intelligence analysis*. Routledge
- Warner, M. (2007). Sources and methods for the study of intelligence. Johnson, L.L. (Ed.) *Handbook of Intelligence Studies* içinde, Routledge
- Weinbaum, C. ve Shanahan, J.N.T. (2018). Intelligence in a data-driven age, *Joint Force Quarterly*, 90(3), ss. 4-9

- Williams, H. J., & Blum, I. (2018). *Defining second generation open source intelligence (OSINT) for the defense enterprise*. Rand Corporation.
- Xu Wu, Daguo Qin, Yang Li (2022) Challenges and Inspirations of AI and Related Technologies in Intelligence Analysis, *IEEE ITAIC*, ss. 451-455
- Yılmaz, S. (2015). *İstihbarat bilimi*. Kripto Kitaplar.

## SİNYAL İSTİHBARATI ANALİZİ BAĞLAMINDA BİR DEĞERLENDİRME: RUBICON OPERASYONU VE TÜRKİYE

Semih SEVİNÇ\*

Sinyal istihbaratı (SİNİS), hedef ülkenin sahip olduğu elektronik harp araçlarının yaydığı elektromanyetik dalga ve frekansların toplanması, değerlendirilmesi ve yorumlanmasıdır. Bu sebeple SİNİS, bir devletin başta politik ve askeri amaçları olmak üzere, iletişim güvenliğini de sağlamak için yerine getirdiği faaliyetleri ifade etmektedir.

Bu makalenin temel amacı, istihbarat toplama teknikleri içinde önemli bir konuma sahip olan SİNİS'in aynı zamanda istihbarata karşı koyma (İKK) boyutu olan iletişim güvenliği konusu ile ele alınması gerekliliğine vurgu yapmaktır. Bu kapsamda önemli istihbarat operasyonlarından biri olan Rubicon Operasyonu'nun hedef ülkelerden biri olan Türkiye üzerindeki etkileri analiz edilmiştir.

Çalışmada analiz yöntemi olarak yapılandırılmış analiz teknikleri arasında bulunan "Anahtar Varsayımların Kontrolü" yöntemi kullanılmıştır. Analize ilişkin varılan sonuçlarla ilgili olarak ise, başta Türkiye olmak üzere diğer hedef ülkelerin karşılaşmaları muhtemel tehditlere karşı ne yapabileceklerine dair değerlendirme ve öneriler sunulmuştur.

**Anahtar Kelimeler:** *İstihbarat, İstihbarat Analizi, Sinyal İstihbaratı, Rubicon Operasyonu, İletişim Güvenliği.*

## AN ASSESSMENT IN THE CONTEXT OF SIGNAL INTELLIGENCE ANALYSIS: OPERATION RUBICON AND TURKEY

### ABSTRACT

Signal intelligence (SIGINT) is the collection, evaluation and interpretation of electromagnetic waves and frequencies emitted by electronic warfare tools owned by the target country. For this reason, SIGINT refers to the activities that a state carries out to realize its basic goals, especially its political and military purposes, and to provide the communication security it needs.

The main purpose of this article is to emphasize the necessity of dealing with SIGINT, which has an important position in intelligence gathering techniques, with the issue of communication security, which is also the dimension of counterintelligence (CI). In this context, the effects of Operation Rubicon, one of the important intelligence operations, in Turkey, one of the target countries, were analyzed.

In this study, the "Key Assumptions Check" method, which has an important place among the structured analysis techniques, was used as an analysis method. Regarding the results of the analysis, evaluations and suggestions were made about what other target countries, especially Turkey, can do against possible threats.

**Keywords:** *Intelligence, Intelligence Analysis, Signal Intelligence, Operation Rubicon, Communication Security.*

---

\* Öğt. Üyesi, Jandarma ve Sahil Güvenlik Akademisi, Güvenlik Araştırmaları Merkezi Müdürlüğü, semihsev2001@gmail.com, ORCID: 0000-0002-1043-5628  
Makale Başvuru Tarihi / Application Date: 29 Aralık 2022 / 29 December 2022  
Makale Kabul Tarihi / Acceptance Date: 16 Ocak 2023 / 16 January 2023

## GİRİŞ

Teknolojinin günlük hayattaki yerinin fazlaşmasıyla beraber, istihbarat alanında sıkça kullanılan olan SİNİS'in de önemi artmıştır. Teknolojik gelişmeler adeta devam eden bir sörf dalgasına benzemesi bakımından süreklilik arz etmektedir. Bu sebeple gelişmeler, ülkeler açısından sürekli izlenmeli ve takip edilmelidir. SİNİS teknolojiyi elinde bulduran ve geliştiren ülkeler için bir istihbarat toplama yöntemi olarak kullanılırken, teknolojiyi satın alan ve kullanan ülkeler için ise İKK faaliyetleri kapsamında değerlendirilmelidir.

2000'li yıllardan itibaren Wikileaks belgelerinin ifşası ile başlayan kişisel mahremiyetin çiğnenmesine ilişkin tartışmalar, 2013 yılı itibariyle Snowden sızıntıları ve 2020 yılında Rubicon Operasyonu'na dair yazılı ve görsel basında yer alan haber ve yayınlarla devam etmiştir. Özellikle 2000'li yıllar sonrası her bireyin edinme şansına sahip olduğu internete bağlı tablet, akıllı telefon ve bilgisayar gibi cihazların (*internet of things*) yaygın olarak kullanılması ve bu cihazlar vasıtasıyla dinleme, izleme ve konum takibi yapılabilmesi gibi gelişmeler bahse konu tartışmaların tırmanmasına sebep olmuştur.

Rubicon Operasyonu, dünyanın her yerinde büyük ilgi ve merak ile takip edilen Edward Snowden'in ifşaatlarının öncüsü olarak görülmektedir. Rubicon Operasyonu'nun başladığı 1950'li yıllarda henüz internet ve akıllı sistemler var olmadığından iletişim kriptografik cihazlar ile sağlanmıştır. Bu dönemde ihtiyaç duyulan cihazların üretimini sağlayan kurum ve ülkeler, diğer devletlere yaptıkları ihracatlar sayesinde hem maddi kazanç elde etmiş hem de kıymetli bilgiler elde etmişlerdir.

Günümüzde yaşanan teknolojik gelişmelere paralel olarak, yukarıda anlatılan durumun devam ettiği söylenebilir. Ülkeler arasında süregelen teknoloji mücadelesi sonucu az gelişmiş devletler maddi kayıpların yanında mahrem bilgilerinin de kaybetmektedirler. Bu sebeple ülkeler arasında devam eden teknolojik savaş aynı zamanda istihbarat toplama yarışına dönüşmüştür.

İstihbarat toplama yöntemi olarak kullanılan en önemli iki unsur İnsan İstihbaratı (İNİS) ve SİNİS'tir. Yukarıda bahsedilen hususlar kapsamında, teknolojik gelişmelerin SİNİS'in de önemini artırdığı söylenebilir. İstihbarat toplama kapsamında teknolojik araç ve gereçler önemli bir yer edinmiş ise de elde edilen bilgileri analiz edecek ve onu kullanacak olan insandır. Bu

bağlamda, insan unsuruna dayalı istihbaratın her dönemde devam edeceği söylenebilir.

Rubicon Operasyonu'nun bu makalenin konusu olarak seçilmesinin sebebi SİNİS'i ilgilendiren gelişmelerin önemine vurgu yapmaktır. Ülkeler arasında devam eden diplomatik, ekonomik, askeri ve siber gelişmeler iki taraflı düşünüldüğünde güçlü tarafın teknolojiyi üretici, zayıf tarafın ise teknolojiyi kullanıcı (tüketen) konumunda olduğu görülmektedir. Bu kapsamda Türkiye geliştirmekte olan bir ülke olarak başta askeri alan olmak üzere her alanda kullandığı cihazlara (uçak, telsiz, akıllı telefon gibi) dikkat etmeli ve gizli bilgilerini korumak maksadıyla İKK prensiplerini eksiksiz bir şekilde uygulamalıdır.

Bu çalışmanın araştırma soruları şunlardır: “Sinyal istihbaratı nedir?”, “Sinyal istihbaratının devletlerin güvenliği açısından önemi nedir?”, “İstihbarat analizi nedir?”, “Yapılandırılmış analiz teknikleri nelerdir ve nasıl kullanılır?”, “Rubicon Operasyonu nedir?”.

Çalışmanın temel araştırma sorusu ise şu şekilde belirlenmiştir: “Rubicon Operasyonu, Türkiye’ye etkisi bakımından nasıl değerlendirilmelidir?”. Belirlenen temel araştırma sorusunu yanıtlamak için yöntem olarak temel varsayımların kontrolü tekniği uygulanacaktır.

Yapılandırılmış analiz teknikleri (Structured Analytic Techniques), istihbarat ürününün verimini artırmak için kullanılan analiz yöntemlerine verilen isimdir. Analizcinin toplanan veriler etrafında bir istihbarat sorusu oluşturması ve bu soruya cevap bulmak adına plan geliştirmesi gerekmektedir. Anlamlı ve doğru bir analiz için her bir veri tek tek ve bir bütün olarak incelenmelidir. “İstihbarat değerlendirmesi nasıl yapılmalı?” sorusu çerçevesinde yapılan çalışmalar, yapılandırılmış analiz tekniklerinin kullanılması gerekliliğini ortaya çıkarmıştır.

İstihbarata ilişkin çalışmaları ile bilinen Sherman Kent analiz tekniklerinin ortaya çıkarılmasına öncülük etmiştir. Kent, analize dahil edilecek bilgiler elde edildikten sonra iki temel husustan bahsetmiştir (Borek, 2019, s.807): eleştirel değerlendirme ve içsel anlamlandırma. Bu bağlamda, analizin ayrılmaz parçaları olarak bilginin anlamlandırılması ve değerlendirilmesi gösterilebilir.

Yapılandırılmış analiz teknikleri yanılğı, sınırlama ve tuzakların analizdeki olumsuz etkisini en aza indirmek için kullanılmaktadır. Ayrıca



etkili bir şekilde iş birliği yapılmasını da sağlayan bu teknikler kaynaklarda farklı şekillerde sınıflandırılmaktadırlar. Yapılandırılmış analiz tekniklerini genel anlamda şu şekilde tasnif etmek mümkündür: tanımlayıcı teknikler (sebeup ve etki değerdendirilmesi), zıt teknikler, örüntü tanıma teknikleri, yaratıcı düşünme teknikleri ve test teknikleri.

Bu çalışmada Rubicon Operasyonu, tanımlayıcı teknikler arasında yer alan temel varsayımların kontrolü ile incelenmiştir. Tanımlayıcı teknikler, analitik varsayım veya bilinmezleri tanımlayarak daha şeffaf hale getirmeye imkân tanır. Aynı zamanda analize ilişkin yargıların temelini yeniden değerdendirilmesini sağlar.

Tanımlayıcı teknikler uygulanırken ortaya çıkarılan geçmişı açıklama ve geleceđi tahmin etme çalışmaları sebeup ve etki (neden ve sonuç) ilişkisine dayanmaktadır. Analizci için bu tür çalışmaların zor olmasının sebebi, üzerinde durulan değışken türleri arasındaki ilişkilerin teori geliştirmeye uygun olmamasıdır. Bu sebeuple analizcinin bilinçli bir yargı ortaya koyması, konusundaki uzmanlığa ve akıl yürütme becerisine bađlıdır.

Sebeup ve etki değerdendirilmesi olarak da bilinen tanımlayıcı teknikler arasında bulunan başlıca analiz teknikleri şunlardır (Heuer ve Pherson, 2011, ss.143-144): yapılandırılmış analogi, kırmızı başlık analizi, rol oynama, dıştan içe düşünme, politik sonuç tahmini ve temel varsayımların kontrolü. Bu teknikler arasında analizcilerce önemli olarak görülen ve en dođru sonuçları verdiđine inanılan teknik temel varsayımların kontrolüdür.

Temel ya da anahtar varsayımların kontrolü yapılırken, temel yargılarda yer alan kritik noktalar kontrol edilir ve incelenir. Bu teknikteki başlıca gereklilikleri şu şekilde sıralamak mümkündür (U.S., 2009, s.7): argümanın ardındaki nedenin tanımlanması ve hatalı çıkarımların ortaya çıkarılması, gelişmeye sebeup olan kritik faktörlerin açıklanması, araştırma sorusuna yönelik olarak geniş çaplı düşünülmesi, ana faktörler arasındaki bađlantıların ortaya çıkarılması, belirli bir varsayımdan vazgeçmeye neden olan etmenlerin tanımlanması, değışen şartlar veya beklenmedik durumlara yönelik olarak düşünce tarzının geliştirilmesi.

Analizci temel varsayımların kontrolünde şu adımları takip etmelidir (Garner ve McGlynn, 2019, s.156): Temel analitik çizgiye yönelik varsayımlar tanımlanır. Olaydaki temel dinamikler daha iyi anlaşılacak şekilde açıklanır. Yeni ve farklı düşünceler oluşturularak bakış açısı kazanılır. Anahtar faktörler arasındaki görünmeyen bađlantılar keşfedilir. Bir

yargının altında yatan varsayımların anlaşılmasının analize dair güveni artıracığı ve yeni bilgilerin eski varsayımları geçersiz kılabileceği unutulmamalıdır.

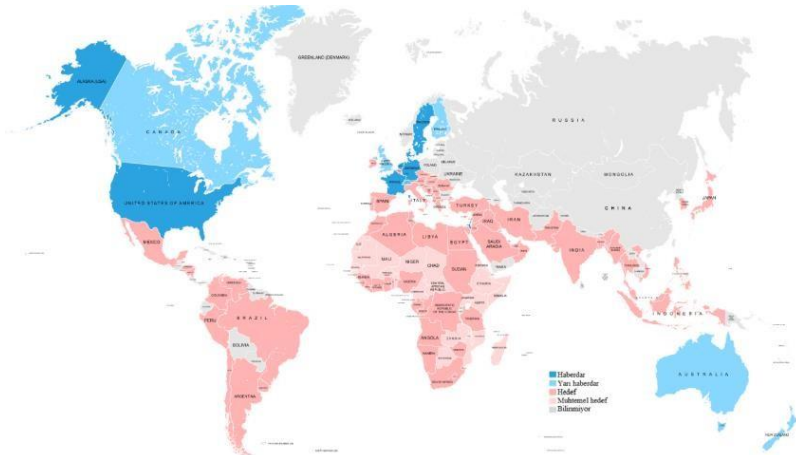
## 1. RUBICON OPERASYONU

Rubicon Operasyonu, 1970'den 1994'e kadar Amerikan Merkezi İstihbarat Teşkilatı (*Central Intelligence Agency, CIA*) ile Almanya Federal Haberalma Servisinin (*Bundesnachrichtendienst, BND*) iş birliğinde 130'dan fazla ülkenin politik yazışma, görüşme ve iletişimlerini takip etme faaliyetlerini kapsamaktadır (Dobson, 2020, ss.608-622). Bu operasyon, Crypto isimli firmaya ait şifreleme cihazlarının üretimi ve hedef ülkelere ihracatı ile gerçekleşmiştir ve temeli SİNİS'e dayanmaktadır.

Rubicon Operasyonu, başlangıçta şifre oluşturma ve şifre kırma gibi teknik yöntemlerin kullanılmasına dayalı olarak İKK amacıyla başlatılsa da devam eden süreçte bu kapsamda sınırlı tutulmayarak, istihbaratın toplanması ve analiz edilmesi süreci ile dünya çapında büyük çaplı bir operasyona dönüşmüştür. Türkiye'nin de hedef ülkeler arasında bulunduğu bu operasyon, tarihteki en sansasyonel istihbarat operasyonları arasında yer almaktadır.

Rubicon Operasyonu'nun amaçladığı (2) ana hedefi; üretilen şifreleme cihazlarının küresel boyutta satışını artırmak ve gözetim dışında kalan coğrafi bölgelerdeki makinelerin kontrolsüz bir şekilde üretim ve ihracatını engellemek olarak gösterilebilir. CIA ve BND'nin 1980 yılı itibariyle hedefindeki devletler aşağıdaki haritada belirtilmiştir.

Şekil-1. Rubicon Operasyonu Kapsamındaki Hedef Ülkeler (Miller, 2020)



Birçok ülkeye cihaz satışı yapılan İsviçre merkezli Crypto isimli şirket, 1950 yılında Boris Hagelin tarafından kurulmuş ve günümüze kadar çeşitli isimlerle (AB Cryptograph, Ingeniörsfirman Teknik, Cryptoteknik, Crypto International AG, CyOne Security AG) faaliyetlerine devam etmiştir. Şirketin kurucusu Hagelin ile ABD Ulusal Güvenlik Ajansı (National Security Agency, NSA)'da baş kriptoloji uzmanı olarak çalışan William Friedman arasında çeşitli anlaşmalar (Centilmen, Lisans ve Thesaurus Anlaşmaları) yapıldığına dair belgeler basında yer almıştır (Shane ve Bowman, 1995). Kısa bir ifadeyle Rubicon Operasyonu kapsamında, Crypto şirketinin CIA ve BND tarafından satın alınarak uzun yıllar boyunca istihbarat servislerine hizmet ettiği söylenebilir.

Rubicon Operasyonu'nun ortaya çıkmasına sebep olan Bühler Vakası (1992) sürecin dönüm noktası olarak gösterilmektedir. Crypto şirketinin satış temsilcisi ve yöneticilerinden olan Hans Bühler İran ve Suudi Arabistan gibi Orta Doğu ülkelerine sıkça ziyaretlerde bulunmuştur. 1992 yılındaki İran seyahatinde ise, Amerika Birleşik Devletleri (ABD) ve Almanya adına casusluk yapmakla suçlanmış ve yakalanmıştır (Aldrich vd., 2020, s.3). Halbuki Bühler de dahil olmak üzere, bahse konu dönemde şirket adına çalışan yetkililerin casuslukla ilgileri bulunmamaktadır.

Bühler'in yakalanmasından sonra, İranlı yetkililer CIA ve BND ile gizli bir şekilde anlaşma sağlama çalışmalarına başlamışlardır. Çalışmalar sonucunda taraflar uzlaşmaya varmış ve 1993 yılında İran' a verilen 1 milyon dolar karşılığında Bühler serbest kalmıştır (Strehle, 1994). Bühler Vakası etik tartışmaları da ortaya çıkarmış ve devam eden operasyonda BND'nin CIA' i yalnız bırakmasında etkili bir etken olarak görülmüştür.

## **2. TÜRKİYE'NİN RUBICON OPERASYONUNDAKİ YERİ**

Türkiye, ilk olarak 16 Ağustos 1950'de Crypto şirketinin ürettiği M-209 makinelerinin satın alınması için talepte bulunmuştur. Bu istek ABD tarafından reddedilse de Türkiye'nin kullanması için başka bir şifreleme cihazı olan CSP-845 teklif edilmiştir (Larner, 1953, s.3). M-209' un reddedilme sebebi olarak, makinelerin tedarik ve imalatının kısıtlı olması gösterilmiştir.

Friedman'ın Hagelin'i ziyareti sonrası 21 Şubat 1955' te oluşturulan raporda ise, Yunanistan'ın ve Türkiye'nin makinelerle ilgilenmesi sebebiyle evrakların ülkelere gönderildiği fakat alışverişin henüz gerçekleşmediği,

ilerleyen günlerde ziyaretin gerçekleştirileceğinin planlandığından bahsedilmektedir (Friedman, 1955, ss.6-10).

Rubicon Operasyonu'nun 1950-2000 yılları arasında sürdürüldüğü düşünüldüğünde, Türkiye'nin bu dönemde karşı karşıya kaldığı önemli olaylar şu şekilde sıralamak mümkündür:

- 25 Haziran 1950: Türkiye'nin BM adına Kore Savaşı'na katılması,
- 18 Şubat 1952: Türkiye'nin NATO'ya katılması,
- 27 Mayıs 1960: Askeri darbenin gerçekleşerek hükümetin değişmesi,
- 20 Mayıs 1963: Ayaklanma ve darbe teşebbüsünün bastırılması,
- 20 Aralık 1963: Kanlı Noel olarak bilinen ve Kıbrıs Türklerine karşı yapılan katliamlar
- 5 Haziran 1964: Türkiye'nin Kıbrıs'a müdahalesini önlemek amacıyla ABD tarafından gönderilen Johnson Mektubu,
- 20 Mayıs 1969: Ordu üst kademesi ve siyasiler arasında yaşanan kriz,
- 12 Mart 1971: 32. Türkiye Cumhuriyeti Devleti Hükümeti'nin istifaya zorlanması,
- 20 Temmuz 1974: Birinci Kıbrıs Harekâtı,
- 18 Ağustos 1974: İkinci Kıbrıs Harekâtı,
- 12 Eylül 1980: Askeri darbenin gerçekleşmesi ve hükümetin değişmesi,
- 25 Aralık 1995: Türkiye ve Yunanistan arasında meydana gelen Kardak Krizi,
- 28 Şubat 1997: Post modern darbe adıyla bilinen muhtıra ile karşılaşılması.

Crypto şirketi tarafından Türkiye'ye yapılan satışlara ilişkin ulaşılan belgeler genellikle 1950'li yıllara aittir ve üretilen cihazların dünya çapındaki satışlarında en yüksek artış 1970 ile 1975 yılları arasında meydana gelmiştir. Bahse konu süreçte Türkiye'yi ilgilendiren en önemli olay olarak

1974 Kıbrıs Harekatı'nın incelenmesinin uygun olacağı değerlendirildiğinden CIA'in 1960'lı yıllarda Kıbrıs konusuna ilişkin oluşturduğu istihbarat raporları analiz edilmiştir.

“Kıbrıs Durum Raporu” isimli CIA raporunda, Türk ve Rum vatandaşları arasında düşünce ayrılıkları olduğu ve Kıbrıs Türklerinin haksız durumlarla karşılaştıkları belirtilmiştir (CIA, 1966). Ayrıca yakın zamanda çözümün beklenmediği ve Türklerin devam eden Rum provokasyonlarına karşı direniş gösterdiklerinden bahsedilmiştir. “Kıbrıs Çatışması ve ABD'nin Güvenlik İsteği” adlı diğer bir raporda ise Birleşik Krallık, Türkiye ve Yunanistan'ın Zürih ve Londra Antlaşmaları ile Kıbrıs adasının bağımsızlığı konusunda mutabık kalarak devlet statüsünü elde ettiği, BM Barış Gücünün 6.000'i aşkın personel ile adaya müdahale etmesine rağmen adadaki çatışmaların devam ettiğinden bahsedilmiştir (RAND, 1967).

“Yeni Bir Kriz: Kıbrıs” isimli raporda, Sovyetler Birliği'nin Türklere yapılan haksızlıklar sebebiyle Ankara ile iletişimi sıklaştırarak Yunanistan'ın Enosis fikrine karşı olduğu şeklinde değerlendirmeler yapılmıştır (CIA, 1971). “Eski Bir Problem: Kıbrıs” adlı bir diğer raporda ise, mevcut problem Türkiye, ABD, Yunanistan, Sovyetler Birliği gibi devletlerin yanında BM ve NATO gibi uluslararası örgütler açısından değerlendirilerek çeşitli senaryolara yer verilmiştir (CIA, 1973).

ABD Dışişleri Bakanlığınca Sinyal Güvenlik Servisine gönderilen “Madrid ve İstanbul'daki Şifreleme Makineleri” konulu mektupta dört adet şifreleme cihazının ihracatı için görüş istenildiği görülmektedir (NSA, 1944). Ayrıca “Kriptografik Cihazların Türkiye'ye Bırakılması” isimli belgede, Türkiye Dışişleri Bakanlığının talebine cevap vermek amacıyla cihaz özelliklerinin değerlendirilmesinden ve ihracatın gerçekleşmesi için somut adımlar atılmasından bahsedilmiştir (CNO, 1952).

William Friedman tarafından NSA'ya gönderilen “Kriptografik Cihazın Türkiye'ye Bırakılması (1952)” konulu Müşterek Operasyonlar Başkanlığı mektubunda, Türkiye'nin Aroflex cihazının gelişmiş bir çeşidi olarak Philips tarafından üretilen Araboflex ve Beroflex isimli cihazları kullandığı anlaşılmaktadır (Friedman, 1952). Ayrıca Birleşik Şifre Makinelerinin (Combined Cipher Machines) Türkiye'ye satış yapılması konusunda tavsiyede bulunmuştur.

“Türk Hükümetine Kriptografik Yardım” konulu belgede, Türkiye'ye satılması planlanan 34 adet cihazın 15'inin hazır olduğu, kalanların ise

ilerleyen günlerde temin edileceğinden bahsedilmiştir (USCIB, 1957). Ayrıca ödeme konusunda kolaylık sağlanacağı ifade edilmiştir. “Türkiye ve Portekiz’e sağlanacak Kriptografik Eğitimler” konulu belgede, makinelerin güvenli kullanımını sağlamak amacıyla uzman personel görevlendirilerek eğitim verilmesi talebi değerlendirilmiştir (Hartstall, 1952).

“Müttefik İletişim Güvenliği” konulu belgede Türkiye’nin iletişim güvenliği konusundaki eksikliklerin farkında olduğu ve diplomatik yazışma dokunulmazlığını garanti edecek şifreleme makinelerine sahip olma çalışmalarından bahsedilmiştir (NSA, 1953a). “Birleşik Şifreleme Makinelerinin (CCM) Türk Hükümetine Verilmesi” adlı belgede, Türkiye tarafından 50 adet cihazın satın alındığından ve ABD ile İngiltere arasında iş birliği ve SİNİS paylaşımı yapılmasından bahsedilmiştir (USCIB, 1953). Bu durum Brusa, Ukusa, Echelon ve Prisma benzeri projeleri anımsatmaktadır.

Diğer bir taraftan NSA’nın sinyal istihbaratına ilişkin olarak yayınladığı “NATO İletişim Güvenliği” isimli belgede, müttefik devletlerin kullandığı cihazların diğer devletlere karşı korunması gerektiğinden ve iletişim güvenliğinin sağlanabilmesi için yapılması gerekenlerden bahsedilmiştir. NSA’nın Yunanistan ve Türkiye’ye dair durumla ilgili olarak Friedman’dan bilgi talep ettiği mektup ile “NATO Ülkeleri Türkiye, Fransa, Portekiz, Yunanistan ve İtalya’ya Sağlanan Kripto Sistemler Hakkında Bilgi Talebi” konulu Friedman’a gönderdiği mektuplarda Türkiye’nin şifreleme cihazlarına sahip olduğu ve diplomatik iletişimde kullandığı anlaşılmaktadır (NSA, 1953b).

1950’li yıllarda başlayan ve İspanya, Fransa, Portekiz, Brezilya, Arjantin, Mısır, Endonezya, Lübnan, Hindistan, Japonya gibi Dünyanın farklı kıtalarındaki birçok ülkeyi de kapsayan bir şekilde 2000’li yıllara kadar devam eden Rubicon Operasyonu kapsamında, çeşitli ülkelerde meydana gelen olaylar, çatışmalar ve insan hakları ihlallerine göz yumulduğuna dair çeşitli makale ve haberler yayınlanmıştır. Benzer şekilde, Kıbrıs’ta adeta kangren haline gelen çözümsüz durumun ve 1960 yılından itibaren Türklerin maruz kaldığı zulüm ve katliamların, güç sahibi ülkelere izlenerek herhangi bir müdahalede bulunulmadığı ve aksine bu çatışmaların tetiklenmiş olabileceği değerlendirilmektedir.

## **SONUÇ: SİNYAL İSTİHBARATI BAĞLAMINDA DEĞERLENDİRME**

Devletlerin ortaya çıktığı ilk zamanlardan bu yana ihtiyaç duyulan bilgilerin elde edilmesi amacıyla çeşitli istihbarat toplama yöntemleri kullanılmaktadır. Bu yöntemlerden en maliyetli fakat verimli olanı teknolojiye (elektromanyetik dalgalar, iletişim ve sinyaller) dayalı olan istihbarat toplama yöntemidir.

Genel bir ifadeyle sinyal, üzerine kodlanan bilgiyi taşıyarak bir yerden başka bir yere ulaştırılmasını sağlayan, anlamlandırarak yayılmasını sağlayan kavramlar olarak adlandırılmaktadır. Bu alanda 19. yüzyılda ortaya çıkan ilk yenilik telefon ve telgrafın bulunması olmuştur. Devamında ise, internet ve diğer elektronik cihazların ortaya çıkışının sinyal ve iletişim alanında büyük bir devrim yarattığı söylenebilir. SİNİS, düşman unsurların kullandığı elektronik haberleşme cihazları tarafından üretilen sinyallerin teknik yöntemlerle elde edilerek işlenmesi, analiz edilmesi ve faydalı bilgiye dönüştürülerek kullanılmasıdır. SİNİS'in iki temel alt dalı olarak, elektronik istihbarat (ELİS) ve iletişim istihbaratı (İLİS) gösterilmektedir.

Genel olarak ELİS, sinyallerin alıcılar vasıtasıyla toplanarak frekans analizinin yapılması ve karşıdaki unsurun düşman veya tehdit olarak algılanması neticesinde radar, atış, füze ve gözetleme gibi erken uyarı ve sinyal bozucu sistemler ile bertaraf edilmesidir. İLİS için ise esas olan, yakalanan sinyallerin analiz edilerek iletişimin dinlenmesi ve hedefe ait amaç, plan, konum gibi unsurların açığa çıkarılarak tespit edilmesi ve kullanılması ile ilgilidir.

SİNİS toplama faaliyetleri diğer istihbarat toplama yöntemlere göre daha pahalı olmakla birlikte, gelişmiş teknoloji ve yetişmiş personel gerektirmektedir. Dünyanın en gelişmiş SİNİS teşkilatı olan NSA'nın 35.000 çalışanı bulunmaktadır. ABD ve Almanya iş birliği ile üretilen ve 130'dan fazla ülkeye ihraç edilen şifreleme makineleri sayesinde, hedef devletlerin tüm diplomatik iletişimlerinin dinlendiği ve yazışmalarının takip edildiğine dair tartışmalar devam etmektedir.

Türkiye'nin de 2000'li yıllara kadar takip edildiği / dinlendiği değerlendirilen Rubicon Operasyonu, SİNİS bakımından Dünya'daki en önemli istihbarat operasyonu olarak bilinmektedir. Yapılan araştırmalar sonucunda NSA'nın dünyanın farklı bölgelerinde gerçekleşmiş olaylarla ilgili olarak önceden bilgi sahibi olduğu tespit edilmiştir. Örneğin; 1982

Falklands Savaşı (Arjantin ve İngiltere) ve 1954-1975 Condor Operasyonları (Şili, Bolivya, Paraguay, Uruguay ve Brezilya) bahse konu kriptografik cihazlar ile takip edilmiştir.

2.Dünya Savaşı sonrasında, 1950'lerden itibaren başlayan ve 2000'li yıllara uzanan Crypto ihracatları düşünüldüğünde, bu durumun dünya üzerinde gerçekleşmiş birçok olaya dair (savaş, seçim, çatışma, ayaklanma, darbe, iş birliği, askeri operasyon ve ticaret anlaşmaları gibi) SİNİS kullanılarak bilgi sahibi olunduğu ve bu olayların gidişatının izlenerek müdahalede bulunduğu düşünülebilir.

Üretici ülkenin kendi inisiyatifine göre oluşturduğu algoritmalar ile çalışan şifreleme cihazlarının istihbarat servislerince adeta birer çifte ajan gibi kullanıldığını söylemek yanlış olmayacaktır. Bu minvalde, makalenin konusu çerçevesinde yayınlanan istihbarat raporları incelenerek, Rubicon Operasyonu'nun Kıbrıs Harekatı'na kamuoyu tarafından görülmesi mümkün olmayan herhangi bir arka plan etkisinin olup olmadığına dair beyin fırtınası yürütülmüştür.

Temel varsayımların kontrolü yöntemi uygulanarak yapılan analiz sonucunda NSA'nın Kıbrıs meselesi sürecinde Türkiye'nin hareket tarzı ve stratejik hamlelerine ilişkin bilgilere harekât gerçekleşmeden önce ya da harekât esnasında şifreleme cihazlarının desteğiyle sahip olabileceğine ilişkin temel bir varsayıma ulaşılmıştır. Bu varsayımı, rapor ve belgelerde görülen 34 adet ve sonrasında 50 adet cihazın Türkiye tarafından kullanılması, adadaki durumun ABD tarafından yakından takip edilmesi, sürece ilişkin oluşturulan senaryo ve faraziyeler, Johnson Mektubu ve harekât sonrasında Türkiye'ye uygulanan çeşitli ambargolar gibi etmenler desteklemektedir.

Rubicon Operasyonu'na benzer şekilde günümüzde gerçekleşebilecek SİNİS faaliyetlerine karşı İKK tedbirlerinin tam olarak uygulanabilmesi gerekmektedir. Bu kapsamda, kritik duruma sahip kurumların personeli tarafından kullanılan akıllı telefonların konumlarının izlenebileceği, görüşmelerin dinlenebileceği, mikrofon, ekran ve kamerasına ulaşılabilceği unutulmamalıdır. Ayrıca kritik tesislerde akıllı telefon bulundurulmaması, sosyal medya kullanımına özen gösterilmesi, az ve güvenilir uygulama veya uygulamaların kullanılması, olası sızma ve siber saldırılara dikkat edilerek gizlilik ilkesine özen gösterilmesi esastır.



Bahsedilen hususların yanında, yerli ve milli cihaz ve yazılımların kullanılması önem arz etmektedir. Son dönemde Türkiye’de güvenlik ve savunma alanlarındaki ilerlemeler SİNİS faaliyetlerinin geliştirilmesini de beraberinde getirmiştir. Türkiye Bilimsel ve Teknolojik Araştırma Kurumu (TÜBİTAK) ve Bayraktar Kardeşler Teknoloji (BAYKAR), Hava Elektronik Sanayii (HAVELSAN), Askeri Elektronik Sanayi (ASELSAN), Türkiye Havacılık ve Uzay Sanayi (TUSAS) ve Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (SSB) gibi kurumların üretmiş oldukları istihbarat, keşif, gözetleme, radar ve elektronik harp araçları hava/kara/denizde yapılan tespit, teşhis, yön bulma, aldatma ve çoklu hedef karıştırma gibi SİNİS faaliyetlerini gerçekleştirebilmektedir.

Tüm bu gelişmeler başta Türk Silahlı Kuvvetleri (TSK) olmak üzere diğer kurumların imkân ve kabiliyetlerine katkı sunarak Türkiye’nin bölgesel çaptaki rekabet gücünü artırmaktadır. Türkiye stratejik anlamda önemli bir konuma sahip olması sebebiyle, savunma ve güvenlik alanındaki kazanımlarını paydaş kurumların iş birliği ve koordinasyonu ile artırarak sürdürmelidir.

## **KAYNAKÇA**

- Aldrich, R.J., Müller, P.F., Ridd, D. ve Schmidt-Eenboom, E. (2020). Operation rubicon: sixty years of german-american success in signals intelligence. *Intelligence and National Security*, 35(5), 603-607. <https://doi.org/10.1080/02684527.2020.1774849>.
- CIA. (1966). Cyprus: a status report. Güncel haftalık özel istihbarat raporu. Erişim tarihi: 10 Mart 2021. Yayınlanma tarihi: 08/02/2008.
- CIA. (1971). Cyprus: a new crisis in the making? Office of national estimates. Erişim tarihi: 10 Mart 2021. Yayınlanma tarihi: 10/03/2006.
- CIA. (1973). Cyprus: an old problem. İstihbarat raporu. Erişim tarihi: 10 Mart 2021.
- Yayınlanma tarihi: 25/05/2006.
- CNO. (1952). EK3 Kriptografik cihazın Türkiye’ye bırakılmasına dair yazı (Mayıs 1952).
- Erişim tarihi: 10.09.2021. Belge Nu: A68124.
- Dobson, M.J. (2020). Operation rubicon: germany as an intelligence ‘great power’? *Intelligence and National Security*, 35(5), ss.608-622. <https://doi.org/10.1080/02684527.2020.1774852>.

- Friedman, W.F. (1955). CAG ziyareti raporu (hagelin), william f. friedman tarafından. Erişim tarihi: 12.12.2021. Belge Nu: A60616.
- Friedman, W.F. (1952). Şifreleme makinelerinin Türkiye'ye bırakılması konulu yazı (Temmuz 1952). Erişim tarihi: 11.11.2021. Belge Nu: A68108.
- Garner, G. ve McGlynn, P. (2019). Intelligence analysis fundamentals. CRC Press.
- Hartstall, P.K. (1952). Türkiye ve Portekiz'e sağlanacak kriptografik eğitim yazısı (Aralık 1952). Erişim tarihi: 20.01.2022 Belge Nu: A66948.
- Heuer, R. ve Pherson, R.H. (2011). Structured analytic techniques for intelligence analysis.
- Washington D.C.
- Larner, T.M. (1953). Converters, m209 memorandum for director, national security agency. 15 December 1953. A66618. Declassified by NSA on 11 June 2014 (EO 13526)
- Miller, G. (2020). The intelligence coup of the century. Erişim tarihi: 20.05.2021.  
<https://www.washingtonpost.com/graphics/2020/world/national-security/cia-cryptography-machines-espionage/>.
- NSA. (1944). EK1 Madrid ve İstanbul'daki şifreleme makineleri konulu yazı (Şubat 1944). Erişim tarihi: 01.02.2022. Belge Nu: A67272.
- NSA. (1953a). EK7 Müttefiklerin iletişim güvenliği konulu yazı (Şubat 1953). Erişim tarihi: 11.11.2021. Belge Nu: A66942.
- NSA. (1953b). NATO iletişim güvenliği. Erişim tarihi: 15.12.2021. Belge Nu: A517801.
- RAND. (1967). The cyprus conflict and u.s. security interest. Yayınlanma tarihi: 19.09.2012.
- Erişim tarihi: 21.02.2022. Dankwart A.Rustow.
- Shane, S. ve Bowman, T. (1995). Rigging the game spy sting: few at the swiss factory knew the mysterious visitors were pulling off a stunning intelligence coup -- perhaps the most audacious in the National Security Agency's long war on foreign codes; no such agency. Baltimore Sun. Yayınlanma tarihi: 15.12.1995. Erişim tarihi: 21.03.2021. <https://www.baltimoresun.com/news/bs-xpm-1995-12-10-1995344001-story.html>.

- Strehle, R. (2020). Bir Teknisyenin Trajedisi. Yayınlanma tarihi: 13.02.2020. Erişim tarihi: 21.03.2021. <https://www.tagesanzeiger.ch/schweiz/standard/die-tragoedieeinestechnikern/story/24215009>.
- U.S. (2009). A tradecraft primer: structured analytic techniques for improving intelligence analysis. American Psychological Association. <https://doi.org/10.1037/e587102011-001>.
- USCIB. (1953). EK8 Türk hükümetine şifreleme makineleri verilmesine dair yazı (Şubat 1953). Erişim tarihi: 12.12.2021. Belge Nu: A60920.
- USCIB. (1957). Türk hükümetine kriptografik yardım konulu yazı (Ekim 1952). Erişim tarihi: 15.12.2021. Belge Nu: A517086.

## PSİKOLOJİK HAREKÂT İSTİHBARATINDA BİR ANALİZ YÖNTEMİ: HEDEF KİTLE ANALİZİ

Ediz EKİNCİ\*

### ÖZET

Psikolojik harekât, hedef olarak seçilen birey, grup veya topluluğun duygu, düşünce, tutum ve davranışlarını değiştirmek amacıyla icra edilen faaliyetlerdir. Psikolojik harekâtın temeli ise istihbarattır. Yeterli ve detaylı bir istihbarat olmaksızın psikolojik harekât hedeflerinin tespiti mümkün olmadığı gibi verilen bir vazifenin de planlanıp, icra edilmesi ihtimal dışıdır. Psikolojik harekâtın karar verme sürecinde vazifenin alınmasından emrin verilmesine kadar ki tüm safhalarda psikolojik harekât istihbaratının oransal olarak çok büyük bir bölümü de “hedef kitle analizinden” başka bir şey değildir. Hedef kitle analizi test ve değerlendirme süreci olmaksızın tek başına sınırlı katkılar sağlayabilir. Gerek psikolojik harekât faaliyetlerini başlatmadan evvel hedef kitleye uygun bir kampanyanın düzenlenmesi için, gerekse faaliyetler icra edildikten sonra başarı derecesinin ne olduğu, elde edilen başarıyı takviye, elde edilemeyen hedeflerin başarılabilmesi için gerekli geri besleme bilgilerinin tekrar sürece sokularak işlenmesi ve komutanın emrettiği vazifenin başarılması için yapılması gerekenlerin tümü ancak test ve değerlendirme süreci ile sağlanabilir. Hedef kitle analizi ile test ve değerlendirme süreci birbiri içine girmiş ayrılmaz parçalardır. Birinin çıktısı diğerinin girdisidir. Süreç devam ederken bu girdi işlenerek çıktı olarak yine tekrar ilkinin girdisi haline gelir. Bu inceleme makalesinin amacı psikolojik harekât faaliyetleri kapsamında ihtiyaç duyulan istihbaratın analiz yöntemi olarak hedef kitle analizi yöntemini ayrıntılı şekilde incelemektir.

**Anahtar Kelimeler:** *Psikolojik Harp, Psikolojik Harekât, İstihbarat, Psikolojik Harekât İstihbaratı, Hedef Kitle Analizi.*

### ABSTRACT

## AN ANALYSIS METHOD IN PSYCHOLOGICAL OPERATIONS INTELLIGENCE: TARGET AUDIENCE ANALYSIS

Psychological operations are the activities carried out to change the emotions, thoughts, attitudes and behaviors of the individual, group or populace, selected as the target. The basis of “Psychological Operations” is intelligence. Without adequate and detailed intelligence, it is not possible to determine the psychological operation’s targets and it is not possible for a given mission to be planned and executed. During the psychological operations decision-making process, a proportionally large part of psychological operations intelligence is actually nothing more than “Target Audience Analysis” at all stages - from assuming the task to giving the operation order. Target audience analysis, on the other hand, can only make limited contributions without a testing and evaluation process. Reinforcing the success

\* Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi Derneği, edizekinci@epenek.com, ORCID: 0000-0002 0470-5257

Makale Başvuru Tarihi / Application Date: 01 Aralık 2022 / 01 December 2022

Makale Kabul Tarihi / Acceptance Date: 04 Ocak 2023 / 04 January 2023

achieved, both in order to organize a campaign suitable for the target audience before starting the psychological operations activities, and what the degree of success is after the activities are carried out. All that needs to be done in order to re-process the necessary feedback information to attain the unachievable targets and to achieve the task ordered by the commander can only be accomplished through testing and evaluation process. Target audience analysis and testing and evaluation process are inseparable parts of each other. The output of one is the input of the other, and while the process continues, this input is processed and is the input of the first one again as an output. The purpose of this review article is to examine the target audience analysis method as the analysis method of intelligence needed within the scope of psychological operations activities.

**Keywords:** *Psychological Warfare, Psychological Operations, Intelligence, Psychological Operations Intelligence, Target Audience Analysis.*

## **GİRİŞ**

Savaş süresince ordunun moralini yüksek tutmak, insan gücünü ve zihnini en iyi şekilde kullanmak için psikoloji bilimine geniş ölçüde yer verilmektedir. Bu kapsamda propaganda da psikoloji biliminden yararlanmaktadır. Yapılan psikolojik araştırmalar kapsamında insanların düşüncelerini etkileyen, morallerini yükselten ya da bozan birçok ilke tespit edilmiştir. Psikolojik harp de bu ilkelerin kullanılmasıyla meydana gelmektedir (Baymur, 1994, s.7). Bu çerçevede ele alındığında psikolojik harp orduların hasımlarını yenebilmesi, savaşları kazanabilmesi için gerekli olan, en az konvansiyonel silah sistemleri kadar önemli araçlardan birisi olarak değerlendirilmektedir.

Bu çalışmada öncelikle psikolojik harp ve harekât kavramları incelenecek, psikolojik harekâtın istihbarat disiplini ile ilişkisi ele alınacak, psikolojik harekât istihbaratı olarak anılan bu istihbarat türüne ait analiz yöntemi olan hedef kitle analizi kavramı incelenecektir.

## **1. PSİKOLOJİK HARP VE HAREKÂT KAVRAMLARI**

Psikolojik harp, çeşitli nedenlerle sınırdan silahlı saldırıyla harekete geçemeyen düşmanın, diğer araçlarla milli bünyeye, vatan sathına girerek ve yerel personelden istifade ederek, içten bölücü ya da içten yıkıcı metotları kapsayan bir saldırı olarak karşımıza çıkmaktadır (Korkut, 1975, s.1). Başka bir ifadeyle psikolojik harp, nihai zaferin elde edilmesini destekleyecek şekilde düşman, tarafsız ve dost toplulukların düşünceleri, hayat görüşleri, hissiyatlarına tesir etmek için propaganda ve ilgili tedbirlerin planlı şekilde kullanılmasıdır. Psikolojik harp hem savaşta hem barışta, insanların duygu,

düşünce ve davranışlarını değiştirmek maksadıyla bilginin kullanılması olarak tanımlanabilir (Tarhan, 2003, s.21). Özellikle askeri literatürde yer alan psikolojik harp kavramı, hasım ülkeyi içten yıkmaya odaklanan, ister sizi destekleyen isterse desteklemeyen ya da tarafsız düşüncelere sahip bireylerin davranışlarını sizin istediğiniz yönde değiştirme amacı güden faaliyetlerin bütünüdür.

Bu çerçevede psikolojik harp, bir devletin ya da devletler grubunun, diğer devlet ya da devletler grubu üzerinde milli menfaatlerini gerçekleştirmek üzere, o ülkede veya başka ülkelerde seçtiği hedef kitlelerin duygu, düşünce, tutum ve davranışlarını kendi amaçları doğrultusunda değiştirmek için, siyasi, askeri, ekonomik, sosyolojik, ideolojik ve teknolojik alanda yapılan faaliyetlerin tümüne denilmektedir. Psikolojik harp devlet çapında uygulanan bir harp türüdür (Yıldırım, 2007, s.129).

Türk Dil Kurumu sözlüğüne göre psikolojik harp tanımı; “Temeli propagandaya dayanan, karşı düşünceli grupların birbirlerini etkileyebilmek ve kendi düşüncelerini kabul ettirmek için aralarında tehdit, şantaj, yıldırma vb. psikolojik öğelerin kullanıldığı mücadele türü” şeklinde ifade edilmektedir (TDK, 2022).

ABD Kara Kuvvetleri “Psikolojik Hareket Talimnamesi” psikolojik harbi, milli hedeflerin ele geçirilmesinde propaganda ve diğer psikolojik faaliyetlerin yabancı düşman grupların fikir, duygu, tutum ve davranışlarını etkilemek maksadıyla planlı kullanımını şeklinde tanımlamaktadır (FM 3-05-30, Haziran 2000). ABD’de, psikolojik harp kavramı 1942’den itibaren Eisenhower’ın karargahında teşkil ettiği Psikolojik Harp Birimleriyle kullanılır hale gelmiştir. 1960’dan sonra ise hem psikolojik harp hem de propaganda kavramlarının insanların zihinlerinde kötileyici etkiler yaratması nedeniyle psikolojik harekât ya da psikolojik operasyon kavramları kullanılmaya başlanmıştır (Güler, 2017, s.179).

Kavramları tam olarak yerine oturtabilmek amacıyla, bu aşamada psikolojik harp ve psikolojik harekât kavramlarının incelenmesinde ve aralarındaki farklılıkların ortaya konulmasında fayda görülmektedir. “Psikolojik harp ile psikolojik harekât tanımları genellikle karıştırılmakta ve sıklıkla birbirleri yerine kullanılmaktadır. Bu iki kavram temelde aynı anlamdadır ancak psikolojik harp kavramı psikolojik harekâtı da kapsamakta, içine almaktadır. Psikolojik harp tüm milli güç unsurlarıyla bir devletin diğer devletler üzerinde milli menfaatlerini geliştirmek üzere icra

ettiği faaliyetler iken psikolojik harekât ise milli menfaatlerin gerçekleştirilmesi için milli güç unsurlarından sadece biriyle gerçekleştirilmektedir. Psikolojik harp devlet çapında yürütülürken, psikolojik harekât ise silahlı kuvvetler çapında yürütülür” (Korkut, 1975, s.8). Devlet çapında uygulanması, devletin, milli güç unsurlarının tümünü harekete geçirebilme yetki ve kabiliyetine sahip olmasındandır.

“Psikolojik harekât; savaş ve barış döneminde dost, tarafsız veya düşman hedef toplumların tutum ve davranışlarını etkileyerek, politik ve askeri hedeflerin elde edilmesini desteklemek için siyasi, ekonomik, ideolojik ve askeri faaliyetleri de kapsayacak şekilde planlanarak uygulanan tüm faaliyetlerdir” (Göksu, 2002, s.363). Diğer bir çalışmaya göre; “Psikolojik harekât; örgütlü, amacı sadece gerçek kişiler olan, mal ve cana yönelik şiddetten ziyade onun yarattığı korku psikozuyla propaganda ve ajitasyon yöntemlerini kullanarak zihinlerde, duygularda ve davranışlarda etki yapmaya yönelik bilimsel, sistematik faaliyetler” şeklinde tanımlanabilir (Çeşme, 2005, s.102). Psikolojik harekâtı “silahlı mücadelenin dışında düşman ülkenin moral gücünü çökertmek, milli birliğini bozmak, iç huzurunu kaçırmak, siyasi ve sosyal karışıklığa düşürmek, devlet ve vatandaşlar arasındaki güveni sarsmak, basın veya hedef ülke kamuoyunu tesir altına almak, korku, telaş ve / veya heyecan yaratmak gibi amaçlarla uygulanan yıpratıcı ve yıkıcı faaliyetler” olarak tanımlamak da mümkündür (Gümüş, 2000, s.692).

İyiat'a (2013, s.19) göre ise psikolojik harbin bir veya birden fazla alanda uyguladığı psikolojik faaliyete psikolojik harekât adı verilmektedir. Başka bir deyişle psikolojik harekât, devlet seviyesinde uygulanan psikolojik harbin bir bölümünü oluşturur. Yani psikolojik harekât denildiğinde, devlet çapında yürütülen psikolojik harbin, devletin organlarından birisi tarafından yürütülen faaliyetler olduğu anlaşılmalıdır. Bu çalışmada ise psikolojik harekâtın silahlı kuvvetler tarafından yürütülen askeri boyutu ele alınmıştır. Milli güç unsurlarının diğer öğelerinin planlayıp uygulanacağı psikolojik harekât faaliyetlerinde de aynı veya benzer yöntem ve metotlar benimsenirken, farklılık, kullanılan araç ve kaynakların her bir milli güç unsurunun özelliklerine ve karakterine uygun olmasından ileri gelir.

Devlet çapında uygulanan psikolojik harpte hasmın milli güç unsurları hedef alınırken, askeri psikolojik harekâta düşmanın komutanları ve hasım askeri birlikler ile dost birlikler hedef alınır. Ayrıca harekât alanında askerî harekâta etkisi olduğu düşünülen devlet dışı silahlı aktörler gibi diğer

unsurlar da hedef olarak değerlendirilir. Askeri psikolojik harekât, diğer askerî harekât çeşitleriyle müşterek ve koordineli olarak icra edilir. Psikolojik harekâtın başarısı; detaylı, müşterek ve merkezi planlama ile merkezi icraya, etkin bir istihbarata, politika ve askerî faaliyetler arasında uyum sağlanmasına ve çok yönlü, kapsamlı bir hazırlık yapılmasına bağlıdır.

Psikolojik harekât, askerî harekâtın çeşitleri olan kara, deniz, hava, özel kuvvet harekâtı, amfibi harekât, hava indirme harekâtı, hava hücum harekâtı, ateşle taarruz harekâtı ve bilgi harekâtı çeşitlerinden bilgi harekâtı kapsamına giren bir harekât olarak da tasnif edilebilmektedir. Psikolojik harekâtın da içinde yer aldığı bilgi harekâtının kapsamında komuta-kontrol harekâtı, istihbarat, sayısal bilgi harekâtı, basın halkla ilişkiler ve sivil-askerî iş birliği faaliyetlerini sinerji yaratacak şekilde birbirleriyle koordineli icra etmek üzere bu faaliyetleri disiplin altına almayı amaçlayan bir yaklaşım bulunmaktadır. Psikolojik harekât, tüm askerî harekât çeşitlerinin içinde kendi fonksiyonunu yerine getiren kendine özgü bir alan olarak nitelendirilmektedir. Bu kapsamda psikolojik harekât, bilginin, insanların fikir, düşünce ve tutumlarını dost kuvvetlerin istekleri doğrultusunda etkilemek maksadıyla kullanılmasıdır (FM 100-6, 2003, ss.2-1,2-24).

Psikolojik harekât planlama ve icracıları, hedef kitle olarak tespit ettikleri, tanımladıkları birey, grup veya topluluğu kendi maksatlarına uygun olarak etkilemek için hedef kitlenin alınan askerî vazifeye doğrudan ilişkisi bulunan özelliklerini öncelikle öğrenmek isterler. Odak noktası dikkat edileceği üzere askerî harekâtın vazifesidir. Vazifenin başarılmasına katkısı olmayacak hususlar inceleme dışında tutulur. Bunun tek nedeni, eldeki zaman, para ve diğer kaynakların getirdiği kısıtlar değil, daha çok vazifeye odaklanılması gereksinimidir. Bir psikolojik harekât kampanyasının hazırlık sürecinde göz önünde bulundurulması gereken en önemli ve kritik husus vazifedir. Psikolojik harekât görevleri açısından bakıldığında vazife hiyerarşik bir komuta zinciri içerisinde hükümetten başlayarak stratejik seviyedeki komutanlığa kadar gelir. Tüm askerî harekât nevelerinde olduğu gibi psikolojik harekâta da askerî hedefler bir stratejik seviyedeki siyasi maksada matuftur. Askerî harekât, siyasi hedeflerin elde edilmesine yönlendirilir. Karar verici veya komutan onayından geçmemiş vazife, vazife olarak değerlendirilemez. Psikolojik harekât, diğer askerî harekât nevelerinden farklı olarak merkezi olarak planlanır ve tek elden icra edilir. Psikolojik harekât planlayıcıları, hedef kitleyi ikna etmek, düşünsel ve duygusal sorgulamalarını etkilemek, yönlendirmek ve psikolojik harekât



kampanyalarını daha etkin hale getirmek için eksiksiz, güncel ve ayrıntılı bilgilere ihtiyaç duyar. Hükümet tarafından verilen direktife bağlı olarak en üst seviyeden en alttaki birliğe kadar kapsamı farklı da olsa bir karar verme süreci başlatılır. Bu karar verme süreci vazifenin alınması, başarının sağlanması için tüm kaynak ve yeteneklerin analitik yöntemlerle ortaya konulması, incelenmesi ve kararın verilmesi, harekât planının hazırlanması ve hedefin ele geçirilmesi ve ondan sonraki evreleri de içine alan devamlı bir süreçtir. Askerî harekâtın maksadı verilen vazifenin başarılmasıdır (FM 3-05.30, 2000, s.7-11).

Yapılan tanımlamalardan yola çıkarak psikolojik harekâtın, hedef birey, grup veya toplulukların- ki bunlar dost, hasım veya tarafsız olabilirler-duygu, düşünce, tutum ve davranışlarını uygulayanın maksatları doğrultusunda değiştirmek için icra edilen faaliyetlerdir. Hedef, temelde insan olduğuna göre istenilen değişimi sağlayabilmenin yollarını ortaya çıkarabilmek için o insanı oldukça iyi tanımak gerekir. Buradan da psikolojik harekât istihbaratının ilgili alanları ortaya çıkmaktadır. Hedefteki insana istenilen duygu, düşünce ve davranışı kazandırabilmek amacıyla, söz konusu insanı motive eden, harekete geçiren unsurların neler olduğunu ortaya çıkarmak için verinin analitik yöntemler kullanılarak elde edilmesi, tasnifi, analizi ve dağıtımı, psikolojik harekât istihbaratının konusunu teşkil etmektedir. Bu çalışmada askerî harekâtın diğer fonksiyon ve yeteneklerinin ne olduğuna değinmeden, çalışmanın özüne odaklanarak psikolojik harekât istihbaratı ve analiz yöntemleri üzerinden incelenecektir.

## **2. PSİKOLOJİK HAREKÂT İSTİHBARATI**

Psikolojik harekâtın istihbarat gereksinimleri konvansiyonel harekâtın istihbarat gereksiniminden oldukça farklıdır. Konvansiyonel birlikler düşmanın kuvveti, muharebe düzenleri, silah sistemleri, hareket tarzları hakkında istihbarata ihtiyaç duyarken, psikolojik harekât birlikleri düşmanın düşüncesi, tutumları, inançları, hassas tarafları, rasyonel veya irrasyonel davranış kalıpları hakkında bilgiye ihtiyaç duyarlar (Daugherty vd., 1958, s.132). Psikolojik harekâtın başlangıç ve bitiş noktası psikolojik harekât istihbaratıdır. Burada kastedilen husus; psikolojik harekât istihbaratının hedef kitlenin tanımlanması ve özellikleri dikkate alınarak nasıl ikna edileceği sorusuyla başlayıp, hedef kitle ikna oldu mu sorusuyla bitmesidir. Psikolojik harekât karar verme sürecinde vazifenin alınmasından harekât emrinin verilmesine kadar ki tüm safhalarda psikolojik harekât istihbaratının büyük kısmını ise hedef kitle analizi oluşturur.

En basit tanımıyla psikolojik harekât faaliyetlerinde kullanılmak için elde edilen istihbarata psikolojik harekât istihbaratı denir. Başka bir deyişle; bir devletin başka bir devlet üzerindeki milli menfaatlerini tahakkuk ettirmesi amacıyla uyguladığı psikolojik harekât faaliyetlerinde kullanacağı, hasım tarafa yönelik hassasiyetlerin, zafiyetlerin tespiti, tasnifi, yorumlanması ve analizi psikolojik harekât istihbaratı olarak tanımlanmaktadır (Kalelioğlu, 2002, s.100). Tanımdan yola çıkarak psikolojik harekât faaliyetlerine yönelik istihbarat çerçevesinde, düşmanın silah sistemleri, birliklerin tertiplenmesi, imkân ve kabiliyetleri, niyeti, karargahının yeri, lojistik sistemleri gibi askeri bilgilerden ziyade düşmanın düşünce yapısı, hassasiyetleri, zayıf yönleri, sosyal, siyasi, ekonomik ve askeri yapısı hakkında ihtiyaç duyulan bilgilerin toplandığı ve analiz edildiği anlaşılmaktadır. Hedef toplumla ilgili psikolojik harekât istihbaratı hedef kitlenin mevcut duruma karşı tutumu, şikayetleri, etnik yapısı, hayal kırıklıkları, kullanılan lisan, problemleri, milli heyecanı gibi konuları kapsar.

Psikolojik harp istihbaratı, psikolojik harbin koordinesi ve yabancı psikolojik harp etkisinin değerlendirilmesi için yapılan bir istihbarat faaliyetidir. Psikolojik harp istihbaratı genel istihbarattan farklı olarak yabancı insan gruplarının fikir, davranış, heyecan ve temayüllerine ait bilgilere dayanır (Kalelioğlu, 2002, s.102). Bu çerçevede psikolojik harekât istihbaratının ilgi alanının sadece bu harekâtın uygulanacağı toplumla alakalı olmadığı aynı zamanda hasım güçlerin kendi toplumumuz üzerine uyguladığı psikolojik harekâtın etkilerini de belirlemek amacıyla üretilen istihbaratı da kapsamı gerektiği anlaşılmaktadır.

Psikolojik harekâtın planlama ve icrası için gerekli olan veri ve bilgilerin büyük bir çoğunluğu açık kaynaklardan elde edilir. Psikolojik harekât istihbaratı gazete, dergi, akademik yayınlar, incelemeler, kitap, ansiklopedi, radyo, televizyon ve internet yayınları gibi açık kaynaklardan, araştırma ve inceleme raporlarından, düşmandan ele geçirilen belgelerden, resmi evraktan, istihbarat raporlarından, mektup, not defteri gibi kişisel belgelerden, biyografik istihbarat belgelerinden, savaş esirlerinden, mültecilerden, yönetici konumundaki sivillerden, kolluk personelinden elde edilebilmektedir (Kalelioğlu, 2002, s.103). İlâveten psikolojik harekât istihbaratının en önemli kaynağı harekât alanındaki yerel halktır. Halkla yapılacak birebir / yüz yüze görüşmeler, yerel halkın kendi ordusu için düşüncelerini, hassas oldukları konuları, hangi konularda nasıl yaklaşılırsa halkın kalbine girilebileceği ve zihinlerinin kazanılabileceğine yönelik

sağlıklı bilgi akışı sağlayacaktır.

Açık kaynaklardan hedef topluma ilişkin; üst düzey askeri ve sivil personelin / bürokratların atamaları, askeri ve sivil teşkilat yapıları ve işleyişleri hakkında bilgiler, devlet yapısının işleyişi, muhalif grupların tepkileri, ortaya çıkan sorunlar, ekonomik durum, ekonomik zorlukların halk üzerindeki etkisi, halkın idareye ve siyasilere karşı tutumu, reaksiyonu, sosyal, demografik ve etnik yapısı, bu yapı içindeki farklılıklar ve problemler gibi konularda değerli ve güncel bilgiler elde edilir. Yayımlanan kitap, araştırma makaleleri, gazete ve dergilerden, hedef toplumun ilgilendiği konular, en son olaylar, kronolojik bir şekilde izlenerek, hedef topluma yönelik yürütülen propaganda faaliyetleri sonucu toplumun tutumundaki değişiklikleri tespit etmek mümkündür. Ayrıca toplumun zayıf tarafları, hassasiyetleri de bu yöntemle ortaya çıkarılabilir. Gazeteler ve dergiler düzenli olarak yayımlandıklarından, olaylardaki ve tutumlardaki değişiklikler bu yayınların takibi sonucu fark edilebilmekte ve propagandaya dahil edilebilmektedir. Bununla beraber psikolojik harekât uzmanı yorumlama ve analiz yaparken, o memleketteki basın hürriyetinin derecesini, hükümetin basın üzerindeki kontrolünü, basının tarafsızlığı gibi basının çalışmasını etkileyen faktörleri göz önünde bulundurur. Ayrıca gazete ve dergilerin dini, ekonomik, siyasal bakımlardan durumları, sempati ve ideolojik gruplar üzerindeki etkileri gibi hususları da bu süreçte dikkate alınmalıdır (Yıldırım, 2007, s.151).

Psikolojik harekât istihbaratının hedefleri;

- İstismarı mümkün olan zafiyetleri ortaya çıkarabilmek,
- Yetki verildiğinde bu bilgilerin toplanmasına yardım etmek ve toplama faaliyetlerini koordine etmek,
- Psikolojik harp faaliyetlerinin etkilerini değerlendirmek,
- Uygulanan psikolojik harp faaliyetlerinin ulaştığı sonuçları tespit etmek,
- Düşmanın zayıf taraflarına ilişkin bilgileri toplamak,
- Propagandayı tam zamanında kullanabilecek durum ve fırsat anlarını tespit etmek,
- Propaganda içeriğinde kullanılmak üzere kıymetlendirilmiş haberleri toplanmak ve elde hazır bulundurmak,
- Düşmana yönelik propaganda faaliyetlerinin etkilerini ölçmek üzere bilgi toplamak,
- Düşmanın tarafımıza yönelttiği propagandanın etkisini ölçmek ve

düşman propagandasını boşa çıkarmak üzere uygun yöntem ve vasıtaları belirlemektir (Yıldırım, 2007, s.151).

Psikolojik harekât istihbaratında ihtiyaç duyulan bilgilerin, istihbaratla görevli kurum, kuruluşlar ve sistemlerden alınması mümkün ise de psikolojik harekâtın kendi doğası gereği bu çalışmaları bizzat psikolojik harekât teşkillerinin eğitilmiş personeli vasıtasıyla hazırlamak da mümkündür. Psikolojik harekât istihbaratının hazırlanması, test ve değerlendirilmesi mutlaka bu konuda eğitim almış psikolojik harekât uzmanları tarafından yapılmalıdır. Ayrıca psikolojik harekât istihbaratı ile ilgili olarak yapılan çalışmalarda nihai maksadın “Hedef Kitle Analizine” girdi olacak bilgiler ile psikolojik harekât faaliyetleri sonucu elde edilen etkinin ne olduğu hususlarını elde etmek olduğu gözden uzak tutulmamalıdır. Bu bağlamda, istihbarat elde edilirken hedef kitle analizinin bir psikolojik hedefi ve ona bağlı destekleyici psikolojik harekât hedeflerini elde etmek için hedef kitlenin nasıl ikna edileceğini belirlemek olduğu daima hatırlanmalıdır. Bu analiz belirli bir hedef kitleden nasıl belirli bir tepki alınacağını belirlemek için oluşturulan bir faaliyet olacaktır (FM 33-1-1, 2003, s.5-1).

Halkın, yani harekât alanında yer alan insanların, duygu ve düşünceleri, örf ve adetleri, hassas tarafları, hoşlandıkları ve sevdikleri şeyler / davranışlar gibi kritik bilginin temini için psikolojik harekât birliklerince hedef kitle analizi yöntemi tercih edilmektedir.

### **3. PSİKOLOJİK HAREKÂT İSTİHBARATININ TEMELİ: HEDEF KİTLE ANALİZİ**

Devletler arasındaki güç dengesi mücadelesinde tarafların isteklerini birbirine zor kullanarak kabul ettirme aşamasına gelindiğinde, yani silahlı çatışma ortamında dahi hasmın fiziksel olarak imha edilmesi gerekli olmayabilir. Bunun birçok gerekçesi olabilir. Hasımın savaşma azminin kırılması, liderlerine olan güvenin azaltılması, hedef kitlede birlik ve beraberlik hislerinin çökertilmesi veya yok edilmesi, her seviyedeki askeri aldatma planındaki senaryolara inandırılması siyasi ve askeri hedeflerin ele geçirilmesini kolaylaştırır (FM 3-0, 2008, s.7-2).

Bu nedenle, hedef kitlenin duygu ve düşünce yapısını ve buna bağlı olarak tutum ve davranışlarını şekillendirmek, mücadeleye olan arzu ve iradesini zayıflatmak, istediğimiz son duruma ikna etmek için hedef kitleyle ilgili ayrıntılı bilgilere ihtiyaç vardır. Öte yandan, dost hedef kitlenin duygu

ve düşüncelerini takviye etmek, tarafsız kitlelerin desteğini kazanmak da psikolojik harekâtın amaçlarındandır. Psikolojik harekâtın hedef kitle analizinde hedef kitle sınıflandırmasına giren birey, grup ve toplumlarla ilgili bilgiye sahip olmak gerekir (FM 3-13, 2003, s.5-8). Kısacası, psikolojik harekât bilgiyi kullanarak etkiyi sağlama çabasıdır

Hedef Kitle Analizi, bir hedef kitlenin kilit özelliklerinin, sorunlarının ve paradigmalarının, özetle olası hassasiyetlerinin tanımlanmasını kapsar. Hedef Kitlenin algı ve genel endişelerinin anlaşılması ve hedef kitlenin buna bağlı olarak nelerden etkilendiğinin ve nelerle harekete geçirilebileceğinin bilinmesini gerektirir (McElroy, 1990, s.23).

Hedef kitle analizi ise test ve değerlendirme süreci olmaksızın tek başına sınırlı katkılar sağlayabilir. Test ve değerlendirme hem başlangıç hem de de bitiş noktasının kritik aşamasıdır. Gerek psikolojik harekât faaliyetlerini başlatmadan önce hedef kitleye uygun bir kampanyanın planlanabilmesi için, gerekse faaliyetlerin icrası esnasında ve sonrasında başarı derecesinin ne olduğu, elde edilen başarının takviye edilmesi, elde edilemeyen hedeflerin başarılabilmesi için gerekli geri besleme bilgilerinin tekrar sürece sokularak işlenmesi ve nihayetinde vazifenin başarılması için yapılması gerekenlerin tümü test ve değerlendirme süreci ile sağlanabilir. Hedef kitle analizi ile test ve değerlendirme süreci birbiri içine girmiş ayrılmaz parçalardır.

Bununla birlikte psikolojik harekât istihbaratı temel olarak kendi araştırma kaynak, araç ve yöntemlerini kullanmak ister. Psikolojik harekât istihbaratı, istihbarat ürünlerini; planlama ve yönetim, ihtiyaçların tespiti, yöneltme, haberlerin toplanması, istihbaratın meydana getirilmesi, işlem ve yayımlama aşamalarını kullanarak meydana getirdiği istihbarat sürecini takip ederek oluşturur (Katz, 1982, s.122).

#### **4. HEDEF KİTLE ANALİZ SÜRECİ**

Hedef kitle analizi, vazifeden çıkarılan psikolojik harekât hedefini ele geçirmeyi sağlayabilecek hedef kitleyi tespit edebilmek için vazifeye ilgili gereken bilgilerin sistematik incelenmesidir. Hedef kitle analizinin nihai maksadı, vazifeye yönelik olarak tespit edilen psikolojik harekât hedefine ulaşabilmek için, seçilmiş hedef kitlenin nasıl ikna edileceğini belirlemektir. Analizde, ikna edilmek ve tutum ve davranış geliştirmesini istediğimiz hedef kitle ile ilgili vazifenin başarılmasına etkisi olmayacak, bilgi kirliliğine neden olabilecek bilgiye nadiren ihtiyaç duyulur (FM 33-1-1, 2003, s.4-8).

Buradaki temel kriter incelenen hedef kitlenin, vazifenin başarılmasına etkisi olan özelliklerinin araştırılmasıdır. Örneğin, hedef kitlenin mensup olduğu dini inanç sisteminin askerî harekâtın vazifesinin başarılmasında herhangi bir destekleyici veya engelleyici etkisinin olmayacağı tespit edilmişse, hedef kitlenin dini inançlarının teferruatlı incelenmesine gerek olmayabilir. Onun yerine haber toplama ve istihbarat oluşturma sürecine tahsis edilen kaynakların daha verimli ve ekonomik kullanılmasına ağırlık verilebilir. Hedef kitle analizinin özü, hangi ikna mesajına karşı hangi tepkinin alınacağını önceden tespitidir. Bu bilgiler çerçevesinde oluşturulan psikolojik harekât ürünlerinin (görsel, işitsel, görsel ve işitsel medya ürünleri) kullanımıyla amaçlanan tepkinin hedef kitleden alınıp alınmadığının tespiti hem yürütülen askerî harekâtın başarısını hem de hedef kitleden amaçlanmayan veya vazifenin yapılmasını riske atacak, insan yaşamı kaybına neden olacak, uluslararası veya kamuoyunun meşru karşılamayacağı tepkilerin önüne geçilmiş olacaktır (FM 33-1-1, 2003, s.1-3).

Askerî harekâta, vazife ve bu vazifelerden çıkarılan görevleri yerine getirebilmek için askerî birlikler, caydırıcılık ve harekât alanının şekillendirilmesi çalışmalarıyla diğer askerî harekât safhalarını icra ederler. Vazifenin başarılmasında caydırıcılık ve harekât ortamının şekillendirilmesi, silâh sistemleri, teknoloji, C4ISR (komuta-kontrol, muhabere, bilgisayar, istihbarat, gözetleme, keşif kelimelerinin İngilizce kısaltması) üstünlüğü gibi yeteneklerle hasım üzerinde caydırıcılık sağlanırken sahip olunan nitelik üstünlüğünün dost, hasım ve tarafsız hedef kitlelere iletilmesi ve algılatılması görevini de psikolojik harekât unsurları yaparlar. Bu kapsamda, harekât ortamının şekillendirilmesinde elde mevcut tüm yetenekler kendi sorumluluk ve faaliyetlerini icra ederken psikolojik harekât uzmanları yine vazifeye uygun tespit edilmiş dost, hasım ve tarafsız hedef kitlelerin duygu, düşünce, tutum ve davranışlarını şekillendirmeye gayret ederler. Gerek caydırma gerekse harekât ortamının şekillendirilmesinde uygulanacak psikolojik harekât görevlerinin plan ve icrası için hedef kitleye yönelik istihbaratın eksiksiz sağlanması kritik önemi haizdir. Öte yandan vazifenin yerine getirmesi için komutan ve karargahının vazifeyi tahlil etmesinden sonra ortaya koyacakları farklı hareket tarzlarının her birine uygun farklı veya birbiriyle kesişimi olan psikolojik harekât planlaması yapılacağından her bir harekât tarzına göre farklı hedef kitleler ve bunlara yönelik ikna mesajlarının geliştirilmesi gerekeceği için tespit edilen hedef kitlelerin her

biri için farklı bilgi ihtiyaçları ortaya çıkacaktır. Hedef kitle analizi vazifeden vazifeye farklılıklar göstereceği gibi aynı vazifenin diğer hareket tarzları için de farklılıklar gösterecektir. Çünkü itici ve dikte edici unsur psikolojik hedefler ve bunun bileşenleri olan destekleyici psikolojik hedeflerdir.

Bununla birlikte, tümünden gelim yöntemiyle, askeri harekâtın başarılması için alınan vazife, vazifenin icracı komutan tarafından tahlil edilmesi, tahlil edilen vazifeyi başaracak hareket tarzlarının tespiti, bu hareket tarzlarından faydası en çok, mahzuru en az olan hareket tarzının seçilmesi, diğer hareket tarzlarının olasılık planları için göz önünde bulundurulması, komutan tarafından seçilen en çok başarı vadeden hareket tarzının karar olarak kabul edilip icra edilecek harekâtın planlamasına esas olması gibi askeri karar alma sürecinin algoritmasını oluşturan evreler psikolojik harekât planlamacıları ve icracıları için ana mihenk taşlarıdır.

Vazifenin tahlili ve hareket tarzlarının belirlenmesinde psikolojik harekât personeli komutana hangi hareket tarzının psikolojik harekât bakış açısından daha etkili sonuçlar ortaya koyacağı konusunda danışmanlık yaparlar. (FM 33-1-1, 2003, s.4-15).

Psikolojik harekât icracıları ve istihbaratçılar, ana harekât ve vazifeyle bağlarını hiçbir şekilde kopartamazlar, bağın zayıflamasına dahi izin veremezler. Hangi seviyede olursa olsun askerî harekâtın karmaşık doğasının ve komutanın üzerine yüklediği sorumluluk nedeniyle komutan ve karargâhı psikolojik harekât teşkillerine tahsis edecek zamanlarının kısıtlı olması nedeniyle söz konusu sıkı bağı ve bunun gerektirdiği koordinasyon ve senkronizasyonu muhafaza etmek birinci derecede psikolojik harekât personelinin sorumluluğunda olmalıdır. Buradaki bir zafiyet tüm askerî harekâtı başarısızlığa ve uluslararası kamuoyu nezdinde ülkenin haksız duruma düşmesine neden olabilir.

## **5. HEDEF KİTLELERİN SEÇİLMESİ**

Psikolojik harekât faaliyetlerinin temel ilgi alanı toplumlar yani kitlelerdir (Özdağ, 2013, s.208). Burada belirtilen “kitle” kelimesi yığın anlamında olup, Le Bon’a (2017, s.19) göre bir araya gelişleri ister tesadüfi ister başka bir gerekçeyle olsun, fert kimliğinden ayrılarak oldukça başka bir karaktere dönüşen insan topluluğu anlamı taşımaktadır. Bu anlamda yine Le Bon’a göre psikolojik harekât farklı amaçlarla bir araya gelen bu toplulukları hedef alır. Psikolojik harekâtın hedef aldığı bu kitlelerin özelliklerini göz önünde bulundurarak özel bir çalışma sonucu plan yapılır (2017, s.24).

Hedef kitle analizi, vazifeden elde edilen/çıkarılan psikolojik hedefin elde edilmesini sağlayacak hedef kitlenin seçilmesi için psikolojik harekât ile ilgili istihbarat ve bilgilerin detaylı ve sistematik incelenmesi sürecidir (FM 33-1-1, 2003, s.3-16).

Hedef kitle analizinin birinci aşaması hedef kitlenin seçimidir. Hedef kitle, psikolojik hedef ve onu destekleyen alt görevler olarak nitelendirilebilecek destekleyici psikolojik hedeflere göre seçilecek, genel olarak bireyler, gruplar veya toplumlardır. Seçim kriteri, hassasiyet, etkilenme derecesi, etkinlik, kitlenin istenen tepkileri verme yeteneği, kitlenin kitle iletişim araçlarına erişebilirliği gibi faktörlerden oluşur.

Hedef kitle analiz süreci aşağıdaki dört temel soruyu cevaplamaya çalışır:

- İstenen davranışsal ve tutumsal tepkiyi elde etmede hangi hedef kitleler en etkin olabilecektir?

- Hangi ikna mesajları hedef kitleyi psikolojik hedefi elde etmek için etkileyecektir?

- Seçilmiş ikna mesajını en etkili olarak hangi kitle iletişim vasıtası iletecektir?

- Hangi olaylar psikolojik harekât gayretlerinin başarı veya başarısızlığının göstergesi olacaktır? (FM 33-1-1, 2003, s.5-1).

Hedef kitlenin mümkün olduğu kadar açık, net ve belirgin olarak tanımlanması psikolojik harekât gayretlerinin başarısı için önemlidir. Bir psikolojik hedef olarak, hedef kitleden istenilen tepkinin alınabilmesi için, seçilen hedef kitlenin özelliklerinin, ihtiyaçlarının ve hassasiyetlerinin kesişim kümesinin mümkün olduğunca geniş olması arzu edilir. Şayet hedef kitle bu nitelikleri taşımıyorsa ya hedef kitle yanlış seçilmiş ya da mevcut psikolojik hedef için uygun olmayan bir hedef kitle alınmıştır. Psikolojik harekât yetenekleri açısından gelişmiş teşkilere ve kaynaklara sahip ülkelerin psikolojik harekât kampanyaları incelendiğinde, bir psikolojik hedefi elde etmek için hedef kitle olma özelliği taşımayan homojen yapılar bulunmaması halinde yıllar süren ve büyük mali kaynaklar harcanarak o psikolojik hedefin ele geçirilmesini sağlayacak hedef kitle inşası operasyonları yapabildikleri görülmektedir.

Bu nedenle hedef kitlenin seçimi psikolojik harekât faaliyetleri açısından kritik önem taşımaktadır. Homojen olmayan hedef kitleler için



yapılacak hedef kitle analizi ve bunun sonucu elde edilecek bilgilerle icra edilecek bir psikolojik harekâtın dost psikolojik hedeflerini elde etmede telafisi zor başarısızlıklara neden olacağı bilinmelidir (FM 33-1-1, 2003, s.5-3).

Psikolojik harekât analizcisi belirli bir hedef kitleyi tanımlamadan önce o hedef kitlenin aşağıdaki karakteristiklere sahip olup olmadığını incelemelidir.

- Hedef kitle benzer koşullara ve benzer hassasiyetlere sahip olmalıdır.
- Hedef kitle belirtilen destekleyici psikolojik harekât hedefine ilişkin olmalıdır.
- Hedef kitle belirtilen destekleyici psikolojik harekât hedefini elde etme kabiliyetini taşımalıdır (FM 33-1-1, 2003, s.5-1).

Hedef kitle analiz sürecinde hedef kitleyi vazifeye yönelik inceleme esnasında psikolojik harekât istihbarat gayretlerinin yoğunlaştırılacağı hususlar ABD Genelkurmay Başkanlığı yayını olan Müşterek Psikolojik Harekât Doktrinin 'de aşağıdaki şekilde tanımlanmıştır.

- Hangi hedef kitle grupları vazifenin başarılmasında plan, karar ve harekât etkinliğine tesir edebilir?

- Bu grupların psikolojik harekâta duyarlılığı ya da etkilenme derecesi nedir?

- Hangi grup davranışları vazifenin başarılmasına yardımcı veya zararlı olabilir?

- Grupların hedef, motivasyon ve özellikleri nelerdir?

- Grubun davranışlarını etkileyebilen liderler kimlerdir?

- Yabancı hedef kitlelere ilişkin kritik bilgi unsuruyla bağlantılı gruplar hangileridir?

- Her bir grubun geçmiş bilgileriyle, bizim istediğimiz veya bize zararlı değerlendirmeleri nelerdir? (Joint Publication 3-53, Doctrine for Joint Psychological Operations, 2003, s.46).

Görüldüğü üzere stratejik seviye olan Genelkurmay Başkanlığı/Müşterek komutanlık seviyesinde hedef kitle seçiminde özellikle vazifenin başarılması ile hedef kitle seçimi arasında güçlü bir bağın olması istenmektedir.

Modern psikolojik harekât birçok safhadan oluşan hedef kitle analizini içerir. İlk safha muhtemel hedef kitleleri belirlemektir. Hedef kitle tespit edildiğinde, hassasiyetleri, hedef kitlenin etkilenme derecesi, koşulları, hedef kitlenin etkinliği gibi özellikleri incelenir. Hassasiyetler, hedef kitleyi etki altına alabilecek psikolojik unsurlar olan algılama, motivasyon, stres ve tutumlardır. Hedef kitlenin etkilenme derecesi, hedef kitlenin aldığı mesaja istenen tepkiyi verme derecesidir. Koşullar ise, hedef kitlenin içinde bulunduğu ve onu etkileyen sosyal, ekonomik, politik, askeri ve fiziki unsurlardır. Hedef kitlenin etkinliği, hedef kitlenin psikolojik harekât personelinin beklediği tepkileri verme yeteneğidir (Goldtein ve Findley, 1996, s.51).

- Koşullar: Hedef kitlenin içinde yaşadığı, onu kapsayan, etkileyen ancak hedef kitlenin bunlar üzerinde sınırlı kontrole sahip olduğu faktörlerdir. Hedef kitleyi etkileyen koşullar sınırsızdır ve bunların pek çoğu destekleyici psikolojik harekât hedefleri ile ilişkili de değildir. Hedef kitle analizi süreci boyunca sadece hedef kitleyi etkileyen ve destekleyici psikolojik harekât hedeflerine ilişkin olanlar göz önünde bulundurulur (FM 33-1-1, 2003, s.5-5).

- Zayıf ve Hassas Taraflar: Hedef kitlenin yoksunluğunu gidermek için çaba sarf ettiği, içinde bulunduğu koşulların ortaya çıkardığı ihtiyaçlardır. Psikolojik harekât personeli, psikolojik hedef ve destekleyici psikolojik hedeflerine uygun olarak istismar edecekleri hedef kitlenin zayıf ve hassas taraflarını eksiksiz bir şekilde tanımlamadan istenen tepkiyi almaları çoğu zaman mümkün değildir. Zayıf ve hassas taraflar, ancak takviye ya da istismar edildiklerinde bir anlam taşırlar. Zayıf ve hassas tarafların kahir ekseriyeti ihtiyaçlardan ortaya çıkar. Hedef kitlenin bir ihtiyacı tatmin etmesi, ona olan ihtiyacı azaltması veya ortadan kaldırması onların davranışlarını değiştirmeye yönelik olarak bir motivasyon sağlar. (FM 33-1-1, 2003, s.5-5)

Bir hedef kitlenin ihtiyaçları o Hedef Kitleyi etkileyen koşulların analiz edilmesi sonucu ortaya çıkarılır. Hassasiyetlerin meydana çıkarılmasındaki aşamalar şu şekilde sıralanabilir.

- Hedef kitleyi etkileyen koşulları temel alan ihtiyaçların tanımlanmasıdır.

- İhtiyaçların sınıflandırılması ve önceliklendirilmesidir. Bu basamaktaki hedef hangi ihtiyaçların en önemli olduğuna ve bunlardan

hangisinin psikolojik harekât uzmanları tarafından ilk önce kullanılması gerektiğine karar vermektedir.

- Çatışan ihtiyaçların ve ne tip bir çatışmanın mevcut olduğuna karar vermektedir. Böylece psikolojik harekât analizcisi belirli bir ihtiyaca ve onun ortaya çıkardığı zayıflık ve hassasiyete en iyi nasıl yaklaşacağını analizciye gösteren, hedef kitlenin çatışmayı çözmek için nasıl bir yol takip edeceğini tahmin edebilir.

- İhtiyaçlar ile destekleyici psikolojik harekât hedefi arasındaki ilişkinin ne olduğuna karar vermektedir. Eğer herhangi bir ihtiyaç destekleyici psikolojik harekât hedefi ile ilişkili ise bu ihtiyaç hedef kitle analizindeki yerini korur. Eğer ilişkili değil ise hedef kitle analizinden çıkartılmalıdır (Ekinci, 2005, s.22).

Sonuç olarak her bir ihtiyaç veya hassasiyet gerekli psikolojik harekât faaliyetini belirlemek için incelenir. Yüksek önceliğe sahip ve destekleyici psikolojik harekât hedefi ile kuvvetli bir ilişkisi olan hassasiyetler destekleyici psikolojik harekât hedefini elde etmek üzere hedef kitleyi etkilemek için istismar edilebilir. Tatmin edildiğinde destekleyici psikolojik harekât hedefinin başarılmasını engelleyecek herhangi bir hassasiyet en aza indirgenmelidir. Diğer düşük öncelikli fakat destekleyici psikolojik harekât hedefi ile kuvvetli bir ilişkisi bulunan hassasiyetler artırılabilir ve ondan sonra da istismar edilebilir (Ekinci, 2005, s.22).

### **5.1. Zayıf ve Hassas Tarafların İhtiyaçlar Teorisiyle İlişkisi**

Abraham Maslow'un 1943 yılında yazdığı "İnsan Motivasyonuna Yönelik Bir Teori" başlıklı makalesindeki ihtiyaçlar hiyerarşisi, ihtiyaçların tatmini açıklaması bakımından en çok bilinendir. Maslow, bir piramit kullanarak bireyin bir sonraki sosyal ihtiyaç basamağına çıkmadan önce temel ihtiyaçlarını tatmin etmesi gerektiğini açıklamıştı. Ayrıca her bir bireyin bir sonraki basamaktan önce diğer basamaklardaki ihtiyaçlarını karşılması gerektiğini ileri sürmüştür (Healy, 2016, s.315).

Çok kriterli karar verme üzerine araştırmaları bulunan Milan Zeleny, Moslow'un ihtiyaçlar hiyerarşisini tamamen reddetmemekle birlikte yeni bir bakış açısı kazandırmıştır. Bu yeni bakış açısına göre Maslow'un dogması insan ihtiyaçlarının bir sıra dahilinde, yüksek derecedeki ihtiyaçlarının ancak daha alt seviyedeki ihtiyaçları yeterli bir şekilde tatmin edildiğinde ortaya çıktığını göstermektedir. Buna göre kendini gerçekleştirme insanoğlunun

nihai ve en üst derecedeki ihtiyaç veya arzudur. Bununla birlikte nefes alma, yeme içme gibi yaşamın ön koşullarının en önde gelen ihtiyaç olarak kabul edilmesi ihtiyaçlar piramidinin yükselmesinde gerekli dayanağı sağlamamaktadır. Zeleny'e göre insan ihtiyaçlarının açıkça tanımlanabilir bir hiyerarşisi yoktur. İnsanoğlu geniş kapsamlı istek, hedef, dürtü ve arzularının eş zamanlı olarak giderilmesi ve bu ihtiyaçlarının dengeli ve aynı anda tatmini için çaba sarf eder. Etkileşim içinde olan karmaşık ihtiyaçlar birbirinden oldukça bağımsızdır ve bu ihtiyaçların tüm alt bileşenleri karşılıklı olarak birbiri ile uyumlu ve birbirini tamamlayandır. Böylesine birbirine paralel ve eş zamanlı ortaya çıkan motivasyonlar en alttan en üstte kadar sıralanamayacak kadar karmaşıktır. Yüksek seviyedeki insan ihtiyaçları aslında daha düşük seviyedeki ihtiyaçları da içinde barındırır. Güvenlik ihtiyacının yanında ait olma ihtiyacı da insanları müşterek ve teşkilatlı toplum oluşturma arayışına iter. Fizyolojik ihtiyaçların yanı sıra saygı görme ihtiyacı avlanan insanı daha etkin ve kabiliyetli olmaya motive eder (Zeleny, 1982, s.21).

Kendini gerçekleştirme ihtiyacı aç, emniyetsiz ve sevgisiz ilkel insana Anadolu'nun pek çok yerinde bulunan mağaralarda görmüş olduğumuz mükemmel güzellikteki duvar resimleri yapmaya zorlar. Bu resimler sanatın en mükemmelini yansıtmakta hatta modern zamanın kendini gerçekleştirmiş sanatçıları tarafından sanat yönü onaylanmış ve hatta bazılarının daha da üstün sanat eserleri olduğu kabul edilen bir sanat gücü ve deneyim derinliği yaymaktadır. İlkel zamanlarda icra edilen sanatın maksat ve işlevleri çeşitli olmakla beraber bu sanatsal üstünlük bir şeyler ortaya koyma arzusundan, estetik ihtiyaçların tatmininden ve kendini ifade etme ihtiyacından kaynaklanıyor görünmektedir (Ekinci, 2005, s.14).

Hapishanedeki mahkumlar, çalışma kamplarındaki hükümlüler ya da birincil ihtiyaçlarını karşılamaktan yoksun bırakılan insanların bahçe işleri ile uğraştıkları, çeşitli sanatsal çalışmalar yaptıkları, çizimler, yazım, şiir ve yeni yeteneklerin elde edilmesi faaliyetleri ile uğraştıkları bilinmektedir. Kör, açlıktan perişan ve üşümüş bir şekilde bir kulede müebbet hapse çarptırılmış olan Dalibor isimli bir adam ile ilgili eski bir Çek hikayesi vardır. Bu adam kendi kendine keman çalmayı öğrenmiştir. Yani perişan ve umutsuz bir hayat Dalibor'a keman çaldırmıştır. Kabul etmesi bazen zor, fakat üst seviyelerdeki ihtiyaçlar pek çok durumda öncelik alabilmektedir (Zeleny, 1982, s.20). Pek çok aç ve yalnız insan kendini gerçekleştirme uğruna çaba sarf ederken, karnı tok sırtı pek birçok insan da kendi ilkel ya da

en alt seviyelerdeki ihtiyaçlarına odaklanmış, kendisinden başka bir şey düşünmeyen bencil bir hayat sürebilmektedir.

## **5.2. İhtiyaçları Giderirken Yeni Zayıflık ve Hassasiyetlerin Ortaya Çıkışı: Çatışma**

Hedef kitlenin ihtiyaçlar bağlamında motivasyon unsurlarını tespit ederken eş zamanlı ortaya çıkan ihtiyaçlarının aynı zamanda sürekli bir çatışmayı da ortaya çıkacağını göz önünde bulundurmak gerekir. Buradan yola çıkarak çoklu çatışan amaçlar veya kriterlerden bahsedilebilir. Fakat şu da bilinmelidir ki ihtiyaçların bizzat kendileri çatışma halinde değildir. Tam tersi, elde edilmeye çalışılan amaçlar bunları elde etme yolunda çeşitli nedenlerle çatışma halindedir, çünkü doğal, ekonomik ve sosyal tehditler elde edilmeye çalışılan çok amaçlılığın aynı anda ve tam olarak gerçekleşmesine izin vermez. Bu tehditleri azalttıkça ihtiyaçlarımızın çeşitliliğini artırır ve sonuç olarak tekrar bir çatışma durumu yaratırız. Aslında yaptığımız şey çatışmaların niceliğini arttırmaya çabalamaktan başka bir şey değildir (Tabucanon, 1989, s.7).

İhtiyaçlarımız bizim sahip olduğumuz hareket tarzlarına bağlı olarak değişebilmektedir. Bu ihtiyaçlar ne birincil ne de ikincil türden ihtiyaçlardır. İhtiyaçlar yaşam tarzımıza göre şekil alır ve ne tür hareket tarzları seçeceğimizi belirler. Harekete geçme ihtiyacı zaten kendi içerisinde bizlerin temel motivasyon unsurlarımızdan biridir. Hareketlerimizin tümü amaçlı, ihtiyaç tatmin edici veya hedefe yönelmiş olmayabilir. Psikolojik harekât analizcisi hedef kitle analiz sürecine devam etmek için hedef kitlenin ihtiyaçlarını sınıflandırmalı ve önceliklendirmelidir. Maslow'un teorisi bu sınıflandırmayı yapmak için kullanılan yollardan sadece biridir. Ancak ihtiyaçlarla ilgili olarak kesin bir sınıflandırmanın olmadığı da Tabucanon ve Zeleny'nin açıklamaları göz önüne alınarak düşünülmelidir.

Bununla birlikte Maslow'un sınıflandırması bazı durumlarda kolaylıkla alt parçalara ayrılabilir. Pek çok insan olağan zamanlarda Maslow'un hiyerarşisine göre davranmakla beraber özellikle zihinsel, duygusal ve fiziksel baskı olarak tanımlanabilecek yüksek stres altında iseler davranışlarını önemli ölçüde değiştirebilmektedirler. Örnek olarak bir çatışma esnasındaki askerler yüksek seviyelerdeki strese dayanabilmekte ve birliğin hedeflerini elde geçirmek için kendi temel ihtiyaçlarının üstesinden gelebilmek üzere eğitilmektedirler. Hedef kitle olarak bu tür insanları değerlendirirken eğitim durumu ve seviyesi de göz önüne alınmalıdır.

Belirli psikolojik hedefleri elde etmek üzere bir hedef ülkede farklı hassasiyetler oluşturmaya yönelik olarak çatışmanın tüm boyutları kullanılarak fiziksel, manevi ve bilgiye yönelik yapılan tüm psikolojik harekât kampanyaları sonucu hedef kitlede hassasiyet artırılmaya ve buna bağlı olarak etkilenebilme derecesi yükseltilmeye çalışılırken, arzulananın tam aksi istikametinde bir tepki oluşabilir ve bu daha öncede bahsedildiği gibi harcanan tüm kaynakların boşa akıtılması yanında milli çıkarlara önemli zararlar verebilir. Böyle bir sonuçla karşılaşmamak için hedef kitle analizi sürecinde hassasiyetler ortaya çıkarılırken ya da yeni hassasiyetler oluşturulmaya çalışılırken hedef kitlenin bir ihtiyacına yönelik olarak hassasiyet eğrisinin ve buna göre marjinal hassasiyet ve ortalama hassasiyet eğrilerinin analizinin iyi yapılması gerekir. Bununla uyumlu olarak etkilenebilme derecesi de marjinallik ve ortalama parametreleri kullanılarak analiz edilmelidir (Ekinci, 2005, s.22).

### **5.3. İhtiyaçların Aciliyetinin Motivasyona Etkisi**

Koşullara bağlı olarak ihtiyaçlar ortaya konduğunda bunlar kritik, kısa vadeli ve uzun vadeli olarak sınıflandırılabilir. Farklı kültürler belirli ihtiyaçlar için farklı öncelikler koymuş olabilirler ve psikolojik harekât uzmanları ihtiyaç sınıflandırmasını buna uygun olarak düzenlemek için kendi uzmanlıklarını ortaya koymaları gerek. Genel bir örnek verecek olursak kritik ihtiyaçlar güvenlik ortamının ciddiyetine bağlı olarak genellikle biyolojik veya muhtemelen güvenlik ile ilgili olacaktır. Kısa dönemli ihtiyaçlar genellikle Maslow'un güvenlik ve ait olma ihtiyaçları olarak sunduğu ihtiyaçlara karşılık gelmektedir. Bunlar hayatı devam ettirmek için derhal tatmin edilmesi gerekmeyen ihtiyaçlardır. Zor ekonomik koşullar, yüksek suç oranı, siyasi özgürlüklerin olmayışı, sağlık ile ilgili imkanların hemen hemen hiç olmaması gibi durumlar kısa vadeli ihtiyaçlara örnek olarak verilebilir. Uzun dönemli ihtiyaçlar Maslow'un saygı görme ve kendini gerçekleştirme ihtiyaçları olarak düşünülmüş olduğu ihtiyaçlardır. Buna verilebilecek örnekler ifade özgürlüğünün mümkün olduğu, istikrarlı bir hükümetin, güçlü bir ekonominin, adil bir adalet sisteminin veya girişim özgürlüğünün bulunması olabilir (FM 33-1-1, 2003, s.5-6).

Önceliklendirme, hedef kitlenin ihtiyaçları tatmin edebilmesi için sahip olduğu arzu ve isteğin derecesini yansıtmalıdır. Farklı koşullara göre ihtiyaç giderme özelliğine sahip bir olgu hedef kitle tarafından daha büyük bir gayret ile elde edilmeye çalışılacağından genellikle daha yüksek önceliğe sahip olabilir. İhtiyaçlar önceliklendirildiğinde psikolojik harekât uzmanına

gayretlerinin önceliğine karar vermede yardımcı olacak şekilde kritik, kısa dönemli ve uzun dönemli olarak sınıflandırılmalıdır. Bu noktada psikolojik harekât analizcisi destekleyici psikolojik harekât hedefi ile ilişkili olmayan herhangi bir ihtiyacı dikkate almayacaktır. Analizci kısa vadeli veya uzun vadeli bir ihtiyaçtan önce tatmin edilmesi gereken kritik bir ihtiyacı gözden kaçırabileceği hususunda çok dikkatli olmalıdır. Kritik ihtiyaçlar çoğunlukla tüm destekleyici psikolojik harekât hedefleri ile uyum sağlar. Bir hedef kitlenin bir ihtiyacını karşılamaya çalıştığı pek çok durumda bir çatışma kaçınılmaz olacaktır. Birbiriyle uyuşmayan iki veya daha fazla güdünün bireyi etkilediği anlarda ortaya çıkan bir durumdur. Birey çoğu kez bunlardan hangisini seçeceğine karar veremez ve sıkıntılı bir durum içerisine girer. Bireyi birbirine karşıt iki ayrı veya daha fazla yöne çeken eğilim ve gereksinimler arasındaki sürtüşmeye çatışma adı verilir (FM 33-1-1, 2003, s.5-18).

#### **5.4. Hedef Kitle, İhtiyaçlarına Ait Çatışmayı Nasıl Çözer?**

Karar verme süreci bazı optimizasyon kriterleri altında optimal sonuçlar ortaya çıkaracak şekilde alternatif faaliyet veya hareket tarzları arasından birinin seçilmesi işlemidir. Hedef kitlelerin koşullarından ortaya çıkan ihtiyaçlara bağlı hassasiyetleri ve buna bağlı “etkilenebilme derecesini” bulabilmek ve buna uygun ürünleri geliştirerek hedef kitleyi psikolojik harekât hedeflerini başarmak üzere etkilemek hedef kitlelerin ihtiyaçlarını tatmin için karar verme süreçlerinin çok iyi bilinmesine bağlıdır. Hedef kitlenin ihtiyaçlarını tatmin sürecinde nasıl ve neye göre karar verdikleri hususunda bilgi sahibi olabilmek için “çok kriterli karar verme” konusunda bazı temel bilgilere ihtiyaç vardır. Şimdi sorun, ihtiyaçların tatmini ise bu sorunu tanımlamadan önce mevcut alternatifler ve kriter kümeleri bilinmeli ve ortaya konmalıdır. Ancak bundan sonra seçim süreci başlayabilir (Tabucanon,1989, s.8).

Çok kriterli karar vermeyi karmaşık yapan husus ihtiyaçları tatminde var olan seçim kriterlerinin fazlalığıdır. Tek amaçlı problemlerde çok fazla alternatifler olsa bile çok amaçlı problemlere nazaran bunların çözümü göreceli olarak daha kolaydır. Özellikle hedef kitlenin içinde bulunduğu karmaşık sosyal sistemlerde “çoklu kriter”, “çoklu amaç”, “çoklu özellik” gibi terimler karar durumlarını tanımlamak için kullanılır. Bu terimler genellikle birbiri yerine kullanılmaktadır. Gerçekten de bu terimler için ortak bir tanım bulmak oldukça güçtür. Çok kriterli karar verme; çok amaçlı karar verme veya çok özellikli karar verme model ve teknikleri ile ilgili kabul

edilmiş bir adlandırma olarak ortaya çıkmıştır. Çok amaçlı karar verme metotları çok sayıda alternatif kümesine sahip problemler için kullanılırken, çok özellikli karar verme metotları daha dar kapsamlı alternatifler arasında en iyi olanını seçmek anlamında kullanılır. Bunlardan çok amaçlı karar verme bir optimizasyon tekniğidir; diğer yandan çok özellikli karar verme ise matematiksel programlama teknikleri gerektirmeyen seçenek bulma tekniğidir (Zeleny, 1982, s.26). Örnek olarak, dondurma yemek isteyen bir kişi bu dondurmadan ne kadar ve hangi cinsten satın alacağını düşünmektedir. Bunu yaparken ödeyeceği parayı ve alacağı kaloriyi en aza indirmeye çalışırken bu dondurmadan alacağı hazzı en üstte çıkarmak istemektedir. Bu çok amaçlı bir karar verme işlemidir. Böyle bir sorunla karşı karşıya gelen kişi cüzdanındaki para ve kilo almamayı istemesinden dolayı sahip olduğu kilo sınırlamaları içerisinde yukarıda da görüldüğü gibi üç kriterle fakat neredeyse sınırsız sayıda düşünülebilecek alternatifle yüz yüzedir. Diğer taraftan çok özellikli karar verme kişinin bu dondurmayı dondurma satan ve göreceli daha az sayıda olan alternatif dondurmacılardan hangisinden en iyi temin edilebileceğine karar vermesini sağlayan bir karar verme sürecidir. Bu örnekteki kriterler de kalite, temizlik ve fiyat olabilir.

Çok kriterli karar vermede gerekli koşul birden fazla kriterin bulunmasıdır. Yeter koşul ise kriterlerin çatışıyor olmasıdır. Kısaca şu tanım yapılabilir; bir ihtiyacın tatmini ile ilgili bir sorun söz konusu olduğunda bunu çok kriterli bir problem olarak adlandırmak için en az iki çatışan kriter ve en az iki alternatif çözüm olmalıdır. Eğer bir ihtiyacın tam olarak tatmin edilmesi diğer bir ihtiyacın tam tatminini engelliyorsa kriterlerin çatışma içinde olduğu söylenir. Daha basit bir ifadeyle söylemek gerekirse, bir ihtiyacın tatminindeki artış diğer bir başka ihtiyacın tatmininde azalışa neden oluyorsa ortada “çok ciddi” bir çatışma söz konusudur. Ancak çok kriterli karar vermede kriterlerin “çok ciddi” şekilde çatışması da gerekli değildir; yeter şart kriterler arasında bir çatışmanın var olmasıdır (Zeleny, 1982, s.26).

Çatışma kişisel veya kişiler arası nedenlerle ortaya çıkabilmektedir. Bir otomobil almak isteyen bir şahıs genellikle kendi kişisel tercihlerinden kaynaklanan çatışmalarla yüz yüze gelmektedir. Örnek olarak, ucuz, konforlu, yüksek performanslı ve lüks bir otomobil sahibi olmayı istemektedir. Ama ne yazık ki bütün bu özelliklerin tek bir otomobilde toplanması genellikle mümkün değildir. Benzer bir durum, fakat kişiler arası nedenlerle ortaya çıkan kriterler çatışmasına örnek olarak işe yakın bir evde oturmak isteyen adam ile alışveriş merkezlerine ve çocukların okuluna yakın



bir yerde oturmak isteyen eşi arasındaki tercih farklılıklarından ortaya çıkan kriterler çatışması verilebilir. İhtiyaçların çatışması yanı sıra ihtiyaçlarını tatminini önleyen, geciktiren, sınırlandıran engellenme olgusu ise elde edilmek istenen bir nesneye, ulaşmak istenen belli bir hedefe ulaşma veya bir gereksinimin giderilmesinin önlenmesi durumunda ortaya çıkan olumsuz duygulardır. Bir ihtiyacı gidermeye yönelik bir davranış; bireysel, fiziksel, toplumsal, kültürel nedenlerle bloke edilebilir (Zeleny, 1982, s.26).

Tüm amaçlar vazgeçilebilir, bunlardan bazıları diğerlerinden önemli olsa bile tümü uzlaşma sürecine dahil edilebilir. Bu olasılıklar çözümü bulmadaki zorluğun derecesindeki azalış açısından düşünülerek sunulmuştur. Çoklu kriterlerin önem derecesini değerlendirmede tamamen hedef kitlenin yargılarına bağlı yöntemler kullanılır (Zeleny, 1982, s.25).

Bu yöntemler tek bir kişi veya bir insan grubundan meydana gelen hedef kitleleri içerir. Genel olarak grupların kullandığı yöntemlerde grup üyeleri sorumlu karar vericinin de dahil olabildiği uzmanlar veya özel eğitilmiş bireylerden oluşur. Fikirleri ölçmek veya belirlemek tek bir bireyden bilgi elde etmek ya da belirli bir ilgi alanında uzman olan birçok kişiden gelen girdileri toplamayı ihtiva eder. Bunlardan en basit olan yöntem bireysel uzman görüşüdür. Uzmanlar kullanılarak yapılan araştırma ve paneller fikir ve düşünceleri belirlemede daha iyi bir yoldur. Bireylerden ziyade grupların düşünce, fikirlerini elde etmenin amacı gruba ait düşüncelerin geniş kapsamlı bilgi yetenek ve deneyimin analize dahil edilmesinin sağlanmasıdır (FM 33-1-1, 2003, s.7-10).

Hedef kitle tüm bu kararları verirken mutlaka rasyonel ve matematik doğruluğu tartışmasız kararlar vermeyecektir. İhtiyacımızı tatmin için girdiğimiz bir giyim mağazasında bazı kereler ihtiyacımız olmayan malları da satın alabilmekteyiz. Bizi buna iten sonsuz sayıda faktörler olabilir. Satıcının güler yüzlü davranması, aynı malın diğer mağazalara göre çok düşük fiyatlarla satılıyor olması, malın rengi, albenisi, o anda mağaza ses yayın siteminde çalan bir müziğin bilinç altımızdaki bazı arzuları dürtmesi gibi sonsuz etken faktörler bizi o malın satın alınması sonucuna götürebilmektedir. İşte bu nedenle ihtiyaçların tatmininde hedef kitlenin içinde bulunduğu koşullardan kaynaklanan ihtiyaçlar ve buna bağlı hassasiyet ve etkilenme dereceleri çok iyi analiz edilmeden psikolojik harekât uzmanları da kendi pazarladığı psikolojik harekât ürünlerini deyim yerindeyse satamazlar. Bu yapılan kampanyanın, harcanan kaynakların yoğunluk ve maliyetinden bağımsız olan bir husustur.

## **6. İKNA MESAJLARI**

Aristoteles ikna etmenin doğuştan gelen bir yetenek değil, retorik yoluyla erişilebilen bir kabiliyet olduğunu, bu kabiliyetin ise ikna edici öğelerin gösterilmesi kabiliyeti olduğunu ifade eder (L'Etang, 2002, s. 190). Bireyleri ikna etmek için gerekli olan kanıtlar bir gösteri eşliğinde sunulmalıdır. Bu gösteri ne kadar etkileyici ise bireyler o kadar ikna olurlar. Retorik kanıtlar simgelerin uygun kullanımını içermektedir (Heath, 2004, s.126). Aristoteles “Retorik” isimli eserinde iknanın “ethos”, “logos” ve “pathos” üçlemesiyle sağlanabileceğini belirtir. “Ethos” retoriği kullanan konuşmacının, ikna etmeye çalışan kişinin karakteri, “logos” ikna için mantığı kullanarak gerçeği gösterme ve “pathos” ise ikna edilecek kitlenin duygularına hitap etme anlamına gelmektedir (Aristoteles, 2004, s.38).

İkna edici iletişim ise hedef kitlenin davranışlarında sınırlı değişiklikler meydana getirmeyi amaçlayan faaliyetleri kapsar. İletişim de kişi, grup ve kitleleri hedef alarak onların davranışlarını değiştirmeyi amaçlar. Bireyler ifade ettikleriyle başkalarının kendisini anlamasını ve anladıklarına tepki verilmesini isterler. Birinci sürece iletişim, ikincisine ise ikna adı verilir. İkna edici iletişim, davranış modellerini değiştirmek amacıyla kullanılan bir mesaj alışverişidir (Schram, 1960, s.71).

Hedef kitle analizi sürecinin çıktısı da ikna edici mesajlardır. Hedef kitleyi kendi maksatlarımız doğrultusunda bir fikre, duyguya, tavır ve davranış değişikliğine yönlendirmek için ikna edilmesi tüm psikolojik harekât çabalarının sonucudur. Algı yönetimi, toplum mühendisliği, etki harekâtı gibi bağlama göre farklı isimler alan ikna çalışmaları hedef kitle analizinin hasılasının alınacağı safhadır. Şayet formüle edilen ikna mesajlarıyla hedef kitleden vazifeyi destekleyecek önceden belirlenmiş tepki alınırsa psikolojik hedef ve onun bileşenleri olan destekleyici psikolojik harekât hedefleri başarılmış demektir. İkna mesajları, analiz sürecinde elde edilen bilgiler ışığında belirli temalar veya sembollerle hedef kitlelere iletilir (Ekinci, 2005, s.28).

İkna mesajlarında kullanılan kelime ve cümle yapılarının hedef kitlenin tarih, kültür, coğrafya ve gelenekleriyle uyumlu olması ve propaganda tekniklerini, propaganda prensip ve kaidelerine uyacak şekilde düzenlenmesi istenen tepkinin alınmasında kilit önemdedir. Propagandanın birinci prensibi propaganda yapıyor izlenimi vermemektir. Tema ve sembollerin seçiminde yerel kişi veya uzmanlardan yararlanmak yapılacak

hataların önüne geçmede etkili bir yoldur. Atasözlerimizden “Müslüman mahallesinde salyangoz satılmaz” sözü ikna mesajlarında kullanılan tema ve sembollerin önemini göstermektedir. Çalışma kapsamında olmağı için propaganda teknikleri konusunda değinilmeyecektir, ancak propaganda teknikleri sadece kitaplarda yazan veya literatürde olanlarla sınırlı olmayabilir (Ekinci, 2005, s.29). Bu nedenle psikolojik harekâtın icra edildiğı bölgelere has özelliklerden yararlanarak denemesi yapılmış, uzman görüşü alınmış, ön testi yapılmış yeni propaganda tekniklerinin geliştirilmesine de ihtiyaç bulunmaktadır.

## **SONUÇ**

Psikolojik harekâtın amacı, hedef kitlenin mevcut tutumunu, hazırlayanın amaçlarını gerçekleştirmesinde etkili olacak eylemleri harekete geçirerek değiştirmek ya da kuvvetlendirmektir. Bu amacı gerçekleştirmek için psikolojik harekât uzmanları tutumun ne olduğu, nasıl oluşturuldukları ve davranışlar üzerindeki etkileri ile ilgili çalışma bilgisine sahip olmalıdırlar. Bu soruların cevaplarına ulaşmak için en uygun metot, ilk olarak bireysel motivasyonu incelemek daha sonra da grup davranışlarını gözden geçirmektir. Psikolojik harekât, planlanan veya icra edilen askerî harekâtın psikolojik harekât desteğini sağlamak, seçilen hedef kitlenin duygu, düşünce, tutum, davranışlarını etkilemek veya amaçlar doğrultusunda değiştirmek için, hedef kitle hakkında ayrıntılı, güncel bilgilere ve istihbarata ihtiyaç duyar. Psikolojik harekât istihbaratı, icra edilen harekât faaliyetlerinin psikolojik harekât desteğini sağlamak amacıyla hedef kitlelerin özellikleri, hassasiyetleri, her türlü sosyal, siyasi, ekonomik ve askeri nitelikleri hakkında ihtiyaç duyulan bilgilerin toplanması ve değerlendirilmesi ile ilgilenir. Bu da hedef kitle analiz sürecine bir girdi olarak katkı sağlayacaktır. Hedef toplumla ilgili psikolojik harekât istihbaratı hedef kitlenin mevcut duruma karşı tutumu, şikayetleri, etnik yapısı, hayal kırıklıkları, kullanılan lisan, problemleri, milli heyecanı gibi konuları kapsar. Bu hususların her biri hedef kitle analiz sürecinde elde etmek istediğimiz bilgilerdir. Psikolojik harekât, hedef kitlenin yani temelde insanın düşüncelerine, ya da duygusal yönlerine, moral gücüne yöneltilen çalışmalar olup, bu özelliğı ile yalnızca askeri hedefleri değil, siyasi, ekonomik veya sosyal yapıyı da etkiler.

İstihbarat üretimi psikolojik harekât için en önemli faaliyettir. Uygun bir istihbarat olmadan psikolojik operasyonlar etkin bir şekilde planlanamaz ve başarılı bir şekilde yürütülemez. Karar vericiler, hasmın hareket tarzını

değerlendirmek, muharebe sahasını anlamak ve düşmanın hareket tarzına göre kendi hareket tarzlarını belirlemek için istihbarata ihtiyaç duyarlar. Psikolojik harekât da diğer askerî harekât türleri gibi uygun istihbarata sahip olmayı gerektirir. Psikolojik harekât; zamanında, doğru ve uygun istihbarat gerektirmektedir. Uygun bir istihbarat akışı olmadan, bir psikolojik harekât kampanyası yanlış hedef kitleye yönlendirilebilir veya doğru hedef kitleye yönlendirilse bile aksi yönde hatta istenmeyen sonuçlar doğurabilir.

Psikolojik harekât için istihbarat gereksinimleri, geleneksel harekât türlerinden önemli ölçüde farklıdır. Askeri birlikler, düşman kuvvetlerinin sayıları, savaş düzeni, silah sistemleri ve hareket tarzları hakkında istihbarata ihtiyaç duyarlarken psikolojik harekât birimleri, hasımlarının algıları, görüşleri, tutumları, inançları, duyarlılıkları ve rasyonel ve rasyonel olmayan davranış kalıplarına ilişkin bilgilere ihtiyaç duyarlar.

Bunun yanı sıra, psikolojik harekât istihbaratının toplanma yöntemi de geleneksel istihbarat toplama yöntemlerinden farklılık göstermektedir. Psikolojik harekât için istihbarat halkla sosyal etkileşim, gazeteler, dergiler, kitaplar, akademik yayınlar gibi açık istihbarat kaynaklarından en iyi şekilde elde edilebilir. Hedef kitle analizi, hedef kitlenin temel sorunlarının, endişelerinin ve temalarının tanımlanmasını kapsar. Bu kapsamda hedef kitle analizinin psikolojik harekât istihbaratının üretilmesinde en önemli yere sahip olduğunu söylemek de mümkündür.

Uluslararası güç mücadelesinde durum üstünlüğünü ele geçirmek ve devam ettirmek, milli çıkarların tahakkuk ettirilmesini temin etmek amacıyla milli güç unsurlarının karşılıklı destek içerisinde hedefe teksif ettirilmesi sürecinde milli gücün en dinamik unsurlarından biri olan askeri gücün kullanılmasında hasım üzerinde caydırıcılık sağlamak, bu mümkün olmadığı takdirde risk ve tehditleri bertaraf etmek üzere hasımın etkisiz hale getirilmesi, tarafsız hedef kitlelerin desteğinin sağlanması ve dost hedef kitlelerin tutum ve davranışlarının takviye edilmesinde psikolojik harekâtın etkin planlanıp uygulanması her şeyden önce gereksiz can kaybını önleyecek, kaynakların en maliyet etkin kullanılmasına imkan sağlayacaktır. Hedef kitlenin analiz sürecinde belirlenmesi ve buna bağlı olarak ikna mesajlarının oluşturulmasında en önemli ve kritik unsur söz konusu mesajlarda hedef kitleye verilen bilginin veya yapılan çağrının her zaman “tamamen doğruyu” ifade ediyor olmasıdır. Doğruluğu şüpheli veya dayandırıldığı esasların zayıflığı hedef kitle tarafından ortaya çıkarılabilecek ikna mesajlarının dosta ve dost harekâta vereceği zarar ve kayıpların telafisi

çoğu zaman mümkün olmamaktır. Psikolojik harekât her zaman “doğruyu” söyler, hiçbir şekilde “yalan” haber, bilgi ve çağrı içermez. Halkla ilişkiler, kamu diplomasisi gibi diğer iletişim türlerinden farkı seçilen zaman, yer, yön, maksat ve kapsamdır. Psikolojik harekât bu açıdan hassas ve özel bir iletişim sahasını temsil eder.

Son cümle olarak, gerek devlet çapında uygulanacak psikolojik harp, gerekse askerî harekâtın desteklenmesinde kullanılan psikolojik harekât uygulamaları iç kamuoyuna yönelik iletişimin kapsamı dışında mütalaa edilmelidir.

### **KAYNAKÇA**

- Aristoteles. (2004). *Retorik* (Çev. M. H. Doğan). İstanbul: Y.K.Y.
- Baymur, F. (1994). *Genel psikoloji*. İnkılap Kitabevi.
- Çeşme, A. (2005). *Psikolojik harekât ve PKK: Kanserli mücadelenin kanlı yüzü*. IQ Kültür.
- Daugherty, W. E., Janowitz, M., Pyk, L. W., Schramm, W., Klapper, J. T., Becker, H. & Young, W. R. (1958). *A psychological warfare casebook*. Research Analysis Corp Mclean VA.
- FM 100-6. (2003). *Information operations: Doctrine, tactics, techniques, and procedures*
- FM 33-1-1. (2003). *Psychological operations tactics, techniques, and procedures*.
- FM 3-0, (2008). *Operations*. Headquarters Department of the Army, Washington, DC.
- Ekinci, E. (2005). *Psikolojik harekât hedef kitle analizi*, Gnkur Yayınları, Ankara.
- Goldstein, Frank L. and Benjamin F. Findley, (ed). *Psychological Operations: Principles and Case Studies*. Alabama: Air University Press, 1996.
- Güler, R. (2017). *Güç ve ikna sanatı stratejik iletişim*. İhtimal Dergisi Yayınevi.
- Göksu, T. (2002). Bir psikolojik harekât yöntemi olarak propagandada gözetilmesi gereken temel ilkeler ve medyaya düşen rol. *Türkiye'nin Güvenliği Sempozyumu Bildiriler*, Elazığ
- Gümüş, B. (2000). Terör ve terörle mücadelede psikolojik harekâtın önemi. *Birinci Milletlerarası Doğu ve Güneydoğu Anadolu'da Güvenlik ve*

*Huzur Sempozyumu Bildirileri, Elazığ*

- Healy, K. (2016). A theory of human motivation by Abraham H. Maslow (1942). *British Journal of Psychiatry*, 208(4), 313-323. doi:10.1192/bjp.bp.115.179622.
- Heath, R. L. (2004). *Halkla ilişkiler için retoriksel bir uygulama*. H. Güz ve S. Y. Becerikli (Ed.), *Halkla İlişkilerde Seçme Yazılar içinde* (s. 107–154). Ankara: Alban Tanıtım.
- İyiat, B. (2013). *Zihin kontrolü: Psikolojik savaşın temel ilkeleri*. Kripto Basım Yayım, Ankara
- Joint Publication 3-53 5 (2003). *Doctrine for joint psychological operations*
- Kalelioğlu, O. (2002). Psikolojik harp istihbaratı. *Avrasya Dosyası-İstihbarat Özel*, 8, 100-108.
- Korkut, R. (1975). *Psikolojik savunma*. TC. Ulaştırma Bakanlığı, Ankara.
- Le Bon, G. (2017). *Kitleler psikolojisi*, Hayat Yayınları, Ankara.
- L'Etang, J. (2002). *Halkla ilişkiler ve retorik*. J. L'Etang ve M. Pieczka (Ed.), *Halkla ilişkilerde eleştirel yaklaşımlar içinde* (s. 189–213). Ankara: Vadi Yayınları.
- McElroy, D. M. PSYOP the Invisible Battlefield. *Military Intelligence Professional Bulletin*. 16(3), pp. 22-25.
- Katz, P.P. (1982). *Intelligence for psychological operations*. Ronald D. McLaurin, ed., *Military Propaganda. Psychological Warfare and Operations*, New York, Praeger, içinde
- Özdağ, Ü. (2013). *İstihbarat teorisi*. Kripto Yayınları, Ankara.
- Schram, W. (1960). *Mass communications*. University of Illinois Press, Illinois.
- Tabucanon, M. T. (1989). *Multiple criteria decision making in industry*, Elsevier Science Ltd, ISBN-10 044470541-4:
- Tarhan, N. (2003). *Psikolojik savaş*. Timaş Yayınları.
- TDK. (2022). *Psikolojik savaş*. Erişim tarihi: 22 Haziran 2022, <https://sozluk.gov.tr/>
- Yıldırım, N. (2007). *Psikolojik savaş teknikleri: Kore ve Irak örneği*. IQ Kültür Sanat Yayıncılık.
- Zeleny, M. (1982) *Multiple criteria decision making*, McGraw-Hill, New York, ISBN 0070727953, 9780070727953.



# İ Ç A D

İstihbarat Çalışmaları ve Araştırmaları Dergisi  
Journal of Intelligence Research and Studies  
Cilt/Volume:2 Sayı/Issue:1 Yıl/Year: 2023 Ocak/January  
ISSN 2822-3349 (Basılı- Print) ISSN 2822-3357 (Çevrimiçi- Online)

## Araştırma Makaleleri

- ❖ Stratejik İstihbarat Analizini Anlamak: Bilimsel Araştırma ile Benzerlikleri ve Farkları / *Understanding Strategic Intelligence Analysis: Similarities and Differences with Scientific Research*  
Müberra HUDOĞLU
- ❖ 21'nci Yüzyılda Açık Kaynak İstihbaratı / *Open Source Intelligence in the 21<sup>st</sup> Century*  
Tolga ÖKTEN
- ❖ Dijital Çağda İstihbarat Analizi / *Intelligence Analysis in The Digital Era*  
M. Hayati TABAN ve Emre AYDİLEK
- ❖ Sinyal İstihbaratı Analizi Bağlamında Bir Değerlendirme: Rubicon Operasyonu ve Türkiye / *An Evaluation in the Context of Signal Intelligence Analysis: Operation Rubicon and Türkiye*  
Semih SEVİNÇ

## İnceleme Makaleleri / Review Articles

- ❖ Psikolojik Harekât İstihbaratında Bir Analiz Yöntemi: Hedef Kitle Analizi / *An Analysis Method in Psychological Operations Intelligence: Target Audience Analysis*  
Ediz EKİNCİ

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