**İstihbarat Çalışmaları ve Araştırmaları Dergisi**

**Journal of Intelligence Research and Studies**

**Ocak 2023, Cilt: 2, Sayı: 1, ss.68-81**

**January 2023, Volume: 2, Issue: 1, pp.68-81**

**ISSN 2822-3349 (Basılı/Print)** **ISSN 2822-3357 (Çevrimiçi/Online)**

**Makaleye ait Bilgiler / Article Information**

Araştırma Makalesi / Research Article

Makale Başvuru Tarihi / Application Date : 29 Aralık 2022 / 29 December 2022

Makale Kabul Tarihi / Acceptance Date : 16 Ocak 2023 / 16 January 2023

**Makalenin Başlığı / Article Title**

Sinyal İstihbaratı Analizi Bağlamında Bir Değerlendirme: Rubicon Operasyonu ve Türkiye

An Evaluation in the Context of Signal Intelligence Analysis: Operation Rubicon and Türkiye

**Yazar(lar) / Writer(s)**

Semih SEVİNÇ

**Atıf Bilgisi / Citation:**

Sevinç, S. (2023). Sinyal İstihbaratı Bağlamında Bir Değerlendirme: Rubicon Operasyonu ve Türkiye. *İstihbarat Çalışmaları ve Araştırmaları Dergisi*, 2(1), ss.68-81, DOI: http://dx.doi.org/10.29228/icad.11

Sevinç, S. (2023). An Evaluation in the Context of Signal Intelligence Analysis: Operation Rubicon and Türkiye. *Journal of Intelligence Research and Studies*, 2(1), pp.68-81, DOI: http://dx.doi.org/10.29228/icad.11

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

İstihbarat Çalışmaları ve Araştırmaları Dergisi-İÇAD, 2023, 2(1) Araştırma Makalesi
Journal of Intelligence Research and Studies-İÇAD, 2023, 2(1) Research Article
DOI: http://dx.doi.org/10.29228/icad.11

# 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 fazlalaşmasıyla 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 bulunduran 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 bilgilerini 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) konumda olduğu görülmektedir. Bu kapsamda Türkiye gelişmekte 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 hususta bahsetmiştir (Borek, 2019, s.807): eleştirel değerlendirme ve içsel anlamlandırma. Bu bağlamda, analizin ayrılmaz parçaları olarak bilginin anlamlandırılması ve değerlendirilmesi gösterilebilir.

Yapılandırılmış analiz teknikleri yanılgı, sınırlama ve tuzakların analizdeki olumsuz etkisini en aza indirgemek 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 (sebep ve etki değerlendirmesi), 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 temelinin yeniden değerlendirilmesini sağlar.

Tanımlayıcı teknikler uygulanırken ortaya çıkarılan geçmişi açıklama ve geleceği tahmin etme çalışmaları sebep ve etki (neden ve sonuç) ilişkisine dayanmaktadır. Analizci için bu tür çalışmaların zor olmasının sebebi, üzerinde durulan değişken türleri arasındaki ilişkilerin teori geliştirmeye uygun olmamasıdır. Bu sebeple analizcinin bilinçli bir yargı ortaya koyması, konusundaki uzmanlığa ve akıl yürütme becerisine bağlıdır.

Sebep ve etki değerlendirmesi olarak da bilinen tanımlayıcı teknikler arasında bulunan başlıca analiz teknikleri şunlardır (Heuer ve Pherson, 2011, ss.143-144): yapılandırılmış analoji, kırmızı başlık analizi, rol oynama, dıştan içe düşünme, politik sonuç tahmini ve temel varsayımların kontrolü. Bu teknikler arasında analizcilerce önemli olarak görülen ve en doğru sonuçları verdiğine 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 sebep olan kritik faktörlerin açıklanması, araştırma sorusuna yönelik olarak geniş çaplı düşünülmesi, ana faktörler arasındaki bağlantıların ortaya çıkarılması, belirli bir varsayımdan vazgeçmeye neden olan etmenlerin tanımlanması, değişen 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 bağlantılar keşfedilir. Bir

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

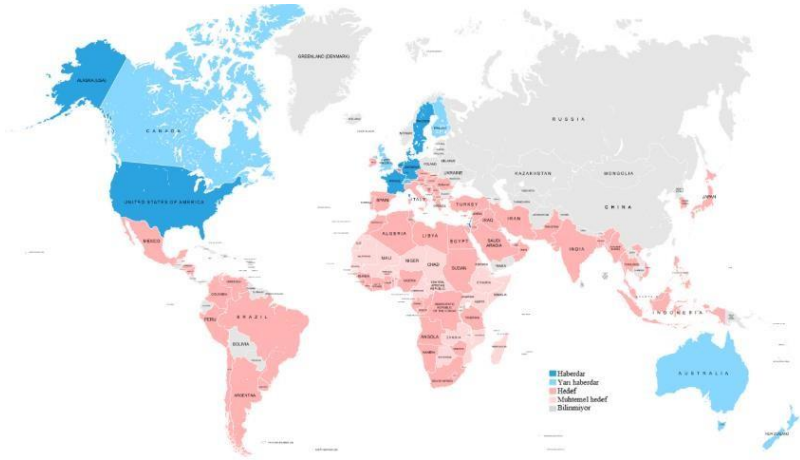
## 1. RUBICON OPERASYONU

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 maksadıyla 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 maksadıyla 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 ülkelerce 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 bulunulduğu 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 ulaşılabileceği unutulmamalıdır. Ayrıca kritik tesislerde akıllı telefon bulundurulmaması, sosyal medya kullanımına özen gösterilmesi, az ve güvenilir uygulama veya aplikasyonların 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 koordinasyonuyla 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 crysis 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: 20.01.2022Belge Nu: A66948.

Heuer, R. ve Pherson, R.H. (2011). Structured analytic tecniques 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-cryptoencryption-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 ınterest. Yayınlanma tarihi: 19.09.2012.

Erişim tarihi: 21.02.2022. Dankwart A.Rustow.

Shane, S. ve Bowman, T. (1995). Rıggıng 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-tragoedieeinestechnikers/story/ 24215009.

U.S. (2009). A tradecraft primer: structured analytic techniques for ımproving ıntelligence 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.