İSTANBUL TOPKAPI ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KAMU GÜVENLİĞİNDE AÇIK KAYNAK İSTİHBARATININ FONKSİYONU VE ÖNEMİ: SILK ROAD VE TAP ÖRNEĞİ

YÜKSEK LİSANS TEZİ

DOĞAN ÇELİK

Güvenlik Bilimleri Anabilim Dalı
Güvenlik Bilimleri Ve Uygulamaları Bilim Dalı

TEMMUZ, 2023

İSTANBUL TOPKAPI ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

KAMU GÜVENLİĞİNDE AÇIK KAYNAK İSTİHBARATININ FONKSİYONU VE ÖNEMİ: SILK ROAD VE TAP ÖRNEĞİ

YÜKSEK LİSANS TEZİ

DOĞAN ÇELİK
20220701004

Güvenlik Bilimleri Anabilim Dalı
Güvenlik Bilimleri Ve Uygulamaları Bilim Dalı

Tez Danışmanı: Doç.Dr. Zeynep Banu DALAMAN

TEMMUZ, 2023

ONAY

İSTANBUL TOPKAPI ÜNİVERSİTESİ | LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

…./…./2023

YÜKSEK LİSANS TEZ ONAY FORMU

Güvenlik Bilimleri Anabilim Dalı, Güvenlik Bilimleri Tezli Yüksek Lisans Programı 20220701004 numaralı öğrencisi **Doğan ÇELİK'in "KAMU GÜVENLİĞİNDE AÇIK KAYNAK İSTİHBARATININ FONKSİYONU VE ÖNEMİ: SİLK ROAD VE TAP ÖRNEĞİ"** konulu Yüksek Lisans tezi Enstitümüz Yönetim Kurulunun 07/06/2023 tarihli ve 2023/08 sayılı Yönetim Kurulu kararıyla oluşturulan jüri tarafından oybirliği/oyçokluğu ile 04/07/2023 tarihinde kabul edilmiştir.

	Unvan	Adı Soyadı	Üniversite	İmza
		ASIL ÜYELER		
Danışman	Doç. Dr.	Zeynep Banu DALAMAN	İstanbul Topkapı Üniversitesi	
1. Üye	Dr. Öğr. Üyesi	Suat DÖNMEZ	İstanbul Topkapı Üniversitesi	
2. Üye	Doç. Dr.	Rüştü Salim Savaş BİÇER	İstanbul Nişantaşı Üniversitesi	
		YEDEK ÜYE		
1. Üye	Dr. Öğr. Üyesi	Gökhan AK	İstanbul Topkapı Üniversitesi	
2. Üye	Doç. Dr.	Hüdayi SAYIN	İstanbul Yeni Yüzyıl Üniversitesi	

ONAY
Prof. Dr. Özlem KUNDAY
Enstitü Müdürü

(*) Oybirliği/Oyçokluğu hâli yazı ile yazılacaktır.
(**) Kabul / Ret veya Düzeltme kararı hâli yazı ile yazılacaktır.

AKADEMİK DÜRÜSTLÜK BEYANI

Yüksek Lisans Tezi olarak sunduğum "Kamu Güvenliğinde Açık Kaynak İstihbaratının Fonksiyonu ve Önemi" başlıklı çalışmanın, bilimsel ahlak ve geleneklere uygun olarak tarafımdan yazıldığını, yararlandığım eserlerin tamamının kaynaklarda gösterildiğini ve çalışmam içerisinde kullanıldıkları her yerde atıf yapıldığını belirtir ve onurumla doğrularım.

Haziran 2023

Doğan ÇELİK

TEŞEKKÜR

Tez çalışmam ve öğrenim sürecimde çalışmalarımıza liderlik yapan Güvenlik Bilimleri Anabilim Dalı Başkanı Sayın Dr. Suat Dönmez'e; fikir ve tecrübesi ile bütün aşamalarda titizlikle ve hassasiyetle yol gösteren kıymetli Danışman Hocam Sayın Doç. Dr. Zeynep Banu Dalaman'a, gerektiği her alanda bize destek olan Araştırma Görevlisi Muhammet Özcan Hocama, öğrenim gördüğümüz süre içerisinde derslerimize giren, ayrıca jüride yer alan hocalarımıza da şükranlarımı sunarım.

Doğan ÇELİK

İÇİNDEKİLER

KISALTMALAR LİSTESİ

ABD : Amerika Birleşik Devletleri
AİHM : Avrupa İnsan Hakları Mahkemesi
AR-GE : Araştırma Geliştirme
ASALA : Ermenistan'ın Kurtuluşu için Ermeni Gizli Ordusu
ASCOPE : Alan, Yapı, Yetenek, Organizasyon, Birey, Olaylar
BBC : British Broadcasting Corporation /Britanya Yayın Kuruluşu
BM : Birleşmiş Milletler
BND : Bundesnachrichtendienst /Almanya Federal Haber Alma Servisi
CIA : Central Intelligence Agency /Merkezi İstihbarat Teşkilatı
CULINT : Cultural Intelligence/ Kültürel İstihbarat
CYBINT : Siber İstihbarat (Cyber Intelligence)
DAEŞ : Irak Şam İslam Devleti
DCRI : Direction Central edu Renseignement Interieur/ İçişleri İstihbarat Merkez Başkanlığı
DEV-SOL : Devrimci Sol
DHKP-C : Devrimci Halk Kurtuluş Partisi-Cephesi
DNI : Dırektor of Natıonal Intelligence / Ulusal İstihbarat Direktörlüğü
DSÖ : Dünya Sağlık Örgütü
ELINT : Electronic Intelligence / Elektromanyetik İstihbarat
FARC : Fuerzas Armadas Revolucionarias de Colombia / Kolombiya Devrimci Silahlı Güçleri
FBI : Federal Bureau of Investigation / Federeal Soruşturma Bürosu
FETÖ : Fetullahçı Terör Örgütü
FININT : Financial Intelligence / Finansal İstihbarat
FISINT : Foreign Instrumentation Signature Intelligence /Yabancı Alet İstihbaratı
GCHQ : Government Communications Headquarters / Hükümet İletişim Merkezi
GEOINT : Geospatial Intelligence / Jeo-Uzamsal İstihbarat
GFT : Google Flu Trends / Google Grip Trendleri
GPHIN : Global Public Health Intelligence Network / Küresel Halk Sağlığı İstihbarat Ağı
GPS : Global Positioning System /Küresel Konumlama Sistemi
HDRAS : Hazard Detection and Risk Assessment System /Tehlike Tespiti ve Risk Değerlendirme Sistemi
HTS : Historical Traffic Search / Geçmiş Trafik Araması
HUMINT : Human Intelligence / İnsan İstihbaratı
IDF : Israel Defense Forces / İsrail Savunma Kuvvetleri
IMF : International Monetary Fund /Uluslararası Para Fonu
IPB : Intelligence preparation of the battlespace /Savaş Alanı Hazırlık İstihbaratı
IRINT : Infared Intelligence / Kızılötesi Işın İstihbaratı

IRTPA : Intelligence Reform and Terrorism Prevention Act / İstihbarat Reformu ve Terörizmi Önleme Yasası
IXP : Internet Exchange Point/ İnternet Değişim Noktası
İHA : İnsansız Hava Aracı
JCAG : Justice Commandos for the Armenian Genocide / Ermeni Soykırımı Adalet Komandoları
KGB : Komitet Gosudarstvennoy Bezopasnosti / Devlet Güvenlik Komitesi
LASINT : Laser Intelligence /Lazer İstihbaratı
MASINT : Measurement and Signature Intelligence / Ölçüm ve İmza İstihbaratı
MI6 : Military Intelligence, Section 6 /Birleşik Krallık Askeri İstihbarat, Sektör 6
MİT : Millî İstihbarat Teşkilâtı
NATO : North Atlantic Treaty Organization /Kuzey Atlantik Antlaşması Örgütü
NLP : Natural Language Prosessing/ Doğal Dil İşleme
NSA : Natıonal Security Agency/ Ulusal Güvenlik Ajansı
NSC : National Security Council /Ulusal Güvenlik Konseyi
OCI : Office of Coordinator of Information/ Haber Alma Eşgüdüm Bürosu
OSINT : Open Source Intelligence/ Açık Kaynak İstihbaratı
OSS : Office of Strategic Services /Stratejik Servisler Ofisi
OWI : Office of War Information /Savaş Bilgi Ofisi
PHEIC : Publıc Health Emergency of international Concern/ Uluslararası Halk Sağlığı Acil Durumu
PKK : Partiya Karkerên Kurdistanê /Kürdistan İşçi Partisi
PMESII : Politik, Askeri, Ekonomik, Sosyal, Enformasyon ve Altyapı
PRISM : Planning Tool for Resource Integration, Synchronization, and Management /Kaynak Entegrasyonu, Senkronizasyon ve Yönetim için Planlama Aracı
RADINT : Radar İstihbaratı
SARS : Severe Acute Respiratory Syndrome / Şiddetli Akut Solunum Yolu Sendromu
SBTF : Yedek Gönüllü Görev Gücü
SETA : Siyaset Ekonomi ve Toplum Araştırmaları Vakfı
SIGINT : Sıgnals Intelligence /Sinyal İstihbaratı
SNA : Social Network Analysis /Sosyal Ağ Analizi
SOCINT : Social-Cultural Intelligence / Sosyo -Kültürel İstihbarat
SOCMINT : Social Media Intelligence / Sosyal Medya İstihbaratı
STK : Sivil Toplum Kuruluşları
STM : Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.
TAP : Terörizm Analiz Platformu
TECHINT : Technical Intelligence / Teknik İstihbarat
TERAM : Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi
UAÖ : Uluslararası Af Örgütü (Amnesty International)
URL : Uniform Resource Locator / Tek Düzen Kaynak Bulucu
YPG : Yekîneyên Parastina Gel / Halk Koruma Birlikleri

ÖZET

KAMU GÜVENLİĞİNDE AÇIK KAYNAK İSTİHBARATININ FONKSİYONU VE ÖNEMİ: SİLK ROAD VE TAP ÖRNEĞİ

İnsan hayatının sosyal olarak günden güne yoğunlaştığı ve etkileşim halinde olduğu yaşadığımız zaman diliminde bireysel akıl ve tecrübe, deneyimsel olarak değişim odaklı bir hat üzerinde ilerlemektedir. Toplumu oluşturan birey sosyolojik olarak doğduğu çevreden, yaşamını sürdürdüğü ortama, kültürel ve politik etkileşimler ile birlikte toplumda nasıl bir konum elde edeceğini belirlemektedir. Dünya nüfusunun ve şehirleşmenin artması ile birlikte daha farklı sorun ve bakış açıları ile yüz yüze kalan birey, teknolojik gelişmelerin hayatına girmesiyle kendisini ya bir suçun faili ya da bir kurbanı olarak bulabilmektedir. Toplum kurallarının geleneksel kültür ve ahlaka göre şekillenmesinin suçu önlemede tek başına yeterli olmadığı görülmektedir. İbn-i Haldun'un bakış açısı ile toplumdan bağımsız olarak düşündüğü ve ayırdığı, bireyin diğer bireylerin saldırılarından korunması amacı ile kurulan 'devlet' kavramı hüküm ve yasalarla birlikte devreye girmektedir. Devlet gerek bireyin ve gerekse toplumun hatta kendi varlığına tehdit unsuru oluşturabilecek tehlikeleri önceden bilmek ve buna bağlı olarak tedbirler almak durumundadır. Kamu güvenliği olarak nitelendirdiğimiz bu durum bireye ve topluma bakan yönü ile devletin meşru sınırlar içinde ve dışında gerek iç hukuk ve gerekse uluslararası hukuktan doğan tüm haklarını kullanarak yaptığı mücadele anlamı taşımaktadır. Çalışma devletin bireye yönelik oluşturulan suç faaliyetlerine karşın yeni nesil tanımı ve mücadele alanlarını, kendisine yönelik olarak oluşan tehdit unsularına karşı önceden bilgi sahibi olma durumunu, yani istihbarat yöntemlerini ve bu yöntemlerden Açık Kaynak İstihbaratını iki örneklem ile ele almaktadır.

Anahtar Kelimeler: *İstihbarat, Güvenlik, Kamu, Açık Kaynak İstihbaratı, Silk Road, Terörizm Analiz Platformu (TAP)*

ABSTRACT

FUNCTION AND IMPORTANCE OF OPEN SOURCE INTELLIGENCE IN PUBLIC SAFETY: SILK ROAD AND TAP

In the time period we live in, where human life is socially concentrated and interacting day by day, individual mind and experience progress on an experiential change-oriented line. The individual who constitutes the society determines sociologically from the environment in which he was born, to the environment in which he lives, what kind of position he will achieve in the society with cultural and political interactions. With the increase in the world population and urbanization, the individual, who is faced with different problems and perspectives in every aspect, can find himself either as a perpetrator or a victim of a crime with the introduction of technological developments. Shaping the rules of society according to traditional culture and morals is not enough to prevent crime alone. The concept of 'state', which was established with the aim of protecting the individual from the attacks of other individuals, which he thought and separated from the society with the point of view of Ibn Khaldun, comes into play together with the provisions and laws. The state has to know in advance the dangers that may pose a threat to the existence of both the individual and the society and even its own existence and take measures accordingly. This situation, which we describe as public security, means the struggle of the state by using all its rights arising from both domestic and international law, within and outside the legitimate borders of the state, with the aspect facing the individual and society. The study deals with the definition of the new generation and the areas of struggle against the criminal activities of the state against the individual, the state of having prior knowledge of the threat elements, namely intelligence methods and Open Source Intelligence from these methods, with two examples.

Keywords: *Intelligence, Security, Public, Open Source Intelligence, Silk Road, Terrorism Analysis Platform (TAP)*

.

1. GİRİŞ

İnsanlık tarihi kadar eski bir zaman diliminde kullanılan istihbarat, uygulama katmanlarının çeşitlenmesi ile birlikte, güvenlik odaklı bir bakış açısı olarak öne çıkmıştır. Geleneksel olarak kabul edilen yöntemler kullanılmakla birlikte, teknolojik gelişmeler istihbarat çalışmalarını yeni boyutlara taşımaktadır. Hayatın hemen her alanında insanlar araştırma amaçlarına göre bir nevi istihbarat çalışması yapmış olmaktadır. Bir iş yeri kurulurken önce konumu, demografik yapısı, bölgede ikamet edenlerin gelir durumu gibi konuları araştırmak aslında bir istihbarat çalışmasını teşkil etmektedir. Yapılan bu araştırmalar karar alma sürecinde verimli bir strateji oluşturulmasına yardımcı olmaktadır. Doğal olarak devletler, kamu kurum ve kuruluşları, özel sektör firmaları da faaliyetlerini sürdürmek amacı ile ihtiyaç, imkân ve vizyonlarına göre istihbarat araştırmaları gerçekleştirmektedir.

Kişisel, sosyal ve kamusal olarak istihbarat hayatın bir parçası olarak önemini sürdürmektedir. Kurumsal olarak istihbarat hem kamunun hem de özel sektörün içerisinde savunma, güvenlik ve terörle mücadele gibi alanlarda faaliyet göstermektedir. Son dönemlerde özellikle dış politikada istihbarat diplomasisi öne çıkmaktadır. Bu nedenle sürekli değişim gösteren tehdit anlayışı güvenlik ve istihbarata olan yaklaşımı dönüştürmektedir. İstihbarat alanında gelişmelerle birlikte yeni zorluklar ortaya çıkmıştır. Şehirleşmenin artması, teknolojinin her birey tarafından erişilir halde olması beraberinde kişiyi ve yaşadığı toplumu da birer hedef haline getirmektedir. Dijital dünya bir kişinin ayak izlerinin izdüşümü olduğu, elde edilen tüm bilgilerin bir strateji oluşturulmasına müsaade edildiği anlamına gelmektedir. Bireysel veya toplumsal karakter seyrini artık yapay zekânın katkısı ile daha öngörülebilir ve analiz edilebilir hale getirilmiş durumdadır.

Özellikle kamuya açık bilgilerin sadece hizmet alımı ve toplumsal rol odaklı değil, tehdit odaklı bir yaklaşımın fırsatı haline getirildiği de yadsınamaz bir gerçektir. Buradan hareketle kamu güvenliğinin ve istihbarata konu olan tüm

bilgi bütününün oluşturulması kapsamında dijital dünyada hiçbir şekilde tümüyle güvende olunmadığını düşünmek ve aynı zamanda güvenliğin sağlanmasında bu faaliyetlerin faydalarını ele almak gerekmektedir. Güvenlik amaçlı veya işlenme amaçlı verilen her izin kişisel özellikleri ile birlikte, ilişkiler ağını yorumlayarak hakkında varsayımlarda bulunan internet ortamı ve içerisinde barındırdığı araçlarla birlikte zafiyetler teşkil etmektedir. Güvenlik amaçlı oluşturulan her bir katman aynı zamanda bir geçiş hattı oluşturmaktadır. Günümüz dünyasının en çok önem atfedilen kavramlarından birisi haline gelen *veri* kavramı bütün güvenlik ve istihbarat çalışmalarının amacını oluşturmaktadır. ‘‘Veriler, kişilere ilişkin enformasyonu, kimin, ne zaman, hangi vesileyle, neyi bildiğini bilmeksizin gönüllü olarak internete konulmaktadır. Ayrıca gönüllü olarak ortalığa saçılan veriler bizzat veri güvenliği kavramını geçersiz kılmaktadır’’ (Chul, 2022, s. 20-21).

Kişisel veriler, ilişki ağları ve iletişim trafiğinden elde edilen veriler internet ortamında ticari veya kamusal amaçlarla ilgili sunuculara servis edilip depolanmakta ve analiz edilmektedir. Amaçların yasal veya illegal yönleri olduğu hesaba katıldığında korunma amaçlı olarak izin verilen her uygulama ve teknoloji ürünü aynı zamanda güvenlik problemleri oluşturmaktadır. Bu bakımdan yaklaşıldığında uluslararası ve ulusal koruma kanunları devreye girmektedir ve kamu, tanımak ve düzenli hizmet verebilmek için güvenliği önceleyerek bazı adımlar atmaktadır. Kişisel verilerin özel olması ve hassasiyeti ne kadar önem teşkil ediyor ise, kamunun stratejik bilgilerinin de korunması önem arz etmektedir. İnsanların internet ile daha çok vakit geçirdiği, çocukların %92’sinin online olduğu gerçeği ile karşı karşıyayız. Haliyle her hareketimizde bir veri üretiyor, gerek sosyal medya da ve gittiğimiz hastanede dahi dijital olarak bir kayıt bırakıyoruz. 2014 yılında yaklaşık 205 milyon e-posta gönderimi, Google’da iki milyon arama yapılmış, Apple’dan 47.000 uygulama indirilmiştir. Günümüz zaman diliminde geldiğimiz nokta bizi veri petrolüne her gün bir damla bırakan varlıklar haline getirmiştir. Doğal olarak veriler nerede toplanıyor ise, illegal faaliyet olarak organize suçlar da veri ve saldırı yöntemleri geliştirmektedir. Devletlerin, hükümetlerin dahi çeşitli fiyaskolar ile sonuçlanan örneklerden yola çıkarak bir gün kendilerinin de kurban gideceğini anlamış olduklarını görmekteyiz (Goodman, 2017, s. 125-129).

Enformasyon çağında, kişi, topluluk veya devletlerden toplanan verilerin bir yerde toplanması, depolanması ve güvenliği ayrı bir çalışma ve maliyet gerektirmektedir. Teknolojiyi illegal olarak kullanan faaliyet alanları zaman içerisinde kullanmada dönüşüme ayak uydurarak varlığını devam ettirmektedir. Bu nedenle devletlerin, kamu adına güvenliği sağlaması amacı ile yapacağı ilk faaliyet olarak istihbarat kavramı devreye girmektedir. Kamu adına devlet ilgili organları ile istihbarat ürününü sağlayan fiziki ve teknik tüm çalışmaları gerçekleştirmektedir. "İstihbarat, devletler için vazgeçilmez bir güvenlik sağlama yöntemidir. Günümüz dünya sisteminde devletler birbirleri ile sıcak savaşa girmekten kaçınmaktadır. Bunun yerine vekalet savaşları, ekonomik yaptırımlar ve ambargolar gibi çok çeşitli yöntemleri kullanmaktadırlar. Bu yöntemlerinde hepsinde istihbarat önemli bir rol oynamaktadır" (Kavsıracı ve Demirbaş, 2020).

İnternet üzerinden yapılan ticaretten başlayıp, dolandırıcılığa, terör örgütlerinin militan kazanma yollarına, mali suçlardan dezenformasyona kadar birçok alanda gözetim, denetim ve gerektiğinde müdahil olma gibi misyonuyla hareket etmektedir. Toplumun güvenliği sadece fiziksel olarak değil aynı zamanda psiko-sosyal yönü ile de korunması gerekmektedir. Özellikle sosyal medyanın yadsınamaz yönlendirme gücü toplumsal olaylarda olumlu ve olumsuz anlamda görülmektedir. İnsanın sınırsız istek ve ihtiyaçları tüketim kanallarını da değiştirmiş ve çeşitlendirmiştir. Pandemi süresinde internetten hiç alışveriş yapmayanların bu alışkanlığı edindiği, kurumların veya üniversitelerin eğitim ve sosyal faaliyetlerinde çevrimiçi görüşmelerle faaliyetleri sürdürdüğü görülmüştür. Bu alışkanlıklar hem avantajlı hem de riskli durumlar oluşturmuştur. Uygulamalar üzerinden açılan bir hesabın bilgileri, yapılan bir konferans görüşmesi veya bir sosyal medya sohbet odasında yapılan konuşma ses kaydını ve ekran görüntüsünü kaydetmiş ve ilgili sunucusuna çoktan servis etmiş olacaktır. Bu tür uygulamalar bir araya gelmeden toplantılar yapılabilen bir avantaj, süreklilik ve verimliliği de beraberinde getirmiştir.

İlk bölümde avantajlı ve riskli durumları güvenlik ve istihbarat açısından ele almak için güvenlik çalışmalarının temelini oluşturan istihbaratın kavramsal, teorik, tarihsel yapısı, türleri ve faaliyet alanları incelenecektir. İkinci bölümde

istihbarat çalışmalarında en çok kullanılan alan olan açık kaynak istihbaratını oluşturan veriler ve bilgi toplama yöntemleri, kullanıldığı alanlar, teknikleri ve analizi ele alınacaktır. Üçüncü bölümde açık kaynak istihbaratı iki örneklem üzerinden bakış açısı ile yorumlanacaktır. Dördüncü bölümde bireysel ve kamusal açıdan bakılan örneklem ile açık kaynak istihbaratının her iki tarafa sağladığı bilinç düzeyi diğer bölümlerde işlenen bilgilerle birlikte yorumlanacaktır. Sonuç olarak bireyin açık kaynak istihbaratına konu olan davranış ve tutumlarında ayak izlerinin nerelere kadar uzanabileceği ve bu durumun güvenlik ve analize ne kadar veri oluşturduğu, kamusal açıdan organizasyon yapısına oluşturduğu tehditle istihbarat ve güvenlik kurumlarının müdahalesinin gerekliliği ortaya konulmaya çalışılacaktır.

1.1. Araştırmanın Yöntemi ve Sınırlılıklar

Çalışmada araştırma problemi olarak açık kaynak istihbaratının kamu güvenliği üzerindeki etkisi ABD ve Türkiye örneklerini kapsayacak şekilde ele alınmıştır. Alınan örneklerde literatürde yer alan kitap, makale ve diğer çalışmalar incelenmiş ve tezin teorik altyapısı hazırlanmıştır. Çalışmanın ele aldığı iki ülkede istihbarat örgütlerinin uyguladığı politikalar analiz edilmiştir. ABD örneğinde FBI'nın Silk Road Operasyonu, Türkiye'de Terörizm Analiz Platformu (TAP) tezin örneklemleri olarak tercih edilmiştir. Diğer operasyon ve örnekler tezin zaman, olay ve olgu sınırlarının dışında tutulmuştur. Tezin araştırma yöntemi olarak ele alınan örneklem üzerinden analizlerle daha sağlam bir çerçeve oluşturulmuştur. Yöntem ve sınırlılıklarda çalışma konusunun dışına çıkılmaması için iki örnek üzerinden hareket edilmiş, teorik altyapı ve okumalar gözetilmiştir.

1.2. Problemin Tanımlanması, Araştırma Soruları ve Model

Problem olarak ele alınan açık kaynak istihbarının kamu güvenliği üzerindeki etkilerinin nasıl olduğu olgusu araştırma sorularıyla yakından ilgilidir. ABD örneğinde olduğu gibi finansal işlemler üzerinden yapılan para transferleri uyuşturucu finansmanı için kullanılabilecek bir hale dönüşmüştür. Kamu güvenliğini direkt olarak tehdit eden mevcut durum açık kaynaklardan elde edilen bilgilerle operasyonun gerçekleştirilmesini sağlamıştır. Türkiye

örneğinde ise Terörizm Analiz Platformu (TAP) terör saldırılarının sayı, yöntem ve sıklık derecelerini ölçmektedir. Bu ölçüm sonrası kamu güvenliği açısından ortaya çıkan güvenlik algısı ele alınmış ve açık kaynaklardan alınan verilerin işlevi görülmüştür. Problemin daha sağlam bir zemin ve teorik çerçeve etrafında analiz edilmesi için iki temel soru tercih edilmiştir. "Açık kaynak istihbaratının yeni nesil suçlarla mücadelede etkisi nedir?" ve "ABD ve Türkiye örneklerinin açık kaynak istihbaratındaki yeri ve önemi nedir?"

1.3. Araştırmanın Tercih Edilmesi ve Önemi

Yeni bir yöntem olarak ortaya çıkan açık kaynak istihbaratının kurumlar tarafından daha sık şekilde kullanılması araştırmanın tercih edilme nedenidir. Bu nedenle istihbarat örgütleri açık kaynakları kullanarak birçok suçun önüne geçmiştir. Türkiye ve ABD örneklerinde olduğu gibi açık kaynaklardan alınan bilgi ve veriler önce analiz edilmiş daha sonrasında uygulamaya konarak operasyonlar gerçekleşmiştir. Buradan hareketle yeni bir trend olarak açık kaynaklardan elde edilen bilgilerle yapılan operasyonlar daha önemli hale gelmiştir. Çalışma yukarıda değinilen önem ve bilgiler ışığında tasarlanmış ve tercih edilmiştir. Yapılacak yorum, analiz ve akademik çalışma ile açık kaynak istihbaratına araştırmalarına da katkı sunulması hedeflenmektedir.

1.4. Veri Toplama, Analiz ve Yorumlama

Kitap, makale, internet siteleri ve tez gibi kaynaklardan alınan teorik çerçeve ve bilgiler akademik analiz ve yorumlamalar gözeterek tercih edilmiştir. Araştırma yöntemi olarak alınan model analiz ve yorumlama teknikleri yardımıyla toplanan veri, olay ve olguların işlenmesini sağlamıştır. Özellikle analiz ve yorumlamaların daha sağlam bir zeminde ilerleyebilmesi için güncel uygulama ve vaka örnekleri kullanılmıştır.

2. TEORİK ÇERCEVE VE İSTİHBARAT

2.1. İstihbaratın Etimolojisi ve Tanımı

İstihbarat kelimesi köken olarak ‘hbr’ kökünden türeyen, yine aynı şekilde Arapça bâb kalıplarından olan ‘İstif’al’ babından oluşturularak ‘istihbar’ mastarının çoğulu olup, akıl, zekâ, anlayış, malumat, yeni bilgiler, duyumlar, bilgi toplama ve haber alma olarak açıklanmaktadır (Delibalta, 2019, s. 13). Kavram İngilizce ve Fransızcada ‘Intelligence’ kelimesi ile ifade edilmektedir. İstihbarat, haber ve haber alma kökenli iken Intelligence, Latince anlamak demek olan intelligere fiilinin türevi intelligentia kelimesinden gelmektedir. 14.yüzyıldan itibaren ‘anlayış, akıl, zekâ’, 15.yüzyıl ortalarından itibaren de ‘gizli bilgi’ anlamını kazanmıştır (Yılmazer, 2020, s. 2). İstihbarat, Arapça kelimesinden türeme bir kelimedir. Haber ise olmuş veya olmakta olan bir şeye dair, orada bulunmayan şahıslara eriştirilen bilgidir. Almancada spionage, İngilizcede intelligence ve espionage, Rusçada ‘spionaj’dır. İspiyon kelimesi de buradan kullanılagelmiştir (Ertekin, 2022, s. 52). Diğer bir tanımda ise istihbarat; “örtülü operasyon diye tanımlanan operatif faaliyetlerden ziyade bilginin toplanması ve analizidir. Bu tanım ‘istihbarat çarkı’ denilen çarkın açılımına dayanmaktadır. Yani istihbarat malumatın toplanması, karşılaştırılması, analizi, birleştirilmesi ve yorumlanması sürecinin sonunda ortaya çıkan üründür” (Özdağ, 2020, s. 29-30). Diğer bir ifadeye göre istihbarat terimi, “devletin gizli bilgi toplama faaliyetlerinin yanı sıra istihbaratın diğer iki operasyonel unsuru olan ‘örtülü operasyon’ ve ‘güvenlik istihbaratını da kapsar” (Bezci, 2023, s. 29).

İstihbaratın tanımı, açıklanması ve analizi hakkında yorumlamaları genişletmek mümkündür. En genel tanımıyla kamu kaynakları tarafından bilgi, haber, havadis ve haber alma gibi kavramların bir bütün halinde değerlendirilmesi olarak tanımlanan istihbarat devletler için vazgeçilmez olarak görülmektedir. Kurumlar aracılıyla kendine kurumsal bir kimlik kazanan istihbarat kavramı tasnif, kıymetlendirme ve yorum gibi süreçlerden geçerek

gerekli mercilerin hizmetine sunulmaktadır. Devletlerin birbirleriyle rekabet süreci göz önüne alındığında istihbarat kavramı daha da önem kazanmaktadır. Farklı devletlerarasındaki istihbarat çalışmaları geçmişten günümüze tarihte kritik bir görev üstlenmiştir. Savaş ve barış dönemlerinde de devletleri, kurumları ve bireyleri yakından ilgilendiren istihbarat kavramı birçok alanı içermektedir. Askeri, ekonomik, sosyal ve teknoloji gibi alanları daha geniş bir perspektifle ele alan istihbarat kavramı üretilebilir bilgilerin toplamı olarak karşımıza çıkmaktadır (MİT, 2023).

İstihbarat planlama, araştırma, delilleri toplama, çeşitli akli ve tecrübi ilmi metotlar ile elde edinilen bilgileri sonuçlandırılmasıyla tamamlanmaktadır. Elde edilen sonuçlar birey, kurum veya karar alıcılar tarafından bir değerlendirmeye tabi tutularak gerekli politikaların işleme alınmasını sağlanmaktadır. İnsanlık tarihinin başlangıcından itibaren var olan bir gerçeklik istihbarat faaliyeti tarihte olduğu gibi devlet, birey ve toplumların geleceğinde önemli bir yer işgal etmektedir. Kamunun güvenliğinin yanı sıra bireylerin kişisel hayatlarının korunmasında da kritik bir işlev üstlenen istihbarat kavramı güvenliğin farklı alanlarında vazgeçilmez bir konumdadır. Hedef, hedef olması olası ve direkt hedef olarak lanse edilen bireyin korunmasında, normal hayatın devam etmesinde sağlıklı bilgi akışının istihbarat ile sağlanması ve gerekli önemlerin alınması gerekmektedir. Bu gerekliliğin bir realite haline dönüşmesi istihbarat kurumlarının kurulmasına ve devam ettirilmesine neden olmuştur. Sağlıklı istihbarat üretimi ile daha da önem kazanan bilgi ve iletişimin sağlanması ise devletler için temel bir öncelik haline gelmiştir (MİT, 2023).

Bu açıdan yaklaşıldığında Millî İstihbarat Teşkilâtı (MİT) istihbarat kavramını, süreçlerini ve hedeflerini şu şekilde tanımlamaktadır. "İnsanlık tarihinin başlangıcından bu yana var olan istihbarat faaliyeti, geçmişte olduğu gibi günümüzde devletlerin geleceğinde rol oynatan önemli ve öncelikli faktörlerden biridir. Çünkü bu faaliyet, hedef ve hedef olması muhtemel kişi, grup, örgüt ve devletlerin imkân ve kabiliyetlerini ortaya çıkarmak, muhtemel hareket tarzlarını önceden tespit etmek için yürütülür. Geleceği öngörebilmek, muhtemel sorunlar hakkında önceden bilgi sahibi olabilmek, olayların gerçek nedenlerine ulaşabilmek, ancak sağlıklı istihbarat üretimi ile mümkün olabilir. Haber, ham bilgiyi ifade eder. İstihbaratın üretilebilmesi için ise, sadece

haberin, bilginin ve belgesinin toparlanması yeterli değildir. Elde edilen haberin, bilginin ve belgenin belli bir sistematik içerisinde işlenmesi gerekir. Önemli bir haber, doğru bir şekilde değerlendirilemediği takdirde yanıltıcı sonuçlara varabilir*"* (MİT, 2023).

Bir kamu kurumu tarafından açıkça ifade edilen istihbarat kavramı, süreç ve hedefleri açıklanmaya çalışan olgunun ne kadar önem arz ettiğini gözler önüne sermektedir. Bilgi sahibi olabilmek kavramsal çerçevesinde hareket eden kurumlar bireyleri, vatandaşları ve devletlerin hareketlerini dikkatlice takip etmekte ve istihbarata konu olacak bilgileri ayıklamaktadır. Bu ayıklamanın bir sonucu olarak sağlıklı bilgi, veri ve olgular gerekli şekilde tasniflenebilmektedir (MİT, 2023).

2.2. İstihbaratın Tarihçesi ve Gelişimi

Tezin araştırma soruları ve konusu gereği istihbarat tarihçesi ve gelişimi bölümünde genel bir tarih anlatımı yapılarak Türkiye ve ABD istihbarat teşkilatları işlenecektir. Böyle bir anlatım şeklinin tercih edilmesinde tezin konusu dışına çıkılmaması içindir. Farklı ülke örneklerine tezde fazlaca yer verilmesi konunun anlaşılmasını zorlaştıracağı göz önünde tutulmuştur. İstihbarat bugünkü anlaşılan manaları ile anlaşılmasa da buna benzer özelliklerde özellikler için kullanılmakta idi. Teolojik olarak ilk istihbarat veya casusluk eylemi, İncil'de geçen olay çerçevesinde yılan, casus; Havva, Muhbir; Âdem ise ilk kurbandır. Nuh Peygamberin tufan sonrasında suların çekilip çekilmediğini öğrenmek amacı ile saldığı kuşlar da teolojik birer örnek olarak verilebilir. İlk yazılı istihbarat kaynakları ise Hitit Kitabeleri kabul edilmektedir (Sarı, 2021, s. 802-807).

Mitolojik açıdan eski çağlarda doğrudan istihbarat tanrısı adı altında bir tanrı olmamakla beraber istihbaratı çağrıştıran Yunan mitolojisindeki İris, aynı şekilde yunandan Hermes Trigmegistus ve Budizm'deki Ganeşa karşımıza çıkmaktadır. Gözdeki İris ile gözetleyen İris arasında kelime olarak bir bağ bulunmaktadır. Hermes ise tanrıların en kurnazı ve en hızlısı olarak kabul edilmektedir. Ganeşa ise göbeği, büyük kulakları fil başlı tasviri ile Echelon olarak anımsanan karakterdir (Ünlü, 2022, s. 137). Geleneksel istihbarat olarak nitelendirebileceğimiz istihbarat anlayışı daha çok gizli verilere ulaşmak

anlayışından oluşuyordu. Musa ve Yuşa'nın casuslarının Kenan ülkesine girmelerinden beri, istihbarat operasyonlarının öncelikli amacı, açık kaynaklardan temin edilemeyen bilgileri gizlice elde etmek olmuştur (Andrew, 2022, s. 12).

Tarihte ilk olarak istihbarat mesleği 'gizli bilim' adıyla ilk defa Kral Tutmosis'in Yafa şehrini ele geçirmek amacıyla casuslarını un çuvalıyla gizlemesi olarak başlamıştır. Büyük İskender, Hannibal gibi önemli komutanlar stratejik, taktik ve operasyonel seviyede istihbaratı kullanmışlardır. İstihbarat faaliyetlerinin artması, karşı istihbarat faaliyetlerini de genişletmiştir. Büyük İskender'in kendine özgü bir şifre geliştirerek mesajları özel bir sopa ile tomar haline getirmesi, ancak aynı tip sopa ile açılmakta idi. (Bozkurt, 2021, s. 860).

'Savaş bir hiledir' diyen Hz. Muhammed döneminde ise, İslam Devleti kurulup vefatına kadar geçen süre içerisinde yirmi yedi savaş ve elli askeri akın düzenlenmiştir. Ayrıca örtülü operasyon olarak tabir edilen operasyonlar da gerçekleştirmiştir. Ka'b b. Eşref'in ölümü için ve Muhammed b. Mesleme'yi, Ebu Rafi'nin ölümü için ise; Abdullah b. Atik'i görevlendirerek ekipler göndermiştir. Açıktan bir öldürülme emri ile Esma Bint Mervan için gönüllü olan Ümeyr b. Adi el-Hatmi'yi görevlendirmesidir. Yine Hz. Muhammed döneminde kontr-espiyonaj faaliyeti olarak; üç sahabenin görevlendirilerek sahabeden Hatib b. Ebu Beltea'nın Mekkeli müşriklere yine bir kadın müşrik tarafından gönderdiği mektubun kendisinin takip edilip alınması emrini verdiğini bilinmektedir. Kadında mektup olduğundan emin olunduğundan üstünü arayacağız ikazından sonra iç çamaşırından çıkartıp mektubu verdiği rivayet edilmektedir. (Andrew, 2022, s. 98-104).

Peygamber döneminden sonra Emeviler döneminin kanlı bir şekilde bitmesinin sebebini ise *Berid* raporlarının yani istihbaratın kendilerinden gizlenmesine, analiz sorunlarına ve siyasi istihbaratın ihmal edilmesine bağlanmaktadır. Abbasi döneminde ise el-Cahiz'in 'Sükût ve Memurlar Üzerine' adlı eseri o dönemde yazılmış olması istihbarat teşkilatını çok aktif bir şekilde kullandıklarını göstermektedir. Yine Abbasi döneminde 'Bilgelik Evi' kurulması ilime çok önem gösterildiğini ve bunun sonuçlarından birisi olarak da Kindi'nin kriptoloji konusunda tarihe adının yazılmasını sağlamıştır. İstihbarat

tarihinin dönemlerinden hiçbiri bu dönemde etkilendiği kadar teoloji ve matematikten etkilenmemiş ve yararlanmamıştır. (Andrew, 2022, s. 108-111).

Sun Tzu istihbarat kavramına ve olgusuna farklı açılardan yaklaşarak devletlerin devamlılığı için gerekli olduğuna vurgu yapmıştır. Devletin ve kurumlarının daha sağlam temeller üzerine yükselmesi için vazgeçilmez olan istihbarat savaşların kazanılmasına da yardımcı olmaktadır. Sun Tzu savaş sanatı isimli eserinde istihbaratın ve haber alma mekanizması hakkında birçok yorum getirmiştir. İstihbaratın tarihi ve işlevi hakkında çok önemli bilgiler sunan mevcut yaklaşım günümüzde istihbarat çalışmalarının da temel kitaplarından biri olarak görülmektedir. Tzu, ordular arasındaki savaşlar üzerinden istihbarat kavramına yaklaşmıştır. Savaşı bir sanat olarak gören Tzu askeri istihbaratın önemine dikkat çekmiştir. Düşman kuvvetlerin hareketlerini, tedarik hatlarını ve stratejisini önceden bilmenin savaşı kazanmanın temeli olduğunu savunan Tzu; zaferin istihbarat faaliyetleriyle mümkün olduğunu söyler. Eski Çin yazıtları arasında devletlerin birbirleriyle nasıl istihbarat savaşlarına girdiğinin de bir göstergesi olarak Sun Tzu'nun savaş sanatı kitabı istihbarat çalışmalarına ve tarihçesine büyük katkı sağlamıştır. Tezin araştırma soruları ve konusu açısından Sun Tzu'nun istihbarat kavramına yaklaşımı önem arz etmektedir. ABD ve Türkiye örneklerine Tzu'nun perspektifinden yaklaşıldığında öncü bilgi toplama ve açık kaynakların etkin şekilde kullanımı sağlıklı toplum yapısı için önem taşır. Sanal suçların önlenmesi ve açık kaynaklardan elde edilen bilgilerin verimli şekilde değerlendirilmesi devletin temel görevi olan kamu düzenini sağlamasına da yardımcı olmaktadır (Tzu, 2022, s. 41).

İstihbarat teşkilatlarına duyulan ilgi ve alaka geçmişten günümüze bir merak konusu olarak insanlar tarafından incelenmiştir. Astrolojiye veya duyumlara dayandığı söylenen ilk istihbarat çalışmaları insanların kabile ve devletler halinde örgütlenmesiyle kurumsal hale gelmiştir. Mezopotamya'da kurulan ilk devletlerin birbirleri hakkında istihbarat faaliyetleri yürüttükleri bilinmektedir. Türk devletlerinin tarih sahnesine çıktığı yüzyıllarda da benzer bir eğilim benimsenmiştir. Çin ve diğer komşu devletlerle çatışmalara giren Türk devletleri düşman kuvvetlerin ne yaptıkları hakkında bilgi toplamak için çabalamıştır. Çinliler de benzer bir istihbarat çalışmaları yürütmüştür. Devlet

yöneticilerinin ve üst düzey komutanların kişisel hayatları üzerinden istihbarat faaliyetleri ve bilgi toplama yöntemlerine başvuran Çinliler devletlerin bölünmesini sağlamıştır. Bir istihbarat çalışmasıyla askeri güç kullanılmadan sağlanan başarı savaşların ekonomik maliyetlerinin de azaltılmasına yardımcı olmuştur. Türk devletleri ise Çin ordularıyla savaş meydanlarında karşılaşmadan önce düşman bölgelerinin arkasına öncü kuvvetler göndererek ordular hakkında istihbarat toplamaya çalışmıştır. Moğol, Hun, Japon ve Kore devletlerinde de benzer örnekleri vermek mümkündür (Ertem, 2021, s. 321-322).

Tarihte istihbarat terminolojisinde '*Körüg*', 'çaşıt-çaşut' kelimesi casuslar için, '*Berid*' kelimesi ise getirilen haber için kullanılmıştır. Aynı zamanda 'münhi, münhiyan, sahib-i haber, dil almak*'* gibi sözcükler de kimi zaman casusluğu, kimi zaman haber verme ve haberciliği tarif etmek için kullanılmıştır (Demir, 2021, s. 13-14).

Hunlar, Göktürkler, Selçuklular, Osmanlılar, Zengiler ve Gazneliler gibi birçok Türk devleti istihbarat faaliyetlerinde bulunmuştur. Devletlerin kuruluş, yükseliş ve düşüş dönemlerine göre farklılık gösteren istihbarat faaliyetleri fetih ve savaşların temel başarısını belirlemiştir. Özellikle Osmanlılar Osman Bey döneminden itibaren istihbarat faaliyetlerini çok ciddi anlamda kullanmıştır. Beyliğin kuruluşunda da aktif olarak iskân politikasının belirlenmesi için öncü kuvvetler bilgi toplamak amacıyla bölgeye gönderilmiştir. Başarılı bir istihbarat ve keşif çalışmasının ardından Osman Bey'in babası Ertuğrul Gazi devletin temellerini atmıştır. Martolos ve Voynuk teşkilatlarını kuran Osmanlılar beyliğe karşı iç ve dış tehlikeleri ayrıntılı şekilde inceleyerek istihbarat bilgileriyle hareket etmişlerdir. (Erdem, 2015).

Büyük Selçuklu devletinde de kamu kurumları arasındaki koordinasyon ve düzen için benzer istihbarat teşkilatları kurulmuştur. Osmanlıların yükseliş ve duraklama dönemlerinde daha fazla önem kazanan istihbarat faaliyetleri büyük devletlerin fethedilmesine ve toprakların büyümesine katkı sağlamıştır. Özellikle diğer devletlerin elçileri aracılıyla istihbarat çalışmaları Osmanlılar için sağlıklı bilgilerin hükümdara aktarılmasına yardımcı olmuştur. Sınır boylarında görevli valilerde diğer ülkeler hakkında bilgi, belge ve hareketleri İstanbul'a ileterek bir nevi istihbarat çalışması yürütmüşlerdir. İletilen

risalelerde düşman kuvvetlerin hareketleri önceden tespit edilmiş ve Osmanlı ordusunun önceden hazırlanması sağlanmıştır (Erdem, 2015, s. 323-324).

Osmanlı'da kuruluş dönemi öncesinde istihbarat kurumsallaşmamış olmasına rağmen, yöntem olarak gönüllü casusluk, ulufeli casusluk, dil alma, tüccar ve gezginlerden yararlanma gibi yöntemlerle istihbarat toplanıyordu. Devlet kurulup büyüdükçe elçiler, mühtediler ve maaşlı elemanlarla gelişmeye devam etmiştir. Özellikle Fatih Sultan Mehmet sonrasında devlet politikası haline gelerek casus sayısı artarak devam etmiştir (Eroğlu, 2003).

1779'de Rusya ile imzalanan Küçük Kaynarca antlaşması ile büyük devlet statüsünü kaybeden Osmanlı diplomatik dengelere önceliklere daha fazla öncelik vermeye başlamıştır. Modern silah teknolojisi ile uyumlu şekilde ilerleyen istihbarat faaliyetleri Osmanlı kamu kurumlarının dönüşmesine neden olmuştur. Kaynarca antlaşmasının ardından Rus istihbaratının Osmanlı üzerindeki faaliyetleri hız kazanmıştır. Ancak Osmanlı'da modern anlamda istihbarat teşkilatının kurumu 1839'da ilan edilen Tanzimat Fermanıyla olmuştur. Kurulan istihbarat teşkilatları başarıya ulaşamazken Teşkilatı Mahsusa'nın dizaynı ile modern bir istihbarat altyapısının temelleri atılmıştır (Ünan, 2017).

Karşı istihbarat, bilgilerin gizli şekilde edinimi ve geleceğe hazırlık için kullanılan iletişim bilgileri Birinci Dünya Savaşında devletin askeri gücüne katkı sunmuştur. Gelişen teknolojiyle birlikte istihbarat toplama, ulaştırma ve değerlendirme aşamaları da dönüşmeye başlamıştır. İkinci Dünya Savaşında önemi daha fazla anlaşılan istihbarat teşkilatları Soğuk Savaş döneminde en fazla öne çıkan örgütler olmuştur. Sovyetler Birliği ve ABD arasında gerçekleşen istihbarat savaşları ülkelerin farklı bloklara katılmasını sağlamış ve birçok iktidar istihbarat çalışmalarıyla etkilenir hale gelmiştir (Hasanov ve Katman, 2019, s. 1145-1149).

ABD istihbarat örgütlenme çalışmalarına 1882 yılında Deniz İstihbarat Ofisini kurarak başlamıştır.1885 yılında Askeri Bilgi Bölümü kurulmuştur.1929 yılında Sinyal Kolordusu ihdas edilmiştir.1941 yılında OCI (Office of Coordinator of Information) Haber Alma Eşgüdüm Bürosu oluşturulmuştur. Sonrasında bu oluşum ikiye bölünerek OSS (Office Strategic Services) Stratejik

Servisler Ofisi ve askeri istihbarattan sorumlu OWI (Office War Information) olarak iki birim halinde yoluna devam etmiştir. CIA, II. Dünya savaşı ile birlikte OSS'nin yerini almıştır.1947 yılında Ulusal Güvenlik Yasası ile birlikte Merkezi Haber Alma Teşkilatı CIA ve Ulusal Güvenlik Konseyi (NSC) olarak şekillenmiştir. ABD İstihbarat topluluğu faaliyetleri 2004 yılında çıkarılan IRTPA (Intelligence Reform and Terrorism Prevention Act) kanunu ile 17 farklı istihbarat teşkilatı tarafından yürütülmektedir. İstihbarat üretimi Ulusal İstihbarat Direktörlüğü (DNI) organizasyonunda gerçekleşmektedir. Dış istihbarattan sorumlu CIA direktörü ABD Başkanı tarafından aday gösterilerek, senato kararı ile atanabilir. CIA Operasyon, Analiz, Bilim ve Teknoloji, Destek, Dijital İnovasyon direktörlüklerinden oluşmaktadır. ABD'de iç istihbarat görevi FBI tarafından yürütülmektedir. Her ne kadar iç istihbarat ile ilgileniyor olsa da FBI'ın 1998 yılında Tel Aviv, Varşova, Buenos, Aires, Kiev, Pretoria gibi şehirlerde ofis açtığı görülmüştür (Bozkurt, 2021, s. 866-871).

Çalışmanın konusu gereği FBI tarihine bu bölümde ayrıntılı olarak değinilecektir. FBI, 1905'te Soruşturma Bürosu adıyla kurulmuş bugün ki halini 1935'te almıştır. Eyaletlerde örgütlenmiş yüzlerce ofisi bulunan FBI iç istihbarat ve güvenlikten sorumludur. Yasa dışı her türlü olaya müdahil olabilen FBI, Adalet Bakanlığı ve Ulusal Güvenlik Direktörüne karşı sorumludur. Terörle mücadeleden uyuşturucu kaçakçılığına kadar birçok ulusal tehditle mücadele eden FBI, polis teşkilatından ayrı bir birim ve kuruluş olarak faaliyetlerini yürütmektedir. Ülkenin eyaletler sistemi nedeniyle federal bir kimlik kazanmış olan teşkilat CIA'nin dış operasyonlarına kıyasla iç tehditlerle ilgilenir (FBI, 2023).

Günümüzde Türkiye'de bir devlet kurumu olarak Millî İstihbarat Teşkilâtı (MİT) bulunmaktadır. Türk Silahlı Kuvvetleri ve Türk Polis Teşkilatının da istihbarat birimleri olmakla birlikte en fazla gündemi işgal eden MİT'tir. Terörizm başta olmak üzere birçok alanda istihbarat faaliyetleri yürüten MİT farklı ülkelerde nokta operasyonlarına öncülük yapmaktadır. Bu operasyonlarda istihbarat konu olan birçok türde bilgi toplamaktadır. İstihbaratın kendi içerisinde türlerine göre ayrımı da MİT'in uyguladığı istihbarat uygulamalarında görülebilir (MİT, 2023).

Diğer ilerleyen bölümlerde daha ayrıntılı olarak işlenecek olan istihbarat türleri bu kısımda istihbarat tarihi ve gelişimi için kısaca tanımlanacaktır. İstihbarat seviye ve faaliyetlerine göre iki şekilde ele alınmıştır. Seviyelerine göre istihbarat türleri taktik, operasyonel ve stratejik olarak üç bölümden oluşmaktadır. Faaliyetlerine göre istihbarat ise siyasi, askeri, ekonomik, sosyal, coğrafi, ulaşım, teknolojik, siber, açık kaynak ve sosyal medya olarak alt alanlarda toplanmaktadır. Bu ayrım genel kabul görmüş bir ayrım olarak literatürde yer almaktadır. Tezin konusu gereği örneklem olarak tercih edilen açık kaynak istihbaratı daha ayrıntılı olarak incelenecek olup diğer alt bölümler bilgi amaçlı literatür ve yorumlamalarda kullanılacaktır. Özelikle Türkiye ve ABD örneğinin daha iyi bir şekilde incelenmesi için böyle bir yöntem tercih edilmiştir.

2.3. Seviyelerine Göre İstihbarat Türleri

Bu bölümde seviyelerine göre istihbarat türleri genel tanımlamaları içerecek şekilde ve literatürde yer alan tartışmaları kapsayacak şekilde işlenecektir. Tezin konusu gözetilerek amaç ve kapsam dışına çıkılmayacaktır. Burada yer alan bilgi, tanım ve literatür tartışmaları tezin son bölümündeki yorumlamalar için kullanılacaktır.

2.3.1. Taktik istihbarat

Taktik istihbarat komutanların veya siyasilerin oluşturacağı stratejinin taktiksel olarak nasıl gelişeceğine dair unsurlar olan, düşmanın konumu, fiziki durumu, imkân ve kabiliyetleri, niyetleri ya da hassas noktaları hakkında talep edilen istihbarat bilgileri için planlanır. Savaş stratejilerinin ve taktiklerinin günden güne çok değişkenlik arz ettiği günümüz koşullarında özellikle terörle mücadele ve karşı ayaklanma operasyonlarında taktik istihbaratın önemi artmaktadır (Seren, 2017, s. 272).

Ayrıca terör örgütleri ile mücadele açısından da taktik istihbarat çok büyük önem taşımaktadır. Taktik istihbarata dayalı mücadele, elde edilen istihbarat çerçevesinde anlık veya çok kısa sürede cevap vermeyi gerektiren bir süreç olarak karşımıza çıkmaktadır. Özellikle büyükşehirleri kendileri için

önemli bir saklanma alanı olarak gören terör örgütleri ile mücadelede taktik istihbaratın değeri oldukça yüksektir (Korkmaz, 2018).

Teknolojinin ilerlemesiyle terör saldırılarının mahiyeti ve etki sahası genişlemiştir. Bireysel olarak gerçekleşen saldırılar ABD başta olmak üzere birçok ülkede istihbarat teşkilatları tarafından yakından takip edilmektedir. Bu saldırıların önceden önlenmesi ve kişilerin tespit edilmesi için taktik istihbarat büyük önem arz etmektedir. Mevcut önemin bir göstergesi olarak istihbarat teşkilatları şüpheli buldukları alım, satım, iletişim ve ulaşım gibi birçok alanı takip etmektedir. Seviyelerine göre istihbaratta günümüzde kamu teşkilatlarının daha fazla tercih ettiği bir tür olarak taktik istihbarat birçok saldırının önceden tespit edilmesini sağlamış ve devletin temel görevi olan vatandaşın güvenliğini sağlama işlevini yerine getirmesine katkı sunmuştur (Koca, 2019, s. 2191).

2.3.2. Operasyonel istihbarat

Diğer ülkelerin bir savaş öncesinde amaçlarını, taktik özelliklerini, muhtemel bir savaş anında hareket ve manevra kabiliyetini, alana süreceği asker sayısını silah kapasitesini, kullanacağı sevkiyat planları gibi başlıkları konu edinen istihbarat alanıdır. Taktiksel istihbarat alanına göre daha hacimli bir alanı kapsar. Operasyonel istihbaratın aşamalarından birisi olan Savaş Alanı Hazırlık İstihbaratı (IPB), düşmanın nereden, ne zaman, nasıl saldırabileceğine ilişkin sorulara cevap arar. Bu kapsamda IPB stratejik ve operasyonel istihbaratı birbirine bağlar. Düşmanın tertip ve savaş düzeni, arazi analizi, hava koşulları ve harekât alanındaki demografik yapı gibi birçok alanı kapsamaktadır (Seren, 2017, s. 273). Askeri nitelik taşıyan operasyonel istihbarat günümüz şartlarına uyum sağlayan bir alan olarak karşımıza çıkmaktadır. Teknolojinin gelişiminin hızla arttığı ve yeni nesil teknolojik trendlerin güçlendiği 21. yüzyılda operasyonel istihbarat gelişerek ve önemi artırarak gelmiştir. Özellikle şehir savaşları, terör örgütleriyle mücadele ve dış operasyonların bölgesel olarak önem kazandığı yeni nesil savaş türleri operasyonel istihbaratın tüm kurumlar arasında koordinasyonla yürütülmesi gerçekliğini tekrar gün yüzüne çıkarmıştır. Belli bir hedefe yönelik olarak tanımlanan operasyonel istihbarata günümüzde MİT'in YPG terör örgütüne karşı Suriye'nin kuzeyinde gerçekleştirdiği operasyonları vermek mümkündür (Koca, 2019, s. 2190-2191).

2.3.3. Stratejik istihbarat

Stratejik istihbarat çalışma alanının önemi ve ihtiyaçları değişkenlik arz eden bir kavram olup zaman zaman kurum ve kuruluşlarda farklı alanlar için kullanılagelmiştir. Ancak taktik ve operasyonel istihbarata göre stratejik istihbarat daha şümul bir şekilde ülke güvenliğini ve uluslararası boyutunu ele alarak hareket etmektedir (Hudoğlu, 2023). Tek bir tanım bulunmamakla birlikte, en sade tanımı Goldman şu şekilde yapmıştır: Ulusal ve Uluslararası seviyelerde politikaların ve askeri planların oluşturulabilmesi için gerekli olan bilgidir. Biyografik, telekomünikasyon, coğrafi, siyasi, bilimsel ve teknik istihbarat bu tanım içerisindeki unsurlardandır (Gül, 2015).

Stratejik istihbaratın çok çeşitli toplama vasıtaları olmakla beraber açık kaynak istihbaratı tüm haber toplama kaynaklarının en önemlisi, maliyeti en az ve en güvenli vasıtasıdır. Düşünce kuruluşları veya enstitüler gibi kurum ve kuruluşlar stratejik istihbarat için önemli veriler üretmektedir. Stratejik istihbarat tarihsel olarak, İlk Dönem, Dönüşüm dönemi, Bilimsel Dönem ve Siber Dönem olarak ele alınabilmektedir. (Sarı, 2021, s. 802-807). İlk Dönemde; istihbaratın tarihçesi bölümünde belirttiğimiz Âdem ile Havva, Hz. Nuh bölümleri, yazılı kaynak olarak Hitit yazılı kitabeleri, Hz. Musa'nın Kenan ülkesine gönderdiği casuslar, Firavun III.Tutmosis'in Yafa şehrini gözetlemek için gönderdiği casuslar, Çinliler tarafından Göktürklere karşı kurdukları casusluk örgütü, Hasan Sabbah'ın örgütü Haşhaşiler casusluk yapılarının ilkleri sayılmaktadır.1568 yılında Avrupa'da kurulan ilk gizli servis İngiliz gizli servisidir. Dönüşüm döneminde ise; Fransızların ilk kurumsal yapılarını ordu içerisinde 1855 yılında, İngilizler ise1877 yılında Askeri İstihbarat Örgütünü ve Donanma İstihbarat Örgütünü kurmuşlardır.1913 yılında Almanya,1917 yılında Rusya,1935 yılında Fransa,1947 yılında modern anlamda gizli servis kurulumlarını gerçekleştirmişlerdir. Bilimsel Dönemde ise; amaç yönünden istihbarat örgütlerine amaç bocalaması yaşatan, soğuk savaşın gerçekleştiği casuslar arasındaki savaş olarak nitelendirilen 1945 Yalta ile başlayıp,1991 Rusya'nın çöküşüne kadar olan dönem olarak nitelendirilmektedir. Siber Dönem ise; risk ve tehditlerin sadece askeri olarak tanımlanmadığı, siyasi, ekonomik ve toplumsal her alanı odak haline getiren çalışmalara yön verilen dönemdir. Devlet dışı aktörlerin önem kazandığı, internetin hayatımıza girdiği, sosyal

medyanın aktif olarak kullanıldığı, yapay zekâ ve siber uzayın yaygınlaşması ile birlikte ‘siber ’olarak adlandırabileceğimiz dönem halen devam etmektedir (Sarı, 2021, s. 802-807).

Stratejik istihbarat bir ülkenin nükleer silah üretimi ve bunun gibi uzun vadeli planlamalarına temel oluşturacak istihbarat türüdür. Akademik literatüre 1970’li yıllarda bir tartışma konusu olarak giren ve 1990’lardan itibaren daha fazla öne çıkan stratejik istihbarat günümüzde sıkça başvurulan bir istihbarat türüdür. Bir doktrin olarak taktik ve operasyonel istihbarattan ayrılan stratejik istihbarat kavramı karar alıcılara yöneliktir. Sherman Kent’e göre bu kavram politika yapıcılar ve karar vericilerin rakip devletlere karşı kendi politikalarında sürekli şekilde sahip olması gereken bilgi yaklaşımıdır. Bu yaklaşım İran nükleer faaliyetlerinde olduğu gibi ABD’nin stratejik istihbarat perspektifinde görülebilir. Özellikle nükleer silah elde etmek için uzun yıllardır çalışma yürüten İran’a karşı ABD ve İsrail stratejik istihbarat türü ile operasyonlar gerçekleştirmektedir. İran’ın nükleer silaha sahip olması kendi rejim güvenliği açısından önem arz ederken bölgesel bir silahlanma yarışına neden olabileceği için İsrail ve ABD sürece karşı çıkmaktadır. Ayrıca iki ülke kendi çıkarlarına uygun olmadığını dile getirdikleri İran nükleer faaliyetleri nedeniyle İran’a yaptırım uygulamıştır. Bu yatırımların belirlenmesinde stratejik istihbaratın büyük bir önemi vardır. Toplanan bilgi ve veriler ABD’nin istihbarat kurumlarında işlenerek devletin İran politikasına uzun vadeli olarak etki etmektedir. Ayrıca stratejik istihbarat;

- Savaş ile ilgili bilgilerin önceden alınmasını sağlar
- Yabancı liderleri diplomatik ve askeri olarak etkiler
- Yeni teknolojik trendlerin takibini sağlar
- Diplomatik süreçlerde güçlenme sağlar
- Karşı istihbaratın işlevini ve hedefini belirler (Koca, 2019, s. 2191-2192).

Stratejik İstihbarat, ABD Müşterek Doktrin 2-00’da fonksiyonel açıdan Ulusal ve Harekât alanı olmak üzere ikiye ayrılmaktadır. Ulusal Stratejik İstihbarat; ABD Başkanı, kongre, savunma bakanı, üstü düzey askeri yetkililer,

komutanlar için üretilir. Harekât Alanı Stratejik İstihbarat ise; düzenlenen çeşitli askeri operasyonlar kapsamında müşterek harekatları desteklemek için kullanılır. Taktik, operasyonel veya stratejik seviyede yürütülen operasyonlar kimi zaman kendi alanları dışında sonuçlar doğurabilirler. Dolayısı ile istihbaratın seviyesi arttıkça, istihbaratın ilgi alanı paralel bir şekilde artış göstermekte buna bağlı olarak odaklandığı alan azalmaktadır (Seren, 2017, s. 274).

İstihbarat ile ilişkili, kimi zaman tek başına kimi zaman faaliyet ve seviyelere ilişkin olarak kullanılan bazı kavramlar vardır, bu kavramlar koruyucu güvenlik kapsamında da değerlendirilmektedir.

Ajitasyon: Bir grubu hükümete karşı isyana sevk etmek için yapılan eylem türünü kapsamaktadır.

Beşinci Kol: Düşman bir devletle iş birliği yapmak ve yıkıcı faaliyetlerde bulunmaya hazır etnik, dini ya da hazır etnik, dini ya da ideolojik gruplar için İspanyol iç savaşından bu yana kullanılmaktadır.

Dezenformasyon: Düşman istihbaratını yanıltmak için kasten yanlış haberler yayma ve yanlış bilgiler ile beslemeye denir.

Espiyonaj: Düşman bir devlette icra edilen casusluk faaliyetleri olarak tanımlanmaktadır.

Karşı İstihbarat: İstihbarata karşı koyma ve kontrespiyonaj olarak da tanımlanır. Düşmanların hassas bilgilere ulaşmasını engelleme faaliyetlerini ifade eder. Faaliyetin bu kısmı pasif tedbirleri kapsamaktadır. Daha aktif tedbirler kısmı olarak ise düşmanları aldatmaya yönelik çalışmalardır.

Kontrespiyonaj: Karşı casusluk ve casusluk eylemlerine karşı aktif korunma tedbirlerini ifade eder. Genişletilmiş olarak ise; bireysel, örgütsel, devletsel her türlü oluşum tarafından gerçekleştirilen girişimleri bertaraf etme faaliyetleridir.

Örtülü Faaliyet: Diplomasi ile savaş arasında orta yol olarak gösterilen propagandadan paramiliter eylemlere kadar değişiklik gösterebilen, siyasal olayları etkilemeye yönelik faaliyetlerdir. İnkâr süreci örtülü faaliyet için en

uygun davranış şeklidir, lakin ihmal ile hareket edildiğinde uluslararası politikada ciddi sıkıntılar doğurabilmektedir.

Propaganda: Belirli bir zümrenin her türlü duygu, düşünce, davranış formlarını değiştirmek ve yönlendirmek amacı ile gerçekleştirilen girişimler bütünüdür. (Demir, 2021, s. 13-39).

2.4. Faaliyet Alanlarına Göre İstihbarat Çeşitleri

Çalışmanın bu bölümünde faaliyet alanlarına göre istihbarat çeşitleri tezin konusu, amacı ve soruları çerçevesinden akademik literatürü ve tartışmaları gözeterek anlatılacaktır. Siyasi, askeri, açık kaynak, sosyal medya, ekonomik, bilimsel ve teknolojik, siber, sosyal istihbarat olarak ayrılan faaliyet alanlarına göre istihbaratı daha çok bölümlere ayırmak mümkündür. Ancak araştırmanın konu sınırlamasını gözeterek bu bölüm çok geniş tutulmamıştır.

2.4.1. Siyasi istihbarat

Kişilerden kurumlara gerek politik ve gerekse kültürel alanlara kadar çok geniş bir ağı kapsar ve bu geniş alan siyasi istihbaratın konusudur. Bir ülkede kanaat önderlerinden devlet adamlarına, tarihinden ideallerine kadar farklı görüşler önem arz etmektedir. Bu nedenle siyasi istihbaratın hedeflerinden birisi ülkelerin kaderlerini değiştirme potansiyeline sahip şahısları tespit etmek ve izlemektir (Seren, 2017, s. 277).

Siyasi istihbarat genel hatlarıyla ülkenin geleceğini ilgilendiren bir alan olmakla birlikte farklı partiler tarafından kullanılabilmektedir. Ancak diğer ülkelerin rakip aktörlere karşı uyguladığı bir tür olarak siyasi istihbarat yaygın olarak kullanılmaktadır (Seren, 2017, s. 278).

Hedefteki bir ülkenin siyasal olarak yapısını meydana getiren ve kamunun altyapısını tümüyle ulaşmayı amaçlayan siyasal istihbarat tarihsel olarak çok eski kökenlere dayanmaktadır. Askeri istihbarat ile yakından ilgili olan siyasi istihbarat farklı dönemlerde aynı anlama gelecek şekilde kullanılmıştır. Ancak 20. yüzyılın son çeyreğinde birbirinden ayrıştırılan askeri ve siyasi istihbarat farklı alanlar olarak araştırılmaya başlanmıştır. Siyasi istihbaratın yeterli olmadığı durumlarda askeri istihbarat devreye girmektedir. Özellikle diplomatik temsilcikler aracılıyla toplanan siyasi istihbaratlar ardından askeri hareketlerle

sonuçlanabilmektedir. Kamu kurumları aracılığıyla da yürütülebilen siyasi istihbarat karşılıklı gerçekleştirilen diplomatik ilişkiler yolu ile de gerçekleştirilebilmektedir (Duramaz ve Gökbunar, 2017, s. 53-54).

2.4.2. Askeri istihbarat

Bir ülkede askeri olarak taktiksel, operasyonel ve stratejik her bilgiyi konu edinen istihbarat alanıdır. ABD Savunma Bakanlığı'nın Askerî Terimler Sözlüğü 'ne göre; Hasım veya hasım olması muhtemel tarafların askerî yeteneklerine dair verilerin işlenmesine yönelik istihbarat türü olarak tanımlanmaktadır (Through As Amended, 2016).

İlk devletlerin kurulmasıyla birlikte aktörler arasında bir tür mücadeleye dönüşen orduların konumu, gücü ve etkisi hakkında bilgi toplanması gerekli olmuştur. Roma, Bizans, Tang, Moğol ve Hitit gibi birçok devletin askeri istihbarat topladığı ve askeri varlıklarını alınan istihbarata göre konumlandırdığı bilinmektedir. Modern devlet anlayışının Westfalya antlaşmasıyla tarih sahnesine çıkması askeri istihbarat çalışmalarını daha kurumsal hale getirmiştir. Din ve devlet işlerinin birbirinden ayrılmasını ifade eden Westfalya antlaşması Almanya'da iç savaşa son verirken diplomatik kuralların gelişmesini sağlamıştır. Askeri alana da yansıyan mevcut kurumsallaşma eğilimi ilerleyen dönemde Fransız devriminde düzenli orduların kurulmasını sağlayacaktır. Gelişen teknoloji askeri elitlerin okullar aracılıyla eğitimini daha kurumsal hale getirmiştir. Bu sayede askeri istihbarat bölümleri önem kazanmış ve orduların bilgi, konum ve hareketleri düşman kuvvetler tarafından tespit edilmeye çalışılmıştır. Çok geniş bir alan olan askeri istihbarat tez konusunun sınırları gereği geniş bir şekilde işlenmeyecektir (Tokmakoğlu, 2022).

2.4.3. Ekonomik istihbarat

Bir ülkenin ekonomik içerikli ticari, finansal, uluslararası ekonomi görüşmeleri, anlaşmaları, planları, altyapıları, rezervleri gibi konuları muhteva edinen istihbarat türüdür. İki amaçla yapılır; kendi ülkesinin çıkarlarını diğer ülkelerden üstün tutarak pazar payını genişletmek, refahı yükseltmek ve ülkesinin ticari hacmini diğer ülkelere karşı artırmaktır. Ekonomik istihbarat kavramını farklı yönlerden tanımlamak mümkündür. Literatürde iletişim sistemi, defansif bir gözlem süreci ve iş istihbarat sistemi gibi farklı isimlerle

ifade edilmektedir. Ekonomik istihbarat kavramı finansal sistemlerin teknolojiyle ilerlemesinin ardından daha fazla öne çıkmıştır. Ekonomi politikalarının bir yansıması olarak ortaya çıkan ve devletlerin diğer istihbarat alanlarında olduğu gibi geleceğiyle yakından ilgili olan ekonomik istihbarat yabancıların ülkelere karşı bir silah gibi kullanabildiği bir alandır. Ekonomide toplanan bilgilerle mevcut ülkeyi dezavantajlı duruma düşürülebilen bilgi ve durumu ifade eden ekonomik istihbarat kamu kurumları tarafından dikkatlice takip edilmektedir (Duramaz ve Gökbunar, 2017, s. 53-54).

Ekonomik istihbaratı elde eden ülke rakip olarak gördüğü ülke hakkında araştırma-geliştirme faaliyetleri, dış ticaret hedefleri, üretkenliği ve rekabet gücü hakkında doğrudan veya dolaylı avantaj sağlayabilir. Örneğin İngiltere'nin Osmanlı ve Çin gibi kadim imparatorluklardan elçilikler aracıyla elde ettiği bilgileri kendi ihracat gücünü artırmak için kullandığı bilinmektedir. İngiltere Osmanlı devletinin üretim yapısı hakkında gözlem ve istihbarat çalışmalarıyla elde ettiği bilgilerden hareketle antlaşmalar imzalatmış ve ülkenin teknolojik olarak geri kalmasına önemli bir rol oynamıştır (Duramaz ve Gökbunar, 2017, s. 53-54).

Ekonomik istihbarat sanayi ve işletme casusluğu, rekabet istihbaratı gibi alanlarda ekonomik espiyonaj adı altında gizli bilgilerin çeşitli yöntemlerle ele geçirmek olarak faaliyet göstermektedir. Ekonomik verilerin toplanıp analiz edilmesi ise açık kaynaklardan temin edilmektedir (Altun, 2015). Ekonomik istihbaratta en sık kullanılan disiplinler Humint ve Sigint' tir. Bilgisayarlara izinsiz giriş (*hack*) yöntemleri de kullanılabilmektedir. Tıbbi teknoloji, yazılım teknolojileri, elektronik bankacılık, vb. ekonomik gelişim içeren çalışmaların sözleşme, maliyet, fiyat, pazarlama faaliyetleri gibi alanları ile ilgilenir. Ekonomik istihbarat yapıldığı kadar, casusluğu önleyici faaliyetler de önemlidir.

2.4.4. Sosyolojik istihbarat

Hedef ülkenin sosyal alanda faaliyet gösterdiği kültürel ve demografik yapısını bölgelere göre alışkanlıklarını, toplumsal refleks noktalarını, dini inançlarını ve ayrıştığı noktaları konu edinen istihbarat alanıdır. Toplumsal veya kültürel istihbarat olarak da ifade edilebilen sosyal istihbarat diğer istihbarat türleriyle bağlantılı olacak bilgi toplamayı hedeflemektedir. Toplumun bütün

katmanları hakkında her türlü demografik bilginin elde edilmesi için başvurulan sosyal istihbarat askeri, siyasi ve teknolojik istihbarat türleriyle bir bütün halinde çalışmaktadır. Kamu kurumlarının korumakla yükümlü oldukları kişilerin sosyal hayatlarıyla ilgili çalışmalar yürüten istihbarat örgütleri elde edilen bilgileri ülke geleceğinde kötü amaçla kullanabilmektedir. Sosyal medya üzerinden fikir beyanlarında bulunan bireyler de sosyal istihbarat çalışmalarına maruz kalanlara örnek olarak verilebilir. Sosyal istihbarat kavramı kendi içerisinde taşıdığı önem ile devletlerin ve bireylerin hayatında kritik bir konuma erişmiştir. Ancak istihbarat faaliyetlerini yürüten kurumlar sosyal istihbaratı diğer alanlarla bağlantılı olacak şekilde tercih etmektedir (Miman, 2007).

Geniş bir alanı kapsayan sosyolojik istihbarat; bir toplumun karakteristik özellikleri, demografik yapısı, dini yapısı, kültürel yapısı, iletişim ve takip edilen medya araçları, eğitim, zihinsel yapısı gibi alanlarla ilgilenmektedir. NATO'nun 2014 yılında yayınlanan İnsan Kaynaklı İstihbaratı Mükemmeliyet Raporuna göre; PMESII (Politik, Askeri, Ekonomik, Sosyal, Enformasyon ve Altyapı), Socint (Sosyo-Kültürel İstihbarat), ASCOPE (Alan, Yapı, Yetenek, Organizasyon, Birey ve Olaylar) ve SNA (Sosyal Ağ Analizi)'nin yerel bir operasyon için Kapsamlı Yaklaşım Stratejisi kapsamında birbiri ile entegre düşünülmesi gerektiği vurgulanmıştır (Seren, 2017, s. 285-291).

Kavramsal olarak her ne kadar ayrı bir başlık olarak incelenmese de Kültürel İstihbarat *(*CULİNT) zaman zaman karşımıza çıkmaktadır. Henüz kesin bir ayrım gerçekleşmediğinden Sosyal İstihbarat başlığı altında incelemekte fayda olacaktır. İnsanların ortak inançları, değer, tutum ve davranış biçimleri operasyonel ortamlarda kritik bir öğe olarak yer almaktadır. Kalp ve zihinlerin desteği anlamına da gelmektedir. Kültürel istihbarat olmadan yapılan operasyonların ağır sonuçları olan başarısızlıkla sonuçlanma ihtimali yükselmektedir. ‘‘Neyi, kime, hangi amaçla sorusunu sorar. Düşmanın nasıl hareket edeceğini tahmin etmek, nüfus güvenini ve iş birliğini kazanmak ve insan istihbaratı toplama yeteneğini geliştirmeyi amaçlar. Kültürel istihbarat sayesinde kimlik ve niyetler, yetki ve gücün kimlerin elinde toplandığı ve nasıl kullanıldığı gibi bilgileri önceden elde edilebilmektedir. Örnek olarak Türk Devleti'nin icra ettiği Fırat Kalkanı ve Zeytin Dalı Harekâtı verilebilir. Halkın

desteği ile DEAŞ, PKK, PYD, YPG gibi örgütlere karşı mücadele edilmiştir (Progonati, 2022).

2.4.5. Bilimsel ve teknolojik istihbarat

Geleneksel istihbarattan günümüze istihbaratın teknoloji ve bilimden yararlanarak birçok değişime personel yapısı ve vizyon olarak yatırım yaptığı ve geliştirildiği görülmektedir. Yeni sanayileşme hamleleri de teknoloji merkezli istihbarat çalışmalarını öne çıkarmıştır. Teknolojik altyapının gelişmişliğiyle yakından ilgili olarak bilimsel istihbarat diğer istihbarat türlerinde olduğu gibi ülkenin geleceği için önem taşımaktadır. Elektronik harp sistemleri üzerinden ülkelerin birbirleriyle ilgili istihbarat topladıkları bilinmektedir. Diğer istihbarat türlerinin kalitesi ve verimliliğiyle de alakalı olarak bilimsel istihbarat taraflar arasındaki ilişkileri etkileyebilmektedir. Örneğin Finlandiya Cumhurbaşkanın Sovyet istihbaratı tarafından teknoloji yardımıyla sürekli dinlenmesi sonrası Finlandiya; Sovyetler Birliğini, Birleşmiş Milletler Genel Kurulunda desteklemek zorunda kalmıştır. Teknolojik imkân ve kabiliyetleri iyi kullanabilen devlet ve kurumlar ülke çıkarlarının maksimum düzeyde gerçekleştirilmesine katkı sunabilmektedir. İstihbarat araştırmaları arasında bilimsel ve teknolojik istihbarat diğerlerine kıyasla ülkenin gelişmişlik düzeyiyle yakından ilgilidir. Finlandiya örneğine kıyasla Sovyetler Birliğinin elde ettiği bilgi ve veriler daha sonra ülke cumhurbaşkanının önüne sunularak bir tehdit haline dönüşmüştür. Sovyet istihbaratının teknolojik dinleme sistemlerini bir silah olarak kullanması ülkeye diplomatik alanda önemli bir avantaj sağlamıştır. Bu avantajın daha sonra Sovyetlerin küresel politikalarına destek şekline dönüşmesi siyasi, diplomatik ve askeri istihbarat kaynaklarına kıyasla nasıl avantajlar elde edilebileceğini göstermektedir (Miman, 2007).

2.4.6. Siber istihbarat

Siber uzayda erişim sağlanan ağ, bilgisayar ve cihazlara sızarak hedeflerin bilgisi olmadan içerdiği bilgilere erişim sağlamaktır. Sızma *(hack)* denilen, virüs, trojan, gibi vb. zararlı yazılımlarla sisteme ya da cihaza girip depolama alanlarındaki bilgileri almakla gerçekleşmektedir. Siber istihbarat geleneksel istihbarat yöntemlerinin teknik olarak uygulandığı espiyonaj faaliyetlerinin yeni uygulama sahası haline gelen bir alanıdır. Özellikle istihbarat odaklı olmayıp

doğrudan altyapılara sistemlere saldırı şeklinde de kullanılabilmektedir (Keleştemur, 2019, s. 11).

Siber alanda tehditler dört farklı alanda değerlendirilebilir: İlk olarak yapılan saldırıların arkasında devletlerin olduğu, tehlikeli ve sonuçları itibari ile maliyetli ve yıkıcı olan saldırılar. İkinci olarak ideolojik gruplar eli ile yapılan saldırılar. Üçüncü olarak daha çok maddi getiri elde etmek amacı ile organize suç örgütleri tarafından yapılan saldırılar. Dördüncü ve son olarak da kişisel motivasyonla hareket eden, bilgisayar ve sistemlere izinsiz erişim elde eden bireysel suçlular (hacker) ve hevesleri yüksek gençler tarafından yapılan münferit saldırılardır. Her aşamada tehlikeler ve sonuçlar farklılıklar gösterebilmektedir. Pasif ve aktif olarak nitelendirilen bu saldırıların hiçbiri hafife alınmamalıdır. Siber alanda yapılan saldırıların genel sebeplerin belirlenmesi, ulusal ve uluslararası yasa hükümlerinin oluşturulması, bu alanda faaliyet gösteren devletler ve kuruluşların iş birliği ve şeffaf çalışması, muhtemel bir siber savaşın önüne geçilmesinin yöntemleridir (Dönmez, 2017, s. 16).

Siber istihbarat faaliyetlerine günümüzde birçok birey, kurum ve devlet maruz kalabilmektedir. Örneğin Letonya, Rusya üzerinden yapılan siber saldırılar nedeniyle 48 saat boyunca ülke geneline elektrik hizmeti verememiştir. Kamu kurumları işlevlerini yerine getirememiş, metro sistemleri çalışmamış ve trafik ışıkları fonksiyonlarını sağlayamamıştır. Yapılan siber saldırılar bir istihbarat açığına neden olmuş ve siber güvenliğin ne kadar önemli olduğu kamu kurumları tarafından daha iyi şekilde kavranmıştır. Siber istihbaratın bir diğer önemli alanını yazılımlar oluşturmaktadır. Devlet ordularının haberleşme ağlarında yaşanabilecek casus yazılımlar gelecek dönemde yaşanabilecek savaşların seyrine önemli derecede etki edebilir. Bu nedenle istihbaratın vazgeçilmez bir alanına dönüşen siber istihbarat önemini artırmaktadır (Eom, 2014, s. 137-143).

ABD Savunma Bakanlığı siber alanı bilgisayar sistemleri, telekomünikasyon ağları ve internet ortamı dâhil olmak üzere bilgi teknolojisi ağından oluşan küresel bilgi alanı olarak tanımlamıştır (Öztürk, 2020).

Siber İstihbarat toplama yöntemleri teknolojinin gelişmesi, casusluğun yeni kullanım şekillerinde siber espiyonaj, savaşların değişimi siber saldırılar, illegal terör faaliyetleri siber terörizm ve mücadele şeklinde gelişmiştir. Açık Kaynak İstihbaratı, Big Data, Derin Web, Kripto para ve yapay zekâ siber toplama yöntemlerinde kullanılan araçlardandır (Darıcılı, 2019).

Siber suçlara insan faktörünün karıştığında nasıl bir sonuca ulaşacağına dair bir örnek Rezwan Ferdaus adındaki Bangladeşli göçmen bir ailenin genç yaştaki çocukları gösterilebilir. Fizik okuduğu okuldan mezun olan Ferdaus internette fazla zaman geçirmeye başladıktan sonra El-Kaideye katılma kararı almıştır. Örgütten birileri ile tanıştıktan sonra etrafındaki kafir olarak nitelediği insanlara karşı katil robotlar planlayarak normal bir teröristten farklı bir usülde saldırı planlamıştır. Üç adet İHA alan Ferdaus C-4 patlayıcılar ile donatarak Kongre Binası ve Pentagonu uçurmayı düşünmüştür. İHA'lar karadan GPS sensörleri vasıtası ile uçurulabildiğinden istenilen yere hareket ettirilip çarpma gerçekleştirilebilmektedir. Eylemi yapmadan önce irtibatta olduğu Müslüman şahsın FBI teşkilatına haber vermesi ile eylemi gerçekleştirememiştir. Dron ve robot yazılım ve teknolojileri geliştikçe ve insanların kullanımına sunuldukça kötü niyetlerin de çoğalacağı bir gerçektir (Goodman, 2017, s. 412-415).

2.4.7. Açık kaynak istihbaratı

Açık kaynak istihbaratı veya İngilizce adıyla Open Source Intelligence (*OSİNT*), açık kaynaklardan elde edilen bilgilerin toplanması, analizi ve değerlendirilmesi yoluyla yapılan istihbarat faaliyetidir. *"*Kamunun erişimine açık her türlü basılı veya dijital ortamdan elden edilen bilgiler olarak tanımlanmaktadır. Amerikan Savunma İstihbaratı eski başkanı Korgeneral Samuel Wilson'a göre; İstihbaratın yüzde doksanı açık kaynaklardan gelmektedir, kalan yüzde onu gizli bilgilerden gelmektedir*"* (Akarslan, 2020, s. 55-102). Wilson'un vurguladığı haliyle Televizyon, radyo, gazete, dergi, broşür, bildiri, katalog ve internet üzerinden yapılan her türlü yayın bir açık kaynak istihbaratı olarak değerlendirilebilir. Sadece istihbarat birimleri değil birey, şirket ve diğer aktörlerde açık kaynak istihbaratına günümüzde sıklıkla başvurabilmektedir. Örneğin bir firma yeni bir şube açma kararını vermeden önce saha araştırmalarına dayanacak şekilde açık kaynaktan aldığı bilgilerle hareket edebilmektedir (Erol, 2022).

İstihbarat türleri arasında açık kaynaklardan elde edilen bilgi toplama yeni bir yöntem değildir. Farklı aktörler akademide, iş hayatında, basın taramasında veya ziyaretlerde istihbarat için bilgi toplayabilmektedir. Online olarak internet ortamında bulunan kaynakları tarayarak veya analiz ederek de istihbarat elde etmek mümkündür. Kitap, makale, süreli yayın, reklam ve katalog gibi açık kaynaklarda birer açık kaynak istihbaratın konusudur. Bir istihbarat türü olarak açık kaynak istihbaratı uyguladığı metot açısından her daim doğru bilgiye ulaşım sağlanabileceği anlamını taşımamaktadır. Elde edilen bilgilerin belli bir süreçten geçirilmesi ve uzman kişiler tarafından analiz edilmesi gerekmektedir. Çünkü bilgilerin propaganda, manipülasyon ve dezenformasyon gibi amaçlar doğrultusunda kullanılması yaygın bir tercihtir. Açık kaynaktan elde edilen bilgilerin istihbarat için kullanılmasının temel bir ihtiyaç olarak günümüzde önem kazanması toplama yöntemlerinin de doğru şekilde işlenmesini gerektirmektedir. Bu bağlamda açık kaynak bilgisi ve açık kaynak istihbaratı arasındaki fark öne çıkmaktadır. Açık kaynak bilgisi herkesin elde edebileceği bilgiyi ifade ederken, açık kaynak istihbaratı açık kaynaklarda bulunan verilerin istihbarat ihtiyaçları doğrultusunda kullanılması anlamına gelmektedir (Benes, 2013, s. 22-35). Bu tanımdan hareketle açık kaynakta yer alan veriler istihbarat için kullanılmazsa açık kaynak istihbaratından söz etmek mümkün değildir.

Açık kaynaklarda elde edilen bilgiler tamamlayıcı nitelik taşıdıkları için istihbarat açısından daha az önemli olarak görülebilmektedir. Ancak açık kaynaktan elde edilen bilgilerin birçok olumlu tarafı bulunmaktadır. Maliyet açısından diğer bilgi toplama yöntemlerine kıyasla daha az finansal harcamaya neden olmaktadır. Kolaylıkla ulaşılması ve kaynak çeşitliliğinde birçok fırsat bulundurması açık kaynak istihbaratını öne çıkarmaktadır. Avantajların yanı sıra dezavantajlar olarak sıralanabilecek durumlar da mevcuttur. Bunlara doğru bilgilere ulaşım, yanıltmanın kolay oluşu ve veri ayrıştırmanın zor oluşu örnek verilebilir (Özdal ve Tiryaki, 2020, s. 270-275).

İnternetin dünya geneline yayılması ve sosyal medya platformlarının gündelik yaşamın bir parçası haline gelmesiyle açık kaynak istihbaratı daha fazla önem kazanmıştır. Günlük milyonlarca bilginin birey, kurum ve organizasyonlar tarafından internete yüklenmesi açık kaynaklardan toplanılacak veri çeşitliliğini artırmıştır. Ağ sistemlerine yüklenen ve sosyal medya

platformlarında paylaşılan bilgi ve veriler istihbarat teşkilatları için çok fazla açık kaynağın varlığına işaret etmektedir. Bu sebep nedeniyle istihbarat teşkilatları günümüzde birçok olay, kişi ve kurum hakkında sosyal paylaşım sitelerinden bilgi toplamakta ve alınan bilgileri analiz ederek istihbarat faaliyeti gerçekleştirmektedir. Ancak doğrudan insanlar üzerinden elde edilen istihbarat faaliyeti açık kaynak istihbaratını tamamlayıcı da bir nitelik taşımaktadır (Özdal ve Tiryaki, 2020, s. 274-275).

Web siteleri, portallar, bloglar ve diğer iletişim kanallarının küresel hale gelmesi açık kaynak istihbaratını öne çıkaran diğer etmenler arasında yer almaktadır. Veri toplama ve bilginin işlenmesinde insanlık tarihinde daha önce görülmemiş şekliyle artan mobilizasyon birçok birey ve kurum hakkında açık kaynaklardan daha fazla bilgi edinilmesini sağlamıştır. Google, Microsoft ve Google Earth gibi uygulama ve programlar mevcut bilgilere örnek olarak verilebilir. Kişinin ev, iş ve konum bilgilerine ulaşmak artık daha kolay hale gelmiştir. İstihbarat teşkilatları mevcut gelişen teknolojik gelişmelerden yararlanırken açık kaynaklardan kişinin en sık gittiği konumları bularak operasyonlar gerçekleştirebilmektedir. Böylelikle potansiyel hedef olan kişilerin takip süreci kısalmakta ve maliyetler ciddi anlamda aşağıya çekilmektedir. Ayrıca bloglarda paylaşım yapan kişilerin karakter özellikleri ve fikirleri rahatlıkla istihbarat teşkilatları tarafından takip edilebilmektedir. Bu açık kaynakların yardımıyla terör saldırılarının önüne daha erken geçilmesi sağlamaktadır (Özdal ve Tiryaki, 2020, s. 274-278).

Açık kaynaktan alınan bilgiler çoğu zaman istihbarat değeri taşımayabilir. Ancak maliyet düşüklüğü ve sürekli bilgilere erişme imkânının oluşu istihbarat faaliyetleri açısından açık kaynakların önemini artırmaktadır. Hiçbir bilgi değersiz değildir algısından hareketle açık kaynak istihbaratı rekabet avantajını artıran bir etkiye sahiptir. İkinci bölümde daha ayrıntılı olarak ele alınacak olan açık kaynak istihbaratı tezin araştırma sorularını gözeterek analiz edilecektir. Özellikle iki örneklemin teorik perspektifi ikinci bölümde ele alınan literatürü gözeterek değerlendirilecektir. Böylelikle araştırmaya konu olan Silk Road ve Terör Analiz Platformunun işlevi daha iyi ortaya çıkacaktır.

2.4.8. Sosyal medya istihbaratı

Bu istihbarat türü sosyal medya platformlarında yayınlanan bilgilerin toplanması, analizi ve işlenmesi yolu ile elde edilen istihbarat faaliyetidir. Operasyonel bir tür olan sosyal medya istihbaratı genellikle açık kaynak istihbaratının bir kategorisi olarak değerlendirilir. Sosyal medya istihbaratında veri toplama web tarayıcıları, doğal dil işleme, olay algılama, tutum verileri, duygu analizi ve ağ analizi yöntemleriyle gerçekleşmektedir (Gök, 2021, s. 543).

Sosyal Medya İstihbaratı sahte haberler, yanlış bilgilendirme ve bilgi çarpıtma gibi yöntemleri kullanan terör örgütleri ve üyeleri hakkında da bilgi toplar. Medya ve sosyal medya mecralarında sansasyonel olayların daha çok yayılması terör örgütlerinin işlevselliğini artırmış ve daha geniş kitlelere ulaşmasını sağlamıştır. Terör ve Medya arasındaki bu etkileşime 'simbiyotik' denilmektedir. Terör grupları artık eylemsel değil, ağ tabanlı gruplar olarak değerlendirilmektedir. Birkaç farklı merkezden yönetilebilen iletişim ve karar stratejisi değişen örgüt yapıları savaş koşullarında; troller, botlar ve diğer aktörler ile çalışabilmektedir (Efe, 2023, s. 317-330).

İnternetin ve teknolojinin gelişmesi ile karşılıklı bir iletişim halinde gerçekleşen enformasyon paylaşımına ve etkileşimine sosyal medya denilmektedir (Howard, 2011). Sosyal Medya araçları dünya geneli toplumlarının kullandığı Facebook, Twitter, Instagram, Tiktok, Youtube ve Google gibi platformlardan oluşmaktadır. Kullanıcılar 'Social Technographics' bölümlendirme çalışmasına göre blog, web sitesi yayınlayan, video veya müzik yükleyen, makale ya da hikâye paylaşanlardan oluşmak üzere yedi kategoride değerlendirilmektedir. İnternetin %24'ü yaratıcılar, %33'ü hoşsohbetler, %37'si eleştirmenlerden oluşturmaktadır. %20'si koleksiyonerler grubunda olan internetin, %59'unu katılımcılar grubundadır. İnternet kullanıcılarının %70'i ise spekülatörler grubunda olup, aktif olmayanlar %17'lik grubu teşkil etmektedir (Cirit, 2021, s. 539).

Sosyal medya istihbaratı internetin gelişmesinin ardından birey, kurum ve devletler açısından vazgeçilmez bir hal almıştır. Sosyal medya uygulamalarının kamu tarafından kontrolü mümkün değil iken herhangi katılım sınırı da bulunmamaktadır. Terör örgütleri propagandası başta olmak üzere birçok

yasadışı olayın gerçekleşebildiği sosyal medya platformları istihbarat çalışmaları açısından çok önemli hale gelmiştir. Batı ve Doğu'da farklı yaklaşımların benimsenmesiyle daha da kritik hale gelen bilgi ve veri güvenliği sosyal medya platformlarının artmasına neden olmuştur. Çin, Japonya, Rusya, ABD ve Hindistan gibi ülkeler kendi sosyal medya uygulamalarıyla piyasada rekabeti oluşturdular. ABD'de kurulan ve küresel hale gelen Twitter, Instagram ve Facebook gibi uygulamalar milyarlarca kişi tarafından tercih edilmiştir. Birçok ülkede vatandaşların en fazla kullandığı platformlar haline gelen uygulamalar merkezi hükümetlerin kontrolünde olmadığı için açık kaynaklardan bilgi edinmeyi daha kolay hale getirmiştir. Bireylerin gönüllü olarak günlük neler yaptığını paylaştığı platformlar siyasi partiler için seçim döneminde seçmenlere ulaşılacak bir araca dönüşmüştür. Bu dönüşüm sonrası ABD'nin farklı ülkelerde seçimlere müdahil olduğu veya tersi durumların olabileceği gündeme gelmiştir. Vatandaşların konum, veri, duygu, düşünce, olay ve bilgi paylaşımlarını yaptığı uygulamalar günümüzde devlet-vatandaş arasındaki ilişkilerin cehresini değiştirmiştir (Erol ve İstikbal, 2020).

Devletlerin yani sıra firmalarda sosyal medya platformlarından etkilenen aktörler arasında bulunaktadır. Şirketlerin reklam, pazarlama, iletişim ve satış için kullandığı sosyal medya platformları firmalara karşı kampanyaları da tetikleyebilecek konuma ulaşmıştır. Sosyal medyada organize olan müşteriler firmaların imajlarına zarar verebilirken satışlarında düşmesine daha fazla etki edebilir hale gelmiştir. Firmalar rakip firmaları sosyal medya üzerinden takip edebilmekte ve rekabet stratejilerini bu bilgiler ışığında oluşturabilmektedir. Şirketlerin istihbarat ve AR-GE birimleri de rakip firmalar hakkındaki bilgi toplama maliyetlerini düşürerek daha verimli çalışabilmektedir. Örneğin Google, Microsoft, Huawei ve Samsung gibi küresel ölçekteki teknoloji firmaları bilgi güvenliği ve istihbarat çalışmalarına daha fazla önem vermeye başlamıştır. Yeni ürünlerin kopyalanmasının yanı sıra tasarım hırsızlıklarının önüne geçmek amacıyla farklı önlemler almışlardır. Örneğin AR-GE biriminde çalışan ve yeni ürün geliştirmekle sorumlu olanların sosyal medya uygulamalarına girmesi ve kullanması firmalar tarafından ağır yaptırımlarla engellenmektedir (Bural, 2022).

Sosyal medya uygulamaları üzerinden istihbarat çalışmalarından rahatsızlık duyan devletler platformların yasaklanması, kullanımının engellenmesi ve rakip uygulamaların yaratılması gibi çalışmalara başvurabilmektedir. Çinli bir firma tarafından piyasaya sürülen Tiktok birçok devletin hedef aldığı bir uygulamadır. Hindistan, ABD ve Endonezya gibi ülkelerde yasaklanma gibi girişimlere maruz kalan uygulamaya karşı en çok eleştiri istihbarat faaliyetleri üzerinden gelmektedir. ABD kamu kurumları Tiktok 'un kamu çalışanları tarafından kullanımını kısıtlarken Hindistan toplum değerlerine aykırı olması nedeniyle uygulamanın ülke genelinde engellenmesi karar vermiştir. Endonezya'da da benzer bir eğilimle uygulamayı ülkede kısıtladı. Çin merkezli firma iddiaları reddederken birçok ülkede Tiktok en fazla indirilen uygulama haline geldi. Özellikle genç nesiller arasında kullanımı çok yaygın olan Tiktok milyonlarca videonun paylaşıldığı bir platform oldu (Erol ve İstikbal, 2020).

Mevcut örnekleri artırmak mümkün olmakla birlikte tez konusu sınırları gözetilerek diğer tartışmalara çalışmanın son bölümünde yer verilecektir. Ancak Çin'de Batı menşeli uygulamaları kendi ülkesinde yasaklayarak yerel platformları rekabete karşı korumaktadır. Ayrıca ülkede bilgi ve rejim güvenliği açısından yerli sosyal medya platformlarıyla hareket etmektedir. Böylelikle açık kaynaklardan bilgi akışını yurtdışına olabildiğince kısıtlamıştır.

2.5. İstihbaratta Bilgi Toplama Yöntemleri

Bilgi toplama hedef ve kaynak itibari ile ele alındığında yerler, kişiler, örgütler ve nesneler olarak ele alınmaktadır. Bilgi toplama yöntemleri klasik ve modern olarak incelenmiştir. Klasik yöntemler beş türe ayrılmaktadır. Bunlar gözlem, adam kullanma, mülakat, sorgulama, teknik ve elektronik faaliyetlerdir. CIA bilgi toplama yöntemlerini altı başlıkta sınıflandırmaktadır. Bunlar SIGINT, IMINT, MASINT, HUMINT, OSINT, GEOINT (Seren, 2017, s. 267). Mark M. Lowenthal ve Robert M. Clark; ABD istihbarat topluluğunda genelde Osint, Humint, Sigint, Geoint ve Masint'tan oluşan beş disiplinin toplama kaynakları olduğunu belirtmişler Humint ve Osint'ın en demokrat iki istihbarat disiplini olarak tanımlamışlardır (Seren, 2017, s. 268).

2.5.1. İnsan kaynaklı istihbarat

Bilinen en eski bilgi toplama yöntemi olan Humint (Human İntelligence) dilimize İngilizceden geçmiş ve halen kullanılan bir kelimedir. İnsani unsura dayanan açık ve kapalı her türlü alanda faaliyet gösteren insani istihbarat; yabancı karar alma sistemine sızma yöntemi ile yabancı sistemin güç ve zayıflıkları, planları ve amaçları öğrenmek için bilgi toplamaktır. Bu tanıma göre insani istihbarat stratejik istihbarata girer, oysa insani istihbarat operasyonel ve taktik istihbaratta çok yoğun kullanılmaktadır (Özdağ, 2020, s. 116-17).

Teknoloji ve açık kaynak istihbaratın getirdiği kolaylıklara rağmen insan kaynaklı istihbaratın önemini yitirmemesinin nedeni rakibin niyetinin tam olarak bilinmesinin insan kaynaklı istihbarat sayesinde mümkün olmasıdır. Örneğin, insansız hava araçları veya uydu istihbaratı ile alınan bir görüntü, sadece var olan fotoğrafı bize sunmaktadır. Bu fotoğrafta, sınırdan geçen bir gurup terörist görüldüğünde bu gurubun neden hareket halinde olduğu ve ne yapmayı amaçladığı bilinememektedir. Fakat insan kaynaklı istihbarat sayesinde ajanlar vasıtası ile alınacak bilgi sonrasında, gurubun bir köy baskınına mı, erzak almaya mı, yoksa bir terörist eylemde bulunmak üzere mi sınırdan geçiş yaptığı öğrenebilmektedir. Başka bir ifadeyle, insan kaynaklı istihbarat bize terörist gurubun amacını, niyetini öğrenmemiz de yardımcı olurken; teknik istihbarat bize sadece bir gurubun fotoğrafını vermektedir. (Kavsıracı ve Demirbaş, 2020).

İnsan Kaynaklı İstihbarat farklı kimliklerde yapılabilmektedir. Bir doktor, öğrenci, şirket çalışanı, akademisyen, arkeolog vb. gibi meslekler altında devletlerin gizli bilgilerini çalmaya yönelik girişimler yapılabilmektedir. Bunları belirli çatı altında toplamak gerekmektedir. Buna göre insan kaynaklı istihbaratta dört guruptan bahsetmek mümkündür: Teşkilat kadrosunda görev alanlar, Ajanlar, Mutemetler ve Muhbirler. Sonuç olarak, insan kaynaklı istihbarat, tarih boyunca vazgeçilmez bir bilgi toplama yöntemi olarak önemini korumuştur. Her ne kadar, istihbarat servisleri bilginin çoğunluğunu açık kaynaklardan toplasa da bilgi toplama da insana duyulan ihtiyaç devam etmektedir (Kavsıracı ve Demirbaş, 2020).

İnsan unsuru kullanılarak elde edilen toplama yöntemlerinden *Humint*, canlı kaynaklar statüsündedir. 'Elemanlama Faaliyeti' olarak da tanımlanabilir. Elemanlama faaliyeti yöntem olarak iç ve dış hulul şeklinde icra edilmektedir. Hedefe dair bir kişinin çeşitli yollarla elemanlaştırılması 'iç hulul', dışarıdan bir elemanın ilgili hedefin içerisine dahil edilmesi ve bilgi toplanması 'dış hulul 'dür. Elemanlaştırma faaliyeti olarak elemanlaştırılacak olan şahsın mimlenmesi, hakkında tahkikat, yaklaşma ve angaje, sevk ve idare, gerekli durumlara bağlı olarak ilişkinin dondurulması şeklinde yürütülmektedir. Yine aynı şekilde insana dayalı bilgi toplama yöntemlerinde fiziki takip, sızdırma, sorgu, keşif ve gözetleme, tahkikat, provoke etmek gibi metotlar da kullanılabilmektedir (Darıcılı, 2023, s. 155-181).

İnsan kaynaklı istihbarat toplama ve karşı casusluk yöntemlerine İsrail devleti iç istihbarat teşkilatlarından Shin Bet 'in 2 Haziran 2023 tarihinde gizliliğini kaldırdığı dosyada adı geçen Ulrich Schnaft gösterilebilir. Soğuk Savaş dönemi casusluk dünyasına göre Ulrich Schnaft'ın sızma konusunda nadir bir yeteneği olduğu düşünülmektedir. Eski bir Nazi ve Waffen-SS askeri olan Schnaft, 1947'de Yahudi bir mülteci kılığına girmiş ve devlet kurulmadan önceki İsrail'e göç etmeye çalışmış ve sonunda yasadışı göçmenler için kullanılan bir İngiliz toplama kampına girmiştir. Orada Siyonist referanslar edinip İbranice öğrenerek, subay olmak için İsrail ordusuna katılmış, o zaman diliminde Mısır casusu olduğu düşünülmektedir. Onlarca yıl sonra, bu köstebeğin ne kadar derine inmeyi başardığı hala belirsizliğini korumaktadır. İsrail istihbarat teşkilatının henüz gizliliğini kaldırdığı dosya, onun altmış beş yıl önceki eylemlerinin bugün için hala hassas olarak görüldüğünü gösteren kısımlar içermektedir. Dosyada, bu türden tespit edilmiş bir öğe olarak, İsrail'deki ana takma adı Gabriel Zusman olan Schnaft'a ait olarak listelenen en az dört takma adından biri olduğu tespit edilmiştir. Dosya, ideolojik güdümlü toplumlara uyum sağlama ve onları kendi amaçları ve hayatta kalma mücadelesi için kullanma becerisine sahip, fırsatçı, cüretkâr ve bazen de çılgın bir adamın portresini çizmektedir. Aynı zamanda, İsrail karşı istihbaratının, savaşın parçaladığı Avrupa'dan binlerce belgesiz kişiyi karşılayıp savaşlar için askere alındığı ilk yıllardaki uyanıklığını ve meydan okumalarını göstermektedir.

Schnaft, 1954'e kadar İsrail'de sahte bir kimlikle altı yıl yaşamıştır (The Times Of Israel, 2023).

Doğu Cephesinde bir Nazi elit birimi olan Waffen-SS'da eski bir asker olan Schnaft, savaşta yaralanmış ve Amerikan birlikleri onu 1944'te savaş esiri olarak yakaladığı Batı cephesine nakletmiştir. Amerikan uluslararası örgütleri tarafından Yahudi mültecilere sağlanan yardımdan yararlanmak için bir Yahudi kılığına girerek Almanya'yı terk etmeye karar vermiş, savaşın harap ettiği Münih'ten 1947 yılında, yakında İsrail olacak olan, ancak hâlâ Birleşik Krallık tarafından yönetilen ve göç yasağına tabi olan Fransa'nın Marsilya kentinde yasadışı Yahudi göçmenlerden oluşan bir gemiye binmiştir. Gemi İngiliz donanması tarafından durdurulmuş ve yolcuları Kıbrıs'ta bir toplama kampına hapsedilmiştir. Schnaft, İsrail Savunma Kuvvetleri'nin çekirdeğini oluşturan paramiliter Yahudi grup Haganah'la bağlantılı mahkûm arkadaşları tarafından düzenlenen birkaç kaçış girişimine katılmıştır (The Times Of Israel, 2023).

Schnaft daha sonra IDF'ye katılmış ve İsrail'in Bağımsızlık Savaşı sırasında görev yapmıştır. Kudüs yakınlarındaki Kiryat Anavim'de yaşamış ve Başbakan David Ben Gurion'un partisi Mapai'ye üye ve aktivist olmuştur. Schnaft'ın, topçu birliklerindeki hizmeti sırasında subay olduğu bilinmektedir. Ancak kariyer subayı olma talebi engellenmiştir. Shin Bet, sarı saçlı ve tipik bir Alman görünümüne sahip olan Schnaft'ın dini geçmişi hakkında daha fazla soruşturma yapılıncaya kadar bunu veto etmiştir. Temsilcilere Schaft hakkında bir notta "Lütfen bu kişinin diniyle ilgili soruları yanıtlayın" yazmaktadır. İsrail karşı istihbaratının Schnaft'ı ilk olarak 1952'de, onun Yahudi olmadığından şüphelenmeye başladıklarında fark ettiği anlaşılmaktadır. Cesaretinin pervasızlığı ve dosyasındaki bir raporda sarhoşken SS üniforması ve Alman Ordusu üniforması içinde iken bir fotoğrafını gösterdiği anlaşılmakta olup, sorulduğunda sadece bir kostüm olduğunu ifade etmiştir (The Times Of Israel, 2023).

Kendisinden şüphelenildiğini hisseden Schnaft, 1954'te İsrail'den ayrılmıştır. Daha sonra, İsrail Savunma Kuvvetleri hakkında sahip olduğu bilgileri Mısır istihbaratıyla paylaşmayı teklif etmek için Mısır'a gittiği tespit edilmiştir. Karşı istihbarat ajanları, bilgiyi değerli ve düşmanın IDF ile yakınlığına büyük bir katkı olarak tanımlamışlardır. 1955'te MOSSAD,

Frankfurt'ta eczacı olarak çalışan Schnaft'ın yerini bulmuş ve onu İsrail'e geri çekmek için amaçlanan bir operasyon düzenlemiştir. Gazeteci kılığına giren bir kadın ajan onu baştan çıkarmış ve İsrail hakkında sahip olduğu bilgilerle ilgilenecek Arap istihbarat ajanlarıyla tanıştırmayı teklif etmiştir. Schnaft'ı, kendisine İsrail'de sahte bir casusluk görevi ve ülkeye girmesi için sahte bir pasaport veren Arap istihbaratı gibi görünen MOSSAD ajanlarıyla tanıştırmıştır. Schnaft, İsrail'e gittiğinde tutuklanmış ve yedi yıl hapis cezasına çarptırılmıştır. Serbest kaldıktan sonra İsrail'i terk ettiği bilinmektedir. Birkaç gazetecinin Almanya'da ve ötesinde izini sürme girişimleri başarılı olmamıştır. Haaretz'de yayınlanmasının ardından, bir okuyucu olan Asaf Yanai, Schnaft'ın kamuya açık kayıtlarına gizliliği kaldırılmış dosyada olmayan doğrulanmamış bir iddia eklemiştir. Schnaft, Yanai'nin babasıyla Aşkelon yakınlarında devriye gezerken Mısır'dan altı casusu tek başına öldürdüğünü yazmıştır. Yanai, casuslar iki İsrail askerinin dinlenmek için durduğu terk edilmiş bir yapıya sığınırken Schnaft'ın en üst kattan zemin kata inerek casusları hızla öldürdüğünü ve muhtemelen babasının hayatını kurtardığını yazmıştır (The Times Of Israel, 2023).

2.5.2. Finansal istihbarat

Finint (Financial İntelligence) Ekonomi piyasalar başta olmak üzere, finansal piyasalarda gerçekleşen hareketleri, terör örgütlerinin para trafiği, örgütsel ilişki ve yapının deşifre edilmesi, kara para aklama gibi konuları ele alarak yapılan istihbarat toplama yöntemidir. Finansal istihbarat, açık kaynak istihbaratı, insana dayalı istihbarat ve sinyal istihbarattan aldığı destekle önemli başarılar sağlamıştır. Örnek olarak Usame bin Ladin'in ekonomi uzmanı ile Muhammed Atta ile gerçekleştirdikleri para transferleri ağız çözülmesinde verim elde edilmesini sağlamıştır (Altun, 2015).

2.5.3. Sinyal istihbaratı

Sigint (Signal İntelligence) elektromanyetik dalgaların ve sinyallerin toplanarak istihbarat çarkından geçirilmesi sonucunda elde edilen istihbarat türüdür. Elektro manyetik sinyallerin sensör ve antenler ile tespit edilmesini kaydedilmesini, kablolu veya kablosuz haberleşme ağının kaydedilmesi yolu ile içerik, trafik, kripto analizi gibi yöntemlerle istihbarata dönüştürülmesini

sağlayan süreci kapsamaktadır. Bu süreç casus uydular, insansın hava araçları, denizaltılar, gemiler, kara araçları gibi yöntemlerle gerçekleşmektedir. Alt disiplin olarak iletişim, elektronik, yabancı cihaz sinyal istihbaratından oluşmaktadır (Bağcı, 2022, s. 2).

Sinyal İstihbaratının kullanıldığı alanlar ise; düşmanın telsiz iletişiminden konum tespiti, mühimmat tespiti, tehlikeli olabilecek sinyal engellenmesi, kendi kuvvet takibimiz, düşmana ait elde edilebilecek tüm verilerin elde edilmesi olarak sıralanabilmektedir. (Değirmenci, 2021, s. 6). Sinyal İstihbaratı Elektronik İstihbarat (Elint), Telemetrik İstihbarat (Telint), Radar İstihbaratı (Radint) ve Siber İstihbarat (Cybınt) başlıklarını da kapsamaktadır. (Seren, 2017, s. 268)

Sinyal İstihbaratı genellikle telefon ve e-posta müdahalesi aracılığı ile iletişim verilerinin toplanmasıdır. Ayrıca internet meta verilerini ve konum verilerini de içerebilmektedir. Sigint'in hassasiyeti nedeniyle, kanuna uygun veri toplama, genellikle uygun olduğunda belirli kişileri hedef alabilen veya toplu olarak veri toplayabilen ulusal istihbarat teşkilatları ve kolluk kuvvetleri tarafından gerçekleştirilmektedir. ABD Ulusal Güvenlik Teşkilatı'nın PRISM ve X-Keyscore'u ya da Birleşik Krallık Hükümeti İletişim Merkezi GCHQ'nun Tempora'sı gibi programların artık internet sunucularının, uyduların, fiber optik kabloların kesişmesi yoluyla iletişim verilerini toplu bir şekilde toplayabildiği bilinmektedir. Kitle iletişim verilerinin toplanması da dâhil olmak üzere, Sigint'in salgın gözetiminde bir araç olarak kullanılması için çeşitli önerilerde bulunulmuştur. Algoritmalar, var olan veri setlerine veya veri toplama parametrelerine arama koşulları uygulayarak potansiyel hastalık salgınlarına ilişkin uyarıları belirlemek için kullanılabilmektedir. Mevcut toplama programları hedeflenen küresel sağlık önceliklerini muhteva edecek şekilde genişletmek, daha sonra insan operatörlerin analiz etmesi ve doğrulaması için erken uyarı ve müdahale hastalıkları erken tespit etme gibi uyarılar sağlamaktadır. Diğer öneriler, Sigint'in temas takibinde enfekte bir kişiyle temas etmiş olabilecek kişilerin tanımlanması ve teşhisinde kullanılabileceği düşünülmektedir (Bernard et al., 2018).

Ancak Sigint'in bulaşıcı hastalık sürveyansında kullanılmasıyla ilgili bazı sorunlar bulunabilmektedir. Özellikle toplu halde veri toplamanın siyasi olarak

hassas bir konu olduğu Snowden sonrası dönemde, ilk ve en önemli konu etik ve yasal konulardır. Greenwald, milyonlarca sıradan insanın iletişimlerinin çok az sorumlulukla dinlenmesinin ciddi gizlilik ihlallerine maruz kalması nedeniyle gizliliğin Sigint ile ilgili en büyük sorun olduğuna inanılmaktadır. Bu tür başka araştırmalar da benzer endişeleri gündeme getirmiştir. Bu bağlamda ulusal istihbarat yeteneklerinin kullanılması pek çok kişi için tatsız olacaktır ve gözetlemenin, yüksek bir tali izinsiz giriş riskini dengeleyecek gereklilik ve orantılılık eşiklerini karşılaması pek olası değildir. Sigint'in pratik olarak konuşlandırılabileceği bağlamlarda, yüksek gelirli ülkeler kendi ulusal sınırları içinde zaten güçlü hastalık sürveyans sistemleri sürdürdükleri için, hastalık sürveyansına katma değer minimum düzeyde olacaktır. Ayrıca, bu tür mahremiyet ihlallerinin, karmaşık jeopolitik ortamlarda sağlık ve insan alanlarında ortaya çıktıkça bilinmeyen etkileri vardır. Toplandıktan sonra verilere ne olacağı ve ev sahibi hükümetler tarafından bir nüfus içindeki gruplara karşı ayrımcılık yapmak için kullanılıp kullanılamayacağı hakkında başka sorular da gündemini korumaktadır (Bernard et al., 2018).

Sigint'in kullanımı ulusal mevzuata tabidir ve herhangi bir ek toplama bu yasal çerçeve tarafından kısıtlanacaktır. Bu gözetleme programları oldukça tartışmalıdır: GCHQ, Avrupa İnsan Hakları Mahkemesi'nde (AİHM) Veri Saklama ve Soruşturma Yetkileri Yasası 2014 kapsamında toplanması nedeniyle sorgulanmıştır ve NSA, Snowden'ın ardından önemli eleştirilerle karşı karşıya kalmıştır. Bu sebeple, Sigint 'in yaygın olarak konuşlandırılması, ilgili bir makamın gözetimine izin veren yasal bir sürecin uygulanmasını gerektirmektedir. Küresel sağlık alanında bu tür bir yönetişimin, ilgili teknolojilerin, kaynakların ve stratejilerin son derece hassas doğası göz önüne alındığında, DSÖ veya BM sisteminin diğer kuruluşları içinde yer alması beklenebilir. Ayrıca, modern *Sigint* teknolojisinin diğer ülkelerdeki sağlık risklerini hedeflemek için nasıl kullanılabileceğine dair pratik veya yasal bir emsal bulunmamaktadır. Sigint ile ilgili ayrıntılı bilgilere erişim sorunludur ve bu sebeple, bir bulaşıcı hastalığın veya PHEIC'nin kullanımını yasal ve etik olarak meşru kılmak için karşılaması gereken tanımlanmış tehdit eşiklerini ölçmek zordur. Bu nedenle Sigint 'in pratik çıktıları ve kullanımları, konuşlandırılmasında sonuçlar belirsizdir. Bir bulaşıcı hastalık salgınını

önceden tahmin etmek için, verileri zamanında toplamak üzere bu tür bir izlemenin sürekli olarak yapılması gerekir; ancak, mevcut bir pandeminin gerekçesi olmadan bulaşıcı bir hastalığın yasal eşikleri karşılaması pek olası değildir (Bernard et al., 2018).

Ayrıca hem halk sağlığı hem de devlet sürveyansın sonuçlarına veya hedeflerine odaklanmalıdır, net bir hedef olmadan veri toplamanın hiçbir gerekçesi yoktur. Sigint, kaynaklar açısından son derece maliyetlidir ve hastalık sürveyansına katma değerin onu gerçekten de maliyet etkin kılıp kılmayacağı şüphelidir. Sigint 'in kapsadığı bilgi hacmi nedeniyle, verilerinin eyleme geçirilebilir istihbarata dönüştürülmesine yardımcı olmak için önemli insan kaynakları gereklidir. GCHQ'nun mevcut programı, verileri filtrelemek için 300'den fazla analist gerektirmekte ve bu maliyet yalnızca elektronik iletişim hacmi genişlemeye devam ettikçe artabilir konumdadır. Sigint'in kullanımını gerektiren rekabet halindeki ulus-devlet öncelikleriyle, küresel sağlık içindeki uygulaması yeterince önemli bir 'tehdit' olarak görülmeyebilmektedir. (Bernard et al., 2018).

Yapılan araştırmalarda devlet dışında herkesin kullanımına açık Sigint uygulaması örnekleri görülmektedir. Denizcilik alanı farkındalık uygulamaları mevcuttur; radyo frekansı (RF) spektrum haritalaması; uydu iletişiminin gizlice dinlenmesi, karışması ve ele geçirilmesi ve siber gözetleme programları bulunmaktadır. Bu yeteneklerin çoğu ticari olarak mevcuttur, çoğu ücretsizdir ve bazıları yasa dışıdır. Görüşümüze göre hem yasal hem de yasa dışı pazarların ve yeteneklerin varlığı, Sigint'in demokratikleştiği veya herkesin kullanımına açık olduğu bir ortamla sonuçlanacaktır (Weinbaum et al., 2017).

2.5.4. Jeo-Uzamsal istihbarat

Geoint (Geospatial İntelligence), bir ülkenin stratejik konumunu, yapısını, yerleşme planlarını, ekonomik askeri veya sosyolojik yerleşim alanlarını, coğrafyaya bağlı olarak gerçekleşen sosyal medya hareketliliğini, vb. konuları muhteva edinen bir toplama yöntemidir. Uydu, insansız hava araçları, veri tabanları, haritalar, gibi çeşitli yöntemlerle her türlü görüntünün toplanarak işlenmesi, analiz edilmesi ve istihbarat haline getirilmesinden oluşan bir istihbarat ürünüdür (Clapper, 2005). Bu tür bir istihbarat kimi zaman taktik,

kimi zaman stratejik veya operasyonel istihbarata hizmet etmektedir. Operasyonel bir ortamın hem ayrıntılı veri analizini ve değerlendirmesini destekleyen hem de bu ortamla başa çıkma sorunlarını araştırmak için bir araç olan nispeten yeni bir istihbarat disiplinidir. Fiziksel özellikleri ve coğrafi olarak referans verilen faaliyetleri tanımlamak, değerlendirmek ve görselleştirmek için görüntülerin ve jeo-uzamsal verilerin analizini kullanır (Keith, 2019).

Geoint alanında son dönemlerdeki en büyük gelişmeler, insansız hava araçlarının, uzaktan yönetilebilen hava araçlarının kullanılması olmuştur. İnsansız hava aracı sistemleri UAS tarafından toplanan verilerin istihbarattaki kullanımının artış hacmi günden güne artacaktır. Özel sektörle de iş birliği yapılması amacı ile örnek olarak ABD'de ayrıca ticaret faaliyetleri açısından, tarım faaliyetleri açısından da kullanılmaktadır (Shepherd Andrew et al., 2017). Geoint ve Osint'in birlikte kullanımlarının kesiştiği kullanım olarak, BBC'de yayınlanan 'Afganistan'da Taliban'ın Uyuşturucu ile Savaşı' başlıklı haber güncel bir örnek teşkil etmektedir. Habere göre; Afganistan'ın Helmand bölgesi afyon üretiminde merkez bir konumda ve ülkenin afyon üretiminin yarısını bu yerleşim alanı karşılamaktadır. Talibanın emri ile yasaklanan afyon üretiminin 2022 ile 2023 arasındaki uydu haritalandırması analizi karşılaştırması afyon üretiminin %90 üzerinde azaldığını göstermektedir. Haberin açık kaynaklardan alınması itibari ile Osint, uydu görüntüleri analizi itibari ile Geoint örneklerini ayrıca uydu analizini sağlayan İngiltere merkezli Alcis Holding özel sektör girişiminin çalışmasının konu olarak alınması ile özel sektör teknoloji ve güvenlik alanında iş birliği bir araya gelmiş bulunmaktadır (Limaye, 2023).

2.5.5. Görüntü istihbaratı

İstihbarat toplamanın görüntü ve sinyal alabilen teknolojiler ile yapılıp, toplanan görüntülerin anlamlı hale getirilmesi, analiz edilmesi ve istihbarat ürünü çıkarılmasına Görüntü İstihbaratı (İmint-Imagery Intelligence) denilmektedir. En bilinen teknolojiler, İHA, Uydu, Radar teknolojileri, Denizaltılar, Kameralar, Sensörleri, Kızıl ötesi kullanılabilen teknolojilerdir (Beyazıt, 2019). Görüntü istihbaratı bir ülkedeki veya hedefteki, silah sistemleri, stratejik yerleşkeler, diğer istihbarat unsurları için konum bilgileri verebilmektedir. ABD, Fransa ve Avrupa Uzay Ajansında, Rusya ve Japonya da

görüntüleme sistemleri mevcuttur. Görüntüler ticarileştirilerek satılabilmektedir.1992 yılı Açık Semalar antlaşması bu anlamda bir tehlike teşkil etmektedir (Federation of American Scientists, 2019).

2.5.6. Teknik istihbarat

Söz konusu devletin veya düşmanın kullandığı silah, mühimmat, cihaz, malzeme, ekipman, yazılım vb. teknolojik olarak yararlandığı argümanların araştırılması ve bunlara yönelik strateji geliştirilmesini konu edinen alandır. Teknik istihbarat (Technical İntelligence), bütün teknolojik cihazların kullanıldığı istihbarat yöntemlerini kapsamaktadır. Bir çalışma ofisinin gizlice dinlenilmesi, bir şahsın gizlice kayıt altına alınması, bir telefon konuşmasının takibi, uzaydan bir bölgenin fotoğrafının çekilmesi gibi hemen her türden bilgi toplama faaliyeti teknik istihbarat çatısı altında değerlendirilmesi gerekmektedir. Bundan dolayı bazı açıklamalar konun daha iyi anlaşılması açısından faydalı olacaktır (Kavsıracı ve Demirbaş, 2020).

Teknik istihbaratın önemli bir yöntemi elektronik istihbarattır. Elektronik istihbarat, özü itibariyle elektronik sinyalleri yakalamak ve çözümlemek ile ilgilidir. Hava araçlarından, kara ve deniz araçlarından gönderilen elektronik sinyallerin rakip tarafından yakalanarak çözümlenmesi sonucunda bilgi elde edilmiş olmaktadır. Teknik istihbaratın ilgi alanına giren bir diğer yöntem de fotoğraf istihbaratıdır. Fotoğraf istihbaratı, günümüzde çok başvurulan bir yöntem değildir. Teknolojik gelişmeler, yeni icatları hayatımıza getirdi ve artık uydu istihbaratı ya da insansız hava araçları gibi sistemler ile görüntü alınabilmektedir (Kavsıracı ve Demirbaş, 2020).

Fakat geçmiş dönemlerde fotoğraf istihbaratı ordular ve servisler için önemli fırsatlar sunmuştur. Örneğin, Sovyetler Birliğinin Küba'da konumlandırdığı nükleer başlıklı füzelerin fark edilmesi, U-2 uçaklarının fotoğraf istihbarı sayesinde gerçekleşmiştir. Günümüzde fotoğraf istihbaratının gelişmiş versiyonu olarak uydu istihbaratından bahsetmek mümkündür. Bugün üretilen teknolojik cihazlar, hızlı ve detaylı görüntüyü uydular vasıtasıyla alma imkânı sunmaktadır. Bu sayede ordular ve istihbarat servisleri hızlı, daha az masraflı, daha az riskli bir şekilde istedikleri bölgeden canlı görüntüler alabilmektedir. Teknolojik gelişmelerin istihbarat servislerine fayda sağladığı

gibi zararları olduğunun bir başka kanıtını da uydu istihbaratında görmek mümkündür. Bugün Google ve Yandex gibi büyük firmalar, uydudan alınan görüntüleri açık kaynak erişimine sunmaktadır. Terör örgütleri devlet kurumlarına yapacağı saldırı öncesi, dışarıdan keşif yapamayacağı bir kurumun iç bahçesini ve etrafındaki bölgeleri masa başından keşif çalışması yapabilmektedir (Kavsıracı ve Demirbaş, 2020).

2.5.7. Ölçüm ve imza istihbaratı

Masint (Measurement and Signature İntelligence) olarak da bilinen, sabit veya hareketli bir hedefin bıraktığı izleri takip eden ve ayırt edici özelliklerini bulup analiz eden istihbarat türüdür. On üç farklı alanla ilgilenerek istihbarat toplamaya çalışır. Nükleer İstihbarat, Radyo Frekansları, Malzeme istihbaratı, Lazer, Optik, Kimyasal ve Biyolojik istihbarat, Kızılötesi istihbarat, Akustik istihbarat, Enerji silahları istihbaratı, Radar, Spektroskopik, Radyasyon, Atık toplama istihbaratı alanları ile ilgilenerek bilgi toplar analiz etmekte ver istihbarat ürünü çıkarmaktadır. Yakın zamana kadar Masint verileri bir yerde toplanıp gerektiğinde erişilebilecek bir pozisyonda değildi. Ordu bünyesinde gerektiğinde her zaman kullanılabilmesi amacı ile veri merkezi kurulmuştur (Federation of Amerikan Scientists, 2000).

2.5.8. Siber istihbarat

Siber İstihbarat (Cybint, Cyber Intelligence), diğer istihbarat kategorilerinden birçok alana destek verebilen ve ilişkili bir alandır. Ayrıca toplama, analiz etme ve yayma açısından birçok değişiklikle birlikte geniş ve yanıltıcı bir yelpazesi vardır (Alsmadi, 2019).

Savaşların günümüzde format değiştirmesi ile birlikte teknoloji desteği ile farklı boyutlara taşınmış durumdadır. Hedefe ciddi tahribat verici boyutlarda sonuçlara ulaştırabilen Siber Savaş yöntemleri, önleyici saldırılar kapsamında da kullanılmaktadır. İran'daki Natanz nükleer santralinin ağına sızan virüs ile işleyişteki bozulmaya sebep veren saldırı önleyici saldırılar kapsamında değerlendirilebilir. (Dönmez, 2017).

Günümüzde kamu hizmetlerinin sunumunda, ticari faaliyetlerde, bankacılık sektöründe, sağlık sisteminde ve daha birçok alandaki faaliyetler

siber alan üzerinden yapılmaktadır. Bu durum da siber alanın güvenliğini daha önemli hâle getirmektedir. Bu güvenliği sağlayıcı etkenlerden bir tanesi olarak siber istihbarat ön plana çıkmaktadır. Siber istihbarat kısaca, siber alana bağlı olan cihazlardan veri elde etmek şeklinde tanımlanabilir. Günümüzde eğitim, sağlık, bankacılık, ticaret, askerî güvenlik sistemleri ve kentlerin güvenliğini takip etmek amacıyla kullanılan sokak kameraları gibi birçok sektör ve cihaz siber alanda faaliyet göstermektedir. Bu kapsamda, günümüzde siber istihbaratın yapılamadığı herhangi bir alan yoktur. Çalışma kapsamında da ifade edildiği gibi, siber saldırıların sektöre göre yıllık maliyetine bakıldığı zaman bankacılık ve kamu hizmetlerinin ilk sırada yer aldığı görülmüştür. (KARASOY, 2022).

Toplumsal olayların önceden tespit edilebilmesi veya gerçekleşen olaylarda geriye dönük araştırma yapılabilmesi için, sosyal medya verileri çok önemli bir istihbarat ortamı haline gelmiştir. Siber istihbarat günümüzde gittikçe daha da önem kazanmaktadır. Ülkeler istihbarat kurumlarında siber istihbarat birimleri oluşturmaya başlamıştır. Gereksinimler doğrultusunda farklı program ve algoritmalar kullanılarak, sosyal medya veri yığınlarından istendik sonuçlara ulaşmak mümkündür (Savaş ve Topaloğlu, 2015).

Siber istihbarat operasyonlarına örnek olarak son dönemde adından çokça bahsedilen İsrail merkezli Pegasus casus yazılımı örnek olarak verilebilir. Dünyada yaklaşık 50 bin kişiyi hedef alan yazılımın, İsrail askeri istihbarat teşkilatı teknik/siber operasyonlardan sorumlu Unıt8200 birimi tarafından geliştirilmiştir. Çoğunlukla Meksika, Fas, Kazakistan, Hindistan, Suudi Arabistan gibi ülkelerden devlet başkanları, iş adamları, akademisyenler, savcılar, avukatlar, gazeteciler ve aktivistler gibi onlarca meslek grubundan kişilerin cihazlarına sızdığı bilgisini Forbidden Stories Platformu ve Uluslararası Af Örgütü (UAÖ) raporlamış bulunmaktadır. Medyada yer alması ve Forbidden Stories Platformu'nun teknik detay raporunu yayınlaması ile yazılımın kötü amaçlar için kullanıldığına ve gizliliği ihlal ettiğine dair TelAviv'e baskılar oluşmuştur. Pegasus yetkilileri bu iddialar karşısında sessiz kalmayı tercih etmişlerdir. Genel olarak bütün akıllı telefonlara sızma özelliği bulunmakta olan yazılım; Oltalama uygulamalardaki açıkları keşfederek sızma, sahte baz istasyonları üzerinden yahut doğrudan fiziksel müdahale yöntemi ile

çalışmaktadır. Sızma işlemi gerçekleştikten sonra elde edilen verilen göz önünde bulundurulduğunda dünyanın en spesifik siber silahı ile karşı karşıya kalmış bulunmaktayız (Çahmutoğlu, 2021).

2.5.9. Açık kaynak istihbaratı

Açık Kaynak İstihbaratı (Osint, Open Source İntelligence), açık kaynak bilgilerinden oluşan verilerinin istihbarat ürünü olarak çalışıldığında herhangi bir karşı koyma durumu olmayan, herkes tarafından ulaşılabilen, korunması söz konusu olmayan, gizlilik derecesi olmayan koşullarda elde edilip anlamlandırılan istihbarat toplama yöntemidir. İnternet hayatımıza girmeden önce açık kaynak bilgisi gazete, kitap, broşür gibi kaynaklardan elde edilmiştir. İnternet ile birlikte medya, kamu, ticari web ve arşiv verilerine daha rahat erişilebilmektedir. (Özdal ve Tiryaki, 2020).

Napolyon açık istihbarat kaynaklarının kullanımı konusunda gizli istihbarat kullanımından daha yaratıcıydı. Düşmanları ve müttefikleri ile ilgili kitapları okumaya onların şifrelerini çözmekten daha meraklı idi. Dışişleri Bakanı Jean-Baptiste de Champagny'ye şöyle yazdığı rivayet edilmektedir: 'Bana İngiliz gazetelerini göndermediğiniz için kızgınım, çünkü bize birliklerinin yerleri hakkında bilgi veriyorlar' (Andrew, 2022, s. 366).

Mevcut birbirine bağlı dünya tarafından üretilen veri miktarı ölçülemez ve bu tür verilerin büyük bir kısmı halka açıktır, bu da herhangi bir kullanıcı tarafından herhangi bir zamanda İnternet'in herhangi bir yerinden erişilebilir olduğu anlamına gelir. Bu açıdan Açık Kaynak İstihbaratı (Osint), bilgi üretmek için tüm siber uzayın noktalarını toplayarak, işleyerek ve ilişkilendirerek bu açık doğadan fiilen yararlanan bir istihbarat türüdür (Javier Pastor Galindo et al., 2020).

Açık Kaynak İstihbaratı toplama, işleme ve analiz sürecinde birçok manuel ve otomatik araç kullanılmaktadır. Metodoloji olarak veri bilimi, istatistik, makine öğrenimi, programlama, veri tabanları, bilgisayar bilimi gibi birçok alanın sentezlenmiş halidir. Açık Kaynak İstihbaratı için genel geçer bir teoriden söz etmek mümkün değildir (Erol, 2022)

Osint şu anda küresel olarak belirli gözetim sistemlerinde kullanılmaktadır ve birçok kamu istihbaratı yeteneğinin temelini oluşturmaktadır. Halk sağlığı

topluluğu bu hizmetlerin kapsamını tanımaya başlamıştır ve şu anda Osint ‘in Uluslararası önem arz eden Halk Sağlığı Acil Durumu (PHEIC) oluşturan hastalıkların belirlenmesine ve izlenmesine nasıl yardımcı olabileceğini araştıran birçok proje mevcuttur. Dünya Sağlık Örgütü (WHO), hastalık istihbaratında Osint'in toplanmasına ve değerlendirilmesine yardımcı olmak için bir program yürütmektedir. Küresel Halk Sağlığı İstihbarat Ağı (GPHIN), web tabanlı salgın istihbarat araçlarını kullanan ve Medisys, GPHIN, Healthmap'ten bilgi toplayan, DSÖ tarafından geliştirilen Tehlike Tespiti ve Risk Değerlendirme Sistemi (HDRAS) adlı daha büyük bir platformun çok önemli bir parçasını teşkil etmektedir. (Bernard et al., 2018).

Yeni gelişen hastalıkları inceleme programı (Promed-mail), diğerleri arasında. GPHIN, dokuz dilde küresel medya kaynaklarını sürekli olarak tarayan, anahtar sözcükleri, deyimleri ve olası hastalık salgınlarını arayan yarı otomatik bir erken uyarı sistemidir. Günlük 2000 ile 4000 arasında rapor oluşturma ve otomatik olarak uyarı üretme kapasitesine sahip bulunmaktadır. GPHIN gibi sağlık gözetimine uygulanan Osint araçları, verileri otomatik olarak toplayıp düzenleyebilmektedir ve böylece çok daha büyük miktarlarda bilgiye atıfta bulunabilmektedir. İlgili raporları filtrelemek için algoritmalar kullanılmaktadır. GPHIN, ProMED ve HealthMap, yüzyılın başından bu yana en ciddi salgınlardan bazıları hakkında uyarılar verebilmiştir. ProMED, Çin medyasından gelen içeriği değerlendirerek SARS için ilk İngilizce uyarısını sağlamış ve hatta ardından Çin Hükümeti tarafından onay istenmiştir. (Bernard et al., 2018).

Yakın tarihli Ebola salgını için bazı işaretler, yerel dilde haber öykülerini tarayabilmesi nedeniyle HealthMap tarafından herhangi bir resmi duyuru yapılmadan önce tespit edilmiştir. Halk sağlığı gözetimi, Sosyal Medya İstihbaratının (Socmint) kullanımını da araştırmaktadır. Socmint, belirli bir konu veya tema hakkında eş zamanlı bilgi sağlamak için küresel olarak artan sosyal medya ve web forumlarını kullanmaktadır. Socmint’ in coğrafi kullanılabilirliği, Osint ’inkinden daha fazla olup: dünyanın birçok yerindeki geleneksel internet kapsama oranları düşükken, bu bölgelerdeki mobil veri kapsamı artmaktadır. Mobil veri üzerinden erişilen en popüler servisler genellikle sosyal medya siteleridir. Bu durumlarda, Facebook genellikle

haberler için kullanılmakta ve geleneksel yayıncılık kaynaklarından daha fazla ham bilgi sunma potansiyeline sahip bulunmaktadır. Osınt'ın kullanımındaki en büyük sınırlamalardan birisi buradadır. Herhangi bir bilgi istihbarata dönüştürülmeden önce değerlendirilmelidir. Artık yapılandırılmamış veri kümelerinden istatistiksel olarak önemli bilgileri çıkarmak için algoritmalardan yararlanabiliyor olsak da bu tür bilgilerin yine de analistler ve araştırmacılar tarafından değerlendirilmesi gerekmektedir. (Bernard et al., 2018).

Düzgün bir şekilde sorgulamadığımız sürece büyük bir veri seti hiçbir işe yaramaz ve bu, halk sağlığı ile ilgili herhangi bir bilgi deposu için geçerli olmaktadır. Örneğin, bir kriz durumunda Sivil Toplum Kuruluşları (STK'lar) bir afet bölgesinin tam uydu görüntülerine ihtiyaç duymazlar ve onlara böyle bir görüntü sağlamak, daha fazla iş yükü oluşturacaktır. İhtiyaç duydukları şey, bu görüntülerin gösterebileceği altyapı hasarı ve nüfus hareketleri gibi spesifik bilgilerdir. Bu nedenle tek başına kullanılan Osint yeterli değildir; diğer kaynaklar ve temsilciler tarafından desteklenmesi gerekmektedir. GPHIN ve benzeri sistemler, kullanılabilirliğin yarattığı bozulmadan zarar görebilecektir. Ek olarak, birden fazla haber kaynağının bir olayı yayınlaması veya rapor etmesi, onun doğruluğunu veya gerçekliğini doğrulamamakta olup, Osint 'in diğer bilgilerle doğrulanması gerekmektedir. Bu, özellikle laboratuvar doğrulaması gerektiren bulaşıcı hastalıklar için geçerlidir. Bilginin kalitesi kontrol edilmediğinden, söylentiler asılsız çıkabilmektedir. (Bernard et al., 2018).

GFT'nin ilk algoritması, alakasız arama terimlerinin fazla takılması nedeniyle yüksek bir başarısızlıkla sonuçlanmıştır. Biyogözetim sistemlerine ilişkin bir inceleme, GPHIN'in insan denetlemesiyle birleştiğinde tespit oranlarını %53 oranında iyileştirdiğini ve teknolojik gelişmelere rağmen insan faktörünün önemini güçlendirdiğini tespit etmiştir. Bu tür sistemler, gerçek değer katmak için fiziksel doğrulama ekipleriyle birlikte kullanılmalıdır, çünkü ortaya çıktıkça salgınların hızlı bir şekilde raporlanmasında sınırlamalar devam etmektedir. Büyük verinin sınırlamaları bunlardan oluşmaktadır. Benzer şekilde, bu şekilde kullanılan Osint'ın birtakım sınırlamaları mevcuttur. İlk olarak, mevcut veri miktarının çok büyük olması nedeniyle, ilgili bilgi parçaları genellikle internetin arka plan gürültüsü arasında kaybolabilmektedir. Aslında,

Osint ile ilgili en büyük sorunlardan biri, analitik türetmeyi zorlaştıracak kadar çok veri olabilmesidir. Gerçekten de GPHIN'in, diğer raporlama yöntemlerine kıyasla o yıl en yüksek sayıda potansiyel uyarı üretmesine rağmen, 2002'de toplam raporlarının %30'undan fazlasını doğrulanmadığı düşünülmektedir. (Bernard et al., 2018).

Halk sağlığı sürveyanının uyarlanmasında yeni istihbarat kaynaklarının kullanılması kritik öneme sahip olsa da istihbarat servislerinin bilgiyi ilgili ve eyleme dönüştürülebilir kılmak için kullandığı tekniklerin dikkate alınması gerekmektedir. En önemli gelişme, statikten aktif veriye geçiş ve haritalama olmuştur. Bu tür teknikler, generaller temsili oyulmuş parçaları haritalar arasında itebildiğinden beri ordu tarafından kullanılmıştır, ancak aktif açık kaynak istihbaratı, harekât planlamasında kullanılabilecek yakın bir temsile izin vermektedir. Bu tür tekniklerin hem avantajları hem de dezavantajları, 2010 yılında Haiti'de meydana gelen deprem sırasında kriz haritalamanın kullanımında gösterilmiştir. Harita, tıbbi ihtiyaçlar da dâhil olmak üzere olayları ve ihtiyaçları haritalamanın bir yolu olarak işlev görürken ve bunları yardım çalışanlarına krizi, kaynakların çeşitliliğini, veri platformlarının uyumsuzluğunu ve toplam miktarı özel olarak ele almalarına izin verecek şekilde analiz etmiştir. (Bernard et al., 2018).

Şubat 2011'de Libya Çatışmasında kriz haritalama yardımı sağlamak üzere Yedek Gönüllü Görev Gücü (SBTF) konuşlandırıldığında, önceden daha net istihbarat yolları açık ve kapalı kaynaklarda harita versiyonları oluşturulmuştur. Bu tür teknikler, pandemiler veya PHEIC'ler durumunda henüz kopyalanmamıştır. HealthMap en yakın olanıdır, ancak HealthMap'i mevcut kriz haritalamadan ayıran şey, kriz ilan edildikten sonra kriz haritalamanın etkinleştirilmesi ve gönüllülerin izlenecek tanımlanmış bir dizi kritere sahip olmasıdır. HealthMap bilgileri küresel olarak yakalar, yani kritik hale gelme potansiyeline sahip olayları daha yaygın vakalardan ayırmanın zor olduğu anlamına gelmektedir. (Bernard et al., 2018).

Veri toplama, bir istihbarat döngüsü ve yerleşik istihbarat yolları, sağlık ve insani krizlerin giderek daha fazla örtüştüğü göz önüne alındığında, bulaşıcı hastalıklarda eşzamanlı kriz haritalamasının kullanımıyla ilgili olarak keşfedilmesi gereken araçlardır. Ancak, bu tür haritalar oluştururken ve

özellikle arama motoru verilerinin kullanımında, Osint'i düşük-orta gelirli ülkelerde uygulamanın zor olduğunun göz önünde bulundurulması gerekmektedir. Kaynak bakımından fakir olan bu ortamlar, özellikle kırılgan ve çatışma sonrası ortamlar, genellikle sağlık güvenliği tehditleri olarak tanımlanan salgınların coğrafi olarak en olası kaynaklarıdır; yine de iletişim altyapıları ve dijital varlıkları genellikle sınırlı bulunmaktadır. GPHIN ve HealthMap gibi Osint araçları, 'daha fazla sayıda medya kuruluşuna ve elektronik iletişim altyapısının daha fazla mevcudiyetine sahip ülkelere yönelik açık bir önyargıya sahiptir. (Bernard et al., 2018).

DSÖ'deki bir teknik görevli tarafından, bunun Osint 'i hastalık sürveyansında kullanmanın en büyük sınırlaması olduğunu doğrulanmıştır. Sosyal medya istihbaratını kullanma konusundaki etik tartışmalı olmaya devam etmektedir. Özellikle daha önce nüfusun bir bölümünü mağdur etmek veya ayrımcılık yapmak için dolaylı yöntemler olarak kullanılmış olan bulaşıcı hastalık salgınları söz konusu olduğunda, kaynakların kamuya açıklanması durumunda bu tür ayrımcılığa katkıda bulunma riski yüksektir. Bu, 2013'teki Boston Maratonu bombalamalarından sonra masum bir öğrencinin tespit edilip mağdur edilmesine yol açan internet kullanıcılarının yanlış şüphelileri tespit etmesiyle ortaya çıkmıştır. Ayrıca, sosyal medya sürekli olarak kişisel ve özel kavramlarımızı yeniden tanımlamaktadır. FaceBook gibi sosyal paylaşım sitelerinde paylaşılan bilgiler herkese açık olabilse de bu tür endişeler, onay istenerek hafifletilebilir. Ancak yine de dijital varlığı olanların sağlık güvenliği tehdidi olarak tanımlanan bulaşıcı hastalık salgınları olasılığının düşük olduğu ülkelerden gelmesi nedeniyle bir kullanılabilirlik yanlışlığı riskiyle karşı karşıya kalınmaktadır. Bu nedenle, bu tür verilerin herhangi bir sistematik kullanımından önce, bunun yapabileceği bir çerçevenin dikkatlice düşünülmesi gerekmektedir. DSÖ, tarafından Osint başarılı bir şekilde konuşlandırmış olup bu araçların yalnızca kullanım ve hassasiyet açısından genişletilmesi muhtemel görünmektedir (Bernard et al., 2018).

2.5.10. Sosyal medya istihbaratı

Sosyal Medya İstihbaratı (Socmint, Social Media İntelligence*)* büyük verinin yapay zekâ kullanılarak eğitim, ağ, duyarlılık, coğrafi, davranış analizi vb. analiz yöntemleri ile elde edilen istihbarat türüdür (Mete, 2021). Sosyal

medyayı izleyerek toplanan istihbaratı ifade eden Socmınt dijital çağın önemli bir parametresine dönüşmüştür. Bu toplama yöntemi ile terör olaylarından adi suçlara kadar ne nerede ne zaman ve kim sorularına zamansal olarak gerçek cevaplar verilebilmektedir (Taban ve Aydilek, 2023).

İstihbarat açısından çok önemli olan sosyal medya siteleri ticari, akademik veya güvenlik amaçlarıyla analiz edilebilir. Bu çalışmada Türkiye'de sosyal medya üzerinde çok tartışılan bir olay analizi gerçekleştirilmiştir. Elde edilen veriler içerisinden bilgi çıkarımı ve görselleştirme işlemleri yapılmıştır. Bazı anlamlı bilgilere ulaşılmıştır. Türkiye'de TT listesinde pek çok paylaşım reklam amaçlı yapılmaktadır. Gerçek verilere ulaşmak için öncelikle veriler içerisinde temizleme işlemi gerçekleştirilmiştir. Veriler URL'lerden ve etiketlerden temizlendiğinde daha anlamlı bilgiler ortaya çıkmıştır. Verileri analizi sırasında görülmüştür ki toplum hafızası, benzer olaylar arasında köprü kurabilmektedir. Ayrıca etiketlenen verilerde de yüksek merkezcilik oranları göstermiştir ki bazı kullanıcılar ve tweetler, pek çok farklı kullanıcı arasında köprü görevi görmektedir (Savaş ve Topaloğlu, 2015).

Sosyal Medya İstihbaratı; karar vericiler için eyleme dönüştürülebilir öngörüler üretmek için sosyal medyadan toplanan verilerin toplanması ve analiz edilmesi anlamına gelmektedir. Sosyal ağ sitelerine ek olarak video paylaşımı siteleri, fotoğraf paylaşım siteleri, inceleme siteleri, sosyal imleme siteleri, sosyal oyun siteleri, forumlar, mikrobloglar, panolar ve bloglar da sosyal medya istihbaratı alanlarındandır. Disiplin olarak Osınt'ın alt dalıdır. Sosyal medya istihbaratı, istihbarat ekiplerini, taktik düzeyde herhangi bir yerde neler olup bittiğine dair anlık bilgi ile, ip koruması, kayıp önleme ve seyahat güvenliği gibi birçok alanda desteklemektedir. Örneğin analistler, bir dizi gönderiden *exıf* verilerini çıkararak bir tehdit aktörünün konumunu belirleyebilir. Daha sonra bu bilgileri, yüksek profilli bir kişinin seyahat ve rota planlamasına yardımcı olması için bir koruma ekibine gönderebilirler (LifeRaft, 2023).

Sosyal medya istihbaratı, kolluk kuvvetleri, istihbarat örgütleri, kamu hizmetlerini daha iyi sürdürmek isteyen kurumlar tarafından kullanılmak üzere yüksek miktarda veri meydana getirmektedir. Her bilginin toplanmasından ziyade, bilginin istihbarat amacı ile toplandığında faydası olmaktadır. Sosyal Medyadan elde edilen verinin genel olarak beş kategoride

değerlendirebilmektedir: Öncelikle her kullanıcının sosyal medya hesaplarından yaptığı paylaşımlar, ikinci olarak cevaplar, üçüncü olarak çoklu ortam alanları, dördüncü alan kullanıcı profilleri, son olarak da etkileşim verileridir. Avantaj ve dezavantajları ile ele alacak olursak; Sosyal medya verisi bize gerçek zamana yakın bilgiler vermektedir. Organize suç ve terör örgütlerinin zihinsel ve davranışsal analizlerini yapmaya elverişli bir veri ortamı teşkil etmektedir. Ayrıca suçları aydınlaştırmadan delil bulmaya yardımcı olmaktadır. Gerçek niyetin hemen tespit edilememesi, büyük veri ile çalışmanın zorlukları, sosyal medyanın değişen dili ve yöntemleri ise zorluklar ve dezavantajlar olarak gösterilebilmektedir. (Bural, 2021, s. 102-131)

Ayrıca sosyal medya istihbaratı ile aktörlerin işinize saldırmak için kullanabilecekleri bilgi tehdidini de belirlenebilmektedir. Örneğin, arkadaşlar veya aile üyeleri tarafından çevrimiçi olarak yayınlanan resimler, önemli bir yöneticinin evini gösterebilir. Alternatif olarak, kötü aktörler, sosyal mühendislik planlarında çevrimiçi olarak yayınlanan çalışan bilgilerinden yararlanabilir veya güvenli tesislere erişebilmektedir. Günümüzde sosyal medya, kamuoyunun nabzını tutmak için gidilecek yeri temsil etmektedir. Şirketiniz ister ticari genişleme konusunda kamuoyu algısını anlamak ister bir halkla ilişkiler krizine uygun şekilde yanıt vermek istiyor olsun, Socmint araştırması yöneticilerin daha bilinçli kararlar almasına yardımcı olabilmektedir. Kuruluşlara yönelik gelişen tehditler, tahmine dayalı, istihbarat odaklı bir strateji gerektirmektedir. Riskleri öngörmek için güvenlik liderlerinin ellerinden geldiğince her yerden bilgi toplaması gerekmektedir. Sosyal medya istihbaratı, karar vericileri bilgilendirmek için giderek daha önemli bir aracı temsil etmektedir. Yalnızca hırsızlık, dolandırıcılık veya şiddet gibi saldırılara karşı korunmaya yardımcı olmakla kalmamaktadır. Ayrıca, kriz durumlarında daha hızlı yanıt verebilmek için ekiplere gerçek zamanlı, konum tabanlı durumsal farkındalık sağlayabilmektedir (Socmint, 2023).

Sosyal medya istihbaratına DAEŞ'in sosyal medya stratejisi örnek olarak gösterilebilmektedir. Özellikle yeni nesil propaganda yöntemi olarak değerlendirilebilecek olursak, kurulacak olan İslam Devleti ideali adı altında sundukları cennet vaadini, sözde hicret eden Müslümanlarda oluşturulduğu düşünülerek misyon yayma faaliyetinin sosyal medya üzerinden

gerçekleştirildiği görülmüştür. DAEŞ militanlarından eğitimli, teknolojiyi iyi kullanabilen ekipler yeni nesil imkânlardan yararlanmıştır. Sosyal medya lokasyon olarak sınır gerektirmediği için, mesajların anlık olarak iletilmesi ve güncellenebilmesi avantajı sağladığından örgüte de dinamik bir yapı göstergesi kazandırmış ve gerçek niyetleri ve hareket tarzını gizleme imkânı oluşturmuştur (Darıcılı, 2023, s. 226-242).

Sosyal Medya İstihbaratının bilgi toplam alanları sadece sosyal medya ağlarında değil, forum, blog, oyun sitelerinde ve video alanlarında da bilgi toplamaktadır. Sosyal Medya bilgileri, etkileşimler, konum, zaman, cihaz türü gibi hassas bilgiler toplanabilmektedir. Söz konusu istihbarat türü, terörizm, cinsel istismar, suç örgütleri, siber suçlar gibi alanlarla mücadele etmek adına aynı zamanda hastalık izleme, afet durumunda takip gibi amaçlarla yapılmaktadır (Maltego Takımı, 2022).

2.6. İstihbarat Çarkı ve Analizi

İstihbarat faaliyeti süresiz olması ve sürekli takip edilmesi gereken bir süreci içerdiği için tüm istihbarat teşkilatları tarafından bir çarka benzetilir. İstihbarat çarkı kendi içerisinde dört evre şeklinde gerçekleşir. Bu evreler sıra ile istihbarat ihtiyaçlarının tespiti ve toplanması çalışmalarının yönlendirilmesi, haberlerin toplanması, haberlerin işlenmesi ve istihbaratın yayımı ve kullanılmasıdır. Birinci evre kamu kurumlarının ihtiyaç duyduğu bilgi ve verilerin toplanması, belirlenmesi ve mevcut çalışmalardan haberdar edilmesi sürecini kapsar. İkinci evre açık ve kapalı olmak üzere kendi içerisinde ikiye ayrılır. Açık kaynaklar olan gazete, dergi, kitap, radyo, televizyon yayınları ve internet siteleridir. Kapalı olan kaynaklar ise toplama bilgilerin teknoloji yardımıyla derlenmesini ifade eder. Üçüncü evre haberlerin işlenmesi olarak gelen bilgilerin tasnif, kıymetlendirme ve yorum aşamalarından geçmesi olarak tanımlanır. Bilgilerin değer sıralamasının iyi bir şekilde yapılması istihbarat sürecinde büyük önem taşımaktadır. Eğer gerekli işlenmemin yapılamaması durumunda istihbarat zafiyeti ortaya çıkabilir. Ortaya çıkan zafiyet devletin veya vatandaşların güvenliğine daha büyük tehditlere de neden olabilir (MİT, 2023).

Dördüncü ve son evre olan istihbaratın yayımı ve kullanılması sonucu ifade etmektedir. Diğer evlerde belli süreçlerden geçen bilgi, verim ve yorumlamalar artık politika haline dönüşerek istihbarat faaliyetinin tamamlanmasını sağlar. Değerlendirmelere tabi tutulan işlemlerin raporlar hazırlanarak zamanında ve sürekli olarak ilgili karar alıcılara ulaştırılması güvenlik zafiyetlerinin önüne geçmektedir. Örneğin istihbarat çarkında meydana gelecek herhangi bir bozulma karar alıcıların yanlış politikalar uygulamasına neden olabilir. ABD'de 11 Eylül'de gerçekleşen ve binlerce insanın ölümüne neden olan saldırılar istihbarat çarkında meydana gelen bir zafiyet nedeniyle gerçekleşmiştir. Bu nedenle ülkeleri açısından istihbarat çarkının verimli, sürekli ve sürdürülebilir halde tutulması en önemli öncelik olarak karşımıza çıkmaktadır (MİT, 2023).

İstihbarat çarkı beş aşamadan oluşmaktadır; planlama-yönetme, toplama, işleme, üretim-analiz, yayım şeklindedir. Genel olarak dairesel döngü ile ifade edilse de her zaman aynı doğrultuda devam etmeyebilmektedir. İstihbarat Çarkı'nın merkezinde verilen görev vardır, çark görevin etrafında konuşlanmaktadır (Demir, 2021).

Genel kabul gören istihbarat çarkları temel noktaları teşkil etmektedir. İstihbarat operasyonel olarak farklı alanlara temas ettikçe farklı başlıklar ve usullerden oluşan çarklar gelişmeye ve kullanılmaya başlanmıştır. Gelişen çark modellerinde, espiyonaj, istihbarat diplomasisi, terörizm ile mücadele, güvenlik tahkikatları, stratejik istihbarat, örtülü faaliyetler, sınır aşan suçlar ile ilgili alanlarda farklı döngüler oluşmuştur (Darıcılı, 2023, s. 23).

İstihbarat çarkının tamamlanması ise bütün süreçlerin en iyi şekilde bitmesiyle mümkün olan durumu ifade etmektedir. İstihbarat teşkilatlarının devamlılığı ve güvenliği açısından istihbarat çarkı toplanan veri ve bilgilerin en sağlıklı şekilde kullanılmasını sağlamaktadır. Böylelikle insanlık tarihinin başından itibaren bir rekabet alanı olan bilgi toplama ve analiz etme süreci istihbarat çarkıyla daha kolay ve kullanılabilir hale gelmiştir. Gerçek istihbarat çarkı, ABD Ulusal İstihbarat Konseyi Eski Başkan Yardımcısı Gregroy F. Treverton'a göre; politikaların çekmesi ile değil, istihbaratın ittirmesi ile hareket ettiğini öne sürer. İstihbarat ürünleri yani raporlar sadece girdi olarak nitelendirilip, çıktıları olarak ise karar verecek ya da harekete geçecek kişilerin

anlayış veya bakış açılarını inşa etmektir. İstihbarat üretiminde, İstihbarat üreticileri, İstihbarat Tüketicileri, İstihbarat Yöneticileri, İstihbarat Kullanıcıları gibi kavramlar sürecin aktörlerini ifade etmektedir (Seren, 2017, s. 249).

İstihbarat ürününün anlamlı hale gelmesi amacı ile belirsizliği azaltmak ve öngörüler çıkartmak üzere gerçekleştirilen zihin faaliyeti olarak İstihbarat Analizi kavramını ele almamız gerekecektir. İstihbarat tüketicilerine, kullanıcılarına ve karar alıcılara bilgiden öte öngörü halinde sunulan bilgi olarak sunulan analiz rafine edilmiş bilgi anlamı da taşımaktadır. İstihbaratın bilgi toplama, işleme, analiz etme, karar alma, yönlendirme, önleme, engelleme veya ters sonuçlar sağlama amaçlarına bağlı olarak analiz fonksiyonuna da bu başlıklardan nerede ihtiyaç duyulduğu ile alakalı olarak değişmektedir.

Analistler istihbaratın her aşamasında, taktik, stratejik ve operasyonel istihbarat üretmektedir. Üretilen istihbarat tanımlama, açıklama ve yorumlama düzeylerinde yapılmaktadır. Son dönem analiz farklılığı dijitalleşmenin artması ile birlikte Açık Kaynak İstihbaratının kullanımının artmasıdır. Açık kaynak bilgilerinin her aşamasında olduğu gibi elde edilen istihbaratın analiz edilmesi ve güvenirliliği sorgulanmalı, doğru ve yanlış kısımları ayıklanmalıdır. İnternetin kullanımının artması ve dijital kaynakların genişlemesi ile birlikte eski zaman dilimlerine göre analistlere daha iyi analizler yapma imkânı sunmaktadır (Taban ve Aydilek, 2022)

2.7. Kamu Güvenliği ve İstihbarat

Uygulama alanları ve çeşitleri ile gerek iç ve gerekse dış tehditler açısından kamu güvenliği devlet tarafından sağlanır. Stratejik olarak temelde güvenlik birimleri istihbarat alanında çalışırken, ilgili bakanlık kurumları da kendi faaliyet alanları ile ilgili olarak çalışmalar yürütebilir. Esasen bir ülkenin istihbarat hedefinin belirlenmesi o ülkenin uzun vadeli hedeflerinin belirlenmesi ile eşanlamlıdır. Kamu güvenliğinin sağlanması, korunması ve sürekli hale getirilmesinde istihbarat birimleri ve teşkilatlarının yadsınamaz bir yeri bulunmaktadır. Güvenlik teriminden başlanarak bir tanımlama yapılması kamu güvenliği kavramının daha sağlam bir zeminde açıklanmasına katkı sağlayacaktır. Güvelik olgusu insanlık tarihinin başlangıcından itibaren önemlidir. İnsanların kendi ürün ve mallarını korumak için kabile, topluluk ve

sonunda devlet halini alan mekanizmalar inşa etmesi temel bir ihtiyaç olan güvenlik olgusunu değer katmıştır. İnsanların kurdukları devletler zamanla dış ve iç saldırılar sonrası yıkılmış ve eski kurumların yerine yeni devletler inşa edilmiştir. Toplumsal yaşam biçiminde adaletin sağlanması ve kanunların uygulanması durumunu ifade eden güvenlik kavramı bireysel anlamda vücut, ahlak ve insani bütünlüğünü koruma durumu olarak tanımlanmaktadır. Güvenlik ihtiyacı insanların toplu yaşamaya başladıkları dönemden itibaren devletlerinde temel konularından biri olagelmiştir. Büyük bir organizma şeklinde gelişim gösteren devletler kendi devamlılıklarını sağlamak ve güvenlik ihtiyaçlarını gidermek için büyük askeri harcamalar yapmış ve ordular beslemiştir (Karabulut, 2011, s. 251-252).

Korunma isteğinin bir yansıması olarak ortaya çıkan ve devletlerin daha kurumsal hale gelmesiyle daha da önem kazanan güvenlik olgusu teknoloji ile değişmiştir. Kamu kurumlarının kendi bilgi ve verileri dışarıdan gelecek olan tehditlere karşı korunmaktadır. Bu korunmanın bir yansıması olarak devlet aygıtları arasında güvenliği sağlamak için bölümler ve kurumlar kurulmuştur. Bir bütün olarak kamunun güvenliği ise ulusal güvenliğin bir parçası olarak devletin her türlü iç ve dış tehditte karşı korunma durumunu ifade etmektedir. Kamu güvenliğinin sürekli bir ihtiyaç olması ve devletin devamlılığında edildiği önem günümüzde yeni teknolojik trendlerle daha fazla ilgi çeken bir konu olmuştur (Ateş, 2012, s. 14-15).

Kamu güvenliği ülke sınırları içerisindeki toplumun, devletin fiziki varlığının, sosyal, psikolojik, kültürel ve toplumsal dokunun süreklilik halinde korunması olarak tanımlanabilir. Sosyal yaşantının bir parçası olarak devlet kurumları toplumla etkileşim halindedir. Toplumu etkileyen ve etkilenen bir sistemsel mekanizma olan devlet aygıtı kurumlarla görünür haldedir. Bu halin farklı dönemlerde tehdit edilmesi ve saldırılara maruz kalması sıkça rastlanan bir durumdur (Hasan, 2012).

Devletin temel görevlerinden biri olan kamu güvenliği tıpkı vatandaşların vücut bütünlüğünün korunmasına benzetilebilir. İnsan vücudu bir bütün olarak korunmazsa gerekli yaşamsal faaliyetler gerçekleştirilemez. Devletin kurumları da insan vücudunda olduğu gibi bütünlüğünün korunması gereken yerlerdir. Güvenlik birimleri tarafından sağlanan kamu güvenliği fiziki olmasının yanı sıra

teknolojik gelişmelerle sanal ortamlara da taşınmıştır. İnternet, online girişimler ve sosyal medya platformlarında kamu güvenliğine yeni tehdit türleri ortaya çıkmıştır. Bu tehditlerin önlenmesi ve yerinde engellenmesi için açık kaynak istihbaratına ihtiyaç duyulmaktadır. Bu ihtiyacın gün geçtikçe artması ise açık kaynak istihbarat çalışmalarını ve örneklerini çoğaltmıştır. Özellikle internet üzerinden kamu kurumlarına yapılan saldırılar sonrası kamu sistemleri büyük oranda zarar görebilmektedir (Ateş, 2012, s. 14-16).

Ülkeler her ne kadar fiziki sınırlar itibari ile korunsa da çevrimiçi dünyanın sınırları belirlenemediği gibi her geçen gün genişlediği düşünülmektedir. Enerji santrallerinden, barajlara, sanayiden iletişim mecralarına kadar dijital ağlara sorgulamaksızın daha da teslim olan bireylerin havaalanlarına, sınırlara vardığımızda güvenli geçişlerinin sağlandığı kadar çevrimiçi ortama suç amacı taşıyan kişilerin sanal konuma rahatlıkla girip çıkabildiğini görmekteyiz. Güvenlik yazılımlarına harcanan bütçenin her gün artmaktadır. Ancak İsrail Teknoloji Enstitüsünden gençler 82 yeni bilgisayar virüsünü, anti virüs arama motorlarına ilettiler ve sonuç olarak meşhur bildiğimiz güvenlik programlarının ilk tehdit algılamaları %5 seviyesinde kalmıştır (Goodman, 2017, s. 28).

2014 yılında 684.000 Facebook içeriği paylaşımı, 34 Milyon Whatsapp mesajı, Twitter ’da 100.000 paylaşım, Instagram ’da 36.000 fotoğraf koyduğumuzu göz önünde bulundurulursa, Zuckerberg ve Eric Schmidt’in ifadesi ile çağı yönetenler her gün bıraktığımız ayak izinin verisine sahip olduğundan çağın patronları oldukları doğrulanmış olacaktır. Zaman içerisinde ayak izi bıraktığımız ve bilgilerimizi verdiğimiz sosyal medya ve dijital platformlar insan davranışını analiz ettiğinden, verimizi nasıl istiyorlar ise, reklam, pazarlama, gözetleme, şantaj, siyasi baskı gibi amaçlarla kullanabileceklerdir. Bu nedenler verilerimizin doğal kaynaklar gibi, hassasiyetle korunması gerekmektedir (Goodman, 2017, s. 126).

Edward Snowden güncel olarak verdiği bir röportajda, kamu güvenliğinin sağlanmasında teknolojinin hızlı gelişmesi, gözetleme kameraları, yüz tanıma sistemleri, yapay zekanın kullanımının artması şimdiye göre 2013 yılında kullanılan teknikleri bir nevi çocuk oyuncağı olduğunu ifade etmektedir. Kişisel mahremiyetin korunmasında 2013 yılında herkesin çok savunmasız bir şekilde

hareket ettiğini, o günlerde hayal gibi görünen uçtan uca şifrelemenin bugün çok katkısı olduğunu söylemiştir. ABD ve İngiltere İstihbarat Teşkilatları Snowden'ın ifşalarının mahremiyet açısından katkı sağladığını düşünüyor ancak istihbaratın doğası gereği istihbarat operasyonları bölümünü kapatmak gibi bir sonucun faydadan daha çok zarar getirdiğini savunmaktadır. Dolayısı ile kişisel mahremiyet, istihbarat ve güvenlik anlayışlarının da görüş ayrılıkları her zaman devam edecektir (Macaskill, 2023).

3. AÇIK KAYNAK İSTİHBARATI

3.1. Açık Kaynaklar

Tarihsel açıdan bakıldığında Soğuk Savaş sonrası açık kaynakların daha fazla öne çıktığını söylemek mümkündür. Soğuk Savaş öncesi istihbarat teşkilatları daha çok devlet merkezli sorunlarla meşgul iken Sovyetlerin dağılmasıyla birlikte incelenmesi gereken olay ve konular genişlemiştir. Terörizm, kitle imha silahları, organize suç, devlet içi çatışmalar, enerji güvenliği, göç ve göçmenlik, kaçakçılık ve iklim değişikliği gibi yeni olgular daha fazla tartışılmaya ve istihbarat teşkilatları tarafından incelenmeye başlanmıştır. 11 Eylül 2001'de ABD'de gerçekleşen terör saldırısı açık kaynak kullanımı için milat olarak kabul edilebilir. Saldırı sonrası hazırlanan raporda açık kaynaklardan alınabilecek bilgilerin göz ardı edilmesi sonrası istihbarat zafiyeti meydana geldiği ve saldırının gerçekleştiği açıklanmıştır. Açık kaynakların öneminin artması ise birçok kuruluşu açık kaynakları daha fazla dikkate almaya itmiştir (Bal ve Erkeç, 2014, s. 186).

Bir bilginin açık kaynak olarak kabul edilmesi için şu şartlar genel anlamıyla aranmaktadır;

- Elde edilmesine karşı konulma durumu olmamalıdır.
- Bilgi herkes tarafından ulaşılabilir olmalıdır.
- Bilginin korunması, saklanması durumu söz konusu olmamalıdır.
- Bilgi ücretsiz şekilde hizmete sunulabilmelidir.
- Bilgi toplamada gizlilik olmamalı ve kolayca ulaşılabilmelidir (Tekek, 2016).

Tekek tarafından ifade edilen bir kaynağın açık kaynak olarak kabul edilmesi şartlarına daha çok özellik eklemek mümkündür. Ancak tezin konusu gereği sınır, amaç ve hedefler gözetilerek daha fazla açıklama yapılmayacak ve yukarıda vurgulanan özellikler üzerinden yorum ve analizler yapılacaktır.

Açık kaynak türleri ise birinci bölümde açıklamalara kıyasla daha geniş bir perspektifle bu bölümde ele alınmaktadır. Açık kaynakların ayrıntılı şekilde işleneceği mevcut bölüm geleneksel medya araçları, internet, kamuya açık veriler, akademik makale ve sunumlar, ticari veriler kısımlarından oluşmaktadır. Böyle bir sınıflandırmanın tercih edilmesinde teorik kısmın sağlam bir zeminde ilerlemesi hedefi bulunmaktadır.

3.1.1. Geleneksel medya araçları

Televizyon geleneksel medya araçları arasında en geniş kitleye ulaşabilen ve her ülkede yaygınlıkla kullanılan bir medya iletişim türüdür. Türkiye ve ABD'de neredeyse her konutta bulunan TV'ler halk-devlet arasındaki iletişiminde temel bileşenlerden biridir. Böylesine önemli hale gelen TV'ler aynı zamanda açık kaynak olarak istihbarat teşkilatlarına önemli bilgiler sağlayabilmektedir. TV programları, haberler, diziler, belgeseller ve filmler birçok olayın gösterildiği televizyonlar kamu tarafından kontrol ve denetim altında tutulmaktadır. Ülkeden ülkeye değişiklik göstermekle birlikte Radyo ve Televizyon Üst Kurulu (RTÜK) benzeri denetleme ve düzenleme kuruluşları bulunmaktadır. TV ve tartışma programları, TV kanallarına kimlerin çıkarılacağı veya toplum-devlet arasındaki iletişimin nasıl sağlıklı yapılacağı gibi birçok soruyu içerisinde barındıran televizyon günümüzde yakından takip edilmektedir (Nedim, 2018). Radyonun ilk ortaya çıkışıyla birlikte ses dalgaları iletişim teknolojisi büyük ilerleme göstermiştir. Guglielmo Marconi tarafından icat edilen radyo frekans sistemi ve dizaynı ilerleyen dönemlerde telsizlerin altyapısını oluşturmuştur. Telsizler orduların daha kolay ve hızlı iletişim kurmasını sağlarken yeni bir istihbarat faaliyet alanı ortaya çıkmıştır. Örneğin Birinci Dünya Savaşı döneminde düşman ülkeler birbirlerinin telsiz hatlarına sızarak orduların hareketlerini tespit etmiştir. Buna benzer uygulamalar halkın dinlediği radyolar üzerinden de yapılabilmektedir. İkinci Dünya Savaşı döneminde Alman istihbaratının İngiliz radyolarını dinlediği ve toplum-devlet arasındaki iletişim kanallarında neler konuşulduğunu analiz etmeye çalıştığı bilinmektedir (Çıtak, 2015).

Gazete yüzyıllardan itibaren haber alma, iletişim ve bilgiye ulaşım için kullanılmaktadır. Antik devletlerde şehir, bölge ve eyaletler arasında iletişimi sağlamak için belli aralıklarla yazıların çıkarıldığı, mektupların gönderildiği ve

bilgi alışverişinde bulunulduğu bilinmektedir. Devletlerin ve toplumların kendi gündem, sorun ve problemlerinin aktarıldığı bir mecra olan gazeteler çok eski dönemlerden itibaren istihbarata konu olmuşlardır. Örneğin gazetelerin takip edilmesi suretiyle Almanya'nın dış ülkelere bilgi sızdırılmaması için sansür uyguladığı bilinmektedir. Birinci ve İkinci Dünya Savaşları döneminde muhalif hareketlerinde iletişim mecralarından biri olan gazeteler hem hükümet hem de iktidar dışı güç odakları tarafından sıklıkla kullanılmıştır. Açık kaynak istihbarat kaynağı olarak gazetelerin günümüzde de benzer bir misyon üstlendiğini söylemek mümkündür. Böylelikle istihbarat teşkilatı büyük bir maliyete katlanmadan ülke gündemi hakkında kolaylıkla bilgi toplayabilmektedir (Çıtak, 2015, s. 755-765).

Dergiler açık kaynak istihbarat kaynakları arasında önemli bir yere sahiptir. Özellikle istihbarat üzerine yayın yapan dergiler açık kaynaklar için büyük veri ve bilgiler sunmaktadır. Türkiye'de Terörizm ve Radikalleşme ile Mücadele Araştırma Merkezi (TERAM), İstihbarat Araştırmaları Dergisi, M5dergi ve İstihbarat Çalışmaları ve Araştırmaları Dergisi, Terörizm Analiz Platformu (TAP) açık kaynak istihbaratında dergilere örnek olarak verilebilir. Dergiler üzerinden taranan bilgiler hem açık kaynak istihbaratında yeni trendlerin kolaylıkla takip edilmesini sağlamaktadır. Periyodik yayınlarda da benzer bir durum vardır. İstihbarat Teşkilatları kolaylıkla bu kaynaklara ulaşırken herhangi bir maliyete katlanmak zorunda değildir. Broşürleri de bu çerçevede değerlendirmek mümkündür. Özellikle seçimler döneminde partilerin neler tasarladıkları hakkında broşürler üzerinden bilgi edinilebilmektedir. Aynı durum birey, kurum, firma ve şirketler için de geçerlidir. Firmalar rakip firmaların neler yaptığı hakkında broşür, sürekli yayın ve dergiler aracılıyla istihbarat faaliyetleri yürütebilir ve bilgiler toplayabilir (Erol, 2022, s. 35-49).

3.1.2. İnternet

Bilgisayar veya cep telefonu yolu ile erişim sağladığımız çevrimiçi yayınlar, bloglar, internet siteleri, sosyal medya hesapları ve çevrimiçi iletişim araçları, vatandaş olarak çevrimiçi ortama girdiğimiz her türlü veriyi kapsayan bir alandır. Günümüzde internet kullanıcı sayısı 4,5 milyar iken 3,8 milyar tane sosyal medya kullanıcısı bulunmaktadır. Bu istatistiklerden hareketle dünya nüfusunun yaklaşık yüzde 60'ının çevrimiçi kullanıcı olduğu görülmektedir.

Devletler için kontrol ve denetim altında tutulması çok zor bir alan olan internetin kullanımı her geçen gün artmaktadır. Devletler interneti aynı zamanda toplumlarına verilen kamu hizmetinin kalitesini yükseltmek için kullanabilmektedir. Türkiye'de hayata geçirilen ve dünyaya örnek bir uygulama haline gelen e-devleti internet üzerinden verilen kamu hizmetine örnek olarak vermek mümkündür. Diğer bir taraftan vatandaşların kişisel bilgilerinin daha ulaşılabilir hale gelmesi internet ortamı düzelmelerinin yapılmasına ve yeni bir hukuki bölümün oluşturulmasına neden olmuştur. Sosyal medya üzerinden yayın yapanların toplum kural ve ahlak yapısına uygun olmayan davranışları yargı tarafından takibe tabii tutulmaktadır. İnternetin ortaya çıkardığı bilgiye ulaşımın daha kolay olması beraberinde bazı zorluklarda getirmiştir. Bu zorlukların başında bilgi güvenliği ve verilerin denetlenmesi gelmektedir. Birey, kurum ve firmaların bilgileri dış saldırı ve sızmalar aracılıyla farklı ortamlarda kullanılabilmektedir (Bal ve Erkeç, 2014).

İnternet gizlenmek istenen veya gizlenmek istenilse bile çok başarılı olunamayan bir alandır. Devletler başta olmak üzere bilgi sızdırma olayları günümüzde sıkça gerçekleşen bir olguya dönüşmüştür. Kamu böyle olayların önüne geçmek için farklı kurumlar kursa da dünyada pek çok devlet siber saldırılara maruz kalabilmektedir. İnternetin yaygınlaşması sonrası genellikle ABD merkezli olarak kurulan sosyal medya uygulamaları açık kaynak istihbaratının önemli bir parçası olmuştur. Twitter, Tiktok, Instagram, Youtube, Google ve Facebook gibi uygumalar dünya genelinde kullanılan sosyal medya platformlarıdır. Bireysel hesapların yanı sıra kurumlarda mevcut sosyal medya uygulamalarında hesap oluşturabilmektedir. Kurumlar daha çok toplumu bilgilendirme amacıyla sosyal medya platformlarını kullanmaktadır. Firma ve şirketler pazarlama, satış, iletişim ve reklam amacıyla medya platformlarını tercih edebilmektedir. Bireyler eğlence, iletişim, sosyalleşme ve alışveriş için sosyal medya uygulamalarını kullandıklarını ifade etmektedir. Böylesine geniş bir kitleye yayılan milyarlarca kişinin verilerini içeren platformlar Batı menşeilidir. Birçok ülke tarafından eleştirilen mevcut yapı devletlerin alternatif sosyal medya uygulamalarını hayata geçirmelerine neden olmuştur. Çin'de Youtube, Instagram, Twitter ve Facebook gibi uygulamalara alternatif olarak

kurulan girişimler ülke içerisinde başarılı olsa da küresel bir alternatif günümüzde mevcut değildir (Erol ve İstikbal, 2020).

3.1.3. Kamuya açık veriler

Kamuya açık veriler kamusal olarak erişime açık konferans, canlı yayın, adli duruşmalar, telefon rehberleri, bütçeler, kamu raporları gibi alanları kapsar. Birçok istihbarat teşkilatı kamuya açık verileri dikkatlice takip etmektedir. Örneğin ABD'nin başkenti Washington DC'de düşünce kuruluşlarında dünya meseleleri konuşulmakta ve analiz edilmektedir. Yapılan açık konferans ve canlı yayınlara ABD devletinde görevli üst düzey çalışanlar dahil edilmekte ve kamu politikaları tartışılmaktadır. Aynı şekilde ABD Kongresinin araştırma birimi farklı konularda Senatör ve Temsilciler için raporlar hazırlamaktadır. Bu rapor ve analizler kamuya açık olup herkes tarafından rahatlıkla indirilip, incelenebilmektedir. Ülkenin dış politikası ve geleceği hakkında birçok resmi ifadenin bulunduğu raporlar istihbarat teşkilatları tarafından da kullanılmakta ve analiz edilmektedir. Sadece istihbarat teşkilatları değil farklı devletlerin kurumları da mevcut Kongre raporlarından yararlanmaktadır (USA, 2023).

Siyasi ve diplomatik raporların yanı sıra Merkez Bankaları tarafından da rapor ve analizler yayınlanmaktadır. Örneğin küresel finansal sistemde büyük önem arz eden ABD Merkez Bankası (FED) birçok kurum ve kuruluş tarafından takip edilmektedir. FED'in atacağı adımların diğer ülkeleri de etkilemesi ve açıkladığı politikaların önem arz etmesi bir açık kaynak olarak FED raporlarının kullanılmasına neden olmaktadır. IMF, Dünya Bankası, Avrupa Merkez Bankası, Türkiye Cumhuriyeti Merkez Bankası, İngiltere Merkez Bankası ve Yeni Kalkınma Bankası rapor ve analizleri de bu şekilde değerlendirilebilir. Firma ve şirketlerde benzer şekilde sektörler hakkında birçok analiz ve rapor yayınlamaktadır. Siyasi, ekonomik, kültür ve sosyal alanları kapsayan kurumların raporlarının yanı sıra istihbarat teşkilatları da rapor, analiz veya görüş şeklinde paylaşımlar yapmaktadır. CIA, FBI, MI6, MİT ve MOSSAD gibi istihbarat teşkilatlarının raporlarına akademi de sürekli rastlanmaktadır. Yeni tehditler, değişimler ve potansiyel taşıyan olaylar istihbarat teşkilatlarının raporlarında işlenebilmektedir. Örneğin CIA tarafından yayınlanan raporlar diğer ülke teşkilatları tarafından ciddi anlamda takip edilmektedir. Raporlarda ifade edilen tehdit veya tehdit potansiyeli taşıyan olaylar karar alıcılara

iletilerek önlemler alınması sağlanmaktadır. Çin, Rusya ve Türkiye gibi ülkelerde de benzer bir durum söz konusudur (Kasapoğlu, 2021).

3.1.4. Akademik yayınlar ve mesleki sunumlar

Akademik olarak yayınlanan tez ve makalelerin veya mesleki görüşlerin yayınlandığı sunumların internet siteleri veya dergilerde yayınlanması ile erişime açık hale gelen verilerle ilgilenen alandır. Birçok kaynak, veri ve görüş akademik yayınlarda kendine yer bulmaktadır. Küresel düzeyde bilgi paylaşımının mümkün olduğu akademik yayınlar süreklilik arz ederek açık kaynak istihbaratına verimli bir kaynak çeşitliliği sağlamaktadır. Kitap, makale, tez veya analiz şeklinde farklı çeşitleri olan akademik yayınlar hem geçmiş hem de gelecek hakkında önemli bilgiler sunmaktadır. Kamunun üst düzey yetkilileri emeklilik dönemlerinde kendi anılarını kitap olarak yayınlayabilmektedir. Bu kaynaklar ülkelerde yaşanan önemli gelişmeler hakkında hem istihbarat teşkilatlarına hem de diğer ilgilere açık bir kaynak sunmaktadır. Mesleki sunumlarda da akademik yayınlarda olduğu gibi bir durum söz konusudur. Ayrıca mesleki sunumlar firma ve şirketler tarafında da kullanılabilmektedir (Kasapoğlu, 2021).

3.1.5. Ticari veriler

Ticari olarak bütçe, faaliyet raporları, vergi raporları, kar bildirimleri, kurulan veya iflas eden işletme sayıları gibi bilgileri araştıran alandır. Devlet, firma, kurum, şirket ve bireyler açısından farklı anlamlar taşıyan ticari veriler rekabet halinde olunan aktörlere karşı rekabet gücünü artıran bir olgudur. Birçok kurum, kuruluş ve firma yıllık, çeyreklik ve aylık olarak harcama ve bütçelerini paylaşmaktadır. Kamunun şeffaflık gereği yaptığı harcamaları senelik olarak paylaşması ve mecliste 12 aylık dönemin değerlendirilmesi yapılmaktadır. Böylelikle vatandaş, kurum ve diğer aktörler harcamaları kolaylıkla kontrol edebilmektedir. Örneğin MİT'in senelik bütçesini kamu kaynakları üzerinden öğrenmek mümkündür. Aynı durum CIA, FBI ve MI6 için de geçerlidir. Genel olarak devletlerin bütünü hakkında paylaşım yapan kurumlarda mevcuttur. IMF, Birleşmiş Milletler ve Dünya Bankası bu kurumlara örnek olarak gösterilebilir. Geçmiş yılları, bugünü ve gelecek hakkında devletlerin toplam ekonomisi, ticareti, yatırımları ve harcamaları

hakkında veri paylaşan mevcut kurumlar büyük bir boşluğu doldurmaktadır. Ayrıca CIA'nin yıllık olarak yayınladığı *Factbook*'larda her devlet hakkında önemli bilgilere ulaşmak mümkündür. Devletlerin sektörlere verdikleri destekler, doğum oranları, hastane sayıları, milli geliri, büyüme hızı, istihdam edilen kişi sayısı ve toplam dış ticaretini CIA'nin kitap, rapor ve analizlerinde yıllık olarak bulmak mümkündür (CIA, 2023).

3.2. Açık Kaynak İstihbaratının Kullanıldığı Alanlar

Açık kaynak istihbaratı birçok alanda kullanılan bir yöntemdir. Genellikle ülke, kurum ve kişi hakkında bilgi edinmek için tercih edilir. Aynı zamanda siber güvenlik, işletme yönetimi, hukuk, tıp ve diğer alanlarda da kullanılabilmektedir. Askeri istihbarat alanında kullanılan açık kaynak istihbaratı askeri taktikler ve ordu konumları hakkında bilgi edinmek için sıklıkla başvurulan bir istihbarat türüdür. Siber güvenlik alanında çevrimiçi alanlara sızma, kimlik tespitinin sağlanması, sosyal medya platformları üzerinden yapılan tartışmalardan haberdar olma, siber saldırılara hazırlıklı olma ve sızma harekâtını engelleme gibi hedefler doğrultusunda açık kaynak istihbaratı kullanılmaktadır. İşletme yönetiminde açık kaynak istihbaratı piyasa araştırması, rekabet analizi, müşteri geri bildirimleri ve pazarlama stratejileri için tercih edilmektedir. Hukuk alanında açık kaynak istihbaratına mahkemede delil toplama ve suçluların tespitini sağlamak için başvurulmaktadır. Açık kaynak istihbaratının kullanıldığı bir diğer alan teknoloji ve bilişim alanıdır. Bu alan rakip devletler arasındaki teknoloji rekabetinde sıklıkla kullanılırken firmalar tarafından da tercih edilebilmektedir. Devletlerin psikolojik, toplumsal ve sosyal karışıklıklardan kaçınmak için açık kaynak istihbaratını kullandığı bir realite olarak karşımıza çıkmaktadır. ABD, Çin, Rusya ve Fransa gibi ülkelerde kamu kurumları toplum arasındaki tartışma ve organizasyonları yakından takip etmektedir. Bu takip sonucu farklı protesto uygulamalarının önüne geçilebilmektedir (Arslan, 2023).

Güvenlik ve istihbarat, ticari sırların açığa çıkarılması, yönetime karşı avantaj elde edilmesi gibi birçok alanda başvurulan bir yöntem olan açık kaynak istihbarata bireysel olarak yaklaşıldığında kişisel bilgilerin korunması hedefi öne çıkmaktadır. Firmalar açısından bakıldığında ticari sırların, rekabet

avantajının ve pazarlama stratejilerinin belirlenmesi ve sürdürülebilir hale getirilmesi önem taşımaktadır. En yüksek yönetim mercii olan devletler açısından açık kaynak istihbaratı ise bilgi ve veri güvenliği anlamını taşımaktadır. Açık kaynak istihbaratına konu olan kaynaklar kolaylıkla ulaşılabildiği için devletlerin geleceğinde, toplumsal barışında ve güvenliğinde önem taşımaktadır. Bu önemin bir göstergesi olarak sosyal medya platformlarında istihbarat teşkilatları hakkındaki bilgiler kolaylıkla ifşa edilebilmektedir. Bu durum yasaklama, engel koyma veya hukuki süreçleri hızla işletme ile çözüme kavuşsa da güvenlik zafiyeti ortaya çıkarmaktadır. Bu zafiyet diğer operasyonel kuvvetlerin hareket alanlarını negatif olarak etkilemektedir. Örneğin Libya'da gizli operasyon yürütenlerin sosyal medya aracılıyla bireyler tarafından yayınlanması basit bir bilginin paylaşılması olarak görülebilir. Ancak açık kaynaklardan alınan bilgi sahada faaliyet yürüten diğer istihbarat çalışanlarını zor durumda bırakmıştır. Operasyonel gücün kimlik olarak ortaya çıkması Türkiye'nin Libya'daki çıkarlarının zedelenmesine neden olmuştur. Bu yönüyle açık kaynak istihbaratı önemini bir kez daha ortaya koymuştur (Ekşim ve Civelek, 2019, s. 827-836).

Oyun şirketleri veya uygulamaların satışında temel amaç verilerdir. Mevcut veriler online olarak her türlü saldırıya açıktır. Bu saldırıların önüne geçilmesinde yazılımlar ve koruma programları önem taşımaktadır. Buradaki yazılım ve koruma programları açık kaynak istihbaratına benzetilebilir. Açık kaynak istihbaratının kullanım alanlarından biri olan siber yazılımlar gelişen teknoloji ile daha fazla öne çıkmıştır. Sadece birey ve kurumlar açısından değil devletler içinde aynı durum geçerlidir. Kamuda çalışanlarının kimlik, veri, bilgi, yetenek ve konum bilgilerine erişimi bulunan sosyal medya platformları her zamankinden daha önemli hale gelmiştir. Bu haliyle açık kaynak istihbaratı diğer alanlarla etkileşim halinde kritik pozisyonunu korumuştur. Mevcut küresel trendler içerisinde teknoloji merkezli dönüşümler genişlemektedir. Buradan hareketle açık kaynaklardan toplanan veri ve bilgilerin de artması ve önem kazanması kaçınılmazdır. Kullanım alanlarını her dönem genişleyen açık kaynak istihbaratı hem devletlerin hem de firmaların açık kaynaklara olan başını da değiştirmektedir (Ekşim ve Civelek, 2019).

3.3. Açık Kaynak İstihbarat Teknikleri

Açık kaynak istihbaratı toplama teknikleri arasında birçok araç ve teknoloji kullanılabilmektedir. Bunlar arasında web tarama araçları, yazılımlar, veri görselleşme araçları, web sorgulama araçları ve veri madenciliği yazılımları bulunmaktadır. Açık kaynak istihbaratı bir istihbarat toplama yöntemi olarak bilgilerin toplanması ve analiz edilmesiyle sağlanmaktadır. Birçok üst ve alt başlığın yanı sıra açık kaynak istihbaratı bireysel olarak da yürütülebilmektedir. Bireyselliğin en yüksek oranda gerçekleştiği açık kaynak istihbaratı diğer alanlarla etkileşim halinde yapılır. Bu etkileşim hali coğrafi istihbaratın kullanım halinde olduğuna işarettir. Uydu ve hava fotoğrafları kullanılarak toplanan istihbarat daha sonra Google Map üzerinden kolaylıkla istihbarat için tercih edilebilir. Sinyal istihbaratı, siber istihbarat, sosyal medyada paylaşılan bilgi, fotoğraf ve konumlar da açık kaynak istihbaratına konu olan alanlardır. İnsan ve kurum istihbaratında belli kısımlarda benzeşen açık kaynak istihbaratı basit konular içinde kullanılabilir. Örneğin iş görüşmeleri ve iş başvurusunda bulunan kişilerin sosyal medya hesapları üzerinden basit istihbarat faaliyetleri yürütülebilir. Hem firma hem de kamu kurumları tarafından mevcut basit istihbarat faaliyeti gerçekleştirilebilir (Durdallı, 2023).

Karşı taraf hakkında bilgi toplamak amacıyla yapılabilen açık kaynak istihbaratı siber suçlar, tehditler ve siber güvenlik faaliyetleri içinde yürütülebilir. Ancak kayıp aile üyelerinin bulunması gibi durumlar amacıyla da açık kaynak istihbaratı kamu kurum ve kuruluşları tarafından kullanılabilir. Kitap, dergi, gazete, halka açık belgeleri, kamu kurumlarının internet siteleri, veri tabanları, TV kanalları, haber arşivleri ve sosyal medya platformları açık kaynak istihbaratının birer kaynağı olarak teknikleri belirlemektedir. Kurum, kişi veya firmaların ihtiyaçlarına göre teknikler farklılaşabilmektedir. İstihbarat teşkilatları için ise genellikle önem arz eden duruma göre teknik ve kaynak tercih edilmektedir (Durdallı, 2023). Açık Kaynak İstihbarat toplama tekniklerinde her şeyden önce belirli bir yöntem takip edilirken, Osınt Framework olarak bilinen araştırma teknikleri başta olmak üzere, Lampyre, Maltego, Recon-Ng, SpiderFoot, Shodan, Google Dork gibi yazılım dilimize bağlı olarak kullanılabilen programlar kullanılabilmektedir. Ayrıca StalkFace, Twitonomy gibi sosyal medya analiz araçları da kullanılmaktadır. Açık Kaynak

İstihbarat analizi için belirli bir strateji doğrultusunda Osint aşamaları olarak adlandırılan profesyonel yöntemler kullanılmaktadır. Hedefe yönelik olarak arama motorları üzerinden basit aramalar yapıldıktan sonra, DNS kayırları ve IP adresleri tespit edilmektedir. Hedefin e-posta tespiti de yapıldıktan sonra kullanılan teknolojik alt yapı hakkında bilgi toplanmaktadır. Bu veriler doğrultusunda kullanılan yazılımlar, programlar, çevrimiçi cihazlar tespit edilmektedir (Durdallı, 2023).

3.4. Açık Kaynak İstihbarat Analizi

Kullanılan teknikler arasında aynı zamanda Doğal Dil İşleme (NLP), veri görselleştirme, ağ analizi, veri madenciliği gibi yöntemler de kullanılmaktadır. Açık kaynak istihbarat analizinde uygulanacak yöntemler ve veriler hedeflenen konulara göre değişkenlik gösterebilmektedir.

Doğal Dil İşleme (NLP): İnsan dilinin doğal yapısını anlayarak, dil verilerini işlemek için kullanılan teknolojidir. Anahtar kelime ve konuları tanımlayarak duygu ve düşünceleri belirlemek için kullanılmaktadır.

Veri görselleştirme*:* Verilerin görsel olarak temsil edilmesi için kullanılan teknolojidir. Büyük veri kümelerini grafik, harita ve diğer görsel biçimleri ile sunuma ve analize hazır hale getirmektedir.

Ağ Analizi*:* Belirli bir ağ üzerindeki veri kaynaklarını ilişkilendirerek bağlantıları analiz için hazır hale getiren tekniktir. Veri Madenciliği: Büyük veri kümelerindeki önemli ve stratejik bilgileri ortaya çıkararak keşif ve analiz yeteneği sunan tekniktir (Arslan, 2023).

4. AÇIK KAYNAK İSTİHBARAT ÖRNEKLEMİ

4.1. Silk Road Örneği

Dread Pirate Roberts kod adı ile dijital yeraltı dünyasında, adını Asya'daki ticaret yolundan esinlenerek Silk Road (İpek Yolu) koyduğu bilinen Ross William Ulbricht adındaki Amerikalı bir gencin kurduğu darknet pazarı web sitesidir. 2011-2013 yılları arasında faaliyet yürüten darknet pazarında 100 binin üzerinde alışveriş yapıldığı bilinmektedir. Uyuşturucu, kanun dışı madde ve diğer ürünlerin satışını yapan Silk Road kara market olarak da anılmaktadır. Milyonlarca dolarlık bir market haline gelen Silk Road'a bilinen internet siteleri üzerinden ulaşmak mümkün değildir. Bu nedenle iki yıl faaliyetlerini kolaylıkla yürütebilen sitenin 2020'de yeniden faal hale geçtiği ve kripto para üzerinden illegal işlemlere devam ettiği görülmüştür. FBI'nın açık kaynaklardan aldığı bilgi ve veriler üzerinden operasyon yapılan ve kurucusunun ömür boyu hapiste olduğu Silk Road darknet pazarının günümüzde hala faal olduğu üzerine tartışmalar yapılmaktadır. Ancak ABD resmi makamlarının ve Avrupa'daki diğer devletlerin darknet pazarları ile mücadele ettiği görülmektedir. 2020'de yapılan yeni operasyonda 3,36 milyar dolarlık kripto para ele geçirilmiş olması ise operasyonların süreceğine işaret olarak gösterilebilir (Department of Defense, 2010).

Ekim 2013'te FBI'ın darknet sitesini ele geçirmesiyle başlayan ve sorumluların cezasıyla sonuçlanan operasyon açık kaynak istihbaratının uygulaması açısından iyi bir örnektir. FBI çalışanları açık kaynaklarda yer alan verilerle hareket etmiş ve kurucu kadroyu yakın takibe almıştır. Silk Road'un kurucularının sosyal medya hesapları üzerinden yapılan bilgi ve veri toplamalar, sık kullanılan konumlarla birleştirilmiş ve operasyonun gerçekleşmesi sağlanmıştır. Silk Road 2.0. ismiyle kurulan yeni bir site de FBI tarafından yürütülen soruşturma ile Onymous Operasyonu adıyla Kasım 2014'te kapatılmıştır. 2020'de yeni bir operasyon daha yapılarak Silk Road evreninin para kaynakları kesilmeye çalışılmıştır. Kripto para olarak tutulan darknet

stoklarının kamu tarafından ele geçirilmesiyle yasal dışı para trafiği de engellenmiştir. Silk Road ile bağlantılı Zhong, kripto para üzerinden yapılan ticari işlemlerde ise kalpazanlık yöntemlerine başvurarak iki farklı suça iştigal etmiştir. FBI mevcut suçların takibini yine açık kaynaklardan yaparak açık kaynak istihbaratının önemini ve işlevini tekrar gözler önüne sermiştir (Balyemez, 2022)

Silk Road operasyonu açık kaynaklar itibari ile FBI tarafından açık kaynak takibi örneğinde kendi sitesinde de yayınladığı bilgilerle örtüşmektedir. 20 Ocak 2011 tarihinde bir vergi temsilcisinin, çevrimiçi bir forumda web sitesi ile ilgili bir gönderi keşfetmesi, bundan sekiz ay sonrasında da aynı kullanıcının bir iş ilanı yayınladığının tespit edilmesi durumu, kullanıcıların Ulbricht'e mail göndermeye yönelttiğini analiz etti. Müfettişlerin mahkeme emirleri kapsamında elde ettikleri ağ trafiği ve kaydının izini sürmeleri sonunda Ulbricht' in şüpheli olarak tespit edildiği anlaşılmıştır (FBI, 2023).

Açık Kaynak tespitine dava duruşmalarında FBI'ın iddiasına göre Ulbricht 'in Lınkedın profilinde bu suçu işlediğini alenen yazılı olduğu ifade edilmektedir. 2010 yılında eğitimini tamamlamasından bu yana, "insanlara, sistemin güç kullanımının olmadığı bir dünyada yaşamanın nasıl bir şey olacağına dair ilk elden bir deneyim yaşatmak için bir ekonomik simülasyon yaratmaya" odaklandığını belirtiyor (Hume, 2013).

İlk modern darknet market olarak Silk Road gizli servis sağlayıcılar üzerinden ve Tor networkuna bağlı olarak kurulmuştur. URL takibinin mümkün oluşu nedeniyle FBI yetkilileri yapılan her işlemi yakından takip etmişlerdir. FBI'da görev yapan Gray Alford Google aracıyla ilk araştırmaya başlamış ve URL ile darknet'e ulamıştır. Bütün Silk Road URL adreslerini teker teker deneyen ve uzun uğraşlar sonrası doğru adresi bulan Alford gizli bilgilerden değil deneme-yanılma yolunu denemiş ve başarılı olmuştur. Açık kaynaklardan internetle yapılan takip sonucu kurucular yakalanmıştır. Bitcoin ve diğer kripto paralar üzerinden yapılan ticari para transferi de böylelikle tespit edilmiştir. FBI'ın uyguladığı açık kaynak istihbaratı The Farmer's Market ve Atlantis gibi yasa dışı siteler için de ilerleyen dönemde örnek teşkil etmiştir. FBI'ın yürüttüğü Silk Road operasyonu daha sonra film, dizi ve makale gibi birçok olay için ilham kaynağı olmuştur. Özellikle yasa dışı para transferi, kalpazanlık

ve uyuşturucu ile mücadelenin teknolojik hale geldiği bir dönemde Silk Road olayı birçok yeni soruşturmanın öncülü haline gelmiştir (Kushner, 2014).

Silk Road ilk darknet pazarı olması nedeniyle birçok ilklere sebep olmuştur. Platformun finansal transferlerde kripto para kullanması ve diğer yasa dışı ürünlerin satışına izin vermesi birçok kanunun online olarak ihlal edilmesini beraberinde getirmiştir. Online sistemlerin yaygınlaşması sonrası kanuni açıkların meydana gelmesi ve kamunun bu açıkları hızlı şekilde kapatamaması diğer alanlara negatif yansımıştır. Özellikle genç nesiller arasında yaygınlaşan online işlem ve uygulamalar kamu düzeni ve güvenliğinin sürekli reform halinde tutulması gerekliliğini gözler önüne sermiştir. Silk Road örneği de bu minvalde ele alındığında kamu kurumlarının kendilerini revize etmeleri gerekliliğinin tekrar göz önüne çıkarmıştır. Kendi içerisindeki ilklerle FBI'ın gerçekleştirdiği operasyonlar uzun yıllara yayılarak online sistemler üzerindeki denetimin artırılmasını sağlamıştır. Günümüzde birçok sosyal platformu denetleme girişimleri olan devletlerin Silk Road benzeri operasyonlarda dersler çıkardığını söylemek mümkündür (Kushner, 2014).

Silk Road platformunun FBI tarafından kapatılması yasa dışı satış ağının diğer alanlara kaymasına neden olmuştur. FBI'ın hesaplamalarına göre Silk Road ağının çökertilmesi sonrası Bitcoin üzerinden yapılan uyuşturucu trafiği iki katına çıkmıştır. Bir istihbarat örgütü olarak FBI ilerleyen dönemde Silk Road operasyonunda edindiği tecrübe ve birikimi farklı online suçların önlenmesinde kullanmıştır. Örneğin 2020'de 1 milyar dolarlık kripto para transferi FBI'yı tekrar hareket geçirmiş ve Silk Road para transfer sistemine operasyon gerçekleştirilmiştir. Farklı ülkeler üzerinden yapılan transfer ABD'deki yasa dışı işlemler için kullanılmıştır. Silk Road operasyonunu gerçekleştiren ekibin birikimlerinden yararlanarak transfer tespit edilmiş ve elde edilen miktar kamu kaynaklarına aktarılmıştır (İnvesting.com, 2020). Silk Road yasa dışı faaliyetlerin yanı sıra online oyunlar üzerinden de iletişim ve alışverişin olduğu bir yapıdır. Bu yapının iletişim kanalları için takibi zorlaştırmak için kullandığı yöntemler istihbarat teşkilatlarının işini zorlaştırmıştır. Ancak açık kaynaklar üzerinden yapılan takip ve araştırma platformun çökertilmesini sağlamıştır. Bu açıdan Silk Road operasyonuna

yaklaşıldığında açık kaynakların nasıl bir öneme haiz olduğu daha fazla öne çıkmaktadır (Hume, 2013).

4.2. Terörizm Analiz Platformu (TAP)

Terörizm Analiz Platformu (TAP) 2017'de Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA) ve STM Savunma tarafından hayata geçirilen bir projedir. TAP, 1970-2020 arasında dünyada meydana gelen terör olaylarının datalarını toplamayı ve analiz etmeyi hedeflemektedir. Ulusal ve uluslararası terör olaylarını açık kaynaklardan toplayarak bir istihbarat faaliyeti yürüten TAP ulusal güvenlik, istihbarat teşkilatları, akademisyenler, araştırmacılar ve terörizm üzerine çalışmalara katkı sunmayı amaçlamaktadır. 2017'de ulusal bir inisiyatif olarak hayata geçirilen TAP yeni saldırıları da kendi data ve veri setlerine eklemektedir. 40 binden fazla terör olayının verilerini gözler önüne seren TAP, Türkiye özelinde PKK saldırılarına odaklanmaktadır. PKK saldırını açık kaynaklardan elde ettiği bilgilerle analiz eden platform Türkiye'de bu minvalde ve büyüklükte veri toplayan en büyük kaynaktır. TAP'ın kuruluşu, gelişimi ve bir inisiyatif haline gelmesinde kamu-özel sektör arasındaki iş birliğinin ve koordinasyonun önemli bir yeri bulunmaktadır (TAP, 2023).

Prof. Dr. Murat Yeşiltaş'ın gözetiminde Sibel Düz'ün editörlüğünde Mehmet Özdemir, Salah Devrim, İsmail Üzen ve Felix Shihundu'nun yardımlarıyla toplanan datalar siteye üye olunmasıyla tam olarak ulaşılabilmektedir. TAP'ın veri ve data toplama yöntemi olarak benimsediği birçok kaynak bulunmaktadır. Kamuya açık kaynaklar üzerinden toplanan veriler bir online havuzda toplanarak elektronik ortama iletilmektedir. Yüksek kaliteli yazılım yardımıyla periyodik olarak güncellenen veriler konum bilgisiyle birlikte hizmete sunulmaktadır. Her terör saldırısının datası bilgi, konum, coğrafi bölge, saldırının derece, etkisi, yaralı ve zayiat sayısı, taktik, hangi terörist grubun sorumluluk üstlendiği gibi bütün bilgiler platformda yer almaktadır. Yeni saldırıların olması halinde açık kaynaklar üzerinden bilgiler yenilenmekte ve platformdaki veriler en güncel şekilde saklanmaya çalışılmaktadır. Türkiye, Suriye ve Irak gibi ülkeler hakkında veri paylaşmanın yanı sıra Latin Amerika, ABD, Orta Asya, Kafkasya, Avrupa ve Balkanlar özelinde de platformdan veri çekmek mümkündür (TAP, 2023).

TAP, Türkiye hakkında topladığı terör saldırıları verilerini iki kaynaktan elde etmektedir. İç İşleri Bakanlığı ve Millî Savunma Bakanlığının resmî açıklamaları birincil kaynak olarak tercih edilmiştir. İkincil kaynak olarak gazete, internet sitesi, röportaj ve açıklamalar dikkate alınmaktadır. Günlük takip edilen terör olaylarında PKK, DHKP-C, DEV-SOL, DEASH, FETO, THKP-C, YPG, ASALA ve JCAG gibi örgütlerin saldırıları mercek altına alınmaktadır. Örgütlerin uyguladığı terör saldırılarının tipi, amacı ve verdiği zarar sistematik olarak kayıt altında tutulmaktadır. İç İşleri ve Millî Savunma Bakanlığının uyguladığı terör operasyonları hakkında ayrıntılı bilgilere de TAP üzerinden ulaşmak mümkündür. İç İşleri Bakanlığının açıklamaları ülke içindeki saldırılarda kullanılırken Millî Savunma Bakanlığının bilgi ve açıklamaları Suriye ve Kuzey Irak'a yapılan terör operasyonlarında tercih edilmektedir. Diğer kurumların rapor, analiz ve açıklamaları da TAP'ın veri setlerine kaydedilerek 50 seneden fazla bir süreçte terörün röntgeni çekilmektedir (TAP, 2023).

50'den fazla ülkede güvenlik birimlerinin resmî web sayfalarından toplanan bilgiler 33 farklı terör organizasyonu içerecek şekilde kaydedilmektedir. Mevcut tercih edilen terör örgütleri daha çok Orta Doğu ve Türkiye'de aktif olarak terör saldırıları gerçekleştirmektedir. Ancak ihtiyaç doğması halinde farklı ülke ve terör örgütleri TAP'a eklenebilmektedir. 10 farklı kanun gücü şeklinde devletlerin terör operasyonları kategorize edilirken 26 farklı terör saldırı tipi datalar da bulunmaktadır. Köy, kasaba ve şehir ayırımı gibi ayrıntılara da TAP'da ulaşmak mümkündür. Bütün bilgilerin açık kaynak ve açıklamalardan elde edildiği TAP uygulaması yeni nesil teknolojik dönüşümleri gözeterek hizmete sunulmuştur. Bu hizmetin bir yansıması olarak birçok kişi terör saldırıları hakkında 50 yıldan fazla bir dönemde bilgi ve verileri ulaşma imkânına kavuşmuştur. Bireylerin yanı sıra kamu kurumları da rahatlıkla verilere ulaşabilmektedir. Açık kaynak istihbaratının önemli bir örneği olan TAP kamu kurumlarının dışında yarı özel bir girişimdir. Bu yarı özel girişim olma altyapısı açık kaynak istihbaratının bireyler tarafından nasıl yürütüleceğine de örnek teşkil etmektedir (TAP, 2023). Silk Road ve TAP örnekleri açık kaynak istihbaratında farklı olay, kurgu ve hedeflerle karşımıza çıkmaktadır. Silk Road kalpazanlık örneği olarak, TAP ise terör olayları

verilerine odaklanan olgulardır. Ancak iki olay da açık kaynak istihbaratı açısından önem taşımaktadır. Yeni nesil teknoloji trendleri de ele alınan iki olayda etkili olmuştur.

TAP uygulaması rapor, analiz ve yorum şeklinde paylaşımlar yapmaktadır. Online olarak ulaşılabilen yayınlar birer açık kaynak örnekleridir. Yıllık olarak terör örgütlerinin yaptığı saldırı ve eylemlerin değerlendirildiği yayınlar ülke, örgüt ve olaya göre ayrıntılı bilgi ve yorumlamalar sunmaktadır. Ayrıca TAP'da uluslararası terörizm ile ilgili yapılmış diğer rapor, analiz ve kurum açıklamalarına da rastlamak mümkündür. Örneğin ülkelere göre her yıl açıklanan Küresel Terörizm İndeksi belli periyotlarla TAP uygulamasında farklı araştırmacılar tarafından analiz edilmektedir (TAP, 2023).

TAP resim, podcast ve uzman görüşlerine yer verme gibi üç farklı şekilde terör saldırılarını analiz etmektedir. Resimler olay örgüsünü içerirken terör olaylarının insan zihninde daha iyi şekilde kurgulanmasını sağlamaktadır. Podcast akademisyen ve uzmanların yorumlarını içeren sesli olay, kurgu ve süreci yorumlamaktadır. Uzman görüşleri TAP sitesinde online olarak yayınlanan makalelerdir. Üç farklı şekilde terör olaylarını yorumlayan ve analiz eden TAP sadece data paylaşmakla kalmayıp terör olaylarının hedef, amaç ve sonuçlarına da yer vermektedir. Yeni araştırmalar hakkında yaz dönemlerini içerecek şekilde eğitim programı düzenleyen Terörizm Analiz Platformu kendi data ve verileri üzerinden uzman yetişmesine de katkı sunmaktadır. Konferans ve seminerler üzerinden de benzer uygulamalar hayata geçirilmektedir. Yapılan eğitim programlarında risk analiz eğitimi ve karşı terör eğitimi verilerek yeni uzmanlar yetiştirilmek istenmektedir (TAP, 2023).

4.3. Karşılaştırma ve Diğer Örnekler

Açık kaynak istihbaratına Walt Disney'in Küresel Güvenlik Departmanı ve Küresel İstihbarat ve Tehdit Analizi birimleri örnek olarak verilebilir. Bu birimler savaş, deniz yetki alanlar, jeopolitik ve itibar riskleri, uluslararası terörizm, aktivizm, kültürel eğilimler ve siber güvenlik üzerinde araştırmalar yapmaktadır. Yaptıkları araştırma ve topladıkları bilgiler özel bir firmanın açık kaynaklardan topladığı veri ve analize dayanmaktadır. Şirketin yaşayabileceği risk ve fırsatlar konusunda rapor, analiz ve gelecek projeksiyonu yapan Küresel

İstihbarat ve Tehdit Analizi birimi elde ettiği bulgularla firmanın korunmasını sağlamaktadır. Disneyland başta olmak üzere tüm şirkete risk ve fırsatlar için yönlendirmeler sunan açık kaynak istihbaratı fırsat, risk ve yönlendirme imkânı sunmaktadır. Gazeteci, araştırmacı ve güvenlik uzmanlarının tıpkı Küresel İstihbarat ve Tehdit Analizi birimi gibi açık kaynak istihbaratına başvurabilmektedir. Örneğin ABD'de bir gazeteci açık kaynak takibi üzerinden yürüttüğü soruşturma sonrası CIA ile Latin Amerika'daki hükümet arasındaki iş birliğinin ifşa etmiştir. Açık kaynak istihbaratı yukarıdaki örneklerde olduğu gibi casusluk veya illegal yöntemler üzerinden yapılmamaktadır. Ayrıca açık kaynak istihbaratının yapılmasında bireysel veya kurumsal hedefler yer alabilmektedir. Kişi veya kurumun niyetlerine göre açık kaynak istihbaratının amaçları değişiklik gösterebilmektedir (Durdallı, 2023).

Türkiye'de açık kaynak istihbaratı yürüten özel firmalar bulunmaktadır. Örneğin ALLSAFE Siber Güvenlik firması belli bir ücret karşılığında kişi, kurum veya kuruluşlar hakkında açık kaynak istihbaratı hizmeti sunmaktadır. Ayrıca açık kaynak istihbaratında toplanan veri ve bilgileri analiz ederek istenilen hizmetin daha geniş hale gelmesine yardımcı olmaktadır. Özellikle online kaynaklarda elde edilen bilgiler firmanın analiz biriminde derlenerek daha geniş bir açıdan birey, kurum ve kuruluşa yaklaşılmasını sağlamaktadır. Kademeli olarak yürütülen araştırma sürecinde firma yasal olmayan herhangi bir kaynağı da kullanmamaktadır (ALLSAFE Siber Güvenlik, n.d.).

Türkiye dışında farklı ülkelerde açık kaynak istihbaratına başvuran farklı kurum, uygulama ve bireylerde bulunmaktadır. Kamu kurumları terörle mücadele aktif olarak açık kaynak istihbaratından yararlanmaktadır. Örneğin radikalleşme günümüzde önemli bir problemdir. Kamu kurumları sosyal medya analizleriyle radikalleşme eğilimi olan kişileri tespit etmekte ve izlemeye almaktadır. Açık kaynaklardan olan sosyal medya ile yapılan bilgi toplama ve analizi daha sonra olabilecek terör saldırılarının büyük oranda önüne geçilebilmektedir. ABD'de belli aralıklarla gerçekleşen bireysel terör saldırılarının daha önceden tespitinde ve önlenmesinde mevcut açık kaynak istihbaratı büyük önem taşımaktadır (Ökten, 2023, s. 31-32).

Açık kaynak istihbaratı hakkında örnekleri çoğaltmak mümkündür. Ancak TAP ve Silk Road örnekleri iyi bir karşılaştırma altyapısı sunmaktadır. TAP

yarı-özel kurumların ve akademisyenlerin açık kaynaklardan aldığı bilgilerle açık kaynak istihbaratı yürütmektedir. Silk Road örneği de kamu kurumları tarafından ele alınan açık kaynakların nasıl yararlı şekilde kullanılabileceğini işaret etmektedir. Özellikle açık kaynakların günümüzde daha fazla önem kazanması, kullanılması ve ilgi çekmesi ilerleyen yıllarda da açık kaynak istihbaratına başvurulabileceğini göstermektedir. Silk Road ve TAP'dan yararlanan kişi, kurum ve kuruluşlara bakıldığında ise kamu güvenliğine yarar gösterdiğini söylemek mümkündür. Terör faaliyetleri için bir havuz oluşturan TAP ve diğer yapılacak siber suçlarla mücadelede yeni yöntemler ortaya koyan Silk Road Operasyonu açık kaynak istihbaratının yarar alanlarına örnek olarak gösterilebilir (Ökten, 2023).

Meta datalar, kod araştırma, kimlik tespiti, telefon numarası bulma, e-mail sertifikasyonu, sosyal medya hesaplarına erişim, resim incelemesi, harita ve topografya araştırması ve internet adresi üzerinden takip gibi birçok yöntem günümüzde açık kaynak istihbaratında kullanılabilmektedir. Meta datalar kişi ve kurum bilgilerine ulaşmak için tercih edilmektedir. Kod araştırma verilere daha rahat erişim için kullanılmaktadır. Kimlik tespiti kurum veya bireyler tarafından rahatlıkla yapılabilmektedir. Telefon numarası bulma işlemleri online siteler kullanılarak gerçekleştirilebilmektedir. E-mail ve sosyal medya hesaplarına erişim kolaylıkla internet üzerinden yapılabilmektedir. Resim incelemesi, harita ve topografya araştırması da diğer açık kaynaklar gibi birey, kurum veya kuruluş tarafından rahatlıkla kullanılabilmektedir. Açık kaynak istihbaratında kullanılan kaynakları artırmak veya daha fazla örnekle desteklemek mümkündür. Ancak araştırma soruları ve tezin içerdiği sınırlar gereği daha fazla örnek vermeye gereksinim duyulmamıştır (Ökten, 2023).

5. İSTİHBARATTA FONKSİYON ANALİZİ

5.1. Kamu Güvenliği ve Açık Kaynak İstihbaratı

Güvenliği sağlama kamunun en asli vazifelerinden biridir. Teknolojideki değişim ve hızlı dönüşümle birlikte güvenlik ihtiyacı farklı alanlarda gelişerek artmıştır. Paylaşım siteleri, casus yazımlar, bilgi teknolojisi ve diğer sahalarda ciddi anlamda yol kat eden günümüz teknolojik altyapısı kamunun güvenliğe bakışını farklılaştırmıştır. İnternet evreni de çok büyük miktarda verinin kolaylıkla ulaşıldığı bir bilgi ağı olarak öne çıkmıştır. Devlet-toplum arasındaki ilişkinin de değişmesine neden olan çevrimiçi ağ, internet ve sosyal platformlar kamu güvenliğinde siber güvenliğe daha fazla önem verilmesine neden olmuştur (Keskin, 2020, s. 195-202).

18. yüzyıldan itibaren ABD açısından kritik konumda olan açık kaynak istihbaratı ülkenin bağımsızlığına katkı sağlamıştır. George Washington, Amerikan devrimi sırasında karşı istihbarat için İngiliz birliklerinin hareketlerini İngiliz gazetelerinden elde ettiği bilgilerle sağlıyordu. Elde edilen bilgiler üzerinden kendi ordularının konumlarını revize eden ve ülkenin bağımsızlığını yürütmeye çalışan Washington daha sonra diğer ülkelere de örnek teşkil etti. 1808'de İspanya'da Fransızlara karşı savaşan İngiliz bir dük Fransızların konumlarını Times gazetesi üzerinden okuyor ve komutanlarına da okuma talimatı veriyordu. Times gazetesi Fransız ordularının konumları hakkında detaylı bilgi sunarken ücretsiz istihbarat çalışmalarının konusuna mahzar oldu. 1863'de General Lee, kuzey bölgelerindeki birliklerin hareketlerini gazeteden sağlanan bilgilerden hareketle belirliyordu. Fransız General Patton, İkinci Dünya Savaşında benzin istasyonlarında yer alan haritalar göre yerini ve ileri harekât noktalarını tespit etmiştir. (Keskin, 2020, s. 198-199).

1939'da İngiliz hükümeti yabancı basın takibi için BBC'ye talimat verdi. Günümüzde BBC Monitoring olarak yayın hayatına devam eden birim aktif olarak çalışmalarına devam etmektedir. 1943'de BBC günlük 1,25 milyon

iletişimi takip etti. 1948'de ABD'de de benzer faaliyetler için Kongre Kütüphanesi devreye alındı. Bugün Federal Araştırma Bölümü olarak faaliyetlerine devam eden birim açık kaynaklar açısından önemli bir boşluğu doldurmaktadır. 1941'de ABD'de kurulan Broadcast Monitoring Service günde 500 bin kelimeyi farklı dillerden çevirerek açık kaynak istihbaratı olarak kullanmaktadır. Aynı servis 1 milyondan fazla harita, 50 bin kitap ve 350 bin derginin tasnifini yapmaktaydı (Olcott, 2012).

Soğuk Savaş döneminde Doğu Almanya istihbarat örgütü, Batı Almanya'da bin dergi ve kitabı, radyo ve televizyon kanallarının takibini yapmaktaydı. Günümüzde Almanya istihbaratı BND'nin bilgileri yüzde 85 açık kaynaklardan elde ettiği düşünülmektedir (Tylutki, 2018). Çin, 1958'de Çin Bilim ve Teknik Bilgi Araştırma Enstitüsünü açarak resmi bir kamu kuruluşu üzerinden açık kaynak istihbaratına başvurmuştur. Yabancı dillerde bilgi toplayan, verilerin analizini sağlayan ve diğer kurumlarla paylaşan Araştırma Enstitüsü ilerleyen dönemlerde genişletilerek etki sahası artırıldı. 1966'a kadar Araştırma Enstitüsü 50'den fazla ülkede 11 bin farklı eseri, 500 bin rapor ve 5 milyon patentin çevirisini yaptı ve diğer kurumlarla paylaştı (Hannas William C. et al., 2013).

Sovyet gizli servisi de benzer yöntemlerle 1950'ler boyunca açık kaynaklardan bilgi elde etmiştir. The New York Times ve Scientific American yazılardan bilgileri Sovyet gizli servisine aktaranlar olmuştur. Polonyalı General Wyzel Sniezyski Çekya hakkında bilgileri genellikle askeri şirketlerin resmi raporları ve gazetelerden elde etmiştir. CIA'de de benzer yöntemlerle birçok ülkede istihbarat faaliyeti yürütmüştür (Keskin, 2020, s. 200-201).

Eski CIA Direktör Yardımcısı Christopher Sartinky, halkı uzun yıllar gizlice dinledikten sonra kendi istekleriyle konum, din, politik görüş, arkadaş listesi, e-mail, adres, telefon numarası ve fotoğraflarını paylaşmaları hakkında şaşırdığını ifade etmiştir. Eben Moglen mevcut yaşanılan durumu Facebook var iken KGB'ye ne ihtiyaç var olarak tanımlamıştır. Eski dünyada insanlar hakkında bilgi almak için işkence yöntemlerine başvurulurken bugün insanlar kendi istekleriyle her türlü bilgiyi internette paylaşabiliyorlar. Artık insanları takip etmenin daha kolay olduğunu vurgulayan Moglen açık kaynak istihbaratının eriştiği boyutlara dikkat çekmiştir (Schechter, 2015).

Lınkedın gibi sosyal medya unsurları üzerinden Alman kamu kurumlarına giriş yapmaya çalıştığı bilinen Çin İstihbarat Servisleri açık kaynak istihbarına verilebilecek diğer bir örnektir. İsrail Gizli Servisi, Messenger adresleri üzerinden yaptığı analizle ABD Elçiliğine olan terör saldırısının önüne geçmiştir. Fransız Gizli Servisi DCRI internet siteleri üzerinden yaptığı açık kaynak taramasıyla farklı dönemlerde terör saldırılarını engellemiştir. Siteler üzerinden yapılan taramalar sonrası Fransa'da tutuklamaların yapıldığı da bilinmektedir (Reck, 2014). Kişilerin farklı şekillerde takip edilerek kişilik analizlerinin yapılması uzun süredir devam eden bir açık kaynak istihbarat yöntemidir. Örneğin 2. Dünya Savaşında İngiliz İstihbaratı Alman telgraf operatörlerinin konuşma tarzı, hızı ve hatalarını tahlil ederek profillerini çıkarmıştır (Keskin, 2020, s. 203).

Rus ayrılıkçıların Doğu Ukrayna'da Malezya Havayollarına ait uçağı düşürmeleri sonrası kimin sorumlu olduğunu bulmak için sosyal medya paylaşımları takip edilmiştir. Aynı yöntem Suriye'de sarın gazı saldırılarında da kullanılmış ve faillerin tespiti sağlanmıştır (Keskin, 2020, s. 204).

Açık kaynak istihbaratının kamu güvenliğinki rolü hakkında diğer bir örneği FBI Direktörü James Comey'in tecrübe ettiği sosyal medya takip olayıdır. Ashley Feingberg isimli gazeteci Comey'in oğlunun oynadığı basketbol takımının sosyal medya beğenilerinden James'in oğlunun sosyal medya hesabını buldu. Ardından istek gönderdi. Sosyal medya James'in oğluyla bağlantılı hesapları önerdi ve Ashley James'in yakınlarının sosyal medya hesaplarına ulaştı. Beğeniler ve resimler üzerinden James'in sahte isimlerle açtığı sosyal medya hesaplarına erişti. FBI Direktörünün çevresine çok kolay açık kaynaklardan ulaşan gazeteci önemli bir istihbarat faaliyeti icra etti. James olayların ortaya çıkmasıyla sosyal medya hesaplarını kapatmak zorunda kaldı. Böyle bir durum kamu güvenliğinin ve karar alıcıların güvenliğinin ne kadar zayıf olduğunu gözler önüne sermiştir (Feinberg, 2017).

İstihbaratın fonksiyonel aşamalarından birisi, sadece kamu eli ile değil, ABD istihbarat sisteminde olduğu gibi, istihbarat birimleri çeşitli özel sektör kuruluşları ile de iş birliği halinde hareket edebilmektedir. 11 Eylül terör olaylarından sonra Başkan Bush tarafından yapılan yönlendirme ile özel istihbarat şirketleri, istihbarat servisleri ile yüksek kapasite halinde çalışmaya

başlamıştır. Bu sürecin hukuki dayanağı olarak, önleyici meşru müdafaa doktrini kabul edilmektedir. Özellikle dış politika üretim sürecinde özel istihbarat şirketleri ile beraberinde akademik yapıların, düşünce kuruluşlarının ve araştırmacıların etkisi ön plana çıkmış, özel sektörden gelen istihbari çalışmalarda etkisini artırmıştır. Bilindiği kadarı ile özel şirketlerin iki bin civarında olduğu ve sektörel olarak 260.000 civarında insan istihdam ettiği düşünülmektedir. Bu sistemin de beraberinde şeffaflık, denetim ve uygulama alanında avantaj ve dezavantajları mevcuttur (Darıcılı, 2023, s. 265).

Yukarıda verilen örnek olaylar ve olgular açık kaynak istihbaratı ve kamu güvenliği arasındaki bağlantının gün geçtikçe güçlendiğine işaret etmektedir. Büyük teknolojik dönüşümler ise mevcut yaşanan güçlenmeyi daha fazla öne çıkarmıştır. Sadece askeri ve güvenlik alanında değil vatandaşların günlük yaşamlarında da açık kaynakların önemi ve etkisi artmıştır. Kamu güvenliğinin sağlanması açısından açık kaynak istihbaratına devletlerin daha fazla önem vermesi geleceğin trendleri arasında yerini alabilir.

5.2. ABD Örneği Üzerinden Kamu Güvenliği

Amerikalılar birey ve devlet olarak mümkün olduğunca açık olmaya çalışırlar ve genellikle kültürel heterojen kökenlerine ve bireysel farklılıklarına rağmen her ne pahasına olursa olsun ambivalenzliğin ortaya çıkmasına engel olurlar (Bauer, 2022, s. 35).

Güvenlik anlayışında ABD'nin jeopolitiğinden kaynaklı olarak gelişen misyon itibari ile dünyanın barış, istikrar ve güvenliğini sağlama amacının temelini oluşturan 2017 Milli Güvenlik Stratejisi Belgesi, güçlü olma felsefesinden hareket eder ve bu durum güvenlik sonuçları olarak tezat durumlar oluşturabilir. Eski dönemlere göre birkaç kutup halinde gördüğümüz dünyanın yapay zekâ ve siber silahlanma yolu ile asimetrik düzende daha tehlikeli bir soğuk savaş dönemi yaşatacağı döneme girdiğini gözlemlemekteyiz (Biçer, 2020, s. 224).

ABD, uluslararası liberal düzende kamu güvenliğine en fazla önem veren devletlerden biridir. İnternet, sosyal medya ve diğer online girişimlerin kuruluş ve kontrol yeri olan ABD mevcut bilgilerinin dışarıya sızmaması için büyük

miktarda yatırım yapmakta ve kaynak ayırmaktadır. Siber güvenliğin sağlanması için Federal bütçeden milyarlarca dolar harcayan ABD ilerleyen dönemde yeni sanayileşmeyle birlikte bu alana daha fazla ilgi duyabilir. Açık kaynaklarda yer alan bilgi ve verilerin dış ülkelere karşı korunması ise kamu kaynaklarıyla pek mümkün değildir. Bireylerin kişisel bilgilerine kolaylıkla ulaşabilen bir küresel internet çağında açık kaynak istihbaratı büyük önem kazanmıştır. Silk Road örneği de kamu güvenliğine açık kaynakların nasıl yarar getirebileceğini göstermektedir. Operasyona kamu güvenliği açısından yaklaşıldığında kamunun yararına olduğunu söylemek mümkündür. Özellikle yasa dışı ürünlerin satışını sağlayan Silk Road kamu güvenliğine tehdit oluşturuyordu. Uyuşturucu madde satışı da yapılan sitede suç örgütlerine finansman sağlayabilecek altyapı mevcuttu. Kripto para üzerinden yapılan transferlerin takibi de mümkün olmadığından kamunun kontrolü dışında oluşmuş oluyordu. Yasadışı faaliyetler nedeniyle hukuki olarak herhangi bir kanunun da işleme alınması söz konusu değildi (Kushner, 2014).

Yeni uygulamaların çok kısa sürede milyonlarca kişiye ulaştığı günümüzde Silk Road olayı benzeri yapıların da farklı zaman zarfında kuvvetlenebileceğini göstermektedir. ABD'de kamu düzeninin korunması ve güvenliğin sürekli hale getirilmesi içinde açık kaynak istihbaratına daha fazla önem verilecektir. ABD Kongresinde Tiktok ve Huawei gibi firmaların sorguya çekilmesi ve bilgi güvenliği hakkında raporlar hazırlanması verilen önemin nasıl bir dereceye ulaştığını göstermektedir. CIA'de kurulan Dijital Yenilik Müdürlüğü yeni çağın bir göstergesi olarak okunabilir (Ackerman, 2016).

ABD DIA Müdürü General Vincent Stewart dijital devrime dikkat çekerek birçok yeni verinin açık kaynaklardan elde edilebileceğini vurgulamıştır. Yeni kaynaklardan yarar sağlamanın kamu tarafından farklı yöntemlerle geliştirilmesi gerektiğini de Stewart dile getirmiştir. Tıpkı Silk Road örneğinde olduğu gibi kamu güvenliği ve otoritesinin devamı için açık kaynaklardan yararlanma üst düzeyde kullanılmalıdır. Stewart'ın deyimiyle her saniyede 15'ten fazla kişi ilk kez sosyal medyayı kullanmaya başlayacaktır. Günde bir milyon insan interneti ilk kez deneyimliyor. ABD Savunma Bakanlığı ise açık kaynak istihbaratını temel yönetim mekanizması olarak belirlemiştir. Ardından Açık Kaynak

Konseyinin (AKK) bakanlık bünyesinde kurulduğunu açıklamıştır (Department of Defense, 2010).

Açık Kaynak Konseyi açık kaynaklarda yer alan bütün bilgileri kamu güvenliği ve bakanlığın çıkarları doğrultusunda analiz etmektedir. AKK, savunma bakanlığı istihbarat teşkilatının altında bir direktörlük olarak dizayn edilmiştir. Savunma Bakanına rapor sunabilen konsey istihbarat reformlarına öncülük yapmaktadır. Konseyin kuruluş amaçları arasında ulusal istihbarat çalışmalarında yeni trenlerin takibi yer almaktadır. Silk Road örneğinde hareketle konseyin faaliyetleri kamu kurumları arasındaki iş birliğini artırabilir. Silk Road operasyonu sonrası elde edilen tecrübe birikimi diğer kurumlarla paylaşılarak kamu güvenliğinde önemli bir gelişmeye neden olmuştur (Department of Defense, 2010).

ABD kamu kurumları açık kaynak istihbaratını kendi içlerine nasıl katacakları hakkında çalışmalara süratle devam etmektedir. Ancak açık kaynaklar teknolojinin gelişmesiyle daha farklı alanlarda etkisini ve gelişimini sürdürmektedir. Mevcut yaşanılan trendlerin takibinde ABD kurumlarının izlediği yol kurumsallaşma üzerine yoğunlaşmaktadır. CIA, FBI ve Savunma Bakanlığı kendi bünyelerinde kurdukları yeni birimlerle sürece uyum sağlamaya çalışmaktadır. Kamu güvenliğini sağlamakla görevli olan ABD kurumları açık kaynak istihbaratının önemini kavramışlardır. Bunun bir göstergesi olarak Silk Road ile bağlantılı olaylara 2020'de de açık kaynaklardan elde ettikleri bilgilerle operasyon gerçekleştirmişlerdir (Keskin, 2020, s. 203-206).

5.3. TAP Örneği Üzerinden Kamu Güvenliği

Kamu güvenliği devletler için teknolojinin gelişimiyle büyük değişim geçirmiştir. Bu değişimlerin başında bilgi ve verilere daha rahat ulaşım gelmektedir. Terör örgütleri de gelişen teknolojiden açık kaynaklar üzerinden rahatlıkla yararlanabilmektedir. TAP örneği ise kamu güvenliği açısından önemli analizler sunmaktadır. TAP'dan elde edilebilecek veri ve bilgiler kamu güvelik birimleri tarafından kolaylıkla ulaşılabilir. Maliyet açısından istihbarat faaliyetleriyle analiz edilmeye çalışılan terör örgütü profil, saldırı ve hedefleri TAP uygulaması aracılıyla erişilebilmektedir. Bir terör örgütünün son 50 yıllık

süreçte gerçekleştirdiği bütün saldırılarını tek bir kaynakta toplayan ve analiz eden bir platform olarak TAP kamu güvenliğine büyük katkı sunmaktadır.

Özellikle kamu kurumlarının envanter çalışmalarına büyük yarar sağlayan TAP uygulaması terör örgütlerinin profillerinin belirlenmesinde de aktif olarak yer almaktadır. Uzman isimlerin analiz, yorum ve raporlarıyla desteklenen veri ve bilgiler terör örgütlerini çalışan araştırmacılara da kolaylık sağlamaktadır. Kamu güvenliğinin bileşenleri olan farklı kurumların tek bir kaynaktan elde edebildiği terör örgütleri hakkındaki bilgiler ilerleyen dönemde farklı saldırıların önlenmesinden kullanılabilir. Devletin temel görevleri arasında yer alan vatandaşlarını koruma ve kamu düzenini sağlama düsturu TAP sağladığı açık kaynak bilgileriyle daha kolay gerçekleştirilebilmektedir. TAP'ın kamu yararına olan bir girişim olduğunu bu perspektiften hareketle söylemek mümkündür. Özellikle kamu kurumlarının üzerinden açık kaynak takip yükünü almakta ve 50 yıllık süreçte güncel data ve veri sunmaktadır (TAP, 2023).

Kamu güvenliğinin ifade ettiği anlam, önlem ve değer teknolojik gelişmelerin etkisiyle daha fazla öne çıkmıştır. Yapay zekâ uygulamaları, sosyal medya platformları, internet siteleri ve bulut teknolojisi kamu güvenliğinin boyutunu ve evrenini değiştirmiştir. Artık yapay zekâ ile kamu kurumlarının gizli kalması gereken verilerine ulaşmak daha kolay hale gelmiştir. Sosyal medya platformları üzerinden karar alıcıların ailelerine erişim hem daha kolay hem de daha tehlikeli bir hal almıştır. Eski FBI direktörünün ailesine ulaşan gazetecinin yaptığı açık kaynak istihbaratı buna örnek olarak verilebilir. Sosyal medya platformlarında paylaşılan kamu yararına olmayan bilgilerde kısa sürede milyonlarca kişiye ulaşabilmektedir. İnternet siteleri üzerinden kamu güvenliğini tehdit eden operasyonlar yapılabilmektedir. Bulut teknolojisi kullanılarak verilerin daha büyük haliyle depolanması ve ardından teknoloji hırsızlığa maruz kalması kamu güvenlik açıklıklarına neden olabilmektedir. Kamu güvenliğinin arz ettiği önem ve kamu kurumlarında analiz edilen bilgilerin gizliliği için Türkiye'de ek önlemler alınmaktadır. Bu önlemlerin daha güvenli hale gelmesinde tıpkı TAP örneğinde olduğu gibi sivil girişimler önem taşımaktadır.

21. yüzyılda devletler arasındaki anlaşmazlıklar diplomasi ve müzakereler yoluyla çözülebilmektedir. Eski dönemlerde devletlerin birbiriyle savaşmasına

neden olabilecek sınır problemleri ve tarihsel sorunlar diplomatik kanalların işletilmesiyle büyümeden ortadan kaldırılabilmektedir. Örneğin ABD-Çin arasında yaşanılan ticaret anlaşmazlıkları karşılıklı diplomasi yoluyla çözümlenmeye çalışılmıştır. Ancak terör örgütleriyle müzakere yürütmek ve diplomatik kanalları çalıştırmak çok zordur. Bu nedenle istihbarat teşkilatları her türlü duruma hazırlık amacıyla terör örgütlerini izlemektedir. İstihbarat teşkilatlarının terör örgütleriyle mücadele etmek amacıyla başvurduğu yöntemlerin teknolojiyle birlikte değişmesi açık kaynak istihbaratını öne çıkarmıştır. TAP örneğinden hareketle açık kaynaklardan elde edilen bilgiler kamu kurumları tarafından kamu güvenliği için kullanılabilir. Özellikle diğer kaynaklara göre daha az maliyetli olmasının yanı sıra açık kaynaklar kamu güvenliğini sağlamada her zaman ulaşılabilirdir. Bu haliyle TAP örneği açık kaynak istihbarat örneklerine kıyasla terör örgütleriyle mücadelede kamu kurumlarına büyük yarar sağlamaktadır (TAP, 2023).

6. SONUÇ

Açık kaynak istihbaratı, göç hareketlerinden, savaş unsurlarına, sağlıktan eğitime, turizmden finansa, birçok alanda hayatımızda yerini almıştır. Faaliyet alanı ise günden güne daha da genişlemektedir. Sadece suç odaklı bakış açısı olarak değil, asayişin de temini için hem iç hem dış güvenlik politikalarında da önemini günden güne artırmaktadır. İstihbaratın diğer alanlarına hizmet sağladığı gibi, diğer alanlarından da aldığı destekle devletin ve kamu birimlerinin işlerini maliyet ve risk açısından avantajlı olarak kullanmasını sağlamaktadır. Kamuda her birimin başta güvenlik ve itibar yapılanmasını açık kaynak istihbaratının çalışma koşullarını sağlayarak kurumsallaştırması ve aktif olarak kullanılması kaçınılmaz bir sonuç olarak yerini alacaktır. İncelediğimiz Silk Road operasyonu bireysel bir suç unsurunun takibi ve kamu güvenliği yararına sonuçlandırılması adına örnek teşkil etmektedir. Ele aldığımız bir veri toplama ve haritalandırma, istatistik ve analiz çıkarımı ve istihbarat raporları yayınlayan TAP projesi başta güvenlik birimleri olmak üzere, Dışişleri, Savunma, Kültür ve Turizm, Sağlık, Ticaret ve Ekonomi, Enerji vb. Bakanlıkların politika belirlemesinde yardımcı olabilecek unsurlar teşkil etmektedir.

Düşünce kuruluşlarının artması ve faaliyetlerini genişletmesi, TAP örneğinde olduğu gibi farklı bakış açıları ve spesifik alanlarda sundukları analiz ve raporlar açık kaynak çalışmalarına günden güne katkıda bulunacaktır. Devletin, akademisyenlerin ve bireylerin bakış açılarına yansıyacak olan bu çalışmalar stratejik olarak istihbarat çalışmalarını da ihtiyaçlar doğrultusunda genişletecektir.

Açık Kaynak İstihbaratı asayişin sağlamasında kişi ve grupların herhangi bir suç unsuru ile isimlerinin yan yana geldiğinde gerçekten suça bulaşma unsuru yok ise gerek teknolojik ve gerekse hukuki olarak birey ve toplumu koruyucu özelliği ile de kullanılmaktadır. Örnek olarak teknik açıdan kişinin kendisinin bir suç unsurunun gerçekleştiği zaman diliminde, söz konusu yerde

değil de sosyal medya hesabından konum bildirimi yaparak bulunmuş olduğu bir paylaşımla, güvenlik açısından cep telefonu HTS kayıtları gibi istihbari ve teknik destek ile teyit edildiğinde fonksiyonel olarak daha çabuk sonuca ulaşma durumu ortaya çıkmaktadır. Açık kaynak istihbaratı askeri, siber güvenlik, işletme yönetimi, hukuk, tıp gibi alanlarda stratejik karar alınırken sıklıkla kullanılan bir araştırma, analiz ve bilgi toplama yöntemi haline gelmiştir. Ancak her yönü ile bilgi toplama yönü ile çalışan istihbarat teşkilatları açısından daha hızlı, riski azaltan ve maliyetsiz yönü ile tercih edilen bir istihbarat türü haline gelmiştir. ABD, Çin, Rusya ve diğer devletler tarafından kullanılan açık kaynaklar devlet, toplum ve kamu kurumlarının içerisinde birimler halinde kurumsallaşarak bilgi toplamada en az analiz birimleri kadar stratejik bir konuma yerleşmiş bulunmaktadır. TAP ve Silk Road örnekleri bu açıdan önem taşımaktadır. Tezin incelediği örnekler olarak iki örnekte kamu güvenliğinin değişen yanlarını yansıtmaktadır.

Silk Road ve TAP örnekleri kamu güvenliğinin değişen yanlarını yansıtırken açık kaynak istihbaratının önem kazandığına işaret etmektedir. Bilinen istihbarat yöntemlerinden farklı olarak maliyet açısından daha avantajlı konumda bulunan açık kaynak istihbaratı dünyanın en büyük istihbarat örgütlerinin başkanları tarafından açıkça övülmektedir. MI6, FBI ve CIA gibi küresel güçlerinin istihbarat örgütleri günümüzde birçok bilgiyi açık kaynaklardan elde etmektedir.

FBI'nın Silk Road operasyonu ve açık kaynaklardan olabildiğince yararlanması buna örnek olarak gösterilebilir. Özellikle FBI direktörünün ailesine ulaşan gazeteci örneği de açık kaynakların istihbarat örgütleri içinde nasıl birer güvenlik açığına dönülebileceğini göstermektedir. TAP'dan hareketle aynı yorum ve analizlere varmak mümkündür. TAP ortaya koyduğu data, analiz ve yorumlarla istihbarat örgütlerinin ve diğer güvenlikle ilgili kamu kurumlarının işlerini kolaylaştırmaktadır. Tersi şekilde düşünüldüğünde ise terör örgütlerinin amaç ve hedeflerini çok açık bir şekilde ortaya koymaktadır. Hem araştırmacılar hem de kamu kurumları için maliyetleri düşüren TAP yeni nesil açık kaynaklar arasında önemli bir konuma sahiptir.

Silk Road yasa dışı ticaretle mücadelede açık kaynakların önemini gösterirken kamunun yeni nesil bireysel suçlarda, TAP örneği ise terör

örgütleriyle mücadelede açık kaynakların kritik yapısını öne çıkarmıştır. Teknolojik değişimin hızı ise mevcut açık kaynak istihbarat trendlerinin daha fazla görünür olmasını sağlamıştır. ABD'de FBI direktörünün maruz kaldığı açık kaynak istihbaratı, ordu generallerinin açık kaynaklardan ordulara yön vermesi ve konumunu belirlemesi, istihbarat teşkilatlarının yüzde 80'den fazla bilgileri açık kaynaklardan elde etmesi ve sosyal medya üzerinden yapılan açık kaynaklara kaynak oluşturabilecek paylaşımlar küresel bir trend halinde açık kaynak istihbaratına başvurulduğunu göstermektedir. Teknolojinin gelişmesi de küresel bir trend haline gelen açık kaynak istihbaratı için yeni kurum, birim ve direktörlüklerin kurulmasını sağlamıştır. Tezin incelediği konu, soru ve örneklere bu perspektifle bakıldığında Silk Road ve TAP örnekleri açık kaynak istihbarat trendinin yükseldiğine işaret etmektedir.

Tezin sonuçları arasında farklı devletlerin açık kaynaklardan daha fazla yararlandığı görülmüştür. Çin, Rusya ve ABD kendi aralarında yaptıkları iş birliği ve rekabette de açık kaynaklardan olabildiğince yararlanmaktadır. Rusya Ukrayna savaşında ABD'li askerleri sosyal medya hesaplarından izlerken, Çin kendi kurduğu ve teşvik ettiği sosyal medya platformları üzerinden bilgi toplamaktadır. Bu bilgi toplama hem Çinli şirketlere para kazandırmakta hem de Çin'in kamu kurumlar istihbarat faaliyetlerine maliyete katlanmadan sahip olabilmektedir. TAP örneğinde de mevcut maliyet yaklaşımının olduğunu söylemek mümkündür. Silk Road'da da benzer bir yaklaşımdan ziyade FBI'ın yeni bir trend olarak ortaya çıkardığı açık kaynak analizleri öne çıkmıştır. Açık kaynak istihbaratı bir bütün olarak ele alındığında istihbaratın algı, alan ve analiz yöntemlerini farklı şekillerde dönüştürmüştür.

Silk Road kamu güvenliği açısından önemli bir başlangıç olmuştur. Operasyon yasa dışı alışveriş ve kripto trafiğini engellerken kamunun otoritesinin sanal alana da yansıdığını göstermiştir. FBI tarafından gerçekleştirilen operasyon ilerleyen dönemlerde diğer operasyonlara kaynak oluşturmuştur. 2020'de de Silk Road'un elde ettiği kripto paralar için yeni bir operasyon gerçekleştirilmiştir. Diğer kamu kurumları ile iş birliği için kurulan AKK ise Amerikan devletinin açık kaynak istihbaratının önemini kavradığına işarettir. TAP örneği içinde benzer yorumlarda bulunmak mümkündür. Özellikle terör örgütleriyle mücadelede büyük önem arz eden açık kaynak istihbaratının

önemi İsrail'in ABD elçiliğine saldırıyı önlediği gibi artmıştır. Ayrıca açık kaynaklar dünyanın dijitalleştiği bir süreçte bireylerin kişisel yaşamlarının korunması gerekliliğini yükseltmiştir. Bu durum vatandaş ve karar alıcılar içinde geçerlidir. Sonuç itibariyle açık kaynak istihbaratı küresel bir realite haline gelerek devletlerin ve kamu güvenliğinin vazgeçilmez girdisi haline gelmiştir.

KAYNAKÇA

Ackerman R. K. (2016, July 1). *The CIA Accelerates Innovation*. SIGNAL. https://www.afcea.org/signal-media/cia-accelerates-innovation

Akarslan. (2020). *Siber Güvenlik ve Savunma: Biyometrik ve Kriptografik Uygulamalar*. NOBEL Akademik Yayıncılık.

ALLSAFE Siber Güvenlik. (n.d.). *Açık Kaynak İstihbarat Analizi Hizmeti*. Retrieved May 22, 2023, from https://www.allsafe.com.tr/hizmetlerimiz/acik-kaynak-istihbarat-analizi/

Alsmadi I. (2019). *Siber İstihbarat Analizi. NICE Siber Güvenlik Çerçevesi: Siber Güvenlik İstihbaratı ve Analitiği.*

Altun M. Ö. (2015). *TERÖRİZMİN Finansmanı İle Mücadelede Finansal İstihbaratın Rolü.* Dumlupınar Üniversitesi.

Andrew C. (2022a). *Gizli Dünya- Dünya İstihbarat Tarihi*. Kronik Yayınları.

Andrew C. (2022b). *Gizli Dünya: Dünya İstihbarat Tarihi*. Kronik Yayınları.

Arslan İ. (2023). *Açık Kaynak İstihbaratı(Osınt) Nedir?* What Is OSINT. https://lastguardsecurity.com/blog/acik-kaynak-istihbaratiosint-nedir/

Ateş H. (2012). *Kamu Güvenliğinde İstihbarat Sisteminin Değerlendirilmesi*. T. C. Atılım Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi Ve Siyaset Bilimi Anabilim Dalı.

Bağcı M. (2022). *Sinyal İstihbaratı ve Diğer Haber Toplama Yöntemleri ile Karşılaştırılması*. T.C. Polis Akademisi Güvenlik Bilimleri Enstitüsü Güvenlik Stratejileri Ve Yönetimi Anabilim Dalı.

Bal A., & Erkeç E. (2014). *İstihbarat Analizinde Karşılaşılan Sorunlar*. Kripto yayınları.

Balyemez O. (2022). *Silk Road'un kayıp Bitcoin gizemi çözüldü: 3,36 milyar dolarlık Bitcoin ele geçirildi*. SİBERBÜLTEN. https://siberbulten.com/dijital-guvenlik/silk-roadun-kayip-bitcoin-gizemi-cozuldu-336-milyar-dolarlik-bitcoin-ele-gecirildi/

Bauer T. (2022). *Dünyanın Tekdüzeleşmesi*. Albaraka Yayınları.

Benes L. (2013). OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. *Journal of Strategic Security, Vol. 6, No. 5*, 22–37.

Bernard, R., Bowsher, G., Milner, C., Boyle, P., Patel, P., & Sullivan, R. (2018). Intelligence and global health: assessing the role of open source and social media intelligence analysis in infectious disease outbreaks. *Journal of Public Health (Germany)*, *26*(5), 509–514. https://doi.org/10.1007/s10389-018-0899-3

Beyazıt A. (2019). Savunma strateji. *M5 Dergi*.

Bezci E. (2023). *Türk İstihbaratı ve Soğuk Savaş*. Kronik Yayınları. Sayfa 29

Biçer S. (2020). *Amerika Birleşik Devletleri. Jeopolitik Düşünce Büyük Güçler ve Türkiye*. Yeditepe yayınları.

Bozkurt İ. (2021). Dünyadaki Bazı İstihbarat Teşkilatlarının Tarihçesi. In Demircioğlu İsmail h., Özcan Ahmet, Çencen Namık, & Yiğit Yücel (Eds.), *Türk İstihbarat Tarihi*. Yeditepe Yayınları S.860-871

Bural E. B. (2022). *Sosyal Medya İstihbaratı*. Yeditepe Yayınları.

Çahmutoğlu E. (2021).İsrail'in Stratejik Siber Silahı: Pegasus Kriter Yıl.6 Sayı.60

Chul-Han B. (2022). *Psikopolitika Neoliberalizm ve Yeni İktidar Teknikleri* (Sökmen Semih, Ed.; Barışcan Haluk). Metis Yayınları.

CIA. (2023). *The World Factbook*. https://www.cia.gov/the-world-factbook/

Cirit İ. (2021). *Siber Ansiklopedi* (Akdemir Naci & Tuncer Can Ozan, Eds.). PEGEM AKADEMİ. S.539

Çıtak E. (2015). Çağımızın Gerekliliği Olarak Sinyal İstihbaratı. *Hitit Üniversitesi Sosyal Bilimler Enstitüsü Dergisi- Yıl 8, Sayı 2,* 751–770.

Clapper J. R. (2005). THIS IS A RUSH TRANSCRIPT AND MAY CONTAIN ERRORS. USERS ARE ADVISED TO CONSULT THEIR OWN TAPES OR NOTES OF THE SESSION IF ABSOLUTE VERIFICATION OF WORDING IS NEEDED. *A Project of the Center for Media & Security New York and Washington, D.C.*

Darıcılı A. B. (2023). İstihbarat 101.Dora Yayınevi

Delibalta Y. (2019). *Selçuklularda İstihbarat*. Yeditepe Yayınları.

Demir K. C. (2021). İstihbarat: Kavram, Süreç ve Temel Prensipler. In Demircioğlu İsmail H., Özcan Ahmet, Çencen Namık, & Yiğit Yücel (Eds.), *Türk İstihbarat Tarihi* (pp. 13–39). Yeditepe Yayınları S.866-871

Department of Defense INSTRUCTION. (2010, August 24). *Open Source Intelligence (OSINT)*. Incorporating Change 2, Effective July 16, 2020. https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/311512p.pdf

Dönmez, S. (2017). Security in cyber age: An introduction to difficulties in security issues in digitalized world. In *Research on Humanities and Social Sciences: Communication, Social Sciences, Arts*. https://doi.org/10.3726/978-3-631-69829-7

Duramaz S, & Gökbunar A. R. (2017). Ekonomik İstihbarat Sisteminin Oluşturulmasına Yönelik Türkiye için Yeni Bir Model Önerisi. *Marmara Üniversitesi Öneri Dergisi • Cilt 12, Sayı 47*, 53.

Durdallı L. (2023). *OSINT – Açık Kaynak İstihbarata Giriş- 1*. Turkcell. https://gelecegiyazanlar.turkcell.com.tr/blog/osint-acik-kaynak-istihbarata-giris-1

Efe İ. (2023). Terörizmin Dönüşümü: Sosyal Medyanın İç Terör Tehditleri Üzerindeki Olası Etkileri. Seta Kitapları S.317-330

Ekşim A., & Civelek İ. (2019). Açık Kaynak İstihbaratı Tabanlı Yarı Otomatik Siber Güvenlik Modeli. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi, Cilt: 7, Sayı: 1*, 827–836.

Eom J. H. (2014). Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace. *International Journal of Software Engineering and Applications, Cilt: 8, Sayı: 9*, 137–146.

Erdem A. (2015). *MİT- Gizli Tarih.* Kriminal Kitaplar.

Eroğlu H. (2003). Klasik Dönemde Osmanlı Devleti'nin İstihbarat Stratejileri. *Dergipark.*

Erol K. M. (2022a). *Açık Kaynak İstihbaratı*. Nobel Bilimsel Eserler.

Erol K. M. (2022b). Açık Kaynak İstihbaratı ve Askeri İstihbarat Cilt: 1, Sayı: 1. *İstihbarat Çalışmaları ve Araştırmaları Dergisi,* 23–59.

Erol M., & İstikbal D. (2020). *ALTERNATIF SOSYAL MEDYA ARAYIŞLARI ÇIN, RUSYA VE JAPONYA*. SETA.

Ertekin F. (2022). İngiliz İstihbaratı ve Osmanlı İmparatorluğu. Yeditepe Yayınları

Ertem A. V. (2022). *Türk İstihbarat Tarihi* Uluslararası Beşerî Bilimler ve Eğitim Dergisi, Clt:8, Sayı:17, 2022, s.320-330

FBI. (2023). *A Brief History*. https://www.fbi.gov/history/brief-history

Federation of American Scientists. (2019). *Operation Security, Intelligence Threat Handbook. Intelligence Collection Actıvıtıes and Dısciplınes*. Federation of American Scientists.

Federation of Amerikan Scientists. (2000). *Measurement and Signature Intelligence (MASINT)*. Intelligence Resource Program. https://irp.fas.org/program/masint.htm

Feinberg A. (2017). *This is Almost Cetainly James Comey's Twitter Account*. Gizmodo. https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641

Gök A. (2021). *Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım* (Akdemir Naci & Tuncer Can Ozan, Eds.). PEGEM AKADEMİ.

Goodman M. (2017). *Geleceğin Suçları, Dijital Dünyanın Karanlık Yüzü*. Timaş Yayınları.

Gül Z. (2015). *İstihbarat Çeşitleri ve Stratejik İstihbarat. Güvenlik Sektöründe Temel Stratejiler*. Nobel Akademik Yayıncılık.

Hannas W. C., Mulvenon J., & Buglisi A. B. (2013). *Chinese Industrial Espipnage: Technology Acquisition and Military Modernization*. Routledge Press.

Hasanov İ., & Katman F. (2019). Soğuk Savaş Döneminde ABD ve SSCB'nin Politik İstihbarat Yöntemlerinin Karşılaştırması. *Akademik Tarih ve Düşünce Dergisi Cilt:6 Sayı:2*, 1138–1150.

Howard A. (2011, August 9). *How Governments Deal With Social Media*. https://www.theatlantic.com/technology/archive/2011/08/how-governments-deal-with-social-media/243288/

Hudoğlu M. (2023). Stratejik İstihbarat Analizini Anlamak: Bilimsel Araştırma ile Benzerlikleri ve Farkları. *İstihbarat Çalışmaları ve Araştırmaları Dergisi (DergiPark)*.

Hume T. (2013). *How FBI caught Ross Ulbricht, alleged creator of criminal Marketplace Silk Road*. https://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html

Javier P. G., Pantaleone N., Felix G. M., & Gregorio M. P. (2020). The not yet exploited goldmine of OSINT: Opportunities, open challenges and future trends. *IEEE Access*. https://www.mendeley.com/catalogue/823345d3-24d8-3fd8-b6af-0c662481d26b/

Karabulut B. (2011). *Güvenlik: Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek*. Barış Kitap .

KARASOY, H. A. (2022). YENİ NESİL SAVAŞ VE SİBER İSTİHBARAT. *Güvenlik Bilimleri Dergisi*. https://doi.org/10.28956/gbd.1015517

Kasapoğlu C. (2021). *Açık-Kaynaklı İstihbaratın Yükselişi*. Anadolu Ajansı. https://www.aa.com.tr/tr/analiz/acik-kaynakli-istihbaratin-yukselisi/2138345

Kavsıracı O., & Demirbaş M. (2020). İstihbarat Faaliyetlerinin Devlet Güvenliği Açısından İncelenmesi. *Anadolu Strateji Dergisi, 2 (1),* 49–64.

Keith C. C. (2019). *International Encyclopedia of Human Geography*. Second Edition.

Keleştemur A. (2019). *Siber İstihbarat Tanımı ve Faaliyet Alanı*. https://www.academia.edu/30032177/Siber_%C4%B0stihbarat_Tan%C4%B1m%C4%B1_ve_Faaliyet_Alan%C4%B1

Keskin M. (2020). *GÜVENLİK YÖNETİMİ VE AÇIK KAYNAK İSTİHBARATININ ÖNEMİ*. Sivas Cumhuriyet Üniversitesi.

Koca H. İ. (2019). Stratejik İstihbarat. *Akademik Tarih ve Düşünce Dergisi Cilt:6 Sayı:4*, 2187–2198.

Korkmaz S. C. (2018, January 22). *Terörle Mücadelede Taktik İstihbarat*. Ortadoğu Araştırmaları Merkezi (ORSAM). https://orsam.org.tr/tr/terorle-mucadelede-taktik-istihbarat/

Kushner D. (2014). *Dead End on Silk Road: Internet Crime Kingpin Ross Ulbricht's Big Fall*. RollingStone. https://www.rollingstone.com/culture/culture-news/dead-end-on-silk-road-internet-crime-kingpin-ross-ulbrichts-big-fall-122158/

LifeRaft. (2023). *Corporate Security Tool for Organizations*. LifeRaft. https://www.liferaftinc.com/blog/socmint-an-essential-corporate-security-tool-for-organizations

Limaye Y. (2023). *Afganistan'da Taliban'ın uyuşturucuyla savaşı: Afyon ekimi büyük ölçüde azaldı*. BBC.

https://www.bbc.com/turkce/articles/cv219q536y3o?at_medium=social&at_format=link&at_bbc_team=editorial&at_link_id=A7D76400-0469-11EE-89B5-ECC5AD7C7D13&at_campaign=Social_Flow&at_link_type=web_link&at_ptr_name=twitter&at_link_origin=bbcturkce&at_campaign_type=owned

Macaskill E. (2023). 'No regrets,' says Edward Snowden, after 10 years in exile. The Guardian. https://www.theguardian.com/us-news/2023/jun/08/no-regrets-says-edward-snowden-after-10-years-in-exile

Maltego Takımı. (2022). *Everything About Social Media Intelligence (SOCMINT) and Investigations*. https://www.maltego.com/blog/everything-about-social-media-intelligence-socmint-and-investigations/

Mete M. (2021). Sosyal Medyada Enformasyon Savaşı: Kurumsal Güvenlik Bağlamında Bireysel Sosyal Medya Kullanımı. *Sosyal Bilimler Çalışmaları Dergisi (Social Sciences Studies Journal). Sayı 86,Cilt 7*, 331.

MİT. (2023a). *İstihbarat Çarkı*. https://www.mit.gov.tr/t-cark.html#

MİT. (2023b). *İstihbarat Oluşumu*. https://mit.gov.tr/isth-olusum.html

MİT. (2023c). *İstihbaratın Tanımı ve İstihbarat Çarkı*. https://mit.gov.tr/tarihce/giris.html

Miman A. T. (2007). *Küreselleşmenin Ordusu Ekonomik İstihbarat* . IQ Kültür Sanat Yayıncılık.

Ökten T. (2023). 21.nci Yüzyılda Açık Kaynak İstihbaratı. *İstihbarat Çalışmaları ve Araştırmaları Dergisi Cilt: 2, Sayı: 1*, 17–38.

Olcott A. (2012). *Open Source Intelligence in a Networked World*. London Press.

Özdağ Ü. (2020a). *İstihbarat Teorisi*. Kripto Yayınları.

Özdağ Ü. (2020b). *İstihbarat Teorisi*. Kripto Yayınları.

Özdal B, & Tiryaki E. (2020). Açık Kaynak İstihbaratında Sosyal Medya Rolünün Analizi. *DergiPark*.

Öztürk U. B. (2020). *Siber İstihbarat Faaliyetlerinde İnsan İstihbarat Yaklaşımı ve Teknikleri* [T.C. MARMARA ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ ULUSLARARASI İLİŞKİLER ANABİLİM DALI İSTİHBARAT BİLİM DALI]. https://acikbilim.yok.gov.tr/handle/20.500.12812/306951

Progonati E. (2022). *Kültürel İstihbarat: Terörizmle Mücadelede Kalpleri ve Zihinleri Kazanmak Sanatı. İstihbarat Araştırmaları*. Necmettin Erbakan Üniversitesi Yayınları.

Sarı G. (2021). Geçmişten Bugüne İstihbarat Çalışmaları. In Demircioğlu İsmail H., Özcan Ahmet, Çencen Namık, & Yiğit Yücel (Eds.), *Türk İstihbarat Tarihi*. Yeditepe Yayınları S.802-807

Savaş S., & Topaloğlu N. (2015). Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri. *VIII. ULUSLARARASI BİLGİ GÜVENLİĞİ VE KRİPTOLOJİ KONFERANSI*, 62–69.

Schechter A. (2015). Who Needs the KGB when we have Facebook? An Interview with Eben Moglen. *Columbia University*. http://moglen.law.columbia.edu/publications/Who-needs-KGB-when-we-have-Facebook-Schechter.pdf

Seren M. (2017a). *Stratejik İstihbarat ve Ulusal Güvenlik*. Orion Kitapevi.

Seren M. (2017b). *Stratejik İstihbarat ve Ulusal Güvenlik.* Orion Kitapevi.

Seren M. (2017c). *Stratejik İstihbarat ve Ulusal Güvenlik*. Orion Kitapevi.

Shepherd A., Kalis S., & Storm R. (2017). *Unmanned Aerial Systems: A Maturing GEOINT Tool*. United States Geospatial Intelligence Foundation. https://medium.com/the-state-and-future-of-geoint-2017-report/unmanned-aerial-systems-a-maturing-geoint-tool-35cba1494c1a

Socmint. (2023). *İstihbarat nedir? türleri nelerdir veri toplama yöntemleri nelerdir*. Türkhackteam.

Suiçmez M. N. (2018). *Gerçek İstihbarat Operasyonları İle "Açık Kaynak İstihbaratı."* Stratejik Ortak-Dergi. https://stratejikortak.com/2018/03/gercek-istihbarat-operasyonlari-ile-acik-kaynak-istihbarati.html

Taban M. H., & Aydilek E. (2023). 'Dijital Çağda İstihbarat Analizi'. *İstihbarat Çalışmaları ve Araştırmaları Dergisi Cilt:2, Sayı:1,2023 ss:39-67*

Taban M. H., & Aydilek E. (2023). 'Dijital Çağda İstihbarat Analizi'. *İstihbarat Çalışmaları ve Araştırmaları Dergisi Cilt:2, Sayı:1,2023 ss:39-67*

TAP. (2023). *What we do?* Terör Analiz Platformu. https://www.tap-data.com/category/about-tap

Tekek M. (2016). Açık Kaynak İstihbaratı ve Düşünce Kuruluşları. *Hidropolitik Akademi*. https://www.hidropolitikakademi.org/tr/article/11752/acik-kaynak-istihbarati-open-source-intelligence-ve-dusunce-kuruluslari

The Times Of Israel. (2023). *İsrail, IDF'ye katılan ve Mısır için casusluk yapan Nazi hakkındaki dosyanın gizliliğini kaldırdı*. https://www.timesofisrael.com/

Through As Amended. (2016). *Department of Defense Dictionary of Military and Associated Terms*. https://irp.fas.org/doddir/dod/jp1_02.pdf

Tokmakoğlu G. (2022). Askeri İstihbaratın Dönüşümü ve Türkiye. *Kriter Ocak 2022 / Yıl 6, Sayı 64*.

Tylutki K. (2018). The information of a mass destruction range – OSINT in intelligence activities. *Internal Security Review 19/18*.

Tzu S. (2022). *Savaş Sanatı* (Ali Alkan İNAL, Ed.). Türkiye İş Bankası Yayınları.

Ünan U. (2017). *ARŞİV BELGELERİNE GÖRE OSMANLI'DA ISTIHBARAT* (148th ed.). Seçil Ofset.

Ünlü F. (2022). *MİT Efsanesi- İstihbaratın Gayriresmi Tarihi*. Sahi Kitap.s.137

USA. (2023). Current Legislative Activities. *Current Legislative Activities*. https://www.congress.gov/

Weinbaum, C., Berner, S., & McClintock, B. (2017). SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain. In *SIGINT for Anyone: The Growing Availability of Signals Intelligence in the Public Domain*. https://doi.org/10.7249/pe273

Yılmazer İ. (2020). *İstihbarat Nedir, Ne Değildir?*

ÖZGEÇMİŞ

Doğan ÇELİK ilk ve orta öğreniminin ardından liseyi Sarıyer İmam Hatip Lisesi'nde, lisans eğitimini Anadolu Üniversitesi Kamu Yönetimi alanında tamamlamıştır. Halen Topkapı Üniversitesi Güvenlik Bilimleri ve Uygulamaları Ana Bilim Dalı, Güvenlik Bilimleri ve Uygulamaları Bilim Dalı'nda yüksek lisans eğitimine devam etmektedir. Uzun yıllar yayıncılık alanında faaliyet gösteren Çelik, halen SETA Vakfı bünyesinde kamu yayıncılığı faaliyetlerine devam etmektedir. Ayrıca istihbarat, güvenlik ve terör alanlarında çalışma ve araştırmalarını sürdürmektedir.