

T.C.
ATILIM ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
ULUSLARARASI İLİŞKİLER YÜKSEK LİSANS PROGRAMI

**TARİHSEL DEĞİŞİM SÜRECİ İÇİNDE İSTİHBARATIN ULUSLARARASI
İLİŞKİLERDE ARTAN ROLÜ**

Yüksek Lisans Tezi

Gözde DİKİCİ

Ankara-2023

T.C.
ATILIM ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI
ULUSLARARASI İLİŞKİLER YÜKSEK LİSANS PROGRAMI

TARİHSEL DEĞİŞİM SÜRECİ İÇİNDE İSTİHBARATIN
ULUSLARARASI İLİŞKİLERDE ARTAN ROLÜ

Yüksek Lisans Tezi

Gözde DİKİCİ

Tez Danışmanı

Doç. Dr. Gözde YILMAZ

Ankara-2023

KABUL VE ONAY

Gözde DİKİCİ tarafından hazırlanan “Tarihsel Değişim Süreci İçinde İstihbaratın Uluslararası İlişkilerde Artan Rolü ” başlıklı bu çalışma, 03 /04 /2023 tarihinde yapılan savunma sınavı sonucunda başarılı bulunarak jürimiz tarafından Uluslararası İlişkiler Ana Bilim Dalı, Uluslararası İlişkiler Programında Yüksek Lisans Tezi olarak oy birliği ile kabul edilmiştir.

Doç. Dr. Nilgün ELİKÜÇÜK YILDIRIM (Başkan)

Doç. Dr. Gözde Yılmaz (Danışman)

Dr. Öğretim Üyesi Mesut ASLAN (Üye)

Doç. Dr. Şule TUZLUKAYA

Enstitü Müdürü

ETİK BEYAN

Atılım Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Kılavuzuna uygun olarak hazırladığım bu tez çalışmasını;

- Akademik ve etik kurallar çerçevesinde hazırladığımı,
- Tüm bilgi, belge, değerlendirme ve sonuçları bilimsel etik ve ahlak kurallarına uygun olarak sunduğumu,
- Tez çalışmasında yararlandığım eserlerin tümüne atıfta bulunarak kaynak gösterdiğimi,
- Bu tezde sunduğum çalışmanın özgün olduğunu bildirir,

Aksi bir durumda aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim.

03/04/2023

Gözde DİKİCİ

ÖZ

DİKİCİ, Gözde, Tarihsel Değişim Sürecinde İstihbaratın Uluslararası İlişkilerde Artan Rolü, Yüksek Lisans Tezi, Ankara, 2023.

İstihbarat, tarihsel olarak insanoğlunun başlangıcından beri süregelenmiş olup, bu süreç içerisinde çeşitli alanlara yayılarak gerek ülkelerin iç işlerinde gerekse dış işlerinde oldukça etkili olmuştur. İstihbarat sadece bilgi toplamak olarak özetlenemeyecek olup, özellikle I. Dünya Savaşından sonra kurumsallaşarak analiz ve yorumlanma aşamaları da bu süreç içerisinde ciddi roller oynamaya başlamıştır. İstihbarat sadece askeri alanlarda değil sivil alanlarda da kullanılmaya başlanmış, aynı zamanda istihbarat kaynakları da çok çeşitlendiğinden yaşamın her alanında önemini arttırarak devam ettirmektedir. Özellikle gelişen teknoloji ile beraber değişen istihbarat alanları uluslararası alanda ilişkilerin farklı boyutlarda değişip düzenlenmesine neden olabilmekte ve dış politikaların yönünün belirlenmesinde rol oynamaktadır. Dünyada yaşanan olaylar nedeni ile özellikle 11 Eylül saldırılarından sonra istihbarat anlayışı ve yapılanması oldukça değişmiş, ülkeler II. Dünya Savaşından sonra kurulan liberal düzeni sorgularken birbirleri hakkında bilgi toplayabilmek oldukça önemli hale gelmiştir. Aynı zamanda sürdürülebilir devlet anlayışında milletlerin kendilerini koruyabilmeleri ve dış politikalarını şekillendirebilmeleri için de istihbarat ve istihbarat örgütlerinin önemi gün geçtikçe artmaktadır. Kurumsallaşan istihbarat teşkilatları, dönem dönem farklı teknikler ve örgütlenme yöntemleri kullanarak, devletin temel amacı olan devamlılığı sağlayabilmek için kullanabilecekleri bilgileri toplamaya çalışmakta ve kendileri hakkında bilgi toplanmasını engellemek amacıyla (karşı istihbarat) çeşitli çalışmaları da devam ettirmektedir. Bu çalışmanın amacı, İstihbaratın tarihin en eski zamanlarından beri insanoğlunun hayatında ne kadar önemli bir yere sahip olduğu konusunda bilgiler vermek ve Dünyada ve Türkiye’de geçirdiği tarihi sürece de değinerek, değişen günümüz koşullarına adaptasyonu ile birlikte uluslararası ilişkilerde artan rolüne değinmek olacaktır.

Anahtar Sözcükler: İstihbarat, İstihbarat Tarihi, Uluslararası İlişkiler, Başarısız İstihbarat, Dış politika.

ABSTRACT

DİKİCİ, Gözde, The Increasing Role of Intelligence in International Relations in The Process of Historical Change, Master's Thesis, Ankara, 2023

Intelligence has been going on historically since the beginning of mankind and has spread to various fields during this process and has been very effective both in the internal affairs of countries and in their external affairs. Intelligence cannot be summarized as just gathering information, especially after the World War I, the stages of analysis and interpretation became institutionalized and began to play serious roles in this process. Intelligence has started to be used not only in military fields but also in civilian fields, and since intelligence sources are very diverse, it continues to increase its importance in all areas of life. Especially with the developing technology, changing intelligence fields can cause international relations to change and regulate in different dimensions and play a role in determining the direction of foreign policies. Due to the events taking place in the world, especially after the September 11 attacks, the understanding and structuring of intelligence have changed quite a lot. While questioning the liberal order established after the World War II, it has become quite important to be able to collect information about each other for all countries. At the same time, the importance of intelligence and intelligence organizations is increasing day by day in order for nations to protect themselves and shape their foreign policies in a sustainable understanding of the state. Institutionalized intelligence agencies try to collect information that they can use to ensure continuity, which is the main goal of the state, using different techniques and organizational methods from time to time, and also carry out various studies in order to prevent the collection of information about themselves (counterintelligence). The purpose of this study in the history of mankind since the most ancient times in the life of intelligence have held an important place in the historical process and to give information about the world and in Turkey, referring to adapt to changing conditions will touch on the increasing role in today's international relations.

Key Words: Intelligence, Intelligence History, International Relations, Intelligence Failures, Foreign policy.

TEŞEKKÜR

Bu çalışmanın her aşamasında bana desteğini esirgemeyen, hızlı geri dönüşleri ve tecrübesi ile benim için çok önemli bir rehber olan değerli danışmanım Doç Dr. Gözde Yılmaz'a,

Gerek tez aşamasında, gerek ders aşamasında emeği geçen tüm hocalarıma ve değerli mesai arkadaşlarıma,

Her zaman bana güvenip bana destek olan annem Meral Dikici ve ablam İlke Dikici'ye,

Beni her zaman destekleyen değerli dostlarıma,

“Eğitimidir ki, bir milleti ya özgür, bağımsız, şanlı, yüksek bir topluluk halinde yaşatır; ya da esaret ve sefaletle terk eder” diyerek eğitimin önemini her zaman vurgulayan ve her alanda yolumuza ışık tutan, tanıdığı hak ve özgürlüklerle bu günlere ve eğitim olanaklarına ulaşabilmemizi sağlayan Gazi Mustafa Kemal Atatürk ve silah arkadaşlarına sonsuz minnet ve saygılarımı sunuyorum.

İÇİNDEKİLER

ÖZ.....	i
ABSTRACT.....	ii
TEŞEKKÜR	iii
TABLolar DİZİNİ	vii
ŞEKİLLER DİZİNİ	viii
SİMGELER VE KISALTMALAR DİZİNİ	ix
GİRİŞ	1
BÖLÜM 1: İSTİHBARAT İLE İLGİLİ KAVRAMLAR	6
1.1. İstihbarat Kavramı.....	6
1.2. İstihbarat Çarkı.....	7
1.3. İstihbaratın Çeşitleri	10
1.3.1. Açık kaynak istihbaratı (AKİST).....	11
1.3.2. Siyasi istihbarat	13
1.3.3. Askeri istihbarat	13
1.3.4. Sosyal istihbarat	14
1.3.5. Stratejik ve taktik istihbarat	14
1.3.6. Ekonomik istihbarat	16
1.3.7. Teknolojik istihbarat ve elektronik istihbarat	16
1.3.8. Coğrafya istihbaratı.....	17
1.3.9. Siber istihbarat (SİBİST).....	18
1.3.10. İnsan istihbaratı (İNİST)	19
1.4. İstihbarat İlkeleri	21
1.5. İstihbarata Karşı Koyma (İKK)	22
BÖLÜM 2: DÖNEMSEL OLARAK İSTİHBARATIN GELİŞİMİ VE	
İSTİHBARAT TARİHİ.....	25
2.1. İstihbarat Tarihi.....	25

2.1.2. Dönemsel olarak değişen istihbarat toplama yöntemleri ve önemli olaylar	28
2.1.2.1 1914-1938 yılları arası istihbarat gelişmeleri.....	28
2.1.2.2. 1939- 1946 yılları arası istihbarat gelişmeleri.....	30
2.1.2.3 1947 yılı ve sonrası istihbarat gelişmeleri.....	32
2.2. Türk İstihbarat Tarihi	38
2.2.1 Türklerde İslamiyet öncesi ve sonrası istihbarat anlayışı	39
2.2.2. Osmanlı Devleti ve sonrası istihbarat faaliyetleri.....	40
2.2.3. Türkiye Cumhuriyeti Devleti ve istihbarat faaliyetleri.....	44
2.3. Dünyadaki İstihbarat Örgütleri.....	47
2.3.1. İngiliz istihbarat örgütleri	47
2.3.2. İsviçre istihbarat örgütleri.....	49
2.3.3. Çin devleti istihbarat örgütleri	50
2.3.4. Amerikan istihbarat örgütleri.....	51
2.3.5. Rus istihbarat örgütleri.....	53
2.3.6. Fransız istihbarat örgütleri.....	54
2.3.7. Alman istihbarat örgütleri.....	55
2.4. Geleneksel İstihbarattan Modern İstihbarata Geçiş Süreci.....	56
BÖLÜM 3: İSTİHBARAT VE ULUSLARARASI İLİŞKİLER.....	58
3.1. İstihbaratın Dış politika Yapımı ve Uluslararası İlişkilere Etkisi	58
3.2. İstihbarat Başarısızlığı ve Uluslararası İlişkiler	63
3.2.1 Başarısız istihbarat tanımı ve nedenleri	63
3.2.1. Dünyadaki başarısız istihbaratlara örnekler	66
3.2.2.1 Pearl Harbour savaşı	66
3.2.2.2. Vietnam savaşı	69
3.2.2.3. 11 Eylül saldırıları.....	71
3.2.2.4. Irak savaşı.....	74
3.3. İstihbaratın Güncel Yönelimleri ve Uluslararası İlişkiler	77
3.3.1. Siber güvenlik ve siber terörizm	77
3.3.2. Medikal istihbarat.....	86
SONUÇ.....	91

TURNİTİN RAPORU	129
ÖZGEÇMİŞ	141



TABLÖLAR DİZİNİ

Tablo 1: 11 Eylül Öncesi El-Kaide'nin ABD'ye Karşı Terör Saldırıları 72

Tablo 2- Medikal İstihbarat Kapsamı..... 88



ŞEKİLLER DİZİNİ

Şekil 1: İstihbarat Çarkı.....	8
Şekil 2: Beşgen İstihbarat Çarkı.....	9
Şekil 3: Sekiz Aşamalı İstihbarat Çarkı.....	10
Şekil 4: CAS'ın Askeri Karar Vermede Kullanımı.....	18
Şekil 5: İnsan İstihbaratında Kaynakların Duyarlılık Sıralaması	20
Şekil 6: Özgürlük ve Güvenlik Arasındaki Sağlıksız Denge	26
Şekil 7: Hibrit Savaş	37
Şekil 8: Başarısız İstihbaratın Kaynağı	64

SİMGELER VE KISALTMALAR DİZİNİ

ABD	: Amerika Birleşik Devletleri
AGİT	: Türkiye ve Avrupa Güvenlik ve İşbirliği Teşkilatı
AISE	: Agenzia Informazioni e Sicurezza Esterna, İtalya İstihbarat ve Dış Güvenlik Kurumu
AKİST	: Açık Kaynak İstihbaratı
BIN	: Badan Intelijen Negara, Endonezya Devlet İstihbarat Teşkilatı
BND	: Bundesnachrichtendienst, Almanya Federal Haber : Alman Servisi
CAS	: Coğrafi Analiz Sistemi
CBS	: Coğrafi Bilgi Sistemi
CIA	: Central Intelligence Agency, Merkezi İstihbarat Örgütü
CISEN	: Center for Investigation and National Security , Meksika Soruşturma ve Ulusal Güvenlik Merkezi
COMINT	: Muhabere İstihbaratı
CSIS	: Canadian Security Intelligence Service, Kanada Güvenlik İstihbarat Servisi
DGSE	: Direction générale de la Sécurité extérieure, Fransız Dış İstihbarat Kurumu
DNRED	: Direction Nationale du Renseignement et des Enquêtes Douanières, Fransa Ulusal İstihbarat ve Gümrük Soruşturmaları Müdürlüğü
DRM	: Direction du renseignement militaire, Fransız Askeri İstihbarat Müdürlüğü
EI	: Ekonomik İstihbarat
ELINT	: Elektronik İstihbarat

FBI	: Federal Bureau of Investigation
FIS	: Federal Intelligence Service
FSB	: Federalnaya slujba bezopasnosti, Rus Federal Güvenlik Servisi
GCHQ	: Government Communications Headquarters
GIP	: General Intelligence Presidency, Suusdi Arabistan Genel İstihbarat Başkanlığı
GÖRİST	: Görüntü İstihbaratı
GRU	: Glavnoye Razvedyvatel'noye Upravleniye, Rus Askeri İstihbarat Direktörlüğü
İKK	: İstihbarata Karşı Koyma
İNİST	: İnsan İstihbaratı
MI5	: Military Intelligence Section 5
MI6	: Military Intelligence Section 6
MND	: Militärischer Nachrichtendienst, İsviçre Askeri istihbaratı
MİT	: Millî İstihbarat Teşkilatı
MOIS	: Ministry of Intelligence and Security, İran İstihbarat ve Güvenlik Bakanlığı
MSS	: Ministry of State Security, Çin Devlet Güvenliği Bakanlığı
MPS	: Ministiry of Public Security, Çin Kamu Güvenliği Bakanlığı
NIS	: National Intelligence Service, Güney Kore Ulusal İstihbarat Hizmeti
PSIA	: Public Security Intelligence Agency, Japon Kamu Güvenliği İstihbarat Ajansı
SIS	: Signal Intelligence Service, Sinyal İstihbarat Servisi

SİBİST	: Siber İstihbarat
SİNİST	: Sinyal İstihbaratı
SVR	: Sluzbə vnješnij rezvjetki, Rus İstihbarat Servisi
T.C.	: Türkiye Cumhuriyeti
TEKİST	: Teknolojik İstihbarat
TRACFIN	: Intelligence Processing and Action Against Illegal Financial Circuits, Fransız İstihbarat İşleme ve Yasadışı Mali Devrelere Karşı Eylem Merkezi
UKUSA	: United States of America Agreement, ABD Anlaşması
Vb.	: Ve Benzeri
Vd.	: Ve Diğerleri
YY	: Yüzyıl

GİRİŞ

İstihbarat, tarihi çok eskilere dayanan, dünyada artık sadece askeri anlamda kullanılmayan sivil alanlarda da oldukça önem kazanan çıkan bir alandır. İstihbarat, bilginin elde edilerek karşılaştırılması, değerlendirilip analiz edilerek birleştirilmesi ve yorumlanması sürecinin sonunda ortaya çıkan üründür (Kavsıracı & Demirbaş, 2020). Bilgi ve istihbarat kavramlarını birbirleriyle karıştırmamak gerekir. Her bilgi istihbarat olamazken, her istihbarat bir bilgi kaynağıdır. Bir bilginin istihbarat olabilmesi için bir süreçten geçerek kullanılabilir hale gelmesi gerekir. Bilgiler toplandıktan sonra yorumlanır, daha sonra değerlendirilir ve en sonunda bir sonuca varılır (Kavsıracı, 2020). Sonuçta elde edilen bilgiler kullanılabilirse buna istihbarat anlamında bir değer yüklenebilir.

17. yüzyılda ortaya çıkmış olan uluslararası ilişkiler disiplini, I. Dünya Savaşından sonra akademik anlamda ilgi çekmiş ve üniversitelerde kürsüler kurulmaya başlamıştır (Ozan, 2014). İlk cevap aradığı sorular ise devletlerarasındaki savaşların nasıl ve neden çıktığı ile nasıl önlenebileceğidir (Gözen, 2021, s. 2). I. Dünya Savaşından sonra akademik olarak düşünülmesinin temel sebeplerinden biri de bu sorduğu sorulara aradığı cevaplardır denilebilir. Bir başka savaşın çıkmasını bir önceki savaşın nedenlerini anlayarak engellemeye çalışan uluslararası ilişkiler disiplininin asıl ortaya çıkışı 1648’de imzalanan Vestfalya anlaşması olmasına rağmen, asıl büyük gelişim atılımını II. Dünya Savaşıyla yapmıştır (Özlük, 2009). Uluslararası ilişkiler disiplinini sadece ulus-devlet mantığında incelemek yanlıştır, çünkü günümüzün küreselleşen dünyasında bu ilişkileri etkileyen sivil toplum kuruluşları (Büyük organizasyonlar, uluslararası kuruluşlar vb.) da vardır (Yurdasev, 2005). Bu yüzden sadece devletlerarası ilişkiler açısından incelemenin eksik olacağı uluslararası ilişkiler disiplininde artık bilgi daha önemli hale gelmiştir. Bu disiplin gerek sivil toplum kuruluşlarının hareketleri, gerekse devletlerin yönetim biçimleri olsun sürekli değişen dünya dengelerinde bir harita gibi düşünülebilir.

Uluslararası ilişkiler alanında hızla genişleyen istihbarat literatürü, hem yerel hem de uluslararası ortamlara doğrudan etkileri olan önemli güvenlik politikalarının nasıl oluşturduğunu ve nasıl uyguladığını araştırır. İstihbarat kurumlarının işlevselliğini arttırarak “doğru istihbarat nasıl elde edilerek etkin bir şekilde kullanılır?” sorusunu temel

alan çalışmalar yapılmaktadır. İstihbarat kurumları, istihbaratın tanımından da anlaşılacağı üzere, yerel ve uluslararası ortamlar hakkında bilgi toplamak, analiz etmek, yorumlamak ve yaymak amacındadır. Siyasi iktidar tarafından daha çok istenen istihbarat çalışmaları, istihbarat kurumlarının da politikaların uygulanmasına aktif olarak katılmasını sağlamaktadır.

İstihbarat sadece bilgi toplamak olarak algılanmamalı aynı zamanda bu konunun çok daha detaylı olarak incelenmesi gerekmektedir. O yüzden literatürde birçok istihbarat tanımı yapılmış ve bunların birçoğu istihbaratın artık akademik yönü olması gerektiğini de ortaya çıkarmıştır. Elde edilen bilgilerin istihbarat olarak kullanılması için gerekli olan bazı özellikler ve analiz aşamaları vardır. Bunları tanımlayabilecek ve analizini yapabilecek istihbarat uzmanlarının da önemini unutmamak gerekir. İstihbarat, devleti korumaya hizmet etmenin dışında, yeni çıkabilecek olan tehditleri de önceden öngörebilmektedir. 11 Eylül 2001'den sonraki dönemde uluslararası terörün boyutunu dünya çok daha iyi anlamış ve yaygın istihbarat anlayışı büyük ölçüde değişmiştir. Yerel terör kavramı yerini uluslararası teröre bıraktığından dünya ülkelerinin genelinde bir korku hâkim olmuş ve istihbarat örgütlerinin çeşitli yöntemlerle geliştirilmesi gerekmiştir.

İstihbarat çeşitli boyutlarda sınıflandırılabilir. Bu sınıflandırmaların amacı istihbaratın nerede, nasıl ve hangi yöntemle kullanılacağını belirlemektir. Uluslararası ilişkiler, istihbaratın hemen hemen her çeşidini içerisinde barındırabilir. Özellikle insan istihbaratı ve açık kaynak istihbaratı en çok kullanılan istihbarat türlerinden olup bunlara tezin içerisinde detaylı olarak yer verilecektir.

İstihbarat tarihinin insanoğlunun ilk dönemlerine kadar uzandığı bilinmekte ancak ilk yazılı olarak beyan edildiği yerin Sun Tzu'nun yazdığı "Savaş Sanatı" adlı eser olduğu, günümüze kadar bir çok çevirisi ve baskısı yapılan eserde askeri istihbaratla ilgili yapılanları yazdığı da unutulmamalıdır (Tzu, 2008). Eskiden genelde askeri istihbarat alanında kullanılan bilgiler, gelişen dünyayla beraber sivil hayata da adapte olmuş ve bazı uluslararası bankalar, kurum ve kuruluşlar tarafından da istihbarat birimleri kurulmuştur. Devletler kendi istihbarat örgütlerini kurarak, farklı devletlerle olan dış politikalarını belirlemede ve uluslararası platformlardaki yardımlaşmalarında kullanılmak üzere bilgiler toplamaya çalışmaktadır. Dünyadaki büyük devletlerin istihbarat yapıları da

birbirlerinden farklı olup, aynı zamanda iç ve dış istihbaratla da ilgilenen bazen birden fazla örgütleri bulunabilmektedir.

Uluslararası ilişkiler, istihbarat faaliyetleri tarafından doğrudan yâda dolaylı olarak etkilenebilen bir disiplindir denilebilir. Çünkü devletlerin birbirlerinin niyetlerini anlamak için ya da olası zarar verici faaliyetlerini engelleyebilmesi bu toplanan bilgilerle mümkündür. Ancak her istihbarat doğru olmayabilir. Bunların sonucunda da ortaya bir istihbarat başarısızlığı çıkacak ve savaşlara kadar neden olabilecektir. Bunun en yakın tarihli örneği de Irak savaşıdır. Tezin ileriki bölümlerinde detayları anlatılacak olan bu savaşın çıkış nedeni yanlış istihbarat raporudur. Bu da uluslararası alanda ciddi sıkıntılara yol açmış, ülkeler arası ilişkiler oldukça gerilmiştir. Sadece yanlış istihbarat raporları değil aynı zamanda 21. Yüzyılda gelişen teknolojiyle beraber artan bilgisayar korsancılığı ve yarattıkları ya da yaratabilecekleri terör olaylarını tahmin edebilmek ancak bilgiyle mümkündür. Aynı zamanda geleceği öngörebilmek için yapılan analiz çalışmalarının verimliliği de oldukça önemlidir. Bu analiz çalışmalarının sonucunda ortaya çıkan istihbarat raporlarında, yorum yapacak istihbarat uzmanlarının eğitilmiş bireyle olması oldukça önem teşkil etmektedir. Son dönemde yaşanan pandemi olayında, medikal istihbarattaki eksikliklerde ortaya çıkmıştır.

Bu çalışmada amaç, geçmişten bugüne kadar dünyanın değişimiyle ortaya çıkan değişik devlet yapılanmalarının ve farklı olayların ışığında akademik bir çalışma haline gelen istihbaratın öneminin vurgulanması ve bu süreç içinde yaşadığı değişimin hangi olaylardan etkilenecek uluslararası ilişkileri de etkilediğinin araştırılmasıdır. Uluslararası ilişkilerin genel anlamda özellikle son yıllarda istihbarat faaliyetlerinden oldukça etkilendiğini, dünya düzenini yavaş yavaş değiştirmeye başladığını ve eskisinden daha çok tehlikenin dünyamızı etkileyebileceği ve ilişkileri bozabileceğini düşündüğümüzde, istihbaratın önemi bir kere daha ortaya çıkmaktadır. Bu çalışmada amaç, istihbaratın ne olduğunu anlatmak ve tarihsel gelişim süreci içerisinde önemini daha da arttığını ve özellikle yaşanan kriz dönemlerinde dış politikaları ve ilişkileri belirlemede ne kadar etkili olduğunu belirtmektir.

Bu tezin birinci bölümünde istihbaratın çok çeşitli tanımları varken çok da çeşidi olduğundan bahsedilecektir. İstihbaratın ana kaynağı insanlar gibi görünse de gelişen ve

küreselleşen dünyamızda istihbaratın da çeşitlediği görülmektedir. Bu tezde üç ayrı başlıkta incelenecek olan istihbarat kavramında en yaygın olarak kullanılan istihbarat türünün açık kaynak istihbaratı olduğu daha sonra insan istihbaratının da en az onun kadar önemli olduğu vurgulanacak, aynı zamanda diğer istihbarat türlerinden de detaylı olarak bahsedilecektir. İstihbaratı elde etmek kadar karşı ülkelerin kendi ülkeniz hakkında elde edebilecekleri engellemek de oldukça önem kazanmıştır. Bu faaliyetlere İstihbarata Karşı Koyma(İKK) faaliyetleri denilmektedir. Bu alanda çalışan istihbarat uzmanlarının psikolojileri çok daha kolay bozulabildiğinden uzun süre bu alanda çalışmamaları gerektiğini beyan eden çalışmalarda bulunmaktadır (Olson, 2001).

Tezin ikinci bölümünde tarih boyunca istihbarata olan bakış açısının da değiştiğinden bahsedilecektir. İstihbarat uzmanlarının çalıştıkları ülkelere göre yapılandırılmaları da farklıdır. Özellikle Soğuk Savaş döneminden sonra güvenliğin artık yalnızca askeri meselelerle alakalı olmadığı, güvenliği uygulayacak aktörlerin çeşitlendiği ve güvenliği sağlanacak olan aktör ve nesnelerin de sayılarının arttığı kabul edilmektedir. Güvenliğin sağlanmasında devlet ana aktörken, bunlara uluslararası örgütler, STK'lar ve uluslararası platformların da eklendiği görülmektedir. Uluslararası alanda devletler kendi güvenliklerini sağlarken en önemli başvurduğu kaynaklar istihbarattan elde edilenlerdir denilebilir. Ülkeler istihbarat alanına yaptıkları yatırımlarda, kurdukları teşkilatlara genel olarak baktığımızda iç ve dış istihbarat yapılanmaları olarak ayırmışlardır. Bu bölümde dünyanın önde gelen ülkelerinin istihbarat teşkilatlanmalarını yapısının detayları ve kuruluşları incelenecektir. Aynı zamanda Türk istihbarat tarihinden de bahsedilecek ve diğer ülkelerle kıyaslanması sağlanacaktır. Teknolojinin çok fazla gelişmediği dönemde kullanılan istihbarat olarak nitelenen geleneksel istihbaratla, 21. Yüzyıldan sonra gelişen teknolojiyle ortaya çıkan modern istihbarat karşılaştırılacak, aynı zamanda dönemselsel olarak değişen istihbarat toplama yöntemleri ve o dönemlerin önemli olayları incelenecektir.

Tezin son bölümünde ise, istihbaratın uluslararası ilişkileri nasıl etkilediğinden bahsedilecektir. İstihbaratın dış politikaya yapımına ve uluslararası alanda devletlerin ilişkilerini nasıl etkilediğine dair örnekler verilecek aynı zamanda istihbarat başarısızlığının tanımı yapılacaktır. İstihbarat başarısızlığı olarak görülen ve dünyaca bilinen olayların nedenleri ve sonuçlarıyla beraber uluslararası arenada ilişkileri nasıl

değiřtirdiđi ve dünya dűzeninin nasıl etkilediđi anlatılacaktır. Aynı zamanda gűncel olaylar olan siber gűvenlik ve medikal istihbarat alanlarının dűnyayı nasıl etkilediđinden ۆrnekler verilerek bahsedilecek ve bu alanlara artık daha fazla yatırımlar yapılması gerektiđini anlayan dűnyanın tavrı belirtilecektir.



BÖLÜM 1: İSTİHBARAT İLE İLGİLİ KAVRAMLAR

1.1. İstihbarat Kavramı

Köken olarak Arapçada “istihbar” kelimesinin çoğul halinden gelen istihbarat, Türkçe anlamıyla haber alma ve yeni öğrenilen bilgiler anlamına gelmektedir. İstihbarat temel anlamda bilgi toplamak manasına gelse de teknik anlamda bakıldığında ülkelerin kendilerini koruma faaliyetleri amacıyla yurt içi ve dışında gerek askeri gerek sivil alanlarda kendi iç ve dış güvenliklerini korumak amaçlı casusluk çalışmaları yapması anlamına da gelmektedir (Bahar, 2011, s. 19). Elde edilen istihbaratın işlenerek, alınan haberleri yorumlama, değerlendirme ve bir sonuca ulaştırabilme de istihbarat tanımının içerisinde yer alır (Avcı, 2004, s.12).

İstihbarat tek bir tanıma sığabilecek bir kavram değildir. Pek çok akademik yayında istihbaratın farklı tanımlarını görebilmek mümkündür. Gill ve Phythian istihbaratı potansiyel tehlikeli olabilecek olaylara karşı önleyici politikaları geliştirmek amaçlı gizli bilgi toplama, bunların planlaması ve analizi olarak görürken (2006, s.7); Muazzez Şenel ve Turhan Şenel’e göre istihbarat düşman veya düşman olması muhtemel devletlerin maksatları, tasavvurları bunları yapabileme kapasiteleri hakkında türlü şekillerde haber toplama veya bilgi sahibi olmaktır (1997, s.32). İstihbarat alanında öncü çalışmalardan biri kabul edilen Sherman Kent’in–CIA Ulusal Tahminler Ofisinin ilk direktörü- kitabında ise istihbarat bilgi toplama, organizasyon ve faaliyete geçme olarak özetlenebilir (1949, s.3-8). Türk akademisyenlerden Ümit Özdağ ise istihbaratın bir bilim olduğunu vurgulamakta ve şu şekilde tanımlamaktadır;

İstihbarat, ulaşılabilen bütün açık, yarı açık ve/veya gizli kaynaklardan her türlü aracın kullanılması sonucunda elde edilen her türlü veri, malumat ve bilginin ulusal genel veya ulusal özel plandaki politikaların gerçekleştirilmesi ve ulusal politikalara zarar verilmesinin engellenmesi amacı ile toplandıktan sonra önemine ve doğruluğuna göre sınıflandırılması, karşılaştırılması, analiz edilerek değerlendirilmesi süreci sonunda ulaşılan bilgidir (2014, s.31).

İstihbarat sadece bilgi toplama ve analiz olarak düşünüldüğünde içerdiği diğer özellikler kaybolacaktır. Bu yüzden de tek bir tanıma sığdırılmaz denilen istihbarat kavramı için birçok yazar yukarıdaki tanımlamaların dışında birçok tanım daha yapmıştır. Kahn’a göre bilginin en geniş anlamı olan istihbarat savunma için değil saldırı için önemliyken, Gill ve Phythian’a göre hem saldırı hem de savunmada istihbarat önemlidir

(Seren, 2017, s224-228). Herman'a göre ise istihbarat siyasi, askeri, ekonomik, toplumsal ve diplomatik gelişmeleri öngörmeyi amaçlayan evrensel bir sosyal bilimdir (Karaağaç, 2021). Micheal Warner ise istihbarata farklı bir yönden bakmış ve istihbaratın devletlerin birbirlerini daha iyi anlamalarına ve etki altına alabilmelerine neden olan bir takım faaliyetler dizisi olarak tanımlamıştır (2002, s.15).

Devletin güvenliğini sürdürülebilmesinde önemli bir rol oynayan istihbaratın, düzgün işleyebilmesi için önemli olan bir takım özellikler de vardır. Bunlar; doğruluk, kesinlik, sürat, gizlilik, organizasyon ve eğitimli personel kullanılmasıdır (Kavsıracı, 2020). İstihbaratın doğru olması devletin uygulayacağı politikaların düzgün işlemesini sağlarken, kesin olması da yöneticilerin doğru kararlar almasına imkân sağlayacaktır. İstihbarat da sürat oldukça önemlidir çünkü zamanı geçtikten sonra ulaşan bilgiler kullanılamaz. Aynı zamanda bu bilgilerin gizlilik seviyeleri de önemlidir; herkesin yapılan analizlerin sonuçlarını öğrenmemeleri gerekir. Sistemli bir şekilde bilgi toplayarak onları bir bütünün içine yedirmekte organizasyonel faaliyetler açısından önemliyken, bu bilgileri yorumlayabilecek öngörüsü yüksek eğitimli personellerin olması da istihbarat faaliyetlerinde önemli özelliklerden biri olarak ortaya çıkmaktadır. Kısacası tüm istihbarat faaliyetlerini bir çatı altında istihbarat örgütleri toplar denilebilir.

İstihbaratın kazandırdığı yararları baktığımızda dört ana başlık görülmektedir. İstihbarat bir baskın yâda sürpriz saldırıya karşı hazırlıklı olunmasını salarken, politika yapıcılara uzun vadeli bir öngörü de sağlamakta, aynı zamanda politika oluşturma sürecine yardımcı olduğu gibi devletin sırlarını saklamakta da yardımcı olmaktadır. (Lowenthal, 2000, s.2-5)

İstihbarat iç ve dış istihbarat olarak ikiye ayrılır. İç istihbarat adından da anlaşılacağı üzere, ülke içindeki terör faaliyetleri, düzen bozucu faaliyetler, karşı istihbarat ve toplumsal ayaklanmaları ve çatışmaları engellemek için yapılan her türlü bilgi toplama faaliyetiyken, dış istihbaratsa kendi ülkeleri dışındaki devletler hakkında siyasi, toplumsal, dini, ekonomik v.b. gibi alanlarda bilgi toplama faaliyetidir (Demircioğlu, Güven & Hınız, 2021).

1.2. İstihbarat Çarkı

İstihbarat, insanoğlunun başlangıcından itibaren var olduğu varsayılan, sürekli

gelişim göstererek önemi gün gittikçe artan bir faaliyettir. Bilgi elde etme olarak özetlenen istihbarat faaliyetleri kesintisiz süregelen bir çalışma olduğundan istihbarat örgütleri arasında bu süreç bir çarka benzetilir (Yılmaz B. , 2020).



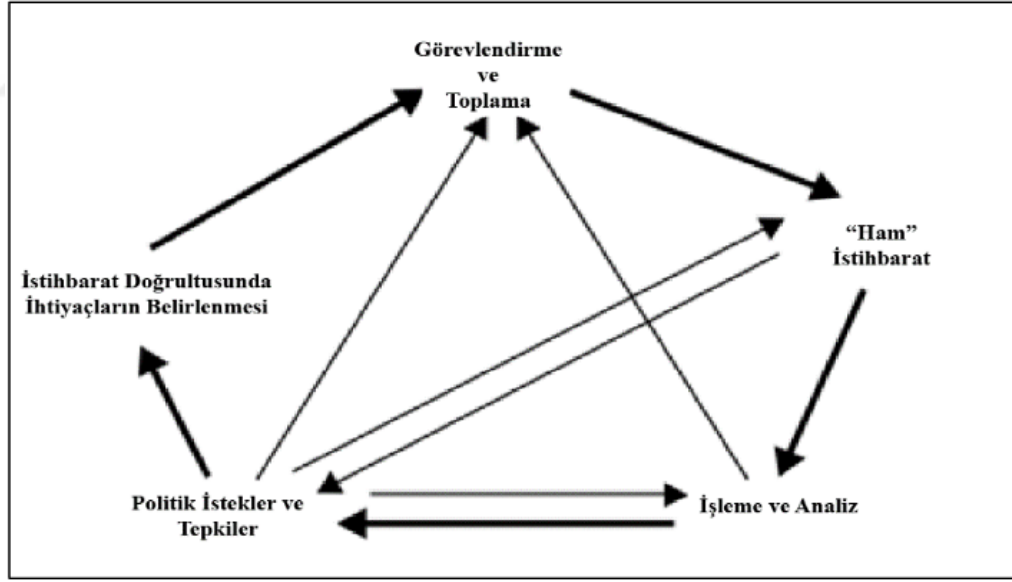
Şekil 1: İstihbarat Çarkı

Kaynak; (MİT, 2022a)

Şekil -1' de görülebileceği üzere; öncelikle istihbarat ihtiyacı belirlenir ve hangi alanlarda haber toplanacağı konusunda yönlendirmeler yapılır. Bu aşamada amaç ham verileri toplamaktır. Haberlerin toplanması süresiyle devam eden bu döngüde kaynak olarak açık ve kapalı kaynaklar kullanılabilir. Açık kaynaklar yazılı basın organları, televizyon ve internet sitelerinden oluşurken kapalı kaynaklar ise belirli bir istihbarat ihtiyacına yönelik bunu yapabilecek yetenekte olan kişilerden oluşur (Tiryaki & Özdal, 2020). Haberlerin toplanmasından sonraki aşamada haberler değerlendirilir yani işlenir. İşlenme de üç aşamadan oluşmaktadır. İlk aşama olan tasnif kısmında benzer bilgiler aynı gruplarda toplanır. İkinci aşama olan kıymetlendirme kısmında ise, haberlerin doğruluk ve güvenilirlikleri saptanır. Üçüncü aşama ise en önemli kısım olan yorum kısmıdır. Bu kısımdaki hedef eldeki bilgilerle benzeri durumları karşılaştırarak bir sonuca ulaşmaktır (Berk & Sarı, 2022). İstihbarat çarkının son aşaması olan istihbaratın yayımı ve kullanılması ise değerlendirilen haberlerin istihbarat niteliği kazandıktan sonra zamanında

ve hızla ilgili yerlere ulaştırılmasıdır (Mit, 2022a). Tüm bu yönleriyle bakıldığında istihbarat çarkının istihbarat teşkilatlarınca işlerin sırasını ve aşama aşama ne yapılması gerektiğini gösteren bir yol haritası olduğu söylenebilir.

En geleneksel anlamdaki istihbarat çarkının aşamaları yukarı da belirtilmiş olsa da literatüre baktığımızda farklı istihbarat çarklarının da kullanıldığı görülmektedir. Örneğin Gregory Treverton 2001 yılında yazdığı kitabında istihbarat çarkını beşgen bir modele benzetmiştir (2001, s.106). Geleneksel modelden farkı ise aşağıdaki Şekil-2'den de görülebileceği üzere gelen ilk verilerin karar vermede yetkili kişilerle paylaşılıp geri bildirim alınmasıdır. Burada karar alıcıları da istihbarat çarkının içerisine dâhil etmiştir. Bunun hem iyi yanları hem de kötü yanları bulunmaktadır. İyi yanı olarak, gereken bilginin bu çarkta görevli kişiler tarafından iyi anlaşılması gösterilebilecekken kötü tarafı ise karışan politika yapıcılarla objektiflik ilkesinden uzaklaşarak çarkın politika süresine dâhil olması gösterilebilir (Berk & Sarı, 2022).

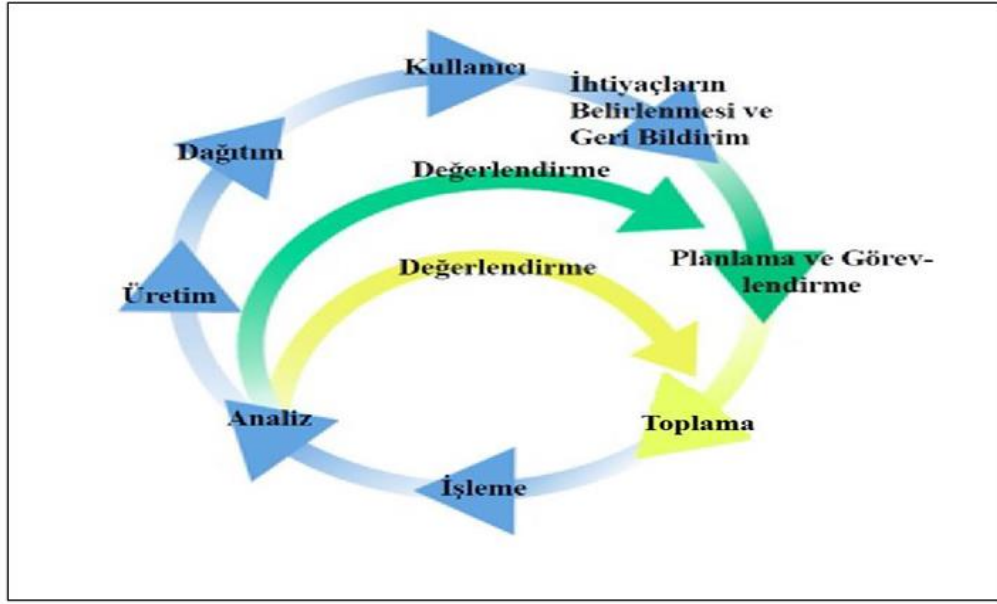


Şekil 2: Beşgen İstihbarat Çarkı

Kaynak: (Berk & Sarı, 2022)

Bir diğer istihbarat çarkının tanımını yapan ve daha geniş perspektifte literatüre sunan kişi ise Lisa Krizan'dır. Şekil-3'de görülen sekiz aşamalı istihbarat çarkı, 1999 yılında yazdığı eserinde istihbarat aşamasını sekiz basamakta belirtmiş ve neredeyse her basamağın birbiriyle ilişkili olduğunu anlatmıştır (Krizan, 1999, s. 8). Krizan,

“Intelligence Essentials for Everyone” adlı kitabında istihbarat çarkının biraz yeniden yapılandırılmış bir görünümünü sunmuş ve Douglas Dearth'tan alıntı yaparken şöyle demiştir: "Bu etiketler ve resim ... istihbarat tek boyutlu ve tek yönlü bir süreç olduğu şeklinde yorumlanmamalıdır. Aslında süreç “çok boyutlu, çok yönlü ve - en önemlisi - etkileşimli ve yineleyici bir süreçtir” (Wheaton, 2011). Bu oluşturulan çarktaki süreçler arasındaki etkileşim her ne kadar daha çok ve kuvvetli olarak görünse de ulaşılan her aşamada değerlendirmeye tabi olunması istihbaratın temel ilkelerinden olan hızlı olma ilkesine aykırı düşebilmektedir.



Şekil 3: Sekiz Aşamalı İstihbarat Çarkı

Kaynak: (Berk & Sarı, 2022)

Literatür incelemesine bakıldığında bunların dışında da pek çok istihbarat çarkı modeli görülebilmektedir. Ancak istihbarat çarkının genel modeli (Şekil-1) en yaygın ve sık kullanılanı olduğundan, ülkemizdeki istihbarat örgütü olan Milli İstihbarat Teşkilatının kendi sitesinde de bu model esas alınmıştır. Buna göre önce bilgi ihtiyacı belirlenir, daha sonra çeşitli yollarla haberlerin toplanması sağlanır üçüncü aşamada değerlendirilen bilgiler son aşamada kullanılır ve ilgili kişi ve/veya birimlere aktarılır.

1.3. İstihbaratın Çeşitleri

İstihbarat tek bir alanda yapılmadığından kendi içinde kaynaklarına ve seviyelerine göre çeşitlendirilmiştir. Aşağıdaki anlatılacak olanlardan stratejik ve taktik

istihbarat seviyelerine göre istihbarat grubunun altında incelenirken (Koca, 2019), diğerleri kaynaklarına göre ayrılan istihbarat çeşitlerindedir (Seccops, 2023). Burada incelenecek olan türler, uluslararası politikalara etki eden ya da edebilecek olan istihbarat alanlarıdır.

1.3.1. Açık kaynak istihbaratı (AKİST)

İstihbaratın en önemli bilgi edinme yöntemi açık kaynak istihbaratıdır ve bilgilerin büyük bir çoğunluğu bu yolla elde edilir (Hot, 1995, s. 57). Bu istihbarat türü, adından da anlaşılacağı üzere, her türlü halka açık bilgilere doğrudan ulaşımıdır. Halka açık kaynaklara baktığımızda ise günlük hayatımızda çok sık kullandığımız internet, gazete, dergi, konferans bildirimleri, medya, makale fotoğraf olarak gösterilebilir. Maliyet açısından bakıldığında da açık kaynak istihbaratı her an her yerde ulaşılabilen bir bilgi olduğundan daha az maliyetli olduğu açıktır (Yılmaz S., 2006, s.126-127). Her ne kadar maliyeti az ve kolay ulaşılabilir bir istihbarat türü olsa da, açık istihbaratta bilgilerin doğruluğunu teyit etmek zor olabilir. Özellikle artan teknolojiyle gelişen internet ortamında bir bilginin doğruluğunun kontrolü güçtür. Bu yüzden ki burada istihbarat uzmanlarına bu bilgileri ayırtırmakta önemli görevler düşmektedir (Kavsıracı, 2020).

Açık kaynakların içerisinde en çok kullanılanlardan biri de ilerlemiş teknolojinin bir ürün olan internettir. Çünkü internet bilgiye ulaşmayı kolaylaştırmıştır (Sapancı, 2007) Ancak internetteki her bilgi doğru olmak zorunda değildir. İstihbarat anlamında kullanılacak bilginin özelliklerinden biri de bilginin güvenilirliği ve doğruluğudur (Özdağ, 2014, s.36). İnternetteki bilgileri doğruluğundan emin olabilmek için dikkat edilmesi gereken hususlarda vardır. Normal şartlar altında internetten elde edilen bilginin doğruluğunun farklı siteler ya da kaynaklar tarafından da desteklenmesi gerekmektedir. Kaynak olarak kullanılan sitenin güvenilirliği de önemli olup, haberin amacının manipüle etmek mi yoksa gerçek haber olup olmadığı da sorgulanmalıdır. Teknolojinin gelişmesiyle beraber artan sosyal medya kullanımından kaynaklı bilginin kaynağına hemen inanılmamalı, özellikle tarih ve kullanılan görsellere dikkat edilmelidir. Her elde edilen bilgi paylaşılmamalı, dikkat çekmek amaçlı abartılı başlıklara güvenilmemeli, internet adreslerinin URL'leri güvenilir sitelerin benzerleri gibi açılacağı unutulmamalı, montaj yapılmış görsellere dikkat edilip, reklam ya da parodi amaçlı sitelerin yapmış

olabileceği haberlere itibar gösterilmemelidir. Bu basamaklar takip edildiğinde bile yapılabilecek bir gözlem hatası doğru bilgiye ulaşmayı engelleyebilir. Her ne kadar internetten bilgi edinmek kolay gibi görünse de, bilginin doğruluğunu özellikle istihbarat olarak kullanılabilen bilgi olarak ortaya çıkarılabilmek sürecini oluşturabilmek oldukça güç olduğu görülmektedir. Bu yüzden istihbarat uzmanlarının bilgi ve yeteneği oldukça önemlidir (Aytekin, 2019).

II. Dünya Savaşı'ndan sonra akademik olarak da tanınan istihbarat kavramı (Ünal ve Yarman, 2015, s.151) değişen teknoloji ve gelişen dünyayla birlikte yeni kaynaklara da sahip olmuştur. Geçmişte gazete, dergi gibi yazılı açık kaynakları tek tek elle inceleme zorunluluğu varken, günümüz teknolojisinde bu kaynaklar bilgisayar ortamında incelenip çok daha hızlı ve az maliyetli bir biçimde istihbarat toplanabilmektedir. Ancak bu, istihbaratı kolaylaştırırken analiz yapma kısmını zorlaştırmıştır. Çünkü CIA eski başkanlarından James Woolly'nin de bahsettiği üzere eskiden ulaşılabilecek kaynaklarla yapılabilecek tahminler daha kolay ve basitken, şimdi küreselleşen dünyada çok daha farklı küçük ve büyük yeni tehditler barındırdığından tahmin kısmı oldukça zor hale gelmiştir (Arı, 2013, s. 174). Açık kaynaklara ulaşımın oldukça kolay olmasından kaynaklı bilgilerin manipüle edilme olasılığı oldukça yüksektir; bu yüzden ki “bilgi” ve “istihbarat” kavramlarını birbirinden ayıracak özellikleri iyi bilmek konunun analizini yaparken oldukça yardımcı olacaktır (Ateş H. , 2013, s. 17).

AKİST'in avantajları olduğu kadar dezavantajları da olduğu bir gerçektir. AKİST maliyeti düşük, kolay kullanımlı yayımı ve elde edilmesi kolay güncel bilgi edinmeyi, ekonomik ve politik analizler için geniş çapta veri tabanı sağlamayı, karşı tarafın amacını anlamının yanında diğer istihbarat yöntemlerinden gelen bilgilerin doğruluğunu belirlemeyi sağlayıp avantaj sağlarken; diğer taraftan yanlış bilgilere karşı hassas oluşu, en iyi kaynağı ararken kaybedilen zaman, aşırı bilgi kirliliği, karar vericilerin kolay etkilenmesi, kaynakların güvenilirliği sorunu, lisans bilgisi gerektirmesi, kolay atlatılabilirliği ve gelişmeyen toplumlar hakkında bilgi edinmekteki zorluğu bakımından da dezavantajları olduğu söylenebilir. Buradaki ana problem güvenilirliktir. Çünkü yukarıda da bahsedildiği üzere her şey bir kaynak olarak kullanılabilirdiğinden, doğruyu yanlıştan ayırt etmek oldukça güçtür. Bu da istihbarat karmaşasına yol açabileceğinden, analiz yeteneği güçlü istihbarat uzmanlarının olması oldukça önemlidir (Berk O. , 2014,

s. 36).

1.3.2. Siyasi istihbarat

Bir ülkenin siyasi yapısını oluşturan, anayasal düzeninin yapısında yer alan bütün unsurlara karşı yapılan istihbarat çeşididir (Özdağ, 2018). İç ve dış siyasi istihbarat olarak kendi içinde ikiye ayrılan kavramda; iç siyasi istihbarat içerdeki siyasi faaliyetleri takip ederken, dış siyasi istihbarat ise adından da anlaşılacağı üzere, ülkelerin diğer ülkelerden aldığı istihbarat anlamına gelmektedir. Bu anlamdan da anlaşılacağı üzere dış politika ve uluslararası ilişkiler açısından kilit konumdaki istihbarat çeşitlerinden biridir (Acar & Turhal, 2007, s.101-105) .

Devletler devamlılıklarını sağlamak adına rakip devletlerin siyasetini öğrenmek ve bunları her zaman göz önüne almak durumunda kalmışlardır (Akar, 2005, s. 77). Çünkü elde ettikleri bu bilgilerle yaptıkları siyasi analizle, uluslararası ilişkilerini de yönetmekte olduklarından sadece savaş döneminde değil barış döneminde de bu bilgilere çok ihtiyaç duymaktadırlar (Serim, 1941, s. 27). Devletlerin istihbarat toplamadaki ana amacının kendi güvenliklerini sağlamak (Lowethal, 2000, s.8) olduğu düşünüldüğünde, siyasi istihbaratın amacının da sosyal ve siyasi istikrarını bozacak hareketleri öngörebilmek olduğu söylenebilir (Akbal & Tılsbık, 2006, s.47).

Siyasi istihbaratın kurumsal anlamda önem taşımaya başladığı ve bir birim olarak çıktığı dönem, II. Dünya Savaşı sonrasına denk gelmektedir. Bu dönemde istihbaratın değişen önemiyle beraber devletler sadece siyasi değil aynı zamanda askeri ve diplomatik kurumları da kapsayan bir istihbarat yapılanmasına girmişlerdir (Seren, 2017).

1.3.3. Askeri istihbarat

Devletlerin sürdürülebilirliklerini devam ettirmeleri önemli olduğundan iç ve dış güvenliklerini sağlamak açısından önemli olan askeri istihbarat, haberlere ulaştıktan sonra komutanların bilgilendirilmesi, hedeflerin tespit ve teşhis edilmeleri, harekât planlanmasının saptanması ve etkinliğin değerlendirilmesi aşamalarından oluşur (Joint Chief of Staff, 2013). Bir devlet, kendisine düşmanlık teşkil edebilecek ya da edemeyecek olsa bile ileriki süreçlerde kendisine tehlike olarak gördüğü devletlerin askeri güçlerini bilmeli ya da tahmin edebilmelidir. Bu bilgi sayesinde kendilerini savunabilecek ya da

savunmaya hazırlanabilecektir. Bu istihbaratla gelen haberler, dış politikada kritik zamanlarda koz olarak kullanılma alanı açmaktadır. Askeri istihbarat sadece savaş döneminde değil sulh döneminde de oldukça önem taşımaktadır (Ho, 2007).

Gültekin Yıldız'a göre askeri istihbarat genel askeri istihbarat (sadece mevcutta ulaşılabilecek istihbarat toplamaz aynı zamanda hedef hakkında önceden bilgi alır) ve güncel istihbarat (genel istihbarattan gelen bilgileri bir düzene sokarak robotlaştırır) olarak ikiye ayrılır (2019, s.16). Günümüz koşullarında savaşların boyutu her ne kadar değişse de varlığını sürdürmek isteyen devletler için hala önemini korumaktadır (Aköz, 2020, s. 31).

1.3.4. Sosyal istihbarat

Ülkenin sosyal altyapısı ve kültürel alanlarına odaklanan bir istihbarat çeşidi olan sosyal istihbarat, dinamik bir yapıya olduğundan geleneksel istihbarat sürecinin gelişmesine katkıda bulunur. Çünkü bir ülkenin gelenek ve göreneklerini, kullandıkları dili ve paylaştıkları kültürleri toplumun temel taşı olduğundan bu alanlardaki tüm bilgileri toplayabilmek devletlerin zayıf noktalarını bilmekte önemlidir (Lister, 2011). Sosyal istihbaratın amacı, hem bu bahsedilen konular hakkında bilgiler toplamak hem de istihbarat toplanmak istenen milletin sağlık, eğitim, sanat ve sosyal alanlardaki kabiliyetlerini öğrenerek oluşabilecek tehlike ve fırsatları analiz etmektir (Özdağ, 2014, s.97-98). Soğuk Savaş'tan sonra ortaya çıkan asimetrik savaşlar düşünüldüğünde sosyal istihbaratın iyi yapılması demek savaş durumunda oldukça etkili baskınlar yapabilmek anlamına da gelebilir (Özer, 2018a, s.63). Çünkü asimetrik savaşın bir yönü de, rakibine göre kuvvetli olan devletin zayıf yönlerinin diğer taraf tarafından kullanılması olduğundan (Karasoy, 2022a), sosyal istihbaratı iyi yapan devletler, karşı tarafın sosyal ve kültürel kaygılarını kullanarak avantaj elde edebilirler.

1.3.5. Stratejik ve taktik istihbarat

Sherman Kent tarafından ortaya atılmış olan stratejik istihbarat kavramı politika yapıcılar ve karar alıcıların düşman ya da dost devletlerin yapabileceklerine, kendi politika ve taahhütlerine zarar vermeyecek şekilde sürekli sahip olunması gereken bilgi türü olarak ifade edilir (Kent, 2003, s.136). Bu tanımdan anlaşılacağı üzere stratejik istihbarat, bir

olay olmadan önce önlemeye yönelik toplanan bir bilgi türüdür. Stratejik istihbarat bir araştırma yöntemidir ve yürütülen araştırmaları politika yapıcılar, karar vericiler ve profesyoneller için politika ve stratejiler geliştirmek için kullanmayı amaçladığından, en yüksek kalitede bilgiler elde etmek stratejik istihbarat alanındaki faaliyetlerin ana hedefidir (Özdağ, 2018). Bu bilgi toplama türü sadece düşman devletlere değil, dost görülebilecek devletlerin de uyguladıkları stratejiler doğrultusunda da yeni politikalar gerçekleştirilmesine yardımcı olmaktadır.

Öncelikli hedefleri arasında politikacıların bilgi ihtiyacını karşılamak olan stratejik istihbarat, aynı zamanda olası tehlikelerin değişen dünyayla beraber değişen yapısını anlayarak iyi bir analiz yapmak ve onlara karşı koyma yöntemleri bulmakla da ilgilenmektedir (Koloğlu, 2003, s. 20). Stratejik istihbarat gerek amacı gerekse kullandığı politik ve askeri kaynaklar düşünüldüğünde en önemli istihbarat türü olarak ortaya çıkmaktadır (Seren, 2017, s. 273-274). Politika yapıcıların, dünyadaki eğilimlere karşı alabilecekleri tedbirler ile kamu düzeni ve güvenliğini sağlamak için alacakları kararların stratejik istihbarattan gelen bilgiler tarafından doğrudan etkilendiği kaçınılmaz bir gerçektir (McDowell, 2009, s. 10-11).

Stratejik istihbarat neticesinde politika yapıcılar ya da karar mekanizmasında görevli kişiler, savaş ihtimaline karşı tedbirler alabildiği gibi, değişen dünyadaki gelişen teknolojiyi takip ederek olası fırsat ve tehditleri tahmin etme ve uluslararası alanlarda yapılabilecek olan diplomasi görüşmelerinde öne geçme şansına sahip olurken, aynı zamanda yapılacak karşı istihbaratın da yönünü belirleme şansları olur (Özdağ, 2014, s.133). Buradan da anlaşılacağı üzere stratejik istihbarat üst düzey politika yapıcılara bilgi sağlayan bir istihbarat türüdür (Köseli, 2009).

Stratejik istihbarat daha çok önleyici ve uzun vadeli bir süreç olması yönüyle ortaya çıkarken (Clark, 2010), taktik istihbarat daha çok günü kurtarmak maksadıyla elde edilen bilgilerin analizidir. Bu yüzden kısa süreli planlarda taktik istihbarat daha çok kullanılmaktadır (Gül, 2014, s. 84). Bu iki istihbarat türü arasındaki diğer farklarda, istihbaratın kapsamında, görüş açısında ve yetkilendirme seviyesinde görülmektedir (Goldman, 2006). Taktik istihbarat hedefteki kaynağın kapasitesini, sınırlılıkları, zayıflıklarını belirleyerek operasyonlarda yarar sağlayacak istihbarat olarak da

tanımlanmaktadır (Kruys, 2007). Taktik istihbarat, anlaşma olmadığında bunların çözümünde anında ya da kısa süre içinde çözüm sağlamaya odaklı bir bilgi toplama yöntemidir (McDowel, 2009). Taktik istihbarat genelde orta düzey yönetici ve politika yapıcılarla paylaşılmaktadır. Her ne kadar taktik istihbarat genelde kısa süreli hedeflerde uygun görülse de stratejik hedeflere ulaşmak amacıyla da kullanıldığı bilinmektedir. Politikacılar daha çok kısa süreli ya da hemen kullanabileceği istihbaratı kullanmayı tercih ettiğinden stratejik bilgiye çok ihtiyaç duyulmamıştır (Gül, 2014). Terör engelleme boyutunda stratejik ve taktik istihbarat anti-terörizmde kullanılmaya devam derken, taktik istihbarat genelde istihbarata karşı koyma(İKK) faaliyetlerinde kullanılmaktadır.

1.3.6. Ekonomik istihbarat

Ekonomik İstihbarat (EI) ekonomik verilerin (ürünler, müşteriler, rakipler vb. hakkında) kuruluşlar içinde toplanmasını, değerlendirilmesini, işlenmesini, analiz edilmesini ve yayılmasını içerir (Briciu, Vrincianu & Florin, 2009). Temelde üç ana özelliği vardır. Birincisi, ekonomik istihbarat kamuya açık kaynakların sömürülmesine dayanmaktadır. Uzmanlar, gerekli tüm bilgilerin %80 ila %90'ının kamuya açık kaynaklardan temin edilebileceğini savunmaktadırlar (Combs & Moorehead, 1992, s.197). İkincisi, ekonomik istihbarat, bilgi elde etmek için yasal yollardan yararlandığı için ekonomik casusluktan açıkça farklıdır (İnan & Doğan, 2018). Üçüncüsü, ekonomik istihbarat arayışı, işletme veya organizasyon düzeyinde, endüstri ve devlet düzeyinde, bilgi ve bilgi alışverişi ve paylaşımı için kolektif kültürle bağlantılıdır. Ekonomik istihbaratın ürünü uygulanabilir bilgidir. Elektronik istihbarat süreci ise, bu kullanılabilir bilginin sistematik olarak edinilmesi, değerlendirilmesi ve üretilmesidir (Clerk, 1998).

1.3.7. Teknolojik istihbarat ve elektronik istihbarat

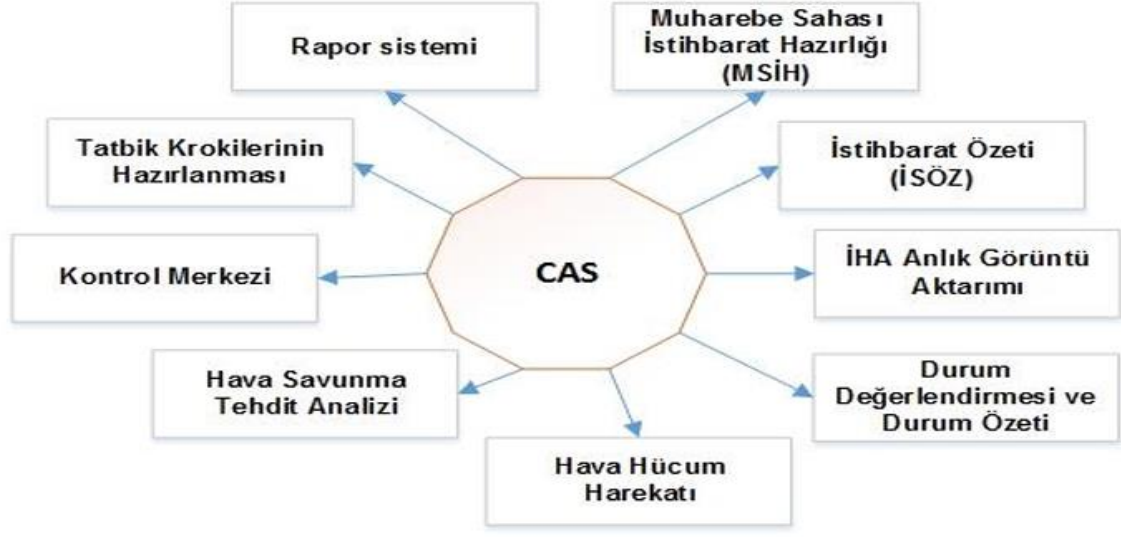
Teknolojik istihbarat, teknolojinin imkânlarının kullanılarak haber toplama sürecini ifade etmektedir. Günümüz teknolojik ilerlemeleriyle beraber, artık birçok ülke oturduğu yerden gerek uzaydaki uydular aracılığıyla gerek yollanan dronelar (insansız hava araçları) ile birçok bilgi edinebilmektedir. Ülkelerin istihbarat çalışmalarında teknolojik istihbarat da önemlidir. Çünkü karşı ülkelerin yaratabileceği tehlikeleri incelerken onların hangi teknolojilere sahip olduklarını bilmek, önceden önlem almayı sağlayacaktır.

Elektronik istihbarat ise, bilginin toplandığı ülkenin iletişim istihbaratı alanına giren yazılı ve sözlü mesajlar dışındaki elektronik sinyallerden bilgi elde etme yöntemleri olarak tanımlanmaktadır (Bernard, 2009). İstihbarat kavramı insan olmadan düşünülemez. Elektronik istihbaratta kullanılacak aletleri de kullanacak olan insandır. O yüzden ki elektronik istihbarat teknik alanda yetenekli insanlar tarafından elde edilebilecek bir istihbarat türüdür. Yani istihbarat insansız yâda elektronik aletlerin yardımı olmadan olmaz. Teknolojinin gelişimiyle beraber elektronik alanda yaşanan gelişmelere paralel olarak, artık herkesin ve her şeyin yeri kolayca tespit edilebilmekte, yeri geldiğinde tüm ortamlar dinlenebilmektedir (Avcı, 2004, s.56).

1.3.8. Coğrafya istihbaratı

Coğrafya istihbaratı, dünyadaki kıtaların ve ülkelerin coğrafi yapılarını ve aralarındaki ilişkileri inceleyerek, kıtalar, gruplar, gruplar arasında topyekûn bir savaş olasılığı durumunda yapılacak askeri harekât ilkelerini içerir (Ucuzsatar, 1986, s. 12). Savaş zamanında düşman devletlerin coğrafi yapısını bilmek ve ona göre havadan ya da karadan ilerleme kararını vermek oldukça önemlidir. Coğrafi istihbarat artık teknolojinin de gelişimiyle beraber çok yönlü analiz yeteneğine de kavuşmuştur. Coğrafya istihbaratının daha verimli hale getirilmesinde CBS (Coğrafi Bilgi Sistemleri) de kullanılmaktadır. CBS, coğrafi olarak tanımlanabilir bibliyografik ve vektörel verileri aynı ortamda bir araya getirerek, verilerin amaca göre sorgulanabilmesi ve analiz edilebilmesini sağlayan bir bilgi sistemidir (Cömert, Bilet, Olcay, Aksoy, Şenöz & Çabuk, 2016). Anlaşılacağı üzere sadece istihbarat alanında kullanılmasa da, bilgi toplama ve coğrafyanın getirdiği avantajları ve dezavantajları kullanmak açısından bu sistemler oldukça önem kazanmıştır. Askeri karar alma sürecince oldukça önemli olan coğrafi veriler, CBS yöntemiyle kolaylıkla toplanmaktadır. Bu sistemin bir alt kolu olan CAS(Coğrafi Analiz Sistemi) ise buradan aldığı sayısal verileri 3 boyutlu olarak inceler ve analizini yapar. Bu yöntemle de klasik yöntemle oranla hem gerçek zamanlı analizler yapılabilirken hem de zaman tasarrufu yapılarak sayısal analiz yeteneği daha çok artırılabilir (Göztepe & Akdağ, 2015). Aynı zamanda aşağıdaki Şekil-4’de görülebileceği üzere CAS istihbarata çok yönlü olarak yardımcı olmaktadır. Coğrafi yapının savaş durumunda nerelere saldıracağına bilinmesinde önem arz etmesinden kaynaklı bu

istihbarat alanı uluslararası ilişkilere de yön verebilecek bir tür olarak görülebilmektedir.



Şekil 4: CAS'ın Askeri Karar Vermede Kullanımı

Kaynak: (Göztepe & Akdağ, 2015)

1.3.9. Siber istihbarat (SİBİST)

Düşman olanların veya potansiyel düşmanların faaliyetlerini engelleme amacıyla siber uzayda gerçekleştirilen tüm faaliyetler, siber istihbarat olarak adlandırılır (Bayraktar, 2014). 21. yüzyılda siber teknolojiler hızla ilerlemekte olduğundan istihbarat teşkilatları yatırımlarını hızla bu alana kaydırmaktadır. Gün geçtikçe gelişen teknolojik sistemler ve internet ağları ile artan açık kaynaklara erişim kolaylığı, sadece herkesin ulaşabildiği bilgiye erişim için değil aynı zamanda bu ağlara bağlı sistemlere sızarak gizli bilgilere ulaşımı da sağlayabilmektedir. (Lewis, 2002). SİBİST ve teknolojik istihbarat birbirlerinden farklıdır. Teknolojik istihbaratın (TEKİST) iki boyutunun var olduğu unutulmamalıdır. Birincisi, potansiyel düşman olarak görülen devletlerin ellerindeki ateşli silah gücü ve bunların teknolojisi anlamındaki istihbarat; ikincisi ise olası ortaya çıkabilecek olan silah potansiyeli ve yeni teknolojilerin savaş stratejilerine etkilerinin analiz edilmesidir (Kemiksiz, 2022). Siber istihbarat ise siber uzayda olan faaliyetlerin takibi olarak ele alınıp, yeni teknoloji olarak düşünülürse teknolojik istihbaratın içinde incelenebilecekken, sahip olduğu çok büyük potansiyeli olduğundan TEKİST'den farklı olarak incelenmektedir.

Siber istihbarat yöntemlerine bakıldığında üç ayrı yöntem görülebilmektedir.

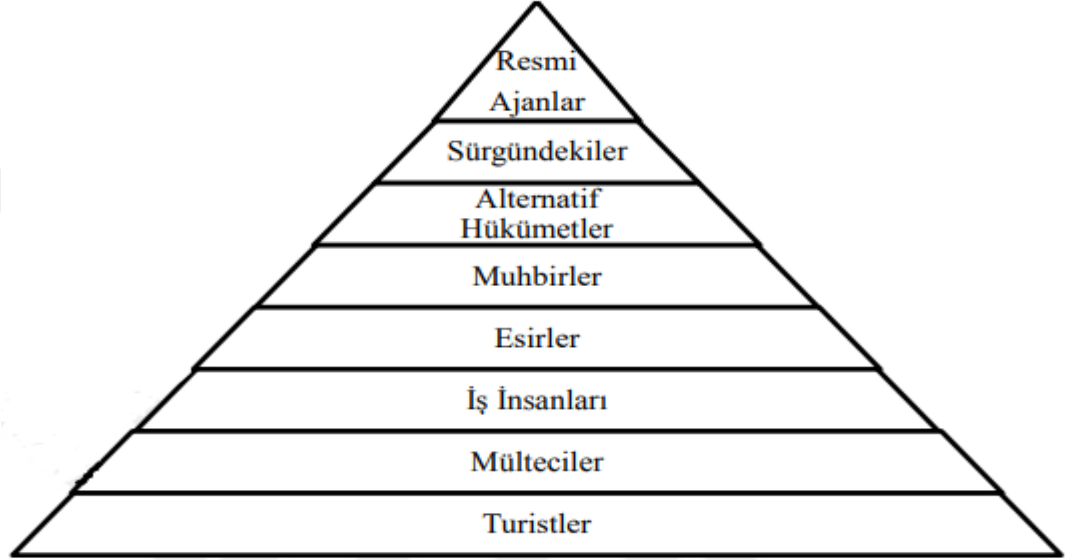
Bunlar siber elektronik istihbarat, siber açık kaynak istihbaratı ve sosyal ağlara dayalı istihbarattır (Bayraktar, 2014). Devletler, resmi ve özel kurum ve kuruluşlar kendi içlerinde oluşturdukları internet ağlarıyla iç sistemler ve çalışanları arasında bilgi paylaşımı yapmaktadırlar. Bu ağlara burada çalışanların dışında kötü niyetli kişilerin ulaşım gizli bilgileri ele geçirebilme olasılıklarıyla siber elektronik istihbarat ilgilenebilmektedir (Ersanel, 2001, s. 23). Sadece buradaki bilgileri elde etmekle kalmaz aynı zamanda bu ağlara sızılarak çeşitli virüs ve yazılım programları da yerleştirebilirler (Egmannt & Sperber, 1996, s.23). Ortam dinlemeleri yani cep telefonu, bilgisayar gibi elektronik aygıtları kullanarak yapılan elektromanyetik dinlemeler, e-posta kanallarıyla yayılan virüsler de bu konu başlığı altındadır (Bayraktar, 2014). Siber açık kaynak istihbaratı ise hem medyanın kolay ve zahmetsiz olarak açık kaynak istihbaratı olarak kullanılmasından (Mazzafaro, 2011), hem de istihbarat teşkilatının bazen medyayı kullanıp kaynak bulmasından dolayı medya ve istihbarat teşkilatları arasındaki karşılıklı etkileşim olarak özetlenebilir. Sosyal ağlara dayalı istihbarat ise Facebook, Twitter gibi oldukça yüksek üye sayısına sahip alanları kullanarak elde edilen istihbarat olarak gösterilebilir ki buna örnek olarak Arap Baharındaki halkın ayaklanmasında bu alanları kullanarak birbirlerine yolladıkları haberler gösterilebilir (Babacan, Haşlak & Hira, 2011).

Siber istihbarat aslında öncelikli olarak siber terörü engellemeye dayanır. İleriki bölümlerde daha detaylı incelenecek olan, siber saldırıların zarar verme amacını güden boyutunda olan siber terör klasik terör anlayışından çok kadar farklı ve tehlikeli olabilir. Klasik terör anlayışına bakıldığında daha dar kapsamlarda, ilgili bilgiler edinilebilirse daha engellenebilir ve görünebilen silahlarla tehdit algılanırken; siber terörizm de yapanları bulmak da nerden nasıl saldırılacağıının anlaşılması da çok mümkün olmadığı gibi etki alanı da oldukça geniş olabildiğinden çok daha tehlikelidir. O yüzden ki son yıllarda siber istihbarat faaliyetlerine daha çok eğilim gösterilmeye başlanmıştır (Bayraktar, 2015) .

1.3.10. İnsan istihbaratı (İNİST)

İnsan istihbaratı, ana kaynağı “insan” olan istihbarat çeşididir (Manual, 2006). İnsanlığın başlangıcından beri, insanların diğer insanların hayatlarını ve kendileri haklarındaki düşüncelerini bilme arzusu, bu bilgileri konuşarak öğrenemediklerinde bilgi

sızdırma yâda çalmaya yönlendirmiştir (Hitz, 2010, s. 2). En genel anlamda insan istihbaratı, bir istihbarat sorununun analizinde veya operasyonel bir faaliyete destek olarak kullanılmak üzere bir insan kaynağı tarafından sağlanan istihbarat bilgisini ifade eder. Uluslararası jargonda HUMINT (İNİST) olarak bilinen insan istihbaratı, aynı zamanda bilginin bir bireyden diğerine doğrudan ya da dolaylı olarak aktarıldığı belirli bir toplama faaliyetini de yansıtmaktadır (Costanza, 2014, s. 1). İnsan istihbaratının ana kaynaklarından biri olan ajanlar, kendilerinden sorumlu ve kadrolu çalışan personele bağlı çalıştığından muhbirlerden ayrılmaktadır (Şenel & Şenel, 2018, s.97-98). Sadece ajanlar değil aynı zamanda mutemetler (hedefteki kişi ya da kurum hakkında bilgi getiren güvenilir kişiler), muhbirler, itirafçılar ve gizli soruşturmacılar da insan istihbaratının önemli kaynaklarıdır (Kavsıracı, 2020).



Şekil 5: İnsan İstihbaratında Kaynakların Duyarlılık Sıralaması

Kaynak: (Herman, 1999, s.63) çevrilmiştir.

Şekil-5’den de görülebileceği üzere, insan istihbaratından kullanılacak insan sayısı birçok meslekten oldukları için oldukça fazladır. Turistlerden, iş insanlarına hatta sürgündeki kişilere kadar pek çok kişi istihbarat için kaynak oluşturabilir. Her ne kadar tüm bu meslek grupları birer kaynak olarak görünseler de, burada en güvenilir ve en net istihbarat kaynağı tabi ki resmi ajanlardır.

Teknolojinin bu kadar geliştiği zamanlarda, insan istihbaratının etkililiği

sorgulanmaya da başlasa; özellikle terör amaçlı olan örgütlerin, yakalanmamak amaçlı teknolojiden uzaklaştıkları bilindiğinden İNİST'in değeri daha çok anlaşılmaktadır (Fink, Pagliery & Segall, 2015)

1.4. İstihbarat İlkeleri

Güvenilir ve başarılı istihbaratın elde edilmesi ülkeler için oldukça önem taşımaktadır. Çünkü gerek iç gerek dış güvenliği sağlayabilmek için oluşabilecek tehditleri önceden öngörebilmek bir milletin devamlılığını sürdürebilmesi için gerekli bir önlemdir. İstihbarat kısaca elde edilen bilgiler olarak düşünüldüğünde, bu bilgilerin elde edilme yöntemlerinin dışında sahip olması gereken bazı özellikler olduğu sonucu da ortaya çıkar. Bunlar: sürat, kesinlik, doğruluk, amaca uygunluk, esneklik ve objektiflik ilkesidir.

İstihbaratın başarılı olabilmesi için önemli bir ilke olan sürat ilkesi, bilginin zamanında ve hızlı biçimde politika yapıcılara ulaştırılması olarak özetlenebilir (Kent, 1965) . Geç gelen bilgi ya da belgeler, alınabilecek önlemleri engeller. Ancak, doğru ve zamanında istihbarat toplayabilmek de zordur. Bunun için gelen istihbaratları analiz eden kişiler önem kazanmaktadır. İstihbarat analizcilerinin bazı olayları ellerindeki istihbaratları değerlendirerek öngörebilme yeteneğine sahip olmalıdırlar. Sonuç olarak baktığımızda, birçok meydana gelen olay istihbaratın elde edilememesinden kaynaklı değil, gerçek istihbaratın ilgili kişiye tam zamanında aktarılmamasından kaynaklanmaktadır (Heart & Gooden, 1995, s.65).

İstihbaratın hızlı bir şekilde elde edilmesi önemli olduğu kadar kesin olması da önemlidir. Elde edilen istihbaratın sonunda yapılan değerlendirmelerin yüzde yüz doğru olacağı beklenmemeli ve kesin istihbaratla birlikte olasılık ayrımları yapılabilmelidir. En muhtemel olan sonuçlardan başlanarak gittikçe azalan gerçekleşme ihtimallerine göre yorumlar yapılmalı ve politika yapıcıların bunlara göre karar verebilmesi sağlanmalıdır (Özdağ, 2014, s.36). Buradan da anlaşılacağı üzere kesinlik ifadesi hedefi on ikiden vuramasa da doğru analize en yakın olabilme durumudur.

Hızlı ve kesin istihbarattan sonraki ilke ise doğruluk ilkesidir. Bir bilgi kaynaktan doğru elde edilemezse ne kadar süratli ya da kesin gelirse gelsin yanlış karar alınmasına sebep olacağından yarardan çok zarar olmasına neden olabilir (Özdağ, 2014, s.36).

Doğruluk ilkesi ve kesinlik ilkesi tanımlarından çıkarılacak temel fark ise, kesinlik ilkesi olasılık hesaplarını yaparken, doğruluk ilkesinde asıl önemli olan şey bilgiyi ana kaynağından doğru olarak elde edip uygun şekilde analiz ederek gerçek istihbarata ulaşabilmektir. Unutulmamalıdır ki yanlış elde edilen istihbarat, istihbarat edinmemekten daha kötü sonuçlar doğurabileceği gibi, devletlerin uluslararası politikalarını da kötü bir biçimde etkileyebilir (Kavsıracı, 2020).

Bilgi toplamak için ihtiyaç duyulan kaynaklar, diğer tüm kaynaklar gibi sınırlıdır. Bu yüzden ki kaynakları israf etmeden ve maksadına uygun bir biçimde kullanmak önemlidir (Özdağ, 2014, s.37). Örneğin bir istihbarat eğer ki dış politikada kullanılacaksa bunun için iç araştırma yaparak zaman kaybedilmemeli, ilgili alanlar belirlenerek gereksiz harcamalardan kaçınarak en hızlı yoldan kesin ve doğru istihbarat edinerek ilgili kişilere iletilmelidir.

Ülkelerin hem iç hem dış güvenliğini sağlamak amacıyla yaptıkları istihbarat faaliyetleri gittikçe önem kazanmış ve sadece bilgi toplamaktan öteye geçip bilimin ve aklın bir arada görüldüğü bir sanat haline gelmiştir (Kavsıracı & Demirbaş, 2020, s.49). Bilgi doğası gereği sürekli değişip gelişebildiği için toplanan istihbaratın da bu koşullara uygun olabilmesi gerekir. Bu da istihbaratın analizini yapan kişinin yenilenen veriler ışığında yaptığı analizi esnetebilmesi anlamına gelmelidir. İstihbarat operasyonları akla ve yargıya dayanır. Prosedürler beklenmedik gereksinimleri karşılamak için esnek olmalıdır. Belirli bir durumun gereklerini karşılayacak şekilde değiştirilemeyen prosedürler genellikle başarısızlığa yol açar (US Army Chemical School , 2022).

İnsan dışında kullanılacak birçok istihbarat kaynağı olmasına rağmen, sonuçta bu verileri yorumlayabilecek ve gerekli çıkarımları yapabilecek bir analiste ihtiyaç vardır. İstihbarat sorumluları her ne kadar verileri bilgisayar ortamlarında analiz edebilse de, yapacağı yorumlar tamamen kendi düşünceleri olacağından objektif olarak olaylara bakabilme kabiliyeti oldukça önemlidir. Karar vericilere gönderilecek bilgilerin objektif olması ve geniş bir perspektiften yorumlanabilmesi alınacak kararların doğruluğunda büyük önem taşımaktadır (Beets, 2003, s. 57-62).

1.5. İstihbarata Karşı Koyma (İKK)

İstihbarata karşı koyma (İKK) önemli bir kaynaktır. Çünkü toplanan istihbaratın

önemi kadar, hakkınızda toplanacak istihbarata da engel olmak önemlidir. Çok büyük miktarlarda ve en gerekli istihbaratları toplasanız bile, etkili karşı istihbarat olmadan hiçbiri tam olarak güvenli sayılmaz. “Karşı İstihbarat” olarak da bilinen İKK, casusluk ve diğer istihbarat faaliyetleri, sabotaj ve yabancı kişiler tarafından veya bunların adına gerçekleştirilen suikastlara veya uluslararası terör faaliyetlerine karşı korunmak için toplanan bilgiler ve yürütülen faaliyetler anlamına gelir (Cornell Law School, 2022). Bu tanımdan anlaşılacağı üzere İKK’da amaç kendi güvenlik bütünlüğünü sağlayarak karşı tarafın bilgi toplamasını engellemekken, istihbaratın amacı ise karşı tarafın güvenlik açıklarını bularak onlar hakkında bilgi toplamaktır. Anlaşılacağı üzere istihbarat ve İKK faaliyetleri birbirleriyle oldukça iç içe geçmiş faaliyetlerdir.

Başarılı olduğunda karşı istihbarat, ulusların güvenliğine yönelik tehditlere karşı hem bir kalkan (hükümetimizin girişimlerine karşı koruma ve güvenlik ve diğer savunma önlemlerini bilgilendirme) hem de bir kılıç (yabancı algıları şekillendirmek ve yabancı istihbarat yeteneklerini aşağılamak için saldırgan İKK operasyonları yürütmek) olarak hizmet eder ve doğrudan ulusal güvenliğe katkıda bulunur (Cleave, 2007, s. 3). Güvenlik denildiğinde bir milletin dış politikasını ve uluslararası ilişkilerini düzenleyeceği diplomasi trafiğinin belirlenmesi ile tüm sınırlarının (askeri ve sivil) muhafaza edilebilme kabiliyeti anlaşılabilir (Yılmaz S., 2006, s.239-246). Buradan da anlaşılacağı üzere, ülkenin iç ve dış güvenliğini sağlamak için istihbarat önemli bir yere sahip olduğu gibi İKK faaliyetleri de en az onun kadar önemlidir. Hatta bunu bir ileri safhada düşündüğümüzde ulusal güvenlik için İKK faaliyetlerinin olmazsa olmaz bir faktör olduğu görülmektedir (Özdağ, 2014, s.143).

İKK faaliyetlerini teori açısından incelediğimizde dört ana temele dayandırıldığını görebiliriz. Bunlar: caydırıcılık, tespit, aldatmaca ve etkisiz hale getirmektir (Pruncun, 2019, s.42).

Karşı istihbaratı iki genel kategoride düzenleyebilmek mümkündür. Bunlar savunmacı ve saldırgan karşı istihbarattır. Savunmacı karşı istihbarat erişim engelleme ve rakipler hakkında bilgi üretme hedefindeyken, saldırgan istihbarat ise manipülasyon yöntemiyle karşı tarafı böl-parçala-yok et sistemiyle engellemeye çalışmayı amaçlamaktadır (Duvange & Solms, 2014). Savunmacı karşı istihbaratın temelde iki

hedefi vardır. Bunlar caydırıcılık ve önceden tespit edebilmektir. Caydırıcılık, bir ülkenin diğer bir ülkenin gücünü, bir bilgi toplama operasyonu oluşturma maliyetlerinin veya risklerinin bir anlamda faydalardan daha ağır bastığına ikna etme yeteneğidir. Aynı zamanda bu bir misilleme biçimi olarak yorumlanabilir. Tespit etmede ise beş temel başlık sayılabilir. Bunlar: olayı tanımlamak, içindeki kişileri tespit etmek, ilgili kişilerin örgütsel hareketlerini incelemek, ilgili kişilerin yerini tespit etmek ve istihbaratı toplamaktır (Prunckun, 2019, s.47). Saldırgan karşı istihbarat ise iki ana amaçla yapılır. Bunlar; aldatmak ve etkisiz hale getirmek olarak sıralanabilir. Ana faaliyet alanı düşman ajan faaliyetlerini önlemek amaçlı karşı ajanları kendi aralarına katmak ya da onların yanlış bilgi edinip evlerine dönmelerini sağlamak olmalıdır (York, 2014). Bu yüzden istihbarat örgütlerinde çalışan kişilerin kayıtları temiz olmasına rağmen, karşı istihbarat örgütlerine geçmeleri mümkün olabildiği gibi, kendi örgütlerinin bunları fark etmemesi de oldukça olası bir durumdur. Bu yüzden de karşı istihbaratçılar için hiçbir şey ortada yokken bile kendi örgütlerine sızıldığını düşünen “profesyonel paranoyaklar” diyebiliriz (Özdağ, 2014, s.145). Sadece aldatma ya da aldatılmanın dışında alınan istihbaratın da etkisiz hale getirilmede kullanılması da amaçlardan biridir.

CIA direktörlerinden James M. Olson’ın yazdığı bir makalede de belirttiği üzere karşı istihbaratın bazı ilkeleri vardır ve bu ilkeler on ana başlıkta sayılmıştır. Olson’a göre karşı istihbarat alanında gelişmek, gerek Amerika gerek diğer ülkeler için çok önemli olmakla beraber bazı kişilerin onun bu fikrine karşı çıkılabileceğini de belirtmiştir (Olson, 2001). Olson’ın bahsettiği bu ilkeler ise; saldırgan ol, karşı istihbaratçıya saygı göster, sokaklara hakim ol, tarihini bil, analizi iyi yapmanın önemini anla, sadece kendi servislerle değil diğer istihbarat servisleriyle de çalışmaya açık ol, eğitimin önemini unutmadan sürekli eğitimini geliştirme halinde ol, diğer istihbaratçıların yapabilecekleri oyunlara hazır olup köşeye itilme, paranoya olma durumuna karşı çok uzun süre karşı istihbarat çalışmalarında kalma ve son olarak da yaptığın işten asla pes edip vazgeçme eğer vazgeçeceksen de başlama olarak sıralanabilmektedir (Olson,2001).

BÖLÜM 2: DÖNEMSEL OLARAK İSTİHBARATIN GELİŞİMİ VE İSTİHBARAT TARİHİ

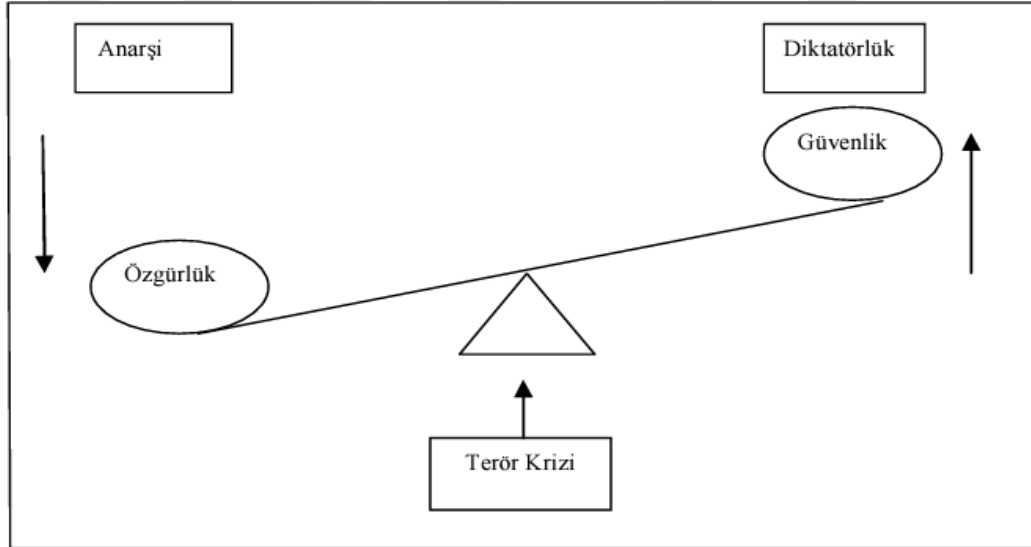
2.1. İstihbarat Tarihi

İnsanlık tarihi kadar eski olan “devlet” kavramının, egemenlik kavramıyla direkt ilişkili olup (Ay & Uçar, 2015), temel amacı sürdürülebilirlik ve topluluk bütünlüğü olmuştur. İnsan, egemenlik ve ülke tanımlarının hepsinin bir arada incelendiği devlet kavramında, bilgi almak ve o bilgileri doğru zaman ve yerde kullanabilmek devletlerin uzun ömürlü olabilmesi açısından önemli olduğu aşikârdır. Bunun içindir ki istihbarat tarihsel anlamda oldukça önemli bir yerde olmuştur. Yani insan, en eskiden beri bilginin ve istihbarat toplamanın önemini algılamış olduğundan devletlerin kuruluşunda ve devamında zarar görmemek adına istihbarat faaliyetlerine önem vermiştir.

Devlet kavramı zaman içerisinde değişik güçlere dayansa da, modern devlet yapılaşmasıyla beraber kapitalizmin de etkisiyle işleyiş yapısı da değişmiştir. Modern devleti kısaca ulus devlet olarak tanımlayabiliriz (Zabunoğlu, 2018). Modern çağın ve uluslararası ilişkilerinde başlangıcı olarak kabul edilebilecek olan Vestfalya Antlaşması (Özel Özcan, 2019) modern devlet tanımının değişiminde önemli bir rol oynamıştır. 30 yıl savaşların ardından 1648 yılında imzalanan Vestfalya Barış Antlaşmasına göre uluslararası sistemin egemen devletlerin kontrolünde olacağı ve devletlerin üstüne geçmeye çalışan kişi ve kuruluşların geçerliliğini yitireceği savunulmuş ve 1945 yılına kadar da bu düşünce geçerliliğini Avrupa’da korumuştur (Kiraz, 2012). Aslında buradan da anlaşılacağı üzere bu antlaşmayla güç sistemi kurulmaya başlanmıştır. 1618-1648 yılları arasında Katolikler ve Protestanların arasındaki din temelli 30 yıl süren savaşlardan sonra imzalanan bu antlaşmayla genel anlamda uluslararası sistemin kuralları belirlenmiş ve devletler birbirlerinin toprak bütünlüklerine saygı duymanın yanı sıra egemenliklerine karışmamaya ve birbirlerinin iç işlerine karışmamaya karar vermişlerdir (Pevehouse & Goldstein, 2017, s.56-63). 1945’ten sonra yani Soğuk Savaşla beraber (1946-1991 yılları) dünya iki süper gücün yani Amerika Birleşik Devletlerinin (ABD) ve Sovyet Sosyalist Cumhuriyetler Birliği’nin (SSCB) çatışmasına tanık olmuştur. Birbirleriyle olacak olan olası sıcak çatışmada kullanılacak nükleer güçlerden çekinildiği için gerçek savaşa girilmeyen bu dönem 1991 yılında SSCB’nin dağılmasıyla sona ermiş ve ABD tek süper

güç olarak kalmıştır (Sönmezoğlu, 2011, s. 28-30). O zamandan sonra ABD'nin mutlak üstünlüğü görülürken, özellikle 2001 yılından sonra ABD'de olan 11 Eylül saldırılarıyla ABD'nin dış politikasının değişmesi ve askeri güce yönelmesiyle kurmaya çalıştığı yenedünya dengesinin kendi aleyhinde bozulmasına başlamasına neden olmuştur (Aydın & Bakıncak, 2016).

2001 yılında ABD'de meydana gelen ikiz kuleler saldırısının istihbarat hatası olduğu gerçeğinden yola çıkan ABD ve Avrupa yeni istihbarat birimleri kurmuş, yetkilerini arttırmışlar hatta daha da ileri giderek özgürlük ve güvenlik dengesinin dahi bozulmasına sebebiyet vermişlerdir (Haubrich, 2003). Şekil-6'dan da görülebileceği üzere terör krizinin yarattığı korkuyla güvenliğe önem veren ABD dâhil bazı ülkeler, bu güvenliği arttırmak istediklerinde diktatörlüğe daha çok yaklaşmaktadırlar. 11 Eylül saldırılarından sonra da ABD'nin bu dengeyi sağlayamadığı görülmüştür (Golden, 2006, s. 401). Bu yüzden ki, literatür araştırmasında bozulan liberal dünya düzeni ile ilgili pek çok araştırma bulunmaktadır.



Şekil 6: Özgürlük ve Güvenlik Arasındaki Sağsızsız Denge

Kaynak: (Golden, 2006) çevrilmiştir.

Genel olarak bakıldığında da anlaşıldığı üzere, insanlar tarafından oluşturulan devlet düzeni, gene insanların devamlılığını istemesinden kaynaklı egemenlik sorunlarıyla karşılaşmış; bu sırada güçler ve özgürlükler arasında denge kurmaya çalışırken ülke ve toprak bütünlüğünü sağlamak içinde gittikçe gelişen dünyada birbirleri hakkında daha çok

bilgiye sahip olmak istemişlerdir. İstihbarat tanımlarından birinin “yeni bilgi toplamak” olduğu gerçeğine dayanarak, bu bilginin önemi özellikle I. Dünya Savaşı ve sonrasında gelişen teknoloji ve küreselleşen dünyada daha çok hissedilmeye başlandığı söylenebilir.

1914 yılındaki Birinci Dünya Savaşı'na kadar olan süreçte istihbaratın ana kaynağının sadece fiziksel istihbarat olduğu söylenebilecekken, özellikle savaş sırasında kullanılan telsizlerle beraber sözlü istihbaratın da önemi ortaya çıkmaya başlamıştır (Berkkan, 2017, s. 3). İngiltere'den sonra istihbarat servisini kurumsallaştıran diğer devlet İsviçre olmuş ve NDB (Nachrichtendienst des Bundes) adlı istihbarat servisini kurulmuştur. Ancak gerçek anlamda istihbarat örgütlerinin faaliyetlerinin Soğuk Savaş döneminde ve sonrasında daha kurumsallaşmaya başladığı görülmekte ve bununla beraber 1909'da İngiltere faaliyete başlayan MI6 teşkilatından sonra ilk kurulan kurumsal istihbarat teşkilatının ise ABD'de 1947 yılında kurulan CIA (Central Intelligence Agency) olduğu bilinmektedir (Tatlı, 2022). Daha sonra sırasıyla 1946'da GIP (Suudi Arabistan), 1946'da BIN (Endonezya), 1952'de PSIA(Japonya), 1956'da BND (Almanya), 1961'de NIS (Güney Kore),1977'de eski adıyla Servizio Per Le Informazioni E La Sicurezza Militare (SISMI) olan AISE (İtalya), 1983'te MSS (Çin), 1982'de DGSE (Fransa), 1984'de CSIS (Kanada), 1984'de MOIS (İran), 1989'da CISEN (Meksika), 1995' de FSB (Rusya), istihbarat örgütleri kurulmuştur.

Özellikle II. Dünya Savaşından sonra tüm ülkeler gelişen teknolojinin de sebep olduğu bir değişikliğe gitmek zorunda kalmıştır. Hem istihbarat örgüt yapılarını hem de bu iş için kullandıkları kaynakları modernleştirmişlerdir. Aynı zamanda istihbaratın toplanmasında devletin hedeflerinin ve olabilecek tehditlerin iyi belirlenmesinin, zaman, para ve emek kaybının önlenmesi açısından ne kadar önemli olduğu da ortaya çıkmıştır (Sel, 1985, s. 181). Bu açıdan bakıldığında II. Dünya Savaşının hemen öncesinde istihbarat yapılarının dünya genelinde kurumsallaşmaya başladığını ve bilimsel bir alan olarak görülmeye başlandığı görülmektedir (Özdağ, 2014, s.49).

Sadece I ve II. Dünya Savaşlarında değil daha sonraları ortaya çıkmış olan Soğuk Savaş'tan sonra da istihbarat faaliyetleri değişmektedir. Dünya tarihindeki istihbaratın dönemsal anlamda nasıl değiştiğini üç ana tarih aralığında inceleyebilmek mümkündür. Bunlar; 1914-1938 yılları arası, 1939-1946 yılları arası ve 1947 ve sonrası olarak aşağıda

detaylı bir biçimde anlatılmaya çalışılacaktır.

2.1.2. Dönemsel olarak değişen istihbarat toplama yöntemleri ve önemli olaylar

2.1.2.1 1914-1938 yılları arası istihbarat gelişmeleri

Tarihsel olarak incelendiğinde, 1914 yılına kadar yani Birinci Dünya Savaşı başlayana kadarki süreçte bilgi toplama sürecinin büyük bir bölümü fiziksel istihbarat aracılığıyla sağlanmıştır. Ancak 1914'te patlak veren I. Dünya Savaşı sırasında telsiz radyoların ve siper telsizlerinin ortaya çıkışıyla beraber savaşın durumu hakkında bilgi almak isteyen komutanlarla ve karargâh arası iletişime ulaşmak önemli olmaya başlamıştır. İnsan istihbaratının tek kaynak olduğu dönem geride kalmaya başlamış ve artık teknolojik altyapının gerekli olduğu dönem baş göstermeye başlamıştır. Bu yüzden ki, sinyal istihbaratı(SİNİST) oldukça önemli olmuş ve bilgi toplama alanı artık elektronik istihbarat(ELİST) alanına kaymaya başlamıştır (Kahn, 2002). Telsiz radyolarından alınan bilgilerle birlikte savaşın seyri, envanter durumları, yaralı asker ve ölümlerin sayısı gibi kritik durumlar öğrenilmiş ve böylelikle sözel istihbaratın da üretimine katkı sağlanmıştır. Bu yıllarda gelişmeye başlayan SİNİST faaliyetleri ile birlikte birçok dinleme istasyonları kurularak, istihbaratın elde edilme sürecinde farklı bir alan yaratılmıştır. Aynı zamanda savaş boyunca görüntü istihbaratında da önemli gelişmeler yaşanmış olup, uçakların bu alanda ne kadar önemli oldukları öne çıkmıştır. 20. yy'ın başlarında görüntüleme faaliyetlerinde uçakların kullanılmasıyla birlikte istihbarat alanında üç farklı fotoğraf türü kullanılmış olup; dikey fotoğraflar hedeflerin hemen üzerinden çekildiğinden uzman bilgisine ihtiyaç duyarken, yatay fotoğraflar hedefin karşından ya da farklı cephesinden çekildiğinden uzman bilgisi gerektirmemiş olup son olarak kullanılan üç boyutlu fotoğraflar ise hedeflerin üst üste bindirilerek çekilmesinden kaynaklı daha fazla bilgi vermekteydiler (Richelson, 1995, s.32).

İkinci Dünya Savaşının hemen öncesinde kurumsal bir kimlik kazanan istihbarat olgusu (Özdağ, 2018, s.49), Birinci Dünya Savaşı ile beraber istihbarat olmadan ordularının bir işe yaramayacağını gören ülkeler açısından daha büyük bir önem kazanmıştır (Herman, 1999, s.25).

Sürekli değişim geçiren istihbaratın hayatın içinde ve her an neredeyse her yerdeki

bilgilere anında ulaşabilmesiyle sadece askeri kanatta değil artık sivil kanatta da kullanılabilmesine olanak sağlamıştır. Bunun için de sadece bilgi teknolojileri yardımıyla değil aynı zamanda, eski yöntemlerden(posta güvercinleri, kuryeler, eğitilmiş köpekler) bu dönemde de çok vazgeçilememiş ve bu alanlarda bazı değişik taktikler geliştirilmiştir (Bozkurt, 2014). Bunlardan biri gazeteler aracılığıyla casusluktur. Gazetelerin yazılarının arasına belirli şifreler yerleştirilmiş ve bunlarla birbirlerine haber yollamaya çalışmışlardır. Bu istihbarat türüne Türklerin ilk aşına oluşu ise İstanbul Sansür Müfettişliği 'ne gelen ve ayrıntılı bir biçimde bunu anlatan bilgilendirme yazısıyla olmuştur. Almanların kullandığı casusluk yöntemlerinin bir tanesi ise daha enteresan gözükabilir. Çünkü Almanlar, Fransız gizli servisini kandırmak için müzik notalarına başvurmuşlar, her notayı bir harfe denk gelecek ve her hafta değiştirilecek şekilde ayarlamışlar, ancak Fransızların bunu fark etmesiyle bu yöntemleri kullanılmaz duruma gelmiştir (Avşar, 2018). Almanların diğer bir kullandığı casusluk yöntemi ise köpeklerdi. Aynı zamanda bu yöntemi Fransızlar da kullanmış ve savaş hattının bir ucundan diğerine haber taşımaya eğitilmiş köpeklerle yapmışlardır (Arıklı & Yavuz, 1974, s.94-95). Fransızların denediği bir başka değişik yöntem de hediye paketlerindeki yiyecekler aracılığıyla haber yollamak olmuştur. Aynı zamanda, Kravatlardan şemsiyelere, sigara kâğıtlarından şişelere kadar neredeyse her şey bu dönemde casusluk faaliyetlerinde kullanılmıştır (Avşar, 2018).

Geleneksel istihbarat ve sinyal istihbaratından yararlanan bu dönemde aynı zamanda yeni sayılabilecek bazı teknik yöntemler de kullanılmıştır. Örneğin, kriptologlar yani diğer bir deyişle şifre kırıcılar kendi ülkelerinde önemli bir hale gelmiş, karşı devletin haberleşme ağını kırmak için kripto büroları kurulmuştur. Bu büroları ilk kuranlar ise Fransa, Avusturya-Macaristan ve Rusya olmuştur (Richelson, 1995, s.15). Kripto olayında en önemli olay ABD'nin savaşa girmesini sağlayan "Zimmerman Telgrafi"dır (Dünya Casusluk Tarihi Ansiklopedisi, 1974, s. 107). Dönemin Alman Başbakanı olan Zimmermann, Washington'daki Alman Büyükelçisine şifreli olarak gönderdiği mesajda Amerika'ya karşı Japonya-Meksika ve Almanya ittifakını kurmaya çalıştıklarını ve Meksika'ya bununun karşılığında birkaç Amerikan eyaletini vereceklerinden bahsetmiş ancak İngilizlerin bu telgrafi ele geçirip deşifre etmesiyle beraber dönemin doktrini olan Monroe Doktrinine göre Amerika'nın artık I. Dünya savaşında tarafsız kalmasının imkânı

kalmamış ve savaşa girmiştir (Armaoğlu, 2005, s. 133). Monroe Doktrinine göre Avrupalı devletler ABD'ye karışamayacak aynı zamanda toprak bütünlüğüne saygı duyacaklardır (Arı, 2013, s. 224-225). Almanya çektiği bu telgrafta Meksika bölgesine müdahalede bulunduğu için artık ABD için bu savaşa katılmamak imkânsız hale gelmiştir. Bu durum savaşın seyrini değiştiren en önemli istihbarat olaylarından biri olarak görülmektedir.

Bu dönemde kullanılan yöntemlere bakıldığında, her ne kadar teknolojinin bu dönemde insan istihbaratının önüne geçtiği düşünülse de, aslında hala insan istihbaratına dayalı bir sistemin işlediği rahatlıkla görülebilmektedir.

2.1.2.2. 1939- 1946 yılları arası istihbarat gelişmeleri

Birinci Dünya Savaşında çözülemeyen nedenlerden ötürü meydana gelen ve 1939 yılında başlayan İkinci Dünya Savaşı'nda şifreleme yöntemleri ile teknolojik istihbaratta çığır açılmıştır. Sinyal istihbaratının ne kadar önemli olduğunu anlayan ABD kablolu haberleşme ağına müdahale edebilmek ve çözümleyebilmek için 1929 yılında SIS'i (Sinyal İstihbarat Teşkilatı) kurmuştur (Richelson, 1995, s.81). Sinyal istihbaratına bu kadar önem verirken insan istihbaratının ve uzmanlarla çalışmanın önemli olduğunun da unutulmaması gerekir. Bunun en acı örneklerinden biri Pearl Harbour saldırısıdır. 1942 yılında Japonya'nın saldırısını diplomatik ilişkilerdeki şifrelerle çözebilecek konumda olan ABD bunu başaramamış, istihbarat paylaşımlarının azlığı ve kurumlar arasındaki rekabetten kaynaklı bu saldırıyı öngörememiştir (Friedman U. , 2012). İstihbaratı değiştiren olaylardan gösterilen bu saldırı son bölümde detaylandırılacaktır.

İkinci Dünya Savaşı'nda İstihbarat Gözetleme ve Keşif (İGK) alanında da oldukça ciddi gelişmeler olmuştur. Değişen teknoloji ile birlikte daha yüksekte ve daha kaliteli çekilen fotoğraflar sayesinde düşman birlikleri hakkında daha kayda değer bilgiler elde edilmesi sağlanırken aktif olarak kullanılmaya başlayan keşif uçaklarıyla beraber, olası bir harekât düzenlenebilecek bölgelerde hasar tespiti tahmininde bulunmak kolaylaşmıştır (Richelson, 1995, s.157-160).

Kriptologların önemi bu dönemde de devam etmiştir. Bunun bir örneği Almanların mesajlarını şifrelemek amacıyla kullandıkları "Enigma" Sistemidir. Almanların İkinci Dünya Savaşı boyunca en yaygın olarak bu şifreleme cihazını kullandıkları bilinirken, bu cihazın şifrelerini uzun uğraşlar sonucunda ilk olarak Polonyalıların kırdığı da

bilinmektedir (Kara O. , 2009). Bundan sonra bu teknolojiyi ele geçiren İngilizler, Enigma'yı takip etmeyi sağlayan "Ultra" sistemini ortaya çıkarmışlar ve Almanya'nın saldırı planlarını önceden bilerek İngiltere'yi işgal etmek isteyen Hitlerin planlarını ortaya çıkarmışlardır (Mc.Lendon, 2002, s. 193).

İkinci Dünya Savaşı'ndaki istihbarat faaliyetlerinden bahsederken hakkında filmler bile çekilmiş olan ve Türkiye'nin Başkenti Ankara'da yaşanan casusluk olayı olan "Çiçero Vakası" nı da açıklamak gerekmektedir. Bu dönemde her ne kadar teknolojik altyapının çok gelişmeye başladığı görülse de insan istihbaratı bu savaşta da oldukça önemli olarak görülmüştür. Bunun en iyi kanıtı da Elyasa Bazna yani diğer bir adıyla "Çiçero" dur. 1918 yılında İstanbul'a gelen ve birçok iş değiştirdikten sonra İngiliz Büyükelçiliği'nde büyükelçinin özel hizmetinde işe başlayan Elyasa Bazna, Almanlarla, İngilizlerden sızdıracağı önemli evraklar karşısında para almak konusunda anlaşma yapmıştır (İlter, 2002, s. 51). 1943 yılında altı ay boyunca İngiliz büyükelçinin özel evraklarına ulaşabilen Elyasa, bu belgelerin fotoğraflarını çekip Almanlara yüksek meblağlara (15.000-20.000 sterlin arası) satmış, Almanlar da bu savaşta stratejik olarak nerelere yayılması gerektiğini ve İngilizlerin asıl planının ne olduğunu öğrenmeye çalışmışlardır (Moyzsich, 2004, s. 131-141). Çiçero'nun getirdiği belgelerin doğruluğuna inanmak isteyen ama test etmeleri gerektiğine inanan Almanlar, bu uğurda Sofya'nın bombalanacağını bilmelerine rağmen susmuşlar ve 4 binden fazla insanın ölmesine göz yummuşlardır (Moyzsich, 2004, s. 143). Çiçero'yu ele veren ise Almanların tarafından Amerika tarafına geçen gerçek adı Cornelia Kapp olan ama Elizabeth olarak kaynaklarda bahsedilen kadındır (Kerasuady, 2011, s. 75). Kapp'ın babası Alman diplomatı ve Ankara'da Alman büyükelçisinin sekreterliğini yapmaktaydı. Bu yüzden de çok çeşitli insanlara ulaşabilmekteydi. Nazilerin egemenliğindeki Almanya'dan anti-nazi olduklarını gizleyerek yaşamak istememelerinden kaynaklı, kendisi ve babasının Amerika'ya ilticasının kabul edilmesinin karşılığında Çiçero'yu ihbar etmiş (Gülmez & Demirkollu, 2013) ve Çiçero'nun yaptıkları ortaya çıkmıştır. Böylelikle casusluk yapmasına imkân kalmayan Çiçero Almanya'ya gitmiş ve 1966'da Münih'te fakir bir bekçi olarak ölmüştür (Hürriyet Gazetesi, 2019). Çiçero'nun getirdiği bilgileri kullanmak yerine sezgileriyle yola devam eden Alman lideri Hitler (Gülmez & Demirkollu, 2013), eğer Elyasa'nın getirdiği bilgilere güvenmiş olsaydı savaşın tüm seyri değişebilir ve savaşı

kaybetmeyebilirdi. Buradan da görüldüğü üzere, istihbarat alanında insanın önemi halen devam etmektedir. Ayrıca buradan istihbarat çarkının da ne kadar yararlı bir çıkarım aracı olduğu görülebilir. Çünkü gelen bilgiler zamanında ve doğru ellere teslim edilip gerekli analizler yapılabilip dördüncü ve son aşamada olan istihbaratın yayılması faaliyeti yapılabilseydi, aslında Çiçero'nun verdiği istihbaratın doğruluğu görülecek ve koca bir savaşın tarihi değiştirilebilecekti.

Tekil casusluk olaylarının dışında aynı zamanda bu dönemde karşı istihbarat alanındaki faaliyetler de dikkat çekicidir. Savaş sırasında İngiltere içerisinde faal olan tüm Alman casuslar yakalanmış ve karşı istihbarat faaliyetlerinde yani İngilizlerin tarafına geçerek Almanlara yanlış istihbarat vermekte kullanılmışlardır (Köylüoğlu, 2017). Aynı zamanda İngilizler, Double Cross (Çift Çapraz) teşkilatını 1941 yılında kurmuş ve burada çalışanlarla beraber karşı istihbarat anlamında dünya rekoru kırmıştır (Volkman, 2004, s. 94) . Bu dönemde Türkiye tarafsız bir politikada olmasına rağmen Sovyetler Birliği ile yakınlığı bilindiğinden diğer istihbarat örgütlerinde çalışan casusların uğrak yeri haline gelmiştir (Özkan, 2004, s.176). O dönemler en çok İngiliz, Alman ve Sovyet istihbaratçıların istihbarat faaliyetlerini Türkiye üzerinden yaptıkları bilinmekteydi (Özkan, 2004, s.177).

Kısacası, İkinci Dünya Savaşı sırasında yaşanan gelişmeler neticesinde, istihbaratın önemi daha fazla anlaşılmıştır. Tüm bu gelişmelerin eşliğinde, istihbarat alanındaki yetersizliklerinin tespit edilebilmesine, keşif uçakları sayesinde Görüntü İstihbaratının(GÖRİST) gelişmesine, Sinyal İstihbaratı (SİNİST)'nin çeşitleri olan Elektronik İstihbarat (ELINT) ve Muhabere İstihbaratının (COMINT) gelişmesine, istihbarat teşkilatlarında birçok farklı uzman personelin istihdam edilmesine, icra edilen casusluk faaliyetlerinde geniş çaplı değişimlerin yaşanmasına, devletlere ait istihbarat teşkilatlarının merkezileşmesine olanak verildiği görülmüştür (Çıtak, 2015).

2.1.2.3 1947 yılı ve sonrası istihbarat gelişmeleri

Neo-realistlere göre güç ve devletin devamlılığı esas olduğundan, soğuk savaş sırasında gelebilecek riskler, doğrudan askeri kabiliyetlerle alakalı ve diğer devletlerin saldırgan olmasından dolayıydı (Waltz, 1979, s. 13). İkinci Dünya savaşından yorgun çıkan ülkeler, büyük kayıplar vermişler ve toparlanmaları oldukça uzun zaman almıştır

(Akın, 2017). Müttefik devletlerden olan İngiltere ve Fransa süreçten oldukça yıpranarak çıkmışlarken ABD ve SSCB güçlerini korumayı bilmişlerdir. Böyle bir savaşın uzun bir süre daha çıkamayacağını öngören batılı devletlerin aksine SSCB ordusuna ve askerine yatırım yapmayı tercih edip, yaptığı savunma sanayi yatırımlarıyla Avrupa'da istediği gibi hareket eden SSCB, yayılcı politikalarla diğer ülkelere gözdağı vermiştir. Bu tehlikeye karşı durabilecek o zamanki tek kuvvet ise ABD olmuştur (Uçarol, 1995, s. 658). Bunun sonucunda devletlerin birbirlerine karşı tamamen güç kullanarak ve silahları ortaya çıkarmayarak ilişkilerini devam ettirecekleri Soğuk Savaş başlamıştır (Sander, 1991, s. 175). Batı Bloğunu ABD'nin, Doğu Blok Liderliğini ise SSCB'nin yaptığı iki kutuplu bir sürece girilmiştir. Bu süreçte sadece askeri anlamda güçlü olmak değil, her türlü bilginin toplanması, incelenip analiz edilip yorumlanması gerektiğinden istihbarat faaliyetlerinin önemi oldukça artmıştır ve bu yüzden 1947 yılında başlayan Soğuk Savaş dönemi sırasında istihbarat teşkilatları yüz binden fazla çalışan sayısı ile dünyanın en geniş endüstrisi olmuştur (Warner, 2006 s.17).

İstihbarat olgusunun Soğuk Savaş dönemindeki gelişimi incelendiğinde yeryüzünde tek hâkim güç olma mücadelesi veren ABD ve SSCB etrafında şekillendiği tespit edilmiştir (Caşın, 2002). II. Dünya Savaşı bittikten sonra, iki yıkılmayan devlet olan SSCB ve ABD kendileri arasında yeni bir savaş başlatarak nükleer silahların kullanılmamalarının tek sebebi ise, iki ülke devlet başkanlarının mantıklı kararlar vererek sadece psikolojik savaşa devam etmeleri olmuştur (Hasanov ve Katman, 2019). Bu dönemde istihbarat faaliyetleri daha kavramsal bir çerçevede ve kurumsallaşma boyutunda gelişmeye başlamıştır. 1947 yılında ABD'nin CIA'yi kurmasıyla başlayan kurumsal örgütlenmeler 1954 yılında Sovyetler Birliği'nin Devlet Güvenlik Komitesi ile devam etmiş, 1970 yılına kadar neredeyse tüm devletler kendi istihbarat teşkilatlarını örgütlemişlerdir (Hasanov & Katman, 2019). Soğuk Savaş döneminde kurumsallaşan istihbarat birimleri sadece bürokratik olarak şekillenmemiş aynı zamanda teknik ve jeopolitik ihtiyaçlar tarafından da etkilenmiştir (Rathmell, 2002).

Soğuk Savaş dönemi; yeni istihbarat örgütlerinin ortaya çıktığı, istihbarat olgusunun yasal düzenlemelerde yer aldığı, hem askerî hem teknolojik gelişmelerin istihbarat faaliyetlerinde kullanıldığı ve istihbaratın askerî ve politik olduğu kadar gerek ekonomik gerekse de bilimsel istihbarat alanında devletler nezdinde önem arz ettiği bir

dönem olmuştur (Çıtak, 2015, s.92). Uzaya gönderilen keşif uydularıyla ve icat edilen telsizlerle gelişen SİNİST ile balonların icadıyla başlayan GÖRİST alanının yanı sıra ilk defa İkinci Dünya Savaşı'nda uçakların uzaktan algılanmasında kullanılan radarlar, Soğuk Savaş döneminde istihbarat elde etme metotlarının gelişmesine katkı sunmuştur (Caşın, 2002).

Soğuk Savaş sırasında ABD istihbarat teşkilatlarının ana odak noktası, Sovyetler Birliği liderliğindeki Doğu bloğu ülkeleri iken; Sovyet istihbarat teşkilatlarının ana odak noktası, Amerika Birleşik Devletleri liderliğindeki Batı Bloğu ülkeleriydi (Hasanov & Katman, 2019). İki süper güç arasındaki mücadele, hem istihbarat ihtiyacını artırmış hem de istihbarat araçlarının ve teknolojilerinin gelişimini teşvik etmiştir. Ancak 1989'da Doğu Avrupa'daki komünist rejimler ve 1991'de Sovyetler Birliği'nin dağılmasıyla Soğuk Savaş dönemi sona ermiş, tek süper güç konumunda kalan ABD kendisine hiçbir dış tehdit kalmadığının düşünerek ilerleyen bölümlerde detaylı olarak anlatılacak olan 11 Eylül saldırılarını öngörememiştir.

Soğuk Savaş sırasında dikkat çeken bir istihbarat türü de ekonomik istihbarattır. Ticaret alanında da rekabet eden iki süper güç birbirlerinden önce bilgi edinme konusunda yarış halinde olmuşlardır. Sovyet ajanları Amerika ve hatta Avrupa'da bile daha piyasaya çıkmamış ticari ürünleri, dünya genelindeki yaygın çalışma ağları sayesinde önceden haber edininip, muadilini ya da aynısı çıkarmak suretiyle pazarı ele geçirmeye çalışmışlardır (Poteat, 2001).

II. Dünya Savaşı'nın hemen ardından ortaya çıkan iki güçten biri olan ABD, Almanların Enigma sistemini kullanmasıyla beraber sinyal istihbaratının gücünü anlamıştır. İngiltere, Avusturalya, Yeni Zelanda ve Kanada'yla beraber, ki o dönemde "Beş Göz" olarak biliniyorlardı, "United States of America Agreement" (UKUSA) anlaşmasını imzalayarak dünyayı beşe bölüp izlemeye karar vermişler ve bunun için de Amerika liderliğinde Echelon projesini başlatarak tüm dünyadaki sinyalleri takip etmeye başlamışlardır (Karlstrom, 2021). Echelon'a kısaca uluslararası bir istihbarat sistemi denilebilir. Asıl amacı 1947-1948 yılları arasında Sovyetler Birliğini izlemek olan sistem sayesinde Dünya'da her yere yayılan ABD, kendini dünyanın jandarması olarak görmüştür (Berkkan, 2017, s. 28). Bugün program, kuşkusuz, terörizmi önlemek için

algılanan bir gereklilikten kaynaklı halkın razı olmasıyla devam etmektedir (Karlstrom, 2021).

Soğuk Savaş sırasında istihbarat alanında her ne kadar ABD güçlü görünse de üç büyük istihbarat hatası yapmıştır. Bunlardan biri Kore Savaşı, diğeri Küba Krizi ve Vietnam savaşıdır. Bu dönemdeki ilk sıcak savaş olan Kore savaşı, ABD'nin yanlış değerlendirmesi yüzünden cereyan etmiştir. İmzalanan Atlantik antlaşmasıyla, SSCB'nin yayılımcı politikasının bittiğine inanmış ve SSCB'nin farklı bir bölgeden saldırdığını hiç tahmin edememiştir. Kuzey ve Güney Kore olarak ikiye ayrılmış Kore yarımadasında, kuzey tarafı komünizm destekçisi olan SSCB tarafından desteklenirken, Güney Kore ise ABD desteklenmekteydi. 1947 yılında ABD'li General Albert Wedemeyer tarafından Kuzey Kore tarafından bir saldırı olacağı konusunda hazırlanan istihbarat raporuna rağmen hem Birleşmiş Milletler hem de ABD hazırlıksız yakalanmıştır (Cumings, 2005, s.203). Kore savaşında teknik istihbaratı çok ihmal ettiği için Güney Kore'de karşılaşacağı silahlara karşı önlem alamamış o yüzden de kayıplarla sonuçlanmıştır (Bolin, 1998, s. 4-5). 1962 Küba Krizinde SSCB'nin Küba'da nükleer füzeleri konuşlandırmadığı hakkındaki yanlış CIA istihbarat raporu sonucu erken müdahale etme şansını kaçırdığından süreç uzamış, dünya neredeyse bir nükleer savaş krizinin ortasına sürüklenmiş ve kriz Birleşmiş Milletler Güvenlik Konseyi'nin de araya girmesiyle daha ileri gitmeden bitirilmiştir (Ataç & Özcan, s.100-105). Vietnam savaşında da ABD, Kore'deki gibi SSCB'nin yayılması ve komünizmin güçlenmesini durdurmak için kendisine saldırıldığı bahanesiyle Kuzey Vietnam'a saldırmış ancak ellerindeki askeri gücü fark edecek bir askeri istihbarat eksikliği yaşadığından barış masasına oturmak zorunda kalmıştır (Arıoğlu, 2012). Bu üç olayda da ortak olan nokta, ABD elinde olan istihbaratı ya değerlendirememiş ya da hatalı bir analiz yapmıştır ve sonuçta kazanabileceği alanları bile sonuçları öngörebilecek teknolojik ve askeri istihbarat raporları eksikliğinden kaybetmiştir. ABD Soğuk Savaş bittikten sonra her ne kadar tek süper güç olarak kalsa ve istihbarat alanına yaptığı yatırımlarla bilinse de daha sonra da istihbarat hatalarına devam etmiştir. Bunlar ileri bölümlerde detaylı olarak incelenecektir.

Soğuk Savaş sonrası istihbarat faaliyetlerinin değişim süreci değerlendirildiğinde üç ana başlık altında toparlanabildiği görülmektedir. Bunlar, bilgi teknolojilerinin gelişmesi, istihbarat elde etme araçlarının artmasıyla merkez teşkilatın istihbarat

faaliyetleri anlayışının kaybolması ve karşılıklı istihbarat rekabetidir (Özdağ, 2018, s.52).

Soğuk Savaş'ın sona ermesiyle, iki kutuplu bir dünyada tam bir nükleer savaş olasılığı ortadan kalkmıştır. Sonuç olarak, ABD ile Rusya arasındaki silahlanma yarışı geçici olarak durmuştur. 21. yy. başında, topyekûn savaşın yerini bölgesel ve asimetrik savaşa bırakmasıyla birlikte (Benbow, 2008), devletlerarası hegemonyanın doğasının önemli ölçüde değiştiği söylenebilir.

Soğuk Savaş bitiminden sonra gerek teknolojinin hızlı gelişimi gerekse bilginin öneminin ön plana çıkmasıyla beraber istihbarat alanına bakışta da değişiklikler olmuştur (Toffler & Toffler, 1994, s.158). İçinde bulunduğumuz bu dönemde, istihbarat servisinin en önemli kaynaklarının arasında “açık kaynak” istihbaratının da olacağı aşikârdır. Çünkü modern istihbarat döneminde artık açık kaynakların fazlalığı ön plana alındığında, istihbarat uzmanları sorunların çözümünde ilk olarak buralara bakacak, daha sonra ise bu bilgiler doğrulamak amacıyla gizli çalışacaktır. Aynı zamanda istihbarat uzmanlarının kendilerinden istenen bilgiyi doğru anlayıp, kaynakları doğru kullanıp, güvenilir ve hızlı bir analiz yapıp zamanında teslim edebilmesi de önem kazanmıştır (Johnson, 2000, s.95). Ayrıca bu dönemde sadece istihbarat değil ‘karşı istihbarat’ da oldukça önemli bir hale gelmiştir. Bilgi çağı olarak görülen bu çağda, bilgi toplamak kadar karşı tarafa eldeki bilgileri vermemenin de önemi yadsınmamalıdır.

Soğuk Savaşın bitiminden sonra olabilecek yeni savaşların boyutları da tartışmalıdır. Savaşlar tamamen sona erebileceği gibi, asla da bitmeyebilir, ancak savaşın tanımının ciddi değişimler yaşanabileceği yönünde görüşler mevcuttur. Bu nedenle artık ‘yeni savaş’ kavramı ortaya çıkmıştır. Yeni savaşlar için; hibrit savaş, düşük yoğunluklu savaş, sınırlı (küçük) savaş, postmodern savaş, yeni nesil savaş gibi isimler de verilebilir. Bu tanımlar savaşın değişen doğasına dikkat çekse de bu değişimi tam olarak ifade etmemektedir. Bu nedenle alana hakim terimler olarak “yeni savaş” ve “yeni savaş anlayışı” kullanılmaktadır (Çıtak, 2019). Hibrit savaşlar birçok teorisyene göre yeni savaş anlayışının bir başka adıdır (Özdemir Küçük & Eminoğlu, 2022). Hibrit savaş demek orduların birbirleriyle çarpışıp alanda kazandığı savaş değil aksine savaşı ilan etmeden düşük yoğunlukta çatışmaktır (Bıçakçı, 2019). Bu kavramı ortaya atan ve akademik anlamda literatüre sokan Frank Hoffman’a göre hibrit savaş hem devletlerarası hem de

devlet dışı aktörleri içerir. Aşağıdaki şekilden de anlaşılacağı üzere hibrit savaş geleneksel ve modern savaşları içerir.



Kaynak: (Can, 2022)

Bilgi savaşını da tanımında bulunduran ‘Hibrit Savaş’ kavramında anlaşıldığı üzere istihbarat kaynaklarının verimli kullanımını da içermektedir. Sadece devletler değil aynı zamanda devlet dışı aktörleri de içerdiğinden dolayı, ne kadar çok doğru istihbarat elde edilirse sahada olmayan bu savaş türü daha çabuk kazanılır. Gelecek de topyekûn savaş yerine bu alan daha çok revaçta olacağından en önemli şey bilgi toplamak olacaktır. Hibrit savaşta ana hedefin devletin kurumları ve siyasi otoriteyi istikrarsız hale getirmek olduğu düşünüldüğünde (Özer, 2018), kaos ortamı yaratabilmede o devletle ilgili bilgileri bilmenin ne kadar önemli olduğunu görmek kaçınılmazdır.

Hibrit savaşlarda mücadelede özellikle üç istihbarat alanı oldukça önemlidir. Bunlar; insan istihbaratı, sinyal istihbaratı ve görüntü istihbaratıdır. İnsan istihbaratının öne çıkmasındaki neden casusluk ve sızma yöntemleriyle kısa sürede bilgi etmektir. Sinyal istihbaratı ise telsiz dinleme, el konuşması ve benzeri gibi sinyaller yoluyla bilgi toplanması yoluyla, muhaliflerden gelebilecek saldırı ihtimaliyle mücadele edebilmenin yanı sıra savaş karşısında atılacak adımlarla ilgili hazırlıklar da yapabilmesine imkân tanır.

Aynı zamanda verilerin şifrelenmesine olanak vererek bilgi hırsızlığını önleyerek karşı istihbaratı destekler. Görüntü istihbaratı ise kızılötesi, uzaydan ultraviyole veya dış fotoğraf teknolojisi kullanılarak görüntülerin/fotoğrafların toplanması yoluyla yapıldığından karşı tarafın gücünü hesaplanmasında önemli rol oynar (Pramitasari , 2022) İstihbarat örgütlerinin bu tür bir savaşı yürütmek için istihbarat geleneklerini güncellemeleri gerekmektedir. Öte yandan, istihbarat örgütleri hibrit tehditlere karşı koymak, rakip hibrit operasyonları bozmak ve hibrit savaşın siyasi etkilerini azaltmak için politikalar/stratejiler geliştirmelidir (Ateş A. , 2020).

İstihbaratın temelinde güvenlik kaygılarının yattığı varsayımından hareketle, Soğuk Savaş sonrasında değişen bazı güvenlik sorunlarına bakarsak eğer; uluslararası alanda ülke sayısının arttığını, bu artışın ilişkilerdeki barış niyetine ve güvenlik alanında sorunların üretilmesine neden olacağını ve devlet dışı aktörlerin bunlardan çıkar elde edebileceğini görebilmekteyiz (Biçer, 2017). Bu gerçeklerin ışığında, devlet dışı aktörlerden olan teröristlerin artabileceği endişesi de ortaya çıkan diğer bir gerçek olarak görülebilir. Gerek terör hareketlerinin artma endişesi, gerekse üstünlük mücadelesi, uluslararası alanda istihbaratın önemini gittikçe ön plana çıkarmıştır. Hali hazırda süper güç olarak kabul edilen ABD, bu üstünlüğünü kaybetmemeye çalışmakta, gelişen devletler ise gerek ekonomik gerekse politik anlamda öne çıkma isteklerinden dolayı, bilgi eskisinden çok daha değerli olmuştur. Bu yüzden ki istihbarat faaliyetleri dış politika ve uluslararası ilişkiler alanında yön belirleyici bir konuma gelmiştir denilebilmektedir.

2.2. Türk İstihbarat Tarihi

Türk istihbarat tarihi incelendiğinde, İslamiyet öncesi ve sonrası, Osmanlı dönemi ve sonrası ile Türkiye Cumhuriyeti sonrası olarak incelemek daha doğru bir yaklaşım olacaktır. Çünkü Türkler tarih boyunca bir çok farklı devlet kurduklarından ve istihbarat kavram olarak olmasa da ilk ortaya çıkışı insanoğlunun başlangıcına kadar evrildiğinden sadece Müslümanlık ya da Osmanlı Dönemine bakmak ve yorum yapmak doğru olmayacaktır. Dünya doğası gereği değiştiğinden kaynaklı istihbaratın dönemsel bazda toplanma kaynakları ve önemi de değişmiş, aynı zamanda sadece askeri yani daha çok güvenlik sağlama amacından çok sivil hayata da girdiği gerçeği bu bölümlerde daha detaylı olarak anlatılacaktır.

2.2.1 Türklerde İslamiyet öncesi ve sonrası istihbarat anlayışı

Türklerin tarihsel süreç içerisinde karşılaştıkları ilk casusluk olayları Çin ve Hun devleti arasında olmuştur. M.Ö. 125 yılında Çinliler tarafından Hun Türklerinin devlet teşkilatının içine sızılarak onların yapısını çözmek amaçlı hazırlanan rapor Türk tarihinde ki ilk casusluk belgelerinden biridir (Karan, 2008, s. 18).

Türklerdeki istihbarat faaliyetleri genel anlamda casusluk faaliyetleri üzerine kurulmuş ve casuslara “çaşut”, casusluk faaliyetlerine de “çaşutlama” denilmiştir (Özcan, 1993, s.166). Türk tarihindeki ilk dönem istihbarat faaliyetlerine bakıldığında dini ve siyasi nitelikte olarak ayrılabilir. Din açısından istihbarat toplayan casuslar Çinlerin dinine ya da Budizm’e bağlı görünmekteydi. Çinlilerdeki casusluk ise üst kademelere gelerek Türkleri gök tanrı dininden uzaklaştırıp kendi dinlerine bağlamaya çalışmaktı. Aynı zamanda Türklerin arasına girer gelenekler ve adetler hakkında bilgiler toplarlardı bunları da “seyahatname” adı altında kendi hükümdarlarına sunarlardı. Bu casuslardan en çok bilineni ise Ch’ang Ch’ien adlı bir askerdir (Arıklı & Yavuz, 1974, s.3). Siyasi nitelikte olan casusluk faaliyetleri ise dini istihbaratın önemini kaybetmesinden sonra ortaya çıkmıştır. Daha çok İran, Hint gibi diğer Türk kavimleri arasında dolaştırılan casusular bu dönemde ortaya çıkmıştır. Amaç bu kavimlerdeki siyasi faaliyetleri yakından izlemek olmuştur (Arıklı ve Yavuz, 1974, s.3).

Türklerin istihbarat örgütlenmelerinin ilk zamanlarına bakıldığında İslamiyet’in kabul edilmesinden sonra olduğu görülmektedir. Bu devletlere örnek olarak; Karahanlılar, Büyük Selçuklu ve Gazneliler verilebilir. Özellikle Gazneliler döneminde organizasyonlu istihbarat faaliyetleri görülebilmektedir (Demircioğlu vd, 2021). Karahanlı hanedanına (840-1212) kadar istihbarat faaliyetleri ağırlıklı olarak dışarıdan yürütülse de, iç gelişmelerin yakından takip edilmesi gerektiğinden iç istihbarat da söz konusuydu. Zira Türkler İslamiyeti din olarak kabul ettiklerinde İslam camiasında ciddi bir mezhep çatışması olmuş ve bu sıkıntılı süreçte Türkler İslamiyete dahil edilmiştir (Şimşek E. , 2004, s. 16-17). Bu anlamda içeride oluşabilecek tehlikelerin de dikkatlice takip edilmesi ve zamanında haber toplanması gerekliydi. Gazneliler zamanında (969-1187) fetih hareketinin artmaya devam ettiği dönemde, ulusal sınırların genişlemesiyle istihbarat faaliyetleri artarak devam etmiştir. Bu dönemde Dîvânü’l-berîd teşkilatı kurulmuş ve

türlü yollardan bilgiler toplamak için araç gereçler geliştirilmiştir (Demircioğlu vd, 2021).

Selçuklular döneminde askeri istihbarat da önemli bir hale gelmiş ve Çağrı Bey'in çıktığı keşif akınıyla ortaya çıkan Rumların fethedilebilir olduğu bilgisi Selçukluların Anadolu'yu fethetmelerinde önemli bir bilgi olmuştur (Abu'lfarac, 1999, s. 293). Büyük Selçuklu Devleti'nin veziri Nizâmü'l-mülk tarafından yazılan "Siyasetname" adlı eserde de dönem içerisindeki istihbarat faaliyetlerinin aktif olduğu aşağıdaki gibi belirtilmiştir (Köymen, 1990, s. 80-81) ;

O böyle yapmazsa ayıp olur gaflet, tembellik ve zulme hamlederler ve memlekette olup biten fesadı ve zulmü biliyor veya bilmiyor. Eğer biliyor da meselenin çaresine bakmıyorsa tıpkı onlar gibi zalimdir ve zulme rıza göstermiştir ve eğer bilmiyorsa gaflete düşürülmüştür. Tembel ve cahildir. Bu her iki hususta iyi değildir. Mutlaka haberciye (sâhib-i berid) ihtiyacı vardır.

Siyasetname'deki bilgiler doğrultusunda Sultan Melikşah zamanında da istihbarat faaliyetlerinin önemli olduğu, iç istihbarat kadar dış istihbarata da önem verildiği anlaşılmaktadır (Köymen, 1990, s. 100). Nizamülmülk istihbaratın önemini bu eserde oldukça fazla ortaya çıkarmıştır. Yazdığı eserde hükümdarın her şeyden haberdar olması gerektiğini, kilometrelerce uzakta olsa dahi bir kişiye ya da canlıya haksızlık yapıldığında bunu yapanların anında cezalandırılması gerekliliğini savunmuş, Sultan Mahmud hakkında bu konuda övgüyle söz etmiştir. Ona göre nerdeyse her şey (elbiseler, sancaklar, hayvanlar vb.) istihbarat araçları olarak kullanılabilirken, Saray ve Sultana ait diğer mekanlar ile resmi devlet kurumları istihbarat toplanma merkezleri olarak görülmüş ve işi istihbarat olan kişiler kadar tellallar ve sıradan insanların da istihbarat görevlisi olabileceğinden bahsetmiştir (Şimşir, 2015).

2.2.2. Osmanlı Devleti ve sonrası istihbarat faaliyetleri

Osmanlı Devleti zamanında ise casusluk faaliyetlerinin daha farklı ve net olduğu görülmektedir. Osmanlı zamanında istihbarat toplama şekilleri incelendiğinde bunların dört ana başlıkta toplandığı görülebilir. Bunlar; gönüllü casusluk, ücretli casusluk, dil alma yöntemi, tüccar ve gezginlerden gelen haberlerdir (Eroğlu, 2003).

Osmanlı İmparatorluğu'nun kuruluşu sırasında "gönüllü casusluk" uygulaması yaygın olarak kullanılmıştır. Maaş karşılığı yani ücretli casusluk faaliyetlerine ise 16. Yüzyıl ortalarında rastlanmaktadır (Eroğlu, 2007 s. 95-96,107). Maaşlı casuslar

hakkındaki ilk bilgilere Tarih-i Selanik kitabında rastlanmaktadır. Bu kitapta ikinci vezir Pertev Paşanın, Göle Kalesi fethi sırasında Hırvat asıllı Karaçı'nın karşı tarafa askeri yardımda bulunduğunu paralı casuslar tarafından öğrendiğinden bahsetmektedir (Mustafa Efendi, 1999, s. 13).

Diğer bir yöntem olan “Dil alma” yöntemi ise düşman hakkında bilgi almak ve/veya düşmanın durumu hakkında bilgi istihbarat elde edilecek birini ele geçirmeyi içerir (Eroğlu, 2003). Bilgi sağlamak için yapılan esir yakalama işine Osmanlı'da “dil alma”, bu esirlere de “dil” deniyordu (İlter, 2002). Selçuklular özellikle dil edinim yöntemlerini etkin bir şekilde kullanmışlardır. Bu yöntem kullanılarak çok değerli bilgiler elde edilebileceği gibi kasıtlı olarak asılsız olan bilgiler de elde edilebilir. Bunun için yakalanan personelin düşman hakkında gerekli ve yeterli bilgiye sahip olması gerekir. Bu anlamda elde edilen bilgilerin detaylı olarak incelenmesi gerekmektedir (Dünyabizim, 2022). Askeri istihbarat açısından Osmanlılar da tıpkı bir önceki Türk devleti gibi dil olarak bilinen düşman tarafından ele geçirilmekten yararlanmışlardır. Savaşta kazanılan dil ve ordunun ve bunlardan elde edilen ülkenin dili saldırganlara rehberlik edecektir. Ancak diller bazen ülkeleri için işe yaramış, sefer yollarını saptırmış ve Türkleri tuzağa düşürmüştür (Özcan, 1993, s.67).

İstihbarat kaynakları olarak görülen tüccar ve gezginlerden gelen belgeler de Osmanlı döneminde oldukça önemli olmuştur. Gerek Osmanlı'daki ticaretle ilgilenen ya da seyahat eden vatandaşlarının diğer ülkelere gittiklerinde sahip oldukları yüksek itibara karşın elde edebildikleri bilgi kaynakları olsun, gerekse Osmanlı'ya karşı devletlerin bu tarz insanlarla casusluk faaliyetleri olsun, bu dönemde oldukça yaygın olarak kullanılmıştır (Eroğlu, 2003).

Osmanlı padişahları arasında en unutulmazlardan biri şüphesiz ki Sultan II. Abdülhamid'dir. II. Abdülhamid, modern bürokratik araçları ve daha da önemlisi bir ideolojiyi kullanarak, Osmanlı Devleti'nde daha önce görülmemiş bir şekilde tüm gücü elinde toplamıştır. İktidarda olduğu süre boyunca devlet, topluma eşi görülmemiş bir düzeyde nüfuz etmeye başlamıştır (Ortaylı, 2001, s. 89-90). Bu dönem hem Türkiye Cumhuriyeti kurulmadan önceki temellerin atıldığı bir dönem hem de olayların oldukça fazla görüldüğü bir zaman dilimidir (Karpaz, 2012, s. 116-117). II. Abdülhamid dönemi

Osmanlı tarihinde isyanlar, savaşlar ve bir sürü krizler dönemi olduğu gibi aynı zamanda II. Abdülhamid'in otoriter yapısını ortaya çıkardığı da bir dönemdir. II. Abdülhamid yönetimindeki istihbarat teşkilatının kurumsal bir profili yoktu ve bazı casus denilebilecek çalışanlar Harbiye Nezareti'ne bağlıydı. Bu dönemde Hafıye teşkilatı adında bilinen bir teşkilat olduğu bilinmektedir (Haydaroglu, 1995). Teşkilat kimliği altında bir kurum olarak Osmanlı döneminde resmi kayıtlarında olmasa da Türkiye Cumhuriyeti kurulmadan hemen önceki istihbarat faaliyetlerini yürüten ve 1884 yılında kurulan Hafıye Teşkilatı, hali hazırda istihbarat faaliyetlerini yürüten MİT teşkilatının atası olarak gösterilmektedir (Sakaoğlu, 2012, s. 52-54). Hafıye, gizli soruşturma memuru olarak kullanılmıştır. İşleri kimseye belli etmeden soruşturan kişiye hafıye memuru veya kısaca hafıye denilmiştir (Gör, 2015, s.19). Aynı zamanda bu dönemde hafıye kelimesi dışında jurnal ve jurnalcilik kelimelerinin de çok kullanıldığı görülmektedir . Fransızcadan dilimize geçmiş olan jurnal kelimesi polis raporu anlamına gelmekle beraber hafıyelerin çoğunun polis memuru olduğu düşünüldüğünde onların getirdiği istihbarat raporu olarak çevrilmesi daha doğru olacaktır. II. Abdülhamit, Osmanlı dönemi padişahlarını arasında en çok konuşulanı olup, birlik ve bütünlüğü sağlamak için aldığı önlemlerle baskı hükümdarlığı kurduğu düşünülen bir yönetici konumundaydı. Bu yüzden de en çok suikast düzenlenen padişahlarından biri olmuştur (Sakaoğlu, 2012, s. 52-54). Padişah düşmanlarını Hafıye Teşkilatı ile takip ettirmiş, kendisi ve yönetimi hakkındaki fikirlerini ele geçirerek birçok tehlikeli planın önüne geçmiştir. Bu yüzden ki istihbarat ağına oldukça önem vermiş ve “hafıye memuru” olarak ülke içi ve dışında görev alan kişilere ihtiyaç duymuştur. Bunlara maaş bağlamış aynı zamanda kendi yaşadığı saray olan Yıldız Sarayında da “Serhafıyelik” makamı kurarak elde edilen tüm bilgileri değerlendirme kısmını buraya bırakmıştır (Gör, 2021).

Hafıye teşkilatının amaçlarına bakıldığında tam bir istihbarat örgütünün amaçlarını görmek mümkündür. Bu amaçlar: Ülkeyi yöneten padişahın korunması, devletin hukukunun korunması ve milletin ve toprakların bütünlüğünün korunması olarak sıralanabilir (Beyhan, 1999). Hafıye teşkilatının içerisinde sadece ücretli casuslar değil gönüllü casuslar da bulunmaktaydı. Bunlar gazeteci bürokrat, yazar gibi çeşitli mesleklerden insanlardan oluşuyordu. Aslında bu teşkilatın Bâb-ı Âlî'ye bağlı olmasına rağmen orayı da atlayarak direk Yıldız Sarayına ulaşmalarından kaynaklı gelen istihbarat

ağı çok genişlemiş (Tahsin Paşa, 1999, s. 37-38), ancak bu aynı zamanda bilgi kirliliğine de yol açmıştır. Herkesin bilgi verme hakkının olduğu yerde doğal olarak insanların da bunu kullanabileceklerini ve üstünlük sağlamaya çalışabileceklerini de düşünmek gerekir. En üstteki insandan en alttaki insana kadar herkes isimsiz jurnallerle saraya bilgi akışında bulunabildiği için gücün kontrolsüz kullanılmasına da neden olmuştur (Alper, 2021). II. Meşrutiyetin sonlanmasıyla tahttan inen II. Abdülhamid'den sonra bu teşkilatın faaliyetlerine son verilmiş ve teşkilata ait olan tüm belge ve bilgiler yakılmıştır (İlter, 2002, s. 7-8)

Zayıflayan Hafiye Teşkilatı ile beraber yeni güç noktaları ortaya çıkmıştır. I. Dünya Savaş öncesi Osmanlı devletine karşı casusluk faaliyetlerinin oldukça arttığı bir dönemdi. Bu faaliyetleri gören Osmanlı Enver Paşa başkanlığında Türkleri bir bayrak altında toplamak ve Panislamizm odağında olmak amacıyla Teşkilatı-Mahsusa'yı (1913-1918) kurdu (Güneş, 2013). Bu teşkilat, zamanın ilerisinde olarak tanımlanabilecek istihbarat örgütlenmesiyle Kafkasya, Yakın Doğu, Orta Doğu, Kuzey Afrika ve Orta Asya gibi geniş coğrafyada başarılı ve çok önemli istihbarat faaliyetleri yürütmüştür (MİT, 2022b). Bu örgütün istihbarat servisinin ne zaman kurulduğu tespit edilemezken, Osmanlı Devletine yönelik yıkıcı faaliyetleri engellemek amacıyla, kalifiye eleman eğiterek onları düşman bölgelerine göndererek doğru istihbarat ulaşmadığında oluşabilecek tehlikeleri önlemek için faaliyetlerine başlamıştır (Sayın, 2007, s. 146-148). Bu teşkilatın istihbarat toplama çabaları her ne kadar istenilen başarıları sağlayamamış olsa da, ana amacı çöken Osmanlı Devletini kurtarmak olduğundan, yaptıkları çalışmalar takdirle karşılanmalıdır (Güneş, 2013). I. Dünya Savaşının sona ermesiyle beraber bu teşkilat da dağılmıştır.

Teşkilat-ı Mahsusa'nın dağılmasının ardından Karakol Cemiyeti (1918-1920) adı altında istihbarat faaliyetleri devam etmiştir. Mondros Ateşkes Antlaşmasıyla kurulan ve 1920'deki İstanbul'un fiilen işgaline kadar süregelen teşkilat, İstanbul dâhil hemen hemen Anadolu'nun her köşesinde aktif olmuş bir organizasyondur. Kurucusu Kara Kemal Bey'dir. Enver Paşa, Teşkilat-ı Mahsusa'nın dağıtılması emrini vermiş ancak istihbarat faaliyetlerinin farklı bir organizasyonla devam etmesi gerektiğini de o zamanın Teşkilatı Mahsusa başkanına söylemiştir (Bal, 2022). Bunun üzerine Karakol Cemiyeti ilk gizli istihbarat teşkilatı olarak kurulmuştur (MİT, 2022b). 16 Mart 1920'de İstanbul'un fiili işgaliyle beraber liderleri yakalanmış ve hücreleri deşifre olmuştur. Bunun üzerine

Ankara'nın kontrol ettiği diğer gizli yer altı örgütlerine elindeki kaynakları aktararak dağılmıştır (Bal, 2022).

Karakol Cemiyeti'nin devamı olarak kabul edilen Zabitan Grubu Üsküdar'da kurulmuştur (MİT, 2022b). Aynı Tarihlerde kurulan Hamza grubunu üyeleri TBMM ordu kadrosuna alınarak Ankara hükümeti tarafından tanınırken Zabitan grubuna güven yoktu. Çünkü bu gruba çok fazla casusun sızdığı düşünülüyordu. 1921'de kendilerini lağvetmeye zorlanarak grup kapatılmıştır (Aydın M. , 1990).

Zabitan Grubunun dağıtılmasıyla beraber, teşkilatın isminin değiştirilmesi ve kadrosunun korunması amacıyla Yavuz Grubu 1921 yılında kurulmuş ve aynı yıl kurucusu Mustafa Bey'in yakalanma ihtimaline karşı Anadolu'ya kaçmasıyla beraber faaliyetleri dağılmıştır (MİT, 2022b).

Hamza grupları adı altında iki şehirde faaliyet göstermeye başlayan gruptan Ankara kanadı Zabitan Grubuyla giriştiği rekabette İstanbul kanadını güçlendirerek hayatına devam etmiştir (MİT, 2022b). Hamza Grubu İstanbul kanadı için ise hali hazırdaki istihbarat teşkilatı olan Milli İstihbarat Teşkilatı'nın sitesinde bu grup ve kuruluş amacı şu şekilde açıklanmaktadır:

Başlangıçta Hamza Grubu ismin alan ve TBMM'nin 23 Nisan 1920 tarihli kararıyla Erkan-ı Harbiye Umumiye Riyaset (Genel Kurmay Başkanlığı)'na bağlanan oluşum, gizli direniş gruplarının tek merkezde yönetilmesi amacıyla kurulmuştur. Bu grubun ismi gerek şifrelerinin gerekse kişilerin deşifre olmasıyla sırasıyla Mücahid, Muharip ve Felah grupları olarak değişmiş ve 1923 yılında faaliyetlerine son vermiştir (MİT, 2022b).

Daha sonra kurulan Müsellah Müdafaa-i Milliye (MİM) Grubu (1921-1923) ağırlıklı olarak Müslüman mahallerde ortaya çıkan mahalle örgütlerini tek bir çatı altında toplayan gruptur. Üye sayısı 10.000'leri bulmuştur. Sadece sivil değil askeri alanda da üyeleri oluşmuştur. Kurtuluş savaşı süresince askerlere cephane ulaşmasını sağlarken, topladığı gizli belgelerle istihbarat alanında oldukça faal bir grup olmuştur (Ülker, 2016). Osmanlı döneminin son teşkilatı olarak görülebilir.

2.2.3. Türkiye Cumhuriyeti Devleti ve istihbarat faaliyetleri

Türkiye Cumhuriyeti'nin yeni kurulduğu zamanlara genel olarak baktığımızda ise iç güvenlik kaygılarının yükseldiği görülmektedir. Bunun yanında sürekli işgal tehdidi ve

bundan dolayı toprak kaybetme korkusu olduğundan dolayı olduğu için ülke güvenliği sağlamak amacıyla yapılan istihbarat faaliyetlerinin iç ve dış olarak ayrılmadan karışık olarak sürdürüldüğü söylenebilir. Bu dönemde özellikle dikkat çeken kişi Avukat Hamdi'dir. Bu iç istihbarat faaliyetleri kapsamında Balıkesir'de Tatar kökenli Avukat Hamdi'nin Çerkezlerle çalıştığı kayıt altına alınmış bu da o dönem istihbarat faaliyetlerinde sadece farklı devletlerin değil farklı etnik kökenlerinde tehdit olarak algılandığı görülmektedir (Kavsıracı, 2020).

İstihbarat örgütlerinin yapılanması açısından bakıldığında ise Osmanlı Devleti dönemi ön plana çıkmaktadır (Karan, 2008, s. 33). Osmanlı Devletinde bulunan devlet ve rejime karşı gelebilecek eylemleri önlemek amaçlı her türlü önlemin alınması geleneği, Türkiye Cumhuriyeti'ne de miras kalmıştır (Bagheri, 2012). Bu yüzdendir ki dönem istihbarat teşkilatlarının adı değişse de istihbaratın önemi değişmemiştir.

Milli Emniyet Hizmeti Riyaseti (M.E.H. / MAH) Cumhuriyet döneminin ilk istihbarat örgütü olarak, Türklere karşı yapılan casusluk faaliyetlerini engellemek amacıyla 6 Ocak 1926'da Atatürk tarafından kurulmuştur (Özkan, 2006, s.166). Kuruluş tarihine kadar olan hizmetlerde dâhil tüm çalışmalar bu kuruma aktarılmıştır. Teşkilat-ı Mahsusa'nın uzantısı olarak düşünülebilecek olan MAH, dönemin koşullarına uygun yapılan değişikliklerle, 1965 yılına kadar Türkiye'nin istihbarat hizmetini karşıladı. 1965'te MİT kurulduktan sonra MİT'in bir şubesi olarak 1980'lere kadar varlığını sürdürmeye devam etti (Kuzu, 2007, s. 250-251).

Bir diğer istihbarat faaliyetleri açısından açılan yapı Özel Harp Dairesi (ÖHD)'dir. Soğuk Savaş sırasında, 1959 yılında, Türk Genelkurmay Başkanlığının içinde Amerikan istihbarat servisi (CIA) ve NATO ile ortak kurulan ve bu çatı altında eylemler gerçekleştiren çalışanlarına kontrgerilla denilen bir örgüttür. Soğuk Savaş döneminde yayılmaya çalışılan anti-komünizme karşı çıkmak komünistliğe işaret ettiğinden vatan hainliği sayılmaktaydı (Kongar, 2007, s. 175). Bu örgütün amacı ise antikomünist hareketleri engellemektir. ÖHD'nin adı değiştirilerek Özel Kuvvetler Komutanlığı olmuş ve hali hazırda Genelkurmay Başkanlığına bağlı olarak ve kontrgerilla faaliyetlerini bitirdiğini söyleyerek faaliyetlerini sürdürmektedir (Erdal, 2010, s.21).

Jandarma İstihbarat ve Terörle Mücadele (JİTEM) ise istihbaratın askeri tarafıdır.

Önceden il ve ilçelerdeki asayiş alanındaki istihbarat bilgilerini toplana bu kuruluş, yerel dilleri bilen insanları da bünyesine alarak bölgesel bazda güçlenmeye çalışmış ve bunu başarmıştır. Ancak askeri istihbarat yâda Milli İstihbarat Teşkilatı boyutunda bir güce erişememiştir (Avcı, 2006, s.13). Jandarma teşkilatı JİTEM in varlığını hiçbir zaman kabul etmemiş olup, halk arasında jandarmadaki istihbarat daire başkanlığının bu şekilde anıldığını iddia etmiştir (Düzel, 2002, s. 124).

Milli İstihbarat Teşkilatı (MİT) ise hali hazırda varlığına devam eden asıl istihbarat organıdır. 6 Temmuz 1965’de MAH’ın organizasyonel olarak değişmesi ihtiyacı sonucunda Meclis kararıyla kurulan ve hali hazırda faaliyetlerine devam etmekte olan istihbarat teşkilatıdır Yurt içinde ve dışında milli çıkarları gözetmek amaçlı ve Türkiye Cumhuriyeti’ne yönelik düşmanca hareketlere karşı önceden bilgi toplayarak tehlikeleri yok etmek ya da en aza indirmek amaçlı kurulmuştur (MİT, 2022b).

MİT dışında istihbarat yapılanmasının içinde Cumhurbaşkanlığına bağlı olan ve bakanlıkların içerisinde istihbarat faaliyetlerinde bulunan kurumlar ile askeriyeyle bağlı istihbarat teşkilatları da bulunmaktadır. Bunlara örnek olarak, İçişleri Bakanlığı’na bağlı Kaçakçılık İstihbarat Harekât ve Bilgi Toplama Dairesi Başkanlığı, Ticaret Bakanlığı’na bağlı Gümrükler Muhafaza Genel Müdürlüğü, Hazine ve Maliye Bakanlığı’na bağlı Mali Suçları Araştırma Kurulu, ya da Tarım ve Orman Bakanlığı’na bağlı Orman Genel Müdürlüğü verilebilir (Tekiner & Gemici, 2019). Milli İstihbarat Dairesi Başkanlığı Türkiye’de ana istihbarat kurumu olmasına rağmen diğer devletler gibi onun da yardımcı olduğu ya da ona yardımcı olan kuruluşlar doğrudan ya da dolaylı olarak Cumhurbaşkanlığı’na bağlı olarak faaliyet göstermektedirler.

Dünya tarihi içerisindeki istihbarat faaliyetlerine ve ülkelerin şu anki istihbarat yapılandırmasına baktığımızda aradaki en bariz farkın diğerlerinde askeri ve sivil istihbaratın bir ayrımı olduğu ve aynı zamanda iç ve dış istihbarat için farklı kurumlar kurulduğu görülürken Türkiye’de bu alanda direk olarak görevlendirilmiş tek kurumun MİT olduğudur. Daha detaylı belirtmek gerekirse, Amerika’daki gibi dış istihbarata bakan CIA, İngiltere dış istihbarat servisi olan SIS gibi dış istihbaratla direk görevli bir kuruluşu yoktur. Terör örgütlerinin hedefi olan Türkiye, sadece milli güvenliği sağlamak açısından değil aynı zamanda kendi çıkarlarını da koruyabilmek amaçlı uluslararası alanda da

pozisyonlarını sağlamlaştırarak kısıtlı istihbarat alanlarıyla değil diğer ülkelerin yaptığı gibi özellikle teknolojik ve sinyal istihbaratı alanlarına yönelerek, gelişen Dünya'ya ayak uydurmalı ve tüm bunları yapmak amaçlı gerekli önlemleri alarak güçlü bir dış politika hedeflerini belirleyerek ona göre hareket etmelidir. Bu yüzden de sadece MİT değil ayrı bir dış istihbarat kurumuna da ihtiyacı olduğu açıktır (Fidan, 1999, s. 74-80)

Dünya tarihindeki ilk istihbarat kurumsal anlamdaki istihbarat örgütünün İngiltere'de kurulduğunu düşünürsek, bu anlamda istihbaratın önemini ilk kavrayan ve bunun için çalışmalar yapan ilk ülkenin İngiltere olduğu söylenebilir. Bundan dolayı istihbarat tarihi deyince akla ilk gelen ülke olan İngiltere'den sonra, İsviçre, Çin, Almanya, Rusya, Fransa ve Almanya gibi büyük ülkelerin istihbarat örgütlerinin yapılanmasını da bilmek tarihsel süreci daha iyi anlamamıza yardımcı olacaktır

2.3. Dünyadaki İstihbarat Örgütleri

2.3.1. İngiliz istihbarat örgütleri

İngiltere, İngiliz gizli kraliyet servisini kurarak ilk kurumsal anlamda istihbarat örgütlerini başlatmıştır (Acar, 2019). Gerçek anlamda bilinen istihbarat örgütleri ise MI5 ve MI6'dır. İngiliz gizli istihbarat servisi olarak da bilinen MI6 dünyanın bilinen en eski gizli servis yapılanmasıdır (Aydın A. , 2020). 1909 yılında gizli servis bürosu olarak kurulan MI5 ve MI6, kısa sürede mütevazı başlangıçlardan profesyonel ve etkili istihbarat teşkilatları haline geldi. Kaptan (daha sonra Tümgeneral) Vernon Kell tarafından kurulan MI5, I. Dünya Savaşı'nın başlangıcında İngiltere'deki Alman istihbarat ajanlarının çoğunun yakalanmasında merkezi bir rol oynamıştır (Hope, 2008). Birinci Dünya Savaşından hemen sonraki yıllar, savaş sonrası maliyet düşürmenin bir sonucu olarak MI5'in boyutunun büyük ölçüde azaldığını görülmüştür. Hizmetini varlığı bir süreliğine tehdit altına girsede 1930'ların başında Birleşik Krallıktaki komünist ve faşist yıkıma karşı koymada yeniden önem kazanmıştı. Ayrıca Sovyet casusluğuna karşı koymada ve Nazi Almanya'sı hakkında bilgi edinmede öncü bir rol oynadı. İkinci Dünya Savaşı sırasında, Güvenlik Servisi düşman casusluğuyla mücadelede, Alman iletişimini kesmede ve yanlış bilgileri Almanya'ya geri göndermede kilit rol oynamıştır. İkinci Dünya Savaşı, Avrupa'nın dönemin iki süper gücü olan ABD ve Sovyetler Birliği arasında bölünmesiyle sona erdi. Komünizmin yayılması ve Sovyet casusluğu, Soğuk Savaş sırasında kilit

kaygıydı ve 1970'lerden itibaren terörizm de ulusal güvenlik için ciddi bir tehdit olarak ortaya çıktı. Soğuk Savaş sona ererken, Kuzey İrlanda ve Kaddafi'nin Libya'sı gibi devletlerden gelen terörist tehditler MI5'in öncelikleri haline geldi (MI5 Security Service, 2022).

MI6 istihbarat örgütünün ise 1909'dan itibaren ve savaş boyunca 'Dış İstihbarat Servisi', 'Gizli Servis', 'Özel İstihbarat Servisi' ve hatta 'C'nin örgütü' gibi çeşitli isimleri vardı. Ancak, 1920 civarında, Gizli İstihbarat Servisi (SIS-MI6) unvanı kabul edilmiştir. Savaş boyunca, özellikle de MI5 (Güvenlik Servisi) ile örgütsel bir bağlantı kurulması gerektiğinde yaygın olarak kullanıldı. 'MI6' yıllar önce resmen kullanılmamasına rağmen, birçok yazar ve gazeteci tanımlamak için kullanmaya devam etmektedir. MI6 faaliyetlerine ilişkin resmi faaliyetlerin açıklanması 1949'da bittiğinden daha fazla bilgi olmamakla beraber MI5 ile yakın çalıştıkları bilinmektedir (Secret Intelligence Service, 2022).

İngiltere bilinen ilk kurumsal anlamda istihbarat örgütünü kurmasına rağmen, diğer ülkelerle kıyaslandığında gerek literatür bakımından gerekse kurumların incelenen internet sayfalarına bakıldığında hakkında en az bilgi veren ülke konumundadır. En bilinen örgütleri MI6 ve MI5 olsa da İngiltere'de farklı istihbarat örgütleri de vardır. Bunlardan biri 1919 yılında Alastair Denniston liderliğinde kurulmuş olan Government Code and Cypher School (GCveCS) olup şimdiki bilinen adı ise Government Communication Headquarter (GCHQ) olan ve aşağıdaki amaçlarla kurulmuş olan istihbarat teşkilatıdır. Bu amaçlar terörle mücadele etmek (Birleşik Krallık'a denizaşırı ülkelerden gelebilecek terör saldırılarını durdurmak), siber güvenliği sağlamak (Birleşik Krallık'ı çevrimiçi yaşamak ve iş yapmak için en güvenli yer haline getirmek), stratejik avantaj sağlamak (düşman devletlerden gelen tehditleri yönetmek, Birleşik Krallık'ın refahını desteklemek ve uluslararası ortamı şekillendirmek), ciddi ve organize suçların azaltılması ve savunmaya destek sağlamaktır (GCHQ, 2023b).

GCHQ özellikle I. Dünya savaşından sonra gelişen sinyal istihbaratının geliştirilmesi için kurulan bir teşkilat olup, iç istihbaratla ilgilenen MI5 ve Dış istihbaratla görevli SIS(MI6) ile birlikte Joint Intelligence Comitee'ye bağlılardır (West, 2014, s. 4). 1936'da kurulan bu örgüt başta güvenlik, savunma ve dışişleri alanlarında olmak üzere

ulusal çıkarlar açısından önem taşıyan hem taktik hem de stratejik konulara bakan değerlendirmelerden ve istihbarat brifinglerinden sorumludur. JIC başkanı özellikle komitenin bu alanlardaki doğrudan ve dolaylı tehditlerin gelişimini izlemesini ve erken uyarı vermesini sağlamakla görevlidir. Ayrıca hükümet bakanlarına ve üst düzey yetkililere operasyonel, planlama ya da politika eylemi gerektiren değerlendirmeler sunarlar. GCHQ ve MI5 istihbaratı bu brifinglere ve değerlendirmelere katkıda bulunur (GCHQ, 2023a).

Sivil tarafta yukarıda bahsi geçen üç ayrı kurumla devam eden İngiliz İstihbaratı, askeri tarafta ise farklı alanlara ayrılmış ve hepsinin farklı görevleri olan istihbarat yapılanmalarıyla ön plana çıkmaktadır. Askeri istihbaratta 'MI1' istihbarat direktörlüğü iken, 'MI2' Avrupa'yla, 'MI3' Almanya'yla, 'MI4' Orta Doğu ile, 'MO5' gelecek durumları ve planları tahmin etmeyle, 'MO12' Hindistanla, ilgilenmektedir (West, 2014, s. 4). İngiliz istihbaratı hem sivil alandaki hem askeri alandaki yapılanmalarıyla diğer ülkelerden daha farklı bir istihbarat örgütlenmesine sahiptir denilebilir.

2.3.2. İsviçre istihbarat örgütleri

İngiltere'den sonra ikinci olarak istihbaratı kurumsallaştıran ülke İsviçre'dir. 1848 yılında NDB'yi (Nachrichtendienst des Bundes) kuran ülke, daha sonra ikinci bir istihbarat servisi olan ve askeri istihbaratla ilgilenen MND (Militärischer Nachrichtendienst)'yi hayata geçirmiştir. NDB, Savunma Bakanlığı'na bağlı olmakla beraber, dış ve iç belirleyicisi olan sivil bir entegre istihbarat servisidir. Buradan da anlaşılacağı üzere hem kendi topraklarında hem de yurtdışında faaliyet göstermektedir. NDB örgütü aynı zamanda FIS (Federal Intelligence Service) olarak da bilinmektedir (Butorac, Miličević & Solomun, 2020). FIS, terörizmin, şiddet içeren aşırılığın, casusluğun, kitle imha silahlarının yayılmasının ve bunların dağıtım sistemi teknolojisinin yanı sıra kritik altyapıya karşı siber saldırıların erken algılanması ve önlenmesi ile ilgilenir. Ayrıca FIS, güvenlik politikası ile ilgili bilgileri yurt dışından alır ve değerlendirir. Bu şekilde, tehdit durumunun kapsamlı bir şekilde değerlendirilmesine kararlı bir şekilde katkıda bulunur. FIS'in önleyici faaliyeti, kolluk kuvvetlerinin baskıcı rolünden açıkça ayırt edilmelidir. FIS bir kolluk kuvveti değildir. Temel görevleri, siyasi liderler adına önleme ve durum değerlendirmesidir (VBS, 2022). İngiltere gibi bu ülke de

hem iç hem dış alanlarda istihbarat faaliyetlerini yürütmekte ve aynı zamanda askeri yapılanmadaki istihbarat faaliyetlerini de MND (Militärischer Nachrichtendienst) adındaki teşkilatla yürütmektedir.

FIS kuruluş amaçlarına baktığımızda temel hedefinin güvenlik olduğu görülmektedir. Politik, ekonomik ve savunma alanlarındaki hedefleriyle öne çıkmasının dışında, aşırılığa, teröre, siber tehditlere, yasal olmayan istihbarata ve olası çoğalma hareketlerine karşı da tedbirler almakla görevlidir. Bu alanlardaki faaliyetlerini göstermek amaçlı “Durum Radarı”nı oluşturmuşlar ve tehditleri olabilecek alanlara göre ayırmışlardır. Buna göre tehdit kaynakları; politik, çoğalma (üreme), yasal olmayan istihbarat, siber uzay tehditleri, terör, aşırıcılar olarak gösterilmiştir (FIS, 2022) .

11 Eylül saldırılarından sonra dünyada değişen istihbaratın önemiyle beraber İsviçre’de 2015 yılında yeni bir yasa çıkarmıştır. Yeni yasa siyasi ve adli makamlardan izin alınması durumunda İsviçre Federal İstihbarat Servisi'nin arabaları ve otel odalarını aramasına, insanları durdurmasına ve sorgulamasına, insanların görev yerlerine müdahale etmesine, özel alanlara gözetim teknolojisi kurmasına, belirli kelimeleri aramak için kabloları dokunmasına ve hedefli siber saldırılar başlatmasına izin verilebileceğini içermektedir. Ayrıca bu yetkinin sınırlı olmamasına karşı siyasiler en fazla yılda 12 kere kullanılacağına izin vermiştir (Guitton, 2017). Bu durumdan da anlaşılmaktadır ki İsviçre istihbarat anlamındaki yetkilerini genişlettiği FIS’e güvenini de arttırmıştır.

2.3.3. Çin devleti istihbarat örgütleri

1949 yılında kurulan Çin, o günden bugüne büyüyen bir ülke olarak hayatına devam etmiş, yirmi yıllık reformların ardından dünya ekonomisinin en önemli güçlerinden biri haline gelmiştir (Gündal, 2015). 20. yüzyılda en dikkat çekici ülkelerden biri Çin’dir. Bunun nedeni 1970’den sonra yönetimi devralan Deng Xiaoping döneminde başlayan dışa açılım politikası olmuştur. Dış ticaretin önem kazanmasıyla Çin 50 yılı aşkın süredir aralıksız büyüyen bir ekonomiye sahip olmuştur (Yılmaz İ. , 2005, s. 77).

Çin Halk Cumhuriyeti bağımsızlığını kazanıp dünya çapında ün kazanmadan önceden beri istihbarat faaliyetleriyle ön plana çıkmıştır. Bu tezin ilk bölümünde de belirtildiği üzere, Sun Tzu’nun 6.yy da yazdığı “Savaş Sanatı” adlı kitapla bahsedilen

istihbaratın zamanında ve doğru olmasını öneminin, Hunlarla aralarındaki casusluk faaliyetlerine kadar uzandığı görülmektedir.

Modern istihbarat anlamında Çin istihbaratı konusunda çok fazla kaynak bulunmamakla beraber, Çin istihbaratının babası olarak gösterilen ve Çin Milliyetçi Partisi sosyal işler bölüm başkanı olan Chiang Kai-Shek Çin istihbaratının kurumsal anlamında temelini attığı bilinmektedir (Stratfor Global Intelligence, 2010, s. 2). Çin istihbaratı askeri ve sivil olmak üzere iki alana ayrılmıştır. Ancak diğer ülkelerden farklı olarak bu ikisinin de bağlı olduğu ve tek elden raporlama yapabilen bir resmi makam yoktur (Feakin, 2013, s. 2). Bu yüzden kararlar verilmeden önce yöneticilerin kafa karışıklığı yaşaması muhtemeldir

Çin istihbarat yapısı sivil ve askeri olarak yapılanmalar olarak ikiye ayrılmıştır. Sivil kanatta MSS ve MPS olarak yani devlet güvenlik bakanlığı ve kamu güvenliği bakanlığı olarak iki ayrı kuruluş görülmektedir. MSS'in faaliyet alanları, karşı istihbarat, karşı casusluk, iç ve dış istihbarat olarak görülürken; MPS'in görev alanları ise ulusal politika yapıcı, iç istihbarat, devlet için ticari ürünleri sertifikalatma olarak özetlenebilir. Her ne kadar bu iki yapının ortak görevi olarak gözüксе de, MSS daha çok dış istihbarattan sorumlu iken, MPS daha çok iç istihbarattan sorumludur (Stratfor Global Intelligence, 2010, s. 5). Askeri kanatta ise Genel Kurmay Başkanlığı istihbarat bürosu (Intelligence Bureau of the Joint Staff Department) bulunmaktadır(Mattis, 2015).

Çin dünyanın en kalabalık ülkelerinden biri olduğundan insan kaynaklı (İNİST) istihbaratın oldukça ön plana çıktığı bir devlet olmasına rağmen, gelişen dünyadaki dijitalleşmeyle beraber buradaki gücünü siber alandaki saldırıları önlemek amacıyla kullanmaya başlamıştır (Mattis ve Brazil, 2019) . MPS daha çok iç istihbaratla ilgilendiği için bu alandaki faaliyetlere askeri istihbarat ve MSS odaklanmıştır. Kamuoyu tarafından bilinen en büyük siber saldırıları ise Taiwan ve ABD'ye karşı olmuş her iki ülkeden de önemli bilgiler elde edilmiştir (Mattis & Brazil, 2019). Bu iki ülkenin de güçleri dikkate alındığında Çin Halk Cumhuriyetinin sadece insan istihbaratında değil siber istihbaratta da oldukça ilerleyip dünya liderine bile karşı durabileceği görülmektedir.

2.3.4. Amerikan istihbarat örgütleri

Modern ve kurumsal anlamda ABD'de gerek sivil gerekse askeri olarak istihbarat

anlayışının oluşması Birinci Dünya Savaşı dönemine rast gelmektedir. Bu dönemde ABD Dışişleri Bakanlığı aracılığı ile diğer ülkelerle de ortak istihbarat çalışmaları yapıldığı görülmektedir (Warner, 2014, s.57-58). 1947 yılında kurulan CIA ve iç istihbarat faaliyetleri için kurulan FBI, ABD deyince akla ilk gelen istihbarat kuruluşlarıdır. ABD'deki istihbarat faaliyetlerinde toplam 18 adet istihbarat kuruluşu bulunmakta ve bunların birbirleriyle bağlantılı olarak çalıştığı bilinmektedir. Bu 18 örgütün toplam haline "İstihbarat Toplumu" denmekte ve bu alanda on binlerce insan istihdam edilmektedir. Bu topluluklar üç ana başlık altında düşünüldüğünde CIA örgütünün tamamen bağımsız olduğu diğerlerinin ise Savunma Bakanlığı'na bağlı ya da diğer bakanlıklara bağlı alt istihbarat kurumları olduğu görülmektedir (Yılmaz S., 2013). ABD Başkanı Harry Truman tarafından Sovyetler Birliği ve yeni ortaya çıkan Çin Devletinin faaliyetlerini araştırmak amaçlı CIA kurulmuştur. FBI iç güvenlik ve kanunların uygulanmasından sorumlu iken CIA sadece bilgi toplama ve düşmanlara karşı casusluk yapmakla görevlidir. Ancak hem CIA için hem de FBI için en büyük felaket 11 Eylül saldırılarının öngörülememesidir. Bu saldırıların üzerine Amerikan Kongresi 2004 yılında yeni bir yapılandırma ile ODNI (Office of the Director of National Intelligence) kurumunu kurmuş ve FBI ve CIA dâhil tüm 18 istihbarat örgütünü bu kuruma bağlamıştır. ABD' de faaliyet gösteren ve bilinen diğer istihbarat kuruluşlarının isimleri ise; Ulusal İstihbarat Direktörü Ofisi (ODNI) ve Merkezi İstihbarat Teşkilatı (CIA); Savunma İstihbarat Teşkilatı (DIA), Ulusal Güvenlik Ajansı (NSA), Ulusal Coğrafi İstihbarat Teşkilatı (NGA), Ulusal Keşif Ofisi (NRO) ve beş Savunma Bakanlığı hizmetinin istihbarat unsurları; Ordu, Donanma, Deniz Piyadeleri, Hava Kuvvetleri ve Uzay Gücü. Enerji Bakanlığı'nın İstihbarat ve Karşı İstihbarat Dairesi; İç Güvenlik Bakanlığı'nın İstihbarat ve Analiz Ofisi ve ABD Sahil Güvenlik İstihbaratı; Adalet Bakanlığı'nın Federal Soruşturma Bürosu ve Uyuşturucu Uygulama Ajansı'nın Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Güvenlik İstihbarat Dairesi; Ulusal Dışişleri

Bakanlığı İstihbarat ve Araştırma Bürosu; ve Hazine Bakanlığı İstihbarat ve Analiz Dairesi'dir (DNI, 2023).

2.3.5. Rus istihbarat örgütleri

16. y.y.'da kurulan Rus polis teşkilatı istihbarat alanındaki ilk hareketleridir ve tarih boyunca kurdukları istihbarat örgütlerinin yaptıkları sadistçe sayılabilecek hareketlerden dolayı insanların gözünde oluşturdukları kötü düşünceleri yok etmek için kurumların sık sık isim değişikliği yaptıkları bilinmektedir. 1880'li yıllarda Okhrana adını alan bu örgüt 1917 yılında Çeka olarak devam etmiş ancak gene yayılan kötü şöhretinden ötürü 1922 yılında GPU, 1924'de OGPU, 1934 yılında NKVD, 1941 senesinde NKVD'ye destek amaçlı NKGB faaliyete başlamış 1946 yılında ise NKGB'nin ismi değiştirilerek KGB (Komitet Gosudarstvennoy Bezopasnosti) olmuştur (Atay, 2002). Resmî adı Devlet Güvenlik Komitesi olan KGB, 1954 yılında Kruşçev döneminde kurulmuştur. Temeli 1917 yılında atılan KGB'nin üç kısımdan oluştuğu bilinmektedir. Bunlar; askeri alanlar, bilimsel ve kültürel alanlar ile ekonomik alanlar olarak sıralanabilir (Duramaz & Gökbnar, 2017). KGB, Ruslar için devlet güvenliğinin korumanın yanı sıra karşı casusluk faaliyetlerini de üstlenmiştir. KGB'de çalışan istihbarat personeli pek çok farklı sektöre ve ülkelere dağılarak bu görevi yerine getirmeye çalışmaktadır. Sadece personeliyle değil aynı zamanda Rusya Bilimler Akademisine bağlı enstitülerde kendisine bilgi kaynağı olarak kullanmakta ve bu enstitüler aracılığıyla Dünyadaki diğer bilim insanlarının neler yaptıklarına da rahatça ulaşmaktadır (Atay, 2002).

KGB'nin tüm Batı Avrupa ülkelerinde faaliyet gösterdiğine inanılmaktadır. Sovyet Büyükelçiliği çalışanlarının yarısı, Aeroflot gibi havayollarının çalışanları, iş adamları, askeri ataşeler, kültür komiserleri, teknik ve tarım uzmanları KGB ve Sovyet Askeri İstihbarat Servisi (GRU) adına faaliyetler yürütmüşlerdir (Atay, 2002). Amacı batıda hassas olarak kabul edilen kurumların içine sızmak ve izlemek, onların ticari faaliyetlerini ve eğitim kurumlarını izlemek, kiliselere ve gençlik örgütlerine katılmak, komünist devrimci bir atmosferin refahını ve gelişmesini sağlamaktır. Diğer sorumluluklar arasında, uluslararası posta ve telgraf iletişimlerini takip etmek için stratejik pozisyonlara katılmak ve buradan belirli konularda bilgi sağlamak yer almaktadır (Andrew ve Mithrokhin, 2001, s.52).

72 yıllık varlığının ardından 1991 yılında yıkılan SSCB'nin yerine kurulan Rusya Federasyonu (Bulut, 2014) döneminde de istihbarat faaliyetleri önemini koruyarak devam ettirmiştir. Sovyetler Birliğinin yıkılmasıyla dağılan KGB yerine Rus Federal Güvenlik Servisi (FSB), Rus İstihbarat Servisi (SVR), Rus Askeri İstihbarat Direktörlüğü (GRU) kurulmuş, FSB ve SVR Rusya Devlet Başkanı'na direkt bağlıyken GRU ise ordunun emrine verilmiştir (Darıcılı & Özdal, 2017). SVR Rusya'nın öncelikle sivil işler için kurulmuş dış istihbarat teşkilatıdır. SVR, KGB Birinci Genel Müdürlüğü (PGU) organizasyonunun halefidir. GRU'nun eşdeğeri olan askeri casuslukta birlikte yakın bir şekilde çalışırlar. SVR'nin merkezi Moskova'nın Yasenevo semtindedir. Rusya Federal Güvenlik Servisi'nin (FSB) aksine, SVR Rusya Federasyonu dışındaki istihbarat ve casusluktan sorumludur. SVR, askeri ve ekonomik casusluk dahil olmak üzere her türlü casusluğu yürütmek ve yurtdışında elektronik gözetim yapmakla görevlidir (Aydın A. , 2020).

Ruslar sadece sivil alanda değil askeri alanda da bir istihbarat servisine sahiptir. Rusya Federasyonu Askerî İstihbarat Birimi (GRU) 1918 yılından bu yana faaliyetlerini sürdüren istihbarat örgütüdür. Ancak sadece askeri alanda değil sivil alanda da faaliyet gösterebilmektedir. Örneğin, 2016 yılındaki ABD başkanlık seçimlerinde de bu örgütün Trump ve yönetimini destekleyerek seçime hile karıştırdıkları iddia edilmişti (Smith, 2018, s. 7). Anlaşıldığı üzere sadece iç istihbarat da değil dış istihbaratta da oldukça güçlü olan Rusya, Sovyetler Birliği'nin yıkılmasında ve sonrasında da istihbarat servislerinin gücünden bir şey kaybetmemiştir.

2.3.6. Fransız istihbarat örgütleri

1914'te I. Dünya Savaşı başladığında, Fransa dünyanın en yetenekli ve iyi organize edilmiş gizli servislerinden birine sahipti. Faaliyetlerin odak noktası Fransa'nın devlet sınırlarının dışındaydı. Soğuk Savaş ve dekolonizasyon döneminde yavaş yavaş dış gizli servisler yeniden yaratıldı (Jager, 2009, s. 35-36).

1982 yılında kurulan Fransa'nın dış istihbarat kurumu olan DGSE (Direction générale de la Sécurité extérieure), ABD'nin CIA'yi durumunda olup; aynı zamanda ABD'nin FBI'yi olarak görülebilecek DGSI (Direction Générale de la Sécurité Intérieure) kurumuyla beraber çalışmaktadır. DGSI, İçişleri Bakanlığı'nın yetkisi altındaki Fransız

özel istihbarat servsidir. Ulusal düzeyde ve tüm Fransız topraklarında kurulmuş, ulusal güvenlik veya Ulusun temel çıkarları ile ilgili istihbaratı araştırmaktan, merkezileştirmekten ve kullanmaktan sorumludur (DGSI, 2022). DGSE ekonomik istihbarat açısından dünyanın en iyilerinden biri olarak görülmektedir (Keck, 2014). DGSE'nin görevlerinden başlıcaları ise eylemlerine ışık tutmak için hükümete güvenilir istihbarat getirmek, ulusal toprakların dışında, Fransa'yı ve Fransız vatandaşlarını hedef alan tehditleri tespit etmek ve engellemek, yurtdışında ulusal çıkarları politik, ekonomik ve güvenlik düzeylerinde teşvik etmek ve korumak olarak özetlenebilir (DGSE, 2022a). DGSE'nin yapılanması incelendiğinde beş ayrı başkanlıkta toplandığı ve bunların yönetim, operasyon, istihbarat, teknik ve strateji olarak ayrıldıkları görülmektedir (DGSE, 2022a).

Fransız istihbarat servisleri de sadece iç ve dış olmak üzer iki adet değil, aynı Amerika'da görülen sistemdeki gibi birden fazladır. Bunlar; DRSD (Defence Intelligence and Security Directorate), DRM (Directorate of Military Intelligence), DNRED (National Directorate of Customs Intelligence and Investigations), TRACFIN (Intelligence Processing and Action Against Illegal Financial Circuits) örgütleridir. Aynı zamanda Fransa'da bir istihbarat Akademisi bulunmakta olup tüm bu merkezlere eleman yetiştirmekle görevlidir (DGSE, 2022b).

2.3.7. Alman istihbarat örgütleri

Almanya'da da birden çok istihbarat teşkilatı bulunmaktadır. Bunlar; Federal İstihbarat Servisi (BND), Federal Anayasayı Koruma Teşkilatı (BFV), Anayasayı Koruma Teşkilatı, Enformasyon Teknolojisi Güvenliği Federal Teşkilatı, Federal Silahlı Kuvvetler İstihbarat Teşkilatı, Askeri Güvenlik Servisi (MAD)'dir (Acar, 2019). BND dış istihbaratla ilgilenen bir kurum olup oldukça güçlü teknolojik altyapıya sahiptir. BND diğer tüm istihbarat birimleriyle ortaklaşa çalışmaktadır (BND, 2022). Federal İstihbarat Servisi, Almanya'nın dış gizli servsidir ve doğrudan Şansölye'ye bağlıdır. 1956'da kurulan, Federal Almanya Cumhuriyeti'nin resmi dış istihbarat teşkilatı olan BND, Soğuk Savaş sırasında NATO'ya katılmıştır ve CIA ile yakın işbirliği içinde çalışmaktadır. Merkezi Berlin'de bulunan, dünyanın en büyük istihbarat merkezidir. BND'nin Almanya ve yurt dışında 300 şubesi bulunmaktadır. 2016 yılında yaklaşık 6.500 kişi istihdam

edilmiştir. Askeri Bilimler Bakanlığı tarafından resmi olarak görevlendirilen bir asker. BND, Almanya'nın en büyük istihbarat teşkilatıdır. Ülkeyi birçok suikast girişiminden kurtardığı bilinmektedir. (Aydın A. , 2020).

BND'nin köklerine baktığımızda II. Dünya Savaşı'na inilmesi gerekir. Adolf Hitler döneminde ki Almanya, Sovyetler Birliği hakkında ellerinden geldiği kadar bilgi toplama yarışındaydılar (Schiel, 2003, s. 12). Bunun için Nazilerden oluşan bir grup, FHO (Foreign Armies Eat) adlı teşkilatı kurmuşlardır. Bu grup gerek askeriye de gerekse sivildeki geniş kaynaklarıyla Sovyetler Birliği hakkında bilgi toplamaya başlamıştır. Her alanda toplayabildikleri bilgilerle birlikte Almanya'nın Sovyetlere karşı üstünlük kazanmasında büyük rol oynamışlardır. Reinhard Gehlen tarafından yönetilen FHO'nun sonunda Hitler'in sahip olduğu güçlü orduyu yenemeyeceğini görmüştür. 1944 yılında Gehlen, Sovyetlerle ilgili bulduğu bütün bilgileri çelik bir kutuya koyarak Alp Dağlarına gömmüştür. 1945 yılında ise Amerikalılar tarafından yakalanarak cezaevine atılmıştır. Ancak Amerikalıların bu bilgileri merak edeceğini bilen Gehlen bir anlaşma yaparak altı hafta sonra cezaevinden tahliye edilmiştir. Gehlen bir anlaşma yaparak casusluk faaliyetlerine devam etmesi karşılığında, Sovyetler hakkında bildiği her şeyi anlatacağını söylemiş, Amerikalılar da bunu üzerine 1946 dan itibaren Gehlen Organizasyonu adı altında casusluk faaliyetlerine devam etmesine izin vermişlerdir (Schiel, 2003, s. 12-18). Kısacası BND'nin kökeni olan Gehlen organizasyonu Amerika tarafından desteklenmiş ve Sovyetler hakkında birçok istihbarat toplayarak zamanında oldukça yararlı bir örgüt olmuştur. 1956 yılından sonra BND olarak devam eden organizasyon dünyanın en büyük istihbarat merkezi olma özelliğini korumaktadır (Aydın A. , 2020).

2.4. Geleneksel İstihbarattan Modern İstihbarata Geçiş Süreci

19. y.y.'a bakıldığında ulaşım ve teknolojik alanlarda oldukça ciddi gelişmelerin olduğu görülmektedir. 1840'lı yıllarda bulunan telgraf sistemi, buharlı trenler ve gemiler ve 1876'da Graham Bell tarafından bulunan telefonla beraber birçok alanda gelişmeler olmuştur. Özellikle telefon ve telgrafın bulunması uzun mesafelerden kısa sürede haberlerin ulaşmasına neden olduğundan bilgi akışını kolaylaştırmıştır. İngiliz ve Fransız istihbaratı bu sayede gelişmeye başlamıştır (Richelson, 1995, s. 3-4). Sadece telekomünikasyon alanında değil aynı zamanda uyduların ortaya çıkması ve hava

araçlarının çok daha fazla işlevli kullanılmasıyla beraber; klasik istihbaratta görülen insan odaklı yaklaşımın dışında teknoloji devreye girmiş ve doğal olarak çok daha fazla bilgi ve belgeye daha kolay ulaşılması sağlanmıştır.

Klasik istihbarattan, modern istihbarat geçişteki en büyük adımlardan biri ise istihbarat faaliyetlerinin kurumsallaştırılmasıdır. Dünya’da bu dönem Soğuk Savaş yıllarında daha belirgin hale gelmiştir (Rathmell, 2002). Değişen teknoloji ve insan kapasitesiyle beraber geçmiş dönem istihbarat anlayışını modern dönemdeki istihbarat anlayışıyla genel olarak kıyasladığımızda birçok fark vardır diyebiliriz. Modern öncesi dediğimiz teknolojinin gelişmesinden önceki dönem ile ve sonrası yani teknolojinin gelişmeye başladığı dönem istihbaratlarına bakıldığında özellikle bilgi kaynaklarında sadece insani istihbarat değil artık teknolojinin de etkisiyle ortaya çıkan yeni istihbarat türleri ve açık kaynakların da önemini arttırdığını görebilmekteyiz. İstihbarat faaliyetlerinin en önemli özelliklerinden biri olan güvenilirlik kısmında ise, modern istihbarata geçiş öncesi olarak görülen 20. yy öncesi dönemde kısmen doğruluğunu kontrol etmek daha zorken, 20. yy sonrasında ise gelişen istihbarat kaynaklarıyla beraber daha güvenilir istihbarat toplanmaya başlanmıştır denilebilir. İstihbaratın temel ilkelerinden bir diğeri olan süratle elde edilebilirlik kısmına baktığımızda da modern çağdaki istihbaratın çok daha hızlı olduğu görülebilmektedir. Aynı zamanda artan uluslararası ilişkilerdeki diplomatik ilişkilerle istihbarat bu dönemde daha çok önem kazanmış ve istihbarat örgütü yapılanmaları daha profesyonel bir hale gelmiştir. Genel olarak istihbarat çarkını oluşturan dört temel aşama olan tespit, toplama, işleme ve dağıtım aşamaları değişmemesine rağmen, gelişen teknolojiyle birlikte bilgiye erişim kolaylığı sağlayan bilgisayar kullanımı, daha önce ihtiyaç olan yoğun insan gücünün kullanılmasını da sınırlamıştır. Kısaca denilebilir ki; modern çağın istihbarat alanına en büyük kazancı teknolojinin gelişmesiyle birlikte gerçekleşen kaynak artışı olmuştur (Erhan, 2002).

BÖLÜM 3: İSTİHBARAT VE ULUSLARASI İLİŞKİLER

3.1. İstihbaratın Dış Politika Yapımı ve Uluslararası İlişkilere Etkisi

İstihbaratın gelişimsel olarak tarihini ve çeşitli ulusların istihbarat örgütlenmelerini incelediğimiz önceki bölümlerde, istihbarat tarihinin oldukça eskiye dayandığını görebilmekteyiz. İnsanlar toplu halde yaşamaya başladıklarında ise istihbaratın sadece savunma ve saldırı amaçlı değil aynı zamanda korunma ve önlem alma amaçlı da kullanmaya başlamışlardır. Buradan da anlaşılabilir üzere, istihbarat, insanların devlet düzenini kurduktan sonra bu devletlerarasındaki ilişkileri de olumlu ya da olumsuz olarak etkilemektedir. Devletlerarası ilişkilerin sebeplerini ve buna bağlı olan sonuçlarını inceleyen uluslararası ilişkiler kuramının doğum tarihi olarak 1648'deki Westphalia Antlaşması kabul edilebilir (Serdar, 2015). Bu anlaşma ulusal devlet egemenliği ilkesini hak olarak tanımıştır (TUIC, 2014). Ulus devlet kavramının temellerinin atıldığı bu antlaşmadan sonra bu fikrin savunucuları da kavramın gittikçe ortaya daha net çıkıp şekillenmesini sağlamışlardır. Bu fikrin savunucularından biri olan Kenneth Waltz'a göre oluşabilecek bir sürü sebepten kaynaklı devletlerarası savaşlar kaçınılmazdır (Karabulut & Değer, 2015). Bundan kaçınmak isteyen devletler için ise güç önemli olduğundan, güç sürekli geliştirilmeli ve artırılmalıdır (UPA, 2019). Buradan da anlaşılabilir üzere, hangi devletlerin ne kadar güçlü oldukları ya da olmadıkları ancak onlar hakkında iç ve dış araştırmalar yapılarak bulunabilir. İstihbarat olgusu da burada önem kazanmaktadır. Çünkü bu güç dengesini sabit tutabilmek için gerekli olan bilgi toplama ve bu bilgileri zamanında kullanmak oldukça önemlidir.

Uluslararası ilişkilerin temel aktörü devletlerdir (Özdemir H. , 2008, s. 128). Uluslararası ilişkiler disiplini; devletlerin diğer devletlerle, uluslararası/bölgesel/hükümetler arası kuruluşlarla, ulus ötesi şirketlerle, uluslararası normlarla ve uluslararası toplumla ilişkilerini inceleyen disiplinler arası bir konudur. Devletleri yönetenler değiştikçe onların dış politikaları da değişeceğinden, dinamik bir yapıya sahiptir. İkinci Dünya Savaşı'ndan sonra ABD öncülüğünde bir liberal dünya düzeni kurulmuştur (Kurtbağ, 2020). Ancak Dünya, 11 Eylül saldırılarına kadar ABD'nin tavrı değiştirerek farklı bir politikaya geçebileceğini öngörememiştir. En büyük istihbarat hatalarından biri olarak gösterilen ve onlarca insanın ölüm ve yaralanmalarıyla sonuçlanan

bu saldırılardan sonra Dünya'nın hem politik anlamda düzeni hem de istihbarat alanında düzeni deđişmiştir. 11 Eylül sonrası dönem başkanı George Bush liberal düzendeki "özgürlük" kavramını hiçe sayarak terörle savaş adı altında Afganistan ve Irak'a saldırmış ve kendi liderliğinde devam eden liberal düzenin artık kalmadığını düşündürmüştür (Duncombe & Dunne, 2018). ABD'nin ulus devlet çıkarlarını ön plana attığı bu dönem tam olarak bitmeden çıkan Covid-19 salgını bu sefer tüm devletlerin ulus devlet mantığındaki realizm politikasına geçtiğini göstermektedir. İleriki bölümlerde detaylandırılacak olan bu iki olay, aslında istihbarat ve uluslararası ilişkilerin birbirleriyle ne kadar ilişkili olduğunun birer göstergesidir.

İstihbarat servisinde çalışanlar dış politika yapıcılara adeta bir rehber görevi görürler (Lowenthal, 2006, s.7). İstihbarat analizcileri, elde ettikleri bilgileri anlamlı bir bütün haline getirerek onlara ulusal güvenliği sağlamak açısından bir anlam kazandırır. Ancak burada birçok insan tarafından yanlış anlaşılan konu ise, istihbaratın elindeki bir anlık verilerle tahmin yaptığını zannetmektir. İstihbaratın asıl amacı, tüm parametrelerin istatistiki bir deđerlendirmeye tutularak hipotezleri ortaya çıkarmak, olası sonuçları öngörerek bunların üzerinden tahminlerde bulunmaktır (Gookins, 2008). Yani istihbarat sadece anlık bilgileri düşünerek hareket etmez, tüm bilgileri sentezleyerek kullanır ve doğru sonuçlar çıkarmaya odaklanır. Bu yüzden istihbarat çalışanları ve yaptıkları analizler politika yapıcılar için oldukça önemlidir. Politika yapıcılar derken kastedilen şey, politik kararlar alınırken etkileyen ya da bizzat karar veren anlamına gelmektedir (Lowenthal, 2006, s.8). Bu anlamda politika yapıcılarının istedikleri istihbaratı toplayan istihbarat birimleri üreticiler olarak görülebilirken, politika yapıcılar ise müşteri olarak görülebilir. Ancak tıpkı üretici ve müşteri arasındaki ilişkiler gibi bu alanda da iletişim sorunları yaşanabilir. Politika yapıcısı önce istediklerini doğru bir şekilde ifade etmelidir ki istihbarat toplamada doğru kaynaklar kullanılabilirsin. Ancak, günümüz koşullarında özellikle açık kaynak istihbaratın gelişen teknolojiyle gittikçe kolay ulaşılabilen bir hal almasıyla beraber, politika yapıcılar kendi analizlerini kendileri yapabileceğini düşünmektedirler. Ancak doğru analiz yapabilme ve doğrulanmış kaynaklardan bilgi elde edebilmek gibi bilgiyi kullanılabilir hale getiren istihbarat analistlerinin ve güvenilir istihbaratın önemini göz ardı edebilmektedir (Center For The Study of Intelligence , 2004, s. 2). Sharman Kent tarafından 1949 yılında yazılan "Strategic Intelligence for American

World Politics” adlı eserde bu konuya değinmiş ve istihbarat toplayan analistler ile politika yapıcı arasındaki ilişkinin çok kopuk ya da çok sıkı olmaması gerektiğini, olduğu takdirde çözüm yeteneklerinin her iki taraf tarafından da kaybedilebileceğinin altını çizmiştir (1949, s.180-206). Bu yüzdendir ki, politika yapıcıların anlık kararlar almamaları ve bunu istihbarat birimlerine sorarak daha detaylı bilgilendirilmeleri önemlidir.

İstihbarat, karar vericiler için gerekli bilgilerin edinilmesini, değerlendirilmesini ve analizini vurgulayan bir süreç olarak da tanımlanabilir (Kent, 2003). İstihbarat, dış politikanın belirlenmesinde ayrılmaz bir unsurdur (Süpürgeci, 2021). Dış politika ve güvenlik denkleminde yalnızca bilgi erişimi olarak değil, aynı zamanda bilginin yeniden üretilmesi ve yapılandırılması yoluyla daha fazla işlevsellik katar. İstihbarat teşkilatları ve dış politika ilişkilerinin tarihsel analizine bakıldığında, istihbaratın dış politika etkinliğini sağlamadaki önemi II. Dünya Savaşı'na kadar sınırlı kaldığı görülebilir. Bununla birlikte, uluslararası politikadaki olay ve olguların geçmişe göre daha fazla devlet temelli etkileşimler sağlamasından sonra, bilginin yoğun bir şekilde işlenmesi ve kullanılması, dünya siyasetinde devlet eylemi için önemli çıkarımlara sahiptir. Bilgi faktörünün artması ve ülkeler arasındaki diplomatik ilişkilerin gelişmesi, istihbarat ve dış politikayı koordine etme kavramının önünü açmıştır.

Dış siyaset konseptinin tatbik ve faaliyet oranının tatmin edici değerler alabilmesi için dış siyaset konseptinin danışma ve askeri argümanlarla desteklenmesinin icap ettiğini devletler geçmiş yüzyılın sonlarındaki olaylardan edinmiş olduğu tecrübeler aracılığıyla anlamış durumdadırlar. Bu tecrübelerden elde edilen bilgiler ışığında, dış politika ve istihbaratın birbirlerini etkilediği sonucuna ulaşılabilir. Bu nedenle, belirli olayların süreçlerini ve genel durumu idrak etme açısından sınıflandırılması istihbarat teşkilatlarından beklenmektedir (Ireland, 2017).

Dış politikanın etkinliğini sağlamak için istihbaratın kilit unsurlarından biri olan politika yapıcıların, özellikle dış politika ve ulusal güvenlik alanında izlenecek adımlara destek ve rehberlik etmesi önemlidir. Karataş'ında dediği gibi (Karataş, 2017, s.33):

Devletin dış politika ve ulusal güvenliği açısından ihtiyaç duyulan rakip ve düşman devletlerin ajanları ve diğer varlıkları hakkında bilgilerin toplanması ve işleminden geçirilmesi, dış politikanın uygulanmasını kolaylaştırmaya yardımcı olacak örtülü

faaliyetlerin yürütülmesi ve resmi olmayan girişimlere karşı hem istihbarat sürecinin hem de istihbarat ürününün korunmasını içeren gizli devlet faaliyetleri olarak değerlendirmek mümkündür.

Soğuk Savaş döneminin bitmesiyle başlayan süreçte, ortaya çıkan küreselleşmeyle beraber bilgi kullanımının ne kadar önemli olduğu da ortaya çıkmıştır (Ingram, 1998). Bilginin temelini haber almakla başladığı düşünüldüğünde istihbaratın ne kadar önem kazandığı görülebilir. Bunun yanında, dış siyaset ve haber alma faaliyetleri birbirine destek sunar özellikle olduğundan dış siyaset etkinliğinin arttırılabileceği düşünülmektedir. Fakat iyi bir haber alma teşkilatı her vakit iyi bir dış siyaset vaat etmeyebilir; ama kötü bir haber alma teşkilatı kötü bir dış politikaya sebep olabilmektedir.

İstihbarat toplamakla yükümlü olan istihbarat teşkilatlarına da önemli görevler düşmektedir. Resmi olarak ilk kurulan istihbarat teşkilatları Birinci Dünya Savaşı'ndan sonra görülmeye başlamış, istihbarat sadece askeri alanda değil ekonomik, sosyal ve politik anlamda da önem arz etmeye başlamıştır (Acar, 2019). Alınan doğru ve güvenilir istihbaratlarla, ulusal güvenlik anlamında doğru adımlar atılabilir, savaşlar önlenebilir, terör saldırıları durdurulabilir hatta 2019 yılından bu zamana yaşadığımız pandemi süreci bile bu kadar uzatılmadan bitirilebilirdi.

İstihbaratın doğru ve güvenilir olması da uluslararası ilişkileri oldukça etkileyen bir kavramdır. Amerika'nın Irak işgalinin sebebi CIA tarafından sağlanan ve Irak'ta bulunduğu söylenen kimyasal kitle imha silahlarının olduğuna dair istihbarat olmasına rağmen bu silahlar bulunamamış ve ABD başkanı istihbarat hatası olduğunu kabul etmiştir (Acar, 2019). Bu savaş sadece Amerika-Irak arasında gibi gözükse de Amerika'nın diğer ülkelerle ilişkisini sarsmıştır. Fransa ve Almanya'nın başını çektiği ülkeler ABD'nin Irak'a müdahalesinin yersiz olduğu konusunda eleştirilerde bulundular ve liberal dünya düzeninin de sorgulanmasına neden olmuştur (Özdikmenli & Ovalı, 2008).

İstihbarat ve uluslararası kuruluşlar arasındaki ilişki, güvenlik ve siyasi kuruluşlara özgü değildir. Dünya Bankası ve Uluslararası Para Fonu (IMF) gibi uluslararası kuruluşların kendi alanlarında ülkeler, uluslararası sorunlar ve küresel trendler hakkında bilgi ve istihbarat topladıkları görülmektedir. Nitekim istihbarat servislerinin ulusal ve uluslararası finans ve kredi kuruluşlarının teşkilatlarında var olduğu bilinmektedir. Örneğin IMF, Dünya Bankası, Avrupa Birliği ve OECD gibi uluslararası kuruluşların mali

suçlarla (kara para aklama, yolsuzluk, tefecilik, yolsuzluk v.b.) mücadele etmek amaçlı faaliyetleri olduğu bilinmektedir (Yüce & Akkaya, 2020). Bu suçları engellemek için de doğru istihbarat kaynaklarını kullanmak önemlidir. Bunlar ve benzeri diğer uluslararası kuruluşların yürüttüğü bilgi toplama ve istihbarat üretimi, askeri operasyonlar ve dış politika kararları için gerekli olanlardan farklı olsa da, nihai olarak bankacılık işlemlerini yürütmek için gereklidir, gizlidir ve amaca yönelik bir süreçten geçer (Erol & Bingöl, 2012). Sonuç itibarıyla sadece siyasi anlamda değil istihbarat aynı zamanda ekonomi alanında da önemli olup, ekonomik kararlar aynı zamanda uluslararası politikada da alınabilecek kararlarda etkili olabilmektedir.

21. yüzyılla beraber askeri alandan çıkarak ekonomik ve sosyal alanlarda da görülen istihbarat faaliyetleri, aslında sadece dış politika yapıcılarının değil aynı zamanda uluslararası oyuncuların da dahil olduğu bir sektör haline gelmiştir. Örneğin NATO kuruluşu ele alınabilir. Brüksel’de bulunan merkezinde neredeyse tüm birimlerinde istihbarat birimleri oluşturulmuş ve klasik terörizmden, siber terörizme hatta ülkelerin sosyal ve ekonomik yapılarındaki değişikliklere kadar araştıran birimler yardımıyla, sadece geleneksel askeri alandaki bilgiler dışında uluslararası ilişkilerin alanındaki problemler ve konular hakkında istihbarat toparlayarak NATO’nun karar mekanizmalarını doğrudan etkileyen bilgiler paylaşmaktadır (Erol ve Bingöl, 2012). Aynı zamanda yaygınlaşan stratejik araştırma merkezleri de uluslararası ilişkilerin istihbaratla ne kadar bağlı olduğunu gösteren kuruluşlardır. Bunlara örnek olarak STRATFOR verilebilir. Bu kuruluş dünyayı yedi alana bölerek bu alandaki tüm bilgileri gerek ekonomik gerekse sosyal olsun bir arada açıklamaktadır. Bu bölümler: Amerika, Asya-Pasifik, Avrupa, Orta Asya ve Kuzey Afrika, Güney Asya, Sahra Altı Afrika ve Avrasya olarak sıralanır (Stratfor, 2023). STRATFOR hazırladığı internet sitesiyle açık kaynak türüne bir örnek olup, bu sitede Dünyanın her yerinde neler olduğunu, ekonomik, siyasal ve askeri alanlardaki gelişmeleri bir araya getirerek kişilerin ve kurumların bilgisine sunmaktadır. Burada yazılan bilgiler eşliğinde karar alma mekanizmaları hangi ülkelerle iş birliği yapabileceği ya da hangi gelişmelerin kendilerini doğrudan etkileyebileceği konusunda istihbarat toplayarak uluslararası arenada işbirlikçilerini seçebilmektedirler. Bir diğer taraftan Avrupa devletlerinin yaşayabileceği tehditlerde siyasi faaliyet ve diyalog kurmakla görevli resmi tüzel bir kişiliği olmayan bir yapı olan Avrupa Güvenlik

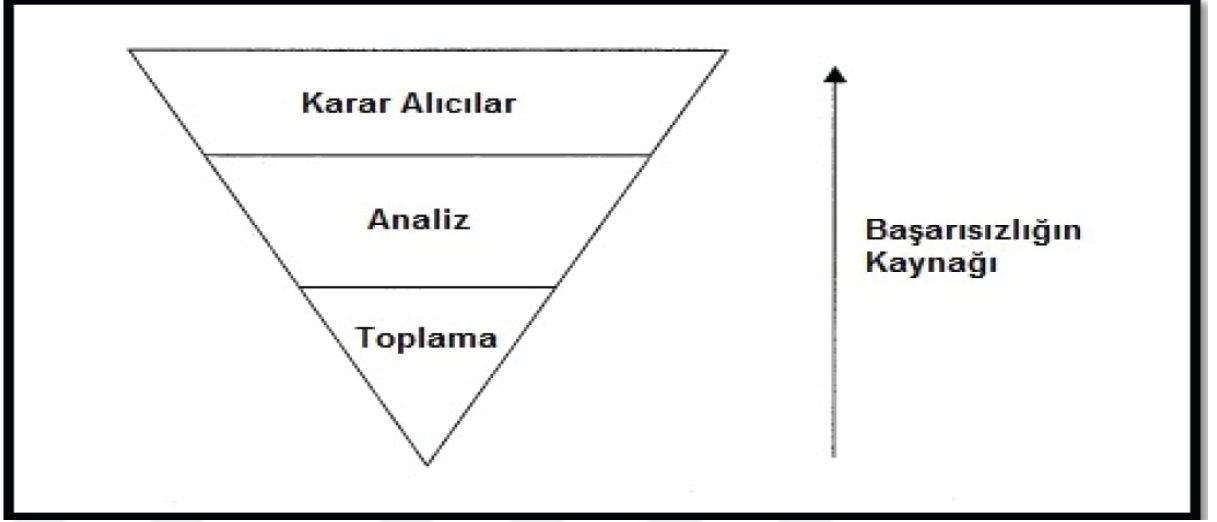
ve İş Birliği teşkilatı (HaberTürk, 2023) içerisinde de istihbarat birimleri olduğu bilinmektedir. Rusya bu teşkilatı kendi birliklerinin konumlarını Ukrayna askeri savaş gücüyle paylaştığını iddia etmiş ancak bunun karşılığında herhangi bir kanıt sunamamıştır (Reuters, 2022). Buradan da anlaşılabilir olduğu üzere, ülkeler herhangi bir savaş anında uluslararası kuruluşları da burada taraf olmakla suçlayabilmekte ve buralara üye olan devletlere de savaş bayraklarını çekebilecek kadar ileri derecede siyasi kararlara girebilmektedir. Sonuç itibarıyla, istihbarat ve uluslararası ilişkiler birbirleriyle hem doğrudan hem de dolaylı yönden alakalıdır. Uluslararası arenada hem dış politika da hem de karar alma süreçlerinde doğrudan etkili olan istihbarat, sadece askeri alanda değil artık sivil alanda da kullanılmakta ve ekonomik alanları ve sosyal hayatı kapsayan geniş bir alan olarak karşımıza çıkmaktadır.

3.2. İstihbarat Başarısızlığı ve Uluslararası İlişkiler

3.2.1 Başarısız istihbarat tanımı ve nedenleri

Müşteri ve üretici arasındaki ilişkiye benzettiğimiz karar alıcılar ve istihbarat analizcilerinin arasındaki ilişkide kopukluk olduğunda alınacak kararların yanlış olabileme ihtimali oldukça yükselecektir. Bu durumda karşımıza “başarısız istihbarat” kavramı çıkması kaçınılmazdır. İstihbarat başarısızlığı, istihbarat çarkının toplama, yorumlama ve analiz etme, üretme ve dağıtma aşamalarından birinin veya birkaçının, ulusal çıkarları ilgilendiren bir konu veya olay hakkında zamanında ve doğru bilgi üretememesidir (Lowenthal, 2000, s.5).

Şekil-8’den de görülebileceği üzere aslında başarısızlığın asıl kaynağı karar alıcılar dediğimiz politikacılarıdır. Ancak bu diğer aşamalarda da başarısızlığa düşülmeyecektir anlamına gelmemelidir. Çünkü istihbarat çarkında bilgi toplamada yapılan bir hata, tüm çarkın işleyişini bozacağı için yapılacak olan analiz de doğru olmayacak ve karar alıcılar yanlış karar verebileceklerdir. Ancak Gill ve Phtiyen’a göre başarısızlığın ana kaynağı bilgi toplama ya da analiz aşamasında değil bunları kullanarak karar veren karar alıcılar kısmında olmaktadır (2006, s.105).



Şekil 8: Başarısız İstihbaratın Kaynağı

Kaynak: (Bulut, 2017)

Merkezi İstihbarat Teşkilatı'nda deneyimli bir istihbarat analisti olan John Hedley'e göre, "İstihbarat başarısızlıklarının incelenmesi belki de istihbarat çalışmasında akademik olarak en gelişmiş alandır" (2005, s.437). Bu, istihbarat başarısızlığı çalışmasında üç ana perspektife bakıldığında kesinlikle doğrudur. İlk ikisi, istihbarat organizasyonunun rolünü ve politika yapıcılarının ve istihbarat analistlerinin bilişsel inançlarını vurgulamaktadır. Buna karşılık, üçüncüsü güvenlik ve istihbarat kurumlarının operasyonel performansını vurgulamaktadır.

Büyük istihbarat başarısızlıkları genellikle toplama başarısızlıklarından değil, analiz başarısızlıklarından kaynaklanır. Çünkü geçerli bir zihinsel modele veya zihniyete uymadığı için ilgili bilgiler göz ardı edilebilir ya da reddedilebilir (Brady, 1993). Buradan istihbarat toplanırken yararlanılan bir harita olan istihbarat çarkındaki basamaklardaki en zor basamağın analiz aşaması olduğu anlaşılmaktadır. Bir dönem ABD Senatosu'nun istihbarat reformu Kilise Komitesi'nin bir personeli olarak görev yapan Loch Johnson, başarısızlığı açıklamak için istihbaratın döngüsel sürecine odaklanmıştır ve ona göre istihbarat döngüsünün her adımında, planlama ve yönlendirmeden toplama, işleme, analiz ve yaymaya kadar zayıflıklar vardır (2006, s.116). Yani sıkıntı organizasyonel alandaki eksikliklerdir. Johnson'ın teorisini takiben, istihbarat çarkında dört olası istihbarat başarısızlığı türü vardır. Bunlar aşağıda tartışılmaktadır (Johnson, 2006, s.118-121);

Planlama ve yönlendirme başarısızlığı

Bu, üst düzey hükümet yetkilileri ve istihbarat müşterileri tarafından iyi tanımlanmış planlama ve yönlendirme eksikliğinden kaynaklanabilir. Buradaki ana problem diyalog eksikliğidir.

Toplama ve işleme başarısızlığı

Veri bolluğundan kaynaklı istihbarat toplayıcıların, zamanında analistlere ellerindeki bilgileri veremediğinden kaynaklı sıkıntılar olabilir.

Analiz başarısızlığı

Johnson, istihbarat analizini, analistin bir bilgi parçasını eyleme geçirilebilir istihbarata dönüştürmek için "iç görüşünü" eklemesini gerektiren istihbarat döngüsünün "kalbi" olarak tanımlar. Mesleki yetersizlik, sınırlı bilgi veya siyasi manipülasyon gibi birkaç faktör zayıf analitik yargıya neden olabilir.

İstihbaratın yayılmasındaki başarısızlık

İstihbarat analistleri, genellikle birbiriyle rekabet eden birden fazla sorunla meşgul olan ulusal güvenlik karar vericilerinin dikkatini çekmede başarısız olabilir. Bu dikkat eksikliğine ek olarak, politika yapımcıların istihbarat raporlarından elde edilen tercih edilen bilgileri "aldatma" eğilimi de yaygınlaştırma başarısızlığına neden olabilir.

Richard Betts'de yaptığı analizde en kritik hataların nadiren ham bilgi toplayıcılar tarafından, ara sıra analizi yapan profesyoneller tarafından ancak çoğunlukla da tüm bu bilgileri elinde tutan karar alıcılar tarafından yapıldığını belirterek Gill ve Phythian'la aynı görüşü paylaşmıştır (Betts, 1978). Richard Heuer ise olaya daha farklı taraftan bakmış ve dört önyargı tanımlamıştır Bunlar; kanıtların değerlendirilmesindeki önyargılar, sebep ve sonuç algısındaki önyargılar, olasılıkları tahmin etmedeki önyargılar, istihbarat raporlamasının değerlendirilmesindeki geriye dönük önyargılardır (1999, s.147-161).

Tüm bu önyargılar bir araya geldiğinde, sadece istihbarat analizcilerinin yeteneklerini kısıtlamakla kalmaz, aynı zamanda stratejik sürprizlere de neden olabilir. Jensen'a göre ise istihbarat başarısızlığı; analist veya analiz ekibinin yaratıcılığının olmaması, analize asılsız varsayımların dahil edilmesi, analiz ekibi içindeki belirli grupların fikirlerinin ısrarla hakimiyeti (grup baskısı), yanlış kanıtlara vurgu, yanlış anlama, olaylar arasındaki yanlış bağlantılar, analitik kaynakların doğrulanması ve ihmalkar ve aldatıcı inkarlar, bir konuya aşırı veya fazla vurgu yapılması vb. gibi

nedenlerden meydana gelebilmektedir (2012, s.264). Bunlardan da anlaşılacağı gibi burada analistin psikolojik durumunun da istihbarat başarısızlığında önemli bir etkidir.

Organizasyonel yani istihbarat çarkındaki hatalardan kaynaklı ve psikolojik yani grup çalışmasından ve kişilerin önyargılarından kaynaklı nedenlerin dışında istihbarat başarısızlığının bir diğer nedeni de operasyonel ya da güvenlik ve istihbarat teşkilatlarının koordineli çalışmaması olarak söylenebilir. Bunun en çarpıcı örneği olarak Pearl Harbour saldırısı gösterilebilir. İleriki bölümde daha detaylı anlatılacak olan bu saldırıda, Elliot Cohen ve John Gooch'a göre sadece istihbarattaki başarısızlık değil aynı zamanda operasyonel bir başarısızlık olmuştur. Çünkü onlara göre, ordu ve donanma arasında oluşan koordinasyon eksikliği gerekli önlemleri almamalarına sebep olmuş ve defansif bir saldırıya karşı hafifletici önlemler almalarını engellemiştir (Cohen & Gooch, 1991, s.142-146) . Bunların dışında da ülkelerin istihbarat hatalarını görmek mümkündür ancak istihbarat örgütleri yaptıkları hataları kolay kolay kabul etmediklerinden, bundan sonraki bölümde kendi hatalarını da kabul ettikleri örnek olaylar sıralanmıştır.

3.2.1. Dünyadaki başarısız istihbaratlara örnekler

Başarısız istihbaratın belli başlı nedenlerini yukarıda açıkladıktan sonra dünya tarihinde yaşanan ve en büyük istihbarat başarısızlığı olarak nitelendirilebilecek olan olayların örnekleri incelenecektir. Bunlardan en bilinen dört tanesini nedenleri ve sonuçlarıyla beraber inceleyecek olup, böylelikle başarısız istihbaratın neden olduğu savaşlar örnekleriyle açıklanmış olacaktır. Bunlar; Pearl Harbour Savaşı, Vietnam Savaşı, 11 Eylül saldırısı ve Irak savaşıdır.

3.2.2.1 Pearl Harbour savaşı

Pearl Harbour saldırısı ABD tarihindeki ciddi istihbarat yanlışlarından biridir. 19. yüzyılın ortaları ve 20. yüzyılın başlarında Japonya, kapalı bir feodal toplumdaki modern bir endüstriyel ve askeri güce dönüşmüştür. 1930'larda, askeri etkiler Japonya'yı bir dizi fetih yapmaya yöneltmiştir. Bu fetihlerin amacı, II. Dünya Savaşı'nın başlamasıyla birlikte Asya'daki Avrupa kolonilerini ele geçirmektir. Bu yayılcı politikaların temel nedeni petrol, kömür, kauçuk ve kalay kaynaklarını ele geçirmektir (Wohlstetter, 1962, s. 50-60). Bu sırada Japonya'nın Amerika Birleşik Devletleri ile

ilişkileri de kötüleşmekteydi. Mevcut sorunlar ABD'nin Pasifik Filosunu 1940 yılının baharında Hawaii'ye taşımasına neden oldu. 1940'tan sonra ABD, Japonya'ya petrol ve diğer savaş malzemeleri sevkiyatını kısıtladı. Bu hareketi ABD ve diğer ülkeler tarafından Japonya'ya karşı daha karmaşık bir ambargo izledi (Mayer, 2002). Aynı zamanda Amerikan istihbaratı bu dönemde çok gizli Japon kodlarını okuyabildiğinden, ABD hayati bilgileri dünyanın her yerindeki Amerikan komutanlarına iletebilecek durumdaydı. Çoğu zaman Washington, Japonya'nın hem diplomatik hamlelerini hem de askeri konuşlandırmalarını tahmin edebiliyordu (Kahn, 1991). Japonya ile müteakip müzakerelere rağmen, 25 Kasım 1941'de Birleşik Devletler yetkilileri Hawaii'ye 32 savaş gemisinden oluşan bir filo da dâhil olmak üzere bir grup ek askeri kuvvet gönderdi. 1941 yılında II. Dünya savaşının en şiddetli çarpışmalarının devam ettiği sırada Japonlar ABD'nin Pearl Harbour Limanındaki donanmasına bir saldırı düzenlemişler ve bunun sonucunda 12 savaş gemisi ciddi hasar almış, 188 savaş uçağı heba olmuş ve 2403 asker ile 68 sivil ölmüştür (Keegan, 2016, s. 258). Japonlar iki dalga halinde yaptıkları saldırıda, ilk yaptıkları dalgada birçok hedefi vurmuş ve bir saat sonra gerçekleştirdikleri ikinci saldırı da ise geri kalan tüm hedeflerini vurmuşlardır (Mueller, 1991). O dönemde daha II. Dünya Savaşına girmemiş olan ABD, gerek halkının baskısıyla gerekse verdiği büyük kaybın acısını çıkartmak maksatlı II. Dünya savaşına dahil olmaya zorunlu kalmıştır (Macksey, 2012). O dönemde de Dünya'nın en güçlü devletlerinden sayılan ABD'nin o zamanlarda on üç adet istihbarat servisi bulunmaktaydı. Taylor ve Goodman'a göre buradaki en büyük problem ise bu kadar çok istihbarat birimi olmasına rağmen aralarındaki koordinasyon eksikliği olmuştur ve bu yaşanan olaydan sonra ABD, tüm bu birimleri merkez bir çatı altına toplayarak CIA'ı kurmuştur (Taylor & Goldman, 2010). Pearl Harbor'daki istihbarat başarısızlıkları, kritik bilgilerden etkin bir şekilde yararlanmak için ne istismar edilen ne de dağıtılan kritik bilgi yakalama alanlarından kaynaklanmıştır. Bunun arkasında belirsiz, çelişkili ve eksik bilgi kaynaklarına dayalı geliştirilmiş istihbaratın etkili kullanılamaması yatmaktadır (Cook, Angus ve Adams, 2004). Bu düşünceyi bu konuda detaylı bir eser yazan Roberta Wohlstetter'da 1962'de çıkarttığı "Pearl Harbor: Warning and Decision" adlı kitabında da savunmuş, buradaki ana istihbarat başarısızlığının nedenini bilgi eksikliği değil, aksine elde olan bilgilerin çeşitli

bürokratik engellerden de kaynaklı olarak doğru yorumlanamaması olarak göstermiştir (Dahl, 2013, s. 30).

Pearl Harbour saldırısı insan istihbaratındaki başarısızlıklara bir örnektir. Amerika Birleşik Devletleri'nin, tarihinin ilk 140 yılı boyunca ABD güvenliğine yönelik neredeyse hiçbir ciddi dış tehdit olmadığı için, zayıf bir istihbarat geleneğine sahip olduğu öne sürülmüştür. Birinci Dünya Savaşı başlayana kadar Birleşik Devletler savunma hazırlıklarını minimumda tutmuştur (Lowenthal, 1984, s.129). Bu duruş nedeniyle, ulusal güvenliğin korunması için istihbarat talep edilmemiştir. Ana fikir, ABD'nin iyi gelişmiş bir istihbarat topluluğuna ihtiyacı olmadığıydı. ABD geride kalırken, dünyanın diğer bölgelerindeki uluslar (özellikle Avrupa), devam eden çatışmalarla başa çıkabilmek için kodların geliştirilmesini ve kırılmasını teşvik etti (Piacine, 1997). Aynı zamanda istihbarat teşkilatları tarafından hazırlanan istihbarat görevlilerine süreklilik ve beceri geliştirme sağlamak için mesleki gelişim programları eksikliği vardı. 1940-1941 yılları arasında sistem, artan operasyonel istihbarat gereksinimlerini karşılamak için yabancı dil uzmanları, alan uzmanları, tüm kaynak analistleri ve kriptanalist ve İNİST uzmanı ile saflarını hızla genişletmek konusunda da bazı sorunlar yaşadı (Piacine, 1997). Pearl Harbour olayında İNİST'in ABD istihbarat topluluğuna neredeyse hiç katkısı olmadı. Bunun ana nedeni, Pearl Harbour saldırısından önce Amerika Birleşik Devletleri'ndeki gizli istihbarat operasyonlarına ve casusluğa karşı genel bir ihmâl tutumu ile ilgiliydi. Amerika Birleşik Devletleri'nin insan istihbarat kaynakları yalnızca diplomatik, askeri ataşe, gözlemci ve karşı istihbarat raporlama sistemlerini içeriyordu, ancak daha fazla istihbarat bilgisi sağlamak için kullanılacak resmi olmayan gizli görevlileri (NOC'ler) veya muhbirleri içermiyordu. NOC'lerin ve istihbarat muhbirlerinin yokluğu, ABD'nin Japonların saldırıdan önce Pearl Harbor ile ilgili niyetlerini gösterebilecek ilgili bilgileri toplama yeteneğini sınırladı (Rusbridger & Nave, 1991, s. 1-16). Saldırıdan önceki dönemde ABD'li karar vericiler mevcut istihbarat kaynaklarına güvenmediler. Bu güven eksikliği en iyi, o sırada ABD'nin Japonya Büyükelçisi olan Joseph C. Grew'in durumuyla örneklendirilebilir. Büyükelçi Grew, Dışişleri Bakanlığı'na bir telgraf göndererek, Japon kuvvetlerinin Pearl Harbour'daki filoya sürpriz bir saldırı düzenleyeceğine dair o sırada Tokyo'da dolaşan bir söylentiden söz etti (Aim Report, 2003). Bu bilgi, saldırı planlayıcılarına yakın olan gizli bir kaynaktan olmaması nedeniyle bu bilgi donanma

istihbarat bölümü tarafından reddedildi. Bilgi, ikinci bir güvenilir istihbarat kaynağı tarafından doğrulanamadı. Japon deniz ve ordu kuvvetlerinin mevcut konumu ve istihdamı hakkında bilinen hiçbir veri yoktu. Öngörülebilir gelecekte Pearl Harbour'a karşı hiçbir hamle yakın veya planlanmış gibi görünmüyordu. Tüm bu güvensizlikler, istihbaratın yanlış yorumlanması ve yanlış konumlandırılan kişiler yüzünden bu saldırı istihbarat hatası olarak tarihe geçen bir olaydır.

Buradaki istihbarat başarısızlığı, tüm dünyanın kaderini etkilemiş ve uluslararası ilişkilerde istihbaratın önemini ortaya koymuştur. Çünkü o zamana kadar savaştan uzak durmak isteyen ve izolasyon politikası izleyen ABD, aldığı bu darbeden ve ağır kayıplardan sonra II. Dünya Savaşına dahil olarak savaşın kaderini değiştirmiştir.

3.2.2.2. Vietnam savaşı

Diğer bir istihbarat başarısızlığı ise Vietnam Savaşında görülmektedir. Çok uzun süre Çin egemenliği altında yaşayan ve zengin yeraltı kaynaklarına sahip olan Vietnam, 1858 yılında Fransa'nın işgaline uğramıştır (Özdek, 1968, s. 17.). 1940 yılında Vietnam'a giren Japonlar, ülkelerinde bağımsızlık isteyen grupları bir araya getirerek "Viet-Minh" savaşçıları oluşturmuşlar (Mutlu, 2001, s. 217). Bu savaşçılar 1954 yılında Vietnam'dan Fransızların çıkmasını sağlamışlardır (Neale ve Tarkan, 2004, s. 105). 1954 yılında on dört devletin katılımıyla toplanan konferansta Vietnam'ın ikiye bölünmesi kabul edilmiş (Özselçuk, 1979, s. 30), Kuzey tarafta Çin desteğiyle komünist bir devlet kurulurken, Güney tarafta ise ABD ve İngiltere destekli bir yönetim başa gelmiştir. ABD komünizmin Asya'ya yayılmasını istemediğinden, Güney Vietnam'a ekonomik ve askeri üstünlükle desteklemiştir (Giap, 1998, s. 229). 1963'de Güney Vietnam'ın lideri olan Diem'in öldürülmesi ve ABD başkanı John F. Kennedy'e düzenlenen suikastla beraber Vietnam politikasında da değişiklikler olmuştur. Yeni başkan olmuş olan Johnson Kuzey Vietnam botlarının ABD destroyerine ateş açtığı iddiasıyla Kuzey Vietnam'ı vurma emri vermiştir (Şimşek M. , 2008). ABD'nin asıl amacı komünizminin yayılmasına engel olmak ve Sovyetler Birliği'nin güçlenmesini durdurmaktı (Arıoğlu, 2012) . Her ne kadar kendi gücünün çok fazla olduğunu düşünse de, ABD 1968'de Kuzey Vietnam'ın "Tet Saldırıları"nda çok ağır kayıplar vermiş ve yenilgiye uğramıştır. Bunun sonucunda askeri bir zaferin kazanılma ihtimalinin olmadığını görerek barış masasına oturmak zorunda

kalmıştır (Arioğlu, 2012). Hükümetin algı ve hesaplamalarının merkezi bir unsuru olan istihbarat değerlendirmesinin, Vietnam Savaşı'nın kökenleri hakkındaki ana akım tartışmalardan neredeyse tamamen uzak kalması dikkat çekicidir. Bazı istisnalar dışında (özellikle Ağustos 1964'teki Tonkin Körfezi olayı sırasında istihbaratın manipüle edildiği iddiası (Hanyok, 2002)) istihbaratın kalitesi ve rolü, savaşın kökenlerine ilişkin genel çalışmalarda nadiren geçici bir referanstan fazlasını alır. Ochiai'ye göre, Vietnam politikası söz konusu olduğunda, düşman niyetleri ve yetenekleriyle ilgili basit bir yanlışlık durumundan ziyade, çatışmanın genel anlayışındaki bilişsel / entelektüel kusurların ve yanıltıcı istihbaratın (abartı, arzulu düşünme, mantıksal sıçramalar ve ayrıntılara yetersiz dikkat gibi) bir karışımıdır (2011, s.9) .

Vietnam Savaşının komutanlarından General Creighton W. Abrams 'İyi olan her şey iyi bir istihbarattan gelir' (Warner, 2010) diyerek aslında savaşın neden Amerika'nın aleyhine döndüğünü anlatmaya çalışmıştır. İstihbaratın operasyonel anlamda kazanılması için 4 şart vardır. Bunlar; operasyon yapılacak alanı tanımak (sosyo-kültürel alanlarını anlamak, diğer toplumlarla ekonomik ilişkilerine ve iletişimlerine bakmak vb gibi), alandaki olası etkilenmeleri belirlemek (arazi analizi, banliyö ve kentsel arazi incelemesi, iletişim hatlarının yerlerinin belirlenmesi vb.), tehditleri değerlendirmek (düşmanı, düşmanın yapabileceklerini, olası güvenlik açıklarını ve komutanların yararlanabileceği fırsatları belirlemek.) ve tehditlerin eylem planlarını belirlemektir (düşmanların hangi kanallardan saldırabilecekleri, hangi tarz silahlar kullanabilecekleri vb.) (Department of the Army, 2007, s. 3-1,3-103).

Bu şartların birçoğunda eksik kalan ABD, Ordu, Deniz Kuvvetleri, Hava Kuvvetleri ve Deniz Piyadeleri gibi (ki bunların birçoğu da onların unsurlarıydı) istihbarat teşkilatları da güçlerini kolektif güçlerini arttırmak için kullanmak yerine çoğu zaman ayrı ve izole kampanyalar yürütmelerine engel olamadı (Warner, 2010). Koordinasyon eksikliği ve operasyon yapılan alanın tam olarak tanınmamasından kaynaklı gelen istihbaratlar doğru analiz edilemedi. Bunların dışında ABD istihbaratının sadece operasyonel sahada değil aynı zamanda net bir merkezi yönlendirmenin olmaması nedeniyle de bu savaşta 3 büyük istihbarat başarısızlığına da imza attığı söylenmektedir. Öncelikle ABD istihbaratı savaşın boyutunu, gücünü, düşmanın savaş düzenini, sızma oranlarını vb. hafife alarak savaşın kapsamını ölçmede başarısız olmuştur. İkinci temel

başarısızlık, ABD istihbaratının düşmanın gücünü, Komünist Parti'yi ve ilgili bürokrasilerini, yani "altyapıyı" ihmal etmesidir. Bu ihmalin sonuçları önemli olmuştur. Müttefiklerin en iyi düşünülmüş planı olan PHOENIX programı (ABD'nin istihbarat koordinasyonunu ve komünist yeraltı örgütlerini tespit edip dağıtmaya yönelik operasyonları geliştirme çabası) hayata geçirilememiştir. Son olarak ise müttefiklerin düşmanın niyetlerini anlamakta sık sık yetersiz kalması, en belirgin olarak da TET saldırısını öngörememeleri, çoğunlukla CIA'in casusluktaki başarısızlığından kaynaklanmıştır (Central Intelligence Agency Collection, 1969).

İstihbarat neyse odur; istihbarat göstergelerini siyasi ya da ideolojik amaçlarla kullanmak, suistimal etmek ya da görmezden gelmek normalde ağır sonuçları olan tehlikeli bir uygulamadır. Bu durum özellikle Tet Saldırısı için geçerli olmuştur. Sonuçta komünistler istihbarat hatalarından dolayı kurtulmuş ve nihai zafere ulaşmışlardır. Kaybeden ABD, zaferle çıkan ise Vietnam olmuştur (Willbanks, 2018). Komünizmin yayılmaması amacıyla girdikleri Vietnam topraklarında, yeterli operasyonel ve stratejik istihbaratı planlayamayan Amerika, dünyadaki güvenini de kaybetmiştir.

3.2.2.3. 11 Eylül saldırıları

Dünyada istihbaratın ne kadar önemli olduğunu kanıtlayan ve CIA, FBI gibi birçok istihbarat teşkilatlarının yapısal değişimlerine neden olan 11 Eylül saldırısında, o tarihe kadar verilen en büyük kayıp yaşandığı kabul edilmektedir (Yılmaz S., 2011). 11 Eylül 2001'de birden fazla sivil uçak kalkıştan kısa bir süre sonra kaçırılmış ve Dünya Ticaret Merkezi ile Pentagon'a çarparak yaklaşık 3.000 kişiyi öldürmüştür (Jackson, 2021). Bu kayıplar Amerikan İç Savaşı'ndan bu yana yaşanan en büyük kayıp olarak kabul edilmektedir (Murphy, 2017, s. 237). 1941 yılındaki Pearl Harbour saldırısından sonra ABD sınırları içerisinde gerçekleşen ikinci saldırı olması açısından oldukça büyük yankı yapmıştır (Yılmaz S., 2011). Bu zorlayıcı vakayla birlikte, Amerikalıların ve dünyanın terörizm ve buna bağlı olarak iç güvenlik hakkındaki düşüncelerinde büyük bir değişiklik olmuş, bununla beraber hem terörizm hem de iç güvenlik konusundaki paradigma değişiklikleri olmuştur. İlk kez bir "küresel terör dalgası" ortaya çıkmaya başlamıştır (Dilmaç & Erkan, 2006, s. 70). Bu dalgaya karşı savaş, Amerika Birleşik Devletleri Başkanı tarafından "Terörle Savaş" olarak adlandırılmıştır. (Bush, 2001). Emniyet

anlayışlarında yeni bir devrin başlangıcı olan bu olay El Kaide terör örgütü tarafından üstlenilmiş, daha sonra da bu örgütün eylemleri artmıştır. Bu yüzden de polis ve istihbarat teşkilatlarının koordineli bir biçimde çalışmasının önemi artmıştır. 11 Eylül saldırısı taktik düzeyde gerçekleştirilirken, stratejik düzeyde yansımaları olmuştur. ABD'nin 11 Eylül saldırılarını engelleyememesi konusunda yapılan hataları inceleyen soruşturma komisyonunun raporuna göre, başarısızlığın temel nedeni istihbarat birimleri arasında iletişim ve koordinasyon eksikliğidir (Özal, 2019, s. 279). Teröristler ‘Asimetrik Savaş’ adı verilen ve oluşturulacak tehdidin nerden nasıl geleceği kestirilemeyen bir taktik izlemektedirler. Bu yüzden de istihbarat oldukça değer kazanmış ve bu savaşa karşı farklı taktikler geliştirmek durumunda kalınmıştır. Aynı zamanda nükleer silah kullanılma tehlikesi de bulunduğu için artık istihbaratın temel amacı bu iki tehlikenin bir araya gelmesini engellemek olmalıdır (Hillsman, 2000).

Tablo 1: 11 Eylül Öncesi El-Kaide'nin ABD'ye Karşı Terör Saldırıları

TERÖR OLAYI TARİHİ	SALDIRI YERİ	SALDIRI SONUÇLARI
23/02/1993	Dünya Ticaret Merkezi	Otopark katında bir kamyonet patlatıldı ve 6 kişi hayatını kaybetti, yüzlerce kişi yaralandı.
25/06/1996	Suudi Arabistan	Hava Kuvvetlerinin Hubar Kulelerine bomba yüklü kamyon ile saldırı yapıldı, 19 kişi hayatını kaybetti, 500 kişiden fazla kişi yaralandı.
07/08/1998	Nairobi, Kenya, Darüsselam ve Tanzanya	Amerikan büyükelçiliklerine bomba yüklü kamyonlarla yapılan saldırılarda, 234 kişi hayatını kaybetti (12'si Amerikan vatandaşı), 5000'den fazla kişi yaralandı.
12/10/2000	Yemen	'USS Cole' gemisine yapılan saldırıda 17 kişi hayatını kaybetti, 39 kişi yaralandı.

Kaynak: (Övet, 2020)

11 Eylül saldırılarında istihbarat hataları arka arkaya gelmiştir. ABD istihbarat topluluğunun dünya gücü olduklarını bilmeleri rahatlığıyla beraber, El-Kaide topluluğunun ne kadar geniş bir alanda olduklarını ve güçlerinin ne kadar çoğaldığını göremedikleri aşikârdır (Friedman G. , 2010, s. 120-136). 11 Eylül'deki olayı tahmin etmesi gereken istihbarat birimleri bu örgütün daha önce 1993'den beri yaptığı saldırıları

dikkate alınmalıydı. Tablo-1’den de görülebileceği üzere 11 Eylül saldırılarından önce dört adet saldırı düzenlenmiş ve bu saldırılarda ki ortak temel gittikçe artan zorluk seviyelerindeki terör atakları olduklarıdır. Burada belirtilen saldırılar sonucunda ABD istihbarat toplulukları 1996 yılından beri ABD’ye savaş açtığı bilinen El-Kaide örgütü ve liderleri Usame Bin Ladin’in 11 Eylül’deki bu saldırıyı planladıklarını tahmin etmeleri gerekmektedir. Ancak bunu görememelerinin başlıca nedeni, Soğuk Savaş’tan da galip çıkan bir ülke olarak kendilerine aşırı bir özgüven duyan siyaset yapıcılar ve istihbarat toplulukları, terörle başarıyla mücadele edebileceklerine inanmış ve yurt içine yönlendirilmeyen istihbarat faaliyetleri bu yöneticilerin önyargılarıyla da birleşince bu saldırı öngörülemeyen hale gelmeleridir. Federal Havacılık Kurumu FBI ve CIA’nin elinde bulunan kara listedeki uçuş engelli kişileri öğrenebilseydi, kaçırılan birden fazla uçakla yapılan bu saldırı önlenebilirdi. Elinde sadece 12 isim olan bu kurum, altmış bin terör nedeniyle takip edilen kişiden haberdar olmadığı için uçak kaçırarak teröriste kalkış izni vermekte sakınca görmemiştir (9/11 Commission Report, 2004, s. 85). İstihbaratın temel görevlerinden biri de ulusal güvenliği sağlamak amacıyla iç ve dış kaynaklı terörü önlemek olduğu düşünüldüğünde, burada yapılan ana hatların sadece önyargı olmadığı aynı zamanda kurumlar arası iletişim eksikliği de olduğu görülmektedir. İstihbarat, terörizmin zararlı boyutlara ulaşmadan engellenmesi için temel basamak olduğundan, burada yapılmış olan bir hata onlarca insanın ölümüyle sonuçlanmıştır.

11 Eylül’ün istihbarat döngüsünde yeri azımsanmayacak kadar fazladır. Küresel terörizm Amerika gibi büyük bir güç tarafından kabul edilmiş ve düşman ülkeler olarak terörü destekleyenler gösterilmiştir (The White House, 2001). Birçok medya kuruluşunda ABD’nin istihbarat hatası olarak yansıtılan bu olay ABD’nin istihbarat yapılına da yeni bir yön vermiş olarak görülmektedir. Pearl Harbour olayındaki gibi burada da ABD bir kez daha bu sürpriz saldırıyı görememiştir. Aynı zamanda bu saldırılar “kamuya açık istihbarat” deyimini ortaya çıkarmıştır. Çünkü bu saldırılarla beraber hükümetler yapabilecekleri her türlü karşı saldırıya temel oluşturmak ve kamuoyu baskısını engellemek amaçlı ellerindeki bilgileri ABD ve İngiltere hükümetleri olmak üzere halka açmışlardır. Öncelikle İngilizler saldırıyı düzenleyen El-Kaide’nin Afganistan bağlantılarını ve Irak hükümetinin elinde bulundurduğu kitle imha silahlarının yerlerini, hemen arkasından da Amerika CIA’nın Irak işgalinden hemen önce hazırladığı kitle imha

silahları ile ilgiyi raporu kamuoyunun erişimine açmıştır (Wark, 2003, s. 8-9) . 11 Eylül saldırılarının önemi sadece ABD için olmamış aynı zamanda dünyadaki küresel güvenlik anlayışını da değiştirmiş ve kendilerine karşı gelebilecek olan tehdit unsurlarının algılanma boyutunu da farklılaştırmıştır (Buzan, 2008, s. 118-119). Aynı zamanda bu tehditler realizmin tekrar gündeme gelmesine neden olmuştur. Çünkü realizme göre insan doğası kötü olduğundan devletler savaşa eğilimlidir (Morgenthau, 1985, s. 32). Realizmin önemli temsilcilerinden Kenneth Waltz devletler birbirlerine karşı şiddete meyilli olduklarından, bazı devletlerin askeri gücünün fazlalığından dolayı diğer devletlerin de buna karşı sürekli tetikte olduklarını söylemektedir (Waltz, 1979, s. 232). Bu yüzden devletler önleyici savaş tekniğini kullanmaya başlamışlardır denilebilir. Buradan da anlaşılacağı üzere eksik istihbarat ve koordinasyon eksikliğinden kaynaklı ortaya çıkan bu saldırılar dünya düzenini değiştirmiş ayrıca gerek ülkelerin istihbarat yapılarını gerekse ülkelerin birbirleriyle olan ilişkilerini kökten değiştirmiştir.

3.2.2.4. Irak savaşı

Başarısız istihbarat örneklerinden biri de Irak Savaşıdır. 11 Eylül saldırılarından hemen sonra dönemin başkanı Bush tarafından yapılan açıklamalarda terörizmin kaynağının bulunarak ortadan kaldırılacağına üstüne basılarak vurgulanmıştır. Hemen arkasından 20 Eylül 2001 tarihli konuşmasında ise bu eylemlerin ardında Suudi kökenli Usame Bin Ladin ve El-kaide örgütünün olduğunu, saldırıların sorumlusunun ise Afganistan'daki Taliban hükümeti olduğunu belirtmiştir (The White House, 2001). Soğuk Savaş döneminde çevreleme taktiği uygulayan ABD, artık terörizme karşı önleyici savaşlar açmakta kararlıdır ve bu Başkan Bush'un doktrininde de açıkça belirtilmiştir (Kayar, 2003, s. 289-291). Çevreleme politikası; ABD'nin Soğuk Savaşın başından beri uyguladığı, SSCB'nin dünya üzerinde artan etkisini sınırlamayı hedefleyen, yayılımcı eğilimlerin durdurulmasının komünizmin yayılmasını engelleyeceğine inanan bir politikadır (Özcan G. , 2019, s. 1). Önleyici savaş ise, saldırıya uğrama tehlikesine karşı, savaş başlamasından önce alınan önlemlerdir (Erkul, 2018, s. 644). Soğuk Savaştan sonra tek egemen güç olarak kalan ABD'nin dönem Başkanı Bush'un doktrini ise 3 temel stratejiyi hedeflemektedir. . Bunlar, terörizm ve zalimlerle mücadele, demokrasinin teşvik edilmesi ve serbest ticaret ve serbest pazarların dünya geneline hakim olunmasına

yardımcı olunmasıdır (Efegil, 2008). Bush Doktrinde yeni bir kavram daha ortaya çıkmış ve önleyici meşru müdafaa kavramı anlatılmıştır. BM sözleşmesinin 51. Maddesine göre meşru müdafaa hakkından bahsedilirken, Irak savaşı sonrası bu hakkın herhangi bir saldırı olmadan kullanılıp kullanılamayacağı tartışmaya açılmıştır (Erkul, 2018). Birleşmiş Milletler Güvenlik Konseyi kararı varsa önleyici meşru müdafaa uluslararası hukuka uygundur görüşü yaygınlaşmıştır (Aksar, 2015, s. 118). Ancak Irak olayında böyle bir karar olmadığından yasal dayanaktan aslında yoksun olan bir harekettir.

Bush doktrini bundan sonra çevreleme politikasını bırakarak direk önleyici savaş mantığında saldırgan bir yapıya geçeceğini beyan etmiştir. 11 Eylül'den sonra 2003 yılında Irak'a karşı başlatılan savaşın temel nedeninin de bu doktrinin ilk maddesinin terörizm kaynağı olarak görülmesidir. ABD burada kitle imha silahları olduğunu ve geliştirilmesinin devam ettiğini beyan ederek kendilerine ve dünya genelinde özgür yaşama aykırı olduğunu iddia ederek Irak'a girmiştir (Aksar, 2015, s. 117). Bu bilgiyi aldıkları kişi ise "güvenilir kaynak" olarak gördükleri ve 2000 yılından beri bilgi aldıkları Iraklı bir sığınmacı olan Rafid El-Cenabi'dir (ABD Senatosu, 2004, s. 148). Bu kişinin dışında aynı zamanda Irak Askeri endüstrisi kurumu başlıklı yazıdaki bazı notlarla bir başka sığınmacı olan ve Irak Ulusal Kongresiyle direk ilişkisi olan bir diğer Iraklıdır. (ABD Senatosu, 2004, s. 150-151). Bilinen gerçeklerden biri de 11 Eylül sonrasında Irak'ı potansiyel düşman olarak gören ABD'nin istihbarat toplamasının sebeplerinden biri kendi önyargılarını doğrulamak olduğudur. Ancak savaşın sonunda görülmüştür ki bu silahların ne şimdi ne de yakın gelecekte Irak'ta üretilmesi ya da muhafazası söz konusu bile değildir (Gray, 2010, s. 618). Buradan da anlaşılmaktadır ki, yanlış istihbarat toplanmış ve politika belirlemek amaçlı değil, kendisine destek bulabilmek ve bilgilerin altını doldurabilmek için istihbarat raporlarını yazdırmış olma ihtimali oldukça fazladır. El-Cenabi bu savaşın ana istihbarat kaynağıdır ve güvenilirliği sorgulanmadan kendisine direk inanıldığından istihbarat çarkı sekteye uğramıştır. ABD Senato İstihbarat Komitesi raporuna göre de buradaki en büyük sıkıntı, istihbarat raporlarının önyargılar üzerine kurulu olduğu ve somut bilgilerle desteklenmemesidir.

Amerika'nın Irak'a karşı uyguladığı yöntem ve sunduğu nedenler de uluslararası hukuk sistemine tamamen aykırıdır (Aksoy, 2016, s. 6). Uluslararası kamuoyu, kitle imha silahlarının varlığının Irak'ın neresinde olduğunu ABD'ye sorarken, İngiltere'de

yayınlanan The Observer Gazetesi, bu konudaki yanlış bilgilendirmeden sorumlu olarak ABD Savunma Bakanlığı içinde kurulan gizli istihbarat servisi Özel Planlar Ofisi (OPS) ile ona bağlı “The Cabal” adlı analiz grubunun sorumlu olduğunu iddia etmiştir (Beden, 2011). ABD’nin bu silahların varlığıyla ilgili istihbarat aldığı CIA’nın baş danışmanı David Kay, ülkede herhangi bir KİS (Kitle İmha Silahları) bulamadıklarını söyleyerek istihbarat hatasını da itiraf etmek zorunda kalmıştır (Milliyet, 2003). Sonuç olarak Irak Savaşı daha önce de bahsedildiği gibi hem yasal dayanaktan yoksundur hem de istihbarat alanında yapılan hatalardan dolayı tarihe ABD aleyhine bir olay olarak geçmiştir.

ABD’nin Irak’a askeri müdahalesi Avrupa tarafından desteklenmemiştir. Soğuk Savaş sonrası ABD öncülüğünde kurulan liberal dünya düzeni bu olayda ABD tarafından hiçe sayıldığından ve aynı zamanda AB, BM ve NATO gibi kuruluşları önemsizleştiren hareketinden dolayı Avrupa’nın desteklediği çok taraflı ulusal düzenden uzaklaşıldığı endişesi ABD’nin bu olayda tek başına kalmasına neden olmuştur. Özellikle Almanya ve Fransa ABD’ye ciddi anlamda karşı durmuşlardır (Özdikmenli & Ovalı, 2008). AB eskiye oranla ABD karşısında neredeyse eşit güç dengesine ulaşmış, gerek para birimleri olan Euro’nun kazandığı ekonomik güçten gerekse uluslararası alanlardaki kuruluşların içlerindeki kazandıkları nüfuzun ve askeri alandaki yükselen güçleriyle beraber uluslararası dengelerde korkusuz duruma gelmiştir (Nye, 2003, s. 36-37). Bu yüzden AB her ne kadar ABD’yi karşısına almasa da bu savaşta ABD’nin gösterdiği tutumdan dolayı artık tek başına hareket edebileceğini öğrenmiştir. Kendi güvenliklerini de sağlamak amaçlı Solona Belgesi olarak bilinen güvenlik stratejilerini 2003 yılında açıklamışlardır. Bu belgeye göre küresel teröre kitle imha silahlarına ve bölgesel çatışmalara karşı AB’nin korunması ve bunun için gerekli adımların beraber atılmasının altını çizmişlerdir. Böylelikle aslında uluslararası ilişkilerde hangi alanlarda müdahale edeceklerinin de bir haritasını çıkarmışlar ve artık ABD’nin tek koruyucu güç olmadığını AB-ABD ortaklığının da önemli olduğunu belirtmeye çalışmışlardır. ABD’nin Irak savaşında yaptığı gibi önleyici savaş politikası yerine, sorunların diplomatik kanallar ve ilişkilerin iyi tutulmasıyla çözülmesi gerektiğine inandıklarını da belirtmişlerdir (Özdikmenli & Ovalı, 2008). Tüm bunlardan hareketle, Avrupa’nın uluslararası platforma kuracağı kuvvetli ilişkilerle önem vereceği, bu yüzden de istihbarat yani bilgi toplama faaliyetlerinin ABD kadar AB’nin de önümüzdeki yıllarda en çok yararlanacağı kaynak

olduğu söylenebilir.

3.3. İstihbaratın Güncel Yönelimleri ve Uluslararası İlişkiler

11 Eylül saldırıları istihbaratın yapısal şekillenmesinde ve öneminin anlanmasında en önemli olay olmuştur denilebilir. Sadece başarısız istihbarat için bir örnek teşkil etmekle kalmamış aynı zamanda yukarı da bahsedildiği gibi ülkelerin istihbarat teşkilat yapılarını da etkilemiştir. Hem istihbarat anlayışını değiştirdiğinden hem de başarısız istihbarata örnek olduğundan yukarıda detaylandırılmış olan bu saldırı istihbaratın aslında dönüm noktasıdır denilebilir. Ancak sadece bu değil aynı zamanda günümüz koşullarında değişime uğrayan dünyamızda istihbaratın öneminin daha belirgin hale gelip daha farklı yapılanma yaşadığı gerçeği de unutulmamalıdır. İkinci bölümde bahsedilen siber istihbaratın önemi giderek artan siber terörizmin önüne geçmede oldukça önemli hale gelmiştir. Özellikle uygulamalarını siber uzay denilen elektronik cihazların birbirine bağlı sistemle ve altyapı aracılığıyla bilgiyi kullandığı operasyonel ağlara aktarmak durumunda kalan ülkeler, bu durumda olabilecek her türlü siber saldırıya da açık hale gelmiştir (Oğuz, Ceyhan & Sağıroğlu, 2015). O yüzden siber alan oldukça önemli hale gelmiştir. Bunun dışında son dönemde yaşanan Covid-19 salgınından sonra da Medikal anlamdaki istihbaratın ne kadar çok ihmal edildiği anlaşılmış olup bu alana daha çok yatırımlar yapılmaya başlamıştır. Bu iki alanda istihbaratın yapılanmasını ve uluslararası ilişkilerin dinamiklerini değiştirdiği için aşağıda daha detaylı olarak incelenecektir.

3.3.1. Siber güvenlik ve siber terörizm

Günümüzde siber uzay; başta siyasi, ekonomik, sosyal ve kültürel olmak üzere pek çok düzeyde etkileşimi içermektedir. Teknoloji ve bilgi alanındaki gelişmeler siber uzayın kapasitesini daha da artırmıştır. Bu konuda yapılabilecekler açısından siber güvenlik doğal olarak çok önemli hale geliyor. Siber ortamlarda yapılan birçok saldırı kötü niyetle düzenlenmekte ve bunlar da birleştikçe ulusal güvenlik sorunu yaratma potansiyeli vardır (Karasoy & Gezici, 2023). Alınabilecek güvenlik önlemleri sayesinde siber tehditler yok edilebileceğinden devletler bunun için nitelikli personel oluşturulması ve altyapı hizmetlerinin sağlanması gibi büyük yatırımlar yaptıkları düşünülmektedir.

Siber güvenlik denilince ilk akla gelen konu siber saldırılar veya tehditlerdir. Siber

sistemleri, ağırları ve kullanıcıları hedef alan doğrudan veya dolaylı zararlı etkenlere siber tehditler; çeşitli araçlar kullanılarak hedeflenen tehditlere ise siber saldırı adı verilir (Bayraktar, 2015, s.82-92). Siber saldırı yöntemleri; bilgi ve veri aldatmacası, truva at (casus yazılım), zararlı yazılımlar, istem dışı alınan e-postalar, sistem güvenliğini kırma (hacking), web sayfası hırsızlığı ve sosyal mühendislik olarak sayılabildiği gibi (Alsay, 2017), gelişen teknolojiyle beraber farklı yöntemlerinde geliştirilebileceği düşünülebilir. Tüm bu yöntemler devletler, gruplar veya kişiler tarafından kullanılabilir. Bazen yalnızca bir bilgisayarı olan kendi kendini yetiştirmiş kişiler ve bazen de devlet destekli bir kuruluş bir siber saldırı başlatabilir.

Siber güvenlik konularının kapsayıcı bir boyutunu yaratmak için, siber mücadelelerin uluslararası sahnede artan etkisini göstermek gerekir. Siber savaş, devletlerarası savaşa ve diğer çatışmalara dönüşmüştür. Bu nedenle siber saldırılar, geleneksel askeri karşılaşmalar ve bağımsız savaşlar için yeni bir alan yaratmıştır (Schimitt, 2012).

Bilgi ve iletişim araçlarının gittikçe gelişip çoğaldığı 21. yy 'da, bu siber saldırıları da içeren siber terörizm ortaya çıkmıştır. Siber terörizm adından da anlaşılacağı gibi, siber alandaki tüm bilgisayar sistemlerindeki bilgileri gayri resmi yollardan elde ederek, kişilere, kurumlara ya da ülkelere, ekonomik ya da fiziksel anlamda zarar verme eğiliminde kullanmak amaçlı yapılan terör saldırılarıdır (Sofaer, Goodman, Cuellar, Drozdova, Elliot, Grove, Lukasik, Putnam & Wilson, 2000). Siber terörizm terimini ilk kullanan Barry Collin, 1980 yılında terimi tanımlarken, bunun bilgisayar teknolojisine duyulan güvensizlik ve teknolojik yoksunluk korkusuna dayandığını açıklamıştır. Siber terörizm, siyasi ve sosyal yetkilileri, bireyleri ve kurumları sindirmek ve bastırmak için devlet kurumlarının bilgisayarlarına, ağ sistemlerine, bilgilerine ve veri tabanlarına yönelik yasa dışı bir tehdit ve yıkıcı saldırdır. Bir saldırının siber terörizm olarak tanımlanabilmesi için kişilere veya mallara yönelik şiddet içermesi ve/veya en azından korkunç hasara yol açması gerektiğinin vurgulanması önemlidir. Bir ülkenin kritik altyapı sistemlerine yönelik bir saldırı, etkisine göre siber terörizm olarak da tanımlanabilir (Sandıklı & Yivciğer, 2004, s.5). Siber terörün hedefi sektörler ise çok farklı olabilir. Finans sektöründen, enerji dağıtım merkezlerine, kamu güvenliğinden, acil servislere, posta dağıtım merkezlerinden sosyal servislere ve birçok alan siber terörün hedefi olabilir

(Seyedi Asl, 2020, s. 333).

Terör örgütlerinin siber saldırılara başvurmalarının en önemli sebeplerinden biri de saldırıyı kimin gerçekleştirdiğini takip emenin zor olmasıdır. Siber saldırı yöntemi gerçek dünyaya göre daha anonim bir ortamda gerçekleştirildiği için saldıran grubun hedef ülkeye ulaşması için gümrük noktalarından ya da hava alanı kontrollerinden geçmesine gerek kalmamaktadır (Gürkaynak & İren 2011, s.267). Her siber saldırı terör amacıyla yapılsa da terör amaçlı yapılan eylemler de daha sonra örnekleriyle anlatılacağı üzere, gerek ülkelere gerek şirketlere oldukça yüksek miktarda hem maddi hem de güvenilirlik açısından zarar verilebilmektedir. Siber terörün ulaşımdan, elektrik dağıtımına; sağlıktan, hukuk sistemine kadar pek çok yere saldırabilme ihtimali vardır.

Siber terör pek çok farklı sektörde olabilmektedir, ancak her saldırı aynı amaç ve kategoride incelenemez. Siber saldırının beş kategori altında toplanabileceği söylenebilir. Bu kategoriler; önemli bilgileri çalmayı amaçlayan saldırı amaçlı siber terör, bilgisayar sistemlerini yok etmeyi amaçlayan tahribat amaçlı korku ve kaos yaratmayı hedefleyen dezenformasyon, çevrim içi çalışan tüm bilgisayarlara saldırı amaçlı çevrim dışı bırakma ve web sitelerini bozma amaçlı tahrif etme olarak özetlenebilir (Erendor, 2020, s.123-124). Beşinde de amaç saldırılan yere zarar vermektir. Siber saldırı diğer terör eylemlerine göre daha az maliyetli olduğundan bu tarz saldırılar gittikçe yaygınlaşmaktadır.

Siber terörizm sadece bir ülkeyi değil aynı anda birçok ülkeyi tehdit edebilecek boyutlara ulaşabilmektedir. Bu da siber terörün amacı ve kimler tarafından desteklendiğine bağlı olarak değişebilmektedir. Siber terörün olay bağlantılarında, eylem ne kadar karmaşıklaşıyorsa o kadar daha fazla hedef çoğalmakta ve o kadar da büyük örgütlenmeler gerektirmektedir (Bayraktar, 2015, s.80). Siber terör propaganda faaliyetleri için, taktiksel ve stratejik eylemleri gerçekleştirmek için kullanılan maliyeti düşük bir örgütsel hareket olarak da özetlenebilir.

Siber saldırılar çok eski yıllara dayanmasa da çok fazla zarar verebilir boyutlara ulaşmışlardır. İlk siber saldırı olarak görülebilecek olay ise Robert Tappan Morris isimli Cornell Üniversitesinde okuyan bir öğrencinin internetin ne kadar büyük olduğunu anlamak amacıyla internette aynı anda kaç bilgisayar olabilir sorusunun cevaplamak için yazmış olduğu program gösterilebilir (Kılıç, 2018). 1988 yılında sadece bir meraktan

böyle bir yazılımı yaparak internette olan tüm bilgisayarlara aynı anda gönderip sunucuların çökmesini sağlayan Morris'in yazılımı terör kapsamında olmasa da o zamanki şartlarda çöken sistemler yüzünden yargılanmış para ve hapis cezası almıştır (Kılıç, 2018). Ancak bundan sonraki saldırılar o kadar masum olmamış milyonlarca dolar zararlara ve kayıplara mal olmuştur. Örneğin 1999 yılında ortaya çıkartılan Melissa virüsü, e-posta yöntemiyle bilgisayarlara sızarak sistemlerin aşırı yüklenmesine sebep olmuş, Microsoft'un da aralarında bulunduğu birçok firmanın sistem ağlarını devre dışı bırakmış 80 milyon doların üzerinde maddi kayba neden olmuştur (MicroDestek, 2021). 2000 yılının Şubat ayında ise 15 yaşındaki Micheal Calce, üniversite kampüs ağlarını ele geçirerek önce Yahoo firmasını arkasından da DELL, E-Bay, CNN ve Amazon firmalarının da kurumsal sunucularını ele geçirip onların da kapanmasını sağlamıştır (Kaspersky, 2020). Belki de siber saldırıların artık çok ciddi boyutlarda olabileceğini tüm dünyaya bu olay göstermiştir. Çünkü bu yaştaki bir çocuk bile bu dev şirketlerin kurumsal yapılarını çökertebiliyorsa çevrimiçi ağlar artık o kadar güvenilir kabul edilmemelidir. Diğer bilinen siber saldırılardan biri de, 2001 yılında ABD-Çin arasında yaşanan siber saldırıdır. 2001 yılında ABD gözetleme uçağı ile Çin hükümetine ait olan savaş uçağı çarpışmış ve bu olay üzerine Çinli bir grup hacker (bilgisayar korsanı) ABD'nin en kritik devlet kurumlarına yani Beyaz Saray'ın kendisinden başlayarak Enerji Bakanlığı ve ABD Hava kuvvetlerine uzanan 1200 siteye aynı anda onlarca bilgisayarlardan saldırı düzenlemişlerdir (Vatis, 2001, s. 8). 2007 yılında Estonya Hükümetine yapılan saldırıya ilk modern siber saldırı olarak görülmektedir (Yeniçağ Gazetesi, 2022). Bu saldırının temelinde Estonyadaki Kızıl Ordu heykelinin kaldırılması olarak gösteren kaynaklar, bu anıtın kaldırılmasından sonra da ülke içi bir karışıklığın da olduğunu; bunu Sovyetler Birliğine hakaret olarak gören Rusya'nın ise bu saldırıyı gerçekleştirip Cumhurbaşkanlığından, gazetelere ve birçok özel ve kamu kurumlarının sitelerine saldırarak Estonya'nın Dünya ile olan bağlantısını kopartıp intikam aldıklarını söylediler de Rusya bunu resmi olarak hiç kabul etmemiştir (BBC Türkçe, 2007). Yahoo'nun 2013'de uğradığı siber saldırıda ise, yaklaşık 3 milyon kullanıcının hesaplarının etkilendiği, şifrelerin çalınmasa da doğum günü, bazı güvenlik sorularının cevapları, telefon numaraları gibi kişisel bilgilerin birçoğu çalınmış; ayrıca bu ortaya çıktıktan sonra da şirketin satış değeri oldukça düşmüştür (Kutsal, 2017).

Siber terör sadece hackerları (bilgisayar korsanları) değil 21. yüzyılda çok popüler bir konu haline gelen yapay zekâyı da kapsamaktadır. Hali hazırda yapay zekânın bir saldırısı olmasa da gelecek günlerde bu zekânın siber alanda nasıl kullanılabileceği ya da hangi amaçla kullanılabileceği bilinmemektedir. Her ne kadar makinelerin zeki davranışlar göstermesi yapay zekâ tanımına girse de bu makinelerde yazılımlar aracılığıyla kullanılmaktadır (Pirim, 2006). Bilinçli hale gelebilmesi için evrim geçirmesi gerektiğine inanılan yapay zekâ kavramı, birçok kişi tarafından dünyayı yakın gelecekte yok edecek buluş olarak görülmektedir (Köroğlu, 2017). Ünlü bilim adamı Stephan Hawking de bu düşünceyi desteklemiş ve dünyanın sonunu yapay zekânın getireceğini söylemiştir (CNN Türk, 2017). Aynı zamanda yazılımlar üzerinden geliştirildiği düşünülürse şu an olmasa bile ileriki zamanlarda yapay zekâ gelecekteki en büyük siber tehlike olabilir.

Siber saldırılar gün geçtikçe daha etkili olabilmektedir. Siber saldırılar gerek bilgi ve para çalmak için gerekse ülkelerin altyapılarını çökertmek için yapılabilmektedir. Sadece belli ülkelere değil her ülkeye saldırı düzenleyebilen bilgisayar korsanları, örneklerden de görülebildiği üzere hayatı felç etme noktalarına kadar ulaşabilmektedirler. Siber terörizmi internet ortamında işlenen diğer suçlardan ayıran temel fark, suçun mağdurunun ülkeyi yöneten devlet olmasıdır ya da bu mağduriyet devlet dışı bir yapı da olsa siyasi nedenlerle mağdur olarak kalmasıdır (Seyedi Asl, 2020). Siber saldırıların ve siber terörün önüne geçilmesi için küresel işbirliğine ihtiyaç olduğu açıktır. Bugüne kadar, siber saldırılarla mücadele etmeyi amaçlayan birkaç kurumla sınırlı sayıda uluslararası anlaşma imzalanmıştır. Avrupa bloğuna yönelik siber saldırılar, Avrupa Birliği ve NATO gibi uluslararası kuruluşları harekete geçirmiş ve siber tehditlere karşı ortak karşılık verilmesi gereğini ortaya çıkarmıştır. Avrupa Konseyi tarafından 23 Kasım 2001 tarihinde düzenlenen siber suçlara karşı yapılan zirve sonrasında kabul edilen metin, bu alandaki ilk uluslararası antlaşmadır (Council of Europe, 2001). Bu anlaşma 2004 yılında yürürlüğe girmiş yirmi iki Avrupa Konseyi üye devleti tarafından imzalanmış ve bilgisayar ortamındaki tüm erişime müdahale, sahtecilik, bilgilere müdahale gibi durumların engellenmesi için tüm devletlerin işbirliği içerisinde olması istenmiştir (Ashmore, 2009, s. 14). AGİT (Avrupa Güvenlik ve İşbirliği Teşkilatı), özellikle üyeleri arasında güvenlik ve işbirliğini teşvik eden ve siber saldırılara karşı önleyici tedbirler alan bir diğer

uluslararası kuruluştur. Estonya ve Litvanya gibi Avrupa ülkelerine yönelik saldırıların ardından grup siber terörizm konusuna daha yakından bakmaya başlamıştır (Ashmore, 2009, s. 15).

Siber saldırıların bu kadar artmasından kaynaklı içerisinde Türkiye'nin de olduğu birçok ülke bunları önleme amaçlı tedbirler almışlardır. Bazı ülkeler sırf bunun için bir kurum kurabildikleri gibi bazıları da mevcut kurumlara bu görevi yüklemişlerdir. Örneğin ABD, Siber Güvenlik ve İletişim Departmanını kurmuş ve bu kuruma acil durumlarda özel sektörle de çalışabilme yetkisini tanımıştır. Almanya'da Federal Bilgi Güvenliği ofisini bu konu için görevlendirerek NATO, Avrupa Birliği, Birleşmiş Milletler gibi kurumların bu konuya karşı ortak çalışması gerekliliğini ön plana çıkarmaktadır (Güleç & Kışman, 2021). Türkiye'de ise siber güvenlik sağlanmak Ulaştırma ve Altyapı Bakanlığına verilmiş, 2012 yılında ilk toplantısını yapan Siber Güvenlik Kurulu oluşturulmuş ve siber saldırılara karşı önlemler alınmaya başlamıştır. (BTK, 2017)

Siber terörizm üzerinde oldukça düşünülmesi gereken bir alan haline gelmiş olup bu yaşananlardan bilgisayarların güvenilirliği konusunda şüpheler de artmıştır. İnsan hayatında kullandığımız birçok şeyde bilgisayar ve siber ağların olduğu düşünülürse, en büyük terör tehlikelerinden biri bu olup, ülkeler de bunun için önlem almaya çalışmaktadır. Siber terörün uluslararası ilişkilere en büyük etkisi yaşamı durdurabilecek sıkıntılar yarattığından dolayı, ülkeleri savaşa götürebilecek potansiyelde oluşudur.

İlk siber silah olarak görülen Stuxnet virüsü (Bağcı & Oral, 2021) siber uzaydan gelen saldırıların gerçek hayatı nasıl etkileyebileceğinin ilk örneğidir. 2010 yılının Haziran ayında İran'daki Natanz uranyum zenginleştirme tesisine saldırı maksadıyla kullanılan bu bilgisayar solucanı, sisteme saldırmak için çevrim içi yollarla tesise sokulmamış, USB ya da hard disk yardımıyla sisteme bulaştırıldığından bu tesiste görevli kişilerden biri tarafından yapıldığı öngörülmektedir (Can, 2014). Burada kullanılan santrifujlerin kontrolünü ele geçirmek maksadıyla yapılan bu virüs, makinelerin 1000 tanesine zarar verip, tesisin beşte birini etkisiz hale getirmiş, bunun yanı sıra yenileme çalışmaları yapılması ve tesisteki makinelerin tüm bu zararlı yazılımdan kurtarılabilmesi için uzun zaman harcanmış olduğundan, İran'daki nükleer çalışmaların iki yıl geriye götürmüştür (Holat, 2021). Uluslararası alanda bu saldırının kim tarafından yapıldığı

bilinmese de, son derece sofistike, saldırgan bir siber araç üretmenin mümkün olduğunu ve faillerin böyle bir saldırıyı gerçekleştirecek kaynaklara sahip olduğunu göstermiştir. Dahası, bu vaka kritik bir altyapının ağını internetten ayırmanın artık yeterli bir güvenlik önlemi olarak kabul edilemeyeceğini göstermiştir. Devletler böyle bir saldırının kurbanı olmamak için harekete geçmeleri gerektiğini fark ettiler. İran gibi bazı devletler siber güvenliğe yatırım yapmaya başlamış ya da yaklaşan bir siber savaş durumunda kabiliyetlerini arttırmak için askeri siber birimler ve/veya merkezler kurmuştur. Bazı devletler de kritik altyapıları kapsayacak ve siber saldırılara yasal olarak karşılık verme kabiliyetlerini güçlendirecek şekilde siber stratejilerini gözden geçirmeye ve güncellemeye başlamıştır (Cavelty, 2012). Bu saldırıda görülen asıl şey ise, siber saldırıların gerçek hayata yansiyabileceğidir. Çünkü burada zarar verilen makinelerdeki nükleer anlamda olabilecek sızıntılar normal yaşamı da etkileyebilecekti. Bu yüzden de bu saldırı ilk siber silah olarak görülmüştür.

Stuxnet saldırısı gelişen teknolojiyle her yerde bilgisayar kullanıldığı için tüm hayatı etkileyebilecek saldırıların düzenlenebileceğinin ilk örneğidir. Buna benzer başka bir örnek olay ise 2015 yılının kış aylarında Ukrayna'da meydana gelmiştir. Ukrayna'da meydana gelen siber saldırıda, ülkenin doğu kısmında yaşayan 80 bin kişi etkilenmiş ve tam olarak 6 saat elektriksiz kalmışlardır ve bu saldırı bir şehrin saatlerce siber saldırıyla elektriksiz bırakılabileceğinin ilk kanıtıdır denilebilir (Erdoğan, 2016). Herhangi bir savaş anında farklı ülkelerin birbirlerine bu yöntemi kullanmaları ve hayatı felce sürüklemeleri birçok elektrik kullanan teçhizatı devre dışı bırakacağından, savaşta büyük avantaj sağlayabilir. Aynı zamanda daha önce bahsedilen örneklerde de olduğu gibi, siber terör amacıyla yapılan saldırılarda birçok bilgi çalınabilmekte maddi ve manevi hasarlar verilebilmektedir. Giderek artan bu siber saldırılara karşı gerek devlet bazında gerekse özel ve kamu sektörü bazında büyük yatırımlar yapıp, siber güvenliği sağlamak amacıyla çeşitli politikalar oluşturulmaya çalışılmaktadır (İstanbul Bilgi Üniversitesi, 2012). Sadece kendi içlerinde değil aynı zamanda devletlerarasında da bu konu ilişkileri etkileyecek boyutlara gelebilmiştir. Bir ülkeye karşı yapılan siber ataklar hangi ülke tarafından desteklendiği ya da nereden yapıldığı belirlenebildiğinden siber güvenlik uluslararası politikayı direkt olarak etkileyebilmekte ve ulusları sıcak çatışmalara sürükleyebilecek kapasiteye ulaşabilmektedir (Güntay, 2018).

Dünyada ortaya çıkan yeni nesil savaş kavramı ile birlikte, daha öncede bahsedildiği gibi amaç sadece askeri alanda değil hükümetlerin kendi içlerinde istikrarsızlığını da sağlamaktır. Doğal olarak güvenlik anlayışı da değişmiş gelişen siber uzay teknolojileriyle beraber siber güvenlikte güvenlik anlayışının tam merkezine yerleşmiştir (Karasoy, 2022b). Siber istihbarat, siber tehditlerle uğraşırken taktik seviyeden stratejik seviyeye karar vericiler için kritik öneme sahiptir. Siber istihbarat, öncelikle bir ülkenin karşılaşılabileceği siber tehditlere karşı durumsal farkındalığı geliştirir. Etkili siber istihbarat, siber tehditlerin oluşturduğu riski azaltır, siber saldırıların etkisini azaltma yeteneğini geliştirir ve siber güvenlik mimarisine ilişkin doğru ve zamanında bilgi, verimli ve uygun maliyetli karar vermeyi sağlar. 21. yüzyılda siber savaş yaklaşımının kaçınılmaz olduğu görüldüğünde karar vericiler tarafından siber istihbarat değerlendirilmeli ve çeşitli ulusların istihbarat birimleri gerekli siber istihbarat araçlarını etkin bir şekilde geliştirmeleri için teşvik edilmeli ve uygulama organize edilmelidir. İstihbarat, gelecekteki siber savaşta aktif bir rol oynayacaktır (Bayraktar, 2015).

Yukarıda bahsi geçen örneklerden yola çıkılacak olursa, siber saldırıların boyutunun her geçen gün daha çok yeri ve kişiyi etkileyebilecek kadar büyük olduğu ve Dünyada ses getirecek kadar güçlü olmaya devam ettiği sonucu bulunabilir. Bu yüzden bu saldırıları önleyebilecek olan siber istihbaratın önemi de gittikçe artmaktadır. Siber istihbarat daha önce de bahsedildiği üzere bilgi teknolojileri bölümünün mevcut ya da olası tehditleri tespit ederek bunların analiz edilip zararlı hale gelmeden engellenmesidir.

Siber güvenlik alanına girdiğimizde ise bir alan daha karşımıza çıkmaktadır; ‘siber tehdit istihbaratı’(STI). STI'nın üç ana unsuru vardır: ilgili, zamanlı ve eyleme geçirilebilir olması. Yalnızca ilgili tehdit verilerinin zamanında toplandığından, analiz edildiğinden ve işlendiğinden ve sonucun karar vermeye yardımcı olacak eyleme geçirilebilir istihbarat üretebildiğinden emin olmak için eksiksiz STI tanımının bu üç unsuru kapsamı gerekir (Abu, Selamat, Ariffin & Yusof, 2018). Literatürde tam olarak tanımlanmış bir hali olmasa da, STI, dikkat ve önlem gerektiren, belirli bir kuruluşa uyarlanmış eyleme geçirilebilir tehdit bilgilerini temsil eder denilebilir. STI, daha hassas savunma stratejileri geliştirmek için belirli bir kuruluşla ilgili tehdit bilgilerini kurtarmak üzere tasarlanmış faaliyetlerden oluşur. Bu bilgiler tehdit türlerini, kaynaklarını, aktörlerini, teknolojilerini ve saldırı vektörlerini içerir (Shin ve Lowry, 2020). Varol siber tehdit istihbaratını, BT

altyapısına ve bu altyapıyı kontrol edenlere dayalı faaliyet iken, siber istihbarat, hedef ne olursa olsun, ulaşabilecek tüm bilgileri toplama ve değerlendirme ve hedefi doğrulama faaliyeti olarak tanımlamıştır (Varol, 2022). Yani siber tehdit istihbaratında toplanan tüm siber istihbarat verileri uzmanlar tarafından değerlendirilmekte ve teknik analize tabi tutulmaktadır. Bu sayede, bireyler, kurumlar veya kuruluşlar için belirsizliği azaltır ve daha hızlı ve daha bilinçli karar vermeyi sağlar (Varol, 2022) . Siber tehdit istihbaratı da siber istihbarat gibi, veri ihlallerini tespit etmede, veri kaybını önlemede, yaratılan olaylara kısa sürede yanıt verilebilmesinde, tehdit ve veri analizi ile bunlardan elde edilen bilgilerin diğer kurumlarla paylaşılması açısından önem taşır (BGA Security, 2019). Buradan da anlaşılabilir ki gelişen teknolojiyle beraber siber istihbaratın içerisinde çıkan bu siber tehdit istihbaratı, daha geniş kitlelerde uygulanabilecek bir saldırıyı önlemede siber istihbarata elde ettiği bilgileri paylaşma yoluyla yardım edebilir. Bu alanda kurum ve kuruluşlara yardımcı olan sivil çalışmacılar mevcut olup, kendilerini bu tarz saldırılardan korumak isteyen şirketler bu uzmanlara başvurabilmektedir.

Neredeyse her kritik sistem bilgi ve iletişim teknolojisine dayanmaktadır. Siber riskler çoğalmaya devam edecek ve kamu ve özel sektördeki kuruluşlar değerli bilgi varlıklarını savunmak ve korumak için harekete geçecektir. Teknolojiye, güvenlik duvarlarına ve saldırı tespit sistemlerine yatırım yapmak yerinde olmakla birlikte tek başına yetersizdir. Diğer pek çok karmaşık güvenlik tehdidinde olduğu gibi istihbarat kilit bir bileşendir. İstihbaratın siber güvenlik misyonunu yönlendirebilmesi için üst düzey yöneticilerin kritik bilgi düzeylerini belirlemeye ve geliştirmeye yardımcı olmaları gerekir. Bu gereksinimler bir yol gösterici olarak kullanıldığında, siber istihbarat işlevi kurumun tehditlerini, güvenlik açıklarını ve potansiyel etkilerini değerlendirecek ve üst düzey liderlere risk ve kaynak kullanımı ile ilgili stratejik kararlar konusunda tavsiyelerde bulunacak şekilde konumlandırılır. Siber istihbarat analistleri, saldırı düzeyindeki değişiklikleri ve kurumun güvenlik açıklarından yararlanma niyet ve kabiliyetine sahip tehdit aktörlerinin faaliyetlerini izleyebilir (Borum, Felker, Kern, Dennesen & Feyes, 2015)

Siber güvenlik alanının çok geniş olması, sürekli gelişmesi, her geçen gün yeni açıklıklar ve zayıflıklar keşfedilmesi bu alanda yaratılabilecek tehlikeleri gittikçe arttırmaktadır. Bir kurum veya kuruluşun zayıflığı, sağlam bir altyapıya sahip olsalar bile

diğer kurumları da saldırılara açık hale getirebilir. Bu nedenle, tüm aktörler arasında koordinasyon ve uluslararası iş birliğinin geliştirilmesi, siber savunma ve siber caydırıcılık için zorunludur (Çakır & Arınmış Uzun, 2021). Her ülke siber güvenlik yatırımlarını arttırmıştır gibi bir genelleme yapılamamakla birlikte siber güvenliğe yatırım yapan ülkelerin teknolojik olarak oldukça gelişmiş olan ülkeler oldukları söylenebilir (Güleç & Kışman, 2021). Bu yüzden siber saldırı neticesinde çıkacak olan bir çatışma iki gelişmiş ülke arasında çıkabileceğinden tüm uluslararası dengeleri bozabilecek kadar büyük olabilecektir.

3.3.2. Medikal istihbarat

Koronavirüs salgını, küresel güvenlikten insan sağlığına kadar devletleri ve toplumları etkileyen tüm alanlarda istihbarat teşkilatlarının kritik rolünü ve önemini bir kez daha vurgulamıştır. Gizli servislerin temel rolü ve beklenen amacı; son derece geniş bir risk ve tehdit yelpazesi için erken farkındalık ve hazırlık yapabilmeleridir. Bu bağlamda 2003 yılında çıkan SARS virüsü, 2012'deki MERS Virüsü ile 2020'de başlayan COVID19 vakaları, bilgi toplamanın tüm disiplinlerinde yetkinlik ve etkililiğe ulaşma ihtiyacını göstermektedir; aynı zamanda "medikal istihbaratın" yükselişini de ortaya çıkarmıştır. Medikal istihbarat aktif bir istihbarat alanı olarak görülmemekle birlikte geliştirilmesi gereken istihbarat alanları arasında yer almaktadır (Seren, 2020b).

Çetinkaya'nın da dediği gibi pandemi ile birlikte hayatımızın içine adapte olan medikal istihbarat kavramı:

Endemik ya da epidemik hastalıkları, halk sağlığı ile ilgili standartları, sağlık hizmetlerinin kalitesini ve ulaşılabilirliğini, Medikal (tıbbi) hizmetleri, sağlık hizmetleri tesislerini, sağlık çalışanlarının durumunu, Bölgeye özgü hastalıkları, bakteri türlerini, böcekleri, mantarları, sporları ve diğer zararlı organizmaları, Yabani hayvan ve bitki hastalıklarını özellikle de insanlara bulaşabilenlerini, Yerel gıda kullanımı ile ilgili sağlık sorunlarını, Kimyasal ve biyolojik ilaçlar ile radyasyonun etkilerini, Operasyon yapılacak alanların irtifa, sıcaklık, soğukluk ve bataklık gibi özelliklerini kapsar (Çetinkaya, 2021).

İlk olarak askeri alanda tanımlanan medikal istihbarat alanı Soğuk Savaş yıllardan sonra birçok istihbarat teşkilatına yayılmış ve bunun için özel birimler kurulmuştur. 1941 yılında ABD'de ordu bünyesinde kurulan medikal istihbarat alt bölümü istihbarat alanını medikal istihbarat kuramıyla tanıştırmıştır (Ünlü, 2020). Daha sonra Amerika'da Savunma İstihbarat Başkanlığına bağlı olarak Ulusal Medikal İstihbarat merkezi sivil

olarak çalışırken Silahlı Kuvvetler Medikal İstihbarat merkezi ise askeri olarak bilgi toplamak amaçlı kurulmuşlar ve diğer birimlerle koordineli çalışmışlardır (Seren, 2020a). Medikal alandaki tehlikeyi ilk fark eden ülke olarak görülebilecek olan ABD, 1989’da bir sahra talimatnamesi yayınlayarak tıbbi tehdit ve medikal istihbaratın ne demek olduğu ve nasıl elde edilebileceği gibi sorulara yanıt aramıştır (Ünlü, 2020).

Medikal istihbarat sadece sağlık alanında kullanılmamakta ayrıca suçluları ortaya çıkarmakta da kullanılabilir. Örneğin CIA, Usame Bin Ladin’in Pakistan’da olduğunu öğrendikten sonra medikal istihbarat birimine hazırlattığı plana göre Abbotabad Bölgesinde sahte bir Hepatit-B aşısı programı başlatmış, böylelikle Usame Bin Ladin’in gerçekten orda olup olmadığını teyidi sağlanmaya çalışmıştır. Bunu da ABD’de ölen Ladin’in kız kardeşiyle aşısı yoluyla elde edecekleri Ladin’in kendi DNA’sını karşılaştırarak yapmak istemişler ancak orada CIA’in bu iş için anlaştığı Pakistanlı doktor yakalanınca istihbarat çalışmaları başarısızlıkla sonuçlanmıştır (Çetinkaya, 2021).

Medikal istihbarat aynı zamanda siber saldırılara karşı olası hastane kargaşalarını engellemek içinde çalışan bir istihbarat türüdür. Örneğin “Wannacry” adı verilen virüs, 2017 yılında 99 ülkede 230.000 bilgisayara bulaşmış, birçok ülkedeki birçok sektöre yollanmıştır. Bu virüsü yayanların amacı bilgisayarlardaki tüm dosyaları elde etmek ve bunları ancak fidye karşılığında sahiplerine geri vermektir (Yılmaz B. , 2020). Tek bir sektörü değil bir çok sektöre saldıran bu virüs türü İngiltere’de sağlık sektörünün kilitlenmesine neden olmuştur (BerQnet, 2023). Çöken sağlık sistemi yüzünden 19.000 hasta randevusu iptal edilmiş ve bu saldırının ülkeye maliyeti 20 milyon sterlin olmuştur (Field, 2018). Bu tarz yapılabilecek saldırılar kamu sağlığını tehdit ettiğinden ulusal güvenlik çatısı altında incelenmekte ve politika yapıcıların kişilerin sağlık bilgilerinin çalınmasını olası biyolojik saldırılara sebep olabileceğinden varsayımın gözden kaçırılması gereken durumlardandır. Medikal istihbarat da bu durumlara karşı hazırlıklı olmak ve alternatif planları devreye almakla görevli bir alandır.

II. Dünya Savaşı’ndan sonra World Health Organization yani Türkçe adıyla bilinen Dünya Sağlık Örgütü, uluslararası sağlık alanında koordinasyonu sağlama amacıyla kurulmuştur (Gediz Oral & Arpazlı Fazlılar, 2019). Dünya Sağlık Örgütü tarafından 11 Mart 2020’de “pandemi” yani küresel salgın olarak nitelendirilen (Güngör,

2020) Covid-19 vakalarıyla beraber dünya düzeni değişime uğramaya başlamıştır. Sadece dünya düzeni değil aynı zamanda istihbarat alanında da öncelikler değişim göstermiştir. Medikal istihbarat özellikle küresel yapı için önemli hale gelmiştir (Bowsher, Milner & Sullivan, 2016). Tablo 2’den de görülebileceği üzere medikal istihbarat kavramı birçok şeyi kapsar. Askeri operasyonlara destek olarak kullanılabilmesi gibi ülke genel veya bazı bölgelere özgü hastalıkları inceleyip durum hakkında kararlar almakta ya da ulaşılabilecek sağlık hizmetlerinin kalitesini belirlemekte de kullanılabilir.

Tablo 2- Medikal İstihbarat Kapsamı

MEDİKAL İSTİHBARAT						
Operasyon yapılacak alanların irtifa, sıcaklık, soğukluk ve bataklık gibi özelliklerini kapsar	Yerel gıda kullanımı ile ilgili sağlık sorunlarını kapsar	Endemik ya da epidemik hastalıkları, halk sağlığı ile ilgili standartları, sağlık hizmetlerinin kalitesini ve ulaşılabilirliğini sağlar	Kimyasal ve biyolojik ilaçlar ile radyasyonun etkilerini inceler	Yabani hayvan ve bitki hastalıklarını özellikle de insanlara bulaşabilenlerini inceler	Bölgeye özgü hastalıkları, bakteri türlerini, böcekleri, mantarları, sporları ve diğer zararlı organizmaları inceler	Medikal (tıbbi) hizmetleri, sağlık hizmetleri tesislerini, sağlık çalışanlarının durumunu kapsar

Kaynak: (Çetinkaya, 2021) alıntılanmıştır.

Dünyada küresel salgın olarak bilinen olaylara genel olarak baktığımızda tarihinin de çok eskilere dayandığı görülebilir. İlk pandemi 1347’de “Kara Veba” ile başlamış ve bulaştığı kişilerin yarısını öldürmüştür (Ersoy, 1996, s. 84). Daha sonra 1817’de kolera salgını görülmüş ve 19. Yüzyılın en ölümcül hastalığı olarak kabul edilmiştir (Artvinli, 2020, s. 48). 1914 yılındaki İspanyol Gribi, 1968 yılında yaşanan Hong Kong gribi gibi salgınlarda dünyada birçok insanın ölümüne neden olmuştur (Tekin, 2021). Buradaki salgın türlerine baktığımızda, art niyetli ülkeler ya da organizasyonların terör amaçlı kullanmak üzere biyolojik silah olarak bu tarz virüsleri geliştirebileceği de öngörülebilmektedir. Medikal istihbarat aynı zamanda bu biyolojik silahların üretimini de

önceden engelleme ve ön görebilme faaliyetlerini de içermektedir.

Korona virüs salgınlarının temeli 2003 yılında Çin’de SARS olarak adlandırılan solunum yollarını etkileyen bir virüsle olmuştur. Bu virüs Dünya çapında 4 ülkede görülmüş ve 8.400 kişiye bulaşmış ancak kısa zamanda kontrol altına alınmıştır (Yılmaz N. , 2021). Bu virüs ve bundan sonra ortaya çıkan salgındaki MERS virüsü de koronavirüs ailesindedir. 2012 yılında Suudi Arabistan’dan yayılmaya başlayan MERS virüsü SARS’tan daha tehlikeli olmuş ve bu hastalığa yakalananların yaklaşık %40’ı hayatını kaybetmiştir (T.C. Sağlık Bakanlığı, 2017). Bu koronavirüs ve türevleri alanlarında neler olduğunu anlayamayan Dünya, medikal istihbaratı çok arka plana ittiği için 2020 yılında ortaya çıkacak olan asıl korona tehlikesini öngörememiştir. 2012 yılında Almanya’da Robert Koch Enstitüsü tarafından müsteşarlıklar ve ordudaki bazı bölümlerin yardımlaşmasıyla yazılan raporda, SARS virüsünün evrim geçirip daha tehlikeli olacağını ve tüm dünyayı etkileyerek binlerce kişinin hayatını kaybedeceğinden bahsedilmesine rağmen (Gülen, 2020) bu alana eğilmeyen Dünya devletleri ve Almanya bunun bedelini COVID-19 virüsü yüzünden ölen binlerce insanla ödemiştir.

Dünyada salgın hastalıklar ve biyolojik tehditler gibi olayların tek muhatabı DSÖ olmamakla birlikte, Avrupa’da Avrupa Hastalıkları Önleme ve Kontrol Merkezi kurulmuş olup halk sağlığını tehdit edebilecek her türlü hastalığa karşı önlem alınmaya çalışılmıştır (ECDC, 2023). Bu da yeterli görülmemiş 2007 yılında Avrupa Komisyonu Medikal İstihbarat servisini kurarak otuz iki farklı dilde haber ve sağlık sitelerini sürekli tarayan bir sistem kurmuştur (European Commission, 2004). Pandemi döneminde bu kuruluşların hiçbirinin tam manasıyla hedefledikleri gibi çalışmadığı ve sistemlerinin çökmesinden kaynaklı ülkelerin paylaşımcılıktan çok sadece kendi iç ihtiyaçlarını karşılamak maksatlı hareket ettikleri görülmektedir.

Pandemi döneminin kanıtladığı en önemli şeylerden biri, iç ve dış politika da en önemli şeyin hala devlet olduğudur. Devlet gerektiğinde sınırlarını kapatarak kendini korumaya geçmiş, kamu sağlığı ve güvenliği adına çok sert tedbirlere başvurabilmiştir. Realist söyleme göre, özellikle kriz dönemlerinde liberal dünya fikrinin aksine devletler birbirleri arasındaki ilişkilere sınır koyar ve risklerini azaltmaya çalışır. Pandeminin en çok can aldığı dönemde, ülkeler uluslararası işbirliğinden vazgeçme pahasına bile olsa

kapılarını kapatmışlar ve realizm tezinin güçlenmesine neden olmuşlardır (Valiyeva, 2020).

Covid-19 salgınında görüldü ki o kadar teknolojik gelişime rağmen hala düşündüğümüz kadar güvende değiliz. Salgın zamanında fark edilememiş, bu yüzden de yayılım ve hasarın boyutu çok büyümüştür. Daha önceki konularda belirtildiği üzere gerek teknolojinin artması gerekse siber terörizm tehlikesinin son yıllarda iyice baş göstermesi nedeniyle medikal istihbarata devletlerin yeterince önem vermemesine neden olmuş olabilir. Ancak, dönemimizde de çıkan haberlere bakıldığında biyolojik silah gibi kullanılabilir birçok virüsün dünya üzerinde olduğunu görebilmekteyiz. Gelecekte medikal istihbarat alanının daha çok yönetilmesi gerekmekte olduğu ortadadır. Çünkü her ne kadar teknolojik alandaki gelişmeleri takip etmek dönemimiz şartlarında çok önemli gözükse de, pandemi dönemlerinde de görüldüğü üzere eğer ki bir devleti ilaçsız ve tedariksiz bırakırsanız o devletin çöküşünü o kadar hızlandırabilirsiniz (Seren, 2020a). Alınan doğru ve güvenilir istihbaratlarla, ulusal güvenlik anlamında doğru adımlar atılabilir, savaşlar önlenir, terör saldırıları durdurulabilir hatta şu yaşadığımız pandemi süreci bile bu kadar uzatılmadan bitirilebilirdi. Bu dönem aynı zamanda tüm ülkelerin kendi içlerine döndükleri bir dönem olarak da bilindiğinden, küresel bir krizde her devletin kendi içine kapanabileceğini de anlamamızı sağlamıştır. Devletlerin yalnız kalması, küreselleşen Dünya’da imkânsız gözüktüğünden; bunun yerine bilgi toplamaya daha çok önem verip bazı olacak olayları, yapılan iyi analizlerle birlikte önleme yollarına gideceklerini tahmin edebiliriz. Buradan hareketle de uluslararası platformlarda ilişkilerin iyi tutulması gerektiği, diplomasinin doğru bir şekilde yönetilmesi gerektiği sonucu çıkarılmaktadır.

SONUÇ

Bu çalışmada, istihbarat ve onunla ilgili kavramlar ile tarihsel süreç içerisinde gelişen ve değişen istihbarat yapıları, gerek ülkeler gerekse dönemsel olaylar bakımından incelenmiş; değişen dünya yapısıyla da beraber uluslararası ilişkiler bakımından istihbaratın giderek artan önemi değerlendirilmiştir. 21. Yüzyılda özellikle değişen teknolojiyle beraber ortaya çıkan önemli istihbarat alanlarının bugün ve gelecekte ülkeler için ne kadar önemli olmaya başlayacağını altı çizilerek, doğru diplomasi kanallarının oluşturulması için doğru ve hızlı bilgi elde etmenin öneminden bahsedilmiştir.

İstihbarat kelimesinin anlamı çok geniş ve kapsamlı olabilmektedir, çünkü istihbarat sadece “bilgi toplama” olarak sınırlandırılabilir bir kavram değildir. Bu yüzden de literatürde birçok tanımı yapılmış, bunların ortak noktası ise istihbaratın sadece bilgi elde etme yöntemi olmasından öte bilimsel bir yaklaşım oluşturarak, ulusal güvenlik açısından hem saldırı hem de savunma zamanlarında kullanılabilir olan araştırma yöntemlerine dayalı bir bilim olduğudur. İstihbarat bilgiyi toplamaz ayrıca analiz ve yorum da yaparak politika yapıcılara yardımcı olur. İstihbarat faaliyetleri öncelikle istihbarat çarkıyla başlar. İstihbarat çarkı dört aşamadan oluşmaktadır. Bunlar; ihtiyacın tespiti, haberin toplanması, değerlendirilmesi ve kullanılmasıdır. Bu çarkın başarılı olabilmesi için doğru istihbarat, kaynakları güvenilir olan istihbarata erişmek çok önemlidir. İstihbarat çarkı genel olarak bu dört aşamadan oluşsa da, aynı istihbaratın tanımı gibi birçok kez modellenmiştir. Her ne kadar birbirlerinden farklı olarak modellenseler de temelde amaç doğru, hızlı, güvenilir bilgileri elde ederek, analiz edip yorumlanması ve istenilen kaynaklara zamanında ulaştırılmasıdır.

Birçok çeşidi olan istihbarat üç ana başlıkta incelenebilir; seviyelerine göre, kaynaklarına göre ve üretim şekillerine göre istihbarat. Bunlardan uluslararası arenada kullanılan istihbarat çeşitleri bizim için değerli konumdadır. Uluslararası ilişkileri yönlendiren, bazen savaş çıkarıp bazense savaşı durdurabilecek güçte olan istihbarat çeşitlerinden biri olan açık kaynak istihbaratı en çok kullanılan istihbarat türlerinden biridir ve ana öznesi halka açık kaynaklardır. Politika deyince aklımıza ilk gelecek olan istihbarat türlerinden biri de siyasi istihbarattır. Ülkelerin birbirleri hakkındaki görüşlerini içeren siyasi istihbarat karar verme sürecinde oldukça önemli olmasıyla birlikte buna

paralel olarak stratejik istihbarat yani devletlerin birbirlerine uygulayacağı stratejiler hakkında bilgi toplamak da önemlidir. Bir ülkenin askeri gücü de en az siyasi yaklaşımı kadar önemli olduğundan askeri istihbarat da uluslararası ilişkilerde önemlidir. Ülkelerin kültürleri kararlarını doğrudan etkileyebileceğinden sosyal istihbarat, önleyici istihbarat olarak gösterilen stratejik istihbarat, günlük verileri kullanarak günü kurtaran olaylara dönük olan taktiksel istihbarat, ekonomik verilerin toplandığı ekonomik istihbarat, teknolojik imkânların belirlenmesinde önemli olan teknolojik istihbarat, elektronik sinyallerin kullanıldığı elektronik istihbarat, askeri hareket ilkelerini belirleyen coğrafik istihbarat, kaynağı insan olan insan istihbaratı ve yükselen teknolojiyle oldukça değerli bir konuma yükselen siber istihbarat da diğer uluslararası alanda önemli olan istihbarat türlerindedir.

İstihbaratın başarılı olabilmesi için gerekli olan temel ilkelerde vardır. İstihbarat kullanılabilir bir zamanda elde edilmesi (sürat ilkesi), yüzde yüz doğruluğu ispat edilemese de bunların analiz edilerek doğruya yakın bir bilgi verebilmesi (kesinlik ilkesi, doğru kaynakların bulunabilmesi (doğruluk ilkesi), amacına uygun bilgilerin toplanabilmesi (amaca uygunluk ilkesi), her duruma ayak uydurmak için esnek olabilmesi (esneklik ilkesi) ve objektif olarak yorumlayabilecek istihbarat uzmanlarının varlığı (objektiflik ilkesi) bir istihbaratın başarısını doğrudan etkileyen özelliklerdir.

İstihbarat faaliyetleri kadar sizin adınıza yapılacak istihbaratı önlemek yâda yanıltmakta oldukça önem kazanmış bir alandır. Karşı istihbarat adı altındaki bu eylemlere, İstihbarata Karşı Koyma (İKK) faaliyetleri denilmektedir. Karşı istihbarat iki temel nedenle yapılır. Bunlar savunmak için yada saldırı için olarak özetlenebilir. Savunmak için yapılan karşı istihbaratta amaç caydırmak ve tehlikeleri tespit etmekken, saldırı için yapılan karşı istihbarat da aldatmak ve etkisiz hale getirmektedir. Yani saldırgan İKK faaliyetleri ana amaçlarından biri karşı ajanı kendi saflarına çekmek ya da yanlış bilgi verip savuşturmadır. İKK faaliyetlerinde çalışan ajanların da işlerinin kolay olmadığı İKK'nın on ilkesiyle James Olson tarafından belirtilmiştir.

Dünyanın yaşadığı dönüşümde istihbarat faaliyetlerinin içeriğinde de dönüşümler olmuştur. Özellikle Birinci Dünya Savaşı sırasında artan teknolojik faaliyetler yüzünden oldukça önemli bir alan hale gelmiştir. Modern hayat yani teknolojiden önceki hayatta

istihbaratın temeli insanken, modern istihbaratla beraber açık kaynak istihbaratı da önemli bir alan haline gelmiştir. Modern istihbaratta ise asıl dönüşümün yaşandığı yerin 11 Eylül saldırıları olduğu da açıktır.

İstihbaratın temeli bilgi olduğundan ve bilgi sürekli değişime uğradığından istihbarat kaynaklarının dönemselsel olarak değiştiği söylenebilir. Gelişen teknoloji ve küreselleşmeyle insan istihbaratı, açık kaynak istihbaratı ve siber istihbarat öne çıkarken, bunların ana kaynağının insan olduğunu düşünürsek, insan istihbaratının da önemini yitirmediğini söylemek doğru olacaktır. Tabii ki her ülkenin istihbarat yapılanması ve örgütlerinin aynı olması beklenemez. İlk olarak kurumsal bir istihbarat organizasyonu kuran İngiltere’de istihbarat örgütleri MI5 ve MI6 olup iç ve dış istihbarat olarak iki alanda faaliyetlerine devam etmektedirler. İkinci resmi oluşumu yapan İsviçre’de ise, NDB ve MND isimli kurumlarla beraber aslında askeri ve sivil olarak istihbarat birimlerini ayırmıştır. Çin devleti ise, dünyanın en kalabalık ülkesi olmasının verdiği avantajı insan istihbaratını kullanmaktadır. Ancak bu ülkedeki yapılanmada tek elden raporlama yapılan bir ana başkanlık olmadığından tüm bilgiler direk başkana gitmekte ve bu da karar alma aşamasında kafa karışıklığına neden olabilmektedir. Çin’de askeri ve sivil olarak istihbarat örgütünü yapılandırmıştır. Amerika da ise en karmaşık yapılanma var denilebilir. 18 istihbarattan sorumlu örgüt ODNI kuruluşuna bağlanmış hepsi birbiriyle ve kurumla beraber hareket etmektedir. Ancak en bilinen organizasyonları CIA ve FBI’dır. Rus istihbarat örgütlerinden biri katılımı ve acımasızlığıyla bilinen KGB yani yeni adıyla FSB’dir. Rus yapılanmasına da baktığımızda sivil ve askeri olarak bölündüğü görülmektedir. Kendi dış istihbarat servisi (SVR) de olan Rusya, hem iç hem dış istihbarat alanlarında oldukça güçlüdür. Fransız istihbarat yapılanmasında ise iç ve dış istihbarat olarak iki ayrı kuruluştan oluşmaktadır. DGSE dış istihbaratla görevliyken DGSI ise iç istihbaratla görevlidir. Ancak sadece iç ve dış olarak iki kurumdan ibaret de değildir. Toplam 4 adet ana istihbarat kuruluşu olup, bunlara personel orada kurulu istihbarat akademisinde yetiştirilmektedir. Alman istihbarat teşkilatlanması ise gene ABD gibi birden çoktur. Toplam 6 kuruluştan ibaret olan istihbarat kuruluşları arasında en geniş olanı BND’dır ve bu dış istihbarat servisidir. BND aynı zamanda dünyanın en büyük istihbarat merkezine sahiptir.

Türkiye açısından istihbarat faaliyetlerine bakıldığında ise iç ve dış istihbaratın

önemine her dönemde rastlamak mümkündür. Ancak bilinen ilk istihbarat teşkilatı Hafıye Teşkilatıdır. Bundan sonra ise sırasıyla, Teşkilat-ı Mahsusa, Karakol Cemiyeti, Zabitan Grubu, Yavuz Grubu, Hamza grupları (İstanbul ve Ankara), Müsellah Müdafaa-i Milliye grubu, Milli Emniyet Hizmeti Riaseti Grubu, Özel Harp Dairesi ve Milli İstihbarat Teşkilatı kurulmuştur. Türkler hem iç hem de dış istihbarata önem vermişlerdir. Ancak dünyada görülen istihbarat yapılanması gibi bir yapılanmaya sahip değildir. Dış ve iç istihbaratla farklı olarak ilgilenen iki kurum olmamakla birlikte sadece MİT teşkilatına bu iki görevde verilmiştir. Her ne kadar farklı yerlere bağlı çalışan farklı istihbarat kurumları olsa da ana kurum MİT teşkilatıdır. Bu yüzden, Türk tarihinde dış istihbarata yönelim özellikle Osmanlı Devleti sırasında çoğalmışken, şu an bu yönde dünyayla kıyaslandığında eksik kalmıştır denilebilir.

Gelişen ve değişen dünyada, her şey gibi istihbarat teknikleri de zamanla değişmiştir. Modern istihbarat dönemi dediğimiz ve teknolojik alanda olan gelişmelerle başlayan dönem insan odaklı istihbaratın yönünü değiştirmiş, teknolojik ve sinyal istihbaratı alanlar geliştirmiştir. 1840 yıllarında bulunan telgraf sistemiyle başlayan bu döngü, 21. Yüzyılda siber uzay kavramının da araya girmesiyle direk bir değişim yaşamıştır. Klasik istihbarattan modern istihbarata geçiş istihbarat kurumlarının kurumsallaştırılmasıyla olurken bu dönem dünyada Soğuk Savaştan sonra daha belirgin görülürken, Türklerde ise Teşkilat-ı Mahsusa'nın kurulmasıyla ortaya çıkmıştır. Bu anlamda Türklerin istihbaratı kurumsallaştırması Dünya devletlerinden daha önce başlamıştır denilebilir.

İstihbaratın uluslararası ilişkilerle doğrudan ilişkili olduğu da bir gerçektir. Waltz'ın da söylediği gibi devletler için güç önemlidir ve bu dönemde gücü sağlamanın kaynağı da “bilgi” sahibi olmaktır. Sahip edinilen bilgilerle devletler dış politikalarını belirleyebilirler. Bilgi toplamakla görevli istihbarat teşkilatları her zaman doğru dış politikalara sebep vermeseler de, kötü bir istihbarat teşkilatı da çok yanlış dış politika kararlarına sebep olabilmektedir. Örneğin ABD'nin Irak işgali istihbarat hatasından başka bir şey değildir ve bu yüzden ABD'nin neredeyse tüm dünyaya karşı tavrı ve duruşu değişmiştir. Sadece askeri ve güvenlik kaynaklı istihbarat değil artık IMF, AB, OECD gibi dünya çapında olan sivil kuruluşlarda özellikle mali suçlarla mücadele etmek amaçlı istihbarat faaliyetleri yürütmektedirler. Kara para aklama ya da kaçakçılık gibi terör

dışında ki kötü amaçlı hareketleri engellemek amaçlı, yâda bu faaliyetlere hangi ülkeler kanallarıyla ulaşıldığını tespit etmek amaçlı istihbarat faaliyetlerini yürütmektedirler. Burada unutulmaması gereken kuruluşlardan biri de gün geçtikçe sayısı artan stratejik araştırma merkezleridir. Bunların hazırladıkları raporlar doğrultusunda hangi ülkelere yatırım yapılabileceği hangilerindeki gelişmelerin kendilerini olumlu ya da olumsuz etkileyebileceğini öğrenebilen devletler uluslararası alanda devlet ilişkilerini ona göre düzenleyebilmektedirler. AGİT’de burada önemli olan bir ilişki sağlayıcıdır. Bu kuruluşun Ukrayna-Rusya savaşında istihbarat bilgilerini Ukrayna ile paylaştığı iddia edilmiş ancak bu Rusya tarafından kanıtlanamamıştır. Tüm bunlardan anlaşılacağı üzere sadece askeri anlamdaki istihbarat değil aynı zamanda özel kuruluşların yaptığı istihbarat da uluslararası siyasi kararları etkilemekte ve devletlerin kendilerini koruyucu ya da daha ileri boyuta geçerek savaş maksatlı politikalarını direk ya da dolaylı yoldan etkilediği bir gerçektir.

Doğru istihbaratın önemli olması kadar yanlış istihbaratında yaratabileceği tahribat unutulmamalıdır. Burada dünya çapında etkisi olan ve uluslararası sistemin temellerini değiştiren olayları hatırlamak gerekir. Başarısız istihbarat, kısaca, istihbarat çarkındaki aşamaların herhangi birinde yanlış yapmak anlamına gelmektedir. Büyük başarısızlıkların çoğu analiz kısmında yapılan hatalardan ötürü olduğu bilinmektedir. Buna örnek olaylardan biri Pearl Harbour baskınıdır. Japonların Pearl Harbour limanındaki ABD askeri güçlerine saldırmaları ve ABD’nin ciddi kayıplar vermesinin sebebi, ABD’nin birçok istihbarat birimi olmasına rağmen bunların arasındaki bilgi ve koordinasyon eksikliği olmasıdır. Bu saldırıyla birlikte II. Dünya Savaşına girme zorunda kalan ABD, bu savaşın da kaderini değiştirmiştir. Bir başka istihbarat başarısızlığı da Vietnam savaşında görülmüştür. ABD komünizmin yayılmasını engellemek amacıyla Kuzey Vietnam’a savaş açarken, buradaki askeri gücü tahmin edememiş ve barış masasına oturmak zorunda kalmıştır. Burada ki askeri istihbarat başarısızlığı, dünyanın ABD’ye olan güvenini de sarsmıştır. En yakın tarihte olan ve ABD’nin kendisine o kadar güvendiği zamanda olan 11 Eylül saldırıları ise dünyanın komple dengesini bozmuştur. ABD, dünyada güç olarak tek başına kalmasının büyümesi altında terörizm tehlikesinin ne kadar çok ve etkili bir şekilde büyüdüğünü görememiş, yurt içi istihbarat faaliyetlerini boşlaması yüzünden gelen terör saldırısını öngörememiştir. İstihbarat hataları genellikle ülkelerin

kolay kabul edebileceği şeyler olamamasına rağmen, 11 Eylül saldırıları için bir güvenlik konseyi kurularak, buradaki hataların görülebilmesi amacıyla raporlar hazırlanmıştır. 11 Eylül öncesinde de aslında El-Kaide örgütünün ABD'ye karşı saldırıları olmuş ve buralarda da birçok sivili kayıplar verilmiştir. Bu saldırı uluslararası alanda da oldukça büyük yankılar yaratmış ve küresel terörizm ilk defa ABD tarafından kabul edilmiştir. Diğer devletler bu konuyla ilgili ellerindeki bilgileri ABD'ye ve kamuya açtıklarından dolayı kamuya açık istihbarat kavramı ortaya çıkmış ve tüm ülkeler teröre karşı ortak hareket etmişlerdir. Bu saldırıyla beraber Soğuk savaştan sonra ABD öncülüğünde kurulan liberal düzen yıkılmaya başlamış ve realizm tekrar gündeme gelmiştir. Neredeyse tüm devletler ellerindeki El-Kaide'yle ilgili bilgileri açıklamaya özen gösterecekler de, ABD artık dünyanın jandarmalığına soyunacağına sinyallerini vermiş ve bu saldırıların sorumlusu olduğunu ilan ettiği ülkelere olan Irak'a savaş açmıştır. Irak'da kitle imha silahları olduğunu iddia eden ABD, hazırladığı istihbarat raporlarında da bunlardan bahsederek, neredeyse tüm ülkelerin karşı çıkmasına rağmen Irak'a karşı savaş başlatmıştır. Dönem başkanı olan Bush doktrinine göre demokrasiyi savunan ve serbest pazarın varlığına inanıp bir taraftan da terörle mücadele edeceğini vurgulayan ABD, Irak'taki bu silahların dünya barışına zarar vereceğini iddia ederek girdiği bu savaşta, sonuçta hazırlatılan istihbarat raporlarının yanlış olduğunu kabul etmek zorunda kalmış ve geri çekilmiştir. Ancak buradaki asıl önemli olan Dünya ABD'nin istediğinde ne kadar bağımsız hareket edebileceğine şahit olmuş, bunun sonucunda da bir kez daha ABD'nin realist politikaları uygulama yönünde eğilimlerinin olabileceği gerçeğiyle karşılaşmıştır. Bu gerçeği gören Avrupa devletleri ise Solona belgesi imzalayarak artık dünyanın tek jandarmasının ABD olmayacağını ve gerekirse kendilerini korumak için saldırı görebilecekleri her şeyde AB olarak beraber hareket edeceklerini beyan etmişlerdir. Aynı zamanda önleyici savaşı destekleyen ABD'nin aksine, diplomatik kanallara yöneleceklerinden bahsettiklerinden, AB için uluslararası ilişkileri sağlamak amacıyla doğru diplomasi olması oldukça önemli hale gelmiştir.

İstihbaratın dönemler içerisinde değiştiği bir gerçektir. Özellikle teknolojik alanda yaşanan gelişmeler kaynaklı istihbarat toplama yöntemleri ve doğal olarak gelebilecek saldırı alanları da değişmiştir. Son zamanlarda önemli olarak ortaya çıkan iki istihbarat alanı vardır. Bunlardan biri siber istihbarat diğeri ise medikal istihbarattır. Siber

güvenliğin sağlanması amacıyla olan siber istihbarat, karşılaşılabilecek siber terör atakları için toplanması gereken aynı zamanda bunu önlemek amacıyla güden bir istihbarat türüdür. Dünyada çok ciddi siber saldırılar düzenlenmiştir. İlk siber saldırı olarak görülen Robert Tappan Morris tarafından yazılmış bir program bir üniversitenin ağını çökertmişken, 2013'te Yahoo'ya yapılan siber saldırıyla 3 milyon kullanıcının özel bilgileri çalınmıştır. Buradan da anlaşılabilir ki, siber terörizm gün geçtikçe daha da çoğalan bir zarar verme kapasitesine sahiptir. Ülkelerin altyapılarına da düzenlenebilecek saldırılarla, bir ülkenin komple elektriksiz kalmasına sebep olunabilir, yâda merkez bankalarına saldırarak tüm sistemlerinin ekonomik anlamda çökmesine neden olunabilir. Aynı zamanda savaş uçaklarının yazılımlarına yâda denizaltıların yazılımlarına saldırarak bir ülkeyi askeri güç anlamında da çökertmek mümkündür. Bunların önlenmesi için siber istihbarat oldukça önemlidir. Çünkü hangi ülkenin bunu yapabilecek insan ve bilgisayar kaynaklarına sahip olduğunu önceden bilip nerelere saldırabileceğini tahmin etmek saldırıya uğrayacak olan ülkeye çok büyük avantaj sağlayacaktır. Bunu önleyici yazılımları sistemlerine ekleyerek saldırı daha başlamadan bitirilebilir. Stuxnet saldırısıyla siber saldırıların gerçek hayatı da etkileyebilecek boyutlara ulaştığı görüldükten sonra, Ukrayna'da 2015 yılında yapılan siber saldırıyla beraber siber savaşların ne kadar ciddi hale gelebileceği bir kere daha görülmüştür. Ukrayna'da bir bölgenin elektrikleri komple kesilmiş ve hayat felce sürüklenmiştir. Burada ana nokta, giderek artan siber saldırılar karşısında dünyadaki Türkiye'nin de içinde olduğu devlet gerek uluslararası alanda yaptıkları anlaşmalar gerekse ülke içerisinde bunlara karşı kurdukları kurumlarla olsun savaşmaya çalışsa da, siber saldırılar uluslararası diplomasiyi ciddi olarak bozabilecek niteliklere ulaşabilmektedir. Bir devlet kendisine yapılan saldırıyı hangi devletin yaptığını gene siber istihbarat kanallarıyla çözebilir ve bu çözüldüğünde ise savaş boyutuna ulaşabilecek kararlar alınabilir. Siber istihbarat genel olarak bakıldığında, teknolojik olarak gelişmiş ülkeler yatırım yaptığından, bu alandaki istihbarat yüzünden çıkabilecek her türlü savaş tüm uluslararası diplomasiyi yerle bir edebilir hatta teknolojisi gelişmemiş küçük devletlerin ortadan kalkmasını sağlayabilir.

Son dönemde asıl üstüne düşülmesi gerekli istihbarat dalı olarak artık medikal istihbarat gösterilmektedir. Yaşanılan pandemi sonrası en güçlü ülkelerin bile yaşadıkları çaresizlik ve panik karşısında yetersiz bilginin Dünyanın başına ciddi işler açabileceği

görülmüştür. Hali hazırda devam eden bu virüs çeşitli varyantlarla insanların hayatını tehdit etmeye devam ettiği gibi bundan çok daha kötüsü de olabilir diyen doktorlar da vardır. İlk Covid-19 hastalığı ortaya çıktığında ellerinde bu hastalıkla savaşmak için hiçbir şey olmayan devletler, kurdukları BM, NATO v.b. gibi küreselleşmeyle gelişen ve yardımlaşma amacındaki toplulukların aslında hiçbir şey yapamadıklarını gördüler. Donald Trump'ın başkanlık döneminde başlayan ABD'deki pandemi süreci, hükümetin bu işi ciddiye almamasıyla gittikçe kontrolden çıkmış ve Dünyaya hükmeden ABD, pandemiye karşı yüzbinlere varan kayıplar vererek bir virüs karşısında diz çökmüştür. "Gizli düşman" diye nitelendirdiği Çin hükümetine karşı basın yayın yoluyla saldırmaktan başka bir şey yapamayan ABD, savunduğu liberalizmin tam tersi hareketlerde bulunmuş, sınırları kapatmış, bilgi paylaşımını durdurmuş ve doğrudan piyasalara müdahalelerde bulunarak kendi kurduğu hareketi kökünden bir kere daha sarsmıştır (Aslan, 2021). Burandan da anlaşılacağı üzere, zamanında alınamayan yada tüm dünyaya yayılmadan ciddiye alınmayan istihbarat, bir işe yaramadığı gibi tüm dünya düzenini etkileyerek ülkeleri birbirlerinde uzaklaştırabilmekte, dış politikada tamamen izolasyon etkisine neden olabilmektedir. 11 Eylüldeki istihbarat hatası dünya düzenini kökten sarsmış, unutulmuş medikal istihbarat faaliyetleriyle yayılan pandemi de bunun üzerine artık eski liberalizm kavramlarından uzaklaşılacağını göstermiştir. En son olan bu salgınla beraber, realizmin temelinde yatan ulus devletinin insanlığın en temel ihtiyaçlarını denetlemesinin önemi bir kez daha anlaşılmaktadır. Ülkeler artık daha korumacı politikalar benimsemiş eğiliminde olacak ve gıda, sağlık, AR-GE konularına daha fazla yatırım yapacaklardır (Ağır, 2021). Bundan kaynaklı olarak da istihbarat etkinlikleri daha çok önem kazanmış ve bu alana daha fazla yatırım gereksinimi artmıştır.

Sonuç olarak, tüm bu bilgiler ışığında uluslararası ilişkilerde istihbaratın çok önemli bir yönlendirici güç olduğu gerçektir. Küreselleşen ve liberalizmi destekleyen dünyada ülkelerin birbiriyle etkileşimi artmış, doğal olarak bu da bazı güvenlik eksikliklerine neden olmuştur. Ülkeler dış politikalarını belirlerken, karşı ülkenin teknolojik alt yapısını, askeri ve ekonomik gücünü, kültürünü ne kadar bilirse kendilerine olacak olan yaklaşımlarını o kadar tahmin edebilirler. Bir başka açıdan bakacak olursak, herhangi bir saldırı halinde kendilerine ne kadar zarar gelebileceği yada onlara ne kadar zarar verebileceklerini tahmin edebilirler. Ama daha önce de belirtildiği gibi, istihbaratın en

önemli olan özelliđi dođru bilgileri bulmaktır. Yanlıř istihbarat yanlıř iliřkiler geliřmesine neden olabilir. Uluslararası iliřkiler anlamında ülkeler dıř politikalarını belirlerlerken yařanan tüm bu deđiřikliklere adapte olmalı ve istihbarat teřkilatlarını buna göre düzenlemelidirler. Günün gerekliliđini görerek teřkilatlarını bu alanlara yönlendiren ve esnek yönetim gösteren devletler uzun soluklu güçlerini koruyabileceklerdir. Tarihsel bazda her dönem farklı istihbarat kaynakları ortaya çıkmıř ve bundan sonra da bilginin dinamik oluřundan kaynaklı daha farklı istihbarat alanları da oluřabilecektir. Ancak istihbaratın uluslararası alanlarda kararlar alırken ki önemi deđiřmemiř aksine gün geçtikçe artmıřtır. Özellikle yařanan 11 Eylül saldırılarıyla beraber küresel terörizmin Amerika tarafından kabul edilmesiyle deđiřen güvenlik anlayıřı, bařarısız istihbaratın uluslararası arenada tüm dünya düzenini etkileyebileceđini göstermiřtir. Buradan da anlaşılacađı üzere istihbarat, tarih boyunca gün geçtikçe uluslararası iliřkilerin içerisindeki yeri ve önemini arttırmıř, gelecek zamanlar içinde çok önemli olduđunu ispatlamıřtır.

KAYNAKÇA

- 9/11 Comission Report. (2004). “9/11 Comission report.” 20 Ocak 2023 tarihinde <https://govinfo.library.unt.edu/911/report/911report.pdf> adresinden erişildi.
- ABD Senatosu. (2004). *Report on the U.S. intelligence community's prewar intelligence assessments on Iraq*. Washington: ABD Senatosu.
- Abu'lfarac, G. (1999). *Abu'lfarac tarihi 1. Cilt*. Ankara: Türk Tarih Kurumu Yayınları.
- Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence—issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), 371-379.
- Acar, Ü. (2019). Yönlendirici güç: İstihbarat servisleri. *Uluslararası Kriz ve Siyaset Araştırmaları Dergisi*, 3(2), 103-134.
- Acar, Ü., & Urhal, Ö. (2007). *Devlet-Güvenlik İstihbarat- Terörizm*. Ankara: Adalet Yayınevi.
- Ağır, O. (2021). Covid-19 sonrası uluslararası politikadaki olası değişimlere yönelik bir değerlendirme. *Fırat Üniversitesi Sosyal Bilimler Dergisi*, 2(31), 887-896.
- Aim Report. (2003). “Bush must rectify pearl harbor smear.” 20 Ocak 2023 tarihinde <https://www.aim.org/aim-report/aim-report-bush-must-rectify-pearl-harbor-smear/> adresinden erişildi
- TUIC Akademi. (2014). “Vestfalya anlaşması.” 19 Aralık 2022 tarihinde <https://www.tuicakademi.org/vestfalya-antlasmasi/> adresinden erişildi.
- Akar, A. (2005). *Casuslar - derin savaşın sıradışı neferleri*. İstanbul: Timaş Yayınları.
- Akbal, Ö., & Tılsbık, N. (2006). *İstihbarat ve Türkiye*. İstanbul: Nüve Kültür Merkezi Yayınları.
- Akın, F. (2017). İkinci Dünya Savaşı sonrası yeni dünya düzeni ve Türkiye. *İş ve Hayat*, 3(5), 119-135.
- Aköz, S. (2020). *Siyasi istihbarat*. Ankara: Gazi Kitapevi.
- Aksar, Y. (2015). *Uluslararası hukuk*. Ankara : Seçkin Yayıncılık.

- Aksoy, M. (2016). Önleyici meşru müdafaa hakkı bağlamında Bush doktrini ve ABD'nin Irak'ı işgali. *Ihh İnsani ve Sosyal Araştırmalar Merkezi*, 1-7.
- Alper, Y. (2021). İstibdâdî idârenin gizli enstrümanlarından hafiyelik ve jurnalın Reşat Nuri Güntekin'in romanlarına yansımaları. *Türkiyat Mecmuası*, 31(2), 649-680.
- Alsay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28.
- Andrew, C., & Mitrokhin, V. (2001). *The Sword and the shield: the mitrokhin archive and the secret history of the KGB*. Newyork: Basic Books.
- Arı, T. (2013). *Uluslararası ilişkiler ve dış politika (10. baskı)*. Bursa: Marmara Kitap Merkezi Yayınları.
- Arıklı, E., & Yavuz, H. (1974). *Başlangıcından bugüne kadar dünya casusluk tarihi (1. cilt)*. İstanbul: Artel Yayınları.
- Arıoğlu, S. (2012). "Bianet". 23 Aralık 2022 tarihinde <https://m.bianet.org/bianet/ifade-ozgurlugu/136446-sendroma-adini-veren-savas> adresinden erişildi.
- Armaoğlu, F. (2005). *20. Yüzyıl siyasi tarihi*. İstanbul: Alkım Yayınevi.
- Artvinli, F. (2020). Salgınların tarihi: toplumsal ve siyasal açıdan kısa bir bakış. *Pandemi ve COVID-19* (pp.129-150). İstanbul: Ayrıntı Yayınları.
- Ashmore, W. (2009). Impact of alleged russian cyber attacks. *Baltic Security ve Defence Review*(11), 4-40.
- Aslan, S. (2021). Covid-19 salgınının küreselleşmeye ve ulus devletlere etkisi. *Elektronik Sosyal Bilimler Dergisi*, 20(80), 1735-1752.
- Ataç, K., & Özcan, B. (2021). 1962 Küba krizi: Amerikan arşivleri üzerinden bir okuma. *Güv. Str. Derg.*, 17(39), 521-562.
- Atay, M. (2002). Rusya gizli istihbarat servisleri: KGB'nin kısa tarihi. *Avrasya Dosyası*, 8(2), 309-328.

- Ateş, A. (2020). Current changes and trends in intelligence. *Güvenlik Bilimleri Dergisi*, 9(1), 177-204.
- Ateş, H. (2013). *Türk istihbarat sisteminin sorunsalları*. Ankara: Detay Yayınları.
- Aytekin, G. (2019). “Doğru habere ulaşmanın doğru yöntemleri”, 20 Aralık 2022 tarihinde <https://www.guvenliweb.org.tr/blog-detay/dogru-habere-ulasmanin-dogru-yontemleri> adresinden erişildi.
- Avcı, G. (2004). *İstihbarat teknikleri (1. Baskı)*. İstanbul: Timaş Yayınları.
- Avcı, G. (2006). *Karanlık ilişkiler*. İstanbul: Birey Yayınları.
- Avşar, S. (2018). Birinci Dünya Savaşı’nda casusluk okulları, casusluk uygulamaları ve Osmanlı Devleti’nin casusluğu önleme faaliyetleri. *Stratejik ve Sosyal Araştırmalar Dergisi*, 2(3), 1-46.
- Ay, H., & Uçar, Ö. (2015). Devletin gelişim süreci. *İşletme Fakültesi Dergisi*, 16(2), 195-206.
- Aydın, A. (2020). “Dünyadaki 16 üst düzey istihbarat teşkilatı.”, 10 Şubat 2023 tarihinde <https://www.stratejikortak.com/2020/03/dunyadaki-istihbarat-teskilatları.html> adresinden erişildi.
- Aydın, A., & Bakıncak, E. (2016). Uluslararası güç dengesi ve iki kutupluluk arasındaki ilişki. *Cumhuriyet Üniversitesi İktisadi ve İdari Bilimler Dergisi*, 17(1), 95-112.
- Aydın, M. (1990). Millî mücâdele yıllarında İstanbul’da faaliyet gösteren gizli bir grup Zâbitân Grubu. *Ankara Üniversitesi Osmanlı Tarihi Araştırma ve Uygulama Merkezi Dergisi*, 1(1), 11-27.
- Babacan, M., Haşlak, İ., & Hira, İ. (2011). Sosyal medya ve Arap baharı. *Sakarya Üniversitesi Sosyal Bilgiler Enstitüsü Akademik İncelemeler Dergisi*, 6(2), 63-91.
- Bagheri, S. (2012). Devlet aklın’ın bir yansıması olarak osmanlı gizli polis teşkilatı. *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, 16(1-2), 87-106.
- Bağcı, S., Oral, N. (2021). “Hibrit savaş bağlamında Stuxnet saldırısı”, 10 Nisan 2023 tarihinde <https://www.tuicakademi.org/hibrit-savas-baglaminda-stuxnet-saldirisi/> adresinde erişildi.

- Bahar, İ. (2011). *Teşkilat-ı Mahsusa MİT ve istihbarat örgütleri*. İstanbul: Kum Saati.
- Bal, M. (2022). Millî Mücadele'nin gizli teşkilatı: Karakol Cemiyeti (1918-1920). *Türk Dünyası Araştırmaları Dergisi*, 130(256), 103-148.
- Bayraktar, G. (2014). Harbin beşinci boyutunun yeni gereksinimi: siber istihbarat. *Güvenlik Stratejileri Dergisi*, 10(20), 119-147.
- Bayraktar, G. (2015). *Siber savaş ve ulusal güvenlik stratejisi*. İstanbul: Yeniüzyıl Yayınları.
- BBC News. (2020). "11 Eylül saldırıları: 2001'de neler yaşandı, 19 yılda neler değişti?." 20 Nisan 2022 tarihinde <https://www.bbc.com/turkce/haberler-dunya-49653233> adresinden erişildi.
- BBC Türkçe. (2007). "Estonya'ya siber saldırı." 30 Aralık 2022 tarihinde https://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml adresinden erişildi.
- Beden, A. (2011). Türk basınına göre 2003 Irak Savaşı'nın temel nedenleri hakkında bir değerlendirme (Kitle imha silahları ve el-kaide bağlantısı). *International Journal of History (ABD ve Büyük Ortadoğu İlişkileri Özel Sayısı)*, 65-80.
- Beets, R. K. (2003). Politization of intelligence: costs and benefit. R. Beets, & T. Mahnken (eds.), *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, (pp. 57-76), London: Frank Cass.
- Benbow, T. (2008). Talking bout our generation? assessing the concept of 'fourth generation warfare. *Comparative Strategy*, 27(2), 148-163.
- Berk, M., & Sarı, G. (2022). İstihbarat çarklarının swot analizi çerçevesinde incelenmesi. *International Journal Of Politics And Security*, 4(2), 65-99.
- Berk, O. (2014). "Türkiye ve açık kaynak istihbaratı." 11 Ağustos, 2022 tarihinde https://www.academia.edu/9832312/a%c3%a7%c4%b1k_kaynak_%c4%b0stihbarat%c4%b1 adresinden erişildi.
- Berkkan, K. (2017). *İstihbarat tarihi*. İstanbul: Eftalya Kitap.

- Bernard, R. (2009). "Electronic Intelligence (ELINT) at NSA." 10 Şubat 2023 tarihinde <https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/misc/elint.pdf> adresinden erişildi.
- Berqnet. (2023). "Tatsız sürpriz: Wannacry virüsü." 29 Ocak 2023 tarihinde <https://berqnet.com/blog/wannacry-virusu> adresinden erişildi.
- Betts, R. (1978). Analysis, war, and decision: why intelligence failures are inevitable. *World Politics*, 31(1), 61-89.
- Beyhan, M. A. (1999). II. Abdülhamid döneminde hafiye teşkilâtı ve jurnaller. *İlmî Araştırmalar: Dil, Edebiyat, Tarih İncelemeleri*, 8, 65-83.
- BGA Security. (2019) "Siber Tehdit İstihbaratı Neden Gereklidir? Faydaları Nelerdir?" 13 Şubat 2023 tarihinde <https://www.bgasecurity.com/2019/05/siber-tehdit-istihbarati-neden-gereklidir-faydolari-nelerdir-bolum-2/> adresinden erişildi.
- Biçer, S. (2017). Ulusal Güvenlik ve İstihbarat Sisteminde Geleneksel Anlayıştan Modern Ve Değişen İhtiyaçlar Dönemine Geçiş. *Ksbd*, 9(2), 435-464.
- Bnd. (2022). "Cooperation." 20 Ocak 2023 tarihinde https://www.bnd.bund.de/en/what-we-do/cooperation/cooperation_node.html adresinden erişildi.
- Bolin, R. (1998). "Fm 34-54, technical intelligence, 30 January 1998." 29 Aralık 2022 tarihinde <http://digitalcommons.unl.edu/dodmilintel/89> adresinden erişildi
- Borum, R., Felker, J., Kern, S., Dennesen, K., & Feyes, T. (2015). Strategic cyber intelligence. *Information and Computer Security*, 23(3), 317-332.
- Bowsher, G., Milner, C., & Sullivan, R. (2016). Medical intelligence, security and global health: the foundations of a new health agenda. *Journal of The Royal Society Of Medicine*, 109(7), 269-273.
- Bozkurt, A. (2014). I. Dünya Savaşı başlarında Osmanlı Devleti'nde casusluk faaliyetleri ve güvenlik algısı (1914-1915). *Otam*, 36, 1-44.
- Brady, C. (1993). Intelligence Failure: Plus Ça change. *Intelligence And National Security*, 8(4), 86-96.

- Briciu, S., Vrîncianu, M., & Florin, M. (2009). Towards a new approach of the economic intelligence process: basic concepts, analysis. *Theoretical And Applied Economics*, 4(533), 21-34.
- BTK. (2017). “Siber Güvenlik Kurumu.” 11 Ocak 2023 tarihinde <https://www.btk.gov.tr/siber-guvenlik-kurulu> adresinden erişildi.
- Bulut, M. (2017). İstihbarat başarısızlığına analitik bir yaklaşım: tanımı, sebepleri ve çözüm önerileri . *Güvenlik Çalışmaları Dergisi*, 19 (1) , 67-90
- Bulut, R. (2014). SSCB’nin dağılması ve Rusya Federasyonu’nda serbest piyasaya geçiş. *Mehmet Akif Ersoy Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 1(2), 7-19.
- Bush, G. (2001). “Address to a joint session of congress and the American.” 15 Kasım 2022 tarihinde <http://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-> adresinden erişildi.
- Butorac, K., Miličević, K., & Solomun, D. (2020). Analysis of the openness of intelligence services. *Visuomenės Saugumas Ir Viešoji Tvarka*, 25, 49-73.
- Buzan, B. (2008). Askeri güvenliğin değişen gündemi. *Uluslararası İlişkiler, Özel Sayı: Güvenlik*, 107-123.
- Can, M., (2014). “Stuxnet ve uluslararası hukuk: Bir siber saldırının anatomisi”. 10 Nisan 2023 tarihinde <https://bilimvegelecek.com.tr/index.php/2014/07/01/stuxnet-ve-uluslararasi-hukuk-bir-siber-saldirinin-anatomisi/> adresinden erişildi.
- Caşın, M. H. (2002). Soğuk Savaş sonrasında askerî stratejik istihbaratın yeni vizyonu. *Avrasya Dosyası İstihbarat Özel*, 8(2), 254-294.
- Cavelty, M.D. (2012). “The militarisation of cyberspace: Why less may be better”, 10 Nisan 2023 tarihinde <https://ieeexplore.ieee.org/document/6243971> adresinden erişildi.
- Center For The Study Of Intelligence. (2004). “Intelligence and policy: The evolving relationship.” 14 Şubat 2023 tarihinde <https://apps.dtic.mil/sti/pdfs/ADA499842.pdf> adresinden erişildi.

- Central Intelligence Agency Collection. (1969). "Intelligence failures in Vietnam: Suggestions for reform." 07 Şubat 2023 tarihinde https://vva.vietnam.ttu.edu/repositories/2/digital_objects/31189 adresinden erişildi.
- Clark, R. (2010). *Intelligence Analysis*. Washington: CQ Press.
- Cleave, M. (2007). *Counterintelligence and national strategy*. Washington: National Defense University.
- Clerk, P. (1998). "Economic Intelligence." 14 Şubat 2023 tarihinde http://cv.uoc.edu/moduls/xw00_79010_00225/web/main/m2/v5.html adresinden erişildi.
- Cnn Türk. (2017). "Hawking: Yapay zeka insanlığı bitirebilir." 30 Aralık 2022 Tarihinde <https://www.cnnturk.com/teknoloji/bilim/hawking-yapay-zeka-insanligi-bitirebilir> adresinden erişildi.
- Cohen, E., & Gooch, J. (1991). *Military misfortune*. New York: Free Press.
- Combs, E., & Moorehead, J. (1992). *The competitive intelligence handbook*. Metuchen: Scarerow Press.
- Cook, M., Angus, C., & Adams, C. (2004). Human factors of intelligence analysis. *Human Performance, Situation Awareness And Automation: Current Research And Trend*, 2, 286-293.
- Cornell Law School. (2022). "Legal information institute." 01 Şubat 2023 tarihinde law.cornell.edu/uscode/text/50/3003#3 adresinden erişildi.
- Costanza, W. (2014). "Academia." 20 Eylül 2022 tarihinde https://www.academia.edu/3995342/human_intelligence_%20humint adresinden erişildi.
- Council Of Europe. (2001). "Convention on cybercrime." 30 Aralık 2022 tarihinde <https://www.europarl.europa.eu/cmsdata/179163/20090225att50418en.pdf> adresinden erişildi.

- Cömert, R., Bilget, Ö., Olcay, F., Aksoy, T., Şenöz, E., & Çabuk, A. (2016). Geotasarımın tarihsel gelişimi ve coğrafi bilgi sistemeleri ile ilişkisi. *Doğu Coğrafya Dergisi*, 21(35), 17-38.
- Cummings, B. (2005). *Korea's place in the sun: a modern history*. New York: W. W. Norton & Company.
- Çakır, H., & Arınmış Uzun, S. (2021). Türkiye'nin siber güvenlik eylem planlarının değerlendirilmesi. *Ekonomi İşletme Siyaset Ve Uluslararası İlişkiler Dergisi*, 7(2), 335-379.
- Çetinkaya, Ş. (2021). Kovid-19 sonrası geleceğin güvenlik kurumları ve stratejik dönüşüm, Ezgi Savaş (ed.), *Covid-19 Salgını Sonrası Güvenlik Algısında Yaşanan Değişim: Medikal İstihbaratın Önemi* (s. 264-271). Ankara:Tasam Yayınları.
- Çıtak, E. (2015). Çağımızın gerekliliği olarak sinyal istihbaratı. *Hitit Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 8(2), 751-770.
- Çıtak, E. (2019). Silahsız savaş sahası: Yeni savaş alanında istihbaratın yeri. *Güvenlik Bilimleri Dergisi*, 8(2), 191-213.
- Dahl, E. (2013). *Intelligence and surprise attack: failure and success from pearl harbor to 9/11 and beyond*. George Town: George Town University Press.
- Darıcı A.B, & Özdal, B. (2017). Rusya Federasyonu'nun siber güvenlik kapasitesini oluşturan enstrümanların analizi. *BİLİG, Güz(83)*, 212-146.
- Demircioğlu, İ., Güven, O., & Hıncı, Y. (2021). İslâmiyet'in kabulünden sonra Türklerde istihbarat felsefesi. *Güvenlik Bilimleri Dergisi (2. Uluslararası Güvenlik Kongresi Özel sayısı (İstihbarat Ve Güvenlik))*, 15-34.
- Department of the army. (2007). *U.S. Army counterinsurgency handbook*. New York: Skyhorse Pub.
- DGSE. (2022a). "Who we are?." 20 Kasım 2022 tarihinde <https://www.dgse.gouv.fr/en/get-to-know-us/who-are-we> adresinden erişildi.
- DGSE. (2022b). "Our missions." 21 Kasım 2021 tarihinde <https://www.dgse.gouv.fr/en/get-to-know-us/our-missions> adresinden erişildi.

- DGSI. (2022). “Our missions.” 12 Aralık 2022 tarihinde <https://www.dgsi.interieur.gouv.fr/decouvrir-la-dgsi/nos-missions/our-missions> adresinden erişildi.
- Dilmaç, S., & Erkan, M. (2006). *Devlet güvenliği terörizm ve istihbarat (1. Baskı)*. Ankara: Egm Yayınları.
- Dni. (2023). “Member of the intelligence community” 23 Ocak 2023 tarihinde <https://www.dni.gov/index.php/what-we-do/members-of-the-ic> adresinden erişildi.
- Duncombe, C., & Dunne, T. (2018). After liberal world order. *International Affairs*, 94(1), 25-42.
- Duramaz, S., & Gökbunar, A. (2017). Ekonomik istihbarat sisteminin oluşturulmasına yönelik Türkiye için yeni bir model önerisi. *Öneri Dergisi*, 12(47), 49-69.
- Duvanage, P., & Solms, S. (2014). Cyber counterintelligence: Back to the future. *Journal Of Information Warfare*, 13(4), 42-56.
- Dünya Casusluk Tarihi Ansiklopedisi. (1974). 1 Cilt. İstanbul: Artel Yayınları.
- Dünyabizim. (2022). “Doğası Gereği Gizli Bir Faaliyet: Casusluk Ve İstihbarat Faaliyetleri.” 01 Aralık 2022 tarihinde <https://www.dunyabizim.com/kitap/dogasi-geregi-gizli-bir-faaliyet-casusluk-ve-istihbarat-faaliyetleri-h42500.html> adresinden erişildi.
- Düzel, N. (2002). *Türkiye'nin gizlenen yüzü*. İstanbul: İletişim Yayınları.
- Ecdc. (2023). “Ecdc Activities on epidemic intelligence and outbreak response.” 16 Ocak 2023 tarihinde <https://www.ecdc.europa.eu/en/about-us/what-we-do/ecdc-activities-epidemic-intelligence-and-outbreak-response> adresinden erişildi.
- Efegil, E. (2008). Bush doktrini ve Dünya güvenliğine etkileri. *Türkiyat Araştırmaları*, (8), 103-122.
- Egmann, R., & Sperber, J. (1996). *Bilgi mafyası*. (K. Ökten, Çev.) İstanbul: Sarmal Yayıncılık.
- Erdal, M. (2010). *Herkesin yargısı kendine*. İstanbul: TESEV Yayınları.

- Erdoğan, Ö. (2016). “Ukrayna’da elektrik neden kesildi?” 30 Aralık 2022 tarihinde <https://webrazzi.com/2016/01/16/ukraynada-elektrikler-neden-kesildi/> adresinden erişildi.
- Erendor, M. (2020). Risk toplumu ve refleksif modernleşme çerçevesinde siber terörizm tanımlama ve tipoloji sorunu. *Cyber Optik Journal*, 1(1), 114-133.
- Erhan, Ç. (2002). Uluslararası güvenlik sorunları ve Türkiye. H. T. Ed. Refet İnanç İçinde, *Soğuk Savaş Sonrası Abd’nin Güvenlik Algılamaları* (pp. 55-82). Ankara: Seçkin Yayıncılık.
- Erkul, S. (2018). Askeri güvenlik çalışmalarına dönüş: önleyici savaş. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 23(2), 643-654.
- Eroğlu, H. (2003). Klasik dönemde Osmanlı Devletinin istihbarat stratejileri. *Tarih Araştırmaları Dergisi*, 22(34), 11-33.
- Eroğlu, H. (2007). *Osmanlılar yönetim ve strateji (2. Baskı)*. İstanbul: Gökkuşbu Yayınları.
- Erol, M., & Bingöl, O. (2012). “Uluslararası ilişkiler ve istihbarat.” 23 Aralık 2022 Tarihinde https://www.academia.edu/7384638/uluslararası%20ilişkiler_ve%20istihbarat adresinden erişildi.
- Ersanel, N. (2001). *Siber istihbarat*. Ankara: Asam.
- Ersoy, T. (1996). *Tıp, tarih, metafor*. Ankara: Öteki Yayınevi.
- European Commission. (2004). “New medical intelligence system will help identify public health threats.” 16 Ocak 2023 tarihinde https://ec.europa.eu/commission/presscorner/detail/en/ip_07_1225 adresinden erişildi.
- Feakin, T. (2013). “Enter the cyber dragon”. 01 Aralık 2022 tarihinde https://www.files.ethz.ch/isn/165376/10_42_31_AM_SR50_chinese_cyber.pdf adresinden erişildi.

- Fidan, H. (1999). *Intelligence and foreign policy: a comparasion of British, American and Turkish intelligence systems*. Yüksek lisans tezi, Bilkent Üniversitesi, Ankara, Türkiye.
- Field, M. (2018). “Wannacry cyber attack cost the nhs £92m as 19,000 appointments cancelled.” 16 Ocak 2023 tarihinde telegraph: <https://www.telegraph.co.uk/technology/2018/10/11/wannacry-cyber-attack-cost-nhs-92m-19000-appointments-cancelled/> adresinden erişildi.
- Fink, E., Pagliery, J., & Segall, L. “Cnn Business.” 20 Eylül 2022 tarihinde <https://money.cnn.com/2015/11/24/technology/targeting-terror-intelligence-isis/index.html> adresinden erişildi.
- FIS. (2022). “FIS.” 31 Ekim 2022 tarihinde www.bundespublikationen.admin.ch/cshop_mimes_bbl/00/0024817f68691ee29fe65419866ea197.pdf adresinden erişildi.
- Friedman, G. (2010). *The Next 100 years: A forecast for the 21st century paperback*. Newyork: Knopf Doubleday Publishing Group.
- Friedman, U. (2012). “The ten biggest american intelligence failures.” 14 Nisan 2022 tarihinde foreign policy: <https://foreignpolicy.com/2012/01/03/the-ten-biggest-american-intelligence-failures/> adresinden erişildi.
- GCHQ. (2023a). “Joint intelligence committee.” 08 Şubat 2023 tarihinde <https://www.gchq.gov.uk/information/joint-intelligence-committee> adresinden erişildi.
- GCHQ . (2023b). “Our origins ve wwi.” 09 Şubat 2023 tarihinde <https://www.gchq.gov.uk/section/history/our-origins-and-wwi> adresinden erişildi.
- Gediz Oral, B., & Arpazlı Fazlılar, T. (2019). Küresel sağlık politikasının aktörleri. *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, 17(4), 249-267.
- Giap, V.N. (1998). *Vietnam halk savaşı*. Ankara: Yar Yayınları.
- Gill, P., & Phythian, M. (2006). *Intelligence in an insecure world*. Cambridge: Uk:Polity Press.

- Golden, R. (2006). What Price Security? The Usa Patriot Act And America's Balance Between The Security And Freedom. İçinde J. M. James Forest (eds.) *Homeland Security And Terrorism* (pp. 402), New York: The Mcgraw-Hill Homeland Security Series.
- Goldman, J. (2006). *Words of intelligence: a dictionary*. Scarecrow Press.
- Gookins, A. (2008). The role of intelligence in policy making. *Jstor*, 28(1), 65-73.
- Gör, E. (2015). *II. Abdülhamid'in Hafiyeye Teşkilatı ve teşkilat hakkında bir risale örneği: "Hafiyelerin Listesi"*. İstanbul: Ötüken Yayınevi.
- Gör, E. (2021). Sultan II. Abdülhamid'in istihbarat şeflerinden Ahmed Celaledin Paşa: "Gözdelikten Firara" hayatı ve faaliyetleri . *Journal of Universal History Studies* , 4 (1) , 30-53 .
- Gözen, R. (2021). *Uluslararası İlişkiler teorileri (3. Baskı)* . Ankara: İletişim Yayınları.
- Göztepe, K., & Akdağ, A. (2015). Coğrafi analiz sistemi (Cas) ile askeri karar verme süreci etkinliğinin artırılması. *Teknolojik Araştırmalar*, 7(2), 56-68.
- Gray, C. (2010). The use of force and the international legal order. M. Evans İçinde, *International Law* (pp. 618-648). Oxford: Oxford University Press.
- Guitton, C. (2017). Beyond appearances: cooperation, structure, and constraints of the swiss intelligence service. *Journal Of Policing, Intelligence And Counter Terrorism*, 12(2), 175-189.
- Gül, Z. (2014). Güvenlik Sektöründe Temel Stratejiler. F. Harmancı, M. Gözübenli ve C. Zengin (Eds.) içinde, *İstihbarat Çeşitleri ve Stratejik İstihbarat* (s. 83-98). Ankara: Nobel Yayıncılık.
- Gülbahar, A. (2019) "Doğru habere ulaşmanın doğru yöntemleri" 14 Şubat 2023 tarihinde <https://www.guvenliweb.org.tr/blog-detay/dogru-habere-ulasmanin-dogru-yontemleri> adresinden erişildi.
- Güleç, Ö., & Kışman, Z. (2021). Uluslararası İlişkiler açısından siber güvenlik ve nato'nun siber güvenlik stratejileri. *Akademik Açık Dergisi*, 1(1), 127-154.

- Gülen, A. (2020). “Almanların 8 Yıllık corona virüsü raporu ortaya çıktı.” 02 Ocak 2023 tarihinde <https://www.sozcu.com.tr/2020/dunya/almanlarin-8-yillik-corona-virusu-raporu-ortaya-cikti-5700592/> adresinden erişildi.
- Gülmez , N., & Demirkollu, C. (2013). Bir istihbarat savaşı: Çiçero olayı. *Celal Bayar Üniversitesi Sosyal Bilimler Dergisi*, 11(2), 414-430.
- Gündal, B. (2015). Çin ekonomisinin yapısal dönüşümü. *Anemon Muş Alparslan Üniversitesi Sosyal Bilimler Dergisi*, 3(2), 55-72.
- Güneş, G. (2013). Teşkilat-ı Mahsusa ve Birinci Dünya Savaşı yıllarındaki faaliyetleri. *Atatürk Araştırma Merkezi Dergisi*, 29(85), 101-130.
- Güngör, B. (2020). Türkiye’de Covid-19 pandemisi süresince alınan önlemlerin kriz yönetimi perspektifinden değerlendirilmesi. *Usbad Uluslararası Sosyal Bilimler Akademi Dergisi*, 2(4), 818-854.
- Güntay, V. (2018). Siber güvenliğin uluslararası politikada etki aracına dönüşmesi ve uluslararası aktörler. *Güvenlik Stratejileri*, 14(27), 79-111.
- Gürkaynak, M., & İren, A. (2011). Reel dünyada sanal açmaz: siber alanda uluslararası ilişkiler. *Süleyman Demirel Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi*, 16(2), 263-279.
- H. Gökçe, Z. (2018). Günümüzde ulus - devlet. *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, 13(1), 535-559.
- Habertürk. (2023). “AGİT nedir?” 16 Ocak 2023 tarihinde <https://www.haberturk.com/tubitak-ansiklopedi/avrupa-guvenlik-ve-isbirligi-teskilati-agit-nedir> adresinden erişildi.
- Hanyok, R. (2002). “Spartans in darkness: American sigint and the indochina war, 1945-1975.” 30 Aralık 2022 tarihinde <https://irp.fas.org/nsa/spartans/> adresinden erişildi.
- Hasanov, İ., & Katman, F. (2019). Soğuk Savaş Döneminde ABD ve SSCB’nin politik istihbarat yöntemlerinin karşılaştırması. *Akademik Tarih ve Düşünce Dergisi*, 6(2), 1138-1150.

- Haubrich, D. (2003). September 11, Anti-Terror laws and civil liberties: Britain, France And Germany compared. *Government and Opposition*, 38(1), 3-28.
- Haydarođlu, İ. P. (1995). II. Abdulhamid döneminde Hafiye Teşkilatı hakkında bir risale. *Tarih Araştırmaları Dergisi* , 17 (28) , 109-133.
- Heart, H., & Goodden, R. (1995). *Strategic intelligence: Theory and application*. Washington: Defence Intelligence Agency.
- Hedley, J. (2005). Learning from intelligence failures. *International Journal of Intelligence and Counter Intelligence*, 18(3), 435-450.
- Herman, M. (1999). *Intelligence power in peace and war*. Cambridge: Cambridge University Press.
- Heuer, R. (1999). *Psychology of intelligence analysis*. Washington D.C.: CIA.
- Hillsman, R. (2000). After The Cold War: the need for intelligence. C. Eisendrath (Ed.) içinde, *National Insecurity, Us Intelligence After The Cold War* (ss. 8-23). Philadelphia: Temple University Press.
- Hitz, F. P. (2010). Human source intelligence. L. K. Johnson (ed.), *Handbook of Intelligence Studies* (s. 257-274). The Oxford Handbook Of National Security Intelligence.
- Ho, S. (2007). An economic analysis of military intelligence. *Defense and Peace Economics*, 18(6), 485-493.
- Holat, O. (2021). Yeni medya ve siber savaş kavramları bağlamında Stuxnet saldırısı örneğinin incelenmesi. *Abant Kültürel Araştırmalar Dergisi*, 6(11), 105-125.
- Hope, J. (2008). Surveillance or Collusion? Maxwell Knight, MI5 and The British Fascisti. *Intelligence and National Security*, 99, 651-675.
- Hot, P. M. (1995). *Secret intelligence and public policy*. USA: Congressional Quarterly Press.
- Hürriyet Gazetesi. (2019). “Çiçero kimdir?”, 24 Kasım 2022 tarihinde <https://www.hurriyet.com.tr/gundem/cicero-kimdir-iste-ciceronun-gercek-ismi-41086339> adresinden erişildi.

- Ingram, S. (1998). The role of USA intelligence in American foreign affairs in The Post Cold War era. *Mcnair Scholars Journal*, 2(1), 38-45.
- Ireland, L. (2017). 21st century intelligence: the need for a one-team-one-fight approach. *The Journall Of Complex Operations*, 7(1), 47-57.
- İlter, E. (2002). *Mit'in Tarihçesi*. Ankara: Mit Yayını.
- İnan, Ş., & Doğan, Y. (2018). Ekonomik istihbarat ve ülke uygulamaları. *Jocress*, 8(1), 317-342.
- İlter, E. (2002). Osmanlılarda İstihbarat (XIV-XIX Yüzyıllar). *Avrasya Dosyası Dergisi*, 8(2), 233-254
- İstanbul Bilgi Üniversitesi. (2012). *Siber güvenlik raporu*. İstanbul: İstanbul Bilgi Üniversitesi Bilişim ve Teknoloji Hukuku Enstitüsü.
- Jackson, P. (2021). "11 Eylül saldırıları: 2001'de nasıl düzenlendi, kaç kişi öldü, sonrasında ne oldu?". 29 Kasım 2022 tarihinde <https://www.bbc.com/turkce/haberler-dunya-58462900> adresinden erişildi.
- Jager, T. (2009). *Geheimdienste in Europa* . Germany: Vs-Verlag.
- Jensen, M. (2012). Intelligence failures: what are they really and what do we do about them. *Intelligence and National Security*, 27(2), 261-282.
- Johnson, L. (2000). *Bombs, bugs, drugs and thugs*. New York: Newyork University Press.
- Johnson, L. (2006). A framework for strengthening U.S. intelligence. *Yalejournal Of International Affairs*, 1(2), 116-131.
- Joint Chief Of Staff. (2013). "Jp 2-0, Joint Intelligence." 15 Aralık 2022 tarihinde https://www.jcs.mil/portals/36/documents/doctrine/pubs/jp2_0.pdf adresinden erişildi.
- Kahn, D. (1991). The intelligence failure of pearl harbor. *Foreign Affairs*, (5), 138-152.
- Kahn, D. (2002). İstihbaratın tarihsel teorisi. *Avrasya Dosyası*, 8(2), 5-20.
- Kara, O. (2009). II. Dünya Savaşı'ndan günümüze kriptoloji: Enigma'dan AES'e şifreleme. *Bilim Ve Teknik*, (Temmuz), 28-33.

- Karaağaç, Y. (2021). Gizli servislerde örtülü operasyon faaliyetleri. *Arhuss*, 4(1). 79-95
- Karabulut, A., & Değer, F. (2015). Uluslararası ilişkilerde güvenlik kavramı ve realist yaklaşım'a genel bakış. *İğüsbd*, 2(2), 69-79.
- Karan, K. (2008). *Türk istihbarat tarihi*. İstanbul: Truva Yayınları.
- Karasoy, H.A. (2022a). Hibrit, asimetrik ve vekalet savaşları: 2022 Rusya - Ukrayna savaşını üçlü sacayağı üzerinde bir inceleme. *Medeniyet Araştırmaları Dergisi*, 7(2), 44-56.
- Karasoy, H. A. (2022b). Yeni nesil savaş ve siber istihbarat. *Güvenlik Bilimleri Dergisi*, 11 (1), 223-240.
- Karasoy, H. & Gezici, H. S. (2023). Bombalardan baytlara: siber güvenliğin ulusal güvenlikteki rolü ve yapay zekânın siber güvenlikteki önemi. *Uluslararası Yönetim Akademisi Dergisi*, 6 (1), 173-188.
- Karataş, K. (2017). *Dünyanın yörüngesini değiştiren güçler: istihbarat örgütleri*. İstanbul: Lades Yayınları.
- Karlstrom, E. (2021). "Echelon, industrial espionage, and the organized stalking terror police state." 2 Aralık 2022 Tarihinde <https://gangstalkingmindcontrolcults.com/eschelon-project/> adresinden erişildi.
- Karpat, K. (2012). *Türk dış politikası tarihi*. İstanbul: Timaş Yayınları.
- Kaspersky. (2020). "Tüm zamanların en (kötü) ünlü on korsanı." 29 Aralık 2022 Tarihinde <https://www.kaspersky.com.tr/resource-center/threats/top-ten-greatest-hackers> adresinden erişildi.
- Kavsıracı, O. (2020). İstihbarat süreci ve insan kaynaklı istihbaratın analizi. *Opus Uluslararası Toplum Araştırmaları Dergisi*, 16(27), 700-719.
- Kavsıracı, O., ve Demirbaş, M. (2020). İstihbarat faaliyetlerinin devlet güvenliği açısından incelenmesi. *Anadolu Strateji Dergisi*, 2(1), 49-64.
- Kayar, M. (2003). *Türk-Amerikan ilişkilerinde Irak Sorunu*. İstanbul: IQ Kültür Sanat Yayınları.

- Keck, Z. (2014). "Robert Gates: Most countries conduct economic espionage." 25 Kasım 2022 tarihinde <http://thediplomat.com/2014/05/robert-gates-most-countries-conduct-economic-espionage/> adresinden erişildi.
- Keegan, J. (2016). *İkinci Dünya Savaşı*. (S. Öksüz, Çev.) İstanbul: Say Yayınları.
- Kemiksiz, N. (2022). İkinci Dünya Savaşı'nda bilimsel ve teknolojik istihbarat. *Tesam*, 9(2), 621-647.
- Kent, S. (1949). *Strategic intelligence for american world policy*. Princeton N. J: Princeton University Press.
- Kent, S. (1965). *Strategic Intelligence for American world policy*. Princeton: Princeton University Press.
- Kent, S. (2003). *Stratejik istihbarat*. Ankara: Asam Yayınları.
- Kerasuady, F. (2011). *Çiçero olayı 1943*. İstanbul: Picus Yayınları.
- Kılıç, Ş. (2018). "30 yıl önce tarihin ilk siber saldırısını düzenleyerek interneti çökerten adam." 29 Aralık 2022 tarihinde [webtekno: https://www.webtekno.com/30-yil-once-tarihin-ilk-siber-saldirisini-duzenleyerek-interneti-cokerten-adam-h56353.html](https://www.webtekno.com/30-yil-once-tarihin-ilk-siber-saldirisini-duzenleyerek-interneti-cokerten-adam-h56353.html) adresinden erişildi.
- Kiraz, S. (2012). Uluslararası ilişkilerde egemenliğin değişen yüzü. *Niğde Üniversitesi İİBF Dergisi*, 5(1), 93-102.
- Koca, H.İ. (2019). Stratejik istihbarat. *Akademik Tarih ve Düşünce Dergisi*, 6(4), 2187-2198.
- Koloğlu, O. (2003). *Lawrance efsanesi*. İstanbul: Alkım Yayınevi.
- Kongar, E. (2007). *Tarihimizle yüzleşmek*. İstanbul: Remzi Kitapevi.
- Koroğlu, Y. (2017). "Yapay zeka'nın teorik ve pratik sınırları." 01 Ocak 2023 tarihinde <https://www.cmpe.boun.edu.tr/~yavuz.koroglu/publications/ebes17.pdf> adresinden erişildi.
- Köseli, M. (2009). Terörle mücadelede istihbaratın rolü. *Polis Bilimleri Dergisi*, 11(2), 51-72.

- Köylüoğlu, B. (2017). “II. Dünya Savaşının ekonomik ve stratejik yönünden analizi: barbarossa'dan stalingard'a giden yol”. 28 Kasım 2022 tarihinde <https://www.stratejivefinans.com/ii-dunya-savasinin-ekonomik-ve-stratejik-yonden-analizi-barbarossadan-stalingrada-giden-yol-1941-1942/> adresinden erişildi.
- Köymen, M. (1990). *Siyasetname (Nizamülmülk)*. Ankara: Kültür Bakanlığı.
- Krizan, L. (1999). *Intelligence essentials for everyone*. Washington: Joint Military Intelligence Collage.
- Kruys, G. (2007). “The role of intelligence in countering terrorism and insurgency.” 01 Ocak 2023 tarihinde https://repository.up.ac.za/bitstream/handle/2263/5638/Kruys_Role%282007%29.pdf?sequence=1 adresinden erişildi.
- Kurtbağ, Ö. (2020). ABD liderliğindeki liberal uluslararası düzenin sonu tartışması. *Marmara Üniversitesi Siyasal Bilimler Dergisi*, 8(2), 379-403.
- Kutsal, S. (2017). “Yahoo’dan açıklama: 3 milyar hesap çalındı.” 30 Aralık 2022 tarihinde <https://digitalage.com.tr/yahoodan-aciklama-3-milyar-hesap-calindi/> adresinden erişildi.
- Kuzu, A. (2007). *MIT MOSSAD CIA GLADIO Dünyanın en büyük istihbarat servisleri operasyonlar suikastler gizli raporlar*. İstanbul: Bilge Karınca Yayınları.
- Lewis, J. (2002). “Assessing the risks of cyber terrorism, cyber war and other cyber threats.” 16 Ekim 2022 tarihinde https://www.researchgate.net/profile/james-lewis-9/publication/245508226_assessing_the_risks_of_cyber_terrorism_cyber_war_and_other_cyber_threats/links/5e25be2192851c89c9b49515/assessing-the-risks-of-cyber-terrorism-cyber-war-and-other-cyber-threats.pdf adresinden erişildi.
- Lister, C. (2011). Cultural awareness and counterinsurgency in Afganisthan. *E-International Relations*, 1-23.
- Lowenthal, M. (1984). *U.S. intelligence: Evolution and anatomy*. New York: Praeger Publishers.

- Lowenthal, M. (2000). *Intelligence: From secrets to policy*. Washington D.C.: IQ Press.
- Lowenthal, M. (2006). *Intelligence from secrets to policy (3. baskı)*. Washington Dc.: IQ Press.
- Macksey, K. (2012). *İkinci Dünya Savaşı'nda askeri hatalar*. (T. Akad, Çev.) İstanbul: İş Bankası Kültür Yayınları.
- Manual, F. (2006). *Pollice intelligence operations*. Washington: Headquarters Department of Army.
- Mattis, P. (2015). "China's military intelligence system is changing." 20 Ocak 2023 tarihinde <https://warontherocks.com/2015/12/chinas-military-intelligence-system-is-changing/> adresinden erişildi.
- Mattis, P., & Brazil, M. (2019). "Chinese communist espionage : an intelligence primer". 20 Eylül 2022 tarihinde <https://eds.p.ebscohost.com/eds/ebookviewer/ebook?sid=e4002e0b-3b1d-4035-ba62-9fff5ee3c253%40redisveid=5verid=7veformat=ek> adresinden erişildi.
- Mayer, S. (2002). Australian screen education. *Academic Search Premier*.28, 6-14.
- Mazzafaro, J. (2011). "Cyber Intelligence: Setting the landscape for an emerging discipline." 15 Kasım 2023 tarihinde https://inteligenciayliderazgo.com/wp-content/uploads/2019/08/insa_cyber_intelligence_2011.pdf adresinden erişildi.
- Mc.Lendon, J. (2002). Enformasyon savaşı: Etkiler ve kaygılar. *Avrasya Dosyası*, 8(2), 183-212.
- Mcdowel, D. (2009). *Strategic intelligence: a handbook for practitioners, managers, and users*. Scarecrow Press.
- MI5 Security Service. (2022). "The History of MI5." 08 Ocak 2023 tarihinde <https://www.mi5.gov.uk/history> adresinden erişildi.
- Microdestek. (2021). "Dünya tarihinde görülen siber saldırılar." 29 Aralık 2022 tarihinde <https://microdestek.com.tr/dunya-tarihinde-gorulen-siber-saldirilar.html> adresinden erişildi.

- Milliyet. (2003). "CIA'den acı itiraf: Irak'ta kitle imha silah stokları bulamadı." 27 Aralık 2022 tarihinde <https://www.milliyet.com.tr/gundem/ciaden-aci-itiraf-irakta-kitle-imha-silah-stoklari-bulamadi-5149877> adresinden erişildi.
- MİT. (2022a). "İstihbarat oluşumu." 12 Nisan 2022 tarihinde <https://www.mit.gov.tr/isth-olusum.html> adresinden erişildi.
- MİT. (2022b). "Tarih boyunca istihbarat." 14 Nisan 2022 tarihinde milli istihbarat teşkilatı: <https://www.mit.gov.tr/emuze/tarihboyunca.html> adresinden erişildi.
- Morgenthau, H. (1985). *Politics among nations: The struggle for power and peace*. New York: Mcgraw Hill.
- Moyzsich, L. (2004). *Çiçero operasyonu*. İstanbul: Q-Matris Yayınları.
- Mueller, J. (1991). Pearl Harbor: Military inconvenience, political disaster. *International Security*, 16(3), 172-203.
- Murphy, S. D. (2017). Terrorist attacks on world trade center and pentagon. *The American Journal of International Law*, 96(1), 237- 255.
- Mustafa Efendi, S. (1999). *Tarih-i Selaniki (971-1003 / 1563-1595) (Cilt 1)*. (M. İpşirli, Dü.) Ankara: Türk Tarih Kurumu.
- Mutlu, M. (2001). *Vietnam 'dan Körfez Savaşı 'na uluslararası uyuşmazlıklarda kamuoyu oluşumu*. Basılmamış doktora tezi, İstanbul Üniversitesi, İstanbul, Türkiye.
- Neale, J., ve Tarkan , D. (2004). *Amerikan Savaşı Vietnam 1960- 1975*. İstanbul.
- Nye, J. (2003). *Amerikan gücünün paradoksu- Dünyanın tek süper gücü neden tek başına davranamaz*. İstanbul: Literatür Yayınları.
- Ochiai, Y. (2011). *U.S. Intelligence and the Origins of The Vietnam War, 1962 - 1965*. Basılmamış doktora Tezi, The University Of Edinburgh, Edinburg, İngiltere.
- Oğuz, S., Ceyhan, E., & Sağıroğlu, Ş. (2015). "Teknolojinin casuslukta kullanılması ve karşı önlemler." 05 Kasım 2022 tarihinde https://www.researchgate.net/publication/303999660_teknolojinin_casuslukta_kullanilmasi_ve_karsi_onlemler adresinden erişildi.

- Olson, J. (2001). "The 10 commandments of counterintelligence." 10 Kasım 2023 tarihinde
https://www.dni.gov/files/ncsc/documents/archives/10commandmentsofc1_cind-2002-01-05.pdf adresinden erişildi.
- Ortaylı, İ. (2001). *İmparatorluğun en uzun yüzyılı*. İstanbul: Timaş Yayınları.
- Ozan, E. (2014). Birinci Dünya Savaşı ve uluslararası ilişkiler disiplininin doğuşu üzerine bir değerlendirme. *Akademik Bakış Dergisi*, 7(14), 197-214
- Övet, T. (2020). Terörizm kaynaklı tehditlerde istihbarat kurumlarının tehdit değerlendirmesi: Geleneksel yaklaşım. *Güvenlik Bilimleri Dergisi*, 9(1), 147-176.
- Özal, İ. B. (2019). *İstihbaratın Kısa Tarihi Gölge Oyunu*. İstanbul: Timaş Yayınları.
- Özcan, A. (1993). *Casus*. Tdv İslâm Ansiklopedisi (Cilt 7, S. 166-169).
- Özcan, G. (2019). "Çevreleme politikası." 10 Ocak 2023 tarihinde
https://trguvenlikportali.com/wp-content/uploads/2019/11/cevreleme_gencerozcan_v.1.pdf adresinden erişildi.
- Özdağ, Ü. (2014). *İstihbarat teorisi* (8. Baskı). Ankara: Kripto Yayınları.
- Özdağ, Ü. (2018). *İstihbarat Teorisi* (10. Baskı). Ankara: Kripto Yayınları.
- Özdek, R. (1968). *Vietnam çıkmazı*. İstanbul: Yağmur Yayınevi.
- Özdemir, H. (2008). Uluslararası ilişkilerde güç: Çok Boyutlu bir değerlendirme. *Ankara Üniversitesi Sbf Dergisi*, 63(03), 113-144.
- Özdemir Küçük, Ş. & Eminoğlu A. (2022). Yeni nesil savaş: Rusya'nın donbas'ta uyguladığı hibrit savaş yöntemi. *Hitit Sosyal Bilimler Dergisi*, 15(1), 67-84.
- Özdikmenli, İ., & Ovalı, Ş. (2008). Irak Savaşı sonrasında liberal dünyanın yapay ikiliği. *Uluslararası İlişkiler Dergisi*, 5(19), 89-118.
- Özel Özcan, M. (2019). Westphalian devletler sistemi ve modernleşmenin geleneksel dünyanın büyük güçleri olan imparatorluklara etkisi. *Jebpir*, 5(1), 49-62.
- Özer, Y. (2018a). *Kültürel istihbarat*. Ankara: Karakum Yayınevi.

- Özer, Y. (2018b). Savaşın değişen karakteri: Teori ve uygulamada hibrit savaş. *Güvenlik Bilimleri Dergisi*, 7 (1), 29-56.
- Özkan, T. (2004). *Mit'in Gizli Tarihi*. İstanbul: Alfa Yayınları.
- Özkan, T. (2006). *Mit'in Gizli Tarihi*. İstanbul: Alfa Basım Yayıncılık.
- Özlük, E. (2009). Uluslararası İlişkiler disiplinin soy kütüğü. *Sosyal Ekonomik Araştırmalar Dergisi*, 9(17), 237-360.
- Özselçuk, N. (1979). *Ana Hatlarıyla Vietnam Savaşları ve Alınan Dersler*. Ankara: Genelkurmay Askeri Tarih Ve Stratejik Etüt Başkanlığı Yayınları.
- Pevehouse, J., & Goldstein, J. (2017). *International relations*. Londra: Pearson Education.
- Piacine, R. (1997). "Pearl Harbor: Failure of intelligence?" 15 Eylül 2022 tarihinde <https://apps.dtic.mil/sti/citations/ada397295#:~:text=many%20scholars%20and%20writers%20state,government%20and%20military%20decision%2dmakers.> adresinden erişildi.
- Pirim, H. (2006). Yapay zeka. *Journal Of Yasar University*, 1(1), 81-93.
- Poteat, S. (2001). "The attack On America's intellectual propherty, espionage after The Cold War." 19 kasım 2022 tarihinde www.tbp.org/pubs/features/w01poteat.pdf adresinden erişildi.
- Pramitasari, A. (2022) The role of intelligence in dealing with the threat of hybrid war. *The International Journal of Business Management and Technology*. 6(1), 276-280.
- Prunckun, H. (2019). *Counterintelligence theory and practice*. Newyork: Rowman ve Littlefield Publishing.
- Rathmell, A. (2002). Towards postmodern intelligence. *Intelligence and National Security*, 17(3), 87-104.
- Reuters. (2022). "Rusya, AGİT'i batılı istihbarat örgütlerine bilgi aktarmakla suçladı." 16 Ocak 2023 tarihinde <https://www.indyturk.com/node/503621/d%3%bcnya/rusya-agi%cc%87ti->

bat% c4% b11% c4% b1-istihbarat-% c3% b6rg% c3% bctlerine-bilgi-aktarmakla-
su% c3% a7lad% c4% b1 adresinden erişildi.

Richelson, J. (1995). *A Century of spies : Intelligence in The 20th century*. Newyork: Oxford University Press.

Rusbridger, J., ve Nave, E. (1991). *Betrayal at Pearl Harbor*. Newyork: Ny: Summit Books.

Sakaoğlu, N. (2012). Yaşamları ve yapıtlarıyla Osmanlılar ansiklopedisi. *Türkiye Mecmuası*, 22/Bahar, 31-59.

Sander, O. (1991). *Siyasi tarih 1918-1990* (2 Baskı). Ankara: İmge Kitapevi.

Sandıklı, A., & Yivciğer, G. (2004). *Siber terörizm*. İstanbul: Tasam.

Sapancı, A. (2007). İnternete dayalı araştırmalarda eleştirel düşünme sorunsalı: 21. yüzyıl skolastiğine doğru . *Sosyal Bilimler Araştırmaları Dergisi* , 2 (2) , 56-71.

Sayın, Ü. (2007). *Dünyayı yöneten gizli güçler*. İstanbul: Neden Kitap.

Schiel, K. (2003). *Inside Germany's Bnd: The federal intelligence service*. New York: The Rosen Publishing Group.

Seccops. (2023). "Siber istihbarat hizmeti". 07 Nisan 2023 tarihinde <https://seccops.com/hizmetler/siber-istihbarat-hizmeti/> adresinden erişildi.

Secret Intelligence Service. (2022). "Our history." 05 Ocak 2023 tarihinde <https://www.sis.gov.uk/our-history.html> adresinden erişildi.

Sel, L. (1985). *İkinci Dünya Savaşında istihbarat*. Ankara: Genel Kurmay Basımevi.

Serdar, İ. (2015). Neorealizm, neoliberalizm, konstruktivizm ve ingiliz okulu modellerinde uluslararası sistemsel değişikliklere bakış. *Jemsos*, 1(1), 14-38.

Seren, M. (2017). *Stratejik istihbarat ve ulusal güvenlik*. Ankara: Orion Yayınevi.

Seren, M. (2020a). Medikal istihbarat. *Kriter Dergi*, 5(47), 42-44.

Seren, M. (2020b) Medikal İstihbaratın Yükselişi. Dış İşleri Bakanlığı (ed.) içinde, *Covid-19 Sonrası Sistem: Eski Sorunlar Yeni Trendler* (s. 86-92). Ankara: Sam Yayınları.

Serim, N. (1941). *Siyasi polis hizmeti istihbarat*. Alaeddin Kırıl Basımevi: Ankara.

- Seyedi Asl, S. (2020). Siber terörizm ve ulusal güvenlik: örnek ülke İran. TASAM, *Devlet Doğasının Değişimi: Güvenliğin Sınırları* (S. 329-345).
- Shin, B., ve Lowry, P. (2020). A review and theoretical explanation of the ‘Cyberthreat-Intelligence(CTI) capability’ that needs to be fostered in information security practitioners and how this can be accomplished. *Computers and Security*, 92, 1-16.
- Smith, B. (2018). *Russian intelligence services and special forces*. London: House Of Commons Library.
- Sofaer, A., Goodman, S., Cuellar, M.-F., Drozdova, E., Elliott, D., Grove, G., . . . Wilson, G. (2000). “A Proposal For An International Convention On Cyber Crime And Terrorism.” 10 Eylül 2022 tarihinde <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/sofaergoodman.pdf> adresinden erişildi.
- Sönmezoğlu, F. (2011). *İki savaş sırası ve arasında Türk dış politikası*. İstanbul: Der Yayınları.
- Sözcü Gazetesi. (2017). “En güçlü istihbarat servisleri.” 10 Ekim 2022 tarihinde <https://www.sozcu.com.tr/2017/gundem/en-guclu-istihbarat-servisleri-2-1643884/> adresinden erişildi.
- Strafor Global Intelligence. (2010). “Espionage with chinese characteristics part 1: Intelligence services.” 18 Ekim 2023 tarihinde <https://books.google.com.tr/books?id=ogyhnqaacaaj> adresinden erişildi.
- Stratfor. (2023). “Regions.” 16 Ocak 2023 tarihinde <https://worldview.stratfor.com/region> adresinden erişildi.
- Süpürgeci, İ. (2021). “İstihbarat milli gücün temel bileşenlerinden birisi olarak değerlendirilebilir mi?.” 11 Ekim 2022 tarihinde <https://www.sde.org.tr/ilyas-supurgeci/genel/istihbarat-milli-gucun-temel-bilesenlerinden-birisi-olarak-degerlendirilebilir-mi-kose-yazisi-24259> adresinden erişildi.
- Şenel, M., ve Şenel, T. (1997). *İstihbarat ve genel güvenlik konularımız* (3. Baskı). Ankara: Emniyet Genel Müdürlüğü Yayınları.

- Şenel, M., ve Şenel, T. (2018). *Temel güvenlik konularımız* (2. Baskı). Ankara: Polis Akademisi Yayınları.
- Şimşek, E. (2004). *Türkiye'de istihbaratçılık ve Mit*. İstanbul: Kum Saati Yayıncılık.
- Şimşek, M. (2008). Türk basınında Vietnam Savaşı: Ulus gazetesi örneği. *Ankara Üniversitesi Türk İnkılâp Tarihi Enstitüsü Atatürk Yolu Dergisi*, 42, 311-330.
- Şimşir, M. (2015). Nizamülmülk'ün Siyasetnamesi ve istihbarata yönelik ilke ve yöntemleri. *Karamanoğlu Mehmetbey Üniversitesi Sosyal Ve Ekonomik Araştırmalar Dergisi*, 2015 (1), 68-79 .
- T.C. Sağlık Bakanlığı. (2017). “Mers-Cov.” 25 Aralık 2023 tarihinde <https://hsgm.saglik.gov.tr/tr/bulasici-hastaliklar/mers-co-v/mers-cov-liste/mers-co-v.html> adresinden erişildi.
- Tahsin Paşa. (1999). *Tahsin Paşa'nın Yıldız hatıraları Sultan Abdülhamid*. İstanbul: Boğaziçi Yayınları.
- Tatlı, E. (2022). “İstihbarat örgütlerinin yapılanmasına etki eden faktörler ve küresel istihbarat örgütleri.” 14 Şubat 2023 tarihinde <https://kriterdergi.com/dosya-turkiyede-ve-dunyada-istihbarat/istihbarat-orgutlerinin-yapilanmasına-etki-eden-faktorler-ve-kuresel-istihbarat-orgutleri> adresinden erişildi.
- Taylor, S., ve Goldman, D. (2010). Intelligence reform: will more agencies, money and personnel help?. *Intelligence And National Security*, 19(3), 416-435.
- Tekin, A. (2021). Tarihten günümüze epidemiler, pandemiler ve ekonomik sonuçları. *Süleyman Demirel Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 40, 330-355.
- Tekiner, M., & Gemici, E. (2019). Türkiye'nin mevcut iç güvenlik yapısı ve 15 temmuz sonrası yeni bir yapılanma modeli. *Anadolu Üniversitesi Sosyal Bilimler Dergisi*, 19 (15 Temmuz Özel Sayısı), 15-40.
- The White House. (2001). “Address to a joint session of congress and the american people” 14 Şubat 2023 tarihinde <https://georgewbush-whitehouse.archives.gov/news/releases/2001/09/20010920-8.html> adresinden erişildi.

- Tiryaki, E., & Özdal, B. (2020). Açık kaynak istihbaratında sosyal medyanın rolünün analizi. *Arhuss*, 3(2), 267-296.
- Toffler, A., & Toffler, H. (1994). *21. Yüzyılın şafağında savaş ve savaş karşıtı mücadele*. (M. Harmancı, Çev.) İstanbul: Sabah Yayınları.
- Treverton, G. (2001). *Reshaping national intelligence for an age of information*. Cambridge: Cambridge University Press.
- Tzu, S. (2008). *Savaş sanatı*. (S. Özbudun, ve Z. Ataman, Çev.) İstanbul: Anahtar Kitaplar.
- Ucuzsatar, N. (1986). *Askeri coğrafya*. İstanbul: Harp Akademileri Basımevi.
- Uçarol, R. (1995). *Siyâsî tarih*. İstanbul: Filiz Kitapevi.
- Upa. (2019). “Uluslararası politika akademisi.” 19 Aralık 2022 tarihinde <http://politikaakademisi.org/2019/10/23/uluslararası-iliskileri-teorileri-acısından-guvenlik-kavrami-i/> adresinden erişildi.
- Us Army Chemical School . (2022). “Tpub.Com.” 26 Eylül 2022 tarihinde intelligence reference and training: <https://armyintelligence.tpub.com/is0342b/basic-principles-of-intelligence-operations-8.htm> adresinden erişildi.
- Ülker, E. (2016). İşgal İstanbul’unda müdafaa-i milliye’nin kuruluşu üzerine bir değerlendirme: itihatçılar, komünistler, sosyalistler. *Kebikeç*, 41, 67-94.
- Ünal, A., & Yarman, S. (2015). *Stratejik karar verme boyutunda bilgi toplama - işleme amaçlı karar destek sistemler*. Ankara: Nobel Yayınları.
- Ünlü, F. (2020). “Medikal istihbaratın esasları.” 02 Ocak 2023 tarihinde sabah gazetesi: <https://www.sabah.com.tr/yazarlar/cumartesi/ferhat-unlu/2020/05/23/medikal-istihbaratin-esaslari> adresinden erişildi.
- Valiyeva, K. (2020). Covid-19 ile ulus devleti yeniden düşünmek. *İstanbul Ticaret Üniversitesi Sosyal Bilimler Dergisi, Özel Ek(37)*, 390-403.
- Varol, A. (2022). “Siber istihbarat ve siber tehdit istihbaratı.” 13 Şubat 2023 tarihinde <https://gaissecurity.com/blog/siber-istihbarat-ve-siber-tehdit-istihbarati/#:~:text=Siber%20%C4%B0stihbarat%C4%B1n%20%C3%96nemive>

text=Dolay% C4% B1s% C4% B1yla% 20veri% 20ihlalinin% 20% C3% B6ncesinde
% 20fark,ya% C5% 9Fanmas% C4% B1% 20olas% C4% B1% 20ihlallerin% 20ger% C
3% A7 adresinden eriřildi.

Vatis, M. (2001). "Cyber attacks during the war on terrorism: A predictive analysis." 04
řubat 2023 tarihinde <https://apps.dtic.mil/sti/pdfs/ada395300.pdf> adresinden
eriřildi.

Vbs. (2022). "Federal Intelligence Service" 24 Ekim 2022 tarihinde
[https://www.vbs.admin.ch/en/ddps/organisation/administrative-
units/intelligence-service.html](https://www.vbs.admin.ch/en/ddps/organisation/administrative-units/intelligence-service.html) adresinden eriřildi.

Volkman, E. (2004). *Casusluk*. (M. A. Sevda Kubilay, Çev.) İstanbul: Truva Yayınları.

Waltz, K. (1979). *Theory of International Politics*. Mc Grew Hill.

Wark, W. (2003). Introduction: Learning to live with intelligence. *Intelligence And
National Security*, 18(4), 1-14.

Warner, M. (2002). "Wanted: A definition of intelligence. studies in intelligence". 07
Nisan 2023 tarihinde <https://apps.dtic.mil/sti/pdfs/ADA525816.pdf> adresinden
eriřildi.

Warner, M. (2006). Sources and methods for the study of intelligence. New York:
Routledge Taylor And Francis Group.

Warner, M. (2010). 'US Intelligence and Vietnam':The Official Version(S). *Intelligence
And National Security*, 25(5), 611-637.

Warner, M. (2014). *The Rise and fall of intelligence: An international security history*.
George Town: George Town University Press.

Wheaton, K.J. "Tweaking The Intelligence Cycle (Let's Kill The Intelligence Cycle)". 07
Nisan 2023 tarihinde [https://sourcesandmethods.blogspot.com/2011/06/part-8-
tweaking-intelligence-cycle-lets.html](https://sourcesandmethods.blogspot.com/2011/06/part-8-tweaking-intelligence-cycle-lets.html) adresinden eriřildi.

West, N. (2014). *Historical dictionary of British intelligence* (2. Baskı). Washington:
Scarecrow Press.

- Willbanks, J. (2018). "Drinking your own bathwater: Tet intelligence failures." 17 Ocak 2023 tarihinde <https://www.historynet.com/drinking-bathwater-tet-intelligence-failures/#:~:text=this%20lack%20of%20coordination%20and,a%20surprise%20when%20it%20came> adresinden erişildi.
- Wohlstetter, R. (1962). *Pearl Harbor: Warning and decision*. California: Stanford University Press.
- Yeniçağ Gazetesi. (2022). "Dünya tarihinde çok ses getiren 10 siber saldırı." 30 Aralık 2022 tarihinde <https://www.yenicaggazetesi.com.tr/hackerlarin-en-buyuk-siber-saldirilari-listesi-521508h.htm> adresinden erişildi.
- Yıldız, G. (2019). *Osmanlı Devletinde askeri istihbarat*. İstanbul: Yeditepe Yayınevi.
- Yılmaz, B. (2020). Siber terörizm ve değişen istihbarat anlayışı. *Anadolu Strateji Dergisi*, 1(1), 65-81.
- Yılmaz, İ. (2005). "Çin Ekonomisi'nde büyümenin dinamikleri." 15 Şubat 2023 tarihinde https://www.academia.edu/31889860/%C3%87in_Ekonomisi_nde_B%C3%BCy%C3%BCmenin_Dinamikleri adresinden erişildi.
- Yılmaz, N. (2021). "Sars-Cov-2'nin laboratuvarından kaçtığı kanıtlandı mı?." 02 Ocak 2023 tarihinde <https://teyit.org/dosya-sars-cov-2-laboratuvaridan-mi-kacti> adresinden erişildi.
- Yılmaz, S. (2006). *21. yüzyılda güvenlik ve istihbarat*. İstanbul: Alfa Yayınları.
- Yılmaz, S. (2011). 11 Eylül sonrasında ABD ve Türkiye'deki iç güvenlik yeniden yapılanmalarının karşılaştırması. *Ç.Ü. Sosyal Bilimler Enstitüsü Dergisi*, 20(3), 361-380.
- Yılmaz, S. (2013). ABD istihbaratı 2013. *Teori Dergisi*, (Nisan), 47-61.
- York, B. (2014). United States counterintelligence. *Global Security Studies*, 5(4), 20-27.
- Yurdasev, N. (2005). Uluslararası ilişkilere teorik bakmak. *Uluslararası İlişkiler Dergisi*, (Özel Sayı: Türkiye'de Uluslararası İlişkiler Çalışmaları ve Eğitimi), 155-163.
- Yüce, M., & Akkaya, H. (2020). Mali suçlarla kurumsal mücadele ve bazı ülke örnekleri. *Uygulamalı Bilimler Fakültesi Dergisi*, 2(2), 40-61

Zabunođlu, H.G. (2018). Günümüzde ulus-devlet. *Erciyes Üniversitesi Hukuk Fakültesi Dergisi*, 13(1), 535-559.



TURNİTİN RAPORU

Gözde Dikici

ORJİNALLİK RAPORU

%8	%8	%2	%4
BENZERLİK ENDEKSİ	İNTERNET KAYNAKLARI	YAYINLAR	ÖĞRENCİ ÖDEVLERİ

BİRİNCİL KAYNAKLAR

1	acikbilim.yok.gov.tr İnternet Kaynağı	%2
2	dergipark.org.tr İnternet Kaynağı	%1
3	www.stratejikortak.com İnternet Kaynağı	<%1
4	www.researchgate.net İnternet Kaynağı	<%1
5	acikerisim.ybu.edu.tr:8080 İnternet Kaynağı	<%1
6	admin.inonu.edu.tr İnternet Kaynağı	<%1
7	cdn-cms.f-static.com İnternet Kaynağı	<%1
8	docplayer.biz.tr İnternet Kaynağı	<%1
9	kho.msu.edu.tr İnternet Kaynağı	<%1

10	www.acarindex.com İnternet Kaynađı	<% 1
11	sortyourgrade.com İnternet Kaynađı	<% 1
12	paperity.org İnternet Kaynađı	<% 1
13	Submitted to Atilim University Öđrenci Ödevi	<% 1
14	Submitted to Istanbul Aydin University Öđrenci Ödevi	<% 1
15	Submitted to Macquarie University Öđrenci Ödevi	<% 1
16	ressjournal.com İnternet Kaynađı	<% 1
17	www.openaccess.hacettepe.edu.tr:8080 İnternet Kaynađı	<% 1
18	Submitted to The Scientific & Technological Research Council of Turkey (TUBITAK) Öđrenci Ödevi	<% 1
19	www.dunyabizim.com İnternet Kaynađı	<% 1
20	Submitted to Loughborough University Öđrenci Ödevi	<% 1
21	stratejikistihbarat.files.wordpress.com	

İnternet Kaynađı

<% 1

22

Submitted to American Public University
System

Öđrenci Ödevi

<% 1

23

Submitted to University of Central Florida

Öđrenci Ödevi

<% 1

24

dspace.baskent.edu.tr

İnternet Kaynađı

<% 1

25

www.mit.gov.tr

İnternet Kaynađı

<% 1

26

Submitted to THK University

Öđrenci Ödevi

<% 1

27

dergipark.gov.tr

İnternet Kaynađı

<% 1

28

ro.ecu.edu.au

İnternet Kaynađı

<% 1

29

acikerisim.aku.edu.tr

İnternet Kaynađı

<% 1

30

"Digital Business Strategies in Blockchain
Ecosystems", Springer Science and Business
Media LLC, 2020

Yayın

<% 1

31

Submitted to European University of Lefke

Öđrenci Ödevi

<% 1

32	Submitted to Massey University Öğrenci Ödevi	<% 1
33	Submitted to Police Academy Öğrenci Ödevi	<% 1
34	dspace.kocaeli.edu.tr:8080 İnternet Kaynağı	<% 1
35	imascon.com İnternet Kaynağı	<% 1
36	kaysem13.gantep.edu.tr İnternet Kaynağı	<% 1
37	kaynakca.hacettepe.edu.tr İnternet Kaynağı	<% 1
38	repository.nwu.ac.za İnternet Kaynağı	<% 1
39	search.trdizin.gov.tr İnternet Kaynağı	<% 1
40	www.hurriyet.com.tr İnternet Kaynağı	<% 1
41	Submitted to Southern New Hampshire University - Continuing Education Öğrenci Ödevi	<% 1
42	acikarsiv.ankara.edu.tr İnternet Kaynağı	<% 1
43	dspace.gazi.edu.tr İnternet Kaynağı	<% 1

		<% 1
44	openaccess.ogu.edu.tr:8080 İnternet Kaynağı	<% 1
45	Submitted to London School of Economics and Political Science Öğrenci Ödevi	<% 1
46	Submitted to University of Maryland, University College Öğrenci Ödevi	<% 1
47	haberajandanet.com İnternet Kaynağı	<% 1
48	Submitted to Beykent Üniversitesi Öğrenci Ödevi	<% 1
49	Submitted to Hacettepe University Öğrenci Ödevi	<% 1
50	link.springer.com İnternet Kaynağı	<% 1
51	openaccess.hku.edu.tr İnternet Kaynağı	<% 1
52	sites.google.com İnternet Kaynağı	<% 1
53	Harry Blutstein. "Chapter 3193 Globalization and World Trade Organization", Springer Science and Business Media LLC, 2022	<% 1

54 Submitted to Instituto Universitário Militar
Öğrenci Ödevi <% 1

55 Submitted to Troy University
Öğrenci Ödevi <% 1

56 iibf.ksu.edu.tr
İnternet Kaynağı <% 1

57 revolution.allbest.ru
İnternet Kaynağı <% 1

58 Submitted to Gaziantep Aniversitesi
Öğrenci Ödevi <% 1

59 dergipark.ulakbim.gov.tr
İnternet Kaynağı <% 1

60 dspace.unive.it
İnternet Kaynağı <% 1

61 genclerle360.cbu.edu.tr
İnternet Kaynağı <% 1

62 zir.nsk.hr
İnternet Kaynağı <% 1

63 9lib.net
İnternet Kaynağı <% 1

64 Submitted to King's College
Öğrenci Ödevi <% 1

65 Submitted to Middle East Technical University

Öğrenci Ödevi

<% 1

66

Submitted to Selçuk Üniversitesi

Öğrenci Ödevi

<% 1

67

Submitted to University of Leicester

Öğrenci Ödevi

<% 1

68

acikarsiv.aydin.edu.tr

İnternet Kaynağı

<% 1

69

ydemokrat.blogspot.com

İnternet Kaynağı

<% 1

70

AKDENİZ, Ayşe Özlem. "OSMANLI'NIN İTALYAN MÜZİSYENLERİ*", Abidin Temizer, 2017.

Yayın

<% 1

71

ALTAY AYDIN, Suna Canan. "Ankara Etnografya Müzesi koleksiyonunda yer alan Art Nouveau üsluplu yıldız porselenleri", Sadberk Hanım Müzesi, 2014.

Yayın

<% 1

72

Submitted to Marmara University

Öğrenci Ödevi

<% 1

73

phdernegi.org

İnternet Kaynağı

<% 1

74

platonunmagarasi.home.blog

İnternet Kaynağı

<% 1

75	www.archeo.ru İnternet Kaynađı	<% 1
76	www.cceol.com İnternet Kaynađı	<% 1
77	www.slideshare.net İnternet Kaynađı	<% 1
78	kriterdergi.com İnternet Kaynađı	<% 1
79	papers.academic-conferences.org İnternet Kaynađı	<% 1
80	tr.scribd.com İnternet Kaynađı	<% 1
81	Davis. 21st Century Psychology Yayın	<% 1
82	Submitted to Rutgers University, New Brunswick Öđrenci Ödevi	<% 1
83	SÜMER, Gültekin. "Dıř politikada süreklilik-deđiřim çekiřmesi", Uluslararası Stratejik Arařtırmalar Kurumu, 2010. Yayın	<% 1
84	app.trdizin.gov.tr İnternet Kaynađı	<% 1
85	archive.org İnternet Kaynađı	<% 1

86 ebin.pub
İnternet Kaynađı <% 1

87 ects.ieu.edu.tr
İnternet Kaynađı <% 1

88 ellinikosthrilos.gr
İnternet Kaynađı <% 1

89 isletmecilik.org
İnternet Kaynađı <% 1

90 libratez.cu.edu.tr
İnternet Kaynađı <% 1

91 sde.org.tr
İnternet Kaynađı <% 1

92 tasam.org
İnternet Kaynađı <% 1

93 trockist.net
İnternet Kaynađı <% 1

94 www.globalsavunma.com.tr
İnternet Kaynađı <% 1

95 www.historynet.com
İnternet Kaynađı <% 1

96 Submitted to Edith Cowan University
Öđrenci Ödevi <% 1

97 Submitted to St.Mary's High School
Öđrenci Ödevi <% 1

98 acikerisim.sakarya.edu.tr <% 1
Internet Kaynađı

99 curve.carleton.ca <% 1
Internet Kaynađı

100 disser.spbu.ru <% 1
Internet Kaynađı

101 doczz.biz.tr <% 1
Internet Kaynađı

102 dokumen.pub <% 1
Internet Kaynađı

103 earsiv.anadolu.edu.tr <% 1
Internet Kaynađı

104 hr.wikipedia.org <% 1
Internet Kaynađı

105 issuu.com <% 1
Internet Kaynađı

106 it.wikipedia.org <% 1
Internet Kaynađı

107 s3-eu-west-1.amazonaws.com <% 1
Internet Kaynađı

108 tokatsempozyum2018.gop.edu.tr <% 1
Internet Kaynađı

109 www.afri-ct.org <% 1
Internet Kaynađı

110	www.insackongre.com İnternet Kaynağı	<% 1
111	www.kho.edu.tr İnternet Kaynağı	<% 1
112	www.tchaber.org İnternet Kaynağı	<% 1
113	www.wikizero.com İnternet Kaynağı	<% 1
114	ytbweb1.blob.core.windows.net İnternet Kaynağı	<% 1
115	ÖZER, Yusuf. "Terörizmle Mücadelede İstihbaratın Rolü: Kültürel İstihbarat Konsepti", İstanbul Gelişim Üniversitesi, 2015. Yayın	<% 1
116	(Ateş, Hasan and Utku, Mustafa Kemal). "Kamu Güvenliğinde İstihbarat Sisteminin Değerlendirilmesi", Atılım Üniversitesi Sosyal Bilimler Enstitüsü Kamu Yönetimi ve Siyaset Bilimi Anabilim Dalı, 2012. Yayın	<% 1
117	Len Scott, Peter Jackson. "The Study of Intelligence in Theory and Practice", Intelligence and National Security, 2004 Yayın	<% 1
118	Submitted to State College of Florida, Manatee - Sarasota (formerly, Manatee	<% 1

Community College)

Öğrenci Ödevi

-
- 119 beynelmilepost.com <% 1
İnternet Kaynağı
-
- 120 www.foruq.com <% 1
İnternet Kaynağı
-
- 121 **IFoA** <% 1
Yayın
-
- 122 YILMAZ, Sefer. "11 Eylül sonrasında ABD ve
Türkiyedeki iç güvenlik yeniden
yapılanmalarının karşılaştırılması", Çukurova
Üniversitesi, 2011. <% 1
Yayın
-
- 123 www.teram.org <% 1
İnternet Kaynağı
-

Alıntılarını çıkart üzerinde
Bibliyografyayı Çıkart üzerinde

Eşleşmeleri çıkar Kapat

ÖZGEÇMİŞ

Adı ve Soyadı: Gözde DİKİCİ

Öğrenim Durumu:

Derece	Alan	Üniversite	Yıl
Lisans	İşletme	İhsan Doğramacı Bilkent Üniversitesi	2005
Yüksek Lisans	Uluslararası İlişkiler	Atılım Üniversitesi	2023

İş Deneyimi:

Çalıştığı Yer	Görev	Yıl
İlbank Genel Müdürlüğü	Uzman	2011

Yabancı Diller: İngilizce

Tarih: 03.04.2023

