

**T.C.**  
**HARP AKADEMİLERİ**  
**STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ**

**KARŞI İSTİHBARATTA İNSAN BOYUTUNUN İRDELENMESİ:**  
**GAFİL MUHBİRLİK ÖRNEĞİ**

**ULUSLARARASI İLİŞKİLER ANABİLİM DALI**  
**YÜKSEK LİSANS TEZİ**

**Hazırlayan**  
**Mehmet Yenal ŞAHİN**

**Tez Danışmanı**  
**Yrd. Doç. Dr. Şamil ÜNSAL**

**İSTANBUL – 2013**

(BU SAYFA BOŞ BIRAKILMIŞTIR)

## TEZ TANITIM FORMU

**YAZAR ADI SOYADI** : Mehmet Yenal ŞAHİN

**TEZİN DİLİ** : Türkçe

**TEZİN ADI** : Karşı İstihbaratta İnsan Boyutunun İrdelenmesi: Gafil Muhbirlik Örneği

**ENSTİTÜ** : Stratejik Araştırmalar Enstitüsü

**ANA BİLİM DALI** : Uluslararası İlişkiler Ana Bilim Dalı

**TEZİN TÜRÜ** : Yüksek Lisans

**TEZİN TARİHİ** : 18 Haziran 2013

**SAYFA SAYISI** : 120

**TEZ DANIŞMANI** : Yrd. Doç Dr. Şamil ÜNSAL

**DİZİN TERİMLERİ** : Karşı İstihbarat, İstihbarata Karşı Koyma (İKK), Casusluk, Karşı Casusluk (Kontrespiyonaj), Pasif ve Aktif İKK Önlemleri, Gafil Muhbirlik.

**TÜRKÇE ÖZET** : Bu çalışmada, karşı istihbarat kavramı ve önemi, etkili bir karşı istihbarat sistemi için alınması gereken pasif ve aktif önlemler, karşı istihbarattaki yadsınamaz insan boyutu ve etkileri ile daha önce araştırma konusu edilmemiş olan “gafil muhbirlik” olgusu ortaya konularak bir durumsal ve kurumsal farkındalık yaratılmaya çalışılacaktır.

**DAĞITIM LİSTESİ** : 1. Stratejik Araştırmalar Enstitüsüne  
2. YÖK Ulusal Tez Merkezine

**Bu tezin içerdiği hususlar bireysel görüşlerimi yansıtır. Türk Silahlı Kuvvetlerinin görüşlerini yansıtmaz.**

Mehmet Yenal ŞAHİN

**T.C.**  
**HARP AKADEMİLERİ**  
**STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ**

**KARŞI İSTİHBARATTA İNSAN BOYUTUNUN İRDELENMESİ:**  
**GAFİL MUHBİRLİK ÖRNEĞİ**

**ULUSLARARASI İLİŞKİLER ANABİLİM DALI**  
**YÜKSEK LİSANS TEZİ**

**Hazırlayan**  
**Mehmet Yenal ŞAHİN**

**Tez Danışmanı**  
**Yrd. Doç. Dr. Şamil ÜNSAL**

**İSTANBUL – 2013**

STRATEJİK ARAŞTIRMALAR ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Mehmet Yenal ŞAHİN'in "Karşı İstihbaratta İnsan Boyutunun İrdelenmesi: Gafil Muhbirlik Örneği" adlı tez çalışması, jürimiz tarafından ULUSLARARASI İLİŞKİLER ana bilim dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

Başkan

Prof.Dr. Tolga YARMAN

Üye

Prof.Dr. Feridun YENİSEY

Üye

Yrd. Doç. Dr. Şamil ÜNSAL

(Danışman)

ONAY

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduğunu onaylarım.

18 / 06 / 2013

Hasip SAYGILI  
Dr. Kurmay Albay  
Enstitü Müdürü

## ÖZET

Karşı istihbarat veya başka bir deyişle istihbarata karşı koyma (İKK), en az istihbarat kadar önemli ve hatta daha da karmaşık ve zorlu bir faaliyettir. Tarih boyunca, istihbarat elde etmek için çabalayan ülkeler, kurumlar ve şirketler yani kısacası her türlü organizasyon, İKK önlemleri için de –istihbarat kadar olmasa bile– oldukça fazla enerji ve kaynak ayırmışlardır.

Günümüzde, gerek istihbarat faaliyetlerine karşı koyabilmek, gerekse dış güçlerin kötü emel ve arzularına boyun eğmemek, her şeyden önce hazırlıklı olmayı gerektirir. Üstünlüğün sağlanması, elde bulundurulması ve sürdürülmesi güvenilir bir istihbarat sisteminin yanında etkili bir İKK sistemi ve çabasıyla mümkündür. Etkin bir karşı istihbarat sistemi kurabilmek için pasif ve aktif olarak ikiye ayrılabilen olan İKK önlemlerinin doğru şekilde tespit edilmesi ve uygulanması gereklidir.

İstihbaratta olduğu gibi karşı istihbaratta da en önemli aktör “insan”dır. Kurulacak olan İKK sisteminin insan etkeni göz önünde bulundurularak oluşturulması lazım gelir. Özellik, zaaf ve davranış yelpazesi çok geniş olan insanlar, birbirinden çok farklıdırlar ve insanların İKK sistemine yapacakları olumlu katkılarının, olumsuz katkılarının fazla olması ancak insan etkenine gereken önemin gösterilmesiyle mümkündür.

Organizasyonun istihbarat bakımından güvenliğine, zaman zaman casusluk kadar tehlikeli olabilen “gafil muhbirlik” olgusu vurgulanarak, gafil muhbirliği engellemek ya da azaltmak için gerekli önlemlerin alınması veya en azından gafil muhbirlik kavramından haberdar olunması sağlanabilecektir.

Bu çalışmada, karşı istihbarat kavramı ve önemi, etkili bir karşı istihbarat sistemi için alınması gereken pasif ve aktif önlemler, karşı istihbarattaki yadsınamaz insan boyutu ve etkileri ile daha önce araştırma konusu edilmemiş olan “gafil muhbirlik” olgusu ortaya konularak bir durumsal ve kurumsal farkındalık yaratılmaya çalışılacaktır.

## **SUMMARY**

Counterintelligence (CI) is at least as important as intelligence and even more complex and challenging activity. Throughout history, the countries, institutions, and companies striving to gather intelligence have a great amount of energy and resource allocation –if not as much as intelligence– for CI.

Today, it is foremost required to be prepared to be able to resist the intelligence activities and to surrender evil ambitions of foreign states and organizations. Achievement and maintenance of the initiative is possible by a reliable intelligence system and next to it an effective CI systems and CI efforts. To establish an effective CI system, it is required the CI measures which can be divided into passive and active measures should correctly be identified and implemented.

The most important actor in CI is “human”, as in intelligence. The CI system is to be established by considering the human factor. People, having a wide feature, weaknesses, and behavior range are very different from each other, and it is just possible the positive effects to be more than negative effects of human beings to the CI system by paying the required importance to the human factor.

By emphasizing the “unwary informant” fact which sometimes could be dangerous to the security of the organization in terms of intelligence, it could be obtained the necessary measures to reduce or prevent unwary informants, or at least to be aware of the notion of the unwary informant.

In this study, it is tried to be created a situational and organizational awareness by putting forth the concept and importance of CI, the passive and active measures should be taken for an effective CI system, the undeniable human dimension, and the effects of it in CI, and the “unwary informant” phenomenon which have not been previously the subject of researches.

## İÇİNDEKİLER

|                                                                         | SAYFA |
|-------------------------------------------------------------------------|-------|
| ÖZET                                                                    | I     |
| SUMMARY                                                                 | II    |
| İÇİNDEKİLER                                                             | III   |
| KISALTMALAR                                                             | V     |
| ÖN SÖZ                                                                  | VI    |
| GİRİŞ                                                                   | 1     |
| BİRİNCİ BÖLÜM: KARŞI İSTİHBARAT / İKK                                   |       |
| 1.1. KARŞI İSTİHBARATIN TANIMI VE ÖNEMİ                                 | 4     |
| 1.2. KARŞI İSTİHBARATIN AMAÇLARI VE GÖREVLERİ                           | 12    |
| 1.3. KARŞI İSTİHBARATIN KAYNAKLARI                                      | 15    |
| 1.4. KARŞI İSTİHBARATTA BAŞARININ İLKELERİ                              | 17    |
| 1.5. KARŞI İSTİHBARATÇIDA BULUNMASI GEREKEN ÖZELLİKLER                  | 19    |
| İKİNCİ BÖLÜM: İKK ÖNLEMLERİ                                             |       |
| 2.1. GENEL                                                              | 23    |
| 2.2. PASİF İKK ÖNLEMLERİ                                                | 26    |
| 2.2.1. Personel Güvenliği / Kişisel Koruyucu Güvenlik                   | 27    |
| 2.2.2. Fiziksel Güvenlik                                                | 30    |
| 2.2.3. Bilgi, Bilgi İşlem, İletişim ve Elektronik Güvenliği             | 34    |
| 2.2.4. Eğitim, Denetim ve Farkındalık                                   | 40    |
| 2.3. AKTİF İKK ÖNLEMLERİ                                                | 45    |
| 2.3.1. Karşı Casusluk / Casusluğa Karşı Koyma                           | 48    |
| 2.3.1.1. Casusluk                                                       | 48    |
| 2.3.1.1.1. Casus Türleri                                                | 50    |
| 2.3.1.1.2. Casusluğa Kılıf Teşkil Eden Meslekler                        | 52    |
| 2.3.1.1.3. İnsanları Casus Olmaya Yönelten Nedenler                     | 56    |
| 2.3.1.1.3.1. Maddi Motifler                                             | 57    |
| 2.3.1.1.3.2. Duygusal Motifler                                          | 58    |
| 2.3.1.1.3.3. İdeolojik Motifler                                         | 59    |
| 2.3.1.1.4. Casus Adaylarında Aranılan Özellikler                        | 60    |
| 2.3.1.1.5. Casusların Bilgi Toplama Yöntem ve Teknikleri                | 62    |
| 2.3.1.2. Casusluğa Karşı Koyma                                          | 65    |
| 2.3.1.2.1. Casusluğun ve İstihbarat Operasyonlarının Olası Göstergeleri | 66    |

|                                                                             |     |
|-----------------------------------------------------------------------------|-----|
| 2.3.1.2.2. Casusluk Girişimlerine Karşı Alınabilecek Önlemler               | 70  |
| 2.3.2. Keşif ve Gözetlemeye Karşı Koyma                                     | 72  |
| 2.3.3. Aldatma                                                              | 72  |
| 2.3.4. Siber ve Elektronik Karşı Tedbirler (EKT)                            | 74  |
| ÜÇÜNCÜ BÖLÜM: KARŞI İSTİHBARATTA İNSAN BOYUTU                               |     |
| 3.1. İNSAN DAVRANIŞLARININ OLUŞUMU                                          | 76  |
| 3.2. İNSAN DAVRANIŞLARININ KARŞI İSTİHBARATA ETKİLERİ                       | 83  |
| 3.2.1. İstihbaratçıların İstismar Edebilecekleri Zayıflıklar ve Davranışlar | 85  |
| 3.2.2. Düşkünlükleri ve Davranışları Şekillendirme Yöntemleri               | 86  |
| 3.3. RUHSAL BOZUKLUKLARIN KARŞI İSTİHBARATA ETKİLERİ                        | 88  |
| 3.3.1. Kişilik Bozuklukları                                                 | 88  |
| 3.3.1.1. Paranoit Kişilik Bozukluğu                                         | 89  |
| 3.3.1.2. Şizoit Kişilik Bozukluğu                                           | 90  |
| 3.3.1.3. Şizotipal Kişilik Bozukluğu                                        | 91  |
| 3.3.1.4. Anti Sosyal Kişilik Bozukluğu                                      | 91  |
| 3.3.1.5. Sınırdaki (Borderline) Kişilik Bozukluğu                           | 93  |
| 3.3.1.6. Histrionik Kişilik Bozukluğu                                       | 93  |
| 3.3.1.7. Narsisistik Kişilik Bozukluğu                                      | 93  |
| 3.3.1.8. Kaçınan (Çekinen) Kişilik Bozukluğu                                | 94  |
| 3.3.1.9. Bağımlı Kişilik Bozukluğu                                          | 95  |
| 3.3.1.10. Obsesif–Kompulsif Kişilik Bozukluğu                               | 96  |
| 3.3.1.11. Pasif–Agresif Kişilik Bozukluğu                                   | 96  |
| 3.3.2. Diğer Ruhsal Bozukluklar                                             | 96  |
| DÖRDÜNCÜ BÖLÜM: GAFİL MUHBİRLİK                                             |     |
| 4.1. MUHBİR KAVRAMI                                                         | 99  |
| 4.2. GAFİL MUHBİRLİK OLGUSU                                                 | 100 |
| 4.3. GAFİL MUHBİRLİĞİ ENGELLEMEK VEYA AZALTMAK İÇİN YAPILMASI GEREKENLER    | 103 |
| 4.4. ÖRNEK OLAYLARDA GAFİL MUHBİRLİK                                        | 107 |
| 4.4.1. Örnek Olay–1: Operasyonu Bozan Kantinci                              | 107 |
| 4.4.2. Örnek Olay–2: İngiliz Casusa Bilgi Veren Türk Casus                  | 108 |
| 4.4.3. Örnek Olay–3: Gurbetçilerin Gafleti                                  | 109 |
| SONUÇ                                                                       | 111 |
| KAYNAKÇA                                                                    | 115 |
| ÖZGEÇMİŞ                                                                    | –   |

## KISALTMALAR

|        |                                                                          |
|--------|--------------------------------------------------------------------------|
| ABD    | : AMERİKA BİRLEŞİK DEVLETLERİ                                            |
| a.g.e. | : ADI GEÇEN ESER                                                         |
| AKİS   | : AÇIK KAYNAK İSTİHBARATI                                                |
| bkz.   | : BAKINIZ                                                                |
| CI     | : COUNTERINTELLIGENCE                                                    |
| CIA    | : CENTRAL INTELLIGENCE AGENCY (ABD MERKEZÎ İSTİHBARAT ÖRGÜTÜ)            |
| ÇEV.   | : ÇEVİREN                                                                |
| DİHMİT | : DEVLET İSTİHBARAT HİZMETLERİ VE MİLLÎ İSTİHBARAT TEŞKİLATI             |
| EKT    | : ELEKTRONİK KARŞI TEDBİRLER                                             |
| FBI    | : FEDERAL BUREAU OF INVESTIGATION (ABD FEDERAL SORUŞTURMA BÜROSU)        |
| GBT    | : GENEL BİLGİ TOPLAMA                                                    |
| GÖRİS  | : GÖRÜNTÜ İSTİHBARATI                                                    |
| İKK    | : İSTİHBARATA KARŞI KOYMA                                                |
| İNİS   | : İNSAN İSTİHBARATI                                                      |
| MI6    | : MILITARY INTELLIGENCE SECTION 6 (İNGİLTERE’NİN DIŞ İSTİHBARAT SERVİSİ) |
| MİT    | : MİLLÎ İSTİHBARAT TEŞKİLATI                                             |
| S.     | : SAYFA                                                                  |
| SİNİS  | : SİNYAL İSTİHBARATI                                                     |
| SS.    | : SAYFA SAYILARI (SAYFA ARALIĞI)                                         |
| SSCB   | : SOVYET SOSYALİST CUMHURİYETLER BİRLİĞİ                                 |
| TCK    | : TÜRK CEZA KANUNU                                                       |
| VB.    | : VE BENZERİ                                                             |

## ÖN SÖZ

Günümüzün istihbarat savaşlarında, karşı istihbarat daha fazla önem kazanmaya başlamıştır. 2001 yılında Amerika Birleşik Devletleri (ABD)'ne yapılan terörist saldırıların başarısının, teröristler açısından etkin bir karşı istihbarat uygulamasının ürünü olduğu göz önünde bulundurulduğunda, söz konusu önemin aratarak devam edeceğini söylemek yanlış olmaz.

Her türlü teknolojik gelişmeye rağmen karşı istihbarat konusunda en önemli aktörler halen insanlardır. İnsanların bireysel özellikleri ve davranışları, istihbarata karşı koyma (İKK) önlemleri bakımından belirleyici rol oynamaktadır.

Çalışmanın birinci bölümünde karşı istihbarat kavramı ve önemi, ikinci bölümünde İKK önlemleri, üçüncü bölümde insan etkeninin karşı istihbarata etkileri, dördüncü bölümde de gafil muhbirlik kavramı örneklerle ortaya konularak karşı istihbaratta bir farkındalık oluşturulmaya çalışılmıştır.

Bu bağlamda öncelikle bana yüksek lisans eğitimi görme imkânı tanıyan Türk Silahlı Kuvvetlerine, tezimin her aşamasında değerli katkı ve rehberliğiyle beni yönlendiren danışman hocam Yrd. Doç. Dr. Şamil ÜNSAL'a, İstanbul'un çeşitli üniversitelerinden gelerek bizleri aydınlatan ve üzerimizde büyük emekleri olan saygıdeğer öğretim üyelerimize ve eğitim süreci boyunca her türlü desteği bizden esirgemeyen tüm Harp Akademileri Komutanlığı Stratejik Araştırmalar Enstitüsü personeline şükranlarımı sunuyorum.

Ömür boyu sürmesini temenni ettiğim dostlukları için Stratejik Araştırmalar Enstitüsü'nde birlikte eğitim aldığım sınıf arkadaşlarıma, daha rahat bir çalışma ortamına sahip olmamda yardım ve desteklerini esirgemeyen anneme / kayınvalideme ve babama / kayınbabama, bana devamlı moral vererek çalışmalarım sırasında gösterdiği fedakârlık ve manevi destek için eşim Özlem'e ve varlığı ile yaşama sevinci veren oğlum Poyraz Efe'ye çok teşekkür ediyorum.

Mehmet Yenal ŞAHİN

## GİRİŞ

Devletler, varlıklarını daha uygun şartlarda sürdürebilmek ve ulusal çıkarlarını gerçekleştirmek amacıyla bir yandan düşman veya düşman olması muhtemel ve hatta dost ve müttefik (bağlaşıık) olarak gördükleri devletlerle ilgili istihbarat toplamaya çabalarırken diğey yandan da kendileri ile ilgili istihbarat toplanmasını önlemek ister ve bu yönde çalışırlar.

Söz konusu uğraşıyı çeşitli biçimlerde adlandırmak mümkündür. Genel olarak “karşı istihbarat” şeklinde kabul gören kavram, Millî İstihbarat Teşkilatı (MİT)’nda “kontrespiyonaj / casusluğa karşı koyma”, askerî terminolojide (terimler dizgesinde) de “istihbarata karşı koyma (İKK)” adıyla kullanılmaktadır.

Karşı istihbarat terimi, taşıdığı anlamın aksine genelde casusluğa karşı koyma veya aktif İKK önlemleri ile karıştırılmakta ve aslında bir anlam daralmasına uğramaktadır. Aynı şekilde İKK terimi de, sadece kişisel koruyucu önlemler veya pasif İKK önlemleri ile karıştırılarak benzer bir anlam daralmasına maruz kalmaktadır.

Bize göre, kurumların karşı istihbarata yaklaşımları ve algıları tamamen karşı istihbarat konusundaki görevlerinden ileri gelmektedir. Zira Türkiye’de karşı istihbaratın aktif yönünden öncelikli ve tek sorumlu kurum olan MİT’in, karşı istihbaratı casusluğa karşı koyma şeklinde tanımlamasının, bu görevinden ileri geldiğı düşünölmektedir. Keza diğey kurumların karşı istihbaratı tamamen koruyucu güvenlik önlemlerine sıkıştırma çabaları da benzer sebeplerden dolayı dibi görünmektedir.

Bu çalışmada, özünde birbiriyle aynı anlamlara gelen “karşı istihbarat” ve “İKK” adlandırmaları eş anlamlı olarak kullanılacaktır. Casusluğa karşı koyma / karşı casusluk ve koruyucu güvenlik kavramları ise bambaşka anlamlar taşıdıkları için ayrıca açıklanacaktır.

Öte yandan karşı istihbarat konusunda her ne kadar teknolojik gelişmeler durdurulamaz şekilde ilerlemeye devam etse de insan etkeninin önceliğini ve önemini yitirmesi olanaksızdır. Zira her şeyden önce kurulan bütün teknolojik sistemleri bile kullanacak olan insanlar olacaktır. Karşı istihbaratın en önemli ve sıralamada en önde gelen aktörü ve kaynağının insan olmasından hareketle, karşı

istihbaratta insan boyutunun ortaya konulmasına gereksinim olduğu değerlendirilmektedir. Bu bağlamda, dış güçlerin hedeflerine ulaşmalarına engel olabilmek ve onları istenilen şekilde yönlendirebilmek yani inisiyatifi her an elde bulundurabilmek için etkili bir karşı istihbarat sistemine sahip olmak gereklidir.

Çalışmanın üç temel problemi vardır. Ulusal kurum ve kuruluşlar başta olmak üzere ulusal yazın ve kamuoyunda karşı istihbarat, karşı casusluk ve koruyucu güvenlik tanımlamalarında hatalı algılamalar ve kullanımların varlığı ve bunların açıklanması ihtiyacı birinci problemi oluşturmaktadır. Karşı istihbaratta göz ardı edilemeyecek bir “insan” boyutunun varlığı ve bu durumun ortaya konulması ihtiyacı çalışmanın ikinci problemidir. Zaman zaman casusluktan daha zararlı olduğu dahi öne sürülebilecek olan “gafil muhbirlik” olgusunun irdelenmesi ve birtakım önlemler sunulması ihtiyacı da çalışmanın üçüncü problemidir.

Hatalı şekilde çoğu zaman birbirleriyle aynı anlamda kullanıldığı değerlendirilen karşı istihbarat, karşı casusluk ve koruyucu güvenlik terimlerinin, sanıldığı ve kullanıldığı gibi aynı anlamları ifade etmediği ortaya konularak var olduğu düşünülen kavram karışıklığına bir açıklık getirilmeye çalışılacaktır.

Ayrıca, karşı istihbaratta insan etkeninin önemi ve rolü, genel olarak ve gafil muhbirlik özelinde ortaya konulmaya çalışılacaktır. Böylece karşı istihbaratın; algılandığı gibi sadece istihbarat veya karşı istihbarat servislerinin görevi olmadığına, onların görevinin ağırlıklı olarak aktif İKK önlemlerini uygulamak (özellikle casuslukla mücadele) olduğuna, pasif İKK önlemlerinin bütün bireylerin (vatandaş, personel, çalışan vb.) katkısıyla anlam ve başarı kazanabileceğine dikkat çekmek amaçlanmaktadır.

Çalışmada öncelikle genel olarak karşı istihbarat kavramı ve yardımcı kavramlar, ardından İKK önlemleri ve genel anlamda karşı istihbaratta insan etkeninin yeri vurgulanacaktır. Ardından gafil muhbirlik olgusu ortaya konulmaya, neticesinde bir durumsal farkındalık oluşturulmaya ve İKK önlemleri kapsamında bireysel hataların önlenmesi bakımından genel bir “önlemler çerçevesi” sunulmaya çalışılacaktır.

Genel anlamda istihbarat ve dolayısıyla da karşı istihbarat için özellikle dilimizde geçerli olan bir kıt kaynak ortamının varlığı yadsınamaz bir gerçektir. Bu bağlamda Türkçe ve İngilizce kaynaklardan yapılan yazın taramasında, karşı

istihbaratta insan boyutu konusunda ortaya konulmuş çok az sayıda akademik çalışmaya rastlanmış, gafil muhbirlik konusunda ise hiçbir kaynağa ulaşılamamıştır. Bu çalışma sayesinde karşı istihbaratta insan boyutunun ve özellikle de daha önce hiç değinilmemiş olan gafil muhbirlik konusunun, karşı istihbarat bakımından önemi ortaya konulmaya çalışılacaktır.

Okuyucuyu tanımlar ve yoğun istihbarat bilgisi vermek suretiyle konudan uzaklaştırmamak ve konunun bütünlüğünü kaybetmemek adına, temel istihbarat kavramları konusunda yeterli bilgiye sahip olunduğu farz ve kabul edilecektir.

Ayrıca deprem gibi doğa olayları ile sabotaj, yıkıcı ve bölücü faaliyetlere karşı alınması gereken İKK önlemleri, ayrı birer araştırma konusu olmaları sebebiyle çalışmaya dâhil edilmeyecektir.

Çalışmanın genelinde bazı sözcüklerin öz Türkçeleri kullanılmak istense de; öz Türkçe karşılıklarının henüz tam anlamıyla kabul görmüş sözcükler olmaması, öz Türkçe sözcüklerin aynı anlamı tam olarak karşılayamaması ve istihbarat söz dağarcığında yerleşik bazı sözcüklerden vazgeçememek gibi nedenlerle (Örneğin angaje etmek sözcüğünün öz Türkçe karşılığı olan bağlamak sözcüğü aynı anlamı tam olarak karşılayamamaktadır.) yabancı kökenli birtakım sözcüklerin kullanılmasına devam edilecektir.

## BİRİNCİ BÖLÜM

### KARŞI İSTİHBARAT / İKK

#### 1.1. KARŞI İSTİHBARATIN TANIMI VE ÖNEMİ

Karşı istihbarat ya da diğer bir deyişle İKK, tarih boyunca istihbarat ile birlikte var olagelmıştır. Yani karşı istihbarat tarihinin, istihbarat tarihi ile aynı zamanlarda başladığı söylenebilir. Öyle ki, askerî strateji ve taktiğin temel kitabı olduğu kabul edilen ve Sun Tzu tarafından milattan önce 6'ncı yüzyılda yazılmış olan “Savaş Sanatı” adlı eserde casuslara karşı alınması gereken önlemler ve casusları lehimize kullanma yolları anlatılmaktadır. 11'inci yüzyıl Karahanlı Uygur Türklerinden Yusuf Has Hacib'in yazdığı Kutadgu Bilig'de ise karşı istihbaratın önemi şu şekilde vurgulanmaktadır: “Öncü kuvveti ile düşmanın yakınlarına kadar sokulmalı, otuna ve suyuna iyice dikkat ederek karargâh kurulmalıdır. (2349) Askerinin az veya çok olduğundan düşman haberli olmamalıdır.”<sup>1</sup>

Karşı istihbarata, günümüz de dâhil olmak üzere hiçbir dönemde hak ettiği önem gösterilmemiş ve istihbarat disiplinleri arasında her zaman “ikinci sınıf” muamelesi görmüştür.<sup>2</sup> Büyük ölçüde bu sebepten ötürü de sistemli olarak bir karşı istihbarat oluşumu ve örgütlenmeye Birinci Dünya Savaşı'na kadar pek rastlanamamaktadır. Birinci Dünya Savaşı ile karşı istihbaratın önemini kavramaya başlayan gelişmiş ülkeler çeşitli karşı istihbarat oluşumlarına başlamışlardır.

Amerika Birleşik Devletleri (ABD)'nde, askeri birlikler arasından seçilen akıllı ve elit kişilerin oluşturduğu ve “Sessiz Bekçiler” adını verdikleri bir Haber alma Örgütü kurulmuştur. Bu görevliler bilhassa; Birinci Dünya Savaşı sırasında yabancı ülkelerde bulunan Amerikan askerlerinin arasındaki hainleri, casusları ve bozguncuları izlemiş ve takip etmişlerdir. Ayrıca tüm görevleri Alman gizli servis görevlilerini avlamak olan “Intelligence Police” yani “İstihbarat Polisi”nin tesis edildiği de bilinmektedir. İkinci Dünya Savaşı, Soğuk savaş ve sonraki dönemlerde ise, İKK faaliyeti gittikçe gelişen ve önemi daha da artan, aynı zamanda daha iyi tekniklerle uygulanan bir statüye gelmiştir.<sup>3</sup>

<sup>1</sup> Bedri Sarıca, “Kutadgu Bilig'de Komutan ve Ordunun Nitelikleri”, *Atatürk Üniversitesi Türkiyat Araştırmaları Enstitüsü Dergisi*, Sayı: 37, Erzurum, 2008, 87–105, s. 98.

<sup>2</sup> The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States*, 2005, 485–497, s. 495.

<sup>3</sup> Gültekin Avcı, *İstihbarat Oyunları: Orduların Karanlık Senaryoları*, Birey Yayıncılık, İstanbul, 2007, s. 99.

Genel olarak “karşı istihbarat” adıyla kullanılan söz konusu kavram, MİT’te “kontrespiyonaj”, askerî terimler dizgesinde de “İKK” şeklinde yer almaktadır. Bu terimlerden de anlaşılabilceği gibi, karşı istihbarat hakkında bir kavram karışıklığı olduğunu söylemek mümkündür. Karşı istihbarat, sık sık ve yanlış bir şekilde, karşı casusluk ve koruyucu güvenlik önlemleri ile de aynı anlamlarda kullanılır.

Öncelikle, sıkça eş anlamda ya da birbirinin yerine kullanılan “karşı istihbarat”, “güvenlik önlemleri” veya “koruyucu güvenlik önlemleri”, “casusluk” ve “karşı casusluk / casusluğa karşı koyma” kavramlarını birbirinden ayırmak veya daha doğru bir ifadeyle tanımlamak gereklidir. Zira karşı istihbarat, söz konusu faaliyet dallarının tamamını kapsayan ve daha fazlasını ifade eden bir üst kavramdır.<sup>4</sup>

Karşı istihbaratın; “karşı istihbarat”, “İKK” veya “İKK istihbaratı” başlıkları altında ve farklı içeriklerde çok değişik tanımları yapılmaktadır. Bu tanımlardan bazıları şöyle sıralanabilir:

– **İKK**; savaş ve barış zamanlarında casusluk, sabotaj ve yıkıcı faaliyetler yoluyla, karşı ve yabancı istihbarat servislerinin belirli yöntemlerle yapmaya çalıştıkları zararlı faaliyetlerin tespiti ve etkisiz hâle getirilmesi ile karşı faaliyet yürüten kişi, grup ve kuruluşlar hakkında bilgi derlenerek bunların faaliyetleri, yöntemleri, hedefleri, amaçları ve yönetim kadrolarının tespitine çalışılması anlamına gelir.<sup>5</sup>

– **İKK istihbaratı**; devletlerin kendileriyle ilgili yaptıkları veya yapmayı planladıkları her türlü faaliyet ve stratejileri ile kendileri için hayati olarak nitelendirdikleri bilgi ve belgeyi düşman ya da düşman olarak nitelendirilebilecek kişi ve kurumlardan korumak, olası girişimleri tespit etmek ve ortaya çıkarmak, etkilerini en aza indirmek veya etkisiz kılmak amacı ile aktif ya da pasif istihbarat yapmaktır.<sup>6</sup>

– **Karşı istihbarat**; yabancı devletlerin istihbarat örgütlerinin ve birimlerinin organizasyon yapılarının ve davranışlarının çalışılması ve elde edilen bilginin uygulamaya sokulmasıdır.<sup>7</sup>

<sup>4</sup> William R. Johnson, *Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer*, Georgetown University Press, Washington D.C., 2009, s. 2.

<sup>5</sup> Avcı, *İstihbarat Oyunları... a.g.e.*, ss. 98–99.

<sup>6</sup> Bekir Çınar, *Devlet Güvenliği, İstihbarat ve Terör*, Sam Yayınları, Ankara, 1997, s. 120.

<sup>7</sup> John Ehrman, “What are We Talking about When We Talk about Counterintelligence?”, *Studies in Intelligence*, Vol.: 53, No.: 2, 2009, 5–20, s. 6.

– **İKK**; rakiplerin istihbarat faaliyetleriyle ilgilenen istihbaratın bir alt disiplini<sup>8</sup>.

– “**İKK**; rakiplerin avantaj sağlamak için istihbarata önem verdiklerini kabul etmek ve bu öngöründen hareketle rakiplerin istihbarat toplama faaliyetlerinin önüne geçmek için önleme faaliyetlerinin yapılmasıdır.”<sup>9</sup>

– **İKK**; yönetimlerin iç ve dış işlerindeki güvenliğini de kapsayacak şekilde ülkenin politik, askerî ve ekonomik gücünü korumak ve kollamak için gereken, casusluk, sabotaj, yıkıcı faaliyetler vb. her türlü yasa dışı yöntemlerle ülkeyi zayıflatmayı veya yıkmayı hedefleyen oluşumlar hakkındaki her türlü bilgi olarak tanımlanabilir.<sup>10</sup>

– **Karşı istihbarat**; diğer ülkelerin istihbarat faaliyetlerini tanımlama, etkisizleştirme ve yönlendirme operasyonları ile bir ülkenin kendisiyle ilgili yapılan sabotajlara, kendi vatandaşlarına karşı yapılan suikastlara ve terörist eylemlere karşı uyguladığı istihbarat faaliyetidir.<sup>11</sup>

– **Karşı istihbarat**; yabancı hükümetler veya onların unsurları, dış güçler, kuruluşlar, kişiler ya da uluslararası terör örgütleri tarafından ya da onların adına yapılan casusluk, diğer istihbarat faaliyetleri, sabotaj veya suikastlara karşı korunmak için toplanan bilgi ve yürütülen aktif faaliyetlerin tamamı anlamına gelir.<sup>12</sup>

– **Karşı istihbarat**; ülkeye yönelen yabancı istihbarat tehditlerini belirlemek ve başa çıkmak işidir. Karşı istihbaratın temel ilgi alanı, yabancı devletlerin istihbarat örgütleri ve ulusötesi terör grupları gibi devlet dışı aktörlerdir. Karşı istihbaratın, ulusal sırların ve varlıkların yabancı istihbarat girişimlerine karşı korunmaları gibi pasif bir görevi ile yabancı istihbarat oluşumlarının ne yapmayı planladıklarını ve hatta daha önemlisi yapmayı hedeflediklerine ulaşamamalarını sağlamanın yollarını bulmak ve uygulamak gibi aktif bir görevi olmak üzere iki önemli görevi vardır.<sup>13</sup>

<sup>8</sup> Vincent H. Bridgeman, “Defence Counterintelligence, Reconceptualized”, *In Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence by Jennifer E. Sims and Burton Gerber*, 2008, 125–148, s. 126.

<sup>9</sup> Mutlu Köseli, *İstihbarat Temel Hususlar ve Güncel Konular*, Adalet Yayınevi, Ankara, 2011, s. 31.

<sup>10</sup> Charles V. Cate, “Counterintelligence for National Security”, *Studies in Intelligence*, Vol.: 2, No.: 4, 1958, 87–92, s. 87.

<sup>11</sup> Ümit Özdağ, *İstihbarat Teorisi*, Kripto Kitaplar, Ankara, 2009, s. 33, 159.

<sup>12</sup> Andreas H. Golovin, *Fundamental Elements of the Counterintelligence Discipline, Volume: 1, Universal Counterintelligence Core Competencies*, Nova Science Publishers Inc., 2011, s. 8.

<sup>13</sup> Ehrman, *a.g.e.*, s. 7.

– “**Karşı istihbarat**; dost, tarafsız, düşman ve düşman olması muhtemel ülkelerin çeşitli istihbarat kaynaklarını kullanarak hakkımızda istihbarat elde etme, zaafılarımızı (düşkünüklüklerimizi) belirleme, belirlenen düşkünüklükleri istismar etme (kötüye kullanma, sömürme), asimetrik etki yaratma ve bilginin güvenliğini hedef alma çabalarını ve faaliyetlerini tespit etme, teşhis etme, izleme, sömürme, engelleme vb. maksatlı yürütülen aktif ve pasif tüm çabalardır.”<sup>14</sup>

– **Karşı istihbarat**; hem bir faaliyet hem de bu faaliyetin bir ürünüdür. Ürün, bir ülkenin gizlice kendisine saldıran düşmanları hakkındaki güvenilir bilgilerdir. Bu düşmanların bazıları profesyonel istihbarat elemanları ve onları görevlendiren ajanlardır. Diğerleri ise casusluk ve karşı istihbarattan ziyade yıkıcılık veya ayaklanmayı teşvik etmek için örtü altında hareket ederler.<sup>15</sup>

Tüm bu tanımlardan yola çıkarak, karşı istihbaratın bizce daha kapsamlı ve doğru bir tanımını yapabilmek amacıyla bazı çıkarımlar ya da tespitler yapmakta yarar vardır. O hâlde karşı istihbarat:

–Düşman, dost, bağlaşıklık, ortak veya rakip olarak görülen herhangi bir kişi, grup, kurum, kuruluş veya devlet tarafından icra edilebilir.

–Ulusal / kurumsal güvenliğini sağlamayı ve ulusal / kurumsal güç unsurlarını ve bütünlüğünü korumayı amaçlar.

–Her kişi, grup, kuruluş veya devletin kendi plan, tasarımı ve stratejilerini yani kendisine ait hassas ve gizli olarak nitelendirdiği her türlü bilgiyi korumak maksadıyla uyguladığı faaliyetler bütünüdür.

–Savaşta ve barışta yani her zaman ve kesintisiz icra edilmesi lazım gelir.

–Bilgi elde etme çabası, açık kaynak istihbaratı (AKİS) gibi yasal yöntemlerle gerçekleştirilebileceği gibi, casusluk gibi yasal olmayan yöntemlerle de gerçekleştirilebilir. Bilgi elde etme çabası içinde olanlar; kişi, grup, kuruluş ve devletler olabilir. Bu unsurların yapısal ve davranışsal incelemesinin yapılması ve elde edilen bilginin uygulamaya geçirilmesi gereklidir.

<sup>14</sup> Avcı, *İstihbarat Oyunları... a.g.e.*, s. 99.

<sup>15</sup> A. C. Wasemiller, “The Anatomy of Counterintelligence”, *Studies in Intelligence*, Vol.: 13, No.: 1, 1969, 9–25, s. 10.

–İstihbarat toplama, casusluk, sabotaj, terör ve anarşi faaliyetleri, suikast, propaganda, elektronik yöntemler gibi çeşitli yöntem ve teknikler kullanılarak bilgi elde edilmesine karşı yapılan bir faaliyettir.

–Pasif / statik / tedafüi / savunucu / koruyucu ve aktif / taarruzî / agresif / saldırgan önlemler ve yöntemler içerir.

–Her türlü yabancı istihbari girişimden öncelikle korunmaya, sonra da bu girişimleri tanımlamaya, etkisini azaltmaya veya tamamen etkisizleştirmeye, yönlendirmeye, değiştirmeye, abartmaya, engellemeye, aleyhinde kullanmaya ve amaçlarını, yöntemlerini ve yönetim kadrolarını tespit etmeye yönelik bir faaliyettir.

–Hem bir faaliyet hem de bu faaliyetin bir ürünüdür.

–İstihbarattan bağımsız veya ayrı bir süreç olarak değil, istihbarat sistemi ve sürecinin her aşamasında var olması ve uygulanması gereken dinamik bir faaliyettir.

Bizce karşı istihbarat tanımında bulunması lazım gelen, yukarıda sayılan hususlardan da faydalanarak, biraz uzun olmasına karşın daha kapsamlı ve kavrayıcı olacağı değerlendirilen şu tanım yapılabilir:

**Karşı istihbarat / İKK;** düşman, dost, bağlaşıklık, ortak veya rakip olarak görülen kişi, grup, kuruluş ve devletlerin, yasal veya yasal olmayan yöntemlerle istihbarat elde etme çabalarına karşı, herhangi bir kişi, grup, kurum, kuruluş veya devlet tarafından, kendi plan, tasarı ve stratejilerini yani kendisine ait hassas ve gizli olarak nitelendirdiği her türlü bilgiyi güvenlik altına almak, ulusal / kurumsal güvenliğini sağlamak, ulusal / kurumsal güç unsurlarını ve dolayısıyla ulusal / kurumsal bütünlüğünü korumak maksadıyla, pasif ve aktif yöntem ve teknikleri içeren önlemler alarak, savaşta ve barışta yani her zaman ve kesintisiz şekilde icra edilmesi gereken bir faaliyet ve bu faaliyetin bir ürünüdür. İstihbarattan bağımsız veya ayrı bir süreç değil, istihbarat sistemi ve sürecinin her aşamasında var olması ve uygulanması gereken yaşayan bir süreçtir.

Karşı istihbaratın tanımını yaptıktan sonra aynı ya da benzer anlamda kullanıldığı diğer terimlere de değinmekte yarar vardır. Bu terimlerden ilki “koruyucu güvenlik önlemleri” olarak karşımıza çıkmaktadır.

Her türlü kurum, kuruluş, birlik, tesis\* ve personelin; her türlü tehdit, tehlike ve tecavüzlere karşı korunması ve güvenliklerinin sağlanması amacıyla kuruluş sınırları ve görev alanı içerisinde, kendi personeli ve olanaklarıyla, bütün seviyelerde, ilgili mevzuat hükümleri çerçevesinde kurulan ve idame ettirilen; baskın, sabotaj, yıkıcı, bölücü, bezdirici ve çözücü saldırılar ile olası istihbarat elde etme girişimlerine karşı savunma önlemlerinin planlanması ve uygulanmasına “koruyucu güvenlik” denir.

“Tanınmış bir güvenlik danışmanı olan Bruce Schneier’in da dediği gibi, ‘Güvenlik bir ürün değil, bir süreçtir.’ Ayrıca güvenlik, bir insan ve yönetim sorunudur.”<sup>16</sup>

“Güvenlik önlemleri” veya “koruyucu güvenlik önlemleri” terimleri tamamen aynı anlamları ifade ederler ve tanımı şöyledir: Hâlihazırdaki, olası ya da potansiyel düşman, dost, tarafsız, bağlaşıklık, rakip veya ortakların, çeşitli amaçlar doğrultusunda ve gizlice veya açık olarak icra edecekleri yöntem ve uygulamalarla hakkımızda istihbarat toplamalarını önlemeyi, her türlü casusluk, gözlem, sabotaj, rahatsız etme veya sürprize engel olmayı yani söz konusu girişim ve faaliyetlerden korunmayı hedefleyen uygulamalardır.<sup>17</sup>

Güvenlik, yürüten kim olursa olsun, tüm düşmanca ve gizli eylemlere karşı pasif ya da durağan savunma kurmak demektir.<sup>18</sup> Güvenlik önlemleri, sonuç olarak tamamen hassas veya gizli bilgi, malzeme ve alanlara erişimi engellemekle ilgilidir. Güvenlik; engellenenin kimliğini, maksadını, yöntemlerini ve vasıtalarını bulmaya çalışmaz. Engellemek, güvenlik önlemlerinin başarısı için yeterlidir.

Casusluk / Espiyonaj ise en basit şekilde; bir devletin, bir kurumun ya da bir kuruluşun, kendisi için hayati olduğunu değerlendirdiği sırlarının ve gizli bilgilerinin, o devletin, kurumun ya da kuruluşun yasa ve kuralları ihlal edilerek yani yasa dışı yöntemlerle elde edilmesi ve diğer bir devlet, kurum veya kuruluşa aktarılması olarak tanımlanabilir.<sup>19</sup>

Karşı casusluk da, casusluk girişimlerine karşı yürütülen faaliyetleri ve ülkeyi casusluktan koruma eylemlerini kapsamaktadır. Yani casusluk faaliyetlerinin

\* Tesis sözcüğü, her türlü bina, kurum, kışla, alan vb. yeri kapsar mahiyette kullanılacaktır.

<sup>16</sup> Kevin D. Mitnick, **Aldatma Sanatı**, Çev.: Nejat Eralp Tezcan, ODTÜ Yayıncılık, Ankara, 2009, s. 4.

<sup>17</sup> Cate, **a.g.e.**, s. 88.

<sup>18</sup> Wasemiller, **a.g.e.**, s. 10.

<sup>19</sup> Gültekin Avcı, **İstihbarat Teknikleri: Aktörleri, Örgütleri ve Açmazları**, Timaş Yayınları, İstanbul, 2004. s. 37.

teşhisini, takibini, bu faaliyetlere katılanların yakalanmalarını, teşkilat ve sistemlerinin imha edilmesini amaç edinen aktif yöntemlerdir.<sup>20</sup>

Karşı istihbaratın, insan istihbaratı (İNİS)'nın bir alt disiplini olduğunu düşünen istihbaratçılar da vardır. Bu düşüncenin doğru olması için karşı istihbaratın sadece karşı İNİS operasyonlarına yönelmesi ve bu yönelmenin de yeterli olması gerekir. Oysa karşı istihbarat; hakkımızdaki her türlü istihbarat elde etme çabalarına yönelik olarak tüm kaynak ve vasıtanın (insan, teknolojik aygıtlar, açık kaynaklar vb.) kullanıldığı çok yönlü ve işlevsel bir alandır. Ayrıca İNİS ulusal güvenliğe, düşman veya rakiple ilgili bilgi toplayarak inisiyatifin sağlanması yönünden katkı sağlarken; karşı istihbarat, düşman veya rakip tarafından elde edilmeye çalışılan bilgiyi etkileyerek (değiştirerek, abartarak, yönlendirerek vb.) farklı ve daha kapsamlı bir katkıda bulunur.<sup>21</sup>

Bütün bu açıklamalardan sonra, karşı istihbaratın kapsamının –her ne kadar istihbaratın bir alt disiplini olarak kabul edilse de– istihbaratın kapsamından daha geniş olduğunu söylemek çok da abartılı olmayacaktır. İstihbaratı, en geniş kapsamlı sosyal bilimlerden birisi olarak gören veya onu bir sanat olarak kabul eden bilim adamları ve istihbaratçılar olduğuna göre karşı istihbarat da bir bilim dalı ve sanat olarak nitelendirilebilir.

Karşı istihbarat, kendine özgü bir mantığa sahiptir. Yabancı istihbarat tehditlerine karşı hem toplanan bilgileri hem de uygulanan faaliyetleri bünyesinde barındırır. Geleneksel anlamdaki karşı casusluk, sabotajlara karşı koyma ve yıkıcı faaliyetlere karşı koymayı da kapsar. Hatta ayaklanmaya karşı koyma ve vatana ihanete karşı koyma gibi alt bölümler eklenerek, karşı istihbaratın kapsamı daha da genişletilebilir. Sonuçta yapılan bu bölümlendirmeler keskin ve tam bir ayrımı ifade etmezler ve aslında birisi için alınacak güvenlik önlemleri, büyük ölçüde tamamı için geçerlidir.<sup>22</sup>

İstihbarat toplayarak, hâlihazırdaki, olası ya da gizil düşman, dost, tarafsız, bağlaşıklık, rakip veya ortakların amaçlarını, planlarını, niyetlerini, kapasitelerini öğrenmek ne kadar önemli ise onların bizim amaçlarımızı, planlarımızı ve

<sup>20</sup> Avcı, *İstihbarat Teknikleri... a.g.e.*, s. 37; A.Turhan Şenel, *İKK ve İKK Operasyonları*, İDB Yayınları No:64, Ankara, 1997, s. 86.

<sup>21</sup> Jerry W. Jones, "CI and HUMINT or HUMINT and CI or CI/HUMINT or TAC HUMINT", *Military Intelligence Professional Bulletin*, Vol.: 28, No.: 1, 2002, 28–33, s. 31.

<sup>22</sup> Michelle K. Van Cleave, "Strategic Counterintelligence: What is it and What Should We Do about it?", *Studies in Intelligence*, Vol.: 51, No.: 2, 2007, 1–13, s. 5; Cate, *a.g.e.*, s. 90.

kapasitelerimizi öğrenmelerini engellemek de o kadar önemlidir. İstihbarat, ulusal güvenliğin sağlanabilmesi için vazgeçilmez ve çok önemli bir etkidir.<sup>23</sup> Karşı istihbarat ise, istihbaratın dahi her aşamasında ve uygulamasında bulunması gereken, istihbarattan çok daha önemli, bir o kadar da zor ve duyarlı bir faaliyettir. Şöyle ki, karşı istihbaratta başarı pamuk ipliğine bağlıdır. Ne kadar iyi bir karşı istihbarat sistemi kurulursa kurulsun ilk sızma veya gedikte, sistem başarısız olarak nitelendirilebilir.

İstihbaratta önemli teknik ve yöntemler bakımından eğitilmiş ve uzmanlık derecesinde yetenekli profesyonel bir takıma gereksinim vardır. Uzmanlaşma son derece önemlidir. Karşı istihbaratta ise profesyonel takım sadece karşı istihbaratın operasyonel anlamdaki yani aktif yönünü icra etmek için gereklidir. Karşı istihbaratın, bize göre aktif yönünden daha fazla öneme sahip olan pasif yönü ise, bütün bireyler tarafından amatör ruhla icra edilmeyi zorunlu kılar.

Karşı istihbarat, harcanan emeğin karşılığını gösteremeyen bir istihbarat disiplini. Yine de, bir devletin istihbarat sistematiği ne kadar gelişmiş olur ise olsun, etkin ve etkili bir karşı istihbarat anlayışına sahip değilse ve kurulmuş iyi bir karşı istihbarat sistemi yoksa istihbarat savaşında başarılı olması oldukça zordur.

Küreselleşmeye paralel olarak, devlet güvenliğini tehdit eden unsurların boyutlarının değişmesi mevcut jeopolitik ve jeostratejik gelişmeler paralelinde istihbarat birimlerinin faaliyetlerinin aynı oranda yoğunlaştığını söylemek gerekir. Nitekim ekonomik gelişmeler ve savunma sanayindeki gelişmelerle birlikte devlet güvenliği için alınması gereken önlemlerin boyutu da önemli ölçüde değişmiştir. Dolayısıyla .. espionaja karşı devlet güvenliği için hayatiyet arz eden bilgi ve materyallerin çok iyi saklanması mecburiyeti daha da önem kazanmıştır. Özellikle, bilgisayar savaşının artarak devam ettiği, başta teknolojik ve elektronik istihbarat olmak üzere haber/bilgi toplama araçlarının geliştiği ve çeşitlendiği günümüzde İstihbarata Karşı Koyma anlamında koruyucu güvenlik önlemlerinin önemi daha da artmıştır... Bu faaliyetler bütün olarak istihbarat sürecinin ve faaliyet alanlarının her aşamasında zorunlu bir döngüsel fonksiyon olarak yer alırlar.<sup>24</sup>

Karşı istihbaratın en ayırt edici özelliği, bir operasyonel işlevinin varlığıdır. İstihbarat için, karşıdaki servisi ve onun faaliyetlerini bilmek bütün hedeftir. Karşı

<sup>23</sup> Özdağ, *a.g.e.*, s. 160.

<sup>24</sup> Ünal Acar ve Ömer Urhal, *Devlet Güvenliği İstihbarat ve Terörizm*, Adalet Yayınevi, Ankara, 2007, s. 164.

istihbarat için ise bilmek henüz yolun başında olduğu ve eldeki istihbarat ile ilgili bir şeyler yapılması gerektiği anlamına gelir.<sup>25</sup>

## 1.2. KARŞI İSTİHBARATIN AMAÇLARI VE GÖREVLERİ

Karşı istihbaratın önemini vurguladıktan sonra, amaçlarına ve görevlerine değinmekte de yarar vardır. Karşı istihbarat, düşman istihbarat servisinin bizimle ilgili her türlü istihbarat planını bozmaya, yönlendirmeye ve engellemeye çalışarak stratejik inisiyatifi ele geçirmeyi amaçlar. Düşmanların veya bağlaşıkların, rakiplerin veya ortakların istihbarat faaliyetlerinin analizi (çözümlemesi), bizimle ilgili çıkarlarını, amaçlarını ve planlarını öğrenebilmek açısından bizi fazlasıyla yararlı sonuçlara götürebilir.

Her istihbarat faaliyetinin politik bir hedefi vardır. Karşı istihbaratın görevi de bu hedefi tespit etmek ve uygun yer ve zamanda engellenebilmesi için gerekli seçenekleri sunmaktır. Karşı istihbarat, düşman veya rakiplerin istihbarat toplama çabalarını çeşitli yöntemler kullanarak engellemeye veya etkisiz kılmaya çalışır. Karşı istihbarat, ülke güvenliğine karşı girişilmesi olası her türlü istihbarat ve casusluk girişimine karşı pasif ve aktif önlemlerle adeta bir kalkan ve bir kılıç görevi üstlenerek ulusal güvenliğin sağlanmasında önemli rol oynar. Ayrıca devlet yönetimindeki kişilere, ülke hakkında bazı operasyonlar planlayan veya yürüten yabancı güçlerin plan, niyet ve yetenekleri hakkında farklı bir pencereden bakabilme olanak ve yeteneği sunar.<sup>26</sup>

Karşı istihbaratın amacının genel olarak şu temel iki sorunun cevaplarını bularak aleyhimizde olan yönlerini lehimize çevirmek veya en azından olası zararlarından en az etkilenecek önlemleri geliştirmek olduğunu söyleyebiliriz:<sup>27</sup>

- Düşmanlarımız, dostlarımız, bağlaşıklarımız, ortaklarımız veya rakiplerimiz bizimle ilgili neyi ve neden öğrenmek istiyorlar? Bunu nasıl yapmaya çalışıyorlar?
- Onları engellemek için biz ne tür önlemler alıyoruz ve alınan önlemler yeterli mi?

<sup>25</sup> Michelle K. Van Cleave, **Counterintelligence and National Strategy**, National Defense University Press, Washington, 2007, s. 8.

<sup>26</sup> Van Cleave, **Counterintelligence...a.g.e.**, s. 3.

<sup>27</sup> Bernhard Douglas, **Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence**, Financial Times, London, 2003, s. 85.

Kullanan tarafa büyük avantaj sağlayacak olan yeni bir silah sisteminin devreye sokulması veya var olan bir silah sisteminin bilinmeyen, yepyeni bir taktik veya stratejiyle kullanılması, söz konusu sistemden bihaber olan ya da olası etkilerine karşı hiçbir karşı önlemi bulunmayan rakip veya düşman için oldukça istenmeyen ve dezavantajlı bir durum yaratacaktır.<sup>28</sup> Karşı istihbaratın ilk görevi, ülkeye ve dolayısıyla onun çıkarlarına karşı yönelmiş istihbarat faaliyetlerini belirlemektir. Bunun için koruyucu güvenlik önlemleri ve operasyonel güvenlik önlemleri gereklidir. Buradaki asıl amaç, tehdit ve tehlikeler karşısında “hazır olabilme” durumunu en üst düzeye çıkarabilme, olası tehdit ve tehlikeleri engelleme veya oluşacak hasarı en az seviyede tutabilmektir. Yani asıl amaç, stratejik sürpriz yaşamamaktır.<sup>29</sup>

Söz konusu maksadın gerçekleştirilebilmesi için etkin bir İKK planlamasına gereksinim vardır. Etkin bir İKK planlaması da, mevcut veya olası düşmanın istihbarat toplama yöntemleri ile ilgili bilgiye gereksinim gösterir. Bu nedenle İKK, istihbarat biliminin ayrılmaz ve tamamlayıcı bir parçasıdır.<sup>30</sup>

Bu durumda karşı istihbaratın en genel anlamda görevi; bize zarar vermeyi amaçlayan dost, bağlaşıklık, ortak, muhalif, rakip ve düşman olarak nitelendirebileceğimiz yabancı güçlerin, terörist grupların ve diğer kuruluşların her türlü istihbarat girişimlerini ve uygulamalarını tanımlamak (tespit ve teşhis etmek), kıymetlendirmek (takip ve teyit etmek), sömürmek (istediğimiz şekilde yönlendirmek) ve etkisiz kılmaktır.<sup>31</sup>

Burada değinilen amaçların gerçekleştirilmesi için karşı istihbaratın ifa etmesi gereken görevlerden bazıları şunlardır:

– Başta casusluk olmak üzere her türlü yabancı ve düşmanca faaliyetin önüne geçebilmek için uygun planlar yapmak, örgütlerini ortadan kaldırmak ve bu gibi faaliyetlere girişenleri önlemek, bulmak ve zararsız hâle getirmek.<sup>32</sup>

– Her türlü bilgi ve belgenin, düşman veya rakiplerin eline geçmesine engel

<sup>28</sup> Bobby Allen, “The New Counterintelligence Response to the Cyberthreat”, *Military Intelligence Professional Bulletin*, Vol.: 29, No.: 3, 2003, 32–35, s. 32.

<sup>29</sup> Van Cleave, *Counterintelligence...a.g.e.*, s. 13.

<sup>30</sup> Serhat Tezsever, *Milli Güvenliğimiz İçinde İstihbarat*, İstanbul Üniversitesi Basımevi, İstanbul, 1999, s. 164; Acar ve Urhal, *a.g.e.*, s. 308.

<sup>31</sup> Jones, *a.g.e.*, s. 30.

<sup>32</sup> Tezsever, *a.g.e.*, s. 303.

olacak önlemler geliřtirmek.<sup>33</sup>

– İKK çözümlmeleri yapmak, zayıf yanlarımızı ve düşkünlüklerimizi incelemek, belirlemek ve bulunan zayıf noktaların kapatılması için alınacak önlemleri geliřtirmek ve yönlendirmek, fırsat kollamak ve çıkan fırsatları deęerlendirmek.

– İcra edilecek olan her türlü operasyonun İKK desteęini saęlamak maksadıyla gerekli önlemleri belirlemek, olası risklere karşı çözüml yolları aramak.<sup>34</sup>

– Yabancı istihbarat servisleri ile ilgili olarak;<sup>35</sup>

- Yabancı (düşman) istihbarat servisleri kimlerdir ve yetenekleri nelerdir?
- Nasıl ve kimler tarafından görevlendirilmektedirler?
- Servisin teşkilat yapısı ve örgütlenmesi nasıldır? Bütçesi ne kadardır?
- Liderlik yapısı nasıldır? Liderleri kimlerdir?
- Liderlerinin ve genel olarak teşkilatların güçlü yönleri ve düşkünlükleri nelerdir? Söz konusu düşkünlüklerden faydalanmak\* mümkün müdür?
- Servisin elemanları nasıl işe alınır? Elemanlar nerede ve nasıl eğitilir? Personel kayıtları nerede tutulur?
- Organizasyon içi bağlantı nasıldır? Bilgi kaynakları ve hedefleri nelerdir (kimlerdir)?
- Kullandıkları yöntem ve teknikler nelerdir? Gibi soruların cevaplarını bulmaktır.

Öte yandan karşı istihbaratın, yasal açık kaynaklardan yabancılar tarafından

---

<sup>33</sup> Acar ve Urhal, **a.g.e.**, s. 303.

<sup>34</sup> Köseli, **a.g.e.**, s. 32.

<sup>35</sup> Van Cleave, "Strategic...**a.g.e.**, s. 5.

\* İnsanların zayıflık ve düşkünlüklerinden faydalanarak istenilen davranışların sergilenmesi ya da bilginin alınabilmesi, uzmanlık gerektiren özel bir alanın daha doğmasına sebep olmuştur. Yazına yakın zamanda giren "sosyal mühendislik" kavramının konusu tam olarak budur.

bilgi toplanmasına karşı, söz konusu bilgi yığını üzerinde çok kısıtlı bir kontrolü vardır ya da hiç kontrolü yoktur. Yine de bu tür yasa dışı olmayan bilginin yerli ve yabancı kişi ve oluşumlar tarafından toplanmasının tespit edilmesi, kıymetlendirilmesi, sömürülmesi ve etkisiz kınması da karşı istihbaratın görevleri ve amaçları arasında yer almaktadır.<sup>36</sup>

### 1.3. KARŞI İSTİHBARATIN KAYNAKLARI

Belirlenen amaçlara ulaşılabilmesi ve görevlerin yerine getirilebilmesi için gereksinim duyulan en önemli girdi “bilgi”dir. Karşı istihbaratta, bazı bilgilere kolaylıkla ulaşılabilirken bazı bilgiler için de sistemli ve kapsamlı çalışmalar yürütmek durumunda kalınır. Bilgiye ulaşmak maksadıyla kullanılabilecek kaynaklar şunlardır:<sup>37</sup>

- Açık kaynaklar,
- Resmî kaynaklar (askerî ve sivil her kişi, grup, kurum ve kuruluş bu kapsamda değerlendirilir),
- Bireysel kaynaklar (casuslar, hainler, politik muhalifler, haber elemanları, muhbirler, mülteciler, tutuklular, savaş esirleri, sürgündekiler, işgal altındaki bölge halkı, iş seyahatindekiler, turistler vb.)
- Muhabere istihbaratı (MUİS), sinyal istihbaratı (SİNİS), teknik istihbarat (TEKİS), ölçme ve iz istihbaratı (ÖZİS), ses istihbaratı (SEİS), radar istihbaratı (RİS), görüntü istihbaratı (GÖRİS) vb. teknolojik istihbarat disiplinleri,
- Belgeler, fotoğraflar, videolar, raporlar, istatistikler, kayıtlar vb.,
- Düşmandan veya rakipten ele geçirilen malzemeler.

Karşı istihbaratın ilgilendiği ve dolayısıyla istihbarat yönünden muhatap olarak değerlendirdiği kişiler vardır. Bu kategorilerdeki kimseler karşı istihbaratın hem pasif hem de aktif yönü açısından değerlendirilir. Pasif anlamda aralarında olması olası

<sup>36</sup> Cate, *a.g.e.*, s. 89.

<sup>37</sup> U.S. Marine Corps, *MCWP 2-14 Counterintelligence*, Washington D.C., 2000, s. 6-8; Michael Herman, *Intelligence Power in Peace and War*, Cambridge University Press, 1999, s. 53.

casusların bulunmasına çalışılırken, aktif anlamda da tespit edilen casus veya muhbirleri istediğimiz şekilde kullanarak rakip ya da düşmanı yanlış yönlendirmeye çalışmak şeklinde olabilir. Birer karşı istihbarat sensörü (duyargası) veya tam tersine karşı istihbarat açığı olma potansiyelindeki söz konusu kişiler şöyle sıralanabilir:<sup>38</sup>

- Düşman toprakları içinde yaşayan vatandaşlarımız veya düşman ülkenin vatandaşı olup da çeşitli sebeplerle bizim hesabımıza çalışan, müzahir (destekleyen) kişi ve gruplar,

- Kendi vazifelerinin yanında, doğal birer istihbarat toplama vasıtası ve kaynağı olma görevi de bulunan askerî birlikler,

- Yurt dışına herhangi bir maksat veya görev için giden personel,

- Özellikle karşı istihbaratın pasif yönü yani koruyucu güvenlik önlemleri açısından ve casusluğa karşı, özellik arz eden kamu görevlileri ve vatandaşlar,

- Çok uluslu güç harekâtları kapsamında veya çeşitli resmî / resmî olmayan ziyaretler için ülkemizde bulunan bağlaşıp ülke personeli,

- Yabancı ülkelerin büyükelçilik ve konsolosluklarında görevli kişiler,

- Çok uluslu şirket, kurum, vakıf vb. yerlerde çalışan yönetici ve çalışan konumundaki yabancı kişiler,

- Mültecilerin arasına karışarak ülkeye sızmaya çalışan şüpheli kişiler,

- Sınırı yasal olmayan her türlü yoldan geçenler,

- Düşman birimlerinden firar edenler,

- Kimlikleri olmayan ya da sahte kimlikleri olan kişiler,

- Geri gönderilen hükümlüler ve savaş esirleri,

- Direniş ve başkaldırı örgütlerinin üyeleri,

---

<sup>38</sup> U.S. Marine Corps, *a.g.e.*, s. 7-3.

- Düşmanla / rakiple işbirliği yapanlar,
- Daha önceden tespit edilmiş olan ve takip edilen hedef kişiler,
- Gönüllü muhbirler ve haber elemanları,
- Gafil muhbirler.

Sayılan kişiler arasında en önemsizi gibi görünen ve listenin sonunda yer alan gafil muhbirler, bu çalışmanın ana konusunu oluşturmaktadırlar ve aslında sanıldığı kadar önemsiz değildirler. Karşı istihbarat sistemini bir kazana benzetirsek, her türlü önlem alındığında bile tamamen engellenmesi mümkün görünmeyen gafil muhbirlik gedikleri veya delikleri, uzun vadede kazanın tamamen boşalmasına sebep olabilecek kadar risklidirler. Bu konu, 4'üncü bölümde ayrıntılı olarak ele alınacaktır.

#### 1.4. KARŞI İSTİHBARATTA BAŞARININ İLKELERİ

Düşmanlar veya rakipler; kendi çıkarlarını gerçekleştirmek, ulusal güvenlik sırlarımıza (bilgiler, planlar, teknoloji, etkinlikler, faaliyetler vb.) sızmak, bilgi toplamak ve ödün koparmak, hile yaparak, bilgileri saptırarak ya da etki operasyonları ile hatalı politikalar, stratejiler ve planlar yapılmasını sağlamak, gizli ulusal güvenlik faaliyetlerini ve çalışmalarını bozmak, sekteye uğratmak ve engellemek, askerî yeteneklerini yükseltmek veya ekonomik avantaj sağlamak maksatlarıyla, sahip oldukları istihbarat yetenekleri vasıtasıyla, bize ait gizli ve yüksek öncelikli bilgileri elde etmeye veya çalmaya çalışabilirler.<sup>39</sup>

Karşı istihbaratın savaşmak zorunda olduğu istihbarat yöntem ve girişimleri alabildiğine geniş ve kestirilemez boyutlardadır. Dolayısıyla karşı istihbaratta başarılı olmak, bu bölümün başında da anlatıldığı gibi oldukça zordur. Zor olmasının başlıca sebebi başarının belirgin ya da rakamsal yani gözle görülür bir göstergesinin olmamasıdır. Karşı istihbaratçılar için en önemli mutluluk ve mesleki doyum, sistemin gediksiz ve kaçaksız çalıştığını görmek, olası girişimleri zamanında tespit edebilmek ve etkisiz hâle getirebilmekten ibarettir. Başarıya ulaşmak için uyulması gereken ilkeler şunlardır:<sup>40</sup>

<sup>39</sup> Van Cleave, *Counterintelligence... a.g.e.*, s. 4.

<sup>40</sup> James M. Olson, "The Ten Commandments of Counterintelligence", *Studies in Intelligence*, Vol.: 45, No.: 5, 2001, 81–87, ss. 83–86.

- Öncelikle potansiyel tehditler doğru algılanarak mevcut veya olası tehlikeler ortaya konulmalıdır.
- Saldırgan olunmalıdır ve en iyi savunmanın saldırmak (taarruz) olduğu akıldan çıkarılmamalıdır.
- Sokaklara hâkim olunmalı ve sahaya inilmelidir.
- İyi bir tarih bilgisine sahip olunmalıdır.
- Çözümlemenin önemi asla unutulmamalıdır.
- Tüm kurum, kuruluş ve kişilerle işbirliği içinde çalışılmaya hazırlıklı olunmalıdır.
- Sürekli eğitim yapılmalı, kişisel ve örgütsel gelişime önem verilmelidir.
- Yapılan işin öneminin küçümsenmesine ve köşeye itilmeye izin verilmemelidir.
- Karşı istihbarat işinde çok uzun kalınmamalıdır.
- Asla pes edilmemeli ve vazgeçilmemelidir.
- Karşı istihbarat, gereken önem ve ciddiyet ile planlanmalı ve icra edilmelidir.
- Gizliliğe hat safhada önem gösterilmelidir.
- Zaman zaman yasalara aykırı faaliyetler yapmaya ve sonuçlarına katlanmaya hazırlıklı olunmalıdır.

Bu ve benzeri ilkeler, karşı istihbaratın başarısı için temel teşkil eder. Temeli sağlam oluşturmadan inşa edilecek hiçbir sistem veya organizasyonun başarılı olması beklenemez. Karşı istihbarat gibi karmaşık ve güçlüklerle dolu bir faaliyet için ilkeli bir sistem oluşturulması gereklidir.

## 1.5. KARŞI İSTİHBARATÇIDA BULUNMASI GEREKEN ÖZELLİKLER

Karşı istihbaratçıda bulunması gereken ya da karşı istihbaratçıdan beklenen özelliklere geçmeden önce, “karşı istihbaratçı” kalıbının altında bu işi profesyonel olarak yapan yani aktif karşı istihbarat yapan uzmanlar ile en sıradan (istihbarat değeri taşıyabilecek herhangi bir bilgiye sahip olan) bireye kadar pasif karşı istihbarat yönünün aktörü olan kitlenin tamamının yer aldığını ifade etmekte yarar vardır. Dolayısıyla söz konusu özellikleri sayarken, genel olarak herkeste bulunması gereken özellikler ve profesyonel karşı istihbaratçılarda bulunması gereken özellikler şeklinde bir ayırım yapmanın daha doğru bir yaklaşım olacağı değerlendirilmektedir.

Sayılacak olan özellikler kesinlikle daha da çoğaltılabilir. Aynı şekilde sayılan bütün özelliklerin her karşı istihbaratçıda bulunmasını beklemek çok gerçekçi bir yaklaşım da olmayabilir. Hatta sayılan özelliklerin tamamının bir tek kişide gerçek anlamda bulunması belki de olanaksızdır. Ancak bir temel oluşturmak ve başlangıç yapmak bakımından yeterli ve önemli sayılabilecek kapsamdadır.

Bu bağlamda öncelikle her bir bireyin (tüm vatandaşların) sahip olması ya da kazandırılması gereken özellikleri ortaya koymak gereklidir. Zira söz konusu özellikler karşı istihbarat için “olmazsa olmaz” özelliklerdir ve bu özelliklere sahip olunmazsa karşı istihbaratın başarılı olması beklenemez. Sayılacak özelliklerin hemen hiçbirisi doğuştan getirilmesi beklenen özelliklerden değildir. Aksine tamamı iyi bir eğitim sayesinde ve karşı istihbarat kültürünün toplumda yerleştirilmesi sonucunda kolaylıkla kazandırılacak özelliklerdir. Bu özellikler şöyle sıralanabilir:<sup>41</sup>

- Ağzı sıkı (ketum) olmak, konuşulmaması gereken zamanlarda ve yerlerde susmayı bilmek,
- Gizlilik ilkelerine sadık olmak,
- Temel seviyede istihbarat ve karşı istihbarat eğitimi almış olmak,
- Çevresinde olup bitenlere duyarlı ve farkındalık düzeyi yüksek olmak.

<sup>41</sup> Aziz Yakın, *İstihbarat, Casusluk ve Casuslukla Mücadele*, Dış İşleri Akademisi Yayınları, Ankara, 1969, s. 92.

Profesyonel karşı istihbaratçılarda ise sayılan temel özelliklere ilave olarak şu özelliklerin bulunması beklenir:<sup>42</sup>

– İstihbaratçılık geçmişine ve deneyimine sahip olmalıdır. Böylece empati kurabilmesi, farklı açılardan olaylara ve durumlara yaklaşabilmesi mümkün olabilecektir. İstihbarat yöntem ve teknikleri konusunda bilgili ve aynı zamanda deneyimli bir karşı istihbaratçının, yabancı kişi, kurum ve / veya servislerin yöntem ve tekniklerine karşı önlemler geliştirme konusunda çok daha başarılı olacağı apaçık ortadadır. Bu, sadece basit bir istihbarat kursu veya eğitimi ile de mümkün değildir. Bizzat istihbarat sahasında aktif görev geçmişine sahip bir karşı istihbaratçının işi kolaylaşacak ve başarılı olma olasılığı artacaktır.

– Zayıf karakterli olmamalı, cesur olmalı ve kötüye kullanılabilecek düşkünlükleri bulunmamalıdır.

– Şan, şöhret, isim, servet düşkünü ve açgözlü olmamalıdır.

– Gerekğinde blöf yapabilmeli, aldatma tekniklerini iyi uygulayabilmelidir.

– Belleği kuvvetli olmalı, gördüklerini ayrıntılı olarak hatırlayabilmeli ve aktarabilmelidir.

– Pratik ve yaratıcı zekâ sahibi olmalıdır.

– İyi bir çözümlemeci olmalıdır. Karşı istihbarat çözümlemecilerinin görevi, düşmanın ya da rakibin gözünden kendisini görerek bu görüntünün istediği gibi olmasını sağlamaktır.

– İyi derecede yazılı ve sözlü iletişim yeteneğine sahip olmalı ve insanlarla iyi ilişkiler kurabilmelidir.

– Sorgulayıcı, tarafsız ve çok yönlü düşünebilme yeteneği ile öngörüye sahip olmalıdır.

– Mensup olduğu istihbarat servisinin tarihi ile ilgili bilgi sahibi olmalıdır.

---

<sup>42</sup> Özdağ, *a.g.e.*, s. 161, 168; Yakın, *a.g.e.*, s. 92; Acar ve Urhal, *a.g.e.*, s. 301; Avcı, *İstihbarat Oyunları... a.g.e.*, s. 122.

- Düşman / rakip istihbarat servis(ler)inin kültür, yönetim, kadro, kapasite, amaç, hedef ve operasyon yöntemleri ile ilgili kapsamlı bilgi sahibi olmalıdır.
- Doğru ve zamanında rapor etme yeteneğine sahip olmalıdır.
- Karşı istihbarat konusunda yetenekli ve bu işe istekli olmalıdır.
- Bilimsel ve deneyime dayalı bilgi ve görgüsünü karşı istihbarat işine uygulayabilmelidir.
- Yeni teknolojiyi takip edebilmeli, kendini uyarlayabilmeli ve uygulayabilmeli, kullanımdan doğabilecek güvenlik zafiyetleri ile ilgili önlemleri ve donanımlı olmalıdır.
- Karşı istihbaratın hukuki tabanı ile ilgili bilgi sahibi olmalıdır.
- Zor şartlar altında soğukkanlılığını koruyabilmelidir
- Eğitimle geliştirilmiş ve terbiye edilmiş gözlem ve tarif becerisi olmalıdır.
- Görevlerin yerine getirilmesi için yeterli fiziksel yetenek ve sağlamlıkta olmalıdır.
- Beden dilini kullanma ve okuma yeteneği olmalıdır.
- Sezgileri güçlü olmalıdır.
- Her zaman şüpheli, meraklı ve temkinli olmalıdır.
- Zor şartlar altında mantıklı ve sakin kalabilmeli ve verimli çalışabilmelidir.
- Mükemmelliğe önem vermeli, teferruata, gereksiz görünen şeylere dahi dikkat etmeli, herkesin göremediği şeyleri görebilmelidir.
- Açık fikirli olmalıdır.
- En az bir meslek veya sanatta ehliyet sahibi olmalıdır.

- Sinirlerine hâkim, metîn, sakin, ağırbaşlı, sabırlı ve dayanıklı olmalıdır.
- Takım çalışmasına yatkın olmalıdır.
- Görev bilinci olmalı ve sorumluluktan kaçmamalıdır.
- En az bir yabancı dili anadili gibi konuşabilmelidir.
- “Karşı istihbaratçılar hiçbir şey olmasa da sürekli kendi örgütlerine sızıldığı şüphesini canlı tutmak zorunda olan profesyonel paranoyaklardır.”

Altın fırsatlar her gün gelip kapıyı çalmaz ama ulusal karşı istihbarat sistemi yaratıcı, çevik, anı yakalayabilen ve yetkin çalışanlar sayesinde o altını arayıp bulabilmeli, fark edebilmeli ve daha da önemlisi altın fırsat doğduğunda onu değerlendirebilmelidir.<sup>43</sup>

Karşı istihbarat sisteminde, sahada çalışan personelin bütün karşı istihbarat teknikleri konusunda yetkin, etkin ve yetenekli olması ile iyi derecede yabancı dili konuşabiliyor olması öncelikli gerekliliklerdir. Yine de karşı istihbarattaki uzmanlık ve deneyim her zaman yabancı dil yeteneğinden daha önemlidir. Zira yabancı dil eksikliğinin telafi edilebilmesi bir şekilde mümkünken, karşı istihbarat yeteneği ve deneyimi vazgeçilmezdir ve eksikliğin herhangi bir kişi tarafından telafi edilmesi mümkün değildir.<sup>44</sup>

Karşı istihbaratçıların özellikli ve seçkin kişiler olması önemlidir fakat tek başına yeterli değildir. Etkili ve ilkeli bir karşı istihbarat sisteminin varlığı da vazgeçilmezdir. Görev, sorumluluk ve yetkiler doğru belirlenerek yetenekli karşı istihbaratçılar tamamen hedefe yönlendirilmelidir. Yanlış uygulama ve yönlendirmeler, hem emek ve çalışmaları boşa çıkaracak hem de sistemin başarısızlığına sebep olabilecektir. Bunun için öncelikle mevcut bütün sistemlerin istihbarata karşı zayıflıkları tespit edilmeli, olası tehlikeler ve İKK önlemleri belirlenmeli, önlemler uygulanmalı ve sonuçlar değerlendirilerek gerekli düzeltmeler yapılmalıdır.

---

<sup>43</sup> Van Cleave, *Counterintelligence...a.g.e.*, s. 16.

<sup>44</sup> Cate, *a.g.e.*, s. 91.

## İKİNCİ BÖLÜM

### İKK ÖNLEMLERİ

#### 2.1. GENEL

Karşı istihbarat, her organizasyonda\* süreklilik ilkesi çerçevesinde ve en gelişmiş olanaklar kullanılarak icra edilmesi gereken bir faaliyettir. Karşı istihbarat yapmak için birçok organizasyonda özel birimler görevlendirilmektedir. Ancak İKK, İKK ile ilgili profesyonellerden oluşan küçük bir kuvvetin tek başına başarabileceği basit bir faaliyet değildir. Aksine, herhangi bir yabancı istihbarat tehlikesini en aza indirmek, tamamen bertaraf etmek veya zararlarını katlanılabilir seviyelerde tutmak için sağduyuyla güvenlik önlemlerini takip etmek, tüm vatandaşların sorumluluğudur. Bu bakımdan İKK önlemlerine geçmeden önce tehdit ya da risklerin tespit edilmesi, istihbarat kaynaklarının söz konusu risklere yöneltilmesi, gerekli değerlendirmelerin ve çıkarımların yapılması ve olası girişimlere karşı “yumuşak karın” olarak nitelendirilebilecek bölgelerin belirlenmesi gereklidir.<sup>45</sup>

Özel bilgileri sızdırılan veya çalınan bir organizasyon, çeşitli sorunlar yaşayabilir. Birbirine rakip olan organizasyonlar, birbirlerine üstünlük sağlamak ve birbirleri hakkındaki sırları ele geçirmek maksadıyla yasal ve ahlaki, yasa dışı ve ahlaki olmayan veya her ikisinin karışımını içeren birtakım yöntemler kullanabilirler. Karşı istihbarat, sadece saldırgan ve yasa dışı bilgi toplama girişimlerine karşı değil, aynı zamanda bir organizasyonun zarar görmesine neden olabilecek ve rekabet yeteneğini etkileyebilecek olan açık ve yasal bilgi toplama çabalarına karşı da korunmak anlamına gelir.<sup>46</sup>

“Engellenmediği takdirde .. zararın doğması ile bitebileceği öngörülen her durumu” tehlike olarak ifade etmek mümkündür.<sup>47</sup> Karşı istihbarat bakımından tehlikelerin genelde dışarıdan gelmesi beklense de asıl tehlikeleri ülke içindeki güvenilir olarak değerlendirilen (düşman tarafından yerleştirilen ve hassas bilgilere ulaşma olanağı olan) kişiler oluşturmaktadır. İKK önlemleri, tehlike sinyallerini tespit etmeli, casusluk girişimlerini bozmalı ve elektronik dinleme gibi yasa dışı faaliyetleri önlemeli, organizasyonun kendisi hakkında yayınladığı her türlü duyarlı bilgiyi

\* Organizasyon sözcüğü, devlet, birlik, kurum, kuruluş, şirket vb. istihbarat ve karşı istihbarat kavramlarıyla ilintili her türlü oluşumu kapsayan bir anlamda kullanılacaktır.

<sup>45</sup> U.S. Army, **FM 34-60 Counterintelligence**, Washington D.C., 1995, s.1-6; Çınar, **a.g.e.**, s. 120.

<sup>46</sup> Douglas, **a.g.e.**, s. 85.

<sup>47</sup> Thomas Würtenberger, **“Tehlike Kavramı” ve Alman Uygulaması Ekseninde Kolluk Hukuku**, Çeviren ve Yorumlayan: Feridun Yenisey, Asayiş Dairesi Başkanlığı, Ankara, 2008, s.12.

kontrol etmeli ve rakiplerinin toplamasını zorlaştırmalı ya da engellemeli ve casusluk çabalarına karşı savunmasız kalan alanlarda farklı koruyucu önlemler geliştirmelidir.

Karşı istihbarat bu tür saldırıları tespit edebilmek ve karşılık verebilmek için yeni ve teknolojik yollar bulmaya çalışır. Yine de çağdaş ve teknolojik güvenlik aygıtları ve yöntemleri; arşiv araştırması, güvenlik soruşturması, farkındalık eğitimi, fiziksel güvenlik önlemleri ve iç denetlemeler gibi geleneksel güvenlik uygulamalarının yerini alamazlar. En azından geleneksel güvenlik önlemleri alınmadan, teknolojik yöntem ve sistemlerin tam anlamıyla başarılı olmaları oldukça zordur.<sup>48</sup>

Bir sırrı çalma veya bir tesisi yok etme amacı güden kötü niyetli kişilerin (casus, hırsız, sabotajcı vb.) iyi yetişmiş oldukları ile tahmin bile edilemeyecek modern (çağcıl) ve en gelişmiş teknolojik araç ve gereçlerle (dinleme cihazları vb.) teçhiz edilmiş olabilecekleri akıldan çıkarılmamalıdır. Bu kişilerin düşünce yapılarını ve uygulayacakları yöntemleri belirleyerek gerekli önlemlerin ve karşı davranışların organize edilmesi daha gerçekçi ve başarı vadeden yoldur.<sup>49</sup>

İKK önlemleri, düşmanın veya rakibin istihbarat, casusluk ve sabotaj girişimleri ile yıkıcı faaliyetleri ve terör tehditlerinden korunmak için tasarlanmış bir dizi etkinliği kapsar. Karşı istihbarat önlemleri genellikle pasif ve aktif olmak üzere iki ayrı grupta tanımlanırlar. İKK'nın pasif yönü, savunucu yani koruyucu bir görev üstlenirken, aktif yönü de yabancı istihbarat birimlerinin planlarını öğrenme ve etkilerini bizim için katlanılabilir seviyelerde tutmak için çabalar. Her ne kadar karşı istihbarat önlemleri için aktif ve pasif şeklinde bir sınıflandırma yapılsa da, bunun keskin bir ayrımı ifade etmediğini baştan kabullenmek lazım gelir. Zira karşı istihbaratta tam bir başarıdan söz edilebilmesi için her türlü İKK önleminin bir bütün olarak değerlendirilmesi ve alınması gerekir. Keskin bir ayırım yapma çabası, istenilen başarılı sonuçlara ulaşmayı önemli ölçüde sekteye uğratır.<sup>50</sup>

Aktif İKK önlemleri, genel anlamda pasif İKK önlemlerine göre, hem daha etkin hem daha düşük maliyetli hem de daha kısa sürede ve daha kesin sonuç vadeden bir yapıya sahiptir. Yabancı bir istihbarat servisinin içinden casus temin edilerek veya eleman sızdırılarak edinilecek bilgilere göre geliştirilecek karşı önlemler, diğer

<sup>48</sup> Douglas, *a.g.e.*, s. 88; Allen, *a.g.e.*, s. 32.

<sup>49</sup> Köseli, *a.g.e.*, s. 31.

<sup>50</sup> Ehrman, *a.g.e.*, s. 20.

tüm pasif önlemlere göre daha etkili olacaktır. Pasif İKK önlemleri ise, etkin bir aktif İKK ile desteklendiği zaman daha anlamlı ve etkili olacaktır. Bu bağlamda aktif ve pasif İKK önlemlerini ve faaliyetlerini birbirinden bağımsız ve ayrı düşünmek yanlış olur.<sup>51</sup>

Öte yandan pasif İKK önlemleri konusunun yeterince açık ve belirlenmiş bir çerçevesi varken, aktif İKK önlemleri ile ilgili yeterli açıklığın olmadığı rahatlıkla söylenebilir. Genel olarak yazında, İNİS'in casusluk ile eş anlamda kullanıldığı göz önünde bulundurulduğunda ve aktif İKK önlemlerinin alınmasının devletin özel birimlerinin görevi (Türkiye'de MİT'in görevi olduğu gibi) olduğu düşünüldüğünde, mevcut gizlilik ile burada fazla yöntem ve önlem sayılamaması kabul edilebilir bir durumdur. Zira söz konusu önlem ve yöntemlerin herkes tarafından bilinmeleri, başarılı olma olasılıklarını düşürebilecektir.

Son olarak ülkemizdeki duruma değinmekte yarar vardır. İKK, 2937 sayılı Devlet İstihbarat Hizmetleri ve Millî İstihbarat Teşkilatı (DİHMİT) Kanunu'nun dördüncü maddesinin "g" fıkrasında MİT'e, beşinci maddesinin "a" fıkrasının 3'üncü bendinde de bakanlıklar ile diğer kamu kurum ve kuruluşlarına verilen görevler arasında yer alır.

MİT İKK Başkanlığı, DİHMİT Kanunu'nun ilgili maddeleri uyarınca, yabancı devletlerin istihbarat servisleri veya dış politikasını belirleyen ve üreten kurumlarıyla ilişkili organizasyonların veya kişilerin, ülke içinde yürüttüğü bilgi toplama, ajitasyon (körükleme), dezenformasyon (bilgi çarpıtma) ve yönlendirme çalışmalarını tespit etmek ve karşı koymakla görevli birimidir. Bu doğrultuda, yabancı devletlere ait istihbarat kuruluşlarının ülkemizdeki çalışma yöntemlerine, olanak ve yeteneklerine, hedeflerine ilişkin bilgi toplamak ve değerlendirmek, söz konusu istihbarat kuruluşlarının yurt içi ya da yurt dışı merkezli olarak sürdürdükleri veya destekledikleri faaliyetlerini açığa çıkarıp zararsız hâle getirmek gibi İKK çalışmalarını yürütmektedir. Ayrıca kamu ve özel sektördeki stratejik önemdeki kurum, kuruluş ve kişilere yönelik yabancı istihbarat servislerinin çalışmalarının engellenmesi, önlemler alınması, bu yönde bireylerin ve kurumların pasif karşı koyma konusunda bilinçlendirilmesi görevi de vardır.<sup>52</sup>

<sup>51</sup> Köseli, *a.g.e.*, s. 34.

<sup>52</sup> MİT Resmî İnternet Sayfası, "*İKK Başkanlığının Görev ve Sorumlulukları*", <http://www.mit.gov.tr/t-ikk.html> (Erişim tarihi: 14 Kasım 2011).

Görüldüğü gibi ülkemizde vatandaşlar, yasal anlamda İKK sistemine dâhil edilmemişlerdir. Aktif anlamda zaten böyle bir görevi olmayan vatandaşın, en azından temel seviyede yani pasif önlemler bakımından karşı istihbarat konusunda bilinçlendirilmesi yönünde düzenleme ve planlama yapılması, daha doğru bir yaklaşım olabilirdi.

Bu bağlamda gizli veya hassas her bilginin, bilinçli olarak veya bilmeden, yetkisi ve ilgisi olmayan kimselere söylenmesi, verilmesi veya gönderilmensin engellenmesi, kişi veya organizasyona verebileceği olası zararların en aza indirilebilmesi için güvenlik önlemlerinin ve düzenlemelerinin en ince ayrıntısına kadar hesap edilerek alınması gereklidir.

## 2.2. PASİF İKK ÖNLEMLERİ

Pasif karşı istihbarat önlemlerini belirleyebilmenin ön koşulu, hangi bilginin\* düşman, rakip, ortak, bağlaşıklık veya dost olarak nitelendirilen organizasyonun eline geçmesinin engelleneceğinin tespit edilmesidir. Bunu yapmanın en etkili yöntemi ise bilgilerin gizlilik açısından derecelendirilmesidir. Bu amaçla organizasyonun güvenliği açısından hassas veya gizli olan bilgiler, hassaslık ve gizlilik düzeylerine göre çeşitli gizlilik derecelerine\*\* ayrılırlar. Gizlilik dereceleri belirlendikten sonra yapılacak ikinci işlem ise her gizlilik derecesindeki bilgiye kimlerin erişebileceğinin belirlenmesidir. Her bir gizlilik derecesindeki bilgiye, yine belli yetki seviyesindeki kişilerin erişebilmesini, yetkisiz ve ilgisiz kişilerin belli bir gizlilik derecesinin üzerindeki bilgiye erişememesini sağlayacak bir düzenleme yapılmalıdır.<sup>53</sup>

Pasif İKK önlemleri, önleyici ve tespit edici olmalıdır. Önleyicilik görevini, düşmanın gizli ve hassas bilgilere erişmesine, yıkıcı faaliyetlerle personeli çökertmesine ve tesisler, sistemler ve komuta kademelerinde kurulmuş olan fiziksel güvenlik bariyerlerini delmesine (sızmasına) engel olarak yapar. Tespit edicilik görevini ise, düşmanın istihbarat toplama, sabotaj, yıkıcı faaliyetler ve terörizme yönelik çabalarını ortaya çıkarma ve etkisiz kılma şeklinde icra eder. Sıradan personel, pasif önlemleri uygulayarak, kendi sorumluluk sahası içindeki düşman girişimlerini ve faaliyetlerini gözlemleyerek ve şüpheli durumları rapor ederek

\* “Bilgi” sözcüğü, her türlü veri, belge ve malzemeyi kapsayan kavrayıcı bir anlamda kullanılacaktır.

\*\* Gizlilik dereceleri ile ilgili ayrıntılı bilgi için bkz. Mustafa Diri ve Mirac Gülçiçek, “Türkiye’de Kamu Hizmetinin Görülmesinde Kullanılmakta Olan Gizlilik Derecesi Tanımları: Uygulamadaki Sorunlar ve Çözüm Önerileri”, *Maliye Dergisi*, Sayı: 162, Ocak–Haziran 2012, ss. 497–537.

<sup>53</sup> Özdağ, *a.g.e.*, s. 162.

üzerine düşen görevi yapmış olur. Belge çevirisi ve çözümlemesi, araştırma, sorgulama gibi diğer teknik ve özel tespit yöntemleri, uzman kişiler tarafından gerçekleştirilir.<sup>54</sup>

Pasif karşı istihbarat, düşmanın yapabileceklerini önlemeyi amaçlar ve alınan önlemlerde savunucu bir tarz söz konusudur. Bu sebeple söz konusu önlemlere koruyucu güvenlik önlemleri de denir. Pasif önlemler; personelin, gizli veya hassas bilginin, önemli tesis ve malzemenin korunması için alınan koruyucu güvenlik önlemlerinin tamamıdır. Pasif İKK önlemleri, düşmanın ele geçirmeye çalıştığı bilgileri gizlemek ve düşmanı bu bilgilerden mahrum bırakmak, personeli yıkıcılık ve terörizmden korumak, kurumları ve malzemeyi sabotajdan korumak gibi amaçlar için tasarlanmıştır. Bu önlemlerin asıl amacı, yetkili olmayanların gizli veya hassas bilgiye ulaşmalarına engel olmaktır. Yani yabancı unsurların olası zararlı girişimlerinin zorlaştırılması, yanıltılması ve engellenmesi amacı güdülmektedir.<sup>55</sup>

Bir bilgi kaybı oluştuktan sonra onunla başa çıkmaya çalışmak yerine rakip girişimlere karşı önceden hazırlanmak ve önlemler almak daha doğru bir hareket tarzıdır. Böylece, rakiplerin olası eylemlerinin başarısız olması ya da en az seviyede başarılı olması sağlanabilir.<sup>56</sup>

Pasif İKK önlemleri; “personel güvenliği / kişisel koruyucu güvenlik”, “fiziksel güvenlik”, “bilgi, bilgi işlem, iletişim ve elektronik güvenliği”, “eğitim, denetim ve farkındalık” başlıkları altında gruplandırılabilir.

### **2.2.1. Personel Güvenliği / Kişisel Koruyucu Güvenlik**

Personel güvenliği; yabancı istihbarat servisleri, yasa dışı oluşumlar ve terör örgütleri tarafından cebir veya tehdit gibi yöntemler ile çeşitli motifler kullanılarak, personelin dinî, siyasi, sosyal ve felsefi inanç, düşünce ve kanaatlerinin değiştirilmesi girişimlerini engellemeye, bahse konu girişimlere maruz kalan veya karışanları ise bu faaliyetlerden vazgeçirmeye veya kurtarmaya yönelik, yasalar çerçevesinde alınması gereken önlemler bütünüdür.

Personel güvenliğinin iki boyutu vardır. Birinci boyutu, bizzat kişilerin güvenliği

<sup>54</sup> U.S. Marine Corps, **a.g.e.**, s. 1-7.

<sup>55</sup> Tezsever, **a.g.e.**, s. 166; U.S. Marine Corps, **a.g.e.**, s. 1-8.

<sup>56</sup> Douglas, **a.g.e.**, s. 94.

için alınan önlemlerdir. İstihbari anlamda önemli sayılabilecek kişilerin, istihbarat birimleri, terör eylemleri, sabotaj ve suikastlara karşı korunmaları, organizasyonların yönetimlerinden ve dolayısıyla da onlar adına bu görevi yürüten güvenlik ve istihbarat / İKK birimlerinden beklenen bir görev ve öncelikli faaliyet sahasıdır.<sup>57</sup> İkinci ve asıl önemli boyutu ise, karşı istihbaratta en önemli unsur olan bireylerin yani en basit bilgiden en önemli sırlara kadar her türlü bilgiye sahip kişilerin yabancı istihbarat birimlerinden korunması için alınan önlemlerdir.

Tespit edilmiş olan casusluk (askerî, politik, ekonomik, vb.) olaylarında, personelin bireysel hata payının oldukça büyük olduğu ortaya çıkmaktadır. Durum her ne kadar böyle olsa da istihbarat örgütleri hiçbir zaman personelin hata yapmasını beklemeyiz. Uygun koşulları oluşturarak personeli hata yapmaya zorlarlar veya düşkünlük ve açıklarını yakalamak suretiyle bilerek ve isteyerek bildiklerini vermelerini sağlamaya çalışırlar. Her personelin casusluk girişimlerine açık olabileceğinden hareketle ve güven–denetim dengesini iyi ayarlayarak birtakım önlemler alınması gereklidir. Bu doğrultuda alınabilecek önlemler şunlardır: <sup>58</sup>

- İşe alım aşamasında personelin özgeçmişi ve yaşantısı incelenmeli (arşiv araştırması ve güvenlik soruşturması), işe alındıktan sonra da gereksinim duyulan personel için tekrarlanmalıdır.

- Özellikle bilgiye doğrudan erişim kolaylığı sağlayan (santral görevlisi, sekreter vb.) görevlere personel seçilirken daha hassas ve özenli davranılmalıdır.

- Her türlü (askerî, siyasi, ticari vb.) sır hakkında personel ile gizlilik anlaşması yapılmalı veya teminat belgesi alınmalıdır.

- Personelin çalıştırılacağı yer ve konuma uygun olan gizli bilgilere ulaşabilmesi için gizlilik derecesi yetkilendirmesi yapılmalıdır.

- Belirli dönemlerde personelin mali durumları denetlenmeli, istihbarat örgütlerince kötüye kullanılabilecek aşırı borçlanma gibi durumların olup olmadığı

<sup>57</sup> Sait Yılmaz, **21.Yüzyılda Güvenlik ve İstihbarat**, Milenyum Yayınları, İstanbul, 2007, s. 119.

<sup>58</sup> Seliina Päälysaho ve Jari Kuusisto, “Informal Ways to Protect Intellectual Property (IP) in KIBS Business”, **Innovation: Management, Policy & Practice**, Vol.: 13, Issue.: 1, 2011, 62–76, s. 69; William M. Fitzpatrick, Samuel A. Dilullo ve Donald R. Burke, “Trade Secret Piracy and Protection: Corporate Espionage, Corporate Security and the Law”, **Advances in Competitiveness Research**, Vol.: 12, No.: 1, 2004, 57–71, s. 62; SECURITAS, **Kurumsal Gizlilik Rehberi**, ss. 3–4, <https://www.securitas.com/PageFiles/32308/Kitap%C3%A7%C4%B1klar/kurumsalgizlilikrehberi.pdf> (Erişim tarihi: 10 Ocak 2013); Yakın, **a.g.e.**, s. 179.

mal bildirimi vb. yöntemlerle tespit ve takip edilmelidir. Aşırı borçlanma gibi düşkünlükleri bulunan personelin, özellikle gizlilik derecesi yüksek bilgiye ulaşabileceği görevlerde çalıştırılmamasına özen gösterilmelidir.

– Görev ve ücret dağılımında adalet sağlanmalıdır. Aldığı ücretin, hak ettiğinden az olduğunu ya da ücret dağılımında adaletsiz davranıldığını, kendisinin diğerlerinden fazla çalıştırıldığını düşünen bir personelin, istihbari açıdan ciddi bir tehlike oluşturacağı unutulmamalıdır.

– Personelde kuruma sadakat duygusu yerleştirilmelidir. Olası sadakatsizliklerin bir nebze önüne geçmek için personelin, belirli veya belirsiz sürelerde görev çeşidi veya görev yeri bakımından rotasyonunun (yer değiştirmesi) yapılması planlanmalıdır.

– Personelin, harici kurum ve kuruluşlar ile yabancılardan hediye, promosyon, eşantyon, malzeme vb. şeyler kabul etmesi yasaklanmalı, alınmasına karşı yaptırımlar belirlenmelidir.

– Büyükelçilik, konsolosluk ve ataşelik gibi, ülke dışında diplomatik ve askerî görevler icra edilen kurum ve kuruluşlarda aşçıdan şoföre, hizmetliden meydancıya kadar tüm çalışanlar kendi ülkemizden gönderilmeli ve yerli halktan personel çalıştırılmamasına özen gösterilmelidir.

– Ziyaretçiler, çalışma ofisleri yerine tahsis edilen ziyaretçi salonlarında kabul edilmelidirler. Kurumda ziyaretçi salonu bulunmuyorsa, ofislerdeki ziyaretçi kabulleri için ayrı bir masa ya da bölüm kullanılmalıdır. Personelin çalıştığı masa ya da makamda yapılması gereken ziyaretçi kabullerinde ise oda içerisindeki ve masa üstündeki önemli bilgiler göz önünden kaldırılmalıdır.

– Temizlik, inşaat, bakım ve onarım gibi işlerle ilgili personelin denetimi yapılmalı, gizli bölgelerin ve hassas belge ve sistemlerin bulunduğu odalarda yapılacak her türlü çalışma gözetim altında yapılmalıdır. Bu faaliyetler, çalışma saatlerinin bitiminde, tatil günlerinde ve personelin tamamının kurumu terk ettiği zamanlarda yapılmamalıdır.

– Yabancıların ülke içindeki seyahatleri ve girebilecekleri bölgeler kısıtlanmalıdır. En azından yabancıların ülkeye giriş ve çıkış kayıtları üzerinden

yapılacak çözümler sonucunda şüpheli görülen kişiler mutlaka takip edilmelidir.

- Kurumdan ayrılmış / emekli olmuş eski personel, en azından belli bir süre (bildiklerinin istihbari değeri kaybolana kadar) takip ve kontrol altında tutulmalıdır.
- Çalışanların, kurum dışından yabancı kişilerce veya kurum içindeki konu ile ilgisiz personel tarafından yapılabilecek bilgi istekleri ile karşılaşmaları durumunda başvurabilecekleri birimler belirli olmalı, yoksa oluşturulmalıdır.

### 2.2.2. Fiziksel Güvenlik

Fiziksel güvenlik; yetkisiz kişilerin hassas bilgiye ulaşmasını önlemek, bunların casusluk, sabotaj, hırsızlık, hasar ve zarar verme gibi eylemlere karşı korunmasını sağlamak maksadıyla alınması gereken yerleşim yeri ve yerleştirme kapsamındaki fiziksel önlemlerdir.<sup>59</sup> Fiziksel güvenlik en basit şekliyle, korunması amaçlanan şeyle ona ulaşmak isteyen kişiler arasına bir engeller sistemi yerleştirmektir. Fiziksel engelleri;<sup>60</sup>

- Doğal engeller (nehirler, dağlar, uçurumlar vb.),
- Yapay engeller (tel örgüler, duvarlar vb.),
- Beşerî engeller (nöbetçi, özel güvenlik birimleri vb.),
- Hayvansal engeller (devriye köpekleri gibi),
- Teknolojik engeller (güvenlik kameraları, sensörler vb.) şeklinde gruplandırmak mümkündür.

Fiziksel güvenlik önlemleri, organizasyonun sahip olduğu tesisleri korumak maksadıyla alınan önlemleri kapsar ve bütünsel bir anlayışla ele alınmalıdır. Örnek vermek gerekirse bilgisayar ve ağların fiziksel açıdan güvenliği kesinlikle göz ardı edilemeyecek bir durumdur. Bilgisayar ve ağ sistemlerinin fiziksel olarak korunmaması, ileri teknoloji içeren güvenlik önlemlerini (şifreleme, anti-virüs programları, güvenlik duvarları vb.) de anlamsız kılar.

<sup>59</sup> Yılmaz, **21. Yüzyılda... a.g.e.**, s. 119.

<sup>60</sup> Acar ve Urhal, **a.g.e.**, s. 303.

Günümüzde fiziksel güvenliğin önemi, teknolojik ve bilimsel gelişmelere paralel olarak oldukça artmıştır. Örneğin, tesislerin etrafına yüksek duvarlar ya da demirler yapılması, tesislerin girişlerinde ve etrafında güvenlik birimlerinin bulundurulması, önemli verilerin tutulduğu odaların kilitlenmesi ya da bu odalara şifreli güvenlik sistemleri ile girilmesi gibi önlemler eskiden sadece askerî tesisler için kullanılmakta iken günümüzde en küçük işletmenin bile çeşitli fiziksel güvenlik önlemleri ile kendi tesislerini koruma çabası içine girdiği görülmektedir.

Güvenlik konusu aynı zamanda, özel sektör için ayrı bir iş dalı doğmasına ve hızla yaygınlaşmasına da sebep olmuştur. Son yıllarda ülkemizde birçok özel güvenlik şirketi kurulmuş ve –verdikleri hizmet, personelinin güvenlik konusundaki sorumluluk, yetki, eğitim ve yeterlilikleri tartışma konusu olsa da<sup>61</sup>– resmî veya resmî olmayan çok sayıda kurum ve kuruluş tarafından bu şirketlerin sağladığı hizmetler kullanılır olmuştur.

Bir organizasyon, düşman ve rakiplerinin yanı sıra kendisini de iyi tanımalıdır. Korunması gereken bilginin tespit edilmesi, söz konusu bilginin hassasiyet derecesinin ve korunma süresinin belirlenmesi önemlidir. Fiziksel güvenlik bakımından sıkı standartlara sahip olan bir organizasyonun, personel maskesi altında düşman için çalışan bir casus tarafından istenmeyen durumlara sokulması işten bile değildir. Mükemmel bir fiziksel güvenliğe ve son derece güvenilir personele sahip olunması, profesyonel bir istihbarat veya casusluk girişimini engellemek için asla yeterli görülmemeli, her zaman diğer önlemlere de gereken önem verilmelidir.<sup>62</sup>

Tüm tesisler önemli ve değerlidir ancak hepsi için aynı derecede fiziksel güvenlik ve koruma sağlamak ekonomik olmayacağı gibi gerekli de olmayabilir. Bu nedenle fiziksel güvenlik gereksinimlerinin öncelikleri ve gerekli olup olmadıkları belirlenmelidir. Gelişen teknolojik olanaklardan da faydalanılarak; mevcut tehdidi karşılayacak, personeli rahatsız etmeyecek ve bunaltmayacak şekilde fiziksel engellerin oluşturulması ve genel anlamda fiziksel güvenlik önlemlerin alınması için çalışılmalıdır. Gereğinden fazla alınan ve bunaltıcı önlemlerin, fayda sağlamak bir yana, zararlı dahi olabileceği unutulmamalıdır.

---

<sup>61</sup> R. Cengiz Derdiman, “Özel Güvenlik Hizmetlerinin Niteliği ve Etkin Bir Şekilde Yürütülmesi İçin Yapılması Gereken Düzenlemeler”, **3. Ulusal Özel Güvenlik Sempozyumu Bildirisi**, Gaziantep, 1–2 Mart 2013, 37–56, ss. 52–53.

<sup>62</sup> Douglas, **a.g.e.**, s. 85.

Tesislerin fiziksel güvenliğinin sağlanması konusunda alınabilecek önlemler şunlardır:<sup>63</sup>

- Tesislerin çevresi, istihbarat elde edilmesine (özellikle gözetlenmeye) karşı korunmak amacıyla yüksek duvarlar veya içerisinin görünmesine engel olan yüksek ve çabuk büyüyen sık ağaçlarla çevrilmelidir. Özellikle gizliliği yüksek tesislerin dışarıdan gözetlenememesi için fiziksel önlemler alınmalıdır (renkli veya aynalı camlar gibi). Çevre güvenlik duvarları; tel örgü, tel üstüvane vb. takviye engel malzemesi ile kuvvetlendirilmelidir.

- Giriş ve çıkış yapılan kapılar en az sayıda (yeterli olabiliyorsa tek kapı) tutulmalı, kapı sayısının çok olması gereken durumlarda her bir kapıya aynı önemi vererek denetim sistemleri oluşturulmalıdır (Kapı miktarının en az sayıda tutulması, bir İKK önlemi olmasının yanında, güvenlik maliyetlerinin azalmasına da katkı sağlayacaktır.).

- Tesisler, kurulacak nöbet ve devriye sistemleri ile (birlikler için askerler, kurumlar ve işletmeler için yerine göre polis veya özel güvenlik görevlileri tarafından) korunmalıdır.

- Önemli tesis ve bölgeler güvenlik kameraları ile izlenmelidir.

- Alarm sistemleri kurularak izinsiz ve yetkisiz girişler tespit edilmelidir.

- Gizleme tekniklerinden olabildiğince çok faydalanılmalıdır.

- Çalışan personel tarafından günlük mesai bitiminde ofisin pencereleri kapatılmalı, perdeler çekilmeli, çalışan büro aletleri, özellikle bilgisayarlar kapatılmalı, disketler kilitli yerlerde muhafaza edilmeli, kapılar kilitlenerek anahtarları güvenlik yöneticisinin belirlediği bir güvenlik odasında, varsa bir prosedüre bağlı olarak işletilen anahtar dolabında bulundurulmalıdır.

- Yedeklenmiş materyal ve yedek sistemler, olası sabotaj vb. kötü maksatlı girişimlere karşı ana tesislerden yeterince uzak bir yerde konuşlandırılmış olmalıdır.

---

<sup>63</sup> SECURITAS, **a.g.e.**, ss. 5–7; R.Mark Halligan ve Richard F. Weynand, “The Economic Valuation of Trade Secret Assets”, **Journal of Internet Law**, Vol.: 9, Issue.: 8, 2006, 19–24, s. 23.

– Hassas bilgilerin bulunduğu yerlere giriş için sadece yetkili personele izin verilmeli ve ziyaretçiler bu gibi yerlerden uzak tutulmalıdır. Güvenli alanlara erişim yetkileri düzenli olarak gözden geçirilmelidir. Kurum içinde, belli duyarlılıktaki veya gizli yerlere sadece yetkili personelin girişine izin verecek şekilde kontrol sistemleri (kartlı, şifreli veya tanıma sistemli girişler gibi) kurulmalıdır.

– Personel ve ziyaretçilerin ses, fotoğraf ve video kaydı yapabilen cep telefonu vb. her türlü cihazı tesislere ve özellikle gizli toplantılara sokmamaları (en üst düzeydeki yönetici dâhil hiçbir istisna olmadan) sağlanmalıdır.

– Tesislere gelen ziyaretçilerin kimlik bilgileri, geliş maksatları, giriş ve çıkış zamanları kaydedilmelidir. Ayrıca tüm personel ve ziyaretçiler tesis içinde, herkes tarafından rahatça tanınabilmelerini sağlayacak olan kimlik kartlarını sürekli takmalıdırlar.

– Ziyaretler ile inşaat, bakım ve onarım gibi çalışmalar, mutlaka refakat, nezaret ve kontrol altında yapılmalıdır. Özellikle tatil günleri ve mesai saatleri dışındaki zamanlarda ziyaretler ve çalışmalar en az seviyede tutulmalı, mümkünse yapılmamalı, yapılması zorunlu ise güvenlik yöneticisinin izni ve nezaret altında yapılmalıdır. Kötü niyetli girişimlere engel olmak için, hassas bölgelerde yapılan çalışmalara nezaret edilmeli, bu faaliyetler için içeri alınan kişiler daha önceden araştırılmalıdır [en azından Genel Bilgi Toplama (GBT) sorgulaması yapılabilir].

– Özel (genel ulaşımına açık olmayan veya gizli odalar gibi) tesisler kolayca ulaşılamayacak yerlere kurulmuş olmalıdır. Bu tür yerler, bina duvarlarındaki ve diğer yerlerdeki yer ve yön bildiren, ulaşımı kolaylaştırıcı işaret, tabela ve levhalarda bulunmamalıdır. Söz konusu yerlere giriş yetkisi olan kişilerin, görevleri gereği bu yerleri bilecekleri, giriş yetkisi olmayan kişilerin de bu yerleri bilmelerine gerek olmadığı göz önünde bulundurulmalıdır. Aynı şekilde bina krokisini gösteren haritalarda bu tür özel yerler gösterilmemelidir. Ayrıca bu tür tesisler dikkat çeken renklere boyanmamalı, gösterişli ve kendini belli eden yapılardan kaçınılmalıdır.

– Oluşturulan sistemler, dışarıdan gelmesi olası tehdit, kötü niyetli girişim ve saldırılara karşı önleyici ve caydırıcı nitelik taşınmalıdır. Tesisleri korumak için hazırlanan sistemlere yapılacak olası girişimlere karşı korunma planları hazırlanmalıdır (sabotajlara karşı korunma planı gibi).

– Alınacak önlemler, tesislere yönelebilecek her türlü tehdidi önleyebilecek kadar kapsamlı ve nitelikli, amacını aşmayacak kadar da ekonomik olacak şekilde geliştirilmelidir. Kısacası, fayda–maliyet değerlendirmesi iyi yapılmalıdır.

### 2.2.3. Bilgi, Bilgi İşlem, İletişim ve Elektronik Güvenliği

Bilgi, bilgi işlem (yazılım, donanım ve siber), iletişim ve elektronik güvenliği konuları aslında her biri farklı güvenlik bölümleri olmalarına rağmen o kadar iç içe geçmişler ve birbirlerine etkileri o kadar üst seviyededir ki hepsini tek başlık altında ele almanın daha doğru bir yaklaşım olacağı değerlendirilmiştir.

Bilgi, her organizasyon için değerli bir varlıktır. Dolayısıyla her değerli varlık gibi güven altında olması istenir. Bilgi güvenliğinin amacı, her türlü organizasyonda yürütülen işlemlerin, korunan her türlü değerli bilginin düşman, rakip, yetkili olmayan veya ilgisiz kimseler tarafından tahrip edilmesine, ele geçirilmesine, kullanılmasına ya da değiştirilmesine engel olmaktır. Bilginin ve bilgiye ait işlemlerin yürütüldüğü bilgi sistemlerinin güvenli olarak kullanılabilmesi, bütünlüğünün ve gizliliğinin korunması ve yetkisiz kişilerin bilgiye ulaşmaları hâlinde tespit edilmelerine yönelik olarak alınan önlemlerin tümü bilgi güvenliği olarak adlandırılabilir.<sup>64</sup>

Gizli kalması gereken bilgi kapsamına şunlar ve burada sayılamayan benzer birçok örnek girebilir: Notlar, tutanaklar, raporlar, muhtıralar, emirler, tebligatlar, çeviriler, talimnameler, yönergeler, yönetmelikler, resimler, fotoğraflar, krokiler, grafikler, planlar, haritalar, fotoğraf negatifleri, fotokopiler, mikrofilmler, ses bantları, müsvedde (karalama) kâğıtlar, karbon kâğıtları, her türlü yazıcı ve daktilolar, bilgisayar kasaları ve bellekler.

Bilginin çok farklı şekillerde muhafaza edilmesi mümkündür. Bilgi yazılı olacak diye bir zorunluluk yoktur. Yazılı, sözlü ya da sadece davranışsal bir durum, bilgi olarak değerlendirilebilir. Ayrıca yazılım, donanım ve malzemenin de başlı başına birer bilgi unsuru olduğunu söylemek gerekir. Bilgi teknolojilerinde yaşanan gelişmeler sonucu her türlü bilgi, bilgi sistemleri üzerinde depolanmaya ve saklanmaya başlanmıştır. Gizlilik dereceli her türlü bilgi ve bilgi işlem sistemleri, yetkisiz erişime ve bozulmaya karşı son derece duyarlıdır. Ayrıca yenilerinin

<sup>64</sup> Günce Öztürk, **Bilgi Güvenliği Politikası Oluşturma Kılavuzu**, TUBİTAK UEKAE, Doküman Kodu: BGYS–0005, 2008, s. 7, <http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0005-bilgi-guvenligi-politikasi-olusturma-kilavuzu.html> (Erişim tarihi: 30 Mart 2013).

yapılması veya yerine konması zaman alıcı ve masraflı olduğu için casusluk ve sabotaj düşüncesindeki kişiler için de ilgi odağı konumundadırlar. Sonuçta önemli olan ve öne çıkan husus, bilginin hangi formda olduğu değil, uygun önlemler alınmak suretiyle mutlaka bir şekilde korunması gerektiğidir.<sup>65</sup>

Kullanımı yaygınlaşan bilgi işlem sistemlerinin (bilgisayarlar, cep telefonları vb.), işleri kolaylaştırmanın yanında erişim risklerini artırdığı da unutulmamalıdır. Ağlara istenmeyen erişimlerin engellenmesi ile zararlı yazılımlardan ve olası saldırılardan korunmak maksadıyla alınan önlemler, her türlü elektronik ortamda yer alan verinin güvenli şekilde depolanması, kullanılması ve iletilebilmesi bakımından son derece önemlidir.<sup>66</sup>

Öte yandan ulusal olmayan bilgi işlem sistemlerinin kullanılmasıyla asla tam anlamıyla bir gizlilik koruması sağlanamayacağı, üretici firmaların her zaman sistemi kendi isteklerine de cevap verebilecek şekilde tasarlayacakları ve sadece kendilerinin bildiği donanım ve yazılım açıkları bırakabilmelerinin mümkün olduğu göz ardı edilmemelidir. Örneğin, herhangi bir devletten satın alınan bir silah ya da araç sisteminin üzerindeki küresel konumlama cihazının, aracın konumunu bize bildirirken aynı anda satın alınan devlete de bildirmeyeceğini düşünmek büyük hata olur. Yine gelişmiş özelliklere sahip bir yazıcının veya fotokopi makinesinin, her yaptığı işlemi belleğine kaydedeceği ve bunları üretici firma ve dolayısıyla rakip devlete aktarabileceğini kestirmek güç değildir.<sup>67</sup>

Düşman ya da rakip unsurlar birbirlerine üstünlük sağlayabilmek adına, tarih boyunca her dönemde birbirlerinin iletişim yöntemlerini tespit etmek, iletişimlerini engellemek, iletişimlerin içeriğini öğrenmek ve sistem içerisine sahte ve yanlış bilgi sokmak için çabalamışlardır. Günümüzde de, teknolojinin hızlı gelişimi, iletişim aygıtlarında kendini fazlasıyla göstermektedir. Her geçen gün yepyeni iletişim yöntem ve sistemleri piyasaya sürülmektedir. Buna paralel olarak iletişim açıkları da artmaktadır. Günlük yaşantıyı kolaylaştıran her iletişim aygıtı aynı zamanda iletişim güvenliği bakımından ciddi riskleri de beraberinde getirmektedir. İletişim güvenliği denilince telli, telsiz ve diğer tüm vasıtalarla iki kişi veya unsur arasında kurulan ve her türlü verinin (ses, görüntü, belge vb.) gönderilip alındığı bir sistemin olası

<sup>65</sup> Acar ve Urhal, **a.g.e.**, s. 307.

<sup>66</sup> Hamza Elbahadır, **Hacking Interface**, Kodlab Yayın Dağıtım, İstanbul, 2011, s. 4.

<sup>67</sup> Olay Salcan, "Bilgi Güvenliği", **Silahlı Kuvvetler Dergisi**, Sayı: 370, Genelkurmay Basımevi, Ankara, 2001, 54-67, s. 59; Tolga Yarman, **Geçmişte ve Bugün Nükleer Enerji Tartışması**, Okan Üniversitesi Yayınları, İstanbul, 2011, s. 155.

tehditlere karşı korunması anlaşılır.

Fiziksel ve personel güvenlik önlemlerinin uygulanması her ne kadar güvenli bir ortam oluşturulmasına yardımcı olsa da bilgi, bilgi işlem, iletişim ve elektronik güvenliğine yönelik önlemler uygulanmadan güvenliğin tam olarak sağlanması mümkün değildir. Bu bağlamda alınması gereken önlemler şunlardır:<sup>68</sup>

- Ülke güvenliği, çıkarları ve saygınlığının korunması bakımından önem taşıyan bilginin ilgili ve yetkili olmayan kişilerin eline geçmesinin ve izinsiz açıklanmasının önlenmesi, içeriğinin önem derecesine ilgililerin dikkatinin çekilmesi, gizlilik ihlaline meydan verilmemesi ve bilginin muhafazasının öngörülen esaslar çerçevesinde sağlanması amacıyla gizlilik dereceleri kullanılmalıdır.

- “Bilmesi gereken ilkesi” kapsamında sınırlı sayıda ve sadece yetkili kişilerin hassas ve gizli bilgilere erişebilmesi sağlanmalıdır.

- Hassas bilginin üzerine gizlilik derecesini gösteren damgalar veya işaretler konulmalı ve yeterli fiziksel önlemin alındığı kilitli yerlerde tutulmalıdır. Bilgi, dijital (sayısal) ortamda saklanması gerektiğinde, mutlaka şifrelenmiş veya kriptolanmış hâlde bulundurulmalıdır.

- Gizli belgelerin ilgisiz veya açık yerlerde bulunması engellenmelidir. Önemli belgeler açıkta bırakılmamalı, işi bitenler dosyalanmalı, diğerleri ise kilitli bir çekmeceye ya da dolaba kaldırılarak muhafaza edilmelidir. Gizlilik derecesi yüksek belgeler ise güvenliğine ayrı önem gösterilen yerlerde saklanmalıdır.

- Gizli, hassas ve hatta önemsiz olarak değerlendirilen her türlü bilginin karalaması, çöp sepetlerine atılmamalı, uygun yöntemler kullanılarak (örneğin kâğıt kırma makinesinden geçirilerek) imha edilmelidir. Tarih boyunca birçok önemli plan ve projenin çöplerdeki karalamalardan toplanarak çalındığı unutulmamalıdır.

- Bilgi işlem sistemlerinin kurulumu ve işletilmesinden sorumlu personel işinin ehli olmalıdır. Özellikle kurumda çalıştırılan personel içinde, bilgi işlem konusunda,

<sup>68</sup> Douglas E. Dexter ve Jessica Beckett-McWalter, “Protecting Trade Secrets: Best Practices from Hiring to Terminating and Everything in Between”, *Licensing Journal*, Vol.: 26, Issue: 1, 2006, 1–5, s. 3; Yakın, *a.g.e.*, s. 179; SECURITAS, *a.g.e.*, ss. 4–9; Salcan, *a.g.e.*, s. 57; Douglas, *a.g.e.*, s. 94; *Muhabere Emniyeti*, <http://www.belgeler.com/blg/h7a/muhabere-emniyeti> (Erişim tarihi: 03 Nisan 2013).

bilgi işlem sorumlusu olan kişiden daha bilgili ve yetenekli kimse bulunmamalıdır.

– Bilgi işlem sistemleri üzerinde bulunan veriler doğru şekilde yedeklenmediği sürece her an kaybedilebilir durumdadır. Verilerin kaybedilmesi beraberinde zaman ve maddi kayıp getirebilir. Bu nedenle personel, kendilerine gösterildiği şekilde ve belgelerin önem derecelerine göre dönemsel olarak yedeklerini alarak bu konudaki riski en aza indirmelidir.

– Kişisel bellek vb. depolama aygıtlarının kurum içerisine sokulmaması veya bu belleklerin denetimli kullanılması sağlanmalıdır. Koşulsuz yasaklamaların faydasından çok zararının olacağı unutulmamalıdır.

– Önemli bilgi içeren bilgisayarlara ve ağlara erişimi kısıtlayabilmek amacıyla şifreler kullanılmalıdır. Şifrelerle ilgili uygun bir sistem oluşturularak belirli aralıklarla şifrelerin değiştirilmesi sağlanmalıdır. Ayrıca şifrelerin kolayca tespit edilemeyecek ve kırlamayacak kadar karmaşık olması da gereklidir. Çok gizli ve hassas bilgi içeren bilgisayarlar için ise şifrelemeye ek olarak parmak izi ve retina tarama gibi sistemlerden de faydalanılmalıdır.

– Hassas veri barındıran bilgisayarların ve çıktı alınan yazıcıların internet ile bağlantısı bulunmamalıdır.

– İnternete bağlı bilgisayar kullanımı kaçınılmaz olan yerlerde, teknik açıklar göz önünde bulundurularak gerekli önlemler alınmalıdır. İnternet ve diğer ağlara bağlı olan bilgi işlem sistemleri, güvenlik duvarı ve sızma tespit sistemleri tarafından korunmalıdırlar.

– Her türlü iletişim aygıtı aracılığıyla iletilecek veriler, mutlaka şifrelenmelidir. Hatta maddi ve teknik olanağı bulunan organizasyonların şifrelemeye ek olarak kriptolama seçeneğini de devreye sokmaları gereklidir.

– Telsiz iletişim sistemlerinin en güvensiz iletişim vasıtaları olduğu unutulmamalı ve telsizlerle kurulan iletişimler, gizli ve hassas bilgi içermemelidir.<sup>69</sup>

– Telli iletişim sistemlerinin (telefon, telgraf vb.) yeterince güvenli

<sup>69</sup> Nuh Gönültaş, "Apo'ya O Kadar Söyledik Cep Telefonu Kullanma Diye...", **Zaman**, 21 Şubat 1999, <http://arsiv.zaman.com.tr/1999/02/21/yazarlar/10.html> (Erişim tarihi: 11 Nisan 2013).

olmadığından hareketle, telefon konuşmaları olabildiğince kısa tutulmalı, gizlilik dereceli konular kesinlikle telefonda açıklanmamalı, veri aktarımlarında şifreleme, kriptolama ve kod kullanma kurallarına uyulmalı ve telefon görüşmelerinin dinlenebileceği hiçbir zaman unutulmamalıdır. Özel toplantı, görev, operasyon gibi önemli faaliyetlerin tarih, saat ve ayrıntıları telefonla veya diğer telli iletişim araçlarıyla bildirilmemeli ve konuşulmamalıdır.

– Telli, telsiz ve diğer bütün iletişim araçlarını korumak amacıyla;

- Maddi güvenlik önlemleri (emin yerde bulundurma, nöbetçilerle koruma, denetim ve depolama vb.),

- Gönderme güvenlik önlemleri (kodlama, emin kurye, iç içe zarf vb.),

- Şifre ve kriptolu güvenlik önlemleri (açık ve kriptolu bilginin aynı yerde bulundurulmaması, şifrelenmiş bilginin açık olarak gönderilmemesi, şifreleme ve kriptolama malzemesinin ve aletlerinin tahribinin kırıltarak ve yakılarak yapılması vb.) alınmalıdır.

– Gizlilik dereceli konuların görüşüldüğü oda ve toplantı salonlarında bulunan iletişim sistemlerinin (dâhili / harici telefonlar, iç konuşma sistemleri, çeviri cihazları, kablolu ve kablosuz mikrofonlar vb.) yapılacak konuşmaların içeriğinin dışarıya taşınmasında kullanılacak uygun birer araç olma özelliğine sahip oldukları ve dolayısıyla büyük tehlike taşıdıkları unutulmamalıdır. Bu bağlamda şu önlemler göz önünde bulundurulmalıdır:<sup>70</sup>

- Bu tür sistemler, mümkün olduğunca organizasyon dışından firma ve kişilere kurdurulmamalıdır.

- Gizli ve hassas konuların görüşüldüğü oda ve salonlarda mümkün olduğunca az teknolojik ve elektronik sistem bulundurulmalıdır.

- Odaların olası dinleme ve izlemelere karşı sık sık teknik denetimleri ile ortam aramaları yaptırılmalıdır.

---

<sup>70</sup> Yakın, **a.g.e.**, s. 179.

- Benzer ve önemli toplantılar sürekli aynı salonlarda değil, zaman zaman son anda yapılacak değişikliklerle ve odaların gerekli denetimleri de yapılarak, farklı odalarda yapılmalıdır. En güvenli olduğu düşünülen oda ve salonların, gizliliği delmek isteyen kötü amaçlı kişiler tarafından öncelikli hedefler olduğu unutulmamalıdır.

- İçinde bulunulan binaların hangi firmalar tarafından yapıldığı dahi önemlidir ve inşaat esnasında, sonradan fark edilmesi mümkün olmayan sistemlerin duvarlara, kolonlara, pencerelere vb. akla gelmeyecek herhangi bir yere yerleştirilmiş olabileceği göz önünde bulundurulmalıdır.

- Teknik ve elektronik izlemeye karşı gereken önlemler alınmalıdır.

- Her türlü elektronik cihazdan yayılan, istenmeyen elektromanyetik enerji yayılımları ve bu yayılımların kontrol altına alınması olarak tanımlanan elektronik emisyon güvenliği (TEMPEST\*), gizlilik dereceli bilgilerin işlendiği bilgi işlem sistemlerinin, elektromanyetik ışıma yoluyla veya yakınında bulunan her türlü iletken vasıtası ile bilgi çalınmasına karşı alınacak tüm önlemleri kapsayan bilgi güvenliği boyutudur. Emisyon güvenliği özel teçhizat ve eğitim gerektirdiğinden uzman kişiler tarafından yapılmalıdır. Elektronik sistem veya cihazların uğrayacağı saldırılara karşı alınacak TEMPEST karşı önlemlerinin, yetkin kişilerce yapılacak olan risk ve tehdit değerlendirmelerine göre belirlenmesi ve uygulanması gerekir.

- Organizasyon dışında kullanılacak olan donanım için yönetim tarafından yetkilendirme yapılmalıdır. Organizasyon dışına çıkarılan donanımın denetim altında tutulmasına (örneğin; önemli belgelerin bulunduğu çantaların ve dizüstü bilgisayarların seyahat hâlindeyken el bagajı olarak taşınmasına ve mola gibi sebeplerle araçtan inilirken de araçta bırakılmamalarına) dikkat edilmelidir. Ayrıca herhangi bir hasar veya arıza durumunda organizasyon dışında bakım ve onarıma gönderilecek olan bilgi işlem malzemesi (bilgisayar, yazıcı vb.), hafızaları tamamen silinmiş\*\* ve bilgi değeri taşımaz hâlde gönderilmelidir.

- Kullanımdan çıkan (hurda) ve işlevini yitiren malzeme, teknik bilgiye sahip

---

\* TEMPEST: Transient ElectroMagnetic Pulse Emanation Standard (Yayılan Elektromanyetik Dalgalardan Bilgiyi Oluşturma). Ayrıntılı bilgi için bkz. Salcan, **a.g.e.**, ss. 54–55.

\*\* Bilgisayarlarda, onlarca defa yapılan formatlamalardan önceki verilerin bile tamamen silinemediği, sırf veri silme işleriyle uğraşan büyük firmaların olduğu, onların da verileri silemedikleri ama bazı tekniklerle sadece ulaşılabilmelerini olanaksız kıldıkları bilinmektedir.

kişilerce kurallarına uygun olarak tahrip ve imha edilmelidir.

– Belgenin hazırlanmasından adresine ulaştırılmasına kadar görevli bütün personelin (belgeyi hazırlayan personel, kayıt görevlileri, şoförler, haberciler, kuryeler gibi) her zaman gizli bilgilere nüfuz edebileceği göz önünde bulundurularak söz konusu personelin seçimi esnasındaki güvenlik soruşturmaları, yeteneklerinin ölçülmesi ve görevleri esnasındaki kontrolleri hassas olarak yapılmalıdır.

– Herhangi bir sebeple (işten ayrılma, istifa, görev veya görev yeri değişikliği gibi) görevi sona erenler, görevi gereği üzerinde bulunan her türlü belge ve malzemeyi teslim ederek ayrılmalıdır. Eğer işten çıkarılma / ayrılma söz konusu ise ve kişi çok gizli bilgiye uzun süre nüfuz etmişse, işten ayrıldıktan sonra da (en azından casusluk vb. bir faaliyet içinde olmadığından emin olunana kadar) takip ve denetim altında tutulmalıdır.

– Gelişmiş siber saldırıları tamamen önlemek mümkün görünmemektedir. Siber saldırı kavramının (özellikle ülkemizde) yeni yeni gerçek anlamda ele alınmaya başladığı ve siber silahların birçoğunun henüz kamuoyu tarafından bilinmediği de göz önünde bulundurulduğunda, saldırılar için hazırlıklı olunması, sistemlerin bu tür saldırılara karşı sıkça kontrol edilmesi ve etkin bir siber güvenlik\* sistemi kurulması gereklidir.

#### **2.2.4. Eğitim, Denetim ve Farkındalık**

İstihbarat ve karşı istihbaratın en fazla üzerinde durduğu, başka bir ifadeyle en çok kullandığı unsur (kaynak, eleman, vasıta vb.) insan ve onun faaliyetleridir. Bu nedenle, tüm personelin istihbarat ve İKK bilincine sahip olacak şekilde eğitilmesi önemlidir. Her türlü casusluk girişiminin engellenmesi konusunda en önemli hususun, personele sürekli eğitim verilerek bu konuda karşılaşılabilecek sorunlar ve durumlar karşısında bir durumsal farkındalık yaratmak olduğu unutulmamalıdır.

Karşı istihbarat eğitimi, personelin farkındalık düzeyini yükseltmeyi ve olası casusluk girişimlerine ve tehditlerine karşı personeli uyarmayı amaçlar. Organizasyonlar; bilgisayar güvenlik duvarları, erişim kontrolü ve diğer güvenlik

---

\* Siber güvenlik kavramı, apayrı bir güvenlik boyutu olarak günümüzün öne çıkan konularından biri olmakla birlikte ayrı bir araştırma konusu olarak ele alınacak kadar geniş bir konu olduğu için burada sadece önemine vurgu yapılmakla yetinilecektir.

önlemleri için milyonlar harcarken, personelin eğitimine genelde çok az bütçe ayırırlar. Temel istihbarat ve İKK konusunda eğitimsiz ve bilinçsiz çalışanlara sahip olundukça, en iyi güvenlik sistemi bile işe yaramayacak ve gedikler verecektir. Temel bilgileri kapsayan ve personelin seviyesine uygun bir İKK ve farkındalık eğitimi, personelin yasal–ahlaki ve yasal olmayan–ahlaki olmayan bilgi toplama teknikleri konusundaki gardını güçlendirecektir.<sup>71</sup>

İstihbarat ve İKK eğitim ve öğretimi, personelin tamamını hedef alan, birbiri ile iç içe ve birbirini tamamlayan, kademeli, sürekli, bireysel ve kitlesel bir eğitim ve öğretim olmalıdır. Özellikle profesyonellerin, eğitim sürecinin sonunda düşmanların, tarafsızların ve hatta dostların niyet ve maksatlarını takip edebilecek, her türlü teknolojik olanaktan yararlanarak zamanında, doğru ve tam olarak istihbarat girişimlerini önleyebilecek bilgi, beceri ve niteliklere sahip olmaları amaçlanır.

Bu bağlamda, İKK eğitiminin, şu dört kategoride düşünülmesi mümkündür ve böyle bir ayırım kişiye göre eğitim ilkesi bakımından daha uygundur:<sup>72</sup>

- Tüm personel için temel İKK eğitimi.
- Profesyonel istihbaratçılar için İKK eğitimi.
- Profesyonel karşı istihbaratçılar için İKK eğitimi.
- Görev ve faaliyet odaklı İKK eğitimi.

Her türlü eğitim ve öğretim sürecinin iyi bir planlama, uygulama, denetim ve geri besleme aşamalarından oluşması gerekir. Karşı istihbarat eğitimi, uygun eğitim yöntemleriyle, görsel ve uygulama ağırlıklı şekilde icra edilmelidir. Ayrıca eğitim ve öğretimin devamlı ve yaşayan bir süreç olduğu göz önünde bulundurularak her türlü gelişme ve yeniliğin sürece dâhil edilmesine özen gösterilmelidir. Teknolojik her gelişme ve buluşun aynı şekilde yeni bir güvenlik açığını beraberinde getirdiği de akıldan çıkarılmamalıdır.

Birçok güvenlik sistemi, profesyonel casuslar tarafından uygulanan bir sızma girişimine karşı koyabilecek yeterlilikte değildir. Bunun en büyük nedeni de

---

<sup>71</sup> Douglas, *a.g.e.*, s. 94.

<sup>72</sup> U.S. Marine Corps, *a.g.e.*, ss. 8-1–8-6.

hazırlanan güvenlik sistemlerinin çoğunun gerçek bir girişime maruz kalmadan önce kapsamlı ve profesyonellerce yapılan deneme ve testlere tabi tutulmamalarıdır. Düzenli bir sızma testi, hem güvenlik sistemini olası açıklara karşı güncelleme ve değiştirme hem de personeli farklı yöntemlere karşı bilinçlendirme görevi üstlenecektir.<sup>73</sup> Diğer güvenlik önlemlerine büyük katkı sağlayan eğitim, denetim ve farkındalık bakımından alınabilecek önlemler şunlardır:<sup>74</sup>

- Casusların kullandıkları istihbarat toplama vasıta, yöntem ve teknikleri hakkında personele uzman kişilerce eğitim verilmelidir.

- Gizliliği sağlamak adına personele, yapacağı işin ve bu iş nedeniyle sahip olabileceği bilgilerin öneminin anlatıldığı oryantasyon (uyum) ve tazeleme eğitimleri planlanmalıdır.

- Personele, karşılaşılması olası her türlü casusluk, sabotaj, terör, anarşi, yıkıcı ve bölücü faaliyetler hakkında gerekli ve yeterince ayrıntılı bilgi verilmelidir. Eğitimlerde, geçmişte yaşanmış örnek ve ibret alınması gereken olaylardan olabildiğince fazla faydalanılmalıdır.

- “Ben ne biliyorum ki?”, “Benim bildiklerimle memleket mi batacak?”, “Bunları zaten herkes biliyor.” şeklindeki tehlikeli düşünce kalıplarının yanlışlığı ve doğurabileceği olumsuz sonuçlar örneklerle personele öğretilmelidir.

- Personel, gerekenden daha fazla bilgiyi aile bireylerine, tanıdıklarına, konuyla ilgili ya da ilgisiz kişilere ve hatta iş arkadaşlarına bile anlatmaması gerektiği konusunda eğitilmelidir.

- Yabancı dil ve bilgisayar kullanımı eğitimlerine önem verilmelidir. Özellikle kişisel bilgisayarların kullanımında dikkat edilmesi gereken hususlar ayrıntılarıyla personele öğretilmelidir. Yabancı dil bilgisinin avantajını en iyi kullanan örneklerden birisi, Kurtuluş Savaşı yıllarında, İngilizceyi birçok aksanıyla mükemmel konuşabilen ve tip olarak da İngilizlere benzeyen İngiliz Kemal'dir. Asıl adı Ahmet Esat Tomruk olan İngiliz Kemal, Kurtuluş Savaşı'nda büyük hizmetler yapmıştır.

---

<sup>73</sup> Douglas, **a.g.e.**, s. 94.

<sup>74</sup> SECURITAS, **a.g.e.**, ss. 3–8; MacDonnell Ulsch ve Michael J. Sullivan, “Protect Intellectual Property and Trade Secrets”, **Baseline**, Issue: 115, 2012, s. 9; Acar ve Urhal, **a.g.e.**, s. 307; Dexter ve Beckett–McWalter, **a.g.e.**, s. 3.

– İnternetin genel olarak kullanımı esnasında ve özellikle sosyal paylaşım siteleri gibi ortamlarda gerçek kişisel bilgilerin kullanılmaması, sır niteliği taşıyan veya taşımayan (en azından kendisinin öyle değerlendirdiği) hiçbir bilginin (belge ve fotoğraf gibi), sosyal iletişim ortamlarında paylaşılması gerektiği ve olası paylaşımların kişisel, kurumsal ve ulusal anlamda maddi ve manevi ciddi zararlar doğurabileceği personele öğretilmelidir.

– Personele; kişisel sorun ve şikâyetleri ile organizasyon içindeki anlaşmazlıkları organizasyon dışına taşımamaları, bu konuların, istihbaratçılar tarafından sömürü unsuru olarak kullanılabileceği anlatılmalıdır.

– Organizasyon dışından yabancı kişilerce veya organizasyon içindeki konu ile ilgisiz personel tarafından yapılabilecek bilgi istekleri ile karşılaşmaları durumunda yapmaları gerekenler ve durumu yetkililere iletmeleri gerektiği personele öğretilmelidir.

– Personele, her türlü kokteyl, yemek ve balo gibi sosyal toplantılarda, alkol tüketimi konusunda dikkatli olunması gerektiği ve haddinden fazla alkol tüketimi sonucu içine düşülebilecek durumların, bu durumdan yararlanmak ve bilgi sızdırmak isteyen istihbaratçılar için önemli bir fırsat yaratacağı anlatılmalıdır.

– Personele tanımadığı kişilerle görüşmelerinde temkinli ve şüpheli davranmaları, kişinin kimliğinden emin olunsu bile, kişisel ve göreve yönelik konularda konuşmamaları öğretilmelidir. Her türlü mesleki giysinin şüphe çekmeden kolayca elde edilebildiği ve profesyonel istihbaratçıların tahmin edebileceğinden daha başarılı bir şekilde kılık değiştirebilecekleri hatırlatılmalıdır.

– Gafil muhbirlik kavramı personele öğretilmelidir.

– Kurumdan ayrılmış / emekli olmuş eski personele karşı hazırlanabilecek olası casusluk düzenleri ile bilgi almaya çalışan kişilere karşı yapılması gerekenler ve bu personelin eski kurumu ile ilgili istihbari değeri olan her türlü konuyu ayrıldıktan sonra unutması gerektiği öğretilmelidir.

– Organizasyon açısından korunması gereken yani istihbari değer taşıyan bilgilerin neler olabileceği ve nedenleri, çok önemsiz bir bilgi gibi görünen sıradan bir verinin bile çok önemli sonuçlar doğurabileceği personele anlatılmalıdır.

– Personeli uyarıcı mahiyette özel mesajlar içeren resimli duvar ilanları ve özlü sözler, çalışma ortamlarında uygun yerlere asılmalıdır.

– Kurumsal farkındalık yaratılması amacıyla, şüpheli olaylarla karşılaştığını düşünen personel, organizasyon içerisinde kiminle ya da hangi birimle irtibata geçmesi gerektiği konusunda bilinçlendirilmelidir.

– Her türlü güvenlik önleminin işlerliğinin ölçülmesi ile sistemdeki hassas noktaların ve açıkların tespit edilmesi maksadıyla saldırı ve savunma tatbikatları yapılmalıdır. Elektronik ve bilgi işlem sistemlerine yapılacak olası girişimlere karşı korunma planları hazırlanmalı ve tatbikatlarla sistemin güvenliliği ve eksiklikleri belirlenip giderilmelidir.

– Personele belirli aralıklarla uyulması gereken gizlilik kuralları ile temel İKK konularında eğitim verilmeli ve kurallara uyulup uyulmadığı dönem dönem yapılacak denetimler ile kontrol edilmelidir. Alınan önlemlerin yeterliliğini ölçmek maksadıyla çeşitli zamanlarda yapılacak gözlem ve denetimler, kurumsal farkındalığı da canlı tutacaktır.

Toplayıcılar, analistler, araştırmacılar ve karşı istihbarat topluluğunda görevli operatörlerin eğitim ve öğretim seviyelerinin, genelde onlardan beklenen performansa eşit olmadığı ve beklentilerin altında kaldığı söylenir. Bu durumun karşı istihbaratın karmaşıklığından ve birçok disiplin ve becerinin bir ustalığını gerektirmesinden ileri geldiğini belirtmekte yarar vardır. Karşı istihbaratın beklentilere daha yüksek seviyede karşılık verebilmesi için, çok disiplinliliğin bir gereği olarak, eğitim mükemmeliyet merkezlerinin kurulması, eğitimde birliğin sağlanması ve seviyesinin yükseltilmesi gereklidir. Söz konusu eğitim merkezlerinin birincil ve öncelikli ihtiyacı ise gerekli eğitimleri verebilecek ve yeterli yeteneklere sahip eğiticilerdir. Öte yandan karşı istihbarat sisteminin ve dolayısıyla servisinin, çağın gereklerine uygun olarak gelişmelere uyum sağlayacak çalışmaları yapmakla görevli bir araştırma ve geliştirme birimine de ihtiyacı olacaktır.<sup>75</sup>

Pasif İKK önlemlerine sıraladıktan sonra en az pasif önlemler kadar önemli ve pasif önlemlerin bütünleyicisi olan aktif İKK önlemlerine geçebiliriz.

---

<sup>75</sup> Golovin, **a.g.e.**, s. 20.

### 2.3. AKTİF İKK ÖNLEMLERİ

Öncelikle, aktif karşı istihbarat dışında hiçbir karşı istihbarat enstrümanının, düşmanın istihbarat toplama yetenekleri ve hedeflerini öğrenmekten daha fazlasını bahsedemeyeceğini söylemek lazım gelir. Oysa İKK'da amaç sadece öğrenmek değildir. Aksine, öğrenmek henüz yolun başıdır ve bir şeyler yapılması gerektiğinin habercisidir.<sup>76</sup> Dolayısıyla karşı istihbaratın yalnızca pasif İKK önlemlerinden ibaret olduğunu söylemek ve bu önlemlerle yetinmek hata olur. İKK kapsamında koruyucu önlemlerin yanında aktif önlemlerin de alınması zorunludur. Çünkü güvenliğe yönelik düşmanca faaliyetlerden önce, bu niyetteki kişilere karşı, zararlı kişilerin deşifre edilmesi (açığa çıkarılması), faaliyetlerin etkisiz kılınması amacıyla bazı çalışmalar yapılması gerekir. Bu bağlamda aktif önlemler; düşman veya düşman olması olası tarafın casusluk, sabotaj ve yıkıcı faaliyetlerinin haber alınması yoluyla ortaya çıkarılması, zararsız hâle getirilmesi veya bertaraf edilmesi (çökertilmesi) için girişilen faaliyetleri kapsar.<sup>77</sup>

Aktif karşı istihbarat; casusluğa karşı koyma, keşfe karşı koyma, sabotajlara karşı koyma, yıkıcı ve bölücü unsurlara karşı koyma önlemleri ile gizleme ve aldatma faaliyetlerini içerebilir, İKK biriminin görevine ve yeteneklerine göre değişkenlik gösterir.<sup>78</sup>

Aktif karşı istihbaratta öncelikle bir tehdit veya düşmanca girişimin tespit edilmiş ve tanımlanmış olması gerekir. Aktif karşı istihbarat, devam eden veya tehdit oluşturan her türlü girişim veya tehdidi önleyebilmek için, rakiplerinin niyetleri, yetenekleri, bütçeleri ve kaynakları ile ilgili doğru ve güvenilir bilgiye gereksinim duyar.<sup>79</sup> Aktif önlemler arama, tespit, teşhis, belgeleme ve bertaraf etme gibi aşamalardan geçer ve saldırgan şekilde gerçekleşir.

Başta istihbari nitelikteki faaliyetler ve casusluk olmak üzere her türlü sabotaj, bölücü ve yıkıcı faaliyetler vb. aktif girişimlere karşı alınması gereken aktif önlemler genellikle kendisine özel olarak görev verilmiş ve bu konuda özel eğitilmiş kişi, grup veya kuruluşlarca yürütülmelidir. Yabancı unsurların istihbarat toplama faaliyetlerine karşı en iyi savunmanın saldırı olduğundan hareketle aktif önlemlerin amacının, söz

<sup>76</sup> Özdağ, *a.g.e.*, s. 170; Justin R. Harber, "Unconventional Spies: The Counterintelligence Threat from Non-State Actors", *International Journal of Intelligence and Counterintelligence*, Vol.: 22, Issue: 2, Washington D.C., 2009, 221–236, s. 228.

<sup>77</sup> Tezsever, *a.g.e.*, s.165.

<sup>78</sup> U.S. Marine Corps, *a.g.e.*, ss. 1-7–1-8.

<sup>79</sup> Douglas, *a.g.e.*, s. 85.

konusu eylemleri yapan kişileri, bu kişilerin kullandığı araç ve aygıtları belirlemek, önlemek ve ele geçirmekten ibaret olduğu söylenebilir.<sup>80</sup>

Bazı istihbaratçılar ve yazarlar aktif karşı istihbarat ile karşı casusluk arasındaki ilişkiyi tanımlarken, aktif karşı istihbaratın yabancı istihbarat servislerinin içinden eleman devşirmek gibi yöntemlerle yabancı servislere saldırı anlamı taşıdığını, karşı casusluğun ise yabancı servislerin benzer saldırılarını tespit, imha ve etkisizleştirme amacının ve görevinin olduğunu ifade etmektedirler.<sup>81</sup> Oysaki böyle bir ilişkilendirme çok yersiz ve kısmen de hatalıdır. Zira karşı casusluk, karşı istihbaratın aktif önlemlerinden veya yöntemlerinden sadece bir tanesidir. Aktif karşı istihbarat daha ziyade rakip istihbarat servislerinin bizimle ilgili istihbarat faaliyetlerinin ve niyetlerinin verebileceği zararları en aza indirmek veya tamamen etkisizleştirebilmek için çalışır.

Aktif karşı istihbarat, İNİS, SİNİS ve GÖRİS gibi birçok istihbarat disiplininin bir arada bulunacağı çok disiplinli bir istihbarat toplama çabasıyla mücadele edebilecek nitelik ve yetenekte tasarlanmalıdır.<sup>82</sup> ABD Savunma Bakanı eski Yardımcısı John Hamre'in de ifade ettiği gibi aktif İKK faaliyetlerinde hedef önceliği, ülkeye giren casusları tespit edip yakalamak değil, onları daha ülkeye giriş yapmaya çalıştıkları ilk noktada tespit edip durdurmak olmalıdır.<sup>83</sup> Saldırgan bir İKK stratejisinin başarıyla yürütülebilmesi ancak hedefin yurt dışından çalışılmaya başlanması ile mümkündür. Bu, "önleyici karşı istihbarat yaklaşımı" olarak da adlandırılabilir. Önleyici karşı istihbarat yaklaşımı, tehditleri fırsata dönüştürebilecek, oldukça yüksek seviyede yaratıcılık gerektirir.

Oturup yıllarca bekleyerek iş işten geçtikten sonra tespit edilen casusluk vb. faaliyetlerin ardından, tekrarlanmamaları için neler yapılması gerektiğini tartışmak çok da istenen bir durum değildir. Ulu önder Mustafa Kemal Atatürk'ün de ifade ettiği gibi "Felaket başa gelmeden önce önleyici ve koruyucu önlemleri düşünmek ve almak gerekir. Felaket başa geldikten sonra dövünmenin faydası yoktur." Bunun yerine taarruzî düşünen bir karşı istihbarat sistemi oluşturulmalı ve sürekli olarak yabancı istihbarat servislerinin nasıl faaliyet gösterdikleri, hassasiyetlerinin ve zayıf yönlerinin neler olduğu, nasıl yanlış yönlendirilebilecekleri, düzenleyebilecekleri

<sup>80</sup> Acar ve Urhal, **a.g.e.**, s. 303.

<sup>81</sup> Özdağ, **a.g.e.**, s. 163.

<sup>82</sup> Abram N. Shulsky ve Gary J. Schmitt, **Silent Warfare: Understanding the World of Intelligence**, Brassey's Inc., Washington, 1993, s. 99.

<sup>83</sup> Van Cleave, "Strategic... **a.g.e.**, s. 5.

operasyonlarla ilgili olarak uyarıcı nitelikteki ipuçlarının ve emarelerin neler olabileceği, her iki taraf için üstünlük sağlayabilecek tuzaklar oluşturma olanağının olup olmadığı, rakibin karar alıcılarını etkilemek ya da istenilen kararları almalarını sağlamak için uygun yolların ve fırsatların bulunup bulunmadığı gibi soruların cevapları aranmalıdır.<sup>84</sup>

Karşı istihbarat, genel anlamda tüm kurum ve kuruluşların görev ve sorumluluğu iken, örtülü ve gizli İKK operasyonları yani aktif karşı istihbarat, çok özel bir görevli grubun yetki ve sorumluluğu içindedir.<sup>85</sup> İstihbarat faaliyetlerinde olduğu gibi İKK faaliyetlerinde de gizlilik ve uzmanlık çok önemlidir. Bu nedenle gizli yöntemleri kullanabilecek yetenekte ve eğitilmiş kişilerden oluşturulan operasyonel birimler vardır. Aslında operasyonel İKK için oluşturulacak bu profesyonel birimler, istihbarat birimlerinin tüm yeteneklerine sahip olmalı hatta onlardan daha üstün yetenekleri bulunmalıdır. Böylece operasyonların gizliliğini ve güvenliğini tehlikeye düşürebilecek hatalar ortadan kaldırılabilir.<sup>86</sup>

Düşmana kendi istihbarat operasyonlarını kullanarak karşılık vermek veya durdurmak yaratıcı İKK operasyonları için harika bir örnektir.<sup>87</sup> Buna paralel olarak çoğu devletin, örtülü operasyon yapma görevini sadece dış istihbarat servisine verdiği de söylenebilir.<sup>88</sup> Gizli ve örtülü operasyonlar, yabancı devletlerin politik, askerî veya ekonomik şartlarının, operasyonları yapan devlete atfedilemeyecek biçimde etkilenmesini veya bozulmasını yani operasyonları yapan devletin dış politikasını destekleme amacını güder. Operasyonları yürüten servis çoğu zaman kendi kamuoyundan dahi bu faaliyetleri gizlemek ve ortaya çıkması durumunda da inkâr etmek zorunda kalır.<sup>89</sup> Çünkü devletlerin birbirlerine karşı icra ettikleri bu operasyonların çoğunluğu, yasa dışı olarak icra edilir ve henüz benimsenmiş ya da belirlenmiş bir uluslararası istihbarat veya İKK hukuku söz konusu değildir.

Ayrıca, içinde bulundukları bir faaliyet nedeniyle yakalanan ve casusluk suçuyla yargılanan kişiler, hizmet ettikleri ülkeler tarafından destek görmek bir yana yalnız bırakılırlar ve halen birçok ülkede, idama varan ağır cezalarla cezalandırılırlar.

<sup>84</sup> Van Cleave, *Counterintelligence... a.g.e.*, s. 14.

<sup>85</sup> Acar ve Urhal, *a.g.e.*, ss. 301–302.

<sup>86</sup> Köseli, *a.g.e.*, s. 34.

<sup>87</sup> Van Cleave, *Counterintelligence... a.g.e.*, s. 9.

<sup>88</sup> Nurullah Aydın, *İşte İstihbarat*, Kum Saati Yayınları, İstanbul, 2011, s. 664.

<sup>89</sup> Sait Yılmaz, “Kriz Yönetimi ve Güç Kullanımı”, *Kara Harp Okulu Savunma Bilimleri Enstitüsü Savunma Bilimleri Dergisi*, Cilt: 7, Sayı: 1, Ankara, 2008, 145–169, s. 151.

### 2.3.1. Karşı Casusluk / Casusluğa Karşı Koyma

Karşı casusluk konusunun daha iyi anlaşılması bakımından, casusluk kavramıyla ilgili bazı temel bilgilere değinmek yararlı olacaktır. Zira etkili ve doğru önlemleri alabilmenin ön koşulu düşmanını tanımaktır.

#### 2.3.1.1. Casusluk

İstihbarat, 1850'li yıllardan Birinci Dünya Savaşı'na kadar ağırlıklı olarak, çeşitli ve binlerce yıldan beri bilinen ve kullanılan klasik (kökleşik) yöntemlerle icra edilen casusluğa dayandırılmıştır. Dönemine göre, keşfedilen her yeni alet, teknik ve yöntem casusluk açısından ciddi gelişmeler sayılmıştır. Napolyon casusluğun önemini, "İnanın bana, savaşların sonuçları incelendiğinde topçunun, süvarinin, piyadenin kahramanlıkları, casusların şu göze görünmez, lanetli ordusu yanında hiç kalır!" sözüyle vurgularken, Prusya Kralı Büyük Frederik, Fransız Mareşal Charles Soubise'yi Rossbach'da mağlup ettiğinde şunları söylemiştir: "O zat, savaşa gittiğinde yanında yüzlerce aşçı götürür. Bense önceden yüzlerce casus gönderirim."<sup>90</sup>

Sun Tzu'nun da ifade ettiği gibi, "doğal üstün zekâya sahip olmayan hiç kimse casus olamaz."<sup>91</sup> Olursa da sonucun başarısızlık ve hüsrana olması kaçınılmazdır. Bu denli tercih edilmesine rağmen casusluk en zor ve riskli istihbarat toplama yöntemlerinden birisidir. Ayrıca casusların belirlenmesi, devşirilmesi ve güvenilirliklerinin denetlenmesinden oluşan elemanlanma süreci zaman alıcıdır. Casusların, onları kontrol eden istihbaratçılarla aralarındaki ilişki ve iletişim sınırlıdır, karmaşıktır ve her an ortaya çıkma riski vardır. Bilgi akışı genellikle yavaştır. Casuslardan alınan her türlü bilgi (özellikle gözlem ve yoruma dayalı olanlar) her türlü insana özgü yanılığa açıktır. Casusların tam anlamıyla kontrolü de zordur ve iki taraflı olup olmadıkları hiçbir zaman tam olarak bilinemez.<sup>92</sup>

Casusluk, özünde bir hırsızlık faaliyetidir. Diğer organizasyonların yasalarını ihlal ederek bilgilerin aşırılması anlamına gelir. Eğer, bilgisi alınan organizasyonun herhangi yasal bir düzenlemesi yoksa o zaman casusluktan söz edilmez. Çünkü çalmayı gerektirecek bir durum oluşmamış demektir. Zira gizli ve korunan bir

<sup>90</sup> Ergun Hiçyılmaz, *Belgelerle Teşkilat-ı Mahsusa ve Casusluk Örgütleri*, Ünsal Kitabevi, İstanbul 1979, s. 2.

<sup>91</sup> Sun Tzu, *Savaş Sanatı*, Çev.: İbrahim Şener, Mitra Yayınları, İstanbul, 2011, s. 69.

<sup>92</sup> Özdağ, *a.g.e.*, s. 50 ve 129.

bilginin, özel teknik ve yöntemler konusunda eğitimli ajanlar tarafından çalınması söz konusu olmasa, yapılan faaliyetin bir gazetecilik faaliyetinden farklı olduğu da söylenemez.<sup>93</sup>

Bütün bu zorluklara ve yüksek riske rağmen casusluk, günümüz de dâhil olmak üzere hiçbir zaman cazibesini ve tercih edilirliliğini kaybetmemiştir. Bunun da en önemli sebebi, her şeye rağmen en etkili ve kesin sonuç aldırıcı yöntem olma özelliğini korumasıdır. Casusluk amaca ulaşabilmek için her yolu mübah kabul eden fütursuz ve acımasız bir ufka sahiptir. Yani “gaye vasıtayı meşru kılar”<sup>\*</sup> mantığı, casusluğun en önemli düsturlarından birisidir.<sup>94</sup>

Öte yandan hemen hemen bütün devletler tarafından kullanılan bir enstrüman olan ve hiçbir yasal dayanağı olmadan icra edilen casusluk, yine bütün devletlerin yasalarında suç olarak (tabi yakalanırsa) tanımlanmış ve ağır cezalar belirlenmiştir. Ülkemizde de, 2004 yılında çıkarılan 5237 kanun numaralı Türk Ceza Kanunu (TCK)’nın yedinci bölümünde, 326–339’uncu maddeler arasında, devlet sırlarına karşı suçlar ve casusluk başlığı altında, casusluk suçları ele alınmış ve cezaları belirlenmiştir.

TCK’ye göre, devletin güvenliğine veya iç veya dış siyasal yararlarına ilişkin belge veya vesikaları kısmen veya tamamen yok eden, tahrip eden, bunlar üzerinde sahtecilik yapan, başka yerlerde ve başka maksatlarla kullanan, hileyle alan veya çalan; gizli kalması gereken bilgileri temin eden, açıklayan, üzerinde bulunduran; devletin yararı gereği girilmesi yasaklanan yerlere gizlice ve hileyle giren; bunların her çeşidine yardım ve yataklık eden, göz yuman, gördüğü halde haber vermeyenlere çeşitli sürelerde hapis cezaları belirlenmiştir.

Ayrıca söz konusu faaliyetleri bilmeden veya istemeden de olsa yapanlarla ilgili de taksir ile meydana gelen sonuçlar nedeniyle, bilinçli kişilere oranla daha az hapis cezaları öngörülmektedir. Yani gafil muhbirlik sonucu verilecek bir bilgi, TCK’nin ilgili maddeleri kapsamında değerlendirilebilecek bir bilgi ise cezasının olduğu unutulmamalıdır.

---

<sup>93</sup> Johnson, **a.g.e.**, s. 2.

<sup>\*</sup> Makyavel felsefesi.

<sup>94</sup> Tezsever, **a.g.e.**, s. 166.

### 2.3.1.1.1. Casus Türleri

Casus türlerine geçmeden önce, genelde birbiriyle eş anlamlı olarak kullanılan casus ve ajan sözcüklerinin ayrımını yapmakta yarar vardır. Casus, kendi sistematüğinde, çoğunlukla kendinden bir ast ve bir üst unsur dışında kimseyi tanımayan, kendisini de kimsenin tanımadığı ve her yönüyle gizli kişidir. Casuslar –bazen çocukluklarından itibaren– uzun soluklu görevler için hazırlanan, çok yönlü ve donanımlı, istihbarat ve karşı istihbarat tekniklerinin neredeyse tamamını çok iyi bilen ve uygulayan, sadece bilgi toplamakla yetinmeyip istihbarat çözümlemeleri de yaparak operasyon düzenleyebilecek yetenek ve kapasite sahibi kişilerdir.<sup>95</sup>

Ajanlar (istihbaratçılar) ise, istihbarat ve karşı istihbarat servislerinin çalışanlarını ifade eder. İstihbaratçılar da gizli işlerle uğraşmalarına rağmen –örneğin istihbarat analistleri– yaptıkları işi genel anlamda herkes bilir ve gizlenmek zorunda değildirler.

Bu bağlamda DİHMİT Kanunu’nda “MİT personeli” ve “MİT mensubu” şeklinde iki ayrı görev tanımı bulunmasının temel sebebi de muhtemelen budur. Örneğin, MİT’in başkanı olan kişiyi herkes tanırken ve yaptığı gizli faaliyetlere rağmen gizlenmesi için çaba harcamasına gerek yokken, yine MİT’te görev yapan herhangi bir bölge sorumlusu özel ajanın kendisini (dolayısıyla görevini) ailesinden dahi gizlemesi gerekir.

Casuslar, birçok yazar ve istihbaratçı tarafından farklı şekillerde sınıflandırılmaktadır. Örneğin Sun Tzu casusları; yöresel casuslar, iç casuslar, devşirme casuslar, hükümlü casuslar ve hayatta kalan casuslar olmak üzere beş gruba ayırmıştır.<sup>96</sup> Şu an tüm casus türlerini kapsamayan bu sınıflandırma, dönemine göre oldukça başarılı ve üst düzey bir ayırım olarak nitelendirilebilir.

Günümüzde casus türlerinin, yapılmış farklı sınıflandırmaları vardır. Casus, ajan ve istihbaratçı kavramları konusunda hâlen ciddi bir karışıklık olduğundan hareketle bu hususa fazla takılmadan, ayrıntılı açıklamalarına girilmeden ve herhangi bir sınıflandırma yapılmadan bilinen casus / ajan çeşitleri ele alınacaktır. İncelenen kaynaklarda, ajan ve casus kavramlarının ayrımı yapılmasına rağmen, sınıflandırmalar genellikle “ajan çeşitleri” olarak yapılmıştır. Oysa sayılan ajan

<sup>95</sup> Ömer Urhal, *Küreselleşen Dünyada Güvenlik*, Adalet Yayınevi, Ankara, 2009, s. 508.

<sup>96</sup> Tzu, *a.g.e.*, s. 68.

çeşitlerinin bir kısmı, yapılan ajan–casus ayrımına göre düşünüldüğünde casus türüdür. Bu bağlamda casus türleri şöyle sıralanabilir:<sup>97</sup>

– **Profesyonel Casus:** Yaptığı işten para kazanan casuslardır. Casusluğu kendilerine meslek edinen ve başka bir iş yapmayan kişilerdir.

– **Hizmet (Resmî) Ajani:** Büyükelçilik, konsolosluk gibi yerlerde, mensubu oldukları ülke adına görev yapan ve bulundukları ülkenin resmî izni ile orada bulunan kişilerdir. Bu kişilerin kimlikleri gizli değildir. Yaptıkları faaliyetler de (genelde) açıktır. Devletler hukukuna göre dokunulmazlıkları vardır. Açık istihbarat toplamalarına da hiçbir engel yoktur.

– **Sızma (Hulul) Casusu:** Herhangi bir organizasyona, o organizasyon ile ilgili bilgi temin etmek üzere sızdırılan kişilerdir. Dışarıdan özellikle bu görev için organizasyona sokulurlar ve işleri bitince ayrılırlar.

– **Devşirme Casus:** Herhangi bir organizasyon mensubunun, çeşitli yöntemlerle, istenilen bilgileri vermeye ikna edilmesi sayesinde edinilen casuslardır.

– **Çift Taraflı (Duble / İkili) Casuslar:** Bir ülkenin istihbarat örgütü adına çalışırken, özellikle açığa çıktıktan sonra, mensubu olduğu ülke ve servis aleyhinde kullanılmaya başlayan casuslardır. En güvenilmez ve sıkı kontrol gerektiren casus türüdür. Bu casus türüne örnek olarak, Kurtuluş Savaşı'nı takip eden yıllarda, İtalyanlar tarafından General Hüseyin Hüsnü Kalkış'a, komutanı olduğu birliğin planlarını bir milyon liraya satmasının teklif edilmesi gösterilebilir. Kalkış, durumu Atatürk'e bildirmiş ve Atatürk'ün talimatıyla birliğin eski planlarını iki milyon liraya İtalyanlara satmıştır.

– **Gönüllü (Kendi Gelen) Casus:** Ellerindeki bilgilerle ilgileneceğini düşündükleri yabancı istihbarat servislerine kendiliklerinden başvuran casuslardır. Bunların, ellerindeki bilgileri vermelerinin çeşitli nedenleri olabilir. Kendi gelenlere genelde güvenilmez. Çünkü ellerindeki bilgileri genelde olduğundan abartılı şekilde servis ederler ve asıl amaçları çoğunlukla casusluk oyununun heyecanını yaşayabilmektir. Asıl önemli olan husus ise kendi gelenlerin, bilerek ya da

<sup>97</sup> Urhal, *a.g.e.*, s. 509; Tezsever, *a.g.e.*, s. 171; Avcı, *İstihbarat Oyunları... a.g.e.*, ss. 110–113; Acar ve Urhal, *a.g.e.*, s. 297; Özdağ, *a.g.e.*, ss. 164–165; Robert Wallace ve H. Keith Melton, *CIA Kendini Anlatıyor: Casusluk*, Çev.: Algan Sezgintüredi, NTV Yayınları, İstanbul, 2010, s. 363.

bilmeyerek bir istihbarat servisinin “yemi” olabilme olasılıklarının yüksekliđidir.

– **İlticacı Casus:** Bir servis adına alıřırken, mensubu olduđu lkeyi ve servisi terk ederek bařka bir lkeye ve servise hizmet etmeye ikna edilen casuslardır.

– **Uyuyan Casus:** Gnderildikleri lkede, uzun sre (bazen yıllarca) hibir faaliyet gstermeyen ve sıradan, her trl olay ve kargařadan uzak ve dikkat ekmeyen bir hayat sren casuslardır. Bu casuslar gnlk yařantılarını srdrrken kendilerine grev verilecek gn beklerler.

Ayrıca, tek ajan, kitle hlinde grev yapan ajanları, provokasyon (kışkırtma) ajanları, bař ajan, destek ajanı ve tutuklu ajan gibi casus trlerinden de bahsedilmektedir.

te yandan sayılan ajan / casus eřitleri tamamen apayrı eřitler deđildir. rneđin; tařıdıđı zelliklere gre devřirme casus olarak nitelendirilen bir casus, aynı zamanda profesyonel casus ve uyuyan casus tanımlarına da uyabilir.

#### **2.3.1.1.2. Casusluđa Kılıf Teřkil Eden Meslekler:**

Casusluđun her trl yntem ve uygulamayı meřru kabul ettiđi ve sınır kabul etmediđi dřnldđnde, belirli mesleklerle sınırlandırılması dođru olmayabilir ancak bazı mesleklerin, casusluk iin dođal birer maske oluřturdukları da yadsınamaz. Dolayısıyla da tarih boyunca casusluđa en ok kılıf teřkil eden meslekler gibi istatistiksel bir sonu ortaya ıkmıřtır.

Casuslar tarafından bir mesleđin tercih edilmesindeki en nemli sebeplerden birisi ve belki de en nde geleni, meslek mensubunun mesleđi sayesinde herhangi bir yabancı lkede rahatlıkla dolařabilmesine olanak tanımasıdır. Diđer nemli bir sebep de mesleđin, yabancı lkedeki birok kiřiyle temasta bulunabilme ve grřebilme fırsatı sunmasıdır.

Bu sonu kuřkusuz sz konusu mesleklerin tm mensuplarını zan altında bırakmaz ama ncelikli olarak kontrol ve takip edilmelerine de engel olmaz. İstihbarat alıřmalarında, maske grevleri olarak; diplomatlık, gazetecilik, arkeologluk, sađlıkılık, iř adamlıđı vb. meslek grupları ile misyonerlik veya hayır

işlerinin kullanıldığına sıkça rastlanmaktadır. Casusların kılıf olarak çoğunlukla kullandıkları meslekler ve faaliyet alanları şunlardır:<sup>98</sup>

– **Diplomatlık:** İşin doğası gereği ezelden beri neredeyse her diplomata casus gözüyle bakılır. Her diplomat bildiğimiz anlamda casusluk faaliyeti içerisinde olmasa da devleti temsil ettiği için “potansiyel casus” olarak değerlendirilir. Sonuçta yapılan bu değerlendirme haksız değildir. Çünkü her diplomat doğal olarak bulunduğu ülkeye ilişkin bilgi toplar ve çeşitli ilişkiler kurar. Casusluk tarihinde, “istenmeyen adam”<sup>\*</sup> ilan edilerek sınır dışı edilen ya da bazı ülkelerde daha ağır şekillerde cezalara çarptırılan diplomatlara rastlamak mümkündür. Eski Türk Devletlerinin, Çinli ve Bizanslı elçilerin bu tür faaliyetleri ile sıkça karşılaştıkları ve tespit edilenlerin ya hapse atıldığı ya da ülkenin uzak diyarlarında ikamet etmeye mecbur edildikleri bilinmektedir.<sup>99</sup> Örneğin, 1960’lı yıllarda, Sovyet Sosyalist Cumhuriyetler Birliği (SSCB)’nin Türkiye Ticaret Ataşeliği’nde görevli bir diplomat olan Rus ajanı Jouri Maximov, angaje ederek istihbarat elde etmek için kullandığı Kegam Levon Pulli’nin yakalanması ve casusluk suçundan hüküm giymesinin ardından istenmeyen adam ilan edilerek sınır dışı edilmiştir.<sup>100</sup>

– **Gazetecilik:** En çok kullanılan kılıf mesleklerin başında gelir. Görevi gereği haber toplamaya ve bu sayede casusluk için en uygun mesleklerden biridir. Dünyanın en önemli istihbarat servisleri casus gazetecileri çokça kullanır. Gazeteciler, haber bahanesi ile rahatlıkla her ortama girebilir, her makamdan kişilere sorular sorabilir ve geniş kitlelere ulaşabilirler. Örneğin, casusluk tarihinin önemli isimlerinden Kim Philby’nin ve Richard Sorge’un maske meslekleri gazeteciliktir.

– **Arkeologluk:** Özellikle İngiliz istihbaratı tarafından 19’uncu yüzyılın sonu ve 20’nci yüzyılın başında arkeologluk, casusların en çok kullandığı maske meslek olmuştur. En bilindik örneklerden birisi Thomas Edward Lawrence (namıdiğer Arabistanlı Lawrence)’dır. Sadece Lawrence değil, Anadolu topraklarında faaliyet gösteren ve tarihe geçmiş başka casuslar da vardır. Gertrude Bell, Michael Buch, Wooly, D. Hogarth, Sykes ve Delbrueck Herzfeld gibi ünlü casuslar da Anadolu coğrafyasında arkeolog olarak çalışmalar yapmış ve bu çalışmalarını bağlı bulundukları servislere sunmuşlardır. Sadece bilgi toplayıp sunmakla da

<sup>98</sup> Atilla Akar, *Casuslar Derin Savaşın Sıradışı Neferleri*, Timaş Yayınları, İstanbul, 2005, s. 28.

<sup>\*</sup> İstenmeyen Adam / Persona Non Grata: Viyana Konvansiyonuna göre, ev sahibi konumundaki bir devlet, ülkesinde görevli olarak bulunan bir yabancı diplomatik görevliyi, casusluk gibi makul sebeplere dayanarak istenmeyen adam ilan edebilir ve ülkesine dönmesini isteyebilir.

<sup>99</sup> İlhan Bahar, *Teşkilat-ı Mahsusa’dan MİT’e*, Kum Saati Yayınları, İstanbul, 2009, s. 41.

<sup>100</sup> Ercan Çitiloğlu, *Gölgedeki Sessiz Tanıklar*, Doğan Kitap, İstanbul, 2007, ss. 1–75.

yetinmemişler, çalışma yaptıkları bölgelerdeki halkı etnik ve kimlik yönünden hareketlendirmeyi de başarmışlardır. Arkeolog unvanlı casusların büyük bir kısmının arkeoloji ile çok az bir ilgisi ve bilgisi bulunduğu, kazı çalışmaları ile pek ilgilenmeyip çoğunlukla gezerek halkla konuştukları (çoğunun başta yerli halkın konuştuğu dil olmak üzere çok sayıda dili konuşabildikleri bilinmektedir), resim ve video çektikleri de gerçek arkeologlar tarafından belirtilmektedir.<sup>101</sup>

– **Doktorluk, Sağlık Görevliliği ve Hemşirelik:** Özellikle 1’inci Dünya Savaşı esnasında doktorlar, sağlık görevlileri ve hemşireler casusluk faaliyetlerinde yoğun olarak kullanılmışlardır. Bunlar en çok cephede düşmanın verdiği kayıplar, ordunun tıbbi ve psikolojik durumu ve benzeri konularda bilgi aktarmışlardır. Meslek olarak değerlendirilemese bile “hasta” maskesi de bu amaçla kullanılabilir. Yıllar önce, lösemi hastası olduğu gerekçesiyle kan bağışı kampanyası başlatan ve toplanan binlerce kan örneğini ABD’ye götüren bir kişinin, doğruluğu ispatlanamasa da, Türklerin gen haritasını çıkarmak maksadıyla ABD tarafından kullanılan bir casus olduğu öne sürülmüştür.

– **Araştırmacılık / Sosyologluk:** Casusluğa uygun bir diğer meslek de sosyolojik araştırmacılıktır. Bunlar, anket, istatistik ve toplumsal araştırma adı altında hedef ülkeye ilişkin bir takım verileri kolaylıkla toplayabilirler. En önemli örneklerden birisi, yirminci yüzyılın ilk çeyreğinde Irak’ta İngiliz gizli servisi adına çalışan bir kadın casus olan ve Irak’ın İngilizler tarafından işgalinde önemli rol oynayan araştırmacı yazar Gertrude Bell’dir.<sup>102</sup>

– **Misyonerlik / Din Görevliliği:** Casusluk faaliyetlerinin en aleni olarak yürütüldüğü meslek ya da görevdir. Casusluk tarihinin bilinen ilk örnekleri genelde din adamlarıdır. Özellikle milattan önceki dönemde Çinli ve milattan sonra da Hristiyan din adamları hep bu tip faaliyetlerin içinde olmuşlardır. Bu gezginci din adamlarının görevleri, bir yandan hedefledikleri –ki hedefte genelde Türkler olmuştur– toplumlara kendi inançlarını benimsetmek, o ülkenin geleneksel, kültürel ve dinî yapısını parçalamak iken diğer yandan toplumun genel yapısı, genel güvenlik konuları ve ülkeyle ilgili her türlü bilgiyi kendi ülkelerine götürmek olmuştur.<sup>103</sup> Kurtuluş Savaşı yıllarında, Anadolu’da misyonerlik faaliyetlerinde bulunan ve ülke içinde kargaşa çıkarmak için isyancı ve casusları yönlendiren “Rahip Fru” lakaplı

<sup>101</sup> Haşım Söylemez, **Casus Arkeologlar**, 07 Ekim 2000, <http://www.aksiyon.com.tr/aksiyon/haber-6809-casus-arkeologlar.html> (Erişim tarihi: 29 Kasım 2012).

<sup>102</sup> Avcı, **İstihbarat Oyunları... a.g.e.**, s. 277.

<sup>103</sup> Bahar, **a.g.e.**, s. 43.

İngiliz casusu Robert Frew en bilinen örneklerdendir.

– **Turistler:** Casusluk tarihinde birçok ülke, ajanlarını yabancı ülkelere turist maskesi altında yollamıştır. Turist oldukları için fotoğraf çekmeleri ya da değişik yerleri gezmeleri hiç kimse tarafından yadırganmaz. Japonların ülke politikası gereği yılda en az iki defa yabancı ülkelere gitmelerinin ve fotoğraf çekmelerinin zorunlu olduğu, kanıtlanmış bir gerçeklik olmasa da, bir komplo teorisi olarak vardır. Böyle bir olasılığın her zaman bulunduğu gerçeği, turistlerin casusluk açısından önemini ortaya koymaktadır. Öte yandan Ocak 2013'te, ülkesinden ilk defa çıkarak Türkiye'ye fotoğraf çekmek maksadıyla (!) gelen ABD vatandaşı Sarai Sierra isimli kadın turistin, gizemli bir şekilde önce kaybolması, sonra da ölü bulunması bu bölümde verilebilecek iyi bir örnektir. Son bir örnek de Kuzey Kıbrıs Türk Cumhuriyeti'nin kurucu Cumhurbaşkanı Rauf Denktaş'tır. Denktaş'ın bilinen fotoğrafçılık hobisi, hobiden biraz ötesini de ifade edebilir. Çünkü önemli basın toplantılarından önce, toplantıya katılan basın mensuplarının fotoğraflarını çekerek daha sonra incelemek ve bazı sonuçlar çıkarmaya çalışmak, bize göre hobiden fazlasını işaret eder niteliktedir.

– **Öğrenciler veya Öğretim Görevlileri:** Geçmişte çok sık karşılaşılmamış (belki sadece açığa çıkarılamadıkları için) olmakla birlikte günümüzde en rahat kullanılacak kılıf mesleklerden biri de öğrencilik veya öğretmenliktir. Çeşitli sebeplerle yurt dışında öğrenim gören öğrenci sayısı eskiye nazaran oldukça fazladır. Genç yaştaki insanlardan casusluk gibi önemli altyapı gerektiren bir görevin beklenemeyeceği gibi yanlış bir inancın bulunması da kılıf meslek olarak öğrenciliğin cazibesini artırmaktadır. Türkiye'de öğrenim gördüğü dönemde angaje edilen ve casusluk yaptığı için yakalanan Necdet Mualla isimli Suriyeli genç bu kapsamdaki örneklerden biridir.<sup>104</sup> ABD Merkezî İstihbarat Örgütü (CIA)'nın, ABD'deki her üniversitede anlaşmalı öğretim üyeleri bulunduğu ve üniversitelerdeki yabancılardan ulaşılmak istenen kişilerle önce bunların irtibat kurduğu, yabancı bilim insanlarının ABD'deki üniversitelerde kalıcı pozisyon bulma şansları olmamasına rağmen kalıcı pozisyon bulmalarına yardımcı olduğuna ilişkin savlar vardır.<sup>105</sup> Bu savları destekler ve farklı bir boyutunu ortaya koyar nitelikteki bir olay da birkaç yıl önce Türkiye'de yaşanmıştır. Bir Türk gazetecinin, İngilizce öğretmeni sıfatıyla üniversitelere gelen bazı ABD'li öğretim görevlilerinin ajan olduklarını öne sürmesi üzerine, öğretim

<sup>104</sup> Çitlioğlu, *a.g.e.*, ss. 77–101.

<sup>105</sup> Nurullah Aydın, "Ajan Akademisyen ve Yazarlar", *Erciyes*, 08 Ekim 2012, <http://www.erciyesgazetesi.com.tr/yazar.asp?yaziID=2614> (Erişim tarihi: 18 Nisan 2013).

görevlileri bu durumdan rahatsız olarak ülkeyi terk etmişlerdir.<sup>106</sup>

– **Sivil Toplum Örgütleri ve İnsani Yardım Kuruluşları:** Son yıllarda artan bu kurumlar ve dolayısıyla çalışanları, geniş kitlelere ve bölgelere, kimsenin şüphesini çekmeden rahatlıkla ulaşabilmektedirler. Doğrudan haber alma faaliyetleri yürüttükleri gibi o ülkenin kamuoyunu yönlendirme konusunda da etkili olabilmektedirler. Barış gönüllülüğünden acil yardım kuruluşlarına ve sağlık birimlerine kadar geniş bir yelpazede faaliyet göstermektedirler. Özellikle insanların ve ülkelerin en çok yardıma muhtaç oldukları doğal afet ve büyük felaket zamanlarında, yardım kuruluşlarının arasına karışan casuslar, istihbarat savaşlarının en acımasız yüzünü gösterirler ve insanların çaresizliklerini sömürürler.

#### **2.3.1.1.3. İnsanları Casus Olmaya Yönelten Nedenler**

İnsanları, isteyerek ya da zorla casusluğa ve bilgi veren olmaya iten nedenler, insan doğasının kendisi kadar karmaşık ve çeşitlidir. İstihbarat ajanları, elde etmek istedikleri bilgileri her zaman kendi başlarına edinmeye çalışmazlar. Ateşi elle tutmak yerine maşayla tutmayı tercih ederler. Daha kolay ve daha güvenli bir yöntem olan “elemanlanma” yöntemine sıkça başvururlar. Elemanlanma, özel yetenekli ve eğitilmiş ajanların uygulayabileceği, karmaşık ve zor bir yöntemdir. Zorluğunun en büyük nedeni, insanların öngörülemez bireysel farklılıklarıdır. Bilgi veren (yani casus, muhbir vb.) olmak üzere seçilen bir hedefin, bu göreve isteyerek veya istemeyerek alınabilmesi için, kişinin her türlü özelliğinin çok iyi bilinmesi, egemen motif(ler)inin\* tespit edilmesi ve kötüye kullanılması gerekir.

Motif, bilgi kaynağının toplayıcılar ile görüşmesini ve bilgiyi vermesini sağlayan neden veya nedenler olarak tanımlanabilir. Bilgi kaynağını toplayıcı ile görüşmeye iten bir takım güdüler vardır. Bunların bilinmesi toplayıcının haber kaynağı teminini kolaylaştırır. Bilgi verenin, vereceği bilgi karşılığındaki beklentisi veya bilgiyi vermedeki amacına da motif denebilir. Haber kaynağının tek bir motifi olmak zorunda değildir. Bazen birden fazla motifi olan kaynaklarla karşılaşılabilir. Bazen de başlangıçta farklı bir motifle başlayan bilgi verme süreci sonradan bambaşka bir motif karşılığına dönüşebilir.

Casusların ve bilgi verenlerin motifleri çoğu zaman kendiliğinden mevcuttur

<sup>106</sup> **Vatan**, “ABD’li Akademisyenler Ajan İddiası Üzerine Şehri Terk Etti!”, <http://haber.gazetevatan.com/Haber/351250/1/Gundem> (Erişim tarihi: 18 Nisan 2013).

\* Motif sözcüğünün öz Türkçe karşılığı “itki” olmasına karşın istihbarat söz dağarcığında yerleşmiş bir sözcük olmasından dolayı motif sözcüğü kullanılmaya devam edecektir.

ancak bazı durumlarda elemanlanma işiyle görevli istihbaratçılar bu motiflerin oluşması için birtakım çalışmalar yaparlar. Motiflerle ilgili temel sınıflandırma, “MICE”dir. Para (Money), ideoloji (Ideology), baskı (Coercion) ve ego (Ego) sözcüklerinin İngilizcilerinin baş harflerinden oluşan MICE,<sup>107</sup> en önemli sayılabilecek motifleri kapsamakla birlikte, içermediği motifler de bulunmaktadır. Genel olarak motifleri; maddi motifler, duygusal motifler ve ideolojik motifler olmak üzere üç ana başlık altında toplamak mümkündür.

#### 2.3.1.1.3.1. Maddi Motifler

**Para:** İlk bakışta en etkili motif gibi görünmekle birlikte genelde en son tercih edilen motiftir. Parayı motif olarak seçen bilgi kaynakları (casus, muhbir vb.), işi ticarete döktükleri için kontrol edilmeleri daha zordur. Aynı bilgiyi birden fazla yere satmış olabilecekleri gibi, verdikleri bilginin, aldıkları paraya göre kendi belirledikleri kadarını verme eğiliminde de olabilirler. Bazı yazarlar, parayı, “maddi servete büyük toplumsal önem veren ülkelerin vatandaşları için çekici”<sup>108</sup> olarak nitelendirse de, paranın motif olabileceği kitleyi bu şekilde daraltmak mümkün değildir. Refah seviyesi çok yüksek olan ve paraya hiç değer vermeyen kişiler ve toplumlar bile bu motif kullanılarak elde edilebilirler. Otuz altın karşılığında İsa peygambere ihanet eden Judus, tarihte para motifinin görüldüğü ilk bilgi verenlerdendir.<sup>109</sup> Öte yandan, son yıllarda kredi ve kredi kartı borçlularının sayısının artması, casus arama sorununu oldukça azaltmıştır.<sup>110</sup>

– **Vatandaşlık Bilinci:** Bu motif, casusluk için çok geçerli bir motif olarak sayılamaz ancak genel bilgi veren motifleri arasında yer alır. Özellikle, 4’üncü bölümde açıklanacak olan muhbirler arasında verdiği bilgiye en çok güvenilen kişilerdir. Zira menfaat sayılabilecek hiçbir beklenti olmaksızın yapılmaktadır.

– **Rahat Yaşam Şartlarına Kavuşma Hevesi:** Bu motif, mevcut yaşantısından memnun olmayıp daha iyi şartlarda bir yaşantı sürmek isteyen kişilerin itkisidir. Yine özellikle muhbirler için daha geçerli görünen, hapisten çıkmak, cezalarını azaltmak veya hapis yaşantısını rahatlatmak isteyen bilgi verenlerin motifi

<sup>107</sup> Wallace ve Melton, *a.g.e.*, s. 362.

<sup>108</sup> *a.g.e.*, s. 363.

<sup>109</sup> Dennis G. Fitzgerald, *Informants and Undercover Investigations: A Practical Guide to Law, Policy, and Procedure*, CRC Press, 2007, s. 21.

<sup>110</sup> Defence Human Resource Activity, *Counterintelligence*, s. 21, <http://www.dhra.mil/perserec/adr/counterintelligence/counterintelligence.pdf> (Erişim tarihi: 12 Aralık 2012).

de çoğunlukla budur.<sup>111</sup>

### 2.3.1.1.3.2. Duygusal Motifler

Duygusal motifleri şu başlıklar altında ele almak mümkündür.<sup>112</sup>

– **Duygusal İlişki:** Bilgi veren veya casus ile bilgiyi alacak olan kişi arasında duygusal bir ilişkinin oluşması, bilgi alışverişini kolaylaştırabilecek motiflerden birisidir.

– **Korku:** Özel hayatlarında veya işlerinde ilişki kurdukları kişilerden herhangi bir sebeple korkan kişiler, bu korkularından kurtarılmaları veya korunmaları maksadıyla seve seve bilgi verebilirler. Suç faaliyetlerinde bulunmasından dolayı yasal olarak ceza alma endişesiyle, suçlamaların kaldırılması veya en azından azaltılması gibi beklentilere sahip kişilerin motifi de farklı bir korkuya dayanır.

– **Öfke / Nefret / Kin / İntikam:** Herhangi bir sebeple, muhtemelen daha önceki yaşanmışlıklarına dayanarak kişi, şirket, kurum ve ülkelere kin besleyen kişiler, düşman olarak nitelendirebilecekleri bu kişi, şirket, kurum ve ülkelerle ilgili her türlü bilgiyi düşünmeden paylaşabilirler. Bu kişilerin kin ve intikam duyguları sınır tanımaz boyutlarda olabilir. Şöyle ki, çalıştığı şirketteki amirine kişisel bir sebeple öfkelenen bir çalışan, sırf amirinin zarar göreceğini düşündüğü için, görevi gereği erişim yetkisi bulunan hassas şirket bilgilerini kolaylıkla sızdırabilecek kadar gözünü karartabilir. İkinci Dünya Savaşı'nda Nazi Almanyası'na hesabına çalışmış en önemli casuslardan biri de İlyas Bazna (Kod adı Çiçero)'dır. Çiçero'nun, babasının ölümünden sorumlu tuttuğu İngilizlere duyduğu kin ve nefret duyguları ile para kazanma arzusu, Ankara'daki İngiliz Büyükelçiliğinde çalışırken önemli bilgileri Almanlara satmasına neden olmuştur.

– **Koruma Arzusu:** Bazı kişiler kendilerini, çocuklarını veya ailelerini bir kişi veya durumdan korumak, tehlikeli kişi ve durumlardan tecrit etmek veya tehlikenin kaynağından sonsuza dek kurtulmak isteği ile bilgi verme konusunda işbirlikçi davranabilirler.

<sup>111</sup> Fitzgerald, *a.g.e.*, s. 29.

<sup>112</sup> Wallace ve Melton, *a.g.e.*, s. 363; Tzu, *a.g.e.*, s. 292; Fitzgerald, *a.g.e.*, ss. 23–37; MIT Resmî İnternet Sayfası, “*İkinci Dünya Savaşı Yıllarında ve Sonrasında Yabancı Servislere Karşı Verilen Mücadele*”, [http://www.mit.gov.tr/text\\_site/ikinci\\_bolum\\_E2\\_1.html](http://www.mit.gov.tr/text_site/ikinci_bolum_E2_1.html) (Erişim tarihi: 10 Mayıs 2013).

– **Psikolojik Rahatsızlık:** En az tercih edilen bilgi veren motiflerinden birisidir. Çünkü bu tür rahatsızlığı olan kişilerin hayal dünyaları da geniştir. Bazen olmamış olayları dahi olmuş gibi gösterebilirler. Bu kişilerle casusluk boyutunda gizli bir irtibat kurmak için çok iyi değerlendirme yapmak gerekir.

– **Pişmanlık:** Özellikle işledikleri suçlardan dolayı topluma karşı kendisini ezik hisseden ve vicdan azabı çeken eski suçluların motifidir. Bu kişiler, kendilerine ve topluma karşı duydukları yoğun pişmanlığı hafifletebilmek maksadıyla, bilgi vermeyi veya casusluğu kabul edebilirler.

– **Heyecan ve Serüven Arayışı:** James Bond sendromu olarak da adlandırılan bu motif, aradığı heyecanı casusluk ya da muhbirlikte bulacağına inanan kişilerin motifidir.

– **Ego:** Genellikle mensubu olduğu organizasyon içindeki öneminin, yetenek ve becerilerinin fark edilmediğine, hak ettiği hâlde ödüllendirilmediğine veya organizasyonunun en önemli parçası olduğu hâlde yeterince takdir edilmediğine inanan kişilerin bilgi veren olma veya casusluk eylemlerine giriş motifidir. Bir organizasyonda işten çıkarılmış, aşırılıkları nedeniyle cezalandırılmış, doğası gereği açgözlü ve hak ettiklerini düşündükleri makamlara yükselememiş kişiler, rakip veya düşman organizasyonlar için ideal ego motiflerine sahiptirler.

– **Baskı ve Şantaj:** Sıkça başvurulanan motiflerden gibi görünse de aslında en risklilerindendir. Çünkü sadece belli kişiliklerde etkili olabilecek bir olumsuz itkidir.

#### 2.3.1.1.3.3. İdeolojik Motifler

Siyasi, ulusal, dinî ve sosyal ideallerin gerçekleşmesi beklentisi olarak ortaya çıkan bu motif, en çok tercih edilen ve aranan motiflerdendir. Herhangi bir ideolojinin taraftarı veya karşıtlığı şeklinde olabilir. Özellikle, istedikleri hâlde kaçıp kurtulamadıkları ya da değiştiremedikleri politik veya ekonomik sisteme karşı yoğun olumsuz duygular besleyen bireylerde etkili bir teşvik silahıdır (Örnek: Muzaffer Çengil<sup>113</sup>).

Motif kavramı genel olarak görüldüğünden daha karmaşıktır. Para genellikle bireylerin bozulmasında en etkili motif gibi gözükse de, öfke ve intikam gibi motifler,

---

<sup>113</sup> Çitlioğlu, *a.g.e.*, ss. 105–222.

özellikle bireylerin terfi konusunda es geçildiklerini veya katkılarının fark edilmediğini düşündükleri durumlarda daha özel motiflere dönüşürler. Motif, statü hakkında derin bir memnuniyetsizlik, güvensizlik, bir azınlık grubunun üyesi olmak, aşırı hırslı veya fanatik olmak ya da bazı saplantılardan da kaynaklanabilir.<sup>114</sup>

Öte yandan motifler her zaman bilinebilir olmayabilir. Ayrıca kaynaklar, sahip olduklarını göstermeye çalıştıkları motifler konusunda her zaman dürüst de olmayabilirler.<sup>115</sup>

#### 2.3.1.1.4. Casus Adaylarında Aranılan Özellikler

Profesyonel istihbaratçılar veya casuslar, kancalayarak kendi emellerine alet etmeye çalıştıkları kişilerin, en azından temel birtakım özelliklere sahip olmalarını isterler ve ararlar. Bu özellikteki kişiler, elemanlanma sürecini hem hızlandırıcı hem de başarıyla sonuçlandırıcı etki yapar.

Bu bağlamda, ulusal ve manevi değerleri zayıf olanlar ile devleti ortadan kaldırmayı amaçlayan yasa dışı oluşumların mensupları casusluk için en öncelikli ve cazip adaylardır. Yine aynı şekilde, şiddet veya tehditle halkın dinî, siyasi, sosyal, felsefi inanç, düşünce ve kanaatini değiştirmeye çalışan grup ve oluşumlara üye olanlarla, bunların faaliyetlerine katılanlar veya bunlara açıkça eğilimli olanlar da güçlü adaylardan sayılabilir. Çünkü kendilerinin amacı devleti yıkmak olan bu kişileri casusluğa yöneltmek için fazla çaba sarf etmeye dahi gerek yoktur.

Maddi anlamda sıkıntı içerisinde bulunanlar ile kısa yoldan zengin olmak ve geleceğini güvence altına almak için her türlü olumsuz davranışta bulunabilecek karakterdeki kişiler de, casusluk açısından en önemli motif olan paranın esirleri oldukları için güçlü adaylar arasındadırlar.<sup>116</sup>

CIA psikologlarının casusluğa eğilim konusunda ortaya koydukları sonuçlar dikkate değerdir. Yapılan araştırmalara göre, sadakatsiz, narsist\* ve isyankâr kişilerin casusluğa eğilimli oldukları ortaya çıkmıştır. Bu yüzden casus temininde evlilik sorunları ve evlilik dışı ilişkileri olan, kariyerleri başarısızlıklarla dolu, ülkesine

<sup>114</sup> Douglas, *a.g.e.*, s. 90.

<sup>115</sup> U.S. Army, *FM 34-60... a.g.e.*, s. Appendix A-69.

<sup>116</sup> Özdağ, *a.g.e.*, s. 131.

\* Narsisizm, kişinin kendisini beğenmesi, sevmesi, değerli, önemli hissetmesi ve kendisinden memnun olmasıdır. 3'üncü bölümde ayrıntılı olarak ele alınacaktır.

ve yönetim biçimine inanmayan hatta aleyhine faaliyetler içinde bulunan, aşırı kendini beğenmiş, kibirli, küstah, ebeveynlerine saygısız ve hiçbir şeyden memnun olmayan kişiler tercih edilmektedir. Casus temininde, sayılan teşvik edici etmenlerden sadece birinin kullanıldığı durumlar çok nadirdir. Genellikle ayartmalar birden fazla düşkünlüğün birleşimine dayandırılır.

Bir casus, hayatta kalmayı ve açığa çıkarılmamayı başarabilmek için üst düzeyde parlak zekâyâ ve demir gibi bir iradeye sahip olmalı ama davranışlarıyla ve görünüşü ile yeterince zeki olmayan, hatta aptal ve sarsak bir kişi görüntüsü vermelidir.<sup>117</sup>

Casus olarak seçilmesi olası kişilerin diğer özellikleri de şöyle sıralanabilir:

- Siyasi ve kişisel hırsla kendini tatmin etmek isteyenler,
- Yabancı hayranlığı içinde olanlar ve yabancı kültürlerin etkisinde olanlar,
- Aşırı denebilecek seviyede kumar oynayanlar, uyuşturucu kullananlar veya satanlar, karşı cinse / hemcinsine ve alkole düşkün olanlar,
- İşledikleri hata, kusur veya suç nedeniyle devlet hizmetlerinden çıkarılanlar.

Öte yandan CIA psikologlarının saptamalarına göre insanların, birçok kültürde orta yaş krizine girdikleri kabul edilen 35–45 yaşlar arasındaki dönemin, casusluk bakımından işe alınmaya en açık ve eyleme en eğilimli oldukları dönem olduğu ortaya çıkmıştır.<sup>118</sup>

Herhangi bir personelin (özellikle istihbarat örgütü mensuplarının), herhangi bir motif kullanılarak yabancı istihbarat servisleri tarafından kullanılıp kullanılmadığını (istihbarat söz dağarcığında “kancalanmak” olarak bilinir) ortaya çıkarmak için birtakım uyarı sistemleri oluşturulmalıdır. Örneğin personelin; kazancıyla tutarsız ve kaynağını açıklayamayacağı kadar fazla para harcaması, şüpheli olarak nitelendirilebilecek duygusal ve cinsel ilişkiler içinde bulunması, yurt içi veya yurt dışına sık ve kısa süreli açıklanması zor tatillere çıkması, görev kapsamı dışındaki alanlar ile ilgili sorular sormaya başlaması gibi davranışlar birer uyarı olarak ele

<sup>117</sup> Wallace ve Melton, *a.g.e.*, s. 382.

<sup>118</sup> *a.g.e.*, s. 362.

alınmalı ve araştırılmalıdır.<sup>119</sup>

#### 2.3.1.1.5. Casusların Bilgi Toplama Yöntem ve Teknikleri

Casuslar, bilgi topladıkları esnada işin doğası gereği gizliliğe üst düzeyde önem gösterirler ve yaptıkları faaliyetlerin anlaşılmasını ve tespit edilmemesi için çaba harcarlar. Bu yönde özel eğitimlere tabi tutuldukları da bir gerçektir. Gizliliği sağlayabilmek için birtakım özel teknikler ve yöntemler kullanırlar. Bu teknik ve yöntemlerin özel olmaları, her birinin ayrı prosedürler takip edilerek en ince ayrıntılara kadar planlanarak icra edilmelerinden ileri gelmektedir. Öyle ki, yapılacak en küçük hata açığa çıkmaya ya da görevin başarısızlıkla sonuçlanmasına sebep olabilecektir.

Casusların kullandıkları temel bilgi toplama yöntemleri; gözlem ve tarif, mülakat (görüşme / sohbet), sızdırma, takip ve tarassut (gözetleme), keşif, hırsızlık, sorgulama, arama, kışkırtma, şantaj ve rüşvet, çöp karıştırma, teknik ve elektronik olanakların kullanılması şeklinde sıralanabilir.<sup>120</sup>

Söz konusu yöntemlerin tamamında haber kaynağına hissettirilmeden istenilen belirli bir bilginin alınması amaçlanır. Örneğin sızdırma tekniğinde, bilgi alınmak istenen kişi veya grubun, konuşmanın amacından haberdar olmadığı ve konuşmanın gidişatından da bu amacı anlayamadığı, sıradan bir sohbet havasının varlığı söz konusudur.<sup>121</sup> Bu yöntemler, sıradan haber toplama yöntemlerine kıyasla daha karmaşıktırlar. Son derece dikkatli ve ayrıntılı bir hazırlık dönemi, planlama ve uygulama gerektirirler.<sup>122</sup> İnsan doğasının getirdiği, kişiden kişiye değişen ama herkes için mutlaka var olan düşkünlükleri kullanmak, bu yöntemlerin temelinde yer alan mantıktır. Zararsız gibi görünen bilgileri istemek, güven duygusu uyandırmak, yardımcı olduğuna inandırmak, yardım istemek, acındırmak, sindirmek ve suçluluk duygusu uyandırmak gibi yüzlerce insana özgü düşkünlüğü kişisel boyutta keşfedip kullanmak bir casusun en iyi yaptığı işlerdendir.

Casuslar yabancı dil bildiklerini gizlerler. Zira yabancıların, yanlarında kendi dillerini bilmediğini düşündükleri birisi varken bazı konuları daha rahat

<sup>119</sup> Özdağ, *a.g.e.*, s. 163.

<sup>120</sup> Douglas, *a.g.e.*, s. 90; Acar ve Urhal, *a.g.e.*, s. 234.

<sup>121</sup> U.S. Army, *FM 34... a.g.e.*, s. Appendix A-8.

<sup>122</sup> U.S. Army, *FM 2-22.3 (FM 34-52) Human Intelligence Collector Operations*, Washington D.C., 2006, s. 9-5.

konusabildiklerini çok iyi bilirler. Öte yandan herhangi bir amaçla yurt dışına giden kişilerin aralarında kendi dillerini konuşmalarının sakıncalı olduğunu ve her zaman konuşulanlarla ilgili ve konuşulan dili anlayan birileri tarafından takip edilme olasılığının bulunduğunu bilerek bu yönde davranırlar. Takip ve takipten kurtulma konusunda çok yetenekli ve eğitimidirler. Herkesten ve her olaydan şüphelenirler ve genel anlamda kimseye güvenmezler. Öğrendikleri her haberin doğruluğuna veya yanlışlığına hemen hükmetmezler ve mutlaka teyit etmeye çalışırlar. Dikkat çekecek bir hareketlilikten ve yaşantıdan her zaman kaçınırlar, sinsice ve sezdirmeden çalışırlar. İkamet veya çalışma için seçtikleri yerlerin birden fazla giriş ve çıkış kapısının olmasına dikkat ederler ve her türlü olasılığa göre kaçış provaları yaparlar.<sup>123</sup>

Özünde bir yöntem ve teknik olarak sayılamayacak olsa bile, casuslukta kadınlardan ve gençlerden çokça faydalandığına da değinmek lazım gelir. Kadınlar, cinsel veya duygusal ilişki, cazibe ve para karşılığında rahatlıkla bilgi temin edebilecekleri gibi başka birçok şeyi de yaptırabilirler.<sup>124</sup> Casusluk tarihi, bilgi almak ve propaganda yapmak hususunda ülkelerine büyük hizmetler etmiş kadın casuslarla doludur. En bilinenlerinden biri, Birinci Dünya Savaşı yıllarında Almanya adına önemli işler yapmış olan Mata Hari'dir.

Her statüdeki gençler ve deneyimsiz personel ise özellikle yaşlarından kaynaklanan ve yetişkinlere göre kendilerini daha cazip birer hedef hâline sokan, üst düzeylerde yaşadıkları duyguları, hevesleri, hassasiyetleri, inançları, dinamizmleri, serüven ve moda tutkuları nedeniyle sıkça casuslar tarafından kötüye kullanılmaya çalışılırlar.

Casuslar, çeşitli sebepler ve kurmaca rastlantılarla hedeflerindeki kişilerle ilişki kurmaya çalışırlar. Yerine göre her kılığa girebilen, çok iyi rol yapan ve iyi yalan söyleyen kişilerdir. Yaptıkları rollerin ve oynadıkları senaryoların yazarları da genelde kendileridir. Bu faaliyetin kusursuz olmasına özen gösterirler ve bu kusursuzluk için çok iyi hazırlık yaparlar. Yine de günümüzde casusların sadece dış görünüşte kusursuz olmaları yeterli değildir. Kılık ve kimliklerine uygun maske mazeretlerinin bulunması da çok önemlidir. Hatta büründükleri kılığı ve kimliği dünya çapında kullanılan sistemlerde dahi yansıtmak zorundadırlar. Örneğin, internetin etkili ve doğru şekilde kullanılarak internet üzerinde, kişinin büründüğü kılıkla tutarlı

---

<sup>123</sup> Yakın, **a.g.e.**, s. 117.

<sup>124</sup> Kazım Karabekir, **Gizli Harp İstihbarat**, Kamer Yayınları, İstanbul, 1998, s. 26.

bilgilerin bulunması, çağcıl casusun kimliğinde, geleneksel sakal–gözlük ikilisi kadar büyük önem taşımaktadır.<sup>125</sup>

Casuslar, amaçlarına ulaşmak için, ülke içinde faaliyet gösteren yasa dışı örgütlerle işbirliği yaparak veya örgütlere maddi destek sağlayarak bu örgütleri her anlamda kullanırlar. Gezi, inceleme, staj, kurs, öğrenim, mübadele vb. maksatlarla ülkeye gelenler ile resmî dış temsilciliklere, kuruluşlara ve yurt dışındaki işçi topluluklarına gizli şekilde eleman yerleştirebilirler. Yabancı ülkelerin temsilciliklerinde çalışan yerel yöneticileri kullanabilirler. Yurt içi ve yurt dışı kuruluşlarda önemli kişilerin kullandığı iletişim vasıtalarını dinleyebilirler.

Casuslar, ahlaki değerleri ikinci hatta üçüncü planda göz önünde bulunduran, acımasız ve amaca giden her yolu mubah kabul eden ve duygularından arınmış kişilerdir. Potansiyel düşkünlüklerin keşfedilip kaşınarak ortaya çıkarılması ve kötüye kullanılması konusunda çok yeteneklidirler. Düşkünlüğün yokluğu onlar için engel değildir. Kumar, alkol, uyuşturucu ve borç batağına çekerek istedikleri zafiyetin oluşmasını sağlarlar. Örneğin, maddi sıkıntı çeken kişileri, karşılıksız yardımlarla, maddi ve manevi borçluluk duygusu oluşturarak kendi emelleri doğrultusunda kullanabilirler. Düşkünlüklerin kullanılmasında başvuru –en son başvurulacak yöntemlerden olsa da– en belirgin yöntemlerden biri de şantaj ve tehdittir. Zira bu yöntemin üstüne uygulanabilecek fazla yöntem yoktur.

Casuslar, asıl amaçlarını hem gizlemek hem de kolaylaştırmak için şirketler, ticarethaneler, genelevler, eğlence yerleri ve oyun salonları gibi düşkünlüklerin üst seviyelerde ortaya çıkarılabildiği yerler kurarak işletirler. Böylece bazı kişileri ağlarına düşürerek bilgi toplama işini kolaylaştırabilirler. Yine benzer şekilde, dedikoduya ve başkalarını çekiştirmeye yönelterek bazı bilgileri elde edebilirler.<sup>126</sup>

Casusların niteliklerinin ve becerilerinin yanı sıra kullandıkları birtakım alet ve araçlar da işlerini kolaylaştırır. Gelişen teknoloji ile uyumlu olarak kendini yenileyen bu aletlerin genel kullanıma sunulmadan önce yıllarca istihbarat örgütleri tarafından kullanıldıkları<sup>127</sup> (belgegeçer gibi) bilinmektedir. Bu alanda kullanılan kökleşik ve her zaman geçerliliğini koruyan araç, gereç ve yöntemlerden bazıları şunlardır:<sup>128</sup>

<sup>125</sup> Wallace ve Melton, *a.g.e.*, s. 383.

<sup>126</sup> Karabekir, *a.g.e.*, s. 27.

<sup>127</sup> Avci, *İstihbarat Oyunları... a.g.e.*, s. 207.

<sup>128</sup> Kemal Girgin, *Uluslararası İlişkiler: Modern İstihbarat ve Türkiye*, Okumuş Adam Yayınları, İstanbul, 2003, ss. 275–276.

- Odalara, araçlara ve kıyafetlere saklanabilen alıcı-verici cihazlar ile pipo, çakmak, kalem, gözlük, yüzük, şemsiye gibi küçük şahsi yardımcı eşyalara gizlenebilen çok küçük kameralar, dinleme cihazları ve çeşitli türde küçük mikrofonlar (yaka rozetinde, düğmelerde, ayakkabı topuğunda vb.),
- Çok üstün teknik nitelikli fotoğraf makineleri ve video kameralar ile çeşitli boyut ve şekillerde, fotoğraf çekebilme özelliği de olan dürbünler,
- Şifreli ileti alma, gönderme, yazma ve çözme teknikleri ve aletleri ile yön ve konum belirleyici ve bildirici minik elektronik aletler (saat gibi),
- Duvarların arkasını dinlemek veya fotoğrafını çekmek maksadıyla duvarda delik açabilen ve şırınga iğnesi kalınlığında borulardan oluşan dinleme veya görüntüleme düzenekleri,
- Görünmez yazı yazılmasında kullanılan özel kâğıtlar ve kimyasallar,
- Kasa ve her türlü kilidi açabilen aletler ve kalıp çıkarma sistemleri,
- Sahte kimlik ve pasaportlar, kamufle edilmeyi sağlayan maske mazeretler, tanınmayı engelleyen kod adlar,
- Çeşitli silahlar, zehirler, kimyasal ve biyolojik maddeler ile insanın hayal gücünün sınırlarını zorlayan daha birçok madde ve yöntem.

Öte yandan “aile içi veya arkadaşlarla yapılan özel, sakınmasız sohbetlerden filtreden geçirilmemiş bilgi edinmede gizli dinleme operasyonları”<sup>129</sup> günümüzde en çok başvurulan yöntemlerden birisi hâline gelmiştir. Casusların kullandığı yöntem ve teknikler, teknolojinin ve çağın gereklerine göre sürekli kendilerini yenileyerek ve geliştirerek casusluğa karşı koyma işini üstlenenleri her zaman zorlamaya devam edeceklerdir.

#### **2.3.1.2. Casusluğa Karşı Koyma**

Karşı casusluk ya da casusluğa karşı koyma, en basit şekliyle casusların ortaya çıkarılması için yapılan her türlü araştırma ve operasyon olarak

<sup>129</sup> Wallace ve Melton, *a.g.e.*, s. 362.

tanımlanabilir. Çok uzun süreleri kapsayan araştırmalar gerektirebilen, sabır isteyen, uzmanlar tarafından icra edilmesi gereken zorlu bir faaliyettir. Uzmanlık konusu tek kişi ile de sınırlı değildir. Deneyimli çözümlemeciler, nitelikli operasyon elemanları, teknik uzmanlar, avukatlar, finans uzmanları, psikologlar vb. birçok kişiden oluşan bir takım çalışması, başarılı bir karşı casusluk için şarttır.<sup>130</sup>

Casusluğa karşı koyma faaliyetleri, İKK faaliyetlerinin aktif yönünün bir bölümünü oluşturur ve öncelikli amacı başlamış bir casusluk faaliyetini nihai amacına ulaşmadan bulup ortaya çıkarabilmektir. Casusların bulunmasından sonra çeşitli operasyonların uygulanması düşünülebilir. Örneğin uygun şartların bulunduğu durumlarda ikili casus operasyonları\* devreye sokulabilir.

Casusluk tam anlamıyla bir uzmanlık işidir ve gizli faaliyetleri yürütebilme deneyimine sahip, özel olarak seçilmiş ve eğitilmiş, belli özellikler taşıyan elemanlar tarafından yürütülmektedir. O hâlde böyle bir çalışmanın karşısında yer alacak karşı koyma hizmetlerinde de en az casus teşkilatlarına yakın ve hatta daha iyi nitelik ve özelliklere sahip mücadele teşkilatları oluşturulması gereklidir. Dolayısıyla karşı casusluk, üstün bir sabır, soğukkanlılık, aceleci olmamayı, sağlam bir bilgi altyapısı ve deneyime sahip olmayı, düşman manevralarını anlayabilme yeteneğini, yaratıcı zekâyı ve şahsın kendisini işine tam olarak vermesini (işe adanmışlık) gerektirir. Ayrıca casusluk konusunda tam bilgi sahibi olunmalıdır ki karşı koymada başarı kazanılabilsin.<sup>131</sup>

Sun Tzu'nun da dediği gibi; "Düşmanı ve kendinizi iyi tanıyorsanız, yüzlerce savaşa bile katılsanız sonucun istediğiniz gibi olacağından emin olabilirsiniz. Kendinizi tanıyıp, düşmanı tanımiyorsanız, kazanacağınız her zafere karşın yenilgiyle de tanışabilirsiniz. Ne kendinizi ne de düşmanı tanıyorsanız, gireceğiniz her savaşta yenilgi sizin için kaçınılmazdır."<sup>132</sup>

#### **2.3.1.2.1. Casusluğun ve İstihbarat Operasyonlarının Olası Göstergeleri**

Casusluğa karşı koyma, aktif olduğu kadar pasif önlemleri de gerektirir. Zira

---

<sup>130</sup> Ehrman, **a.g.e.**, s. 19.

\* İkili casus operasyonu, casusluk yaparken tespit edilenlerden uygun olduğu değerlendirilenlerin çift taraflı casus olarak kullanılması faaliyetidir.

<sup>131</sup> Acar ve Urhal, **a.g.e.**, s. 300.

<sup>132</sup> Tzu, **a.g.e.**, s. 19.

bir casusun açığa çıkarılmasında profesyonel karşı istihbaratçıların olduğu kadar sıradan vatandaşın farkındalığı ve katkısı da çok önemlidir. Bu bağlamda casus olabileceğinden şüphelenilmesi gereken kişilerin genel özelliklerinin bilinmesinde yarar vardır. Bu özellikler kuşkusuz casusluğun kesin ipuçları olmayabilir, belki bambaşka bir sebebin sonucu da olabilir ama casusluk göstergesi olma olasılığı da göz ardı edilmemelidir.

Söz konusu göstergeleri tahmin etmek aslında çok da zor değildir. Çoğu kökleşik sayılabilecek ve normal şartlarda dikkat çekecek göstergelerdir. Bunların başında kumar tutkusu gelir. Eğer bir kişi kazandığından fazlasını kumarda kaybediyorsa ve bu kazancın açıklanabilir bir yönü yoksa casusluktan şüphelenilebilir. Aynı şekilde kazancının çok üzerinde ve bol keseden para sarf edenler, gelirleriyle orantısız lüks bir yaşam sürdürenler ve her zaman kolay yoldan zengin olmanın yollarını arayanlardan bir anda ve açıklanamayacak şekilde maddi anlamda iyi seviyelere yükselenlere de casusluk şüphesiyle yaklaşılabılır.<sup>133</sup>

Anlamsız ve nedensizce tanışmaya çalışanlar ile ilk defa karşılaşılmasına rağmen kendisini ilgilendirmeyen ama önemli konulara ilişkin sorular soran kimseler; farklı kimlikler, kılık ve kıyafetlerle farklı yerlerde karşılaşılan veya görülen kimseler; yakın bölgelere yeni taşınıp çok sık iş değiştiren, çoğu zaman mesleğini söylemekten dahi kaçınan kişiler; işi veya görevinin haricinde sıkça kısa süreli yurt dışına çıkanlar ile sürekli ülkenin önemli olabilecek tesis ve bölgelerini gezenler; geçici (turist, görev vb.) veya yerleşik olarak ülkeye gelen, turistik yerlerin dışındaki bölgelerde dolaşan yabancı uyruklular ve Türk uyruklu yabancılar; ideolojik düşüncelerinin esiri olmuş, ülkenin yönetim biçimini beğenmeyen, ülkede yaşamaktan memnun olmayan, ülkeye ve ulusa kin ve garez besleyenler ve bunu çekinmeden dillendirenler casus olduğu yönünde şüphelenilmesi gereken kişilerden sayılabilir.

Bu bağlamda casusluğun veya istihbarat toplama girişimlerinin olası göstergeleri şunlar olabilir.<sup>134</sup>

– Hâlihazırdaki veya şüphelenilen bir casusluk vb. istihbarat faaliyeti içinde olduğu açıkça bilinen ya da öyle olduğuna inanılan kişilerle ilgisiz bir sebeple

<sup>133</sup> Yakın, *a.g.e.*, ss. 214–215.

<sup>134</sup> Department of Defence of U.S.A., *Directive: Counterintelligence, Awareness and Reporting (CIAR)*, No.: 5240.06, 17 Mayıs 2011, Enclosure 4, ss. 13–14; Douglas, *a.g.e.*, s. 91.

bağlantı kuran kişiler,

- Yabancı diplomatik tesislere (büyükkelçilik gibi) yapılan, sebebi ve amacı açıklanamayan veya resmî görevlerle uyuşmayan ziyaretlerde bulunan kişiler,

- Yabancıların, özellikle belli konularda sorular sormaları, sürekli bir bilgi alma çabası içinde olmaları ve bazı tesisleri ziyaret etmek için çabalamaları,

- İnsanları; özel muamele, iyilikler, hediyeler ve para ile aldıklarının karşılığını vermek zorunda bırakacak bir duruma sokmaya çalışanlar,

- Şantaj veya zor kullanma yöntemlerini uygulayabilmek için iş arkadaşlarını ayartma ve onları bir suç batağının içine çekme çabası içinde olanlar,

- Bir görevin parçası olmayan, mantıklı seyahat görünümünden uzak, tutarsız ve personelin resmî görevi veya parasal kapasitesi ile uyuşmayan seyahatler,

- Bireyin gelir seviyesinin karşılayamayacağı derecede pahalı alışverişler yapması veya birden edindiği servetini, miras, kumarda şans veya başarılı bir iş girişiminin meyveleri olarak açıklama çabası gibi akla yatmayan ve usulsüz zenginlik ile kötü giden bir parasal durumun aniden düzeltilmesi veya yüksek tutardaki vergilerin veya borçların aniden ödenmesi,

- Düşman veya rakiplerin, bizimle ilgili sır, gizli faaliyet, yeni ürün ve stratejilerden her zaman önceden haberdar olmaları ve buna göre davranmaları; aynı rakiplere karşı rekabet ortamlarında sürekli kaybetme durumu ve yapılması planlanan faaliyetler ile ürünlerin çok benzerlerinin rakipler tarafından daha önce yapılarak piyasaya sürülmesi,

- Kendisine görev verilmediği ve zorunda olmadıkları hâlde gönüllü olmak yoluyla bazı işleri yapmaya ve böylece gizli bilgilere erişebilme yetkisi kazanmaya çalışanlar,

- Yetkili olmadıkları hâlde gizli ve hassas bilgilere erişim sağlamaya çalışanlar ile elde edilmesine ön ayak olanlar veya göz yumanlar,

- Gizlilik dereceli ve hassas bilgilerin konuşulduğu, bulunduğu veya

saklandığı yerlerde yapılan kontrollerde gizli dinleme, izleme ve kayıt gereçlerinin tespit edilmesi,

– Bilgisayar, silah, gizli belge vb. bazı önemli yazılım ve donanımın kaybolması veya çalınması,

– Önemli makamlardaki çalışanların ayrılarak düşman veya rakip için çalışmaya başlaması,

– Nedensiz ve sıkça fazla mesai yapılması,

– Bilinçli ve kasıtlı olarak, gizlilik dereceli ve hassas bilginin;

- Güvenli olmayan iletişim araçları ve gereçleriyle iletilmesi,

- İlgisiz yer, zaman ve yerlerde okunması veya konuşulması,

- Güvenli bölgeler dışına yetkisiz ve izinsiz çıkarılması,

- Yetkisiz ve izinsiz şekilde depolanması,

- Yetkisiz olarak kopyalanması, çıktısının alınması, e-posta ve belgegeçer gibi yollarla gönderilmesi,

- Üzerindeki gizlilik derecesini gösteren işaretlerin, uygun olmayan yol ve yöntemlerle değiştirilmesi veya tamamen kaldırılmasıdır.

Casusluk, insanoğlunun hayal gücüyle ve zekâsıyla doğru orantılı bir meslek olduğu içindir ki, ne kadar çok ipucu varmış gibi görünse de birçok casusluk olayının ortaya çıkarılması uzun yıllar almıştır. Casusluk tarihinde, en önemli kurum ve servislerin önemli makamlarına kadar yükselmeyi başarmış ve yıllarca bu yerlerde casusluk yapmış olan kişilere rastlamak mümkündür. Robert Hanssen, ABD Federal Soruşturma Bürosu (FBI)'nda özel ajan olarak görev yapan bir Rus casusu olarak yirmi iki yıl sonra yakalanabilmiştir. Yine “asrın casusu” olarak nitelendirilen Kim Philby de, SSCB'nin bir casusu olarak çok uzun yıllar görev yaparken İngiliz Dış

İstihbarat Servisi (MI6)'nde operasyon şefliğine kadar yükselmiştir.<sup>135</sup>

#### **2.3.1.2.2. Casusluk Girişimlerine Karşı Alınabilecek Önlemler**

Casusların tespit edilmesi çok zordur. Tespit edilmiş casuslar, cezalandırıldıkları için zaten tehlikeli tarafları kalmamaktadır. Tespit edilememiş yani bilinmeyen bir düşmana karşı önlemler almak da çok mantıklı görünmemektedir. Alınacak önlemler ve hareket tarzları adı altında sıralanacak hususlar sayesinde bazı yöntem ve teknikleri vurgulamak ve olasılıkları hatırlatmak istenmektedir. Olası düşmanın daha önceki uygulamalarından yola çıkarak bir uygulamalar yelpazesi sunmak amaçlanmaktadır. Yoksa etrafımızdaki herkese casus şüphesiyle davranmak gerekir ki, böyle davranmak hem anlamsız hem de sağlıksız bir paranoyaya yol açmaktan başka bir işe yaramaz.

Belirlenen önlem ve hareket tarzlarının casusluğa karşı tamamen koruyucu bir nitelikte olması da mümkün değildir. Çünkü casusluk, hâlen birçok yöntem ve tekniği bilinmeyen bir alandır. Dolayısıyla bu önlemlerin asıl ve nihai amacı, casusluk konusundaki bilinci yükseltmek ve bir farkındalık yaratabilmektir. Bu bağlamda alınabilecek önlem ve uygulanması gereken hareket tarzları şöyle sıralanabilir:<sup>136</sup>

– İçki, uyuşturucu gibi iradeyi körelten maddelerden uzak durulmalı, özellikle tanınmayan ve rastlantı eseri karşılaşılan kadınlarla ilişkiye girilmemelidir. Para, cinsellik, kumar, alkol, uyuşturucu madde, hediye alma vb. konularda düşkünlüğü bulunanların takibi yapılmalıdır. Özellikle önemli makamlardaki kişilerin, olası tuzaklara karşı uyanık olmaları sağlanmalı, bilmedikleri yerlere gitmemeleri, yalnız eğlenmemeleri ve alkol almamaları, tanımadıkları kadınlarla birlikte olmamaları öğütlenmelidir.

– Şantaj ve tehdit malzemesi olarak kullanılabilecek her türlü yasa dışı faaliyet ve oluşum ile gizli kapaklı işlerden uzak durulmalı, yasal olmayan ilişkilerden kaçınılmalıdır.

– İşyerindeki geçimsizlik ve hoşnutsuzlukları dışa yansıtmaktan kaçınılmalıdır. İş ve görevle ilgili hususlar işyeri dışında, aile ortamında, telefonda

<sup>135</sup> Avcı, *İstihbarat Oyunları... a.g.e.*, s. 252.

<sup>136</sup> Yakın, *a.g.e.*, s. 117.

vb. hiçbir yerde iş arkadaşları ve konuyla ilgili kişilerle dahi konuşulmamalıdır.

– Her türlü tuzağa karşı uyanık olunmalı, bilgiçlik taslayıp, oltaya gelip çok konuşulmamalı, bu tür ortamlardan olabildiğince uzak durulmalıdır. Çok iyi bilinen bir konuda fikir ve yorum istendiğinde, yerine göre konuyu ilk defa duyuyormuş ya da hiçbir bilgiye sahip değilmiş gibi davranılmalıdır.

– Bulunulan ülkenin veya kendi ülkesinin yönetim biçimini eleştirenlere dikkat edilmelidir.

– Yabancılarla gereksiz yakın dostluklar kurulmamalıdır. İyilik amacıyla yapılacak bazı yardımların kurulmuş bir tuzak olabileceği hatırdan çıkarılmamalı, her türlü olaydan (hazırlanmış bir senaryo gereği içine çekilmeye çalışıldığımız bir durum olabileceği olasılığı düşünülerek) uzak durma prensibi unutulmamalıdır.

– Telefonların dinlendiğini ve diğer her türlü iletişimin takip edildiği unutulmamalıdır.

– Özellikle personel ve iletişim güvenliği hususları başta olmak üzere tüm pasif İKK önlemlerine eksiksiz uyulmalıdır.

– Dış ülkelerdeki büyükelçilik ve konsolosluk gibi yerlerde kendi vatandaşlarımız çalıştırılmalı, zorunlu hâller dışında yerel kişiler çalıştırılmamalıdır.

– Yabancı servislerin tuzağına düşüldüğünde, ceza alma vb. sonuçları dahi göze alarak durum derhâl ilgili birimlere bildirilmeli, ilerleyen zamanlarda yakalanılması durumunda kaybedilebileceklerin daha büyük olacağı akıldan çıkarılmamalıdır.

– Olabildiğince yalnız hareket edilmemelidir.

– Herhangi bir görev verilmediği, yetkin ve eğitilmiş olunmadığı hâlde, kendi kendine durumdan vazife çıkarıp çeşitli şekillerde istihbarat toplama çabasına girilmemelidir.

– Sıkça birlik ve kurum ve kuruluşların yakınlarında görülen, çöplerini karıştıran, yakınlarda seyyar satıcılık, dilencilik vb. faaliyetlerde bulunanlar kontrol

altında tutulmalıdır.

– Turistik, bilimsel, ticari, askerî vb. maksatlarla ülkeye gelen yabancıların istihbarat faaliyetinde bulunma olasılığına karşı takip ve kontrolleri yapılmalıdır.

– Öte yandan düşman veya rakiplerden ele geçirilen veya bulunan casusluk malzemeleri incelemeye tabi tutulmalı, yapılacak çözümlemeler sayesinde rakiplerin teknikleri, taktikleri ve teknolojik seviyeleri tespit edilmelidir. Bu faaliyetleri yürütecek ve gerekli incelemeyi yapmakla görevli bir birim oluşturulmalıdır. Böylece yeni teknoloji kazanımı ve karşı önlemlerin belirlenmesi de mümkün olacaktır.<sup>137</sup>

– Casusluk olayından şüphelenen personel, duruma ve şüpheli şahsa ilişkin olarak kendiliğinden araştırma yapmamalı, kişiyi yakalamaya çalışmamalı ve durumu yetkili birimlere ve kişilere bildirmelidir. Yetkisiz ve ilgisiz kişilere (samimi arkadaşlar dâhil) durumdan bahsedilmemelidir. Böyle bir hareket personel için son derece tehlikeli olabileceği gibi, delilleri yok etmeden şahsı yakalama olanağını da yok edebilir. Unutulmamalıdır ki, takip ve yakalama, bu konuda uzmanlaşmış kişilerin görevidir ve sanıldığından daha karmaşık bir iştir. Zira önemli olan sadece söz konusu kişinin yakalanması değil sistemin ve bağlantıların tamamının ortaya çıkarılarak tabiri caizse büyük balığın ele geçirilmesidir.

### **2.3.2. Keşif ve Gözetlemeye Karşı Koyma**

Düşmanın istihbarat oluşturmak maksadıyla, keşif vasıtalarıyla dost unsurların tertibini, niyet ve faaliyetlerini ortaya çıkarma gayretlerinin engellenmesi, “keşfe karşı koyma” şeklinde tanımlanabilir. Burada “keşif vasıtası”; bir uydu, bir keşif uçağı veya tek bir düşman ajanı olabilir. “Gözetlemeye karşı koymak” da bu kapsamda değerlendirilebilir.

### **2.3.3. Aldatma**

Aktif karşı istihbarat, sadece casusluğa karşı koyma ile sınırlı değildir. Diğer etkili bir yöntem de aldatmadır. Aldatma, düşman veya rakip tarafından bizim niyet ve faaliyetlerimizin tam ve doğru olarak tespit edilmesini önlemek için gerçek hareketin ve tertiplenmenin gizlenmesi olabileceği gibi, hiç olmayan bir durum ve faaliyeti varmış gibi göstermek amacıyla yapılan düşmanı yanlış reaksiyonlar

<sup>137</sup> Wallace ve Melton, *a.g.e.*, s. 360.

vermeye sevk eden aldatıcı hareketler de olabilir. Aldatmada hedef düşmanın veya rakibin düşünce ve inançlarını istediğimiz şekilde yönlendirmek, eylemlerini arzu ettiğimiz yöne çevirmek ve bu eylemlerden kendi çıkarlarımız doğrultusunda yararlanmaktır.

Aldatma, bizim olanak ve yeteneklerimizi, ağırlık merkezlerimizi, güvenlik açıklarımızı, planlarımızı ve niyetlerimizi öğrenmek isteyen ve bu yönde faaliyet gösteren düşmanı yanıltmaya veya şaşırtmaya yani yapay bir gerçekliğe çekmeye çabalar. Aldatma; aldatmacalar, hileler, yalanlar, kamufraj, gösteriler, önyargılar oluşturma ve düşmana yanlış bilgi sağlama şeklinde olabilir.<sup>138</sup>

Aldatma; işinin uzmanı ve yetenekli, hedefini iyi tanıyan, onun duygularını, düşünce dünyasını, tutum ve davranışlarını algılayabilecek çözümlemecilere gereksinim duyar. Çözümlemecilerin tespitlerini uygulayacak olan kişiler de en az çözümlemeciler kadar ve hatta daha iyi olmalıdırlar. İkinci Dünya Savaşı tarihçisi F. Harry Hinsley, aldatmanın başarıyla uygulanabilmesi için düşmanın bizim bilmesini istemediğimiz konularla ilgili tam bir karanlığa hapsedilmesi ve düşmanın her an ne düşündüğünün ve ne bildiğinin bilinmesi gerektiğini ifade etmektedir.<sup>139</sup> Aslında aldatmanın, Hinsley'in ifade ettiklerinden daha önemli ve başarı vadeden başka bir girdisi vardır. O da yanlış bilgi vererek veya doğru bilginin akışını engelleyerek düşmanın bizim istediklerimizi bilmesini ve öğrenmesini sağlayabilmektir.

Bütün bu gereklilikler yerine getirilse ve düşmanı aldatmak için en iyi personele ve tekniklere sahip olursa bile düşman doğru bir zihinsel ve uygulayıcı tavır içerisindeyse aldatılması oldukça zordur.<sup>140</sup>

Aktif karşı istihbaratın nihai hedefi, rakiplerin gizli saydıkları faaliyetlerinin ve operasyonlarının içine sızabilmektir. Yani rakiplerin bilgisi olmadan onların hesaplamalarının ve operasyonlarının tamamlayıcı ve işlevsel bir parçası olmaktır. Bu bağlamda taarruzî karşı istihbarat, düşmanın karar alıcılarının aldıkları kararlarda en önemli yönlendirici görevi üstlenen istihbarat raporlarını yanıltmaya ve kendi istediğimiz şekilde oluşmalarını sağlamaya çalışmak gibi bir görev de üstlenir. Yani rakibin, bizim onun yapmasını istediğimiz bir seçimi, gönüllü olarak yapmasını

<sup>138</sup> U.S. Marine Corps, *a.g.e.*, ss. 1-7-1-8.

<sup>139</sup> Van Cleave, *Counterintelligence... a.g.e.*, s. 10.

<sup>140</sup> Özdağ, *a.g.e.*, s. 202.

sağlamak için de çabalar ve çalışır.<sup>141</sup> Aslında, genel anlamda düşünüldüğünde, aktif karşı istihbarat faaliyetleri arasında en önemlisinin ve en zorunun bu olduğu bile söylenebilir.

#### **2.3.4. Siber ve Elektronik Karşı Tedbirler (EKT)**

EKT, düşmanın elektromanyetik ortamı etkili bir biçimde kullanmasını önlemek veya azaltmak amacıyla yapılan hususları kapsar. EKT'nin hedefi düşman elektronik sistemlerini zayıflatma, iş göremez hâle getirme, karıştırma veya aldatmadır. Burada asıl amaç, düşmanın istihbarat oluşturmak maksadıyla elektromanyetik ortamı ve elektronik cihazları kullanarak dost kuvvetlerle ilgili her türlü bilgiyi ve faaliyeti öğrenebilme gayretini engellemek veya yanlış öğrenmesini sağlanmaktır.

Günümüzde interneti de kapsayan tüm bilgi ve iletişim ağlarının oluşturduğu küresel alana “siber uzay” denmektedir. Siber saldırı ise, siber uzaydaki her türlü veri, program ve ağ sisteminin değiştirilmesi, bozulması, sahtesinin üretilmesi, kesintiye uğratılması ya da yok edilmesi olarak tanımlanabilir. Siber uzayın fiziksel dünya ile bütünleşerek devletlerin her türlü altyapısına bağlanması, ciddi yararlar ve zaman kazandırmıştır. Ancak kazandırdıklarının yanında daha önce karşılaşılmayan risk ve tehditlerin doğmasına neden olduğu da bir gerçektir. Siber uzayla birlikte yepyeni bir muharebe cephesi daha ortaya çıkmıştır ve bu cephe eski cephelerin hepsinden daha tehlikeli ve daha yok edici boyutlardadır. Siber sistemlere bağımlı bir yaşama doğru hızla ilerlerken olası bir siber saldırıda yaşamın felç olması durumu söz konusudur. Bu yüzden siber uzaydan gelebilecek her türlü saldırı ve tehditlere karşı kurum, kuruluş ve kullanıcıların varlıklarını korumak ve devamlılığını sağlamak amacıyla siber güvenlik sistemleri oluşturulmalıdır.

Siber ve EKT'ler, uzman ve yetenekli kişilerden oluşturulacak kurum, kuruluş ve birlikler tarafından belirlenmesi, uygulanması ve kontrol edilmesi gereken teknik aktif karşı önlemlerdir. Pasif yönlerinden tamamen bağımsız olarak düşünülmeleri hatalı olur. Aktif ve pasif siber ve elektronik önlemler, birbirini bütünleyen ve kollayan bir yapıda organize edilmelidirler.

İstihbarat ve özellikle karşı istihbarat konusunda tarihimizin en parlak ve başarılı döneminin Kurtuluş Savaşı yılları olduğunu söylemek yanlış olmaz. Özellikle karşı istihbarat konusunda yapılan çalışmalar ve çok sayıda casusun açığa

<sup>141</sup> Van Cleave, *Counterintelligence... a.g.e.*, s. 27.

ıkarılarak faaliyetlerinin nlenmesi dikkate deęerdir. Mustafa Sagir, Robert Frew, Sait Molla gibi ok bilindik olanların yanında adı dahi duyulmayan ok sayıda casusun etkisiz hale getirilmesi, nemli bir casusluęa karşı koyma başarısıdır. En nemli ve topyekn bir casusluęa ve dolayısıyla İKK başarısı sayılabilecek olay ise, casusların cirit attıęı bir ortamda, Byk Taarruzun her trl hazırlık, tertiplenme ve planının, harekt bařlayana kadar –dost ve dřman– kimse tarafından ęrenilememiř olmasıdır.

## ÜÇÜNCÜ BÖLÜM

### KARŞI İSTİHBARATTA İNSAN BOYUTU

Bu bölümde karşı istihbarat faaliyetinin veya sürecinin, en önemli aktörü (kaynağı, vasıtası, uygulayıcısı vb.) olan insanın, davranışlarının oluşumu ve değişimi fazla ayrıntıya inilmeden fizyolojik, psikolojik ve sosyolojik temellerde irdelenmeye çalışılacaktır. Böylece, insan davranışlarının ve düşkünlüklerinin İKK anlamında oluşturduğu potansiyel tehlike ve dolayısıyla İKK önlemlerinin belirlenmesinde oynayacakları roller ortaya konulmaya çalışılacaktır.

#### 3.1. İNSAN DAVRANIŞLARININ OLUŞUMU

Davranış kavramı, her canlının içinde bulunduğu doğal ya da toplumsal ortamdaki iç ve dış uyaranlara karşı başlattığı bir hareketlenme sürecidir. Her davranış bir nedene dayanır, bir hedefi vardır ve belirli bir etki veya bazı güdülerin sonucunda oluşur. Özde iki tür davranış biçimi olduğu söylenebilir. Birinci davranış biçimi; özgür seçim içermeyen, içgüdüsel ve refleks davranışlardır. Daha çok otonom sinir sistemi tarafından yönlendirilen ve herhangi bir istencin etkin olmadığı bu tür davranışlar otomatik tepkilerden oluşan, bireysellik taşımayan davranış biçimleridir ve tüm insanlarda ortaktır. İkinci davranış biçimi ise; organizmanın, alınan uyarıcıya yorumunu katarak oluşturduğu irade içeren davranışlardır.<sup>142</sup>

İnsan davranışlarını ve bu davranışların oluşmasına sebep olan etmenleri açıklamak oldukça zordur. Davranışlar, insanın gereksinim ve güdülerinin, kişiliğinin, algılarının, tutumlarının, öğrendiklerinin, kültürünün, inançlarının ve daha birçok bilinmeyen etkisi altındadır.<sup>143</sup>

İnsanlar, alet ya da makineler gibi, davranışları teknik olarak kolayca açıklanabilecek basit organizmalar değildir. İnsanların kişilikleri, mizaçları, karakterleri, genetik yapıları, algılamaları, bilgi birikimleri (bellekleri), beklentileri, deneyimleri, heyecanları, duyguları, korkuları, güdüler, tutumları, inançları, sevinçleri, hastalıkları, üzüntüleri, kızgınlıkları ve gereksinimleri (beslenme, sevilme, ait olma gibi) ortaya koyacakları davranışlarda belirleyici rol oynar. Çevresel koşulların (iklim, coğrafya vb.) davranışlar üzerindeki etkisi de yadsınamaz.

<sup>142</sup> Mehmet Silah, **Sosyal Psikoloji Davranış Bilimi**, Seçkin Yayıncılık, Ankara, 2005, s. 33.

<sup>143</sup> H. İbrahim Özmen, "Liderlik Davranışını Etkileyen Toplumsal Normların Analizi", Sosyal Bilimler Enstitüsü, Süleyman Demirel Üniversitesi, Isparta, 2009 (**Yayınlanmamış Doktora Tezi**), s. 1.

Davranışları etkileyen nedenlerden önemli bir bölümü geçmişte yaşanmış köklü olaylara dayanır.<sup>144</sup> İşte bu yüzden, insanların çeşitli durumlar karşısında ortaya koyacakları davranışların anlaşılması için olayın, bireyin yetiştirme tarzının\* ve tepkinin gösterildiği andaki koşulların incelenmesi gereklidir. Davranışları etkileyen bireysel etkenler çok çeşitli ve oldukça karmaşıktır ama bir bireyin farklı zaman ve koşullarda aynı uyarılara karşı farklı davranışlarda bulunabilmesi olasılığı da vardır. Yani davranışların oluşumunda içinde bulunulan şartlar da belirleyici rol oynamaktadır.

Dolayısıyla, davranışların iki öğenin ürünü olduğunu söylemek mümkündür. Bunlar; davranışı gerçekleştiren bireyin yapısı ve davranışın gerçekleştiği andaki içinde bulunulan koşullardır.<sup>145</sup> Yani davranış, bireyin ve ortamın bir işlevi olarak kabul edilebilir. Bu durumda, farklı insanların aynı koşullarda farklı davranabilecekleri (bireysel yapı farklarından ötürü) ve aynı insanın farklı koşullarda farklı davranabileceği çıkarımı yapılabilir. O hâlde davranışları değiştirmek veya istenilen yönde bir davranış sergilenmesi için uyarıcı, içinde bulunulan koşullar veya birey üzerinde değişiklikler yapılması gereklidir.

İnsan, yaşayan bir organizma olarak, hem kalıtsal olarak doğuştan getirdiği mirasa hem de çevresel etkenlere bağlı olarak ve onların etkisinde sonradan kazandığı özelliklerinin bir yansıması olarak görünüm ve davranış bakımından farklılaşır. Saldırganlık, barınma, sevmek–sevilme vb. özellikler tüm canlılar için geçerli iken; dil, akıl ve din gibi özellikler yalnızca insana özgü niteliklerdir.<sup>146</sup>

Karşı istihbaratta insan etkeni konusuyla ilgisi bakımından, bireysel farklılıkları açıklamak için uğraşan kişilik psikolojisi ve kişinin içinde bulunduğu koşullara göre davranışlarının açıklanmasına çabalayan sosyal psikolojiye göre davranışı etkileyen önemli unsurlar aşağıdaki gibi ifade edilebilir:<sup>147</sup>

– **Bireyin biyolojik yapısı:** Organizmanın cinsiyeti, yaşı, fizyolojik ve biyolojik gereksinimleri gibi biyolojik veya organik özelliklerinin davranışlara önemli etkisi vardır. Örneğin; oyuncak satılan bir mağazanın vitrininin önünden geçen çocukla dedenin davranışlarının aynı olmaması veya aç insanların suç işlemeye (özellikle

<sup>144</sup> Erol Eren, *Örgütsel Davranış ve Yönetim Psikolojisi*, Beta Basım Yayım, İstanbul, 2010, s. 218.

\* Psikoloji biliminde "Personel History / Kişisel Geçmiş" olarak geçmektedir.

<sup>145</sup> Eren, *a.g.e.*, s. 217.

<sup>146</sup> Türkiye Biyoloji Sitesi, *Genetik Yapımız ve Davranışlarımız Arasındaki İlişki*, [http://www.biyolojici.com/Genetik\\_Yapimiz\\_ve\\_Davranislarimiz\\_Arasindaki\\_Iliski.html](http://www.biyolojici.com/Genetik_Yapimiz_ve_Davranislarimiz_Arasindaki_Iliski.html) (Erişim tarihi: 27 Nisan 2013).

<sup>147</sup> Özmen, *a.g.e.*, s. 65.

hırsızlık) daha eğilimli olmaları gibi.

– **Bireyin genel ve anlık psikolojik (içsel) durumu:** Dalgın, yorgun, isteksiz, üzüntülü, heyecanlı, içine kapanık olma, sakin olma, soğukkanlı olma, psikolojik rahatsızlığı bulunma gibi özellikler davranışları etkilerler. Örneğin; çocuğun neşeli olduğu durumlarda hoplayıp zıplaması, öfkeli olduğu durumlarda kendini yere atması, korktuğu durumlarda titremesi ya da ağlaması gibi.

– **Bireyin geçmiş yaşantısı ve deneyimleri:** Bireyin çocukluğu, gençliği, eğitimi, alışkanlıkları, deneyimleri gibi daha önceki yaşantısı da davranışlarını etkiler. Örneğin geçmişinde boğulma tehlikesi atlatan bir kişinin denizden veya deniz araçlarından uzak durması veya köpek tarafından ısırılan bir kişinin, ısırılmayacağından emin olunan köpeklerden dahi korkması gibi.

– **Bireyin içinde yaşadığı fiziksel çevre:** İçinde bulunulan sıcak–soğuk, gürültülü–sessiz, yalnız–kalabalık gibi fiziksel çevre özellikleri davranışları etkiler. Örneğin soğuk havalarda kalın kıyafetler giyinilmesinde, karanlıkta dışarıda yalnız gezinmek konusunda tedirginlik ve isteksizlik yaşanmasında fiziksel çevrenin etkisi vardır. Yine sıcak iklimlerde yaşayan insanların sıcakkanlı ve cana yakın olması; soğuk iklimlerde yaşayan insanların soğuk ve geç harekete geçen yapıları çevresel etkenlerden birisi olan iklimin sonuçlarıdır.

– **Bireyin içinde yaşadığı sosyal çevre:** Toplumun zengin veya fakir oluşu, inançları, ahlaki kuralları, örf ve adetleri gibi sosyal çevre özellikleri davranışları etkiler. Örneğin otobüste yaşlılara yer verme (saygı davranışı) davranışı sosyal çevrenin etkisinde şekillenir.

– **Bireyin tutum ve beklentileri:** Kişinin bir olay veya duruma ilişkin duygu düşünce, bilgi, inanç ve değerlendirmeleri ve beklentileri davranışlarını etkiler. Örneğin yarışa hazır atletlerin, başlama işareti verilmeden önce harekete geçmelerinde beklentilerin etkisi vardır.

– **Kişinin fenomenleri\*:** “Fenomenoloji, en genel anlamıyla kişinin kendisini ve çevresini kendine özgü bir şekilde algılama ve anlama biçimi olarak tanımlanabilir.” Bireyin davranışını, çevre koşulları, organizmadaki biyolojik dürtüler, istekler ve gereksinimlerden daha fazla oranda biçimlendiren ve belirleyen etken,

---

\* Fenomen sözcüğünün öz Türkçe karşılığı görüngüdür.

onun kendini ve çevreyi o andaki anlamlandırış biçimi, başka bir deyişle bireyin o andaki fenomenidir. İnsan davranışını ve dolayısıyla insanı anlayabilmek için, onun yaşamında neyin anlamlı olduğunu ve neyi gerçekleştirmeye çalıştığını yani onun fenomenini anlamak gerekir.<sup>148</sup> İki insan, aynı duruma tepki olarak birbirlerinden oldukça farklı davranabilirler ancak her birinin aynı olayı nasıl yorumladığı öğrenilerek davranışları tamamen kestirilebilir hâle gelebilir.<sup>149</sup>

Davranışların oluşumunda belirleyici olan etkenlerden biri de, gereksinimlerdir. Hümanistik psikologlara göre, açlık, susuzluk, cinsellik gibi fizyolojik gereksinimler önemli ve temel gereksinimlerdir ancak bu gereksinimler insanın ayırt edici özellikleri değildir. Bunlar tüm canlılar için geçerli olan gereksinimler ve dürtülerdir. İnsanı diğer canlılardan ayıran, sadece insana özgü olan başarmak, saygı görmek, aidiyet, sevmek ve sevilme gibi üst düzeydeki psikolojik gereksinimlerdir.<sup>150</sup>

Maslow'un insan gereksinimleri piramidinin en alt katında biyolojik gereksinimler yer alır. Biyolojik (fizyolojik) gereksinimler hava, açlık, susuzluk, uyku ve cinsel gereksinimler gibi belki ilkel ama hayati olanlardır. Biyolojik gereksinimlerin hemen üst katında güvenlik ihtiyacı bulunur. İnsan dış etkilere karşı kendisini korumak (sağlık, iş, barınma vb.) ve güven içinde yaşamak ister. İhtiyaçlar piramidinin üçüncü katında aidiyet ve sevgi ihtiyacı vardır. İnsanlar başka insanlarla ilişkiler kurmak, kabul edilmek ve kendisini bir yere ait hissetmek isterler. Dördüncü katta başarılı olmak, saygı görmek, prestij kazanmak, yeterli olmak, kendisini benimsetmek ve toplum tarafından kabul görmek gibi değer gereksinimleri yer alır. İhtiyaçlar hiyerarşisinin en üstünde ise tüm insan davranışlarını yöneten ve belirleyen en önemli güdü olarak "kendini gerçekleştirme" güdüsü bulunur. Bu sıralamaya göre bir basamaktaki ihtiyaç giderilmeden, bir sonraki ihtiyaç oluşmaz. Örneğin aç ya da susuz bir insanın, güvenlik ihtiyacını düşünmesi olanaksızdır.

Gereksinimlerin temel seviyede giderilmesi yeterlidir ve üst düzeydeki bir güdüye gidebilmek için alt düzeydeki bütün güdülerin tam anlamıyla doyuma ulaşmasına da gerek yoktur. Aile ortamı ve kültür gibi pek çok etki, bireysel anlamda hangi düzeydeki güdülerin daha baskın olacağını belirler. Davranışların ortaya

<sup>148</sup> Doğan Cüceloğlu, *İnsan ve Davranış: Psikolojinin Temel Kavramları*, Remzi Kitabevi, İstanbul, 2011, s. 32.

<sup>149</sup> Başak Karagöz, "İnsancıl Yaklaşım'da Bireyin Fenomenolojisi: Varoluşçu Psikoloji'den İnsancıl Psikoloji'ye, 'Fenomenoloji'ye Kısa Bir Bakış", *Pivotka*, Sayı: 20, Mart 2007, 13–15, s. 13.

<sup>150</sup> Yıldız Kuzgun, "Kendini Gerçekleştirme", *Araştırma Ankara Üniversitesi Dil ve Tarih-Coğrafya Fakültesi Felsefe Bölümü Dergisi*, 1972, 10.1, s. 169.

çıkışında önemli etkisi olan bu gereksinimler hiyerarşisinden habersiz kişilerin, insanları ve davranışlarını anlamaları pek mümkün değildir.<sup>151</sup> Karşı istihbaratta insan etkenini ele aldığımız bu bölümde, herhangi bir insan davranışının çözümleme sürecinde ele alınması durumunda gereksinimler hiyerarşisinin göz önünde bulundurulması lazım gelir.

İnsanların tutum, yetenek, tarz, huy, benlik, karakter ve mizaç gibi özelliklerinin bir bütünü olarak tanımlanan kişilik de davranışlar üzerinde önemli etkiye sahiptir.<sup>152</sup> Kişiliğin oluşması ve gelişmesinde iki etken önemli rol oynar. Bunlar; doğuştan getirilen genetik özellikler ile kültür, aile, arkadaş grubu gibi çevresel özelliklerdir.

Psikologlar kişiliği, kişiye özel ve ayırt edici davranışlar bütünü olarak tanımlarlar. Bu davranışlar, kişinin sıkça yaptığı ve kendisine has davranışlardır. İşte bu yüzden bir bireyin kişiliğini betimlerken hoşgörülü, cömert, saldırgan, tez canlı vb. davranış anlatan ifadeler kullanılır. Kişilikle gelen davranışlar, bireyin kolay kolay –genelde hiçbir zaman– değişmeyen, kişiye özel ve olası davranışları ile ilgili beklenti ve tahminler oluşturmak ve önceden davranış kestiriminde bulunmak bakımından basmakalıp denebilecek özelliktedir. Dolayısıyla bireyin davranışlarının belirlenmesi, şekillendirilmesi, yönlendirilmesi veya tahmin edilebilmesi için kişiliğinin göz önünde bulundurulması önemlidir.<sup>153</sup> Bu sayede daha etkin ve başarılı karşı istihbarat çözümlemeleri ve faaliyetleri yapılabilmesi mümkün olacaktır.

İnsan, sürekli olarak gerek fizyolojik gerekse psikolojik dış etkenlere maruz kalarak etkilenmektedir. İnsan davranışlarını önemli ölçüde belirleyen etkenlerden biri de çevredir. Fiziksel olarak çevreyi oluşturan her şey psikolojiyi, dolayısıyla da davranışları etkiler. Davranışların hangi çevresel koşullardan etkilendiğini tespit etmek, insan davranışlarının çözümlemesi ve şekillendirilmesi konusunda karşı istihbarat bakımından önemli ipuçları verebilir.

Davranışları etkileyen çevresel etkenlerden en önemlisi kültürdür. Toplumun belleği olarak da tanımlanabilen kültür, davranışların asli unsurlarındandır. İnsan davranışının şekillenmesinde, bireyin içinde büyüüp yaşadığı toplumun kültürü önemli bir rol oynar. Kültür, toplumsal ahlakın, geleneklerin, göreneklerin, örflerin, âdetlerin, değerlerin, hukuki kuralların ve toplumsal alışkanlıkların oluşturduğu

---

<sup>151</sup> Cüceloğlu, **a.g.e.**, s. 236.

<sup>152</sup> Feriha (Balkış) Baymur, **Genel Psikoloji**, İnkılâp Kitabevi, İstanbul, 2004, s. 273.

<sup>153</sup> Silah, **a.g.e.**, s. 201.

karmaşık bir olgudur. Kültür, insandan insana, kuşaktan kuşağa bilgi ve görgü aktarımını sağlayan ortamı oluşturur. Çoğunlukla soyut kavramlardan oluşan kültür, insanların algılama ve uygulamalarıyla davranışlara yansiyarak somutlaşmaktadır. Yine de bireysel farklılıklardan ötürü benzer ve hatta aynı uyarıcılara karşı gösterilen tepkiler ve davranışlar farklı olmaktadır.

Kültür, belirli türden davranışları istenen, uygun, beğenilen davranışlar olarak kabul edip pekiştirirken; bazı davranışları ise yererek ve aşağılayarak zamanla söndürülmesini sağlar. Dolayısıyla insanlar kendilerini kültürlerinin öngördüğü davranışları yapmak, hoş görmediklerinden sakınmak zorunda hissederler. Zira her toplumun kültürü, o toplumun insanlarını, belirli bir sosyal değerler (normlar) sistemi içinde ödüllendirir ya da cezalandırır. Davranışları olumlu yönde geliştirebilmek için toplumların kendi köklerinden beslenmeleri ve kültürel devamlılığı sağlamaları gerekmektedir. Bu sebeptendir ki, hızlı kültür değişmesi geçiren toplumlarda davranış ve kişilik bozukluklarında artışlar görmek mümkündür.<sup>154</sup>

Dil (konuşulan lisan), kültürün en belirleyici ve taşıyıcı unsurlarının başında gelir. Bilindiği gibi dil kavramlardan oluşur ve bu kavramlar düşünen insanların davranışlarını da şekillendirir. Karşı istihbaratta insan etkenini ele alırken dilin insan davranışlarına yansması göz ardı edilmemelidir. Dildeki kavramlar ve kullanılışları ele alınarak, insan davranışları yönünden önemli bulgulara ulaşmak mümkün olabilir.

Din ve inançlar da, kültürü etkileyen unsurlar arasında başat rol oynarlar. İman ve inançta sorgulama kısıtlıdır ve bir kabullenme söz konusudur. Dolayısıyla da insan davranışlarını en çok etkileyen ve belirleyen unsurlardan biridir. Farklı dinlere ve hatta aynı dinin farklı mezhep ve tarikatlarına mensup kişilerin davranışları önemli ölçüde farklılık gösterir. Örneğin inançlı bir Müslüman domuz eti yemez ve içki içmezken, inançlı bir Katolik Hristiyan asla boşanmaz.<sup>155</sup>

İnsanların, duyuları (işitme, görme, koklama, dokunma ve tatma) yardımıyla elde ettikleri bilgileri bir araya getirerek anlamlandırmalarına, kanaat, varsayım ve fikir oluşturmalarına algılama denir. Algılar da davranışlar üzerinde etkilidirler. Örneğin doğup büyüdüğü ve yaşadıkları çevreden kaynaklanan kültürel önyargıları

<sup>154</sup> Hüseyin Emin Sert, *Kültür ve Davranış*, <http://www.eminsert.org/component/content/article/54-insani-ve-sosyal-gelisim-merkezi/196-kultur-ve-davrans.html> (Erişim tarihi: 27 Nisan 2013).

<sup>155</sup> Ayhan Özçimbit, *İnsan ve Davranışlarının Analizi*, 12 Kasım 2012, <http://blog.milliyet.com.tr/insan-ve-davranislarinin-analizi/Blog/?BlogNo=388844> (Erişim tarihi: 27 Nisan 2013).

ile önceden öğrendiklerinden oluşan bilgisel önyargıları vardır. Önyargılar, davranışları önemli ölçüde ve genellikle olumsuz etkilerler. Bu önyargıların üst kademesinde ise tutumlar yer alır. Tutum, bir bireye atfedilen ve onun bir psikolojik objeyle ilgili düşünce, duygu ve davranışlarını düzenli bir biçimde oluşturan eğilimdir. Yani tutum, gözle görülür bir özellik değil, bireyin davranışlarından çıkarım yapılarak o bireye yüklenebilecek bir eğilimdir. Tutumların oluşumu da davranışlar gibi genetik, fizyolojik, psikolojik ve sosyolojik çok sayıda etkenin katkısıyla gerçekleşir.

Yapılan araştırma ve deneyler, tutumların her zaman beklenen bir davranışla sonuçlanmayabileceğini göstermektedir. Bunun üzerine tutumların hangi durumlarda davranışları belirleyici rol oynadığı araştırmaları ağırlık kazanmış ve tutumlardan kaynaklanan davranışların tahmin edilebilmesi için, davranışın gerçekleştiği şartlar, zaman ve yer ile tutumun güç derecesi, tutumun ulaşılabilirliği ve tutumun farkında olup olunmadığının önemli olduğu sonucuna varılmıştır. İnsan davranışlarında belirleyici rol oynayan tutumların, her türlü karşı istihbarat faaliyetinde göz önünde bulundurulması lazım gelir.<sup>156</sup>

Duygular, olumlu veya olumsuz olarak çok şiddetli yaşandıklarında organizmada bir heyecana neden olurlar. Bu heyecanlar da fiziksel ve davranışsal olarak bir dışa vurum gösterir. Heyecanlanan kişilerde; kan basıncı ve kalp atış hızında değişim, tüylerin dikleşmesi, göz bebeklerinin büyümesi, mide ve bağırsak bozulmaları, terleme vb. otonom sinir sisteminin gerçekleştirdiği ve kontrol altına alınamayacak\* fizyolojik tepkiler gözlemlenir. Heyecanlar, özellikle bilinçsiz davranışların oluşumunda önemli pay sahibidirler ve insanlar heyecanlı oldukları zamanlarda kontrolsüz ve sonradan pişman olabilecekleri davranışları daha kolay sergilerler. En başarılı istihbaratçıların duygularını iyi gizleyebilen, tavır ve hareketleriyle hiçbir şüphe uyandırmayan kişiler olduğunu unutmamak gerekir.<sup>157</sup>

Görüldüğü gibi aslında ihtiyaç, tutum, değer, kişilik, kültür, algı, beklenti, kalıtım vb. davranış şekillendiren her türlü biyolojik, psikolojik ve sosyolojik olgu birbirinden bağımsız ve ayrı ayrı ele alınabilecek unsurlar değil tamamen iç içe geçmiş ve birbirlerini dahi etkileyen unsurlardır.

<sup>156</sup> Eren, **a.g.e.**, s. 69; Özdağ, **a.g.e.**, s. 202, 203; Çiğdem Kağıtçıbaşı, **Yeni İnsan ve İnsanlar**, Evrim Yayınevi, İstanbul, 2004, ss. 102–114; A. Can Baysal ve Erdal Tekarslan, **Davranış Bilimleri**, Avcıol Basım Yayın, İstanbul, 2004, s. 309.

\* Kontrol altına alınamayan bu fizyolojik tepkiler, halk arasında yalan makinesi olarak bilinen makinelerin temel çalışma mantığını oluştururlar.

<sup>157</sup> Baymur, **a.g.e.**, ss. 81–85.

İnsan davranışlarını etkileyen, belirleyen, şekillendiren bütün bu etkenleri kısaca ele aldıktan sonra şekillenmiş insan davranışlarının karşı istihbarata olan etkilerini ortaya koymakta fayda vardır.

### 3.2. İNSAN DAVRANIŞLARININ KARŞI İSTİHBARATA ETKİLERİ

Her insan, kendisini diğerlerinden ayıran ve tahmin edilemeyecek kadar fazla fiziksel, zihinsel ve duygusal özelliğe sahiptir. Ayrıca doğuştan getirilen farklılıklara ek olarak yetiştirme ve eğitim süreçlerinde karşılaşılan şartlar, yaşanan deneyimler ve çevresel faktörler de çok farklı olduğundan farklılaşma artarak devam eder. İnsanlar değişik, ilginç ve özgün yönleriyle fark edilirler, tanınırlar ve hatırlanırlar. Hatta birçok insan için diğerlerinden farklı olabilmek, bir meziyet olarak kabul edilir. Ancak insanları değerli kılmasının yanında karşı istihbarat bakımından insanın en riskli etken olmasının temel nedeni de taşıdığı farklı özelliklerdir.

“Karşı casusluk ajanlarının söylediği gibi, en dikkatli casusların bile ölümcül hata yapmalarının nedeni hep küçük insan zafiyetleri olmuştur.”<sup>158</sup> Örneğin SSCB adına Almanya’da çalışan zamanın önemli casuslarından Richard Sorge, Japon bir kadına olan tutkulu aşkının bedelini hayatıyla ödemiştir.<sup>159</sup>

Her türlü karşı istihbarat ve dolayısıyla güvenlik sistemi, insanlar tarafından oluşturulur ve insanlar tarafından güvence altına alınır. Sistemlerin oluşturulması ve güvence altına alınması, hiçbir zaman tam anlamıyla yeterli değildir. İşin bir de uygulayıcı yani personel boyutu vardır. İKK önlemleri, personel tarafından tam olarak bilinmiyorsa, uygulanmıyorsa veya benimsenmemişse en ileri teknoloji kullanılarak kurulan bir karşı istihbarat sisteminin dahi başarılı olmasından bahsedilemez. Günümüzde karşı istihbarat faaliyetlerindeki her türlü teknik ve insansız sistemlere doğru giden hızlı gelişmeye rağmen insan faktörünün etkisi hâlen vazgeçilmezdir.

O hâlde karşı istihbaratta en önemli unsurun personel yani insan olduğu söylenebilir. İnsanı karşı istihbaratın en önemli unsuru yapan başlıca neden ise insanın karşı istihbaratın en zayıf ve en riskli parçası olmasıdır. Önlemler en üst seviyede alınsa bile insanın içinde yer aldığı her sistemde bir aksaklık meydana

<sup>158</sup> Niyazi Tılısbık ve Özdemir Akbal, *Intelligence: İstihbarat ve Türkiye*, İKİA Yayıncılık, İstanbul, 2006, s. 157.

<sup>159</sup> Avcı, *İstihbarat Oyunları... a.g.e.*, s. 273.

gelmesi ve bir açığın oluşması mümkündür. Çünkü insan bir makine gibi düşünmeden, hissetmeden ve hiçbir dış etkenden etkilenmeden monoton ve otomatik olarak çalışamaz. Birçok kararı ve davranışı, önemli ölçüde, fizyolojik, psikolojik, sosyolojik, duygusal ve zihinsel yapısının etkisinde şekillenir.

Bu yapı, insanı zaman zaman (hatta sıkça) hataya sevk edebilir. Sonuç olarak bu hatalar ve insanların kuralları tam olarak uygulamaması, sistemlerde ciddi güvenlik açıklarının oluşmasına sebep olabilir. Yapılacak basit bir ihmal ya da hata, bütün İKK önlemlerini boşa çıkarabilir. Bu da, İKK önlemlerinin odağında yer alan insanı, İKK zincirinin en zayıf halkası konumuna sokar.

İnsanın fizyolojisi, psikolojisi ve sosyolojisi ile bazı teknikler bilindikten sonra insana her istenilen yaptırılabilir. İnsanların gereksinimleri ve dürtüleri dil, din, ırk ayrımı gözetmeksizin aynıdır yani evrenseldir. Sadece bu gereksinimlerin ve dürtülerin şiddeti ve dışa vuruluş şekli farklıdır. İşte burada düşkünlükler ortaya çıkar. Her insanın düşkünlükleri değişkenlik arz eder. İstihbaratçıların ustalıkları da, bu düşkünlüklerin keşfedilip iyi değerlendirmesinde kendini gösterir.

En son teknolojik ve teknik olanaklar kullanılmış olsa dahi karşı istihbarat sisteminin en büyük bilinmeyişi, bireysel olarak davranışı kesin bir şekilde tahmin edilemeyen insandır. İnsanlar, çeşitli nedenlerle kasıtlı olarak bir casusluk faaliyeti içinde olabilecekleri gibi kasıtsız ama hatalı davranışlarından dolayı önemli bilgilerin düşmanların eline geçmesine de sebep olabilirler. Dolayısıyla bilginin korunması için gizli bilgileri bilme veya bunlara kolaylıkla yaklaşabilme olanak ve yetkisine sahip insanlar üzerinde önemle durulması kaçınılmazdır. Organizasyonlarda İKK açısından ideal bireylere sahip olmanın önemli şartlarından birisi de bilimsel olarak davranışların şekillendirilmesi yani bireyin istenilen davranışlara yönlendirilmesidir. Bu tür kişiler, eğitim ve durumsal farkındalık düzeyi yüksek, sadakat duygusu gelişmiş ve bilinçli bireyler olmalıdır.

İnsan, etkilenen ve etkileşen bir varlık olarak sosyal bilimlerin temel araştırma konusudur. Bu bilimlerin temelinde insanı anlama ve davranışlarının altında yatan nedenleri mantıksal bir çerçeveye oturtabilme arayışı vardır. Karşı istihbaratta insan etkeninin doğru şekilde değerlendirilebilmesi için insan davranışını konu alan biyoloji, psikoloji, sosyal psikoloji, sosyoloji gibi bilim dallarından en üst seviyede faydalanılmalıdır. Bu şekilde insan tutum ve davranışlarının sebeplerini oluşturan gereksinimlerin ve dürtülerin bilinerek davranışların yani tepkilerin anlaşılıp

öngörülmesi, davranışları şekillendirmek, davranışları önlemek veya son çare olarak davranışlara önlemler geliştirmek mümkün olabilir.

Alınacak her türlü önleme rağmen, işinin uzmanı istihbaratçıların kötüye kullanabilecekleri insana özgü düşkünlükleri tamamen ortadan kaldırmak olanaksızdır. Bu düşkünlüklerin davranışlar üzerindeki belirleyici rolü de dikkate alındığında yetenekli istihbaratçıların işi aslında o kadar da zor değilmiş gibi görünmektedir.

### **3.2.1. İstihbaratçıların İstismar Edebilecekleri Zayıflıklar ve Davranışlar**

Yabancı bir istihbarat görevlisinin belirlemeye (kancalamaya) çalışacağı ve kötüye kullanabileceği zayıflıklar ve davranışlar gösteren kişiler, genellikle şu özelliklere sahip kişilerdir:<sup>160</sup>

- Genel kabul gören sosyal kuralları ihlal etme çabası içindeki kişiler (yalancı, hilebaz, dolandırıcı, hırsız, uyuşturucu satan vb.),
- Yolsuzluk, dolandırıcılık, hırsızlık, zimmetine geçirme, insan kaçakçılığı vb. suçlara karışmış olanlar,
- Organize suç örgütleri ve terör örgütleri ile ilişkisi bulunanlar,
- Serüvene ve risk almaya eğilimli ve kolay yoldan zengin olma çabası içindeki kişiler,
- Övülme, kendisini önemli hissetme ya da zeki bir kişi olarak tanınma isteği ve hırsı bulunanlar,
- Mesleki disiplini ve çalışma isteği olmayanlar (mesai saatleri içerisinde internet, borsa takibi, şans oyunları vb. gibi görevle ilgisi olmayan faaliyetlerle uğraşanlar),
- Yaşadığı ülkenin yönetim biçimini veya genel politikasını benimsemeyen ve ideolojik olarak farklı düşünenler,

---

<sup>160</sup> Defence Human Resource Activity, **a.g.e.**, ss. 13–21.

- Ulusal ve manevi deęerleri zayıf kiřiler,
- Yöneticilere ya da işverene öfke veya kin besleyenler,
- Kendisine veya başka bir yakınına çeřitli konularda (konut, iş, saęlık, eęitim vb.) yararlar ve yardımlar saęlanan kiřiler,
- Karřılanamayan masrafları olan kiřiler (çocukların okul masrafları, çocuk veya eşin ciddi bir hastalığının olması, boşanma sonucu doğan masraflar, eşin işini kaybetmesi sebebiyle maddi gelir azalması, büyük kumar kayıpları ve emekli yaşantısına maddi anlamda hazırlıksız şekilde emekli olmak ya da iflasa yakın olma riski gibi herhangi bir nedenle paraya acil ihtiyaç gerektiren bir duruma düşenler),
- Baskıya ve sindirilmeye karşı hassasiyet gösterdikleri belli olan ürkek kiřiler,
- Toplum tarafından veya kendi kendini değersiz ve işe yaramaz olarak nitelendiren kiřiler,
- Uyuřturucu kullanımı, aşırı alkol kullanımı, aşırı kumar ve şans oyunları oynamak gibi kötü tutkunlukları bulunanlar,
- Cinsellięe aşırı ve deęiřik boyutlarda ilgisi olanlar ile ahlaki çöküntü içinde olanlar (çocuk, yaşlı vb. sömürüsü gibi),
- Gerçekte var olan veya olmadığı hâlde varmış gibi algıladıkları kötü muamele vb. sebeplerle organizasyona sadakat duygusunu yitirenler veya baęlılık ve sadakat gibi duyguları hiç olmayanlar,
- Düşüncesiz ve toy kiřiler.

### **3.2.2. Düşkünlükleri ve Davranışları Şekillendirme Yöntemleri**

İnsan düşkünlüklerini ve davranışlarını şekillendirmekte kullanılan tekniklerin tamamı, özünde zorlayıcı niteliktedir. Zira ortada olmayan bir davranış biçiminin toplumda ya da bireyde yerleştirilmesi için çaba harcanıyor olması, uygulama hissettirilmeden ya da doğal bir süreçle yapılsa bile zorlayıcı kabul edilmelidir.

Bu tekniklerin genel amacı, kişiye dışarıdan güçlü bir psikolojik baskı uygulayarak direnme gücünü zayıflatmak ve direnç düzeyinde geri çekilme sağlayarak davranışta bir seviye geri gitmektir. Bu sayede kişinin direnç gösterdiği davranış biçiminden, işbirliği yaparak bilgi alınabilecek seviyeye gelmesi beklenmektedir.

CIA'nın 1983 yılında çıkardığı İnsan İstismarı Eğitim Kitapçığı'nda insanların davranış ve düşüncelerinin, zorlayıcı ve zorlayıcı olmayan birtakım yöntemlerle istenilen yöne çekilebileceği vurgulanmaktadır. Özellikle sorgulamalarda kullanılmak üzere belirlenen bu yöntemler, genel olarak davranışların yönlendirilmesi için de rahatlıkla kullanılabilir. Yöntemlerin sayısı ve içeriği, yöntemleri uygulayanların hayal gücüyle ve yetenekleri ile sınırlıdır yani sınırsızdır.

Zorlayıcı olmayan yöntemlerin birçoğu hemen herkes tarafından bilinir hâle gelmiştir. Yine de, “Biz zaten her şeyi biliyoruz, bir de senden dinleyelim.”, “Arkadaşların her şeyi anlattı.”, “Aslında senin bir suçun yok.” gibi cümlelerle başlayan ve herkesçe bilinen zorlayıcı olmayan yöntemlerin başarısı, yetenekli uygulayıcılar sayesinde hâlen çok yüksektir.<sup>161</sup>

Zorlayıcı yöntemler ise, yüzyıllardır kullanılagelen kökleşik yöntemler olmakla birlikte, henüz kamuoyu tarafından bilinmeyen, duyulmamış ve hayal bile edilemeyecek yöntemlerin olduğu da bir gerçektir. Bunun en önemli sebeplerinin başında uygulanan yöntemlerin çoğunun insan haklarına aykırı ve dolayısıyla yasa dışı olmaları gelmektedir. Bu yöntemler, bilgi alınmak istenen kişiyi fiziksel olarak güçsüz bırakmak veya bırakmakla tehdit etmek (aşırı yormak), yeme, içme, uyuma gibi gereksinimlerden yoksun bırakmak, her türlü ihtiyacın karşılanması için bir bağımlılık oluşturmak, yoğun korku ve endişe tesis etmek gibi prensiplere dayanır.

Özellikle fiziksel acı oluşturmayı ve psikolojik çöküntü yaratmayı hedefleyen birtakım alet ve makinelerin, çeşitli kimyasalların (ilaçlar, anestezi, uyuşturucu vb.), hipnoz ve telkin gibi yöntemlerin kullanıldığı bilinmektedir.<sup>162</sup> Günümüzde istihbarat örgütlerinin üzerine en çok kafa yordukları çalışmalar, “zihin kontrolü” üzerinedir. Bu konuda önemli gelişmeler kaydedildiği de bilinmektedir.

Normal sayılan insan davranışlarının karşı istihbarata olan sınırsız etkisini

<sup>161</sup> CIA Manual, *Human Resource Exploitation Training Manual*, 1983, ss. J-4–J-12.

<sup>162</sup> CIA Manual, *KUBARK Counterintelligence Interrogation*, Create Space Independent Publishing Platform, Washington D.C., 1963, s. 2.

ortay koyduktan sonra bir de normal olmayan davranışların karşı istihbarata etkilerine değinmekte yarar vardır. Zira ruhsal rahatsızlıkları bulunan kişilerin sömürülebilmesi, ruhsal açıdan sağlıklı sayılan kişilere göre daha kolay olabilir.

### 3.3. RUHSAL BOZUKLUKLARIN KARŞI İSTİHBARATA ETKİLERİ

Burada ele alınacak husus, ruh sağlığı bozuk kişilerin karşı istihbarata olumsuz etkilerinin neler olabileceğinin belirlenebilmesidir. Bu amaca ulaşabilmek için de ruh sağlığı bozuk kişilerin olası rahatsızlık belirtileri ile ruh bilimciler tarafından ortaya konmuş olan davranışlarını ele almak lazım gelir. Zira istihbaratçıların eleman temininde en çok aradıkları kişiler arasında davranışları doğal birer düşkünlük teşkil eden ruh sağlığı bozuk olan kimseler önemli yer tutar.

Davranış veya duyguların ruhsal bozukluk olarak nitelendirilebilmeleri için uzun sürmeleri veya şiddetli yaşanmaları gereklidir ancak kalıtsal ve çevresel birçok koşulun da bozuklukların oluşumunda etkili faktörler olduğu unutulmamalıdır.<sup>163</sup> Her ruhsal rahatsızlığın toplum içinde kendini belli edecek yoğunlukta ve şiddette yaşandığı da söylenemez. Bazı ruh sağlığı bozuk kişilerin, ruhsal açıdan sağlıklı insanlar arasından seçilmeleri dahi oldukça zordur.

Bu bağlamda ruhsal rahatsızlıklardan, karşı istihbarat için önemli görülenlerini, olası davranışlarını ve neden önemli olduklarını kısaca ele almakta yarar vardır. Bu rahatsızlıklardan birçoğunu kısa süreli ve düşük şiddette, yani ruhsal rahatsızlık olarak değerlendirilmeyen boyutta hemen herkesin yaşayabileceği söylenebilir. Dolayısıyla ruhsal bozukluk neticesinde sergilenebilecek davranışları ortaya koymak karşı istihbarat sistemi için faydalı olacaktır. Yapılacak tespit ve açıklamaların davranış bilimleri açısından bir hedefi veya değeri olmayabilir ancak karşı istihbarat açısından önemli olduğu düşünüldüğü için burada yer verilmiştir.

#### 3.3.1. Kişilik Bozuklukları

Amerikan Psikiyatri Birliği, Mental Bozuklukların Tanısal ve Sayımsal El Kitabı'nda kişilik bozukluklarını paranoit, şizoit, şizotipal, anti sosyal, sınırda (borderline), histrionik, narsisistik, kaçınan (çekingen), bağımlı, obsesif–kompulsif ve pasif–agresif kişilik bozukluğu olmak üzere on bir gruba ayırmaktadır.<sup>164</sup>

<sup>163</sup> Özcan Köknel, *Günlük Hayatta Ruh Sağlığı*, Alfa Kitabevi, İstanbul, 2009, s. 1.

<sup>164</sup> Köknel, *a.g.e.*, s. 263.

Kişilik bozuklukları tamamen birbirinden bağımsız ve farklı özellikler sergileyen rahatsızlıklar değildir. Birden fazla bozukluğun davranışlarını aynı anda sergileyen kişiler olabilir. Ortaya çıkmalarında birçok kalıtsal ve çevresel etken rol oynar. Uç sayılabilecek davranışlar dışındaki davranışları çok da normal dışı davranışlar olmadığından dolayı kişilik bozukluklarının belirlenmesi oldukça güçtür. Erkeklerde, kadınlardan 4–5 kat daha sık görülebilen kişilik bozukluklarının toplumsal yaygınlık oranı ise yüzde beş ila yirmi arasındadır. Psikologlar için birer hastalık olan bu bozukluklar, karşı istihbarat için birer bireysel zayıflık ve zafiyet olarak nitelendirilebilirler.<sup>165</sup>

### 3.3.1.1. Paranoit Kişilik Bozukluğu

Paranoyanın en genel tanımı, kişinin çevresine karşı sürekli bir güvensizlik hissetmesi, aşırı kuşkulu olma durumudur. Paranoit kişi, yakınlarının ve yabancıların güvenilirliğini ve sadakatini sorgular. Başkalarına anlatılmasından korktuğu için kimseye kendisiyle ilgili konulardan bahsetmez. Sıradan konuşmalar ve olaylardan kendini küçültücü ya da tehdit edici anlamlar çıkarır. Yani alıngandır ve çabuk incinir. Herhangi bir dayanağı olmadığı hâlde, başkaları tarafından sömürüleceği ya da kendisine zarar verileceği inancı içindedir. Kendisine yapılan hareketlere derhâl karşılık verir ve asla affetmez.<sup>166</sup>

Paranoya ciddi bir güvenlik konusudur ve paranoit kişiler, işverenini veya hükümetini kolayca düşman olarak görerek intikam ve kin duyguları ile hareket edebilirler. İntikam arzusu casusluk, sabotaj, terörizm, şiddet içeren saldırılar ve diğer yasa dışı davranışları tetikleyebilir. Bilinen birçok casusun, kindar özellikte olduğu örneklerle (İlyas Bazna örneğinde olduğu gibi) sabit bir gerçekliktir.<sup>167</sup>

Öte yandan paranoit kişilerin güvenmezlik ve kuşkuculuk özelliklerinden dolayı kancalanmaları da kolay değildir. Zira insanların kendilerine yakınlaşmasının altında bir takım çıkarlar olduğunu, kendilerinin çok özel ve çok iyi olduklarını, hiç kimsenin onları sevmediğini düşünürler. Ayrıca kendilerine iyi davrananları çıkarıcı, kötü davrananları ise düşman olarak mimlerler.<sup>168</sup>

<sup>165</sup> Saliha Bayat ve Nebile Kübra Şengül, *Kişilik Bozuklukları*, 2007, s. 40, <http://bilka.org.tr/upload/file/KISILIK%20BOZUKLUKLARI.doc> (Erişim tarihi: 30 Nisan 2013).

<sup>166</sup> Engin Geçtan, *Psikodinamik Psikiyatri ve Normaldışı Davranışlar*, Metis Yayınları, İstanbul, 2004, ss. 246–247.

<sup>167</sup> Defence Human Resource Activity, *a.g.e.*, s. 39.

<sup>168</sup> Bayat ve Şengül, *a.g.e.*, s. 8.

Karşı istihbarat yönünden doğru sonuçlara ulaşabilmek için olaylara ve davranışlara çok yönlü bir bakış açısıyla yaklaşarak değerlendirmek daha doğrudur. Paranoit davranış, tamamen olgusal bir temele sahip olabilir. Yani bir kişinin sürekli dinleme cihazları veya gizli kameraları arıyor olması sıradan bir paranoit davranış olabileceği gibi yasa dışı faaliyet içinde bulunmanın verdiği aşırı endişe ve korkuların bir yansıması da olabilir.<sup>169</sup>

### 3.3.1.2. Şizoit Kişilik Bozukluğu

Şizoit kişilik bozukluğu, toplumsal ilişkilerde çekingenlik, insanlara ilgisizlik, yakın ilişki kurmaktan kaçma ve duygusal donukluk şeklinde kendini gösterir. Şizoit kişi, dalgın, ilgisiz, içe dönük, isteksiz, çevreden kopuk bir görünüm sergiler, ilişki ve iletişim kurmada zorlanır ve ilişkileri uzun süre sürdüremez. Başkalarıyla konuşurken küçük düşmekten ve istemediği şeyler duymaktan çekinir. Bu yüzden genelde fazla konuşmaz.<sup>170</sup> Başka insanlarla birlikte olmak istemez ve zevk almaz. Toplumdan uzak ve yalnız yaşamayı sever. Duygularını dışa yansıtması içte yaşadığının çok altındadır. Sevinç, hüznün ve öfkesini dışarıdan anlamak kolay değildir ve bu tür duyguları yokmuş izlenimi verir. Başkalarının kendisi hakkındaki duygu ve düşüncesi pek umurunda değildir. Eleştiri ve övgülere karşı duyarsızdır. Rekabet, hırs gibi tutkular gerektirmeyen ve tek başına olacağı işlerde çalışmayı tercih eder.<sup>171</sup>

Sağlıklı ve uzun vadeli kişisel veya iş ilişkileri kuramamak ciddi bir güvenlik ve İKK sorunudur. Zira bu durum, sosyal aidiyet ve mesleki olarak bağlılık tesis etme konusunda ciddi bir zafiyeti işaret eder. Bu konuda en iyi örneklerden biri, Christopher John Boyce'dur. Boyce, babası sayesinde çalışmaya başladığı gizlilik derecesi yüksek bir kurumda nüfuz edebildiği, ABD'nin çok hassas haberleşme uydusu programlarına ait bilgileri, SSCB'ye satmak suçundan 1977 yılında yakalanarak hüküm giymiştir. Boyce'u, Meksika'da SSCB büyükelçiliği önünde bir adamı öldürmek suçuyla tutuklanan ve üzerinde çok gizli bilgilerin olduğu bir mikrofilm çıkan çocukluk ve suç arkadaşı Andrew Daulton Lee ele vermiştir. Boyce'un, lise yıllarında dinî ve ulusal duygularını kaybetmeye başladığı, yakalanmadan önceki son üç yılda üç ayrı kolejden atıldığı, son iki yılda altı farklı yarı zamanlı işte çalıştığı ve bu altı işin üçünden haber dahi vermeden ayrıldığı, kaldığı evin kirasını dahi ödemediği kaçtığı, çalıştığı işlere özellikle pazartesi günleri

<sup>169</sup> Defence Human Resource Activity, *a.g.e.*, s. 40.

<sup>170</sup> Köknel, *a.g.e.*, s. 265.

<sup>171</sup> Bayat ve Şengül, *a.g.e.*, s. 12.

akşamdan kalma bir hâlde geldiği gibi bilgiler daha önceden tespit edilebilmiş olsaydı, babasının katkısıyla olsa dahi, hassas bilgilere erişebileceği bir göreve getirilmesi önlenebilirdi.<sup>172</sup>

Bu konudaki ikinci örnek, soğuk savaş döneminin en önemli çift taraflı casusu olarak anılan ve önce MI6'nın hatırı sayılır bir casus iken sonra SSCB'nin istihbarat servisi KGB için çalışmaya başlayan Kim Philby'dir. Philby, yaşamının son dönemlerinde, "İhanet etmek mi? İhanet etmek için insanın bir yere bağlanması gerekir. Oysa ben hiçbir yere ve hiçbir zaman bağlanmadım." demiştir.<sup>173</sup>

### 3.3.1.3. Şizotipal Kişilik Bozukluğu

Şizotipal kişiler, geleceği görme, altıncı his, gaipden haber alma gibi doğaüstü güçleri olduğuna inanırlar. İnsanların düşüncelerini okuyabilme yeteneğine sahip olduklarını düşünürler. Yakın dostluklar ve düzgün ilişkiler kuramazlar. Özellikle tanımadıkları kişilerin oluşturduğu sosyal topluluk ve ortamlarda aşırı tedirgin olurlar. Dış görünüşleri sıra dışıdır. Alışlagelmişin dışında hareket ve konuşmalar yapabilirler.<sup>174</sup>

Sıra dışı ve aşırı giyimiyle etrafındakilerin ilgisini çekmeyi çok seven ve hislerine alabildiğine güvenen ünlü casus Mata Hari bu bozukluk için iyi bir örnek olabilir.<sup>175</sup>

### 3.3.1.4. Anti Sosyal Kişilik Bozukluğu

Anti sosyal kişiler, uyumsuz, düzensiz ve saldırgan bir hayat sürerler. Kendilerini beğenen kibirli kişilerdir. Sürekli suç işlerler ve başları derde girer. Kendilerine ve başkalarına zarar verebilirler ve bundan zevk duyarlar. Sinirli ve kavgacıdırlar. Bunlarda nadiren bir vicdan azabı veya pişmanlığa rastlanabilir.<sup>176</sup>

Anti sosyal kişilik bozukluğu olan kişiler, diğer insanları hafife alarak kendi çıkarlarına hizmet etmeleri için onları kullanırlar. Sosyal kurallara uymamak ve şiddetle karşı çıkmak en belirgin davranışları arasındadır. Sistemi yakalanmadan

<sup>172</sup> Defence Human Resource Activity, *a.g.e.*, s. 38.

<sup>173</sup> Aydın, *İşte... a.g.e.*, s. 78.

<sup>174</sup> Bayat ve Şengül, *a.g.e.*, s. 15.

<sup>175</sup> Ercan Arıklı, *Başlangıcından Bugüne Kadar Dünya Casusluk Tarihi*, Cilt: 1, Artel Yayınları, İstanbul, 1974, s. 162.

<sup>176</sup> Geçtan, *a.g.e.*, ss. 259–262.

bozmaktan veya sekteye uğratmaktan zevk alırlar. Sıkça yalan söylerler. Çalıştıkları işlerde uzun süre kalamazlar. Çalma, aşırma, vergi kaçırma, vandalizm\* (tahripçilik), park ücretlerini ödememe, saldırgan ve dikkatsiz araç kullanma, parası olduğu hâlde faturalarını ödememe, kolayca kavga çıkarabilme, hafifmeşreplik, cinsel taciz, hayvanlara eziyet etme, çocuk / eş / yaşlı sömürüsü gibi örnekler anti sosyal davranışlara örnek olarak verilebilir.

Serüven ve risk arayışı da, anti sosyal davranışın belirgin bir özelliğidir. Anti sosyaller riskleri görmezden gelebilirler, önemsiz görebilirler ya da çok zeki ve yetenekli oldukları için risklerin kendileri için geçerli olmadığını düşünebilirler. Dolayısıyla risk fırsatlarını asla geri çevirmezler. Yakalanmadan kuralları ihlal ederek bazı şeyler yapabildiklerin görmek onlar için karşı konulamaz bir hazdır. Sırf bu serüven ve risk tutkuları bile anti sosyal kişilik bozukluğu olan kişileri casus olmaya eğilimli hâle getirmeye yeterlidir. Bu tür kişiler karşı istihbarat açısından ciddi ve potansiyel bir tehdit oluştururlar. Görevleri gereğinin ötesinde edebildikleri bilgileri, sırf zevk aldıkları için bile sızdırabilirler. İKK önlemlerini bir kurallar bütünü olarak düşünürsek anti sosyal kişilik bozukluğu olan kişilerin bu kuralları bozmak için faaliyetlerde bulunabilmeleri olasıdır.

Bu şartları en iyi gösterecek örneklerden birisi olan SSCB adına casusluk yapan Richard Sorge'un boşandığı eşi, onun alkol bağımlısı bir anti sosyal olduğunu öne sürmüştür.<sup>177</sup> Yine, SSCB adına ABD Deniz Kuvvetleri'nde çalışan başka bir casus olan John Walker, gençliğinde kullanılmış lastikleri yüksek tepelerden, aşağıdan geçen araçlara fırlatan, okul camlarına taş atan, cüzdanlardan ve bir yerlere asılmış ceketlerden para çalan, kiliselerde fakirlere yardım toplanan kutulardan para aşırın, yangınlar çıkaran ve araçların farlarına ateş eden bir kişidir. On yedili yaşlarında altı soygun girişimi olduğunu itiraf etmiştir. Kardeş kadar yakın olduklarını öne süren bir çocukluk arkadaşı Walker için, "kurnaz, zeki, akıllı, cana yakın ve özde tam bir şeytandır" ifadelerini kullanmıştır. Neredeyse bütün ailesini ve arkadaşlarını casusluk yaparken kullanan ve onları da angaje etmek için çalışan Walker, yakalandıktan sonra kendisini kullandıkları gerekçesiyle ailesini ve arkadaşlarını suçlamıştır. Tek ve en büyük hatasının, sonuçta kendisini mahvedecek olan zayıf kişilerin etrafına toplanmasına izin vermek olduğunu ve içine düştüğü durumda kendisinin asıl kurban olduğunu söylemiştir.<sup>178</sup>

\* Tahripçilik (Vandalizm); bir bireyin, kamu mallarını ya da hiç tanımadığı başka kişilerin mallarını hedef alan, bilinçli ve kasıtlı olarak zarar verici davranışlarda bulunma eğilimidir.

<sup>177</sup> Avci, *İstihbarat Oyunları... a.g.e.*, s. 274.

<sup>178</sup> Defence Human Resource Activity, *a.g.e.*, s. 31.

### 3.3.1.5. Sınırdaki (Borderline) Kişilik Bozukluğu

Sınırdaki kişilik bozukluğu olan kişiler, terk edilme ve yalnızlık korkusunu aşırı denebilecek boyutlarda yaşarlar. Her konuda kararsızlık içine düşerler. Sınırdaki kişilik bozukluğu olan kişiler; şizotipal, anti sosyal, narsisistik ve histrionik kişilik bozuklukları ile benzer tanı ölçütleri sergilerler.<sup>179</sup>

Çoğunlukla kestirilemez ve dengesiz davranışlar sergileyen sınırdaki kişilik bozukluğu olan kişiler, sürekli bir kriz durumundadırlar. Özellikle kendilerine, nadiren de başkalarına, zarar verici eylemlere başvururlar.<sup>180</sup>

Şizotipal, anti sosyal, narsisistik ve histrionik kişilik bozuklukları ile tanı ölçütleri benzer olduğu için casus örnekleri de örtüşürülebilir.

### 3.3.1.6. Histrionik Kişilik Bozukluğu

Histrionik kişilik bozukluğu olan kişiler, duygularını abartılı ve çoğu zaman şartlarla uyumsuz coşkunlukta yaşarlar. Övülmek, beğenilmek ve ilgi görmekten hoşlanırlar. Olayları ve durumları dramatize etme eğilimleri vardır. Yeni tanıştıkları kişilere sarılabilir, sıradan durumlara ağlayabilirler. İsteklerinin derhâl yerine getirilmesini isterler, kaygısız ve çokbilmiş davranırlar. Davranış ve sözlerinde abartı, saptırma, yalan ve uydurmaya sıkça rastlanır. Sorumluluk almak istemezler. Etkilenmeleri kolaydır.<sup>181</sup>

Geçmişteki ünlü casuslar arasında yerini almış olan Arabistanlı Lawrence, yaptığı her işi abartması ve başkalarının yaptığı işleri de kendisi yapmış gibi göstermesi sayesinde, hakkı olmadığı ve gerçekleri yansıtmadığı hâlde, birçok casusun ortak bir –İngiliz casuslar açısından– başarısıyla Arabistan’da başlayan isyanların “ilham perisi” ve “taçsız kral” olarak tanınmayı başarmıştır.

### 3.3.1.7. Narsisistik Kişilik Bozukluğu

Narsisizm (özseverlik), kişinin kendisini çok değerli ve eşi bulunmaz olarak görmesidir. Narsisistik kişilik bozukluğu olan kişiler, hep beğenilen, onaylanan ve

<sup>179</sup> Bayat ve Şengül, *a.g.e.*, s. 23.

<sup>180</sup> M. Hakan Türkçapar ve Banu Işık, “Borderline Kişilik Bozukluğu”, *Psikiyatri Dünyası*, 2000, 4, s. 47.

<sup>181</sup> Köknel, *a.g.e.*, ss. 269–270.

övülen olmak isterler. Kendilerini beğenmiş ve kibirli bir yapıları vardır. Kendilerine saygı göstermeyen herkesi küçümser ve hor görürler. Beklentilerine ulaşamadıklarında öfkelerine hâkim olamaz, saldırganlaşır ve çökerler. Her şeyin kendileri için var olduğunu düşünürler. Başkalarına sürekli imrenirler ve kıskançlık duyguları yüksektir. Başarısızlıkları başarı gibi göstermek ve kendilerini haklı çıkarabilmek için gerçekleri çarpıtırlar.<sup>182</sup>

Narsisistik kişilik bozukluğu için en iyi örneklerden biri, ABD Deniz Kuvvetlerinde İstihbarat Çözümlemecisi olarak görev yaparken İsrail adına casusluk yaptığı için yakalanan Jonathan Jay Pollard'dır. Genç yaşlardan itibaren İsrail'i düşmanlarından koruyan bir strateji ustası ve süper kahraman olma hayali kuran Pollard, İsrail'in karşı karşıya olduğu tehditleri bertaraf etme ve bu ülkeye hizmet etme konusunda takıntılı bir hâle gelir. Kolej yıllarında arkadaşlarına kendisinin çifte vatandaşlığı olduğunu ve İsrail Ordusunda bir albay olduğunu, hatta okul masraflarını bile onların karşıladığını söylerken yakalandıktan sonra bütün bunların bir şakadan ibaret olduğunu ve kendisini kimsenin ciddiye almadığını söylemiştir. Çözümlemecilik görevini sürdürürken, palavracı, kendini beğenmiş ve çokbilmiş tavırlarından dolayı arkadaşları arasında pek sevilen bir kişi olmayan Pollard, kendisini yakalamaya çalışacak kişilerden çok daha zeki olduğu için asla yakalanmayacağını düşünürken, kendisini olduğundan daha önemli göstermek için söylediği bir yalanın tespit edilmesi neticesinde yakalanmıştır.<sup>183</sup>

Anti sosyal kişilik bozukluğu için verilen John Walker örneği, narsisistik açıdan da iyi bir örnektir. Zira Walker ile 160 saate yakın mülakat yapan ve onu iyi tanıyan bir yazarın kanısı onun, utanmaz, doğru–yanlış ve ahlak kavramlarından yoksun, sadece kendi istek ve gereksinimlerini düşünen ve istediği anda gerçekleştirmelerini bekleyen, bu uğurda vatanına ihanet eden, eşini ve çocuklarını duygusal olarak yıkıma sürükleyen, arkadaşlarını kandıran, sonuç olarak da kendisini diğer insanlardan farklı değil ama daha akıllı gören birisi olduğu yönündedir.<sup>184</sup>

### 3.3.1.8. Kaçınan (Çekingen) Kişilik Bozukluğu

Çekingen kişiler sıkılgan, utangaç, soğuk, içine kapanık, yalnız ve korkaktırlar. Aşağılanmaktan ve yenilmekten alabildiğine korkarlar. Beğenilmeme veya

<sup>182</sup> Bayat ve Şengül, *a.g.e.*, s. 31.

<sup>183</sup> Defence Human Resource Activity, *a.g.e.*, ss. 34–35.

<sup>184</sup> *a.g.e.*, s. 32.

eleştirilme korkusuyla sosyal ortamlardan kaçınırlar. Kuruntulu bir düşünce yapısına sahiptirler. Kendilerini toplumda seilmeyen, aşağılanan ve beceriksiz kişiler olarak görürler.<sup>185</sup>

FBI'nın özel ajanı olarak yirmi yılı aşkın süre Ruslar için casusluk yaptıktan sonra 2001 yılında yakalanan Robert Hanssen, işinde ve evinde sakin ve çekingen bir hayat sürmesine rağmen çocukluk arkadaşları onun davranışlarını, önlemsiz ve fütursuz olarak nitelendirmişlerdir. Bir arkadaşı onun için, yapmayı kafasına koyduğu şey fazlasıyla riskli olsa dahi onu durdurabilecek hiçbir şey olmadığını söylemiştir. Arkadaşlarını ve kendisini tehlikeye atan davranışları gençlik ve yetişkinlik hayatı boyunca devam eden Hanssen'in, evlilik ve cinsel hayatı da benzer şekilde gelişmiştir. Eşini, eski kız arkadaşı ile aldatan, baldızına tacizde bulunan, çeşitli internet sitelerine, gerçek kimliklerini kullanarak, kendisi ve eşiyle ilgili erotik hikâyeler gönderen ve daha rahatsız edici zevkleri olan bir kişidir. Çocukluğundan itibaren KGB'nin casusluk faaliyetlerinden çok etkilenegelmiştir. FBI'daki işine, KGB ajanlarını yakalamak hevesiyle idealist bir havada başlayan Hanssen, iş arkadaşlarının Rus istihbaratına karşı koyma konusunda kendisiyle aynı coşkuyu taşımadıkları düşüncesiyle heves ve isteğini kaybetmiştir. Bu durumda kendini boşlukta hissetmiş ve eski bir hevesi tekrar canlanmıştır: Dünyanın gördüğü gelmiş geçmiş en iyi casus olmak. Önlemsizliği ve fütursuzluğu casusluk yılları boyunca devam etmiştir. Entelektüel mükemmelliğinin, FBI ve KGB ajanlarına karşı her zaman kendisini ulaşılamaz kıldığına ve çok riskli olduğunu bildiği casusluk konusunda yenilmez olduğuna inanmıştır.<sup>186</sup>

### 3.3.1.9. Bağımlı Kişilik Bozukluğu

Bağımlı kişilik bozukluğu olan kişiler, kendilerine güvenmezler. Kendi kararlarını alırken bile başkalarının desteğine gereksinimleri olduğunu düşünürler. Her türlü ilişki ve yaşantısında uyumlu, kabullenici, aşırı uzlaşmacı ve verici davranışlar sergilerler. Çoğunlukla bir konuda görüşleri yoktur, varsa da savunmaktan çekinirler. Sorumluluk almayı sevmezler.<sup>187</sup>

Bu tür kişilik bozukluğu olan kişiler, aslında casusluk için çok iyi hedefler gibi görünseler de, kendilerine olan güvensizlikleri ve desteksiz iş yapamama özellikleri

<sup>185</sup> M.Hamid Boztaş ve Mehmet Z. Sungur, "Kaçınan Kişilik Bozukluğu", *Psikoloji Dünyası*, 2001, 5, s. 72.

<sup>186</sup> Defence Human Resource Activity, *a.g.e.*, ss. 36–37.

<sup>187</sup> Geçtan, *a.g.e.*, s. 265.

nedeniyle pek tercih edilmezler.

### **3.3.1.10. Obsesif–Kompulsif Kişilik Bozukluğu**

Obsesif–kompulsif kişiler, sabit fikirli, kuralcı, aşırı ayrıntıcı ve rahatsız edecek derecede titizdirler. Gereksiz ayrıntılara takılıp asıl amaçtan saparlar, bazen işi dahi bitirmezler. Kurallara çok önem verirler, her faaliyetin bir düzen içinde yapılması gerektiğini düşünürler ve düzen ve kuralların bozulmasına ve ihlal edilmesine tahammülleri yoktur. Temizlik için uzun süreler ayırırlar ve uğraşırlar. Diğer kişileri de kendileri gibi davranmaya zorlarlar. Kolay kolay değişmeyen değer yargıları ve dünya görüşleri vardır. Bunun yanında sorumluluk duyguları aşırı gelişmiş çok çalışkan kişilerdir.<sup>188</sup>

Orta Doğu'daki mücadelede Almanların, İngilizlerin efsane saydıkları casusları Arabistanlı Lawrence'ın karşısına çıkmak üzere gönderdikleri üç casustan birisi olan Otto Von Niedermayer kendisi ve özellikle emrinde çalışanlara karşı gösterdiği takıntı seviyesinde disiplin ve katı kuralcılığıyla tanınan, hataya tahammülü olmayan bir casus olarak obsesif–kompulsif kişilik bozukluğu için iyi bir örnektir.<sup>189</sup>

### **3.3.1.11. Pasif–Agresif Kişilik Bozukluğu**

Pasif–saldırgan kişilik bozukluğu olan kişiler, üzerine düşen görev ve sorumluluklara karşı direniş gösterirler. Unutmak gibi çeşitli bahaneler öne sürerek sorumluluklarını yerine getirmekten kaçarlar. Başkalarının sandığından daha başarılı olduklarından, yanlış anlaşılmaktan ve hak ettikleri değeri görmediklerinden yakınırlar. Otoriteyi ve diğer insanları eleştirme ve küçümseme eğilimindedirler.<sup>190</sup>

Casusluk ciddi bir sorumluluk gerektirdiğinden bu rahatsızlığın görüldüğü kişilerin uygun bir casus adayı olması zordur.

### **3.3.2. Diğer Ruhsal Bozukluklar**

Kişilik bozukluklarından ayrı ya da birlikte görülebilecek ve karşı istihbarat yönünden önemli görülen diğer ruhsal rahatsızlıklar ise şunlardır:<sup>191</sup>

---

<sup>188</sup> Bayat ve Şengül, *a.g.e.*, s. 36.

<sup>189</sup> Arıklı, *a.g.e.*, s. 201.

<sup>190</sup> Geçtan, *a.g.e.*, s. 271.

<sup>191</sup> Köknel, *a.g.e.*, ss. 228–377.

- Kaygı Bozuklukları: Panik atak, fobiler, stres, uyum bozuklukları, histeri, hastalık hastalığı vb.
- Temel Gereksinim Bozuklukları: Beslenme bozuklukları (aşırı yeme, hiç yememe gibi), cinsel işlev ve davranış bozuklukları, uyku bozuklukları vb.
- Organik Ruhsal Bozukluklar: Bunama, alzheimer vb.
- Duygulanım Bozuklukları: Depresyon, mani vb.
- Madde Bağımlılıklarına Dayalı Ruhsal Bozukluklar: Alkol sarası, alkol amnezisi, çeşitli uyuşturucu ve ilaçların sebep olduğu bozukluklar vb.,

İKK açısından düşünüldüğünde, ruhsal bozuklukları tıbbi olarak teşhis edilmiş ve tedavi altına alınmış olan kişiler çok önemli değildir. Bu kişiler, genel bir personel temin ilkesi olarak, hassas bilgilere erişim kolaylığı sağlayan görevlere alınmazlar. Önemli olan davranış bozukluğu olduğu hâlde bunu belli etmeyen kişilerdir. Bu kişilerin tespit edilmesi zordur.

Özellikle kişilik bozuklukları üzerinde durulmasının temel sebebi de diğer ruhsal rahatsızlıkların daha belirgin özellikleri ve belirtileri olmasına rağmen kişilik bozukluklarında bu özelliklerin birçoğunu dışarıdan anlamak kolay değildir. Ayrıca kişilik bozukluğu göstergesi olarak belirlenmiş birçok davranış hem birbiriyle iç içe girmiş hem de zaman zaman normal kişilerin dahi gösterebilecekleri türden davranışlardır.

Her şeye rağmen İKK sistemlerinin en büyük düşmanları ruhsal bozukluğu olanlar değildir. Ruhsal olarak çok sağlıklı olmalarına rağmen farklı sebeplerle istihbarat zafiyeti gösteren ve karşı istihbaratın hedefi kişiler hâline gelen normal insanlar daha çoğunluktadır.

Öte yandan hiç hesaba katılmayan, herhangi bir motif, düşkünlük ve rahatsızlığı olmadığı hâlde bilgi veren konumuna düşen kişiler de vardır. Gafil muhbir diye adlandırılan bu kişiler, bakıldığında motif, düşkünlük veya rahatsızlık sebebiyle bilgi veren konumuna düşen / düşürülen kişilerden sayıca çok az olabilirler. Gafil muhbirlerin verdiği bilgiler, diğerlerinin verdikleriyle kıyaslanmayacak kadar değersiz de olabilir ancak istihbaratçıların ve casusların, küçük bilgilerden

büyük sonuçlar çıkarabilme yetenekleri göz ardı edilmemelidir. Mükemmele yakın bir karşı istihbarat sistemi hedefleniyorsa gafil muhbirliğin göz ardı edilmemesi ve karşı istihbarat çabasının içinde değerlendirilmesi gereklidir.

## DÖRDÜNCÜ BÖLÜM

### GAFİL MUHBİRLİK

#### 4.1. MUHBİR KAVRAMI

Muhbir kavramı da birçok istihbarat ve karşı istihbarat kavramı gibi tam olarak açıklığa kavuşmamış konulardan birisidir. Bu yüzden kesin bir tanımını yapmak da kolay değildir. Muhbir sözcüğü sözlükte, “haber ulaştırıcı, haber veren kimse veya yasa dışı olan bir durumu yetkili makamlara bildiren kimse, ihbarcı”<sup>192</sup> olarak geçmektedir.

Muhbir, kolluk güçleri ve savcılara göre, herhangi bir suçla ilgili güvenilir bilgi temin eden kişiler için kullanılan genel bir terimdir. Oysa tek bir olayı vatandaşlık görevi olarak ihbar eden kişileri “ihbarcı” olarak nitelendirmek daha doğrudur. Sorgulanarak bilgi alınan kişiler veya bir suçla ilgili tanık olarak bilgi veren kişiler de “tanık” kapsamında değerlendirilmelidir. Muhbir ise, yasa ihlalleriyle ilgili bilgi verme işini sürekli ve gönüllü bir faaliyet olarak yapan, bu işi yapmak için bir motifi olan ve genelde kimliği gizli tutulan kişidir.<sup>193</sup>

ABD Adalet Bakanlığının öncü soruşturma teşkilatı olan FBI, muhbir terimini, teşkilata gizli ve güvenilir bir yöntemle bilgi sağlayan herhangi bir gerçek veya tüzel kişi olarak tanımlamaktadır.<sup>194</sup>

Bazı yazarlar, bir istihbarat örgütünün profesyonel ajanlarının, istihbari bir amaç için bulundukları dış ülkelerde bilgi almak maksadıyla kullandıkları kişileri de muhbir olarak tanımlamaktadır.<sup>195</sup> Oysa bu kişiler, casus ya da daha farklı bir sözcükle adlandırılmalıdırlar. Çünkü eğer muhbir olsaydılar, yakalandıklarında casusluk ve vatana ihanetten değil, yasalarda suç olarak belirtilmemiş olan muhbirlik suçundan yargılanmaları lazım gelirdi.

Muhbir terimi, kendisinden herhangi bir bilgi temin edilen herkes için kullanılabilir. Ancak muhbir teriminin kapsamı düşünüldüğünde, yanlış bir kullanımdır. İşlenen veya işlenmekte olan suçlarla ilgili olarak ihbarda bulunan kişiler, muhbir tanımının dışındadır. Muhbir terimine yüklenen asıl anlam, önleyici

<sup>192</sup> Türk Dil Kurumu, **Türkçe Sözlük**, Türk Dil Kurumu Yayınları, Ankara, 2005, s. 1416.

<sup>193</sup> Fitzgerald, **a.g.e.**, s. 36.

<sup>194</sup> FBI Manual, **Manual of Investigative Operations and Guidelines (MIOG)**, 1998, s. 173-3.

<sup>195</sup> Yakın, **a.g.e.**, s. 117.

faaliyetler yani istihbarat bakımından taşıdığı anlamdır.

Bize göre, muhbir kavramı daha ziyade ülke içi ve suça yönelik istihbarat ile ilişkilendirilebilecek bir kavram gibi görünmektedir. Çünkü birçok ülkenin iç istihbarat servislerinin kullandığı ve genelde yasalarda da yeri olan bir kavramdır. Muhbirlerin faaliyetleri ve verdikleri bilgi tamamen yasal sınırlar içindedir ve sadece yasa dışı faaliyet ve oluşumlara zarar verici niteliktedir.

Dış istihbarat ile ilgili olarak ise “haber elemanı” tabirini kullanmak daha doğru olacaktır. Çünkü dış istihbarat kapsamında icra edilen bilgi verme faaliyetinin mahiyeti muhbirden farklıdır. Haber elemanı da muhbirde olduğu gibi kendisini kullanan taraf için faydalı bir iş yapar ancak –muhbirden farklı olarak– yaptığı faaliyetleri, aleyhinde çalıştığı organizasyonun yasalarını ihlal ederek yerine getirir ve faaliyetleri ortaya çıktığı anda haber elemanı olarak değil, casus olarak muamele görür.

Öte yandan haber elemanının, aldığı yüksek risk ve tehlike göz önüne alındığında, temininden kullanılmasına kadar (hem kullanan hem de kullanılan açısından) muhbire kıyasla daha üst düzey bir uzmanlık gerektirdiği ve daha özel eğitime ihtiyaç duyduğunu da ifade etmek gerekir.<sup>196</sup>

“İnsanları Casusluğa Yönelten Nedenler” başlığı altında açıklanan motif yelpazesi daha çok casusluktan önceki son dönemde bulunan haber elemanları için geçerlidir. Muhbirler için maddi motifler daha ön plana çıkarken, haber elemanlarının maddi motiflerden çok daha güçlü motiflere gereksinimleri vardır.

#### 4.2. GAFİL MUHBİRLİK OLGUSU

Gafil muhbirlik kavramı, yazında yer yer kullanılmakla birlikte, sözlüklerde ya da akademik yayınlarda herhangi bir tanımı bulunmamaktadır. Gafil sözcüğü sözlükte; “aymaz”, gafillik sözcüğü de; “çevresindeki gerçekleri görememe ve sezememe” olarak tanımlanmaktadır.<sup>197</sup>

Gafil muhbir sıfatı halk arasında, başkasının işlediği bir suç veya kabahati

<sup>196</sup> Murat Durmuş, “Özel Hayatın Korunması Hakkı ve Bu Çerçeve İstihbarat Faaliyetleri”, Sosyal Bilimler Enstitüsü, Kırıkkale Üniversitesi, Kırıkkale, 2006 (**Yayınlanmamış Yüksek Lisans Tezi**), ss. 80–81.

<sup>197</sup> Türk Dil Kurumu, **a.g.e.**, s. 722.

yetkili makamlara bildirirken, genelde kendi işlediği bir suç veya kabahati de, istemeden ortaya çıkaran kişiler için kullanılır. Ancak bu kullanım, gafil muhbirlik kavramının taşıdığı anlamı tam olarak karşılayamamaktadır.

Gafil muhbirlik, istihbarat ve karşı istihbarat bakımından, sözcüklerin teker teker sözlük anlamlarından çok daha fazlasını ifade eder. Gafil muhbir, etrafında olan bitenin, çevresindeki insanların olası amaçlarının farkında değildir. Aynı zamanda kendi yaptıklarının veya davranışlarının sonuçlarının ve bu sonuçların organizasyon güvenliğine ve bekasına ciddi tehlike oluşturduğunun da farkında değildir. Gafil muhbirlikte, istihbari değer taşıyan bilginin, bu bilgiyi elde etmek için çok hevesli olabilecek kişilere, bilinçsizce ve gönüllü olarak servis edilmesi söz konusudur.

Gafil muhbirlik, istihbarat toplama tekniklerinden sızdırma ile benzer ve farklı özellikler gösterir. Benzerlik tarafları, her ikisinde de bilgiyi veren kişilerin, yaptıklarının farkında bile olmamalarıdır. Farklılık olarak ise;

- Gafil muhbirin verdiği bilgiyi alacak olan kişinin (istihbaratçının), böyle bir bilgi verileceğinden haberi yokken, sızdırmayı yapacak olan istihbaratçı durumu bilir.
- Gafil muhbir ile bilgiyi servis ettiği kişi arasında yaşanan her şey tamamen rastlantısal ve hazırlıksız gerçekleşirken, sızdırma tekniği için detaylı bir planlama, hazırlık ve uygulama gerekir.
- Gafil muhbirin hediyesi olan bilgiyi değerlendirecek kişi, farkındalık düzeyi yüksek sıradan bir kişi dahi olabilirken, sızdırma tekniğini uygulayacak kişilerin bu konuda uzmanlık seviyesinde özel eğitim almış kişiler olmaları gereklidir.
- Basit bir benzetmeyle; sızdırma ile elde edilen bilgi emeğin karşılığı olarak alınan ücret (maaş) iken, gafil muhbirlerden alınan bilgi yerde bulunan para gibidir.

Günümüzde casusluk sektörünün alabildiğine büyüdüğü bilinmektedir. Casuslar, halk arasında dolaşarak sadece aleni konuşmalar esnasında işe yarar bilgileri toplamak suretiyle dahi çok başarılı hizmetler yapabilmektedirler. Çünkü az biraz geveze, İKK bilinci yerleşmemiş ve bildikleri sayesinde, örneğin sosyal kabul

görme peşinde koşan gafil muhbirler, tam da casusların aradığı kişilerdir.<sup>198</sup>

Yabancı turistlerin, turistik bölgelerde fotoğraflar çekmeleri kuşkusuz engellenemez. Ancak en azından ülke güvenliği için önemli olduğu bilinen tesislere yakın yerlerde fotoğraf çekilmesi engellenebilir. Bazı yasaklar ve yetkili kişilerin görevlendirilmesi ise her zaman yeterli olmayabilir. Bu önleminin sağlanabilmesi için İKK bilinci ve farkındalık seviyesi yüksek sıradan vatandaşlara ihtiyaç olduğu kesindir. Şu anki durum çoğunlukla bunun tam tersidir. Vatandaşlar bu tür bir durumu engellemek bir tarafa yardım bile etmektedirler. Güler yüzle, bazen bozuk şivesiyle, yeni öğrendiği birkaç Türkçe sözcükle, çoğunlukla da işaretlerle fotoğrafını çekmesi istendiğinde bunu bir vatandaşlık görevini yerine getirmiş gibi zevkle ve sevinçle yapanlar çoğunluktadır. “Bizim bazı orijinalliklerimiz ve tabii yanlarımız, yabancılara çok ilginç gelmektedir. Bu yüzden ilgileniyorlar ve çok resim çekiyorlar” şeklindeki her türlü art niyetten arınmış bir düşünce şekli gafil muhbirlerin tam da içinde bulundukları bilinç durumunu betimler niteliktedir.<sup>199</sup>

Gafil muhbirlerin, genellikle motifleri yoktur. Güvenlik güçlerine yardım etmek ve kendilerine çıkar sağlamak gibi bir hedefleri de yoktur. Bilgileri kendi iradeleri dışında ve farkında olmadan verirler.<sup>200</sup> Gafil muhbirlerden bilgi koparılması durumu genelde rastlantısal ve plansız gerçekleşen bir süreç gibi görünse ve çoğunlukla öyle olsa bile, bilgiyi alacak kişiler için aslında durum bu kadar basit değildir. Bilgi alma niyetindeki kişiler (casuslar, güvenlik güçleri vb.), gafil muhbir olabilecek kişileri arayıp bulmak ve istediklerini alabilmek amacıyla uygun şartları ve ortamı oluşturmak için çaba gösterirler. Yani gaflet durumu bilgi verenler için geçerlidir. Bilgi alan kişiler, zaman zaman şanslarının yardımıyla sonuca ulaşırlar da, çoğu zaman işlerini şansa bırakmazlar. Bilgiyi alan ile gafil muhbir arasında rastlantısal olarak başlayan ilişki, zamanla gafletin kaldırıldığı planlı ve sistemli bir muhbirlik şekline dönüşebilir ancak bu zor, tehlikeli ve uzun bir süreçtir ve her zaman kaynağı tamamen kaybetme riski vardır.

Gafil muhbirlerin özellikleri nelerdir sorusuna verilebilecek net bir cevap yoktur. Her an herkesin gafil muhbir olabilmesi mümkündür. Bir bilginin önemsiz olduğu veya herkesçe bilindiği gerekçeleriyle, o bilgiyi öğrenmeye can atan kişilere verilmesi sıkça rastlanan durumlardan biridir. Yine de gafil muhbirlik ile

<sup>198</sup> Aydın, *İşte... a.g.e.*, s. 54.

<sup>199</sup> Oğuz Kalelioğlu, “Psikolojik Harp İstihbaratı”, *Avrasya Dosyası*, Cilt: 8, Sayı:2, Yorum Matbaası, Ankara, 2002, s.103.

<sup>200</sup> Fitzgerald, *a.g.e.*, s. 36.

ilişkilendirilebilecek, birbiriyle iç içe geçmiş, iki temel özellik vardır: Düşüncesizlik ve bilinçsizlik.

Yabancı istihbarat servislerine bilinçsiz ancak gönüllü olarak kendi kurumu ile ilgili bilgileri veren toy ve genç personelin çoğu, olası sonuçlarını düşünmeden ani bir karar verdiklerini ifade etmektedirler. Bu kişiler, yaptıklarını, tamamen aldıkları büyük tatmin duygusu veya anlık maddi sorunlarını çözdüğü için, kendileri ve diğer kişiler üzerinde uzun vadeli olası etkilerini düşünmeden yaparlar. Düşüncesiz ve olgunlaşmamış davranışlar sergileyen bireyler birçok konuda kendini kontrolden yoksundur. Dolayısıyla, toyluk ve bilinçsizlik tanımına uyan kişiler başlı başına birer potansiyel gafil muhbirdirler ve güvenlik sorunudurlar.<sup>201</sup>

Gafil muhbirlik, tamamen ortadan kaldırılabilir bir istihbarat zafiyeti değildir. Çünkü ne zaman, nerede ve kimin gafil muhbirlik yapabileceğini kestirmek olanaksızdır. Alınması gereken en iyi önlem, bireyleri etkili bir İKK eğitime tabi tutmak ve gafil muhbirliği öğretmektir. Temel İKK eğitime sahip kişilerin, bu eğitimden geçmemiş kişilere oranla, gafil muhbir olma olasılıklarının daha düşük olacağı rahatlıkla söylenebilir.

#### **4.3. GAFİL MUHBİRLİĞİ ENGELLEMELİK VEYA AZALTMAK İÇİN YAPILMASI GEREKENLER**

Gafil muhbirliği tamamen engellemek oldukça zor hatta olanaksızdır. Ancak bazı önlemler alınarak en azından kabul edilebilir seviyelere indirebilmek mümkün olabilir. Bu bağlamda alınabilecek önlemler şunlar olabilir:<sup>202</sup>

– Ağzı sıkılığın bir erdem, boşboğazlığın ise büyük bir kusur olduğu ve bildiklerini, ilgisiz ve yetkisiz kişilerle konuşmamak gerektiği unutulmamalıdır. “Yerin kulağı vardır.” atasözü ilke olarak benimsetilmelidir. Aile bireylerinin yapılan iş ve faaliyetlerle ilgili konuları bilmesine gerek olmadığı hatırlatılmalıdır.

– Görevle ve organizasyon ile ilgili bilgi ve malzemenin organizasyon dışına çıkarılmaması sağlanmalı ve bu bilinç personele işlenmelidir.

<sup>201</sup> Defence Human Resource Activity, *a.g.e.*, s. 35.

<sup>202</sup> Yakın, *a.g.e.*, s. 186; Van Cleave, “Strategic... *a.g.e.*, s. 5; Tezsever, *a.g.e.*, s. 177; *İstihbarata Karşı Koyma Brifingi*, <http://www.ayyildiz.org/portal/gruplar.php?id=4> (Erişim tarihi: 09 Ocak 2013).

– İki ve uyuşturuu gibi, aşırı kullanılması hâlinde bilin kaybı, diline hâkim olamama gibi eksikliklere neden olabilecek maddeler, özellikle yabancıısı olunan ortamlarda ve yalnızken kullanılmamalıdır.

– Yeterince tanınmayan veya yeni tanışılan kişilerle gereğinden samimi ilişkiler kurulmamalı ve ilişkilerde her zaman temkinli ve mesafeli davranılmalıdır.

– Dinleme yeteneklerinin teknolojik olarak ok ilerlediğı ve “kulağına bir şey söyleyeceğim” gibi ifadelerin günümüzde hükmünü yitirdiğı, her ortamda akla gelmeyecek yöntemlerle dinleme yapılabileceğı unutulmamalıdır.

– Şüphelenilen kişi ve durumların derhâl ilgili birimlere bildirilmesi bilinci personele yerleştirmeli ve “adam sendecilik” önlenmelidir. Yakınlarında meydana gelen İKK ihlallerini bildirmemenin de bir eşit gafil muhbirlik olacağı akıldan çıkarılmamalıdır.

– Parola ve şifreler ve bunları seçerken uygulanan yöntemler, en güvenilir görülen arkadaş ortamlarında dahi söylenmemeli ve sık sık değıştirilmelidir.

– Gizlilik içinde yürütölmesi gereken faaliyetlerde dosta (sempatik kanaldan) iş görölmemelidir.

– İnternete bağılı bilgisayarlarda asla gizlilik dereceli işlemler yapılmamalı ve gizlilik dereceli bilgi bulundurulmamalıdır.

– İmha ve tahrip işlemleri yöntemine uygun yapılmalı ve bilgisayarlardaki verilerin tamamen yok edilemediğı unutulmamalıdır.

– alışılan kurum veya şirketle ilgili, önemsiz ve herkes tarafından bilinebileceğı düşünölen hiçbir bilgi, hiçbir ortamda ve hiç kimse ile paylaşılmamalıdır (Eğer herkes biliyorsa neden bir de sen söyleyesin.).

– Bilgi koparmaya alışan kişilerin, her yerde oldukları asla unutulmamalıdır.

– Karşılık beklemeksizin yardım eden ve bize birtakım faydalar sağılayan kişilerin, farklı ve zararlı maksatları olabileceğı akıldan çıkarılmamalıdır.

- Ödün vermenin sonunun olmadığı unutulmamalıdır.
- Personele yönelik olarak alım ve sonraki aşamalarda, güvenlik araştırması ve soruşturması, ciddi ve ilkeli şekilde yapılmalıdır.
- Güvenilir kişi olduğu kanıtlanmamış kişilerin gizlilik dereceli bilgiye erişimi önlenmelidir.
- Basın ve bunların muhabirleri ile ilişkilerde istemeden de olsa bazı gizlilik dereceli bilgilerin açıklanması tehlikesinin her zaman mevcut olduğu ve bu gibi ilişkilerden mümkün olduğu kadar kaçmanın en doğru davranış biçimi olacağı unutulmamalıdır.
- Bilerek ya da bilmeden ihanet edilmiş olmasının, ihanetin sonuçlarını değiştirmeyeceği ve kayıpları yerine koymanın mümkün olmadığı hatırlatılmalıdır.
- Disiplinsizliğin ve bilinçsizliğin, gafil muhbirliğe davetiye çıkaracağı unutulmamalıdır.
- Yabancı kültürle beğenisi ve eğilimi olanların, önemli birer casus ve gafil muhbir adayı oldukları unutulmamalıdır.
- Yabancı ülkelerdeki resmî temsilciliklerde, üniversitelerde, çeşitli kurum ve kuruluşlarda, işçi topluluklarında ve derneklerde bulunan kişilere, istihbarat servislerinin hedefindeki potansiyel birer casus ve gafil muhbir adayı oldukları akıldan çıkarılmamalıdır.
- Ülkeye gelen, turistler dâhil bütün yabancılar, olası birer casus olarak değerlendirilmelidir. Misafirperverlik ile gafil muhbirlik arasındaki ince çizgi korunmalıdır.
- Tarihsel olarak, büyükelçilikler ve diğer diplomatik kuruluşlar, sağladıkları operasyonel güvenlik nedeniyle yabancı istihbarat faaliyetleri için gözde birer merkez olarak kullanılmışlardır ve muhtemelen hâlen kullanılmaktadırlar. İngiliz hükûmetinin 1800'lü yılların sonlarında, Osmanlı Devleti'nde görev yapan konsoloslarına verdiği askerî ve siyasi görevler durumu tüm açıklığıyla gözler önüne sermek için yeterlidir. "Osmanlı ülkesindeki millî, etnik hareketleri izlemek ... çeşitli

toplumsal sınıfların nüfus durumunu incelemek, vilayetlerin nasıl yönetildiğini izlemek ... Osmanlı ordusunun örgütlenişi, yönetimi, birlik hareketlerini izlemek, bu ülkede bir savaş olması durumunda İngiliz Hükümeti'nin işine yarayabilecek her türlü topoğrafik ve istatistikî bilgiyi toplamak.”<sup>203</sup> Bu yüzden buralara başvururken dikkatli olunmalıdır. Basit bir vize başvurusu esnasında, farkında olunmadan çok önemli bilgilerin verilmesi işten bile değildir.

– Yurt dışında yaşayan ve çalışan kişiler, ülke hakkındaki bilgileri yaşadıkları ülkede konuşmamalıdır.

– Yabancı sermayeli binlerce ticari işyeri, yabancı ortaklı kurum ve kuruluşlar, kamu ve özel sektörde artan yurt dışı seyahatleri (ticaret, iş, görev, turistik vb. sebeplerle), taraf olunan anlaşmalar ve uluslararası oluşumlar nedeniyle özellikle askerî birliklerin katıldığı birleşik harekâtlar\* ile yüz binlerce öğrenci ve öğretim elemanının karşılıklı değişimi gibi durumlar, ülke güvenliğinin istihbari açıdan nüfuz edilebilirliğini kolaylaştırmaktadır. Buralarda görev yapanlar, çalışanlar ve öğrenim görenler potansiyel gafil muhbirlerdir. Bu bakımdan, mensubu olunan organizasyon ile ilgili bilgilerin, konuşmalarda, yazılı hazırlanan raporlar, ödevler ve tezlerde bulunmamasına dikkat edilmelidir.

– Sorulacak bazı (hatta çoğu) sorulara, konu en ince ayrıntısına kadar bilinse dahi, “Bilmiyorum, duymadım, görmedim.” şeklinde cevap verilebilmelidir.

– “Ben kimim ki?”, “Ben ne biliyorum ki?”, “Bunları zaten herkes biliyor.” vb. sakat zihniyetlerin yok edilmesi için çabalanmalıdır. Onların yerine “Benim kim olduğum ya da ne kadar önemli bilgiye sahip olduğumun önemi yok. Ben, bildiklerimi ilgisiz ve yetkisiz kişilere, hem de sırf konuşmuş olmak için anlatmamam ve düşüncesizliklerimden kaynaklanan İKK zafiyetleri göstermemem gerektiği bilinciyle hareket etmek zorundayım.” veya “Benim bildiklerim, dünyanın en büyük sırlarıdır ve bunları kimseyle paylaşmamalıyım.” gibi düşünce kalıpları gafil muhbirlik hatalarını önemli ölçüde azaltacaktır.

– Gafil muhbirliğin, sanıldığı kadar basit bir hata olmadığı, doğuracağı olumsuz sonuçlar nedeniyle, TCK'nin 326 ilâ 329'uncu maddeleri arasında

<sup>203</sup> Funda Adıtatar, “İzmir İngiliz Başkonsolosluğunun Askeri İstihbarat Faaliyetleri (1878–1914)”, *Tarih İncelemeleri Dergisi*, Cilt: XXVI, Sayı: 1, 2011, 1–34, s. 4.

\* Birden fazla ülke silahlı kuvvetlerinin birlikte katıldıkları harekâta, “Birleşik Harekât” denir.

tanımlanan, casusluk ile ilgili suçların taksirle işlenenleri kapsamında değerlendirilebileceği ve uzun süreli hapis cezalarının alınabileceği unutulmamalıdır.

#### **4.4. ÖRNEK OLAYLARDA GAFİL MUHBİRLİK**

##### **4.4.1. Örnek Olay–1: Operasyonu Bozan Kantinci**

İç güvenlik bölgesinde görev yapan A Birliği, bir grup teröristin B bölgesine geldiği ve kışı geçirmek üzere hazırlıklara başladığı istihbaratını alır. İki tabur ile operasyon hazırlığı yapılır. Hazırlıklar devam ederken, kantin sorumlusu operasyona çıkacakların gereksinimlerini karşılamak üzere alışveriş yapması için C'yi ilçeye gönderir.

C, kantin aracını her zaman mal aldığı, ilçenin tek büyük marketinin önüne park ettirir. İçeri girer ve siparişleri vermeye başlar. Market sahibi, “Hayrola komutan, bugün sizin gününüz değildi” der. C, ağzından bir şey kaçırmamaya dikkat ederek “Elimizdeki mal çabuk bitti.” der ve geçiştirmeye çalışır. C'nin telaşlı ve kaçamak cevapları market sahibini kuşkulandırır ama başka bir şey de soramaz.

Marketin çırağı ve kantin görevlisi E, malzemeleri araca yüklemeye başlarlar. Yükleme esnasında çırak, E'ye “Bu kadar çikolatayı ne yapacaksınız?” diye sorar. E, hiç düşünmeden “Operasyona gidenler hep çikolata alıyor” şeklinde cevap verir. Çırağın “Şunların kökünü kazıyın artık.” demesi üzerine de E, “Merak etmeyin, bizimkiler bir grup terörist tespit etti. Yarın onların işini göreceğiz” der. Yükleme işlemi tamamlanır ve birliğe dönülür.

Ertesi gün sabaha karşı başlayan operasyonda planlandığı ve istihbar edildiği gibi B bölgesine gidilir ancak hiçbir teröriste rastlanmaz. Bıraktıkları izlerden, teröristlerin bölgeyi yeni terk ettikleri anlaşılır. Çok daha sonra aynı bölgede ele geçirilen bir teröristin sorgusunda, bahse konu operasyonu, ilçedeki işbirlikçilerinden haber aldıkları ve o gün bölgede 70 kişi oldukları öğrenilir.

E'nin, belki istemediği çırağa verdiği bilgi nedeniyle, teröristlerin yerlerinin tespit edilmesi istihbaratının elde edilmesinden birliğin operasyona çıkışına kadar bütün emekler ve uğraşlar boşa gitmiştir. Oysa bu tür halkla iç içe görev yapan personelin özellikle uyarılması ve eğitilmesi gerekir. Çırağın bilgi sızdırmadaki ustalığını da yabana atmamak gerekir ama çok temel seviyede verilecek olan İKK eğitimi ile bu tür olayların önüne kolaylıkla geçilebilir.

#### 4.4.2. Örnek Olay–2: İngiliz Casusa Bilgi Veren Türk Casus<sup>204</sup>

Kurtuluş Savaşı yıllarında, Anadolu’da görev yapan bir İngiliz casusu, rastlantı eseri karşılaştığı ve önemli bazı bilgileri sızdırdığı, Mustafa Hilmi kod adlı Türk ajanı İsmail Hakkı ile ilgili ülkesine gönderdiği bir raporda kendi ağzından şunları anlatmaktadır:

...Ulu Kışla’daki otelde, Kayseri’nin 40 mil batısında bulunan Nevşehir’li iki Türk’le tanıştım; iş için Adana’ya gidiyorlardı. Bunlardan, İsmail Hakkı adındaki kişinin alelâde bir tüccar olmadığından kuşkulananarak, onunla konuşmaya başladım. Bir Türk gibi görünerek, bu ülkenin kâfirlerin topuğu altında ezilmesinden ötürü üzüntümü belirttim. Kurmuş olduğum tuzağa hemen düştü ve bana “Ulusal Savunma” Derneği’nin amaç ve eylemleri hakkında aydınlatıcı bilgi verdi. Bu sırada karargâhı Sivas’ta bulunan .. Mustafa Kemal’in Türkiye’de bir akım örgütlediğini .. söyledi.

Bu akımın başarısızlığa uğrayabileceği ve Mustafa Kemal’in bencil amaçlar için çalıştığını öne sürdüm. Bunun üzerine, İsmail Hakkı, bu akım ulusal ve dinsel olduğundan, kişisel faktörün söz konusu olmadığı yolunda bana güvence verdi...

Raporun devamında, İsmail Hakkı’nın casusa, İstanbul’da İngiliz yandaşı Türkler tarafından kurulan İngiliz Muhipleri Cemiyeti’nin çeşitli uygulamalarından biri hakkında verdiği ayrıntılı bilgi yer almaktadır:

Bu dernek, çeşitli kentlerdeki gizli ajanları aracılığıyla her üyesine, biri kırmızı ve biri beyaz olmak üzere iki kart sağlamıştır. Kırmızı kartların üzerinde basılı olarak “İngiltere’nin dostları – bu adam (adamın adı) İngiliz yandaşıdır ve siyasete karışmaz” sözcükleri vardır. Beyaz kartta ise adamın kişiliği hakkında bilgi verilmektedir. Böylece, derneğin bir üyesi, İngiliz yandaşı olduğunu kanıtlamak amacıyla herhangi bir anda bu kartları İngiliz yetkililerine gösterebilir.

Mustafa Kemal kurnazca davranarak bu kartlardan 5.000 adet sağlamış ve kendi ajanlarına dağıtmıştır; onlar da bu kartlara doğru dürüst kişisel bilgi, ama sahte adlar koymuşlardır. Bu da İngiliz’leri aldatmak için kullanılan yararlı bir araçtır.

<sup>204</sup> Salâhi R. Sonyel, *Kurtuluş Savaşı Günlerinde İngiliz İstihbarat Servisi’nin Türkiye’deki Eylemleri*, Türk Tarih Kurumu Basımevi, Ankara, 1995, ss. 39–40.

Olayda, maske mazeretini iyi seçememiş olan bir casusun, kendisinden daha yetenekli başka bir casus tarafından tespit edilmesi ve bilgi sızdırılması söz konusudur. İngiliz casus, İsmail Hakkı'yı, bilgi alabilmek için hemen oracıkta hazırladığı basit ve kökleşik tuzağa çekmeyi başarmıştır. Olayda, İsmail Hakkı açısından tam bir İKK zafiyeti söz konusudur. Aynı zamanda ciddi anlamda bir gafil muhbirlikten de bahsedilebilir. Konuyla hiç ilgisi olmayan ve yeni tanıdığı bir kişiye gizli bilgileri anlatmak şeklinde gerçekleşen bu gafil muhbirlik olayı, yapılan önemli bir istihbarat başarısının çöpe gitmesine sebep olmuş ve İngiliz Muhipleri Cemiyeti'nden gizlice temin edilen kartları kullanan birçok Türk casusun açığa çıkması gibi çok daha kötü sonuçlara davetiye çıkarmıştır. Hiçbir çıkar veya motifle ilişkilendirilemeyecek olan bu davranış, tamamen kişisel önlemsizlik ve boşboğazlığın bir sonucudur. Kuşkusuz, onu bu davranışa yönelten İngiliz casusun başarısı göz ardı edilmemelidir ama sonuç olarak görülüyor ki, profesyonel bir casusun bile gafil muhbir olabilmesi mümkündür.

#### 4.4.3. Örnek Olay–3: Gurbetçilerin Gafleti<sup>205</sup>

Yurt dışında bir ülkede çalışan ve hemşehri olan iki köylü, kısa süreli izinlerini geçirmek üzere köylerine gelirler. Köyde bulundukları sürede, köyün içinde ve civarında geceleri kimliği belirsiz kişilerce sık sık ateş edildiğini fark ederler. Rahatsız olurlar ve durumu köylerindeki Jandarma karakoluna bildirirler fakat karakoldan herhangi bir tepki alamazlar.

İzinleri bittikten sonra çalıştıkları ülkeye geri dönen iki arkadaş, sadece Türklerin gittiği bir derneğinde, başka arkadaşlarına köylerinde yaşadıkları bu durumu anlatmaya başlarlar. Duydukları üzüntü ve korkunun yanında karakoldan hiçbir tepki gelmemesinden dolayı hayal kırıklığına uğradıklarını da söylerler. Ayrıca, karakoldaki durumun tam bir başıboşluktan ibaret olduğunu, çoğu zaman nöbet dahi tutulmadığını ve iki örgüt militanının rahatlıkla karakolun tamamını ele geçirebileceğini ifade ederler.

Rastlantı eseri arka masada oturan A terör örgütü mensubu iki kişi, tüm konuşulanları sinsice dinler ve öğrendiklerini hemen örgüte bildirirler. Örgüt tarafından yapılan araştırma sonucu verilen bilginin doğruluğu teyit edilir ve karakola eylem yapılmasına karar verilir.

<sup>205</sup> Orhan Seçkin, *Devlet Güvenliği ve Haberalma*, SFN Yayıncılık, Ankara, 2001, ss. 67–69.

Düzenlenen baskınla, beş kişilik bir militan grubu tarafından, karakoldaki tüm askerler ve o sırada karakolda bulunan köy muhtarı şehit edilir. Militanlar, tüm silah ve cephaneyi alarak hiçbir tepkiyle karşılaşmadan geldikleri gibi araçla kaçarlar.

İki gurbetçi vatandaşın, tamamen saf duygularla arkadaş arasında yaptıkları bir sohbetle söylediklerinin neticesinde bir karakol dolusu asker şehit olmuştur. Bu örnek olay, gafil muhbirliğin ne kadar ağır sonuçları olabileceğini en iyi gösteren örneklerden biridir. Hiç alakası olmayan bir ülkede, köylerini hiç bilmeyen kişilerin yanında yapılan bir konuşma esnasında söylenenlerin bile ne kadar tehlikeli olabileceğini ispatlar niteliktedir. Bu iki vatandaşın, köylerinden ayrılmadan önce bu düşüncelerini karakol veya karakolun bağlı olduğu bir üst birlikle paylaşarak gerekli uyarıları yapmaları çok daha doğru bir hareket tarzı olabilirdi.

## SONUÇ

İKK önlemleri, aktif ve pasif önlemler olarak bir ayrıma tabi tutulmalarına rağmen birbirlerini tamamlayan önlemlerdir. Çağımızın istihbarat savaşları düşünüldüğünde, aktif önlemlerin uygulanması, hem daha fazla profesyonellik gerektirir hem de daha külfetlidir. O hâlde öncelikle, görece daha kolay olan pasif önlemler eksiksiz şekilde uygulanmalı, sonra ihtiyaç duyulan alanlarda aktif önlemler devreye sokulmalıdır.

Günümüzde, herhangi bir bireyin internetten birçok bilgiye ulaşabilmesi, sahte kimlik kullanarak işe girmesi, gizlice şifreleri ele geçirmesi ve hassas bilgiye kolayca ulaşabilmesi mümkündür. İşin içine insanların dikkatsizlik, saflık, cehalet ve gafleti de girince bu durumu önlemek aslında çok da kolay görünmemektedir. Teknik bakımdan İKK önlemleri ne kadar iyi düzenlenir ve işletilirse karşı istihbarat teşkilatlarının görevleri de o oranda kolaylaşmış olacaktır.

Güvenlik sistemlerine saldırmak isteyen ve sisteme girme yetkisi olmayan kişiler, karşı istihbarat sistemleri için ciddi bir tehdit oluştururlar ancak organizasyonların, sistemi her yönüyle iyi bilen kendi personeli, daha ciddi bir tehdit unsurudur. Zira çalışanlar, organizasyondaki sistemlerin çalışma prensiplerini ve sistemlerin güvenlik kontrol noktalarını çok iyi bilirler ve sistemlerin belirli noktalarına erişim yetkileri vardır. Kötü niyetli ya da angaje edilmiş çalışanlar, bu erişim yeteneklerini kullanarak, sistemlerin birçok güvenlik kontrol noktasını atlatarak sistemlere ciddi zararlar verebilirler.

Her nerede olursa olsun, şayet bir casusluk vb. faaliyetin sonucunda önemli bilgiler çaldırılmışsa, bu tek başına profesyonel karşı istihbaratçıların değil, genel anlamda karşı istihbarat sisteminin ve önlemlerinin başarısızlığının bir göstergesi olacaktır. Bu bağlamda teknolojik gelişmelere paralel olarak sürekli güncellenen ve güçlendirilen, aktif ve pasif her türlü İKK önlemi, yöntemi ve tekniğiyle, yaşayan bir karşı istihbarat sistemi kurulmasının önemi bir kere daha ortaya çıkmaktadır.

Afet planlaması veya yönetiminde “zarar görebilirlik”<sup>\*</sup> kavramı vardır. Afetin büyüklüğünün ve sonuçlarının ağırlığının belirleyicisi zarar görebilirlik düzeyidir. Deprem gibi doğa olayları, birçok devlet için sonucu maddi ve manevi büyük

---

<sup>\*</sup> Zarar görebilirlik kavramıyla ilgili ayrıntılı bilgi için bkz. **Zarar Görebilirlik Nedir?**, [http://www.afetler.net/zarar\\_gorebilirlik.aspx](http://www.afetler.net/zarar_gorebilirlik.aspx) (Erişim tarihi: 07 Mayıs 2013).

kayıplar ve zararlarla sonuçlandığından dolayı bir afet olarak nitelendirilirken, Japonya gibi önlemlerini almış ve depremle yaşamayı öğrenmiş bir devlet için sıradan bir olaydır ve afet sayılmaz. Afet, bir olay veya tehlikenin kendisi değil yol açtığı kayıplar, yani olumsuz sonuçlardır.

Zarar görülebilirlik kavramını karşı istihbarata uyarılmanın ve bu yönde bir planlama ve uygulama yapmanın doğru hareket tarzı olacağı değerlendirilmektedir. Karşı istihbarat eksikliğinden kaynaklanan bir bilgi kaybını, bir karşı istihbarat afeti olarak değerlendirmek mümkündür. Her organizasyon, kısmen veya hiç bilmediği istihbarat tehlikelerine her an maruz kalabilir. Önemli olan tehlikelerden kaçmak değil, tehlikelere hazırlıklı olmak ve tehlikelerden mümkün olan en az zararla kurtulabilmektir.

Şimdilik, katı güvenlik politikaları yürütmek ve gelişigüzel kontrollerle desteklenen farkındalık eğitimleri uygulamak en mantıklı ve başarı vaat edici çözüm gibi görünse de, aktif önlemlerin uzman kişiler tarafından alınması gerektiği göz önünde bulundurulduğunda, personelin pasif önlemler bakımından yetiştirilmesi ve eğitilmesi, kurumun ve dolayısıyla da ülkenin karşı istihbarat çabalarına ciddi katkı sağlayacaktır.

Karşı istihbaratta, teknolojik gelişmeler çok üst düzeye ulaşmış olmasına rağmen hâlen güvenlik duvarlarının kolayca aşıldığı sayısız örnek yaşanmaya devam etmektedir. Bu tür olayların yaşanmasının sebebi, mekanik sistemlerin doğru çalışmaması değil, insanların kolaylıkla hatalar yapabilmesidir. Sonuçta hemen her makineyi kullanan bir insan vardır ve insanlar alabildiğine zayıflıklarla donatılmış canlılardır.

Karşı istihbaratta insan boyutu, diğer bütün boyutlardan daha önde gelmektedir. İnsan boyutunun olması gerektiği gibi anlaşılamaması ve gerektiği kadar dikkate alınmaması durumunda diğer boyutlar bütün önemini ve başarısını yitirebilecektir. Her türlü İKK ve dolayısıyla casusluğa karşı koyma önleminin ana unsuru insandır ve organizasyondaki her bir personel potansiyel birer karşı istihbarat açığıdır. Bu nedenle İKK önlemlerinde insan etkeninin üzerine ayrıca eğilmek gereklidir.

Karşı istihbaratta, özellikle düşkünlükler ve hatalar bakımından öne çıkan unsur, doğal olarak “insan” olmaktadır. Genel anlamda her sistemde eğitilmiş ve

bilinçli insanlara duyulan ihtiyaç üst seviyededir ancak karşı istihbaratta bu etken hayati görünmektedir. Zira eğitimsiz, bilinçsiz, yaptığıının ulusal güvenliğe zarar vereceğinin farkında bile olmayan insanlar, mevcut karşı istihbarat sisteminin başarı ya da başarısızlığında doğrudan etkilidirler ve hatta en önemli aktördürler.

Konu, insan ve olumsuz yönleri, düşkünlükleri ve zayıflıkları olunca, Albert Einstein'ın şu veciz sözünü hatırlamamak mümkün değildir: "İki şey sonsuzdur, evren ve insanoğlunun aptallığı... Aslında evrenin sonsuzluğundan o kadar da emin değilim." Karşı istihbarat bakımından en önemli unsur olan insanların, aptallıklarını ya da daha doğru bir ifadeyle zayıflıklarını tamamen ortadan kaldırmak mümkün görünmediğine göre, karşı istihbaratta başarıyı elde etmenin yolu insan etkeninin çok iyi değerlendirilmesinden yani düşkünlüklerin en aza indirilmesinden ya da kontrol altında tutulmasından geçmektedir.

İstihbarat kaçaklarının önlenmesi, verimli ve etkili bir karşı istihbarat sistemi kurulabilmesi ve gafil muhbirliğin en aza indirgenebilmesi için her şeyden önce karşı istihbarat konusunda iyi eğitilmiş, en azından bilinçli, hiç olmazsa da farkında olan insanlara büyük ihtiyaç duyulduğu ortadadır. Karşı istihbarat zincirinin en zayıf halkası olarak itham edilen "insan"dan kaynaklanan, maliyeti yüksek ve bedeli ağır olan karşı istihbarat düşkünlüklerini en aza indirebilmek için bilinç, duyarlılık, farkındalık ve uyanıklığı yükseltecek, benimsetme ve bilinçlendirme odaklı, mantıklı ve etkili bir İKK eğitime ihtiyaç vardır.

Gafil muhbirlerin verdiği bilgiler, diğerlerinin verdikleriyle kıyaslanmayacak kadar değersiz olabilir ancak istihbaratçıların ve casusların, en küçük bilgi kırıntılarını tıpkı bir yapbozun küçük parçalarını bir araya getirir gibi birleştirerek büyük resme ulaşma konusunda çok yetenekli oldukları unutulmamalıdır. Her türlü önlem alınsa bile tamamen engellenmesi mümkün görünmeyen küçük gafil muhbirlik gedikleri veya delikleri, uzun vadede çok büyük kayıplara ve olumsuz sonuçlara sebep olabilecek kadar risklidirler.

Sonuç olarak, gafil muhbirler ile kendisinden bilgi sızdırılanlar veya casuslar arasında yöntem, teknik, bilinç ve irade farklılıkları olmakla birlikte, verilen bilgilerin doğurabileceği sonuçlar benzerdir ve hatta çoğu zaman aynı oranda yıkıcıdır. Gizli veya hassas bilgileri, yetkisiz ve ilgisiz kişilere açıklamakta hiçbir sakınca görmeyen, dahası bunun hatalı bir davranış olduğunun farkında dahi olmayan gafil muhbirler çok olduğu sürece teknik olarak alınmış bütün önlemler ve emek boşa gitmiş

demektir. Gereksiz, yersiz ve zamansız söylenecek bir sözün ve yapılacak bir davranışın çok önemli bir tesisin yok olmasına, bir muharebenin kaybedilmesine ve hatta bir ulusun mahvolmasına sebep olabileceği unutulmamalıdır.

***“Beni evhamlı sanıyorlardı. Hayır! Ben sadece gafil değildim. O kadar...”***

***II. Abdülhamid***

## KAYNAKÇA

### KİTAPLAR

- ACAR Ünal ve URHAL Ömer, Devlet Güvenliği İstihbarat ve Terörizm, Adalet Yayınevi, Ankara, 2007.
- AKAR Atilla, Casuslar Derin Savaşın Sıradışı Neferleri, Timaş Yayınları, İstanbul, 2005.
- ARIKLI Ercan, Başlangıcından Bugüne Kadar Dünya Casusluk Tarihi, Cilt: 1, Artel Yayınları, İstanbul, 1974.
- AVCI Gültekin, İstihbarat Oyunları: Orduların Karanlık Senaryoları, Birey Yayıncılık, İstanbul, 2007.
- AVCI Gültekin, İstihbarat Teknikleri: Aktörleri, Örgütleri ve Açmazları, Timaş Yayınları, İstanbul, 2004.
- AYDIN Nurullah, İşte İstihbarat, Kum Saati Yayınları, İstanbul, 2011.
- BAHAR İlhan, Teşkilat-ı Mahsusa'dan MİT'e, Kum Saati Yayınları, İstanbul, 2009.
- BAYMUR Feriha (BALKIŞ), Genel Psikoloji, İnkılâp Kitabevi, İstanbul, 2004.
- BAYSAL A. Can ve TEKARSLAN Erdal, Davranış Bilimleri, Avcıol Basım Yayın, İstanbul, 2004.
- CÜCELOĞLU Doğan, İnsan ve Davranışı: Psikolojinin Temel Kavramları, Remzi Kitabevi, İstanbul, 2011.
- ÇINAR Bekir, Devlet Güvenliği, İstihbarat ve Terör, Sam Yayınları, Ankara, 1997.
- ÇİTLİOĞLU Ercan, Gölgedeki Sessiz Tanıklar, Doğan Kitap, İstanbul, 2007.
- DOUGLAS Bernhardt, Competitive Intelligence: How to Acquire and Use Corporate Intelligence and Counter-Intelligence, Financial Times, London, 2003.
- ELBAHADIR Hamza, Hacking Interface, Kodlab Yayın Dağıtım, İstanbul, 2013.
- EREN Erol, Örgütsel Davranış ve Yönetim Psikolojisi, Beta Basım Yayım, İstanbul, 2010.
- ERSANEL Nedret, Siber İstihbarat: Küresel ve Nano Casusluğun Anatomisi, Hayykitap Yayınları, İstanbul, 2005.
- FITZGERALD Dennis G., Informants and Undercover Investigations: A Practical Guide to Law, Policy, and Procedure, CRC Press, 2007.
- GEÇTAN Engin, Psikodinamik Psikiyatri ve Normaldışı Davranışlar, Metis Yayınları, İstanbul, 2004.
- GİRGİN Kemal, Uluslararası İlişkiler: Modern İstihbarat ve Türkiye, Okumuş Adam Yayınları, İstanbul, 2003.

- GOLOVIN Andreas H., Fundamental Elements of the Counterintelligence Discipline, Volume:1, Universal Counterintelligence Core Competencies, Nova Science Publishers Inc., 2011.
- HERMAN Michael, Intelligence Power in Peace and War, Cambridge University Press, 1999.
- HİÇYILMAZ Ergun, Belgelerle Teşkilat-ı Mahsusa ve Casusluk Örgütleri, Ünsal Kitabevi, İstanbul 1979.
- JOHNSON William R., Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer, Georgetown University Press, Washington D.C., 2009.
- KAĞITÇIBAŞI Çiğdem, Yeni İnsan ve İnsanlar: Sosyal Psikolojiye Giriş, Evrim Yayınevi, İstanbul, 2004.
- KARABEKİR Kazım, Gizli Harp İstihbarat, Kamer Yayınları, İstanbul, 1998.
- KÖKNEL Özcan, Günlük Hayatta Ruh Sağlığı, Alfa Kitabevi, İstanbul, 2009.
- KÖSELİ Mutlu, İstihbarat Temel Hususlar ve Güncel Konular, Adalet Yayınevi, Ankara, 2011.
- MITNICK Kevin D., Aldatma Sanatı, Çev.: Nejat Eralp Tezcan, ODTÜ Yayıncılık, Ankara, 2009.
- ÖZDAĞ Ümit, İstihbarat Teorisi, Kripto Kitaplar, Ankara, 2009.
- SEÇKİN Orhan, Devlet Güvenliği ve Haberalma, SFN Yayıncılık, Ankara, 2001.
- SHULSKY Abram N. ve SCHMITT Gary J., Silent Warfare: Understanding the World of Intelligence, Brasley Inc., Washington D.C., 1993.
- SİLAH Mehmet, Sosyal Psikoloji Davranış Bilimi, Seçkin Yayıncılık, Ankara, 2005.
- SONYEL Salâhi R., Kurtuluş Savaşı Günlerinde İngiliz İstihbarat Servisi'nin Türkiye'deki Eylemleri, Türk Tarih Kurumu Basımevi, Ankara, 1995.
- ŞENEL A.Turhan, İKK ve İKK Operasyonları, İDB Yayınları No:64, Ankara, 1997.
- TEZSEVER Serhat, Milli Güvenliğimiz İçinde İstihbarat, İstanbul Üniversitesi Basımevi, İstanbul, 1999.
- TILISBIK Niyazi ve AKBAL Özdemir, Intelligence: İstihbarat ve Türkiye, İKİA Yayıncılık, İstanbul, 2006.
- TZU Sun, Savaş Sanatı, Çev.: İbrahim Şener, Mitra Yayınları, İstanbul, 2011.
- URHAL Ömer, Küreselleşen Dünyada Güvenlik, Adalet Yayınevi, Ankara, 2009.
- VAN CLEAVE Michelle K., Counterintelligence and National Strategy, National Defense University Press, Washington D.C., 2007.

WALLACE Robert ve MELTON H. Keith, CIA Kendini Anlatıyor: Casusluk, Çev.: Algan Sezgintüredi, NTV Yayınları, İstanbul, 2010.

WÜRTENBERGER Thomas, “Tehlike Kavramı” ve Alman Uygulaması Ekseninde Kolluk Hukuku, Çeviren ve Yorumlayan: Feridun Yenisey, Asayiş Dairesi Başkanlığı, Ankara, 2008.

YAKIN Aziz, İstihbarat, Casusluk ve Casuslukla Mücadele, Dış İşleri Akademisi Yayınları, Ankara, 1969.

YARMAN Tolga, Geçmişte ve Bugün Nükleer Enerji Tartışması, Okan Üniversitesi Yayınları, İstanbul, 2011.

YILMAZ Sait, 21.Yüzyılda Güvenlik ve İstihbarat, Milenyum Yayınları, İstanbul, 2007.

## MAKALELER

ADITATAR Funda, “İzmir İngiliz Başkonsolosluğunun Askeri İstihbarat Faaliyetleri (1878–1914)”, Tarih İncelemeleri Dergisi, Cilt: XXVI, Sayı: 1, 2011, ss. 1–34.

ALLEN Bobby, “The New Counterintelligence Response to the Cyberthreat”, Military Intelligence Professional Bulletin, Vol.: 29, No.: 3, 2003, ss. 32–35.

BOZTAŞ M.Hamid ve Mehmet Z. SUNGUR, “Kaçınan Kişilik Bozukluğu”, Psikoloji Dünyası, 2001, 5, ss. 71–79.

BRIDGEMAN Vincent H., “Defence Counterintelligence, Reconceptualized”, In Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence by Jennifer E. Sims and Burton Gerber, 2008, ss. 125–148.

CATE Charles V., “Counterintelligence for National Security”, Studies in Intelligence, Vol.: 2, No.: 4, 1958, ss. 87–92.

DERDİMAN R. Cengiz, “Özel Güvenlik Hizmetlerinin Niteliği ve Etkin Bir Şekilde Yürütülmesi İçin Yapılması Gereken Düzenlemeler”, 3. Ulusal Özel Güvenlik Sempozyumu Bildirisi, Gaziantep, 1–2 Mart 2013, ss. 37–56.

DEXTER Douglas E. ve BECKETT–MCWALTER Jessica, “Protecting Trade Secrets: Best Practices from Hiring to Terminating and Everything in Between”, Licensing Journal, Vol.: 26 Issue: 1, 2006, s. 1–5.

DİRİ Mustafa ve GÜLÇİÇEK Mirac, “Türkiye’de Kamu Hizmetinin Görülmesinde Kullanılmakta Olan Gizlilik Derecesi Tanımları: Uygulamadaki Sorunlar ve Çözüm Önerileri”, Maliye Dergisi, Sayı: 162, Ocak–Haziran 2012, ss. 497–537.

EHRMAN John, “What are We Talking about When We Talk about Counterintelligence?”, Studies in Intelligence, Vol.: 53, No.: 2, 2009. ss. 5–20.

FITZPATRICK William M., DILULLO Samuel A. ve BURKE Donald R., “Trade Secret Piracy and Protection: Corporate Espionage, Corporate Security and the Law”, Advances in Competitiveness Research, Vol.: 12, No.: 1, 2004, ss. 57–71.

- HALLIGAN R. Mark ve WEYNAND Richard F., "The Economic Valuation of Trade Secret Assets", *Journal of Internet Law*, Vol.: 9, Issue.: 8, 2006, ss. 19–24.
- HARBER Justin R., "Unconventional Spies: The Counterintelligence Threat from Non–State Actors", *International Journal of Intelligence and Counterintelligence*, Vol.: 22, Issue: 2, 2009, ss. 221–236.
- JONES Jerry W., "CI and HUMINT or HUMINT and CI or CI/HUMINT or TAC HUMINT", *Military Intelligence Professional Bulletin*, Vol.: 28, No.: 1, 2002, ss. 28–33.
- KALELİOĞLU Oğuz, "Psikolojik Harp İstihbaratı", *Avrasya Dosyası–İstihbarat Özel*, Cilt: 8, Sayı:2, Yorum Matbaası, Ankara, 2002, ss. 100–108.
- KARAGÖZ Başak, "İnsancıl Yaklaşım'da Bireyin Fenomenolojisi: Varoluşçu Psikoloji'den İnsancıl Psikoloji'ye, 'Fenomenoloji'ye Kısa Bir Bakış", *Pivolka*, Sayı: 20, Başkent Üniversitesi, Mart 2007, ss. 13–15.
- KUZGUN Yıldız, "Kendini Gerçekleştirme", *Araştırma Ankara Üniversitesi Dil ve Tarih–Coğrafya Fakültesi Felsefe Bölümü Dergisi*, 1972, 10.1, ss. 162–178.
- OLSON James M., "The Ten Commandments of Counterintelligence", *Studies in Intelligence*, Vol: 45, No.: 5, Washington, 2001, ss. 81–87.
- PÄÄLLYSAHO Seliina ve KUUSISTO Jari, "Informal Ways to Protect Intellectual Property (IP) in KIBS Business", *Innovation: Management, Policy & Practice*, Vol.: 13, Issue.: 1, 2011, ss. 62–76.
- SALCAN Olay, "Bilgi Güvenliği", *Silahlı Kuvvetler Dergisi*, Sayı: 370, Genelkurmay Basımevi, Ankara, 2001, ss. 54–67.
- SARICA Bedri, "Kutadgu Bilig'de Komutan ve Ordunun Nitelikleri", *Atatürk Üniversitesi Türkiyat Araştırmaları Enstitüsü Dergisi*, Sayı: 37, Erzurum, 2008, ss. 87–105.
- TAYMUR İbrahim ve TÜRKÇAPAR M. Hakan, "Kişilik: Tanımı, Sınıflaması ve Değerlendirmesi", *Psikiyatride Güncel Yaklaşımlar*, 2012, 4(2), ss. 154–177.
- ULSCH MacDonnell ve SULLIVAN Michael J., "Protect Intellectual Property And Trade Secrets", *Baseline*, Issue: 115, 2012, s. 9.
- VAN CLEAVE Michelle K., "Strategic Counterintelligence: What is it and What Should We Do about it?", *Studies in Intelligence*, Vol.: 51, No.: 2, 2007, ss. 1–13.
- WASEMILLER A. C., "The Anatomy of Counterintelligence", *Studies in Intelligence*, Vol.: 13, No.: 1, 1969, ss. 9–25.
- YILMAZ Sait, "Kriz Yönetimi ve Güç Kullanımı", *Kara Harp Okulu Savunma Bilimleri Enstitüsü Savunma Bilimleri Dergisi*, Cilt: 7, Sayı: 1, Ankara, 2008, ss. 145–169.

## **TEZLER**

DURMUŞ Murat, “Özel Hayatın Korunması Hakkı ve Bu Çerçeve İstihbarat Faaliyetleri”, Sosyal Bilimler Enstitüsü, Kırıkkale Üniversitesi, Kırıkkale, 2006 (Yayınlanmamış Yüksek Lisans Tezi).

ÖZMEN H. İbrahim, “Liderlik Davranışını Etkileyen Toplumsal Normların Analizi”, Sosyal Bilimler Enstitüsü, Süleyman Demirel Üniversitesi, Isparta, 2009 (Yayınlanmamış Doktora Tezi).

## **RESMÎ YAYINLAR**

CIA Manual, Human Resource Exploitation Training Manual, 1983.

CIA Manual, KUBARK Counterintelligence Interrogation, Create Space Independent Publishing Platform, Washington D.C., 1963.

Department of Defence of U.S.A., Directive: Counterintelligence, Awareness and Reporting (CIAR), No.: 5240.06, 17 Mayıs 2011.

FBI Manual, Manual of Investigative Operations and Guidelines (MIOG), 1998.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Report to the President of the United States, 2005, ss. 485–497.

Türk Dil Kurumu, Türkçe Sözlük, Türk Dil Kurumu Yayınları, Ankara, 2005.

U.S. Army, FM 2–22.3 (FM 34–52) Human Intelligence Collector Operations, Washington D.C., 2006.

U.S. Army, FM 34–60 Counterintelligence, Washington D.C., 1995.

U.S. Marine Corps, MCWP 2–14 Counterintelligence, Washington D.C., 2000.

## **İNTERNET KAYNAKLARI**

AYDIN Nurullah, “Ajan Akademisyen ve Yazarlar”, Erciyes, 08 Ekim 2012, <http://www.erciyesgazetesi.com.tr/yazar.asp?yaziID=2614> (Erişim tarihi: 18 Nisan 2013).

BAYAT Saliha ve ŞENGÜL Nebile Kübra, Kişilik Bozuklukları, 2007, <http://bilka.org.tr/upload/file/KISILIK%20BOZUKLUKLARI.doc> (Erişim tarihi: 30 Nisan 2013).

Defence Human Resource Activity, Counterintelligence, <http://www.dhra.mil/perserec/adr/counterintelligence/counterintelligence.pdf> (Erişim tarihi: 12 Aralık 2012).

GÖNÜLTAŞ Nuh, “Apo’ya O Kadar Söyledik Cep Telefonu Kullanma Diye...”, Zaman, 21 Şubat 1999, <http://arsiv.zaman.com.tr/1999/02/21/yazarlar/10.html> (Erişim tarihi: 11 Nisan 2013).

İstihbarata Karşı Koyma Brifingi, <http://www.ayyildiz.org/portal/gruplar.php?id=4> (Erişim tarihi: 09 Ocak 2013).

MİT Resmî İnternet Sayfası, “İkinci Dünya Savaşı Yıllarında ve Sonrasında Yabancı Servislere Karşı Verilen Mücadele”, [http://www.mit.gov.tr/text\\_site/ikinci\\_bolum\\_E2\\_1.html](http://www.mit.gov.tr/text_site/ikinci_bolum_E2_1.html) (Erişim tarihi: 10 Mayıs 2013).

MİT Resmî İnternet Sayfası, “İKK Başkanlığının Görev ve Sorumlulukları”, <http://www.mit.gov.tr/t-ikk.html> (Erişim tarihi: 14 Kasım 2011).

Muhabere Emniyeti, <http://www.belgeler.com/blg/h7a/muhabere-emniyeti> (Erişim tarihi: 03 Nisan 2013).

ÖZCİMBİT Ayhan, İnsan ve Davranışlarının Analizi, 12 Kasım 2012, <http://blog.milliyet.com.tr/insan-ve-davranislarinin-analizi/Blog/?BlogNo=388844> (Erişim tarihi: 27 Nisan 2013).

ÖZTÜRK Günce, Bilgi Güvenliği Politikası Oluşturma Kılavuzu, TÜBİTAK UEKAE, Doküman Kodu: BGYS-0005, 2008, <http://www.bilgiguvenligi.gov.tr/bilgi-guvenligi-yonetimi-dokumanlari/uekae-bgys-0005-bilgi-guvenligi-politikasi-olusturma-kilavuzu.html> (Erişim tarihi: 30 Mart 2013).

SÖYLEMEZ Haşım, Casus Arkeologlar, 07 Ekim 2000, <http://www.aksiyon.com.tr/aksiyon/haber-6809-casus-arkeologlar.html> (Erişim tarihi: 29 Kasım 2012).

SECURITAS, Kurumsal Gizlilik Rehberi, <https://www.securitas.com/PageFiles/32308/Kitap%C3%A7%C4%B1klar/kurumsalgizlilikrehberi.pdf> (Erişim tarihi: 10 Ocak 2013).

SERT Hüseyin Emin, Kültür ve Davranış, <http://www.eminsert.org/component/content/article/54-insani-ve-sosyal-gelisim-merkezi/196-kultur-ve-davrans.html> (Erişim tarihi: 27 Nisan 2013).

Türkiye Biyoloji Sitesi, Genetik Yapımız ve Davranışlarımız Arasındaki İlişki, [http://www.biyolojici.com/Genetik\\_Yapimiz\\_ve\\_Davranislarimiz\\_Arasindaki\\_Iliski.html](http://www.biyolojici.com/Genetik_Yapimiz_ve_Davranislarimiz_Arasindaki_Iliski.html) (Erişim tarihi: 27 Nisan 2013).

Vatan, “ABD’li Akademisyenler Ajan İddiası Üzerine Şehri Terk Etti!”, <http://haber.gazetevatan.com/Haber/351250/1/Gundem> (Erişim tarihi: 18 Nisan 2013).

Zarar Görebilirlik Nedir?, [http://www.afetler.net/zarar\\_gorebilirlik.aspx](http://www.afetler.net/zarar_gorebilirlik.aspx) (Erişim tarihi: 07 Mayıs 2013).

## **ÖZ GEÇMİŞ**

Mehmet Yenai ŞAHİN, 1979 yılında Uşak'ta doğmuştur. İlk ve orta öğrenimini Manisa ve İzmir'de tamamlayarak 2001 yılında Kara Harp Okulu'ndan mezun olmuştur. 2002–2011 yılları arasında Türk Silahlı Kuvvetlerinin çeşitli birliklerinde ve karargâhlarında görev yapmıştır. 2011–2013 yılları arasında, Harp Akademileri Stratejik Araştırmalar Enstitüsü Uluslararası İlişkiler Ana Bilim Dalında, İstihbarat Yüksek Lisans Eğitimiini başarıyla tamamlamıştır.

Mehmet Yenai ŞAHİN, evli ve bir çocuk babası olup, İngilizce ve Fransızca bilmektedir.

(BU SAYFA BOŞ BIRAKILMIŞTIR)