TÜRKİYE CUMHURİYETİ
İSTANBUL GEDİK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

SİBER İSTİHBARATIN KAMU GÜVENLİĞİ İÇİN ROLÜ VE ÖNEMİ

SAİM ATALAY KELEŞTEMUR

YÜKSEK LİSANS TEZİ

SİYASET BİLİMİ VE KAMU YÖNETİMİ ANA BİLİM DALI

DANIŞMAN
PROF. DR. ALİ ÖZTEKİN

İSTANBUL - 2018

BEYAN

Bu tez çalışmasının kendi çalışmam olduğunu, tezin planlamasından yazımına kadar bütün safhalarda etik dışı davranışımın olmadığını, bu tezdeki bütün bilgileri akademik ve etik kurallar içinde elde ettiğimi, bu tez çalışmasıyla elde edilmeyen bütün bilgi ve yorumlara kaynak gösterdiğimi ve bu kaynakları da kaynaklar listesine aldığımı, yine bu tezin çalışılması ve yazımı sırasında patent ve telif haklarını ihlal edici bir davranışımın olmadığını beyan ederim.

Öğrencinin Adı, Soyadı

İmza

TEŞEKKÜR

Eğitim, öğretim ve tez çalışmam süresince kıymetli bilgi, birikim ve tecrübeleri ile bana yol gösteren, bu tez çalışmasının hayat bulmasında büyük emekleri olan değerli danışman hocam Sayın Prof. Dr. Ali Öztekin'e ve ilgi, öneri ve desteğini göstermekten kaçınmayan değerli hocam Sayın Yrd. Doç. Dr. Ahmet Özcan'a sonsuz teşekkür ve saygılarımı sunarım.

İÇİNDEKİLER

İKİNCİ BÖLÜM

ÜÇÜNCÜ BÖLÜM

TABLOLAR LİSTESİ

ÇİZELGELER LİSTESİ

KISALTMALAR LİSTESİ

AB : Avrupa Birliği

ABD : Amerika Birleşik Devletleri

ACINT : Acoustical Intelligence

AET : Advanced Evasion Techniques

APT : Advanced Persistent Threat

CCTV : Closed Circuit Television

CD : Compact Disc

CIA : Central Intelligence Agency

COMINT : Communications Intelligence

CPNI : Centre for the Protection of National Infrastructure

CRSF : Cross Site Request Forgery

CSOC : Cyber Security Operations Centre

DDoS : Distributed Denial of Service

DKK : Deniz Kuvvetleri Komutanlığı

DMK : Devlet Memurları Kanunu

DoS : Denial of Service

EGM : Emniyet Genel Müdürlüğü

ELINT : Electronical Intelligence

FAPSI : Federalnoe Agenstvo Pravitelstvennoi Svyazi i Informatsii

FBI : Federal Bureau of Investigation

FSB : Federalnaya Sluzhba Bezopasnosti

GCHQ : Government Communications Headquarters

GSM : Global System for Mobile

HTML : Hyper Text Markup Language

HUMINT : Human Intelligence

İKK : İstihbarata Karşı Koyma

IMINT : Imagery Intelligence

IRINT : Infrared Intelligence

KDGM : Kamu Düzeni ve Güvenliği Müsteşarlığı

KHK : Kanun Hükmünde Kararname

KİHBİ : Kaçakçılık, İstihbarat, Harekat ve Bilgi Toplama Daire Bşk.

KİKK : Kaçakçılık İstihbarat Koordinasyon Kurulu

KİS : Kitle İmha Silahı

MASINT : Measurement and Signature Intelligence

MI5 : Military Intelligence Section 5

MI6 : Military Intelligence Section 6

MİT : Milli İstihbarat Teşkilatı

MOSSAD : İsrail Dış İstihbarat Servisi

NASA : National Aeronautics and Space Administration

NATO : North Atlantic Treaty Organization

NSA : National Security Agency

NUCINT : Nuclear Intelligence

OCSIA : Office of Cyber Security and Information Assurance

OSINT : Open Source Intelligence

PDoS : Permanent Denial of Service

PGP : Pretty Good Privacy

PHOTINT : Photographic Intelligence

RADINT : Radar Intelligence

SATINT : Satellite Intelligence

SCADA : Supervisory Control And Data Acquisitiona

SIGINT : Signals Intelligence

SQL : Structured Query Language

SSCB : Sovyet Sosyalist Cumhuriyeti Birliği

TCK : Türk Ceza Kanunu

TDK : Türk Dil Kurumu

TECHINT : Technical Intelligence

TELINT : Telemetry Intelligence

TOR : The Onion Routing

TSK : Türk Silahlı Kuvvetleri

USB : Universal Serial Bus

VIDINT : Video Intelligence

VoIP : Voice Over IP

VPN : Virtual Private Network

XSS : Cross Site Scripting

ÖZET

Bu tez çalışmasının amacı, kamu güvenliğinin sağlanması açısından siber istihbaratın önemini incelemektir. Çalışmada, dünyadaki siber istihbarat faaliyetleri yürüten teşkilatlar ve geçmişte yaşanmış siber savaş olayları ele alınmıştır. Siber istihbarat çalışmalarının yapılabilmesi için gerekli siber saldırı yöntemlerinden, günümüzde en popüler olanlarına değinilmiş ve siber güvenlik/insan faktörü ilişkisine vurgu yapılmıştır. Çalışmanın temel varsayımı, siber istihbarat faaliyetlerinin kamu güvenliği bakımından etkin bir araç olarak kullanılabileceği, ancak bunun için ilgili birimlerde çalışan personelin gerekli bilgi ve beceriyle birlikte, yasal izne sahip olması gerektiğidir.

Anahtar Kelimeler: Siber İstihbarat, Kamu Güvenliği, Terörizm, İstihbarata Karşı Koyma, Siber Güvenlik

ABSTRACT

The objective of this thesis is analyzing the importance of cyber intelligence in the aspect of public safety. In the study, the secret services carrying out cyber intelligence activities and cyber war incidents occurred in the past have been discussed. In the study it is also mentioned the popular cyber attack methodologies necessary to carry out cyber intelligence activities and highlighted the relation of cyber security/human factor. The basis hypothesis of the study is the usage of cyber intelligence activities for public safety as a tool; therefore, for the staff in charge it is a necessity to have the essential knowledge and talent, besides legal permission.

Keywords: Cyber Intelligence, Public Safety, Terrorism, Counter Intelligence, Cyber Security

GİRİŞ

TEZİN KONUSU, YÖNTEMİ VE AMACI (TEMEL VARSAYIMI) KONULARINDA ÖZET BİLGİLER

Teknolojinin gelişmesi ve günlük hayatın bir parçası haline gelmesiyle birlikte içinde bulunduğumuz dünya düzeninde çeşitli gelişmeler ve buna bağlı olarak da olumlu/olumsuz değişimler yaşanmaktadır. Bu değişimlerin olumsuz olma sebebi, teknolojinin kötü amaçlı kişilerin eline geçmesi ya da bu kişiler tarafından kullanılmasıdır. Bugüne kadar, insanoğlunun faydalanması, ihtiyaçlarının karşılanması amacıyla bulunmuş, keşfedilmiş bir çok teknoloji, yine kötü amaçlı kullanım sebebiyle kitleler halinde ölümlere dahi sebep olmuştur.

Bilgi güvenliği kavramı önceleri sadece matbu bilgilerin korunmasına yönelik çalışmaları ifade etmekteyken, bugün siber uzayın büyümesi ve günlük yaşamın büyük bir parçası haline gelmesiyle birlikte çok daha geniş bir konu haline gelmiştir. Bilginin korunması için siber güvenlik gibi yeni kavramlar ortaya çıkmış ve buna bağlı olarak da koruyucu faaliyetlerin sınırları genişlemiştir. Siber uzayın gelişmesiyle birlikte siber saldırı, siber suç, siber terörizm ve bunların hemen hepsini kapsamakta olan siber savaşlar, sınırları henüz netlik kazanmamış olan bu büyük alan içerisinde etkisi artan bir şekilde makineleri ve insanları tehdit etmektedir.

A) Araştırmanın Amacı

İnternetin günlük hayatın bir parçası haline gelmesiyle birlikte devletler de sistemlerini ve faaliyetlerini siber uzaya taşıyarak, e-devlet hizmetleri vermeye

başlamıştır. Bu sistemlerde yer alan veriler ise terör örgütleri ve gizli servislerin hedefi olmaktadır. Vatandaşın kişisel bilgileri ile birlikte, devletlere ve buna bağlı kurumlara ait kritik veriler de yine siber uzayda yer almaktadır. Her ne kadar bu sistemlerin büyük bir kısmı internete bağlanmıyor olsa da siber uzayda yer alması halinde yine saldırılara maruz kalabilmekte ve hatta bu sistemlere sızılabilmektedir.

Çeşitli hacking grupları, örgütler, hackerlar ve gizli servisler, bağlı oldukları devletler adına siber saldırı ve siber istihbarat faaliyetleri düzenleyerek, bu bilgilere erişmenin, rakip veya hasım devletlere karşı üstün gelmenin çabası içindedirler. Snowden'in sızdırdığı bilgiler ışığında, ABD'nin ne tür siber faaliyetler yürüttüğü bir nebze de olsa gün yüzüne çıkmış olsa da ABD ve diğer ülkelerin siber istihbarat imkan ve kabiliyetleri hakkında kesin bir bilgi bulunmamaktadır. Dolayısıyla, ülkemizdeki siber uzayda yer alan sistemler ve bunlara bağlı hassas verilerin korunmasına yönelik siber güvenlik ve siber istihbarata karşı koyma faaliyetlerinin ivediklikle, en etkin şekilde yapılmasına matuf yasal düzenlemelerin ve ihtiyaç duyulan nitelikli insan kaynağına sahip olunması gerekmektedir.

Çalışmada, etkin bir siber istihbarat faaliyeti gerçekleştirebilmek için gerekli olan siber saldırı yöntem ve silahları ile İKK faaliyetleri için önem arz eden savunma yöntem ve sistemleri açıklanmaktadır. Araştırmada kullanılan veriler kütüphaneler, akademik veri tabanları, bilimsel yayın tarama siteleri, medya ve internet arşivleri, resmi internet sitelerinden elde edilen birincil ve ikincil kaynaklardan istifade edilmiştir. Ayrıca kamu kurumlarına eğitim ve danışmanlık hizmeti vermekte olan siber güvenlik firmalarının yöneticileri ile anket yapılmıştır.

B) Araştırmanın Kapsamı

Siber istihbarat, özellikle 2000'li yılların başlarından beri ABD, İsrail, Rusya ve Çin gibi ülkelerin gizli servis teşkilatları tarafından birincil veya destek istihbarat toplama yöntemi olarak kullanılmaktadır. ABD gizli servisi NSA'de önemli görevlerde yer almış olan Edward Snowden'in de yapmış olduğu açıklamalar ışığında, ABD'nin ulusal güvenlik kapsamında tüm dünyayı siber uzay üzerinden dinlemiş, hatta bununla kalmayıp hasım ülkelere karşı çeşitli operasyonlar düzenlemiş olduğu

ortaya çıkmıştır. Bugün kullanılmakta olan birçok cihaz üzerinde istihbari operasyon amaçlı kullanılan arkakapı ve tuş dinleyicilerin olduğu bilinmektedir. Ancak bunların ülkemize giriş çıkışları ile yazılım ve donanım seviyesinde incelenmemesi, yabancı devletlerin ülkemize karşı siber uzay üzerinden istihbarat operasyonları düzenlemelerini kolaylaştırmaktadır.

Diğer taraftan, ABD siber güvenlikle ilgili önlemlerini genişleterek, 2009 yılında siber saldırılara karşı "Siber Savaş Komutanlığı" kurmuş ve başına bir general atamıştır. Türkiye, ne yazık ki bu konuda yeterli bilgi ve tecrübeye sahip olmamakla birlikte, gerekli sayıda "nitelikli" insan kaynağını da henüz sağlayamamaktadır. Bu sebeple, ülkemizin siber uzay üzerinden gelebilecek her türlü saldırıya karşı etkin bir koruma sağlaması, içinde bulunduğumuz durumda mümkün görünmemektedir. Bu tez çalışmasında siber uzay, siber güvenlik ve siber istihbarat gibi kavramların tanımlarının doğru yapılması ile bu faaliyetlerin gerek insan faktörü ele alınarak, gerekse de siber saldırı metodolojilerini kullanarak kamu düzeni ve güvenliğine matuf iç istihbaratın nasıl oluşturulabileceği konuları, çalışma kapsamına alınmıştır.

C) Araştırmanın Yöntemi

Araştırmada literatür ve arşiv taraması ile kamu kurumlarına siber güvenlikle ilgili dışarıdan danışmanlık ve eğitim hizmetleri veren firmalarda yönetici pozisyonunda, her biri alanında uzman siber güvenlik uzmanları ile anket çalışması gerçekleştirilmiştir. Ankete katılan uzmanların bir kısmı, "underground" olarak tabir edilen, internetin karanlık yüzünde uzun yıllar, "siyah şapkalı hacker" olarak çeşitli faaliyetlerde bulunmuş kişilerdir. Bu kişilerle yapılan mülakatlar da siber istihbarat faaliyetlerinin nasıl yapılması gerektiği, özellikle siber terör faaliyetlerinin ne şekilde önlenebileceği gibi konulara ışık tutmaktadır.

D) Araştırmanın Varsayımı, Varsayımları (Hipotezi, Hipotezleri)

Bu çalışmadaki temel varsayım, içinde bulunduğumuz 21. yüzyılda internetin yaygınlaşmasıyla birlikte, harbin beşinci boyutu olarak adlandırılan siber uzayda, istihbarat faaliyetleri gerçekleştirmenin ve istihbarata karşı koymanın kamu düzeni ve güvenliği açısından ne derece önemli olduğudur.

BİRİNCİ BÖLÜM

1. İSTİHBARAT BİLİMİNE AİT GENEL BİLGİLER

1.1. İstihbarat Kavramı

İnsanoğlunun yaradılışı gereği gizliyi öğrenmeye eğilimli olması, onu sürekli olarak bilinmeyeni keşfetme ve sırları açığa çıkartmaya yöneltmiştir. Merak ve öğrenme arzusu, zamanın ve koşulların değişmesiyle birlikte bilimsel araştırmalara, bunlar da zamanla yerini istihbarat kavramına bırakmıştır. İstihbarat ise yıllar içinde evrimleşerek bugün bir bilim dalı haline gelmiştir. İstihbarat, günlük hayatta hemen herkesin kullandığı bir kavramdır.

Bir iş görüşmesine gitmeden önce internet üzerinden, iş başvurusu yapılan firma hakkında bilgi toplamak, sosyal medya siteleri üzerinden firmanın insan kaynakları departmanında çalışan kişileri tespit etmek ve bu kişilerin kişisel sayfalarını inceleyerek, ne gibi sorularla karşılaşılabileceği ya da nasıl bir tavır sergilenebileceği konusunda bir analiz yapmak, en basit haliyle bir istihbarat faaliyetidir.

Daha basit bir örnekle, şehirler arası yolculuk yapmadan önce, varılacak şehrin o günkü hava durumunu araştırmak ve buna göre hazırlıklı olmak da yine bir istihbarat faaliyetidir. Görüldüğü üzere, farkında olmadan dahi günlük hayatta birçok kez istihbarat ile ilgili haber toplama, değerlendirme ve hatta kimi zaman raporlama gibi istihbarat süreçlerinden geçmekte ve buna göre gerekli önlemler alınmaktadır.

Günümüzdeyse istihbarat özel kurumların ve devletlerin barışta ve savaşta birbirlerine karşı bilgi elde etmek ya da sahip oldukları bilgiyi korumak için gerkçekleştirdiği faaliyetler olarak ifade edilmektedir. Bir başka deyişle istihbarat, bir şirketin rakip şirketlere karşı ekonomik ve teknolojik üstünlük kurması için büyük faydalar sağlamaktayken, bir devletin ise hasmın ya da rakip devletin durumu hakkında cari ya da stratejik bilgilerin önceden tespit edilmesi ve buna uygun politikaların geliştirilmesi konusunda önemli bir faaliyetler sürecidir.

Burada önemli olan bir başka konuysa, karar alıcıların ya da analizcilerin elde edilen bilgiyi ne derece yorumlayabildiği, bunu istihbarat haline getirebildiği ve kullanabildiğidir. Tarihte, ilk istihbarat faaliyetlerinin avcılık yapmak için avının izini süren insanlar tarafından başlatıldığı, daha sonra ise hayvan yerine düşmanın izini sürerek istihbarat faaliyetlerinin kapsamının ve sürecinin değişime uğradığı yorumu yapılmaktadır. Örneğin Eski Mısır'daki istihbarat seksiyonu içinde esir sorgulayıcılardan iz sürücülere kadar farklı alt birimlerin ve bu birimlere bağlı görevlilerin olduğu görülmektedir (Özdağ, 2013, s. 41).

Eski Türkler, Orta Asya topraklarında yaşamlarını uzun bir süre avcılık ile sürdürmüşlerdir. Dolayısıyla da istihbaratın çıkış noktası olarak kabul edilebilecek avcılığın iz sürme, yer tespit etme ve avın özelliklerini belirleme gibi unsurlarını, Türkler etkin bir şekilde kullanmışlardır. Özellikle Çin devletleri ile yaşanan mücadeleler sırasında çaşıt denilen, ilerleyen zamanlardaysa Martolos adı verilen devşirme casuslar kullanarak istihbarat faaliyetleri yürütülmüştür. Bu dönemde Türkler, modern casusluk faaliyetlerinden çok, haber toplamak amacıyla eleman kullanmıştır.

Oluşturulan teşkilatlar, gizli operasyonlardan ziyade hakana haber ulaştırmak faaliyetlerini üstlenmektedir. Ayrıca casusluk faaliyetleri yürütülmesine karşın, etkin bir karşı casusluk yapan bir teşkilat yapısı oluşturulmamıştır. Diğer taraftan Çinliler ise Türkler'e karşı istihbarat ve psikolojik savaş ögelerini kullanarak, Türk devletlerinin yıkılmalarına sebep olmuşlardır. Bir Türk boyu olan Topalar, Büyük Hun İmparatorluğu'nun kurulmasından yaklaşık 300 sene önce, Çin istihbarat ve psikolojik

harp yöntemleri karşısında yenik düşmüş ve Çinlileşerek yok olmuşlardır (Özkan, 2005, s.24).

Tarihte büyük istihbarat faaliyetleri gerçekleştirilmiş ve bu yolla elde edilen hassas bilgilerin savaş meydanlarında kullanılarak zaferler elde edildiğine tanıklık edilmiştir. Eski komutanların kullandığı istihbarat yöntemleri bugün dahi önemini korumaktadır. M.Ö 500'lü yıllarda yaşamış olan Çinli komutan Sun Tzu, Savaş Sanatı isimli eserinde "Düşmanı ve kendinizi iyi tanıyorsanız, yüzlerce savaşa girseniz dahi sonuçtan korkmayın. Kendinizi tanıyor ancak düşmanınızı tanımıyorsanız, ne kadar zafer kazanırsanız, o kadar da kaybedersiniz. Ne düşmanınızı ne de kendinizi tanımıyorsanız, girdiğiniz her savaşı kaybedersiniz" demiş ve özellikle askeri alanda istihbaratın önemini vurgulamıştır.

Sun Tzu ayrıca, "İstihbarat, ruhlardan öğrenilmez; ne tümevarım yöntemleriyle deneyimlerden ne de tümdengelim yöntemleriyle yapılan hesaplamalarla elde edilebilir. Düşmanın niyeti ancak başka insanlardan öğrenilebilir" sözüyle o dönemde istihbaratın haber toplama faaliyetleri ve bunların komutanlar tarafından değerlendirilmesi şeklinde yorumlamıştır. Osman Pamukoğlu ise Sun Tzu'nun bu sözünden hareketle, en sağlam istihbaratın insandan insana olanı olduğunu, diğerlerinin ikinci sınıf olduğunu ifade etmiştir (Pamukoğlu, 2014, s.200).

Pamukoğlu ayrıca, casusluğun tehlikeli bir iş olduğunu, yakalananların sonunun ölüm olabileceğini de vurgulamıştır. Pamukoğlu'nun bu yorumu, Sun Tzu'nun istihbarat ve casuslukla ilgili yapmış olduğu yorumlara istinaden olup, günümüzde casusluk faaliyetleri sonucunda yakalanan kişilerin farklı cezai müeyyidelerle karşılaştığı görülmektedir.

ABD gizli servisi CIA'de İKK Direktörü olarak 1999-2001 yılları arasında görev yapmış Barry Royden, bir casusun operasyon sırasında yakalanması halinde genellikle hapis cezası aldığı, ancak Rus istihbarat görevlilerinin, dubl ajanlık[1] yaptığının tespit edilmesi halinde ölüm cezasına çarptırılabileceğini belirtmiştir. Royden ayrıca, ABD

[1] Dubl Ajan: İki gizli servise ajanlık yapan, bir servise diğeri hakkında bilgi veren kişi.

gibi ülkeler adına hizmet eden casusların diplomatik unvanlar çatısı altında faaliyet yürütmesi halinde, diplomatik dokunulmazlığa sahip olduklarının altını çizmektedir[2]. Bundan hareketle, günümüzde çeşitli istihbarat faaliyetlerinin diplomatik unvan ve ilişkilerle yürütüldüğü de görülmektedir.

İstihbarat, görüldüğü üzere milattan önce yaşanmış savaşlarda etkin bir biçimde kullanılmıştır ve insanlık tarihinin en eski mesleklerinden biri olarak nitelendirilmektedir. Avrupa'da casus şebekelerinin kullanılması ve istihbaratın bir nosyon haline dönüşmesi 16. yy'da İngiltere'de VIII. Henry'nin krallığı zamanında başlamış, daha sonraysa Cromwell zamanında şekillenmiştir (Weir, 2008, s.338). 18. yy. sonlarına kadar istihbarat faaliyetleri sadece askeri alan ve kralın kişisel çıkarları için kullanılmak suretiyle sınırlı kalmıştır.

İstihbaratın bugünkü kurumsal yapıya kavuşmasının temelleriyse Napoleon Bonaparte ile atılmaya başlamıştır. Napoleon, istihbaratı başarılı bir şekilde kullanarak birçok savaştan zaferle ayrılmayı başarmıştır. Ancak onun öngörüsü sayesinde, kardeşi Lucien Bonaparte ve Jean Antoine Chaptal ile birlikte dönemin İçişleri Bakanlığı bünyesinde "İstatistik Bürosu" kurulmuştur. Bu dönemde Napoleon, İngiltere başta olmak üzere, hasım ülkelerin ekonomik durumlarına ilişkin istatistiksel raporlar toplamış ve bunları analiz etmiştir (Nicholls, 1999, s.236).

Napoleon'un bu faaliyetlerini bugün, stratejik ve ekonomik istihbarat çatısı altında değerlendirmek mümkündür. İstihbarata büyük ölçüde katkıda bulunan teknolojik gelişmeler sayesinde özellikle modern toplumlarda istihbarat faaliyetleri daha bilimsel bir yaklaşımla gerçekleştirilmiş, yeni istihbarat ve karşı istihbarat yöntemleri üretilmiştir.

19. yy.'ın sonlarına doğru istihbarat alanında teknolojiden de faydalanılmaya başlandığı görülmüştür. Dönemin iletişim imkanları olan demiryolları ve telgraf haberleşme sistemi, etkin bir şekilde kullanılmıştır. Demiryollarının gelişmesi ve yaygınlaşması sayesinde daha hızlı bir istihbarat ağı oluşturulabilmiş ve ağ içi iletişim

[2] http://www.businessinsider.com, Erişim tarihi: 08 Aralık 2017.

hızında artış sağlanmıştır. İletişimi etkin kullanan devletler, hasımlarına karşı sürpriz hamleler düzenleyebilmiştir (Özdağ, 2013, s.48).

19. yy'ın ilk yarısıyla birlikte basının gelişmesi sayesinde, açık kaynak istihbarat kavramı da önplana çıkmıştır. Özellikle Prusya'nın ilk kez 1817 yılında atadığı askeri ateşe ve daha sonraki yıllarda atanan ateşelerin, istihbarat seksiyonunun birer parçası haline gelmesiyle birlikte, açık kaynak istihbaratın sıkça kullanıldığı görülmüştür (Wafe, 1999, s.35). Birinci Dünya Savaşı'nda da istihbarat daha ziyade açık kaynaklardan elde edilmiştir.

Gazete, kitap, raporlar ve seyahat notları gibi dokümanlar sayesinde istihbarat analizi gerçekleştirilebilmiştir. Bunun dışında yine cephelerde görev yapan istihbarat elemanlarının, insani istihbarat raporları da savaşın gidişatını önemli ölçüde etkilemiştir. Bu yıllarda kullanılan görünmez mürekkep gibi yöntemler, istihbaratta teknolojinin öneminin kavrandığını göstermektedir.

İkinci Dünya Savaşı ise istihbaratın teknolojiden en çok faydalanmaya başladığı dönem olarak nitelendirilebilir. Sinyal istihbarat (SIGINT) ve görüntü istihbaratı (IMINT) gibi yöntemler insani istihbaratla birlikte paralel olarak kullanılmaya başlanmıştır. Bu dönemde, teknolojik üstünlüğe sahip devletler, hasımlarına karşı istihbarat operasyonlarında da üstünlük sağlamış, bu sayede de zaferin kapısını aralamışlardır.

İkinci Dünya Savaşı, kriptografinin de istihbarat bilimi içindeki yerini aldığı dönem olarak nitelendirilebilir. Gizli servisler yeni kriptografik sistemler geliştirmiş, elde edilen şifrelenmiş verilerin deşifre edilmesi için algoritma çalışmaları yapılmıştır. Haberleşme artık düz metin şeklinde değil, bir takım kriptografik sistemler kullanılarak şifrelenmiş olarak yapılmıştır (Churchouse, 2002, s.133). Kriptografi, bugün siber istihbarat ve siber güvenlik alanlarında büyük bir öneme sahiptir.

Soğuk Savaş dönemi ise istihbaratın bilgi teknolojileri ile paralel bir şekilde yürütüldüğü yıllar olarak nitelendirilmektedir. Bu dönemde ABD, istihbarat faaliyetleri için uydu sistemleri başta olmak üzere birçok yeni teknoloji ve cihaz

geliştirmiştir. Soğuk Savaş sırasında Rusya ise geleneksel istihbarat yöntemlerini kullanmayı tercih etmiştir. 1940'lı yılların sonlarına doğru ABD, İngiltere ile birlikte Sovyet kablolarına saplama yapmış ve tüm iletişimi deşifre etmiştir.

ABD gizli servisi 1950'li yıllarda ise uydu sistemleri ve uçaklara yatırım yaparak, teknolojiyi istihbarat faaliyetlerinde de etkin bir şekilde kullanmıştır. 1970'lerde ise Sovyet Rusya, insani istihbarat unsurlarını kullanarak, ABD'nin sahip olduğu casus teknolojileri hakkında daha fazla bilgi sahibi olabilmiştir (Macrakis, 2010, s.379-381). Görüldüğü üzere, istihbarat faaliyetlerinde teknik istihbarat ve insan istihbaratı birlikte kullanılarak, çok daha verimli bir sonuç elde edilebilmektedir.

İstihbarat kurumları, devlete karşı yıkıcı ve bölücü faaliyetlerle iç ve dış tehditlere karşı gerekli bilgiyi önceden tespit etmeli, gerekli analizi yapmalı ve karar alıcılara konuyla ilgili ayrıntılı rapor sunmalıdır. Lowenthal'a göre üst düzey siyasi yöneticiler, bürokratlara nazaran daha hızlı değişmektedirler. Görevlerine geldiklerinde mevcut ve potansiyel tehditlerle ilgili gerekli bilgilendirmenin yapılması gerekmektedir. Bu görev ise istihbarat kurumlarına düşmektedir.

Devletin istihbarat kurumları ayrıca uzun vadeli politika üretilmesi konusunda da karar alıcılara danışmanlık hizmeti sunmalıdır. Diğer taraftan karar alıcılar, cari istihbarat raporları talebinde bulunmaktadır. Bu raporlar sayesinde mevcut politikalarla ilgili daha doğru kararlar alınabilmektedir. Cari istihbarat genellikle bir ya da iki haftalık geleceğe yönelik analiz ve raporlardan oluşmaktadır (Lowenthal, 2012, s.122). İstihbarat kurumları, müşteriye çeşitli bilgi ve belgeleri sunarak onlara yardımcı olmaktadır. Ancak bunu yaparken istihbarat elemanı/yöneticisi, tavsiyede bulunmaktan kaçınmalıdır.

İstihbarat kurumu için bir diğer önem teşkil eden konuysa, müşterinin (karar alıcının) kendisine verdiği görevleri yerine getirirken, işi doğru yapmak kaygısına kapılmasıdır. Bu kaygı istihbarat elemanının, doğru işi yapmak gerçeğini görmesini engellemektedir. Siber İstihbarat, günün şartlarına uygun bir biçimde, geleneksel istihbarat yöntemleri ile birlikte etkin bir şekilde kullanılması halinde daha hızlı

istihbarat oluşturulmasını sağlamaktadır. Gelişmiş ülkelere bağlı gizli servisler siber istihbarat aracılığıyla ulusal güvenliğin sağlanmasında aktif rol oynamakta, karar alıcılara strateji ve politika oluşturulması konusunda da yardımcı olmaktadır.

1.2. İstihbarat Tanımları

İstihbarat ile ilgili yapılan tanımlar, istihbarat kavramını tek başlarına açıklamakta yetersiz kalmaktadır. Gerek kitaplarda gerekse de akademik yayınlarda yapılan istihbarat tanımları, genellikle birbirine benzemektedir ve entelijans ve istihbar kelimelerinin anlamlarına dayandırılmaktadır. Oysa ki istihbarat, sadece haber toplamak ve bunları akıl yoluyla işlemek değil, aynı zamanda devamlılık gösteren ve bir takım kurallardan oluşan faaliyetler sürecidir.

Dünya genelinde, iç ve dış istihbarat oluşturmakla görevli her kurum, kendi yetkisi ve görevi çerçevesinde çeşitli tanımlar yapmış olup, tam olarak istihbaratın ne olduğu konusunda net bir açıklama getirmemektedir. İstihbarat teşkilatlarında görev yapmış kimseler tarafından yapılan tanımlar da aynı şekilde, bağlı olduğu kurumda kendisine verilen görevler nispetinde olmuştur. Dolayısıyla da tüm bu tanımlar tek başlarına istihbaratın ne olduğu ve ne olmadığı konusunda kesin bir bilgi sunamamaktadır.

İstihbaratın tanımının net bir şekilde yapılamamasındaki bir diğer önemli konu da istihbaratın sadece açık kaynaklardan değil, aynı zamanda gizli faaliyetlerle de yapılmasıdır. Bu faaliyetlerin içeriği, nasıl yapıldığı gibi konularda, daha önce uzun yıllar iç ve dış görevlerde bulunmuş emekli istihbaratçıların hatıratları ve kitaplarında anlatıldığı kadar gün yüzüne çıkmaktadır.

Dolayısıyla istihbarat seksiyonu içinde yer alan kişi, unvan, birim ve yöntem gibi konular hakkında kesin bir bilgi bulunmamaktadır. Daha doğru bir ifadeyle, bu ögeler her kurum içinde farklılık göterebilmektedir ve bu sebeple de istihbaratla ilgili genel geçer bir tanımın yapılması da oldukça güçtür.

İstihbarat denildiğinde akla gizlilik de gelmektedir. Gizliliğin olduğu yerde, teknolojinin de kullanılması günümüz şartlarında artık kaçınılmazdır. Teknolojinin,

istihbarat ve siber istihbarat gibi kavramlar dahilinde etkin bir şekilde kullanılmaması halindeyse gizliliğin sağlanması söz konusu olmamaktadır. Bu durumda da istihbarat teşkilatının iyi bir İKK çalışması yaptığından söz edilememektedir. Siber uzay üzerinden elde edilen bilgi hızlı ve geniş bir hacme sahiptir. Dolayısıyla da bu bilginin doğruluğunun teyidi ve analiz edilmesi de siber istihbaratı daha karmaşık bir hale sokmaktadır. Bundan hareketle, sadece istihbaratın değil, aynı zamanda siber istihbaratın da doğru bir şekilde tanımlanması gerekmektedir.

İstihbarat, geleneksel haber alma teknolojilerinden siber teknolojilere, insani istihbarat toplama yöntemlerinden kriptografiye kadar geniş bir yelpazeye sahiptir. İstihbarat, dışarıdan gözlemlendiğinde, dar kapsamda gizli faaliyetler sonucu haber ve bilgi toplamak olarak değerlendirilse de psikoloji ve yabancı dil uzmanlığı gibi pek çok farklı alanı da içinde barındırır ve hayal edilenden çok daha büyük bir faaliyete ev sahipliği yapmaktadır. Bu anlamda istihbarata bir bilim dalı olarak, gerekli önemin verilmesi ve istihbarata akademik açıdan bakılması, incelenmesi gerekmektedir. İstihbaratın ne olduğunu incelemeden önce, istihbarat kelimesinin anlamına ve bu konuda yapılmış tanımlara bakmakta fayda vardır.

Çeşitli sözlüklerde istihbarat; "akıl, zeka, malumat, haber, bilgi, havadis, bilgi toplama, haber alma" şeklinde tanımlanmaktadır. Arapça'da haber, bilgi alma anlamına gelen istihbar kelimesinin çoğulu olan istihbarat, İngilizce ve Fransızca gibi dillerde ise "intelligence" yani "akıl, zeka" şeklinde ifade edilmektedir. Bu sebeple, geçmiş yıllarda görev almış emekli istihbarat elemanları bugün dahi istihbarat yerine Fransızca'dan dilimize geçen "entelijans" sözcüğünü kullanmaktadır. İstihbarat, TDK'nın modern Türkçe sözlüğünde "Yeni öğrenilen bilgiler, haberler, duyumlar" ve "Bilgi toplama, haber alma" olarak tanımlanmıştır[3].

Görüldüğü üzere, aynı coğrafyada yüzyıllardır yaşamakta olan toplumlar, istihbaratı farklı şekillerde yorumlamaktadır. Arapça ve Türkçe'de istihbarat, haber toplamak şeklinde tanımlamaktayken, Batılılar akıl ve zeka kullanarak, elde edilen

[3] http://www.tdk.gov.tr/index.php?option=com_gts&kelime=İSTİHBARAT, Erişim tarihi: 08 Aralık 2017.

bilginin analiz edilmesi şeklinde değerlendirmektedir. İstihbaratı kısaca tanımlayacak olursak, "toplanan haberin, akıl ve zeka yardımıyla işlenmesi faaliyeti" olarak ifade etmek mümkündür. Bu basit tanımdan yola çıkarak, istihbarat hakkında yapılmış farklı tanımları incelemek daha açıklayıcı olacaktır.

ABD Genel Kurmay Başkanlığı Askeri Terimler Sözlüğü'ndeyse istihbarat, "Yabancı devletler, düşman veya potansiyel düşman kuvvetler, ögeler veya mevcut/olası operasyon bölgeleri hakkında toplama, işleme, bütünleşme, değerlendirme, analiz ve yorumlama işlemlerinden geçen bilgilerin, üretilmesi sürecidir" şeklinde ifade edilmektedir[4]. ABD Genel Kurmay Başkanlığı, konuyu daha ziyade operasyonel anlamda ele almış ve istihbarat faaliyetlerini düşman kuvvetler ve onların mevcut/potansiyel operasyon bölgeleriyle kısıtlamıştır. Buradan hareketle, askeri istihbarat servislerinin, müşterilerine daha çok, taktik ve operasyonel istihbarat konularında destek verdiği söylenebilir.

ABD'nin dış istihbarat oluşturmakla görevli gizli servisi CIA'in resmi sitesinde yayınlanan bir makalede istihbarat basit haliyle şu şekilde tanımlanmıştır: "İstihbarat, etrafımızdakilerle ilgili bilgi ve önbilgidir. Amerikan karar alıcılarının, karar ve faaliyetlerinin başlangıcıdır" (Warner, 2002, s.16). Warner ayrıca istihbaratı güvenlilir kaynaklara dayanan, etkili yöntemler sayesinde devlet görevlileri tarafından, devlet için toplanan bilginin üretilmesi ve dağıtılması süreci olarak da tanımlamaktadır.

Warner, yapmış olduğu bu tanımda "etrafımızdakilerle" sözüyle, diğer ülkelere karşı istihbari faaliyetlerde bulunarak, politika yapıcıların doğru karar vermelerini sağlamak açısından önemli derecede bilgi paylaşımında bulunduklarının altını çizmektedir. Bu tanım, istihbarat faaliyetlerini diğer ülkelerle kısıtlamaktadır. Oysa ki devlet çapında istihbarat, iç güvenlik ve iç politika için de yapılmaktadır. Buna örnek olarak ülkemizde EGM'ye bağlı İstihbarat Daire Başkanlığı ve Jandarma İstihbarat Başkanlığı verilebilir.

[4] http://www.dtic.mil/doctrine/new_pubs/dictionary.pdf, Erişim tarihi: 08 Aralık 2017.

Bir başka ABD gizli servisi FBI'ın resmi web sitesinde ise istihbarat, "Politika yapıcıların ulus güvenliğini tehdit eden unsurlara karşı doğru karar vermeleri için gerekli olan analiz edilmiş ve arıtılmış bilgidir" şeklinde ifade edilmiştir. Aralarında FBI'ın da bulunduğu ABD İstihbarat Konseyi'nin içinde yer alan kurumlar ise istihbaratı üç farklı şekilde tanımlamaktadır:

1. İstihbarat, karar alıcıların ihtiyaçlarını karşılayacak, arıtılmış bilgiden oluşan bir üründür.
2. İstihbarat, ayrıca bu bilginin tanımlandığı, toplandığı ve analiz edildiği bir süreçtir.
3. İstihbarat, karar alıcıların kullanımı için ham veriyi, istihbarat ürününe dönüştüren her örgütün ve bu örgütlerin oluşturduğu daha büyük topluluğa denilmektedir[5].

FBI ve ABD Ulusal İstihbarat Konseyi içinde yer alan kurumların yapmış olduğu bu son tanım, aslında istihbaratı en iyi tanımlayan ifadelerden biridir. Bu tanımla birlikte istihbarat ne sadece askeri ve dış operasyonlarla kısıtlanmıştır ne de sadece bir ürün olarak görülmektedir. İstihbaratı tüm bunları kapsayan bir faaliyetler bütünü olarak ele almaktadır.

Devlet çapında istihbarat oluşturmakla görevli olan Milli İstihbarat Teşkilatı'nın resmi sitesinde ayrıca, istihbaratın üretilebilmesi için sadece haber, bilgi ve belgenin toplanmasının yeterli olmadığı, edinilen haber, bilgi ve belgenin belli bir sistematik içinde işlenmesi gerektiği ifadesine yer verilmiştir[6].

MİT ayrıca, teknik olarak istihbarat kelimesinin kapsamının haberlerin işlenmesi, sonucu üretilen bir ürün veya bilgi olduğuna değinmiş ve istihbarat tekniğinin, faaliyet ve teşkilat itibariyle olması gereken konu ve organları içine aldığını belirtmiştir.

[5] https://www.fbi.gov/about/leadership-and-structure/intelligence-branch, Erişim tarihi: 09 Aralık 2017.
[6] http://www.mit.gov.tr/isth-olusum.html, Erişim tarihi: 09 Aralık 2017.

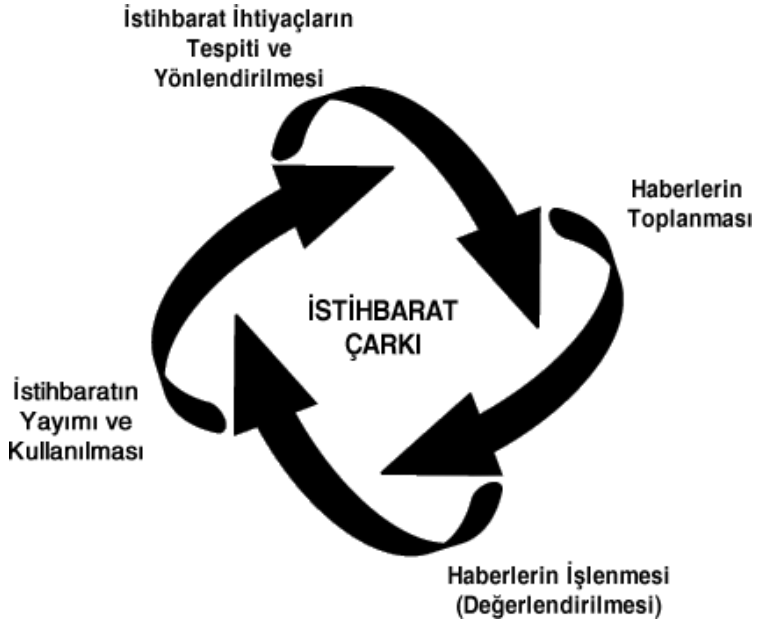
Bir başka deyişle MİT'e göre istihbarat; planlama, araştırma, delil toplama, çeşitli akli ve tecrübi ilim yöntemleri kullanarak bunların değerlendirilmesi ve analiz edildikten sonra raporlanması faaliyetleridir. MİT'in yapmış olduğu istihbarat tanımı mevcut tanımlar içinde en kapsamlısı olup, istihbaratı bir ürün ve faaliyetler bütünü olarak ele almaktadır.

1.3. İstihbarat Çarkı

İstihbarat, kesintisiz olarak süren, bir başka deyişle hiç durmadan devam eden bir süreçtir. Ham bilgilerin istihbarat haline gelebilmesi için tasnif, kıymetlendirme, yorum ve yayım aşamalarından geçmesi gerekmektedir. Dünya üzerindeki tüm istihbarat teşkilatları bu süreci, kesintisiz olmasından dolayı bir çarka benzetmektedir.

Çeşitli istihbarat teşkilatları, bu çarkı beş, hatta altı aşamalı olarak göstermektedir. Milli İstihbarat Teşkilatı'nın resmi sitesinde istihbarat çarkı, dört aşamalı olarak ele alınmaktadır. İstihbaratın Türkiye'deki kamu güvenliği için rolü ve önemi incelendiği için bu çalışmada MİT'in istihbarat çarkının aşamaları ele alınmaktadır.

Çizelge 1: MİT İstihbarat Çarkı



Kaynak: MİT, "İstihbarat Oluşumu", http://www.mit.gov.tr/isth-olusum.html, Erişim tarihi: 09 Aralık 2017.

1.3.1. İhtiyacın Tespiti ve Toplama Çalışmalarının Yönlendirilmesi

İstihbarat teşkilatları, ürettiği istihbaratı müşterilerine sunmaktadır. Müşteri ise ihtiyaç duyduğu istihbarat ile ilgili talepte bulunmaktadır. Bu talep doğrultusunda da istihbarat ihtiyacının tespiti aşaması başlamaktadır. Devlet çapında istihbarat oluşturulması halinde müşteri, karar alıcılardır. Karar alıcılar, ihtiyaç duyduğu bilgilerin toplanması için istihbarat teşkilatlarından istekte bulunarak, istihbarat çarkını harekete geçirmektedir.

İstihbaratın diplomasiye de yardımcı olması beklenmektedir. Bundan hareketle istihbarat teşkilatları, diplomatları, dış birim görevlilerini ve dış politika konusunda karar alıcıları bilgilendirme, karar verme ve destekleme görevlerini de üstlenmektedir (Köseli, 2011, s.12). İstihbaratın görevleri arasında herhangi bir çatışma olasılığına karşı, konuya ilişkin olasılık ve fırsatları tespit etmek, devlete karar alma hususunda yardımcı olacak istihbari bilgileri sağlamak, devleti ve vatandaşı koruyarak güvenliği maksimize etmek gibi görevleri bulunmaktadır (Gill, 2006, s.8).

Bu sayılan görevler çerçevesinde, öncelikle istihbarat ihtiyacı tespit edilmektedir. Bir başka deyişle istihbarat, bir ihtiyaç ve talep üzerine oluşturulmaya başlanmaktadır. Aksi takdirde her konuya ilişkin bilgi edinmek ve bunları değerlendirerek bir istihbarat haline getirmek gerek bütçe, gerek zaman gerekse de insan kaynağı açısından büyük zorluklar demektir. Hızlı ve etkin bir istihbarat için öncelikle ihtiyacın doğru bir şekilde tespit edilmesi gerekmektedir.

İstihbarat ihtiyaçlarının doğru tespit edilememesi halinde, gerek insan kaynağı gerekse de zaman anlamında gereksiz kayıp yaşanabilmektedir. Bunun önüne geçebilmek için karar alıcıların talimatları ile istihbarat memurlarının ortak görüşleri doğrultusunta istihbarat tespiti oluşturulmalı ve çarkın birinci evresine geçilmelidir.

Çarkın birinci evresi olan bu süreçte toplama planı hazırlanmakta, bilgi toplama emirleri yayınlamakta ve haber toplama çalışmaları yönlendirilmektedir. Yönlendirmenin yapılmasıyla birlikte artık haberlerin toplanması aşamasına geçilmektedir.

1.3.2. Haberlerin Toplanması

İstihbarat çarkının ikinci evresindeyse, açık ve gizli kaynaklardan haber toplanmaktadır. Açık kaynaklar; gazete, radyo, televizyon kitap, internet siteleri, blog sayfaları ve sosyal medya hesapları gibi yayınlardan oluşmaktadır. Bu kaynaklar üzerinden istihbarat oluşturulmasınaysa açık kaynak istihbarat denilmektedir. Açık kaynak istihbarat, daha az tehlikeli olmakla birlikte, çok daha az maddi kaynak ihtiyacı doğurmaktadır. Açık kaynak istihbaratın en büyük dezavantajı, haberlerin doğruluğunun tespit edilmesinin zorluğudur.

Gizli kaynaklarsa çeşitli istihbarat yöntemleri kullanılarak haberin elde edildiği kaynak olarak adlandırılmaktadır. Haberler, teknik veya insani istihbarat yöntemleriyle toplanmaktadır. Gizli kaynaklardan elde edilecek haberler, görece olarak daha hassas bilgileri içerebilmektedir. Bu sebeple sadece analiz uzmanlarının değil, haberi toplayacak personelin de özel eğitimli olması gerekmektedir. Bir başka deyişle gizli kaynaklardan haber toplamak için daha fazla uzmanlık alanine ihtiyaç duyulmaktadır.

1.3.3. Haberlerin İşlenmesi (Değerlendirilmesi)

Açık ve gizli kaynaklardan elde edilen haberler daha sonra bilgi ve belgelerin tasnifi, kıymetlendirilmesi ve yorum aşamasından geçirilerek, değerlendirme süreci başlamaktadır. Değerlendirme sürecinde, karargaha gelen bilgiler doğruluk, önem vb. açılardan ele alınarak bir değerlendirmeden geçmektedir.

Daha sonra küresel ve bölgesel gelişmeler, devletlerin karar mekanizmaları ve süreçleri, ilişkileri, dış politikaları vb. göz önüne alınarak analiz edilmektedir. Analiz, farklı istihbarat teşkilatlarınca ayrı bir süreç olarak da ele alınmaktadır. Haberin değerlendirilmesi sürecine ayrıca haberin işlenmesi de denilmektedir.

1.3.4. İstihbaratın Yayımı ve Kullanılması

Haber, değerlendirme sürecinden geçtikten sonra artık işlenmiştir ve istihbarat niteliği taşımaktadır. Yayım ve kullanım aşamasında istihbarat, zamanında ve etkin bir şekilde müşteriye ulaştırılmaktadır. Karar alıcılar da kendisine sunulan bu bilgileri

amaçları doğrultusunda kullanmaktadır. İstihbarat çarkından da anlaşılacağı üzere gizli servisler, karar alıcılara önemli ölçüde destek sağlamaktadır.

Yukarıda yer alan istihbarat çarkı ve bu çark içindeki her bir süreç devamlı olarak gözden geçirilmektedir. Yeni istihbarat ihtiyaçlarının tespit edilmesiyle birlikte çarkın ilk safhasına geri dönülmektedir ve ardından yine yayım ve kullanıma kadarki faaliyetler devam etmektedir.

İstihbarat, raporlama türlerine göre de değişiklik arz etmektedir. Özdağ'a göre cari tanımlayıcı istihbarat, temel tanımsal istihbarat ve spekülatif değerlendirme istihbaratı olmak üzere üç çeşit istihbarat türü vardır ve raporlamalar bunlara göre yapılmaktadır. Cari tanımlayıcı istihbarat, üzerinde çalışılan konuya matuf son gelişmelerle ilgili bilgi toplanmasıdır. Cari tanımlayıcı istihbarat, genellikle bir veya iki değişik kaynaktan gelmektedir ve en çok üretilen, en pahalı istihbarat ürünüdür. "Bir süre önce ne oldu?" ve "Şimdi ne oluyor?" gibi soruların cevapları cari istihbarat raporlarında yer almaktadır.

Temel tanımsal istihbarat ise istihbartın kalbi ve ruhu olarak tanımlanmaktadır. Temel tanımsal istihbaratın hedefi; sabit veri, malumat ve bilginin toplanmasıdır. Bir ülkenin mevcut askeri kapasitesi, petrol üretimi, komşu ülkelerle ilişkileri gibi konular, temel tanımsal istihbarat raporlarının konusunu oluşturmaktadır. Temel tanımsal istihbarat yapılabilmesi için, ülkenin tarihi, stratejik önemi, politik, ekonomik ve sosyal konumu hakkında bilgi toplanması faydalı olmaktadır.

Spekülatif değerlendirme istihbaratı ise, daha çok geleceğe yöneliktir ve çeşitli öngörülerde bulunmaktadır. Yaklaşılan olaya göre spekülatif değerlendirmeci istihbarat; stratejik, operasyonel ve taktik istihbarat niteliği de taşıyabilmektedir. Bu sebeple özellikle değişik zamanlarda tekrarlayan olayların incelenmesiyle geliştirilen kurallara dayanılarak yapılmaktadır. Örneğin bir ülk rejiminin devrilip devrilmeyeceğine ilişkin analizler, spekülatif değerlendirmeci istihbarat raporlarında yer almaktadır (Özdağ, 2013, s.240-242).

Tablo 1: Örnek İstihbarat Çarkı Senaryosu

İstihbarat Çarkı	**Örnek Olay**	**Kurumlar**
İstihbarat İhtiyacı	İsrail, Kudüs'ün başkenti olması konusuna ilişkin Filistin'den başka bölgedeki ülkelere yaptırım uygulayabilir mi? Bu yaptırımlar askeri bir harekatla sonuçlanır mı?	- Cumhurbaşkanlığı - Başbakanlık
Planlama	Karargah, İsrail ve cari politikaları hakkında bilgi toplanması için görevi, imkan ve kabiliyetlerine göre bünyesindeki birimleri görevlendirir. Dışişleri Bakanlığı ilgili devletlerle temasa geçerek diplomasi süreci başlatır. Genelkurmay Başkanlığı bölgede yaşanabilecek askeri operasyonların Türkiye'ye sıçraması olasılığını değerlendirir ve gerekli hazırlıkları başlatır.	- Dışişleri Bakanlığı - Genelkurmay Başkanlığı
Toplama	Toplama birimleri tarafından haberin hangi kaynaklardan toplanacağı planlanır. İlgili görevliler tarafından açık ve gizli kaynaklardan bilgi toplanır.	- MİT Yurtdışı Birimleri - MİT Bölge Birimleri - Büyükelçilikler - Askeri Ataşelikler
Değerlendirme ve Analiz	Karargaha toplama birimleri ve sair kaynaklardan gelen bilgileri, doğruluğu ve önemi gibi hususlara göre değerlendirir. Bu bilgiler daha sonra konu devletlerin karar alıcıları, devlet mekanizmaları, dış politikaları, diğer ülkelerle ilişkileri ile, yaşanmış olaylar vb. dikkate alınarak analiz edilir.	- Karargah
Raporlama ve Yayım	Değerlendirilen ve analiz edilen bilgiler, istihbarat raporuna dönüştürülür. Oluşturulan bu raporlarsa daha sonra ilgili kurumlara gönderilir.	- Karargah
Kullanım	İstihbarat teşkilatı tarafından sunulan raporlar kullanılarak, karar verilir.	- Cumhurbaşkanlığı - Başbakanlık

1.4. İstihbaratın Sınıflandırılması

İstihbaratın bir bilim dalı haline gelmesiyle birlikte, çeşitli sınıflandırmalara gidildiği de görülmektedir. Bu sınıflandırmalardan bazıları temel olarak tüm gizli servislerde aynı şekilde ele alınmaktadır. İstihbarat bugün, sadece askeri alanı değil ekonomi, sosyoloji, teknoloji, siyasi vb. pek çok farklı alanları kapsamaktadır.

İstihbaratı ayrı birer uzmanlık alanı haline dönüştürmek ihtisaslaşmayı da beraberinde getirmektedir. Örneğin aynı gizli servis içinde çalışmakta olan bir kontr terör uzmanı ile İKK uzmanı, aynı seksiyon içinde, farklı alanlarda görev almaktadır. Bir başka deyişle her ikisi de istihbaratçı olmasına karşın, uzmanlık alanları farklılık göstermektedir. Bu da istihbarat faaliyetinin daha etkin yapılmasını sağlamaktadır. Özdağ, istihbaratı alanlarına, toplama tekniklerine ve ölçeklerine göre sınıflandırmaktadır (Özdağ, 2013, s.55-115-131).

1.4.1. Ölçeklerine Göre İstihbarat

Bu başlığın alt başlıklarında stratejik, operasyonel ve taktik istihbarat konuları örneklerle açıklanmaya çalışılacaktır.

1.4.1.1. Stratejik İstihbarat

Temel olarak askeri bir terim olan strateji, bir ulus ya da uluslar topluluğunun savaş ya da barış döneminde, benimsenen politikalara en çok desteği verebilmek maksadıyla ekonomik, politik, psikolojik ve askeri güçleri bir arada kullanma bilimi ve sanatı olarak nitelendirilmektedir7. Strateji ayrıca, askeri kıtaların savaş meydanlarında nasıl konuşlanacağını, nereye hangi yollarla sevk edileceğini planlamak için kullanılan bir terimdir.

Strateji, savaşın hedefini elde etmek için muharebeyi kullanma sanatıdır. Bir başka deyişle strateji, savaşın planlanmasıdır ve son karara kadar gerekli olan tüm süreçleri kapsamaktadır (Clausewitz, 1996, s.177). Ancak stratejinin askeri alanla kısıtlanması günümüz modern dünyasında doğru değildir. Ertuğrul Güven strateji için

[7] http://www.tdk.gov.tr/index.php?option=com_gts&kelime=STRATEJİ, Erişim tarihi: 10 Aralık 2017.

"gücün doğru zamanda doğru yerde kullanılmasıdır" demiştir. Güven ayrıca stratejik istihbaratın, stratejinin etkin bir şekilde kullanımı için gerekli olan bilgilerin toplanması ve analiz edilerek amaca uygun kullanılması olduğunu belirtmiştir (Güven, 2013, s.124). Stratejik istihbarat sayesinde karar alıcılara diğer devletlerin politikaları, kültürel eğilimleri, niyetleri, kapasiteleri, kısıtlamaları, hassas noktaları, projeleri, yatırımları, dost ve düşmanları gibi kritik bilgiler sunulmaktadır. Bir başka deyişle stratejik istihbarat, orta ve uzun vadede rakibin imkan ve yetenekleri ile zaafları ve eksikliklerini önceden tespit ederek, geliştirilecek politikayı yönlendirmek, yardımcı olmak için kullanılmaktadır.

1.4.1.2. Operasyonel İstihbarat

Operasyonel istihbarat, ilk olarak Prusyalı general Friedrich Wilhelm Freiherr von Bülow tarafından öne sürülmüş bir kavram olup, büyük elçilik ve generallik gibi yüksek mevkide olan ancak nihai siyasi karar alma gücüne sahip olmayan kişilerin yaptığı istihbari faaliyetlerini ele almıştır (Özdağ, 2013, s.138). Askeri anlamda operasyonel istihbarat, kuvvet komutanına ihtiyaç duyduğu bilginin ulaştırılması için gereken desteğin verilmesi için kullanılmaktadır.

Ana merkezle devamlı irtibatta olan ve operasyon alanı, düşman birliğinin nitelik ve niceliğini tespit etmeye yönelik istihbaratın toplanmasını ifade etmektedir. Bir terör örgütünün eylem hazırlığı içinde olması ve bunun öğrenilmesi üzerine, istihbarat teşkilatının eylemciler hakkında kimlik bilgisi, personel sayısı, morali, gücü, iletişim yöntemleri ve işbirlikçileri gibi bilgilerin toplanmasına yönelik çalışmalar, operasyonel istihbarat faaliyetleri kapsamında yer almaktadır.

1.4.1.3. Taktik İstihbarat

Taktik istihbarat, sürmekte olan bir operasyon için gerekli bilgilerin toplanmasıdır. Karşı tarafın amacını, ne yaptığını veya neler yapabileceğini tespit etmek için kullanılmaktadır (Köseli, 2011, s.29). İstihbaratçı operasyonun başındaki kişiye, yani yöneticisine aldığı bilgiyi anında gönderir. Askeri anlamda taktik istihbarat, düşman birliklerinin sayısı, silah tipi ve sayısı, bulunduğu coğrafya ve nerede konuşlandığı, örgüt yapısı, malzeme ve teçhizat sayı ve özellikleri, taktiklerinin

neler olabileceği, askerin morali, kumanya ve malzeme kalitesi, önceki deneyimleri ve komutanları hakkında toplanan istihbarattır.

Taktik istihbarat mevcut tüm imkanlar kullanılarak kara, hava, deniz ve uzay üzerinden yapılabilmektedir. Bugün, harbin beşinci boyutu olan siber uzay üzerinden de taktik istihbarat yapılmaktadır. Siber uzay üzerinden elde edilen istihbaratın hızlı ve güncel olması, müşterilere yani karar alıcılara zamanında gönderilmesi açısından çoğu durumda tercih sebebidir (Keleştemur, 2015, s.49). Siber istihbaratın, taktik istihbarata matuf kullanımı, özellikle terör faaliyetlerinin tespiti ve önlenmesi açısından büyük önem arz etmektedir.

Tablo 2: İstihbarat Ölçekleri

Stratejik İstihbarat	**Operasyonel İstihbarat**	**Taktik İstihbarat**
Ulusal strateji ve politikanın gelişmesine katkı sağlar	Düşman ordusunun kapasite ve niyetine odaklanır	Muharebe, angajman ve diğer askeri faaliyetlerin planlanması ve yürütülmesini destekler
Uluslararası ya da küresel durumu gözlemler	Operasyon ortamını analiz eder	Operasyon ortamındaki olası tehlikeler ve değişimlerle ilgili komutanı bilgilendirir
Askeri planların geliştirilmesine yardımcı olur	Kritik zafiyetlerleri tespit eder	Düşman hakkında nitelik ve nicelik bakımından komutanları bilgilendirir
Askeri araç gereç ve silah sistemleri ihtiyaçlarının tespitine yardımcı olur	Genel kurmay başkanının ilgi alanına yönelik faaliyetleri gözlemler	
Stratejik operasyonların yönetilmesini destekler	Askeri harekatların planlanması ve yönetilmesini destekler	

Kaynak: http://www.dtic.mil/doctrine/new_pubs/jp2_0.pdf Joint Intelligence, Joint Publication 2-0, 2013, Erişim tarihi: 10 Aralık 2017.

1.4.2. Alanlarına Göre İstihbarat

Bu başlık ve alt başlıklarında alanlarına göre istihbarat olarak; siyasi, askeri, ekonomik, sosyal, coğrafi, biyografik, ulaştırma ve iletişim, bilim ve teknik ile siber istihbarat konuları örneklerle açıklanmaya çalışılacaktır.

Her devlet, rakip ve hasım devletlerin mevcut ve olası güç unsurları hakkında bilgi sahibi olmak istemektedir. Bu bilgi stratejik istihbarat ile elde edilmektedir. Bir başka deyişle, stratejik istihbarat faaliyetleri sonucu bir ülkenin milli gücü tespit edilebilebilmektedir. Milli güç, bir ulusun bir başka ulus üzerinde baskı uygulamak için kullandığı askeri ya da barışçıl metotlar ve bunlara bağlı baskı gücüdür. Bu güç ulusun tarihi, siyasi, askeri, psikolojik, ekonomik vb. etkenlerine bağlı olarak değişim göstermektedir (Hirschman, 1992, s.13).

Özdağ ise bu tanımı biraz daha açarak milli gücün bir devletin gerçekleştirmek istediği hedeflere ulaşmak için kullandığı nüfusu, yeraltı ve yerüstü kaynakları, sanayii gibi varlıklarını ifade ettiğini belirtmiştir (Özdağ, 2013, s.55). Karar alıcıların, diğer devletlerle olan dış politikaları ve sair ilişkilerinin belirlenmesi ve hedeflerin gerçekleştirilmesi için, milli güç unsurlarının bilinmesi gerekmektedir. Bu noktada devreye istihbarat teşkilatları girmektedir. İstihbarat teşkilatı tarafından, ihtiyaç duyulan bu bilgiler sunulmadığı takdirde, karar alıcının durumu karanlık bir odada, ışık olmadan yürümeye benzemektedir.

1.4.2.1. Siyasi İstihbarat

Günümüzde politika ve siyasetle ilgili çeşitli tanımlar yapılmaktadır. Öztekin'e göre siyaset, en büyük kamu tüzel kişiliği olan devletten, küçük bir örgüte kadar tüm örgütleri kapsamaktadır. Ayrıca bir örgütün farklı konulardaki eylem ve planları da o örgütün belirli bir konuya ait izlediği siyaset olarak nitelendirilmektedir (Öztekin, 2014, s.23).

Siyaset içinde yer alan tüm örgütler ve bu örgütlerin izlediği ve izlemesi olası siyasetini tespit etmek için siyasi istihbarat yapılmaktadır. Siyasi istihbarat yapmadan

önce, hedef ülkenin kültürünü, tarihini ve inançlarını iyi bilmek gerekmektedir. Mevcut toplumsal yapı ve ülkenin yönetimi, geçmişe de dayanmaktadır.

Devletin yönetim biçimi, anayasal düzeni, yasa ve kararların alınması sırasında ne gibi engellerin çıkabileceği, siyasi partilerin mevcut ve olası oy oranları gibi konular siyasi istihbaratın faaliyet alanı içinde yer almaktadır. Siyasi istihbaratın konusu olan ögelere ilişkin bilgilere günümüzde gazete, radyo, dergi ve televizyon gibi kaynaklar sayesinde kolayca ulaşılabilmektedir. İnternetin dünya genelinde yayılmasıyla birlikte gerek internet siteleri gerekse de sosyal medya hesaplarını takip ederek daha hızlı bir bilgi toplama faaliyeti söz konusu olmaktadır.

1.4.2.2. Askeri İstihbarat

Sun Tzu ve Napolyon gibi komutanlar, istihbaratı etkin bir şekilde kullanarak savaş alanlarından galip ayrılmışlardır. Sun Tzu, "Devlet ve usta komutan, casusluk amacıyla ordunun istihbarat gücünü en iyi şekilde kullanırsa, büyük başarılar elde eder. Casus kullanımı, savaşın en önemli unsurudur. Çünkü ordunun hareketleri buna bağlıdır" sözüyle askeri alanda istihbaratın ne kadar önemli olduğunu vurgulamıştır.

Ordunun casusluk kanadını en iyi kullanan hükümdar bilgi hükümdar, en iyi değerlendiren komutansa usta komudandır. Casusluk sonuç getirir. Ordunun harekattaki başarısı casusların becerisi ile orantılıdır. Bilge Komutan Sun Tzu ayrıca iyi bir komutanın, diğer askerlere göre kolaylıkla savaş kazanıp, zafere ulaşmasını da istihbarata bağlamaktadır. (Sun Tzu, 2008, s.83).

Askeri istihbarat, bir ülkenin askeri kapasitesini, askerin moralini, teknik imkanlarını, muharebe ve savunma gücünü tespit etmek için oluşturulan istihbarattır. Askeri istihbarat sadece düşman hakkında değil, düşmanın bulunduğu kara, deniz, hava, uzay ve siber uzayı kapsayan harekat alanlarını da kapsamaktadır. 19. yy'a kadar askeri istihbaratın daha çok, insani istihbarat ile yapıldığı görülmektedir. Daha ilerleyen dönemlerde, özellikle II. Dünya Savaşı ile birlikte teknik istihbarat da kullanılmaya başlanmıştır. Günümüzdeyse, özellikle siber istihbaratın gelişmesiyle birlikte, mikro saniye hızında bilgi transferi yapılabilmektedir.

1.4.2.3. Ekonomik İstihbarat

Devletlerin hedeflerine ulaşabilmesi için yeterli ekonomik güce sahip olması gerekmektedir. Bir ülkenin ekonomik gücü refah, mutluluk, güvenlik ve gelişim için kullanılan kaynakların toplam kapasitesi ve bu amaçlar için üretilen değerlerin oluşturduğu sonuçtur8. Ekonomik istihbarat, rakip ya da hasım ülkelerin genel ekonomik durumları ile sanayi, ticari, tarım, ham madde, stok, ambargo, dış borç, bağımlılık ve vergi gibi konulara ilişkin, karar alıcıları bilgilendirmek üzere yapılan istihbarattır.

Ekonomik istihbarat ile ülkenin üretim gücü hakkında bilgi edinilebileceği gibi, aynı zamanda dünya ekonomisine sunduğu ürünlerin, pazarı ne kadar etkileyeceği gibi küresel verilere de ulaşmak mümkündür. Ekonomik istihbarat, göreceli olsa da daha ekonomik ve hızlı bir şekilde yapılabilmektedir. Zira, bir ülkenin ekonomik durumuyla ilgili bilgi almak için açık kaynaklar kullanılabilmektedir.

İstihbaratın elde edilmesi için yüzde 90 oranında açık kaynaklardan faydalanılmaktadır (Güven, 2013, s.119). Ekonomik gelişmelerin tespiti için uydular aracılığıyla çekilen fotoğralar da önemli derecede yardımcı olmaktadır. Bu fotoğraflar sayesinde yeni oluşturulan alanlar, yeni inşa edilen yapılar ve coğrafi değişimler de o ülkeye ait ekonomik değişimleri gösterebilmektedir.

1.4.2.4. Sosyal İstihbarat

Toplumların tarihleri, kültürleri, yaşam biçimleri ve birbirleriyle olan ilişkileri, diğer devletlerin ilgi alanına girmektedir. Özellikle örtülü operasyonların başarılı olabilmesi için, hedef ülkenin toplum yapısının bilinmesi gerekmektedir. Her ülkenin, kendine özgü bir sosyal yapısı bulunmaktadır. Sosyal istihbarat, bu yapıyı çözümlemek için gereken veri toplama ve analiz süreçlerini kapsamaktadır (Özdağ, 2013, s.84).

[8] http://www.21yyte.org/tr/arastirma/ekonomik-arastirmalari-merkezi/2014/01/20/7390/ekonomik-istihbarat, Erişim tarihi: 11 Aralık 2017.

Sosyal istihbarat, bölge ya da ülkenin nüfusu, yerleşim alanları, nüfusun artış oranları, yaş ve cinsiyet oranları, iş gücü, okuma-yazma oranları, etnik kökenleri, askerlik çağındaki erkekleri, kadınları, yaşlıları gibi pek çok özelliği kapsamaktadır. Bundan başka, bölgedeki sosyal hareketlilik, resmi ve gayrı resmi örgütler, basın yayın organları, dini gruplar ve liderler, sağlık ve sosyal güvenlik sistemi, ekonomik gelir ve gelir dağılımı gibi konular da yine sosyal istihbarat aracılığıyla öğrenilebilmektedir (Keleştemur, 2015, s.70). Bu sayılan ögelerin neredeyse tamamı bugün birçok sosyal medya platformu sayesinde analiz edilebilmektedir.

1.4.2.5. Coğrafi İstihbarat

Coğrafya, yer kabuğunu fiziksel, ekonomik, beşeri ve siyasal açılardan inceleyen bilim dalıdır. Bu tanımdan hareketle, coğrafyanın toplumlar üzerindeki etkisi büyüktür. Mekan ve insan arasındaki ilişki de coğrafyanın konusunu oluşturmaktadır. Coğrafya, geniş yönlü yapısı sayesinde bölgedeki yaşam, sosyolojik durum, siyasi kararlar ve gelecek planları gibi birçok konuda akıl yürütmek konusunda yardımcı olmaktadır.

Coğrafya, ayrıca milli güç unsurlarının haritaya işlenmesini de sağlamaktadır (Özdağ, 2013, s.96). Dolayısıyla hem karar alıcılar hem de komutanlar için ayrı önem taşımaktadır. Mustafa Kemal Atatürk'ün "Ben siyasi meseleleri de askeri vaziyetler gibi harita üzerinde mütalaa ederim" sözü, gerek bir asker gerekse de siyasetçi olarak ulu önderin coğrafya bilimine verdiği önemi vurgulamaktadır. Askeri Coğrafi İstihbarat bir alt dal olup, askeri bir operasyonu etkileyebilecek tüm fiziksel ve sınır, yeryüzü şekli, yerleşim yeri gibi unsurları içermektedir.

Coğrafi istihbarat, insana dayalı ve görüntü istihbaratı gibi farklı yöntemlerle elde edilebilmektedir. Ancak; günümüzde gelişmiş uydu sistemleri ve yazılımlar sayesinde daha kolay bir şekilde coğrafi istihbarat elde etmek mümkündür. Gelişmiş ülkeler, uzaya istihbarat amaçlı uydular göndererek, tek bir kontrol merkezi üzerinden tüm dünya üzerinde coğrafi istihbarat yapabilmektedir.

1.4.2.6. Biyografik İstihbarat

Biyografik istihbarat, toplum için mevcut ya da potansiyel önem taşıyan kişilere yönelik yapılmaktadır. Bu kişiler politik, ekonomik, kültürel ya da askeri yönden öneme sahip olduklarından, toplumu çeşitli konularda yönlendirebilmektedir. Biyografik istihbarat ayrıca, şüpheli kimselerle gizli ilişikler içinde olduğu düşünülen kişiler için de yapılmaktadır. Biyografik istihbarat oldukça uzun süreli bir faaliyet olup, hedef kişiyle ilgili, tıpkı bir elektrik süpürgesiyle çeker gibi, tüm bilgiler elde edilmektedir. Elde edilen bilgiler, şahıs hakkında analiz yapılmasını sağlamaktadır.

Biyografik istihbarat, hedef kişinin alışkanlıkları, huyları, özellikleri, yetenekleri ve ilişkileri gibi konuları kapsamaktadır. Bu konulara ilişkin bilgiler gazeteler, dergiler, biyografik ve otobiyografik kitaplarla, hatıratlar ya da internet siteleri gibi açık kaynaklardan ya da gizli faaliyetlerle elde edilmektedir (Smith, 2009, s.1). Biyografik istihbarat mafya ve terör örgütleri içinde önemli kademelerdeki kimseler ve liderlere ilişkin yapılması halinde oldukça önemli bilgiler elde edilebilmektedir.

1.4.2.7. Ulaştırma ve İletişim İstihbaratı

Teknolojinin gelişmesiyle birlikte ulaşım ve iletişimde de önemli gelişmeler yaşanmaktadır. Günümüzde 600 km/s hızı aşan trenler[9] ve ışık hızında transfer edilen dijital veriler bulunmaktadır. Sürekli gelişmekte olan ulaştırma ve iletişim teknolojilerinin takibi zordur ve özellikle istihbarat faaliyetlerinin önemli birer ögesidir.

Ulaştırma istihbaratı, bir devletin sahip olduğu kara, hava, deniz, demir yolları gibi ulaşım hatlarıyla birlikte, sahip olduğu boru hatları, su yolları, havalimanları, lojistik kapasiteleri vb. yönelik bilginin toplanması ve analiz edilmesidir. Radyo, televizyon, telefon, GSM baz istasyonları, uydu sistemleri, denizaltı kabloları, kablolu ve kablosuz ağlar gibi altyapılarsa iletişim istihbaratının kapsamındadır.

[9] https://www.theguardian.com/world/2015/apr/21/japans-maglev-train-notches-up-new-world-speed-record-in-test-run, Erişim tarihi: 11 Aralık 2017.

1.4.2.8. Bilim ve Teknik İstihbaratı

Bilim ve teknik istihbaratı bir milletin bilimsel ve teknik imkan ve kabiliyetleriyle, buna bağlı olarak faaliyetlerini tespit etmeye yönelik faaliyetlerdir (Özdağ, 2013, s.107). Bilim ve teknik istihbaratın, geçmişte özellikle askeri teknolojileri ele aldığı görülmüştür. Bu anlamda Soğuk Savaş döneminde, ABD ve SSCB'nin sürekli olarak birbirinden teknoloji çalmaya ilişkin istihbarat faaliyetleri yürüttüğü bilinmektedir. 1950'li yıllarda SSCB'nin nükleer silah ürettiği bilgisinin ulaşmasıyla birlikte ABD'li karar alıcılar bu silahların ne kadar gelişmiş olduğu ve kapasitelerinin ne olduğu gibi soruların yanıtlarını istemiştir.

Bu yanıtları vermek adına, ABD'nin dış istihbaratından sorumlu gizli servisi CIA'in, o dönem yaptığı faaliyetler bilim ve teknik istihbaratın kapsamındadır[10]. Günümüzde güçlü devlet olabilmek için sadece ekonomik ve askeri alanlarda değil, aynı zamanda bilim ve teknikte de ilerlemiş olmak gerekmektedir. Bundan hareketle, bilim ve teknik istihbarat sadece askeri alanı değil, sibernetik ve ekonomi başta olmak üzere pek çok farklı alanı kapsamaktadır.

1.4.2.9. Siber İstihbarat

Siber İstihbarat; bir ülkenin siber uzaydaki cihazları, enerji üreticileri, kabloları, internet servis sağlayıcıları, sunucuları vb donanımlarla birlikte yazılımları, ve bundan başka siber güvenlik, siber saldırı, siber istihbarat vb. faaliyetlerde bulunacak teknokratların, görevlilerin nitelik ve nicelik gibi özellikleriyle ilgili bilgi toplanması ve analiz edilmesidir.

Hedef ülkeye siber istihbarat faaliyeti gerçekleştirmeden önce, bu ülkeye ait siber uzaydaki varlıklarla ilgili bir istihbarat faaliyetinin yapılması gerekmektedir. Daha sonra siber istihbarat faaliyetlerinin başarılı olabilmesi için, siber güvenlik ve siber saldırı teknikleri ile sosyal mühendislik gibi metodolojiler kullanılarak operasyonlar

[10] https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/article04.html, Erişim tarihi: 11 Aralık 2017.

düzenlenmektedir. Bir istihbarat disiplini olarak kabul edilen Siber İstihbarat, ayrıca istihbarat toplama yöntemi olarak da kullanılmaktadır.

1.5. Toplama Yöntemlerine Göre İstihbarat

İstihbarat günün, olayın ve mekanın şartları ile imkan ve kabiliyetler nispetinde farklı yöntemlerle toplanmaktadır. Bu yöntemler, ülkenin ve dolaylı olarak da istihbarat teşkilatının gelişmişlik seviyesine göre de çeşitlilik arz etmektedir. Tarih boyunca, insana dayalı istihbarat büyük bir önem teşkil etmekteyken, bugün teknolojinin gelişmesiyle birlikte artık daha farklı ve kimi durumda daha etkin istihbarat toplama yöntemleri kullanılmaktadır.

Köseli, bilinen en eski ve her zaman önemini koruyan insana dayalı istihbaratın, teknolojik istihbarat toplama yöntemlerine göre dezavantajlarının bulunduğunu vurgulamaktadır. Köseli ayrıca, istihbarat toplama yöntemlerini insan kaynaklı ve teknik olarak ikiye ayırmıştır. (Köseli, 2011, s.66). Çağa ayak uydurabilmiş, ekonomik imkanları yüksek devletler, uzaya göndermiş oldukları uydular aracılığıyla, uydu ve görüntü istihbaratı yapabilirken, bu imkan ve kabiliyete sahip olmayan gizli servisler farklı yöntemlerle istihbarat toplamaktadır.

Bugünse, özellikle siber uzayın genişlemesi ve sunduğu imkan ve kabiliyetlerin yüksek kapasitede kullanarak, önemli ölçüde istihbarat oluşturmak mümkündür. Ancak burada dikkat edilmesi gereken husus, insana dayalı istihbarat ile teknik istihbaratın birbirine tercih edilmemesi ve kıyaslanmaması gerektiğidir. Her iki istihbarat yönteminin de bir bütün olarak kullanılması, daha doğru ve etkin istihbarat toplanması sonucunu doğurmaktadır.

1.5.1. İnsani İstihbarat (HUMINT)

İnsani istihbarat, ingilizcede human intelligence olarak isimlendirilmiş olup, Türk istihbarat seksiyonunda insana dayalı istihbarat şeklinde de adlandırılmaktadır. İnsani istihbarat, insan unsurunun kullanılarak, hedef sisteme sızma yöntemiyle ihtiyaç duyulan istihbaratın toplanmasıdır. İnsani istihbarat, açık ve gizli kaynaklardan bilgi toplama faaliyetlerini içermektedir. İnsani istihbarat legal ve illegal casusluk

yöntemleriyle yapılabilmektedir. Bir ülkeye gönderilen diplomatlar, legal casusluk faaliyetlerinde bulunabilirken, herhangi bir diplomatik unvana sahip olmayıp, sıradan yollarla hedef ülkeye sızmış bir kimsenin illegal casusluk faaliyetleri yapabilmektedir.

İnsani istihbaratın önemli zorluklarından biri de potansiyel ajanların mimlenmesi ve angaje edilmesidir. Ajan olarak hizmet etmesi beklenen kimselerin güvenilir olduğunun denetlenmesi zaman gerektiren bir süreçtir ve ayrı bir iş yükü anlamına gelmektedir. Kimi zaman bu ajanlar, çeşitli motiflere istinaden, bağlı bulundukları servislere ihanet etmek ya da birden fazla servise hizmet edebilmektedir.

İstihbarat faaliyetinde bulunmak için belirli konularda uzman olmak gerekmektedir. İstihbarat mesleğinin önemi ve çalışmaların gizliliği açısından bu durum zorunluluk haline gelmiştir. İstihbaratçılar özel yeteneklere sahip kişiler arasından seçilmektedir. Gerek iş yoğunluğu gerekse de ihtiyaç duyulan eylemlerin yüksek eğitim ihtiyacı sebebiyle, istihbaratçıların özel yetiştirilmiş olması ve zaman içerisinde kendini mesleki olarak geliştirmesi gerekmektedir (Çınar, 1997, s.131).

Ayrıca istihbari bilgi ve haberlerin toplanması için kullanılan insan faktörünü de göz önünde bulundurmak gerekmektedir. Kaynaklar yurtdışında çalışan personel, hedef bölgede yaşamakta olan yerel halk, iş adamları, savaş esirleri, mülteciler vb. olabilmektedir. Kaynağın; bilgi vermemesi, ihanet etmesi, aşırı taleplerinin olması, istihbarat birimleriyle olan ilişkisini kişisel menfaatleri için kullanması ve istihbarat prensipleri dışında hareket etmesi halinde ilişiğinin kesilmesi gerekmektedir (Köseli, 2011, s.72). Köseli ayrıca açıktan yapılan HUMINT faaliyetlerini irtibat görevlileri, gözlem, denetleme ve izleme, sorgulama, mülakat ve sızdırma şeklinde, gizli HUMINT faaliyetlerini ise muhbirler, gizli görevliler ve gizli tanıklarla yapılan çalışmalar şeklinde ayırmıştır.

1.5.2. Teknik İstihbarat (TECHINT)

Teknik istihbarat, çeşitli teknik yöntemler kullanılarak istihbarat ele edilmesini ifade etmektedir. Teknik istihbaratın sağlanabilmesi için gerekli teknoloji ve altyapıyla birlikte, bunları etkin bir şekilde kullanabilecek personele de ihtiyaç duyulmaktadır.

Teknik istihbaratın, insani istihbarata destek unsur olduğu düşünülmektedir. Ancak bugün, teknik istihbarat kullanılarak hızlı bir şekilde büyük boyutlarda verilerin elde edilebilmesi sebebiyle, kimi durumda birincil nitelik taşır hale gelmiştir.

Daha önce Amerikan gizli servisi NSA'de görev yapmış olan Edward Snowden'in sızdırmış olduğu belgelere göre Obama Yönetimi, PRISM isimli projeleri sayesinde, aralarında Microsoft, Yahoo, Google, Facebook ve Apple gibi internet ve yazılım devlerinin de bulunduğu birçok firmanın e-posta, arama motoru, video ve iletişim ağları üzerinden istihbarat elde etmiştir[11].

Günümüzde, gelişmiş devletlere bağlı istihbarat servisleri siber istihbarat başta olmak üzere diğer birçok teknik istihbarat faaliyetlerini etkin bir şekilde kullanarak hem insani istihbarata destek hem de doğrudan istihbarat oluşturmak maksatlı faaliyetlerde bulunmaktadır. CIA gibi gizli servisler ayrıca, siber istihbarata karşı koymak ve bilgi güvenliğini sağlamak amaçlı, bünyesinde çeşitli pozisyonlarda personel görevlendirmektedir[12].

1.5.2.1. Sinyal İstihbaratı (SIGINT)

Sinyal istihbaratı elektromanyetik dalgaların alınması, kaydedilmesi, değerlendirilmesi ve yorumlanması ile elde edilen istihbarattır. 19. yüzyılda gizli servislerin, telgraf haberleşmelerini deşifre etme çalışmalarıyla başlamıştır. 20. yy'dan itibaren ise etkin bir şekilde kullanılmaktadır. CIA'de 1953-1961 yılları arasında direktörlük yapmış olan Allen W. Dulles, sinyal istihbaratıyla ilgili olarak bir "devletin bir diğeriyle ilgili istihbarat elde etmek için kullanılan en iyi yöntemdi" şeklinde açıklamada bulunmuştur (Aid ve Wiebes, 2001, s.11).

Soğuk Savaş dönemindeyse Amerikan ve Rus istihbarat servislerinin SIGINT için ayırdığı bütçede önemli artışların olduğu görülmüştür. Küba Savunma Eski Bakanı Raul Castro da 1993 yılında yaptığı bir açıklamada Rusya'nın Küba'yla ilgili elde edilen stratejik askeri istihbaratın yüzde 75'ine yakınını SIGINT aracılığıyla

[11] https://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data, Erişim tarihi: 12 Aralık 2017.
[12] https://www.cia.gov/careers/opportunities/cia-jobs, Erişim tarihi: 12 Aralık 2017.

oluşturduğunu ifade etmiştir (Pantano, 2009, s.2). Sinyal istihbaratı, iletişim istihbaratı (COMINT), elektronik istihbarat (ELINT) ve telemetre istihbaratı (TELINT) gibi alt istihbarat disiplinlerini kapsamaktadır.

COMINT, iletişim hatlarının müdahale edilmesiyle istihbarat elde etmektir. COMINT, ses ve tele yazıcı trafik, video, mors kodu trafiği, faks mesajları vb. ile hava dalgaları, fiber optik kablolar gibi geniş bir iletişim hattı yelpazisini kapsamaktadır. ELINT ise iletişim dışında kalan, örneğin radar gibi farklı iletim hatları üzerinden istihbarat elde edilmesidir. ELINT, sinyal göndericinin merkezi, desteklediği sistemler ve bunların özelliklerini tespit etmeye yöneliktir. TELINT ise bugün birçok kaynakta FISINT olarak geçmektedir. Telemetri birimleri, düşmanın silah sistemlerinin operasyonel kabiliyeti, yakıt kapasitesi, menzili gibi karakteristik özelliklerini tespit etmeye yöneliktir.

1.5.2.2. Ölçüm ve İz İstihbaratı (MASINT)

Ölçüm ve iz istihbaratı, çeşitli teknik sensörler aracılığıyla kaynak alıcı vericinin izlerini algılamak, kimliklendirmek, tanımlamak ve izlemek gibi faaliyetlerle obje ya da olayın tanımlanmasını sağlamak için kullanılan istihbarat yöntemidir. Ölçüm, metrik parametrelerin toplanması için elde edilen veriyi ifade etmektedir. İz ise bilgi toplayan cihaz tarafından elde edilen olay, ekipman ya da nesnelere ait özellikleri ifade etmektedir. Bu özellikler, karşılaştırılarak yorum yapılmakta ve hedefin sahip olduğu fiziksel özellikler ve özgün karakteristikleri doğrultusunda tanımlanmasını sağlamaktadır (OPSEC, 1996, s.7).

MASINT çatısı altında radar istihbaratı (RADINT), kızılötesi istihbarat (IRINT) ve nükleer istihbarat (NUCINT), akustik istihbarat (ACINT), sismik istihbarat, manyetik istihbarat, kimyasal istihbarat ve biyolojik istihbarat gibi farklı disiplinler de bulunmaktadır. Sismik istihbarat düşmana ait hareket halindeki tank, obüs gibi askeri araçları, akustik istihbarat ise gemi ve denizaltı gibi araçları, ses ve titreşimlerinin ölçülerek tespit edilmesinde kullanılmaktadır. Ayrıca kızılötesi sensörler ve benzeri bileşenlerle hedeflerin yeri tespit edilmekte ve vurulmaktadır.

1.5.2.3. Görüntü İstihbaratı (IMINT)

Görüntü İstihbaratı, 20. yy'ın başlarında, fotoğraf ve havacılığın gelişmesiyle ortaya çıkmıştır. 1970'lerin sonlarına kadar PHOTINT olarak adlandırılmaktayken, ilerleyen dönemlerde IMINT olarak tanımlanmıştır. Soğuk Savaş Dönemi'nde, istihbarat faaliyetleri için geliştirilmiş olan teknolojiler ve özellikle uzaya gönderilen uydular sayesinde IMINT'in kullanım alanı artmıştır (Duthel, 2014, s.277).

Önceleri balon ve zeplinlere takılan fotoğraf makineleriyle çekilen fotoğraflarla başlayan görüntü istihbaratı, bugün dijital fotoğraf makineleri, CCTV kameralar, webcam'ler, uydular ve göğün gözü olarak da adlandırılan insansız hava araçları vb. aracılığıyla yapılmaktadır. Görüntü istihbaratı bugün, fotoğraf istihbaratı (PHOTINT), video istihbaratı (VIDINT) ve uydu istihbaratı (SATINT) gibi alt dallara da ayrılmaktadır. Demir'e göre her istihbarat teşkilatı fotoğraf ve görüntü elde almak ve analiz etmek konularında uzmanlaşmış personele ihtiyacı bulunmaktadır (Demir, 2015, s.241).

1.5.3. Açık Kaynak İstihbaratı (OSINT)

Açık kaynak istihbaratı, gizlilik gerektirmeyen, herkese açık bilgilerin, istihbarat çarkından geçirilmesiyle elde edilen istihbarattır. Tasnif edilmemiş bu bilgilerin, planlı ve sistematik bir şekilde uygulanması halinde, gizli yöntemlere duyulan ihtiyaç azalabilmektedir ve sadece açık kaynaklardan toplanması mümkün olmayan bilgilerin, gizli faaliyetlerle toplanması ihtiyacı duyulmaktadır.

Açık kaynak istihbaratı, geleneksel medya dışında özellikle 1994 yılından itibaren gelişmekte ve büyümekte olan internet üzerinden de yapılabilmektedir. Özellikle hızlı karar alması gereken kişiler için internet üzerinden AKİ yapmak oldukça verimlidir. İnternet, ücretsiz ve ücretli birçok içeriğin bulunduğu bir kaynak olarak da değerlendirilmektedir (NATO, 2011, s.6).

Bugün, gizli operasyonlarla elde edilen fotoğraflar, Google Earth gibi uygulamalar aracılığıyla teyit edilebilmektedir. İnternet ve sibernetik içinde yer alan uygulamaların, etkin bir şekilde kullanılmasıyla, birçok önemli bilgiye ulaşmak

mümkündür. Terör örgütü, IŞİD üyelerinin sosyal medya hesapları üzerinden paylaştıkları eğitim ve tatbikatlara ait fotoğraflar, dikkatli internet kullanıcıları tarafından ayrıntılı bir şekilde incelenmiş, görsellerde bulunan yapı, akarsu vb. coğrafi şekillerin Google Earth üzerinden eşleştirilmesiyle, eğitim kamplarının yeri tespit edilmiştir[13].

1.6. İstihbarata Karşı Koyma (İKK)

Devletler, gerek iç güvenliğin sağlanması gerekse de stratejilerin geliştirilebilmesi için istihbarat oluşturmak istemektedir. Diğer devletlere karşı istihbarat faaliyetleri yürütülürken, aynı zamanda kendisine yönelik gerçekleştirilen benzer çalışmaların da önüne geçmek istemektedir.

İstihbarat oluşturulmasını önlemek için gerçekleştirilen faaliyetlere, İKK yani istihbarata karşı koyma denilmektedir (Özdağ, 2013, s.143). John Ehrman ise İKK'yı "yabancı devletlere ait istibarat teşkilatlarının örgütsel yapıları ve faaliyetleriyle ilgili yapılan çalışmalardır" şeklinde tanımlamaktadır (Ehrman, 2009, s.6). Devlete ait hassas bilgilerin hasımları tarafından ele geçirilmesi, devletin tüm stratejileriyle birlikte güvenliğini de tehlikeye sokacağından, istihbarata karşı koyma faaliyetleri büyük önem arz etmektedir.

Bu kavram, karşı istihbarat ya da karşı casusluk gibi tanımlarla karıştırılmaktadır. Ancak temel olarak, İKK için "her türlü istihbari faaliyetin önüne geçmek için gerçekleştirilen faaliyetler bütünüdür" demek mümkündür. İKK'nın etkin bir şekilde sürdürülebilmesi için istihbarat sürecinin de etkin geçirilmesi gerekmektedir. Bu anlamda, İKK'nın istihbarat toplama ve değerleme süreçlerinden daha zor olduğu ifade edilebilmektedir. Zira hasmın başvuracağı yol ve yöntemler hakkında bilgi ve beceri sahibi olmak, daha geniş bir uzmanlı alanı ihtiyacı doğurmaktadır. Dahası, gelebilecek her türlü tehdit ve tehlikeyi algılayabilmek için İKK uzmanının bir

[13] https://www.bellingcat.com/resources/case-studies/2014/08/22/gun-safety-self-defense-and-road-marches-finding-an-isis-training-camp, Erişim tarihi: 13 Aralık 2017.

istihbarat elemanı ya da analizcisinden daha üst düzey kültür ve bilgiye sahip olması beklenmektedir.

Bir İKK operasyonunda kullanılmaya matuf kesin bir yöntemsellik bulunmamaktadır. İKK faaliyetleri, aktif ve pasif olmak üzere ikiye ayrılmaktadır. Pasif İKK, neyin kimler tarafından eline geçmesinin engelleneceğinin tespit edilmesiyle başlar ve bilginin korunmasına yönelik alınan kişisel ve fiziksel güvenlik önlemlerini kapsamaktadır. Daha geniş bir ifadeyle pasif yöntemler, sahip olunan varlık, bilgi ve belgelerin hasım istihbarat teşkilatlarının eline geçmemesi için alınan tedbirleri ifade etmektedir. Bu anlamda öncelikle bilgi güvenliği kapsamında bilgilerin sınıflandırılması yapılmaktadır (Kartal, 2015, s.316-317). Bu sınıflandırma günümüzde, siber uzay üzerinden de dijital verinin korunmasına yönelik gerçekleştirilmektedir. Bu anlamda bilgi güvenliğiyle ilgili uluslararası standartların uygulanması önem arz etmektedir.

Aktif İKK ise, yabancı bir gizli servis tarafından, istihbarat oluşturmaya yönelik faaliyetleri önlemeye matuf gerçekleştirilen aktif eylemleri kapsamaktadır (Özdağ, 2013, s.145-146). Aktif İKK'yı daha da açmak gerekirse, tehdit olabilecek hedeflerin muhtemel eylemlerini ya da bu hedeflerden kaynaklanan zararları önlemeye yönelik, kullanılan malzemeler, yöntemleri, araç ve kişileri tespit etmek ve bunların kullanılmasını önlemek ya da ele geçirmek için alınan önlemlerdir şeklinde ifade edilebilmektedir.

İstihbarata Karşı Koyma, istihbarat faaliyetlerinin tersi gibi bir anlam şeklinde çağrışım yapmasına karşın, istihbaratın bir gerekliliği olarak nitelendirilmektedir. İstihbaratın olduğu her yerde İKK faaliyetleri de bulunmaktadır. Etkin bir İKK gerçekleşmemesi halinde, istihbarat teşkilatları tarafından gerçekleştirilen tüm faaliyetler anlamını kaybedebileceği gibi, önemli bilgi ve belgelerin hasmın eline geçmesi de söz konusu olabilmektedir. İKK'nın sadece istihbarat üretimi ile değil, algı yönetimine ilişkin unsurlarla birlikte düşünülmesi gerekmektedir.

İKİNCİ BÖLÜM

2. KAMU DÜZENİ VE GÜVENLİĞİNDEN SORUMLU KURUM VE KURULUŞLAR HAKKINDA GENEL BİLGİLER

2.1. Devlet Tanımı, Kavramı, Ögeleri ve Temel Görevleri

Tarih boyunca birçok topluluk, çeşitli dönemlerde farklı devletler kurmuştur. Bu devletlerden bazıları büyümüş ve dünyayı fethetme girişimlerinde bulunmuşken, bazılarıysa bir süre sonra yıkılmaya mahkum olmuştur. Bu devletlerin kurulma ve siyasi aşamaları farklılık teşkil ettiği için, tarihin ilk dönemlerinde farklı devlet tanımları yapılmış olup, birçok akademisyen ve yazar, devleti farklı alanlarda incelemiştir.

Devletin tanımı ve ne olduğuna ilişkin sorular, yüzyılardır düşünürlerin ele aldığı önemli konulardan biridir. Antik Yunan döneminden günümüze kadarki süreç içinde devletin tanımı ve devlet kavramı üzerinde yoğunlaşılmıştır. Devlet; gözle görülemeyen, elle tutulamayan soyut bir kavramdır ve vatandaşlarına karşı en büyük yaptırım gücüne sahip tüzel kişiliktir (Öztekin, 2014, s.48).

Devlet egemendir, toplumda yer alan tüm birlik ve gruplar üzerinde mutlak ve sınırlandırılmamış bir iktidara sahiptir. Sivil toplumda yer alan özel kurumlara karşılık, devlet kurumlarıysa kamusal olarak tanımlanmaktadır. Devletin kararları, toplumun üyeleri bakımından bağlayıcı kabul edilmektedir. Çünkü devletin aldığı bu kararlar, kamunun yararına olmaktadır. Devlet otoritesi zorla desteklenmektedir ve itaati sağlamak, kanunları ihlal edenleri cezalandırmak gücüne sahiptir.

Devletin, ülkesi üzerindeki yetkileri, coğrafi olarak tanımlanmıştır. Bu yetki, ister vatandaşı olsun ister olmasın sınırları içinde yaşayan herkesi kapsamaktadır. Bundan hareketle devlet, otonom bir varlık olarak görülmektedir (Heywood, 2015, s.89). Devletin asli görevinin olumsuz olduğu söylenmektedir. Devletin olumsuz görevi, toplum içinde zararlı olan tüm ögelere engel olmak, iç güveni ve dış güvenliği sağlamaktır. Devletin modern göreviyse olumludur.

Buna göre devletin bir diğer görevi toplumun ortak ihtiyaç duyduğu mal ve hizmeti üretmektir (Eryılmaz, 2000, s.49). Devlet, toplumun birliği ve düzenini sağlamak için üstün bir yaptırım uygulama gücüne sahiptir. Bu güç, tek taraflı olduğu gibi gerekli hallerde zor kullanma yetkisini de içinde barındırmaktadır. Bu amaçla devlet; polis, jandarma ve silahlı kuvvetler gibi kurum ve güçlere sahiptir (Aydın, 2013, s.44).

Aydın'ın bu cümlesinden hareketle, devletin kamu düzeni ve güvenliğini sağlamak için her türlü üstün güce sahip olduğunu söylemek mümkündür. Ancak devletin bu üstünlüğe sahip olması, kişisel hak ve özgürlüklükleri kısıtlamamalıdır. Bunun için de istihbarat teşkilatları ile kolluk kuvvetlerinin gerekli yasal düzenlemelere sahip olması gerekmektedir.

Devleti oluşturan temel ögeler insan, ülke ve siyasal örgütlenmedir. Devletin temel ögeleri arasında en önemlisi kuşkusuz insan topluluğudur. İnsan topluluğu olmadan devletin olması mümkün değildir. Ayrıca devletin olabilmesi için, bu insan topluluğunun devlete vatandaşlık bağları ile bağlı olması gerekmektedir. Devletin ikinci temel ögesiyse, birinci öge olan insanların yaşadığı, sınırlı belli bir toprak parçası yani ülkedir.

Ülke sadece kara parçasını değil, sınırları içindeki deniz, göl, nehir ve hava sahasını da kapsamaktadır. Devletin üçüncü ögesiyse hükümet ya da siyasi örgütlenmedir. Hükümet, devlet adına siyasal iktidar ve otoriteyi kullanmaktadır ve devlete nazaran daha somut bir kavramdır (Öztekin, 2014, s.52). Öztekin'e göre bu ögelerden birinin dahi eksik olması halinde, devletin varlığından söz edilememektedir.

2.2. Kamu Yönetimi

Kamu, halk hizmeti gören devlet organlarının tamamı anlamına gelmektedir. Kamu ayrıca bir ülkede yaşayanların tümü, halk anlamını da taşımaktadır. Kamu yönetimi halkın yani toplumun yaşadığı sorunları işleyen bir idari mekanizma olarak değerlendirilmektedir. Eryılmaz'a göre toplumlar gerek hacim olarak gerekse de ilişkilerinin yoğunluğu bakımından gelişim gösterdikçe devletler de yapıları ve işlevleri bakımından büyümüktedir.

Bu durum beraberinde kurumların uzmanlaşmalarını ve farklılaşmalarını doğurmaktadır. Bundan hareketle, yönetim faaliyetlerini yürütmekte olan kamu kurumlarının da yapısı ve işleyişi karmaşıklaşmakta ve daha teknik bir hale gelmektedir. Bu da kamu yönetimi kavramına ait tanımların çeşitliliki göstermesine sebep olmaktadır. Kamu yönetimi, siyaset biliminden hukuka, iktisattan işletmeye kadar geniş bir yelpazede yer alan bilim dallarını içermektedir. Tüm bu farklı bilimler bir araya getirilerek, doğru ve etkin bir kamu yönetimi sağlanmaktadır.

Kamu yönetimi, devlet ve toplum düzeninin kesintisiz işlemesi, kamunun ortak ihtiyaçlarını karşılamak için üretilen mal ve hizmetlerin halka sunulmasını sağlayan sistemdir (Eryılmaz, 2000, s. 9). Kamu yönetimini anlayabilmek için, amacının ne olduğunu bilmekte fayda bulunmaktadır. Kamu yönetiminin amacı, ülkenin gelişmesini yönlendirmek, planlamak ve temel politikalarını tespit ederek yönetmektir. Kamu yönetimi ayrıca, kamu düzeni ve güvenliğinden de sorumludur.

Öztekin; devlet, hükümet-kamu yönetimi ilişkisine dikkat çekmiş ve birbirlerini nasıl etkilediklerini anlatabilmek ve somutlaştırmak adına, devleti insan bedenine, devletin güçleri olan yasama ve yargı güçlerini de kollarına benzetmiştir. Kollar dışındaki ana yapıyı yürütme gücüne, kafa kısmını hükümete, kalan kısmını da kamu yönetiminin idari yapılanmasına benzetmiştir.

Bu benzetmeden hareketle, devlet örgütlenmesinin sürekli ve verimli olabilmesi için insan vücuduna benzetilen bu yapının da sağlıklı olması gerekmektedir. Kamu yönetimi denilen, devletin yürütmeyle ilgili örgütsel yapısı, hükümetle uyumlu bir

işleyiş içinde olmalıdır. Kamu yönetimi içinde yer alan kurum ve kuruluşların da toplumun iyiliği, güvenliği, sağlığı ve mutluluğu için birbirini frenlemeli, dengelemeli ve şekilde kamu yararı için, uyumlu bir şekilde çalışmalıdır (Öztekin, 2012, s.254).

Kamunun uyumlu çalışabilmesi, dahası topluma iyi hizmet sunabilmesi için kamu görevlilerinin de ihtiyaçlara uygun, uzman kişilerden oluşması gerekmektedir. Liyakat sisteminin olmadığı örgüt yapılanmaları, bırakın iyi ve verimli hizmet vermeyi, örgütün yapısının bozulmasına ve hatta bir süre sonra çökmesine dahi sebep olabilmektedir. Bu anlamda sadece sistem değil, sistem içinde yer alan personel, yani kamu görevlileri de büyük önem arz etmektedir.

2.3. Kamu Görevlisi

Kamu görevlileri, kamu yönetiminin insan unsurunu oluşturmaktadır. 1982 Anayasası kamuda görevli kimseler için "kamu hizmeti görevlileri" ifadesini kullanmaktadır (m.128). Bir kişinin, kamu görevlisi olabilmesi için, bir kamu kurumuna bağlı çalışması gerekmektedir. Örneğin bir doktor, kamu hizmeti yapmasına rağmen, çalışmakta olduğu kurum, bir kamu kurumu değilse, hizmeti veren doktor, kamu görevlisi olarak nitelendirilmemektedir. Kamu görevlileri, Devlet Memurları Kanunu'nun kendilerine tanıdığı haklara göre, farklı hukuki statülere sahiptir. Bir kamu kurumunda çalışan, işçiden Cumhurbaşkanına kadar herkes, kamu görevlisi olarak nitelendirilmektedir (Aygün, 2008, s.260). DMK'ya göre kamu görevlileri, dört şekilde istihtam edilmektedir:

- Memur
- Sözleşmeli Personel
- Geçici Personel
- İşçiler

657 sayılı DMK'ya göre "Mevcut kuruluş biçimine bakılmaksızın, Devlet ve diğer kamu tüzel kişiliklerince genel idare esaslarına göre yürütülen asli ve sürekli kamu hizmetlerini ifa ile görevlendirilenler, bu Kanunun uygulanmasında memur sayılır". Memurlar, nitelik ve mesleklerine göre on iki farklı sınıfa ayrılmaktadır:

- Genel İdare Hizmetleri Sınıfı
- Teknik Hizmetler Sınıfı
- Sağlık Hizmetleri ve Yardımcı Sağlık Hizmetleri Sınıfı
- Eğitim ve Öğretim Hizmetleri Sınıfı
- Avukatlık Hizmetleri Sınıfı
- Din Hizmetleri Sınıfı
- Emniyet Hizmetleri Sınıfı
- Yardımcı Hizmetler Sınıfı
- Mülki İdare Amirliği Hizmetleri Sınıfı
- Milli İstihbarat Hizmetleri Sınıfı
- Jandarma Hizmetleri Sınıfı
- Sahil Güvenlik Hizmetleri Sınıfı

Tablo 3: Kamu Görevlilerinin Sınıflara Göre Dağılımı (2017)

Sınıflar	**Dolu Kadro**
Genel İdare Hizmetleri Sınıfı	537.730
Mülki İdare Amirliği Sınıfı	2.107
Sağlık Hizmetleri ve Yardımcı Sağlık Hizmetleri Sınıfı	406.539
Teknik Hizmetler Sınıfı	144.027
Eğitim Öğretim Hizmetleri Sınıfı	878.952
Avukatlık Hizmetleri Sınıfı	4.827
Emniyet Hizmetleri Sınıfı	261.625
Din Hizmetleri Sınıfı	102.725
Yardımcı Hizmetler Sınıfı	111.006
Jandarma Hizmetleri ve Sahil Güvenlik Hizmetleri Sınıfı	88.001
Toplam (*)	2.537.539

Kaynak: http://www.dpb.gov.tr, Erişim tarihi: 15 Aralık 2017.

(*) MİT Müsteşarlığı personeli bu sayılara dahil değildir.

Bunlardan başka, kamu kurumlarında planlama, programlama, araştırma, genel politika tespiti, yönetim ve denetim vb. işlerde görev yapanlar ya da yetkili olanlar da memur sayılmaktadır.

2.4. Kamu Kuruluşu ve Kamu Hizmeti

Doğrudan ya da dolaylı olarak kamu yararına yönelik, kamu hizmeti yapmak ya da yaptırmak amacı ile kurulmuş, kamu mallarına sahip, kamu görevlilerinin çalıştığı kuruluşlara, kamu kuruluşu denilmektedir (Öztekin, 2012, s.91). Bu kuruluşlar, devletin bir bütün olarak idaresinden ve işleyişinden sorumludur. Kamu kuruluşları, farklı hizmetler için örgütlenmiştir ve ortak amacı, kamuya hizmet vermeye devam etmektir.

Hizmet, mevzuatta yapılması ya da yapılmaması öngörülen konulardan, emir verme yetkisine sahip kişilerce yazılı ya da sözlü olarak emredilen ya da yasaklanan işlerdir. Bundan hareketle kamu hizmeti için, kamu kurumları tarafından veya bunların gözetimindeki özel girişimler tarafından sağlanan her türlü hizmet denilmektedir (Aydın, 2013, s.111). Kamu hizmetinin sunulmasında eşitlik ilkesi gözetilmektedir. Hizmet, kamu yararınadır ve yerel, ülkesel ya da bölgesel olabilmektedir. Kamu hizmetleri çoğunlukla maddi bir bedel olmaksızın sunulur ve süreklilik arz etmektedir.

2.5. Kamu Düzeni ve Güvenliği

Güvenlik, yüzyıllardır insanoğlunun ihtiyaç duyduğu en önemli kavramlardan biridir. Bu kavram, zaman içerisinde, yaşanmış olaylar neticesinde değişim göstermiştir. Önceleri bireylerin kendi güvenlikleri söz konusuyken, daha sonra bir arada yaşamayla birlikte toplum ögesi oluşmuş ve bununla birlikte kamu güvenliği, devlet güvenliği, iç güvenlik, ulusal güvenlik gibi farklı kavramlar ortaya çıkmıştır.

Sosyal hayatın en temel gereksinimlerinden biri olan kamu güvenliği, ülke sınırları içinde yaşayan halkın, can ve mal güvenliğinin devlet tarafından korunması faaliyetleridir. Devletin birincil ödevlerinin başında, kamu güvenliğinin sağlanması gelmektedir ve bununla ilgili olarak kolluk örgütü kurması, gerekli araç ve olanakları sağlaması, yterli önlemleri zamanında alması gerekmektedir (Yayla, 2010, s.39).

Tarihin bilinen ilk devletlerinden bugüne, toplum güvenliği için devletler çeşitli kurumlar kurmuş, bu kurumlar bünyesinde kamu görevlileri istihdam etmiştir. Kamu güvenliğinin sağlanması için polis ve jandarma gibi iç güvenlikle ilgili kurumlara, dış güvenliğin sağlanması içinse silahlı kuvvetlere özel yetkiler verilmiştir. Maslow'un ihtiyaçlar hiyerarşisine göre güvenlik, insanoğlunun fizyolojik ihtiyaçlarından sonraki en önemli ihtiyacıdır.

Çizelge 2: Maslow'un İhtiyaçlar Hiyerarşisi

Kaynak: https://endustrimuhendisiyim.com/maslow-ihtiyaclar-hiyerarsisi

Ayhan, toplumsal yaşamın varlığının, iç düzenin sağlanmasına ve bu amaca hizmet eden kolluk faaliyetlerine bağlamaktadır ve bu faaliyetlerin, kamu yararı gerekçesiyle bireysel hak ve özgürlükleri kısıtlamasını bir zorunluluk olarak görmektedir (Ayhan, 2008, s.124). Bundan hareketle, kamu güvenliğinin söz konusu olduğu yerde, bireysel hak ve özgürlüklerin ikincil plana atıldığını söylemek mümkündür. Kolluk, bireysel hak ve özgürlükleri kısıtlama yoluna giderken, bunu yasalar çerçevesi içinde yapmalıdır.

Demokratik hukuk devletleri örgütlenme ve diğer hizmetleriyle ilgili çalışmalar yürütürken, öncelikli olarak genel güvenliğin sağlanması ve kamu düzeninin

sürdürülebilir duruma getirilmesi konularına eğilmektedir. Kösereli, istihbaratın da masum bireylerin temel hak ve özgürlüklerinin güvence altında olduğu bir düzen içinde yaşamalarına imkan sağlamasını amaçladığını vurgulamaktadır (Kösereli, 2015, s.100).

Kamu güvenliğinin sağlanması için kolluk ve istihbaratın bir arada hareket etmesi, bunu yaparken de hukuki kuralların belirlemiş olduğu sınırlar içinde kalması gerekmektedir. Kamu düzeni, kamu işlerinin en etkin şekilde yapılmasını, devletin güveni ve düzeniyle, bireylerin birbirleriyle olan ilişkilerinde dirliği sağlamak için uygulanan kurallar bütünüdür.

Emniyet ve asayişle ilgili kanunların bir kısmı, kamu düzeninin sağlanmasına ilişkindir. Türkiye Cumhuriyeti Anayasası'nın ikinci kısmında yer alan, Temel Hak ve Ödevler başlığı altındaki maddeler de kamu düzenine sürdürülmesine ilişkindir. Bundan hareketle, kamu güvenliği ve kamu düzeni için devlet tarafından sunulan hizmetler, anayasaya uygun şekilde yapılmaktadır.

2.6. Kamu Güvenliği Açısından İstihbarat

Kamu güvenliğinin sağlanması, vatandaşların huzurlu bir şekilde yaşayabilmesi ve daha sonra da kamu kurumları ile özel işletmelere ait binaların muhtemel sabotaj ve vb. tehlikelerden korunması için iç istihbarat faaliyetlerinin yapılması gerekmektedir. Tehlikenin önceden tespiti ve gerekli koruyucu güvenlik önlemlerinin alınması açısından, etkin bir istihbarat büyük bir önem taşımaktadır. Günümüzde, bu özellikle gelişen teknolojiyle birlikte teknik istihbarat konusunda olumlu gelişmeler yaşanmaktadır.

Kolluk kuvvetlerinin, iç güvenliğe yönelik hizmetlerini yerine getirebilmesi için, kendilerine önceden bir takım bilgilerin sunulması faydalı olmaktadır. Bu anlamda istihbarat teşkilatlarının, gerek kendi aralarında gerekse de kolluk kuvvetleriyle koordinasyon içinde çalışması gerekmektedir. Türkiye'de bu konuya ilişkin çalışmalar bir süredir devam etmekle birlikte, mevcut yapıya göre istihbarat faaliyetlerine ilişkin koordinasyon, Milli İstihbarat Teşkilatı tarafından yürütülmektedir.

Kamu güvenliğinin sağlanmasına yönelik eylem ve işlemler, hukuka bağlı olmalıdır. Toplumun dinamik yapısı göz önünde bulundurulmalı ve buna göre gerekli hukuki düzenlemeler zamanında yerine getirilmelidir. Hukukun üstünlüğü, kolluk kuvvetlerinin halkın yanında olduğu ve de en önemlisi, güvenlik için yürütmekte olduğu faaliyetlerin meşruluğuna vatandaşın inandırılması gerekmektedir.

Ancak bu sayede vatandaş, devletin ilgili birimleriyle uyumlu olabilecek ve hatta gerektiği hallerde yardımcı olacaktır. Halk, genellikle istihbari bilgi paylaşımını, ispiyonlamak şeklinde algılamaktadır. Oysa ki bu algı tamamen yanlıştır ve istihbarat, kamu güvenliği açısından büyük önem taşımaktadır. Günümüzde, istihbarat faaliyetleri yürütmekte olan kurumlar ile kolluk kuvvetlerine ait web sitelerinde vatandaşın ihbarda bulunabilmesini sağlayan sayfalar bulunmaktadır.

Bu sayfalar, şifrelenmekte olduğundan, ihbarda bulunanla ilgili merci arasındaki bağlantı güvenli olmaktadır. Bu teknik imkanlara rağmen vatandaş kimi zaman çekinmekte hatta korkmaktadır. Milli İstihbarat Teşkilatı'nın resmi sitesinde, bu algıyı ortadan kaldırmak için, ilgili bölüm "Nasıl Yardım Edebilirsin" şeklinde isimlendirilmiştir[14]. Türkiye'de istihbaratın toplum geneline yayılması ve bu bilim dalına karşı önyargıyı kırmak amacıyla son yıllarda, yerli televizyon dizileri yayınlanmaya başlamıştır. Vatandaşın, istihbarat teşkilatlarını çeşitli tehdit ve potansiyel tehlikelere karşı uyarması işleminin bir ispiyonlama değil, haber verme olduğu algısının oluşturulmasıyla birlikte, çok daha verimli sonuçların oluşması beklenmektedir.

Kamu güvenliğini en çok tehdit eden, terörle mücadele için de etkin bir istihbarat faaliyeti yürütmek gerekmektedir. Bu anlamda 5952 sayılı kanun kapsamında, İçişleri Bakanlığı'na bağlı, terörle mücadeleye ilişkin politika ve stratejileri geliştirmek üzere Kamu Düzeni ve Güvenliği Müsteşarlığı kurulmuştur. Müsteşarlık ayrıca terörle mücadele konusunda, ilgili kurum ve kuruluşlar arasındaki koordinasyonu sağlamakla görevlendirilmiştir.

[14] https://www.mit.gov.tr/katkiniz.html, Erişim tarihi: 17 Aralık 2017.

İçişleri Bakanlığı'na bağlı Emniyet Genel Müdürlüğü bünyesindeki Siber Suçlarla Mücadele Daire Başkanlığı ve Başkanlığa bağlı Siber Suçlarla Mücadele Şube Müdürlükleri de Türkiye Cumhuriyeti vatandaşlarının, siber uzaydaki güvenliklerine yönelik faaliyetler yürütmektedir.

Bu anlamda kolluk kuvvetlerinin, siber güvenlik ve siber suçlara yönelik faaliyetlerinin de İçişleri Bakanlığı'na bağlı olarak yürütüldüğü söylenebilir. Diğer taraftan, siber terörizm gibi günümüzde çok büyük önem arz eden, kamu düzeni ve güvenliğini tehdit edici konularda da yine ilgili kolluk kuvvetleri bünyesinde görevlendirilmiş birimler, proaktif faaliyetlerini sürdürmektedir.

Ancak, sözü edilen bu faaliyetlerin daha etkin olabilmesi için, siber güvenlik ve siber saldırı konularındaki metodolojilerin doğru bir şekilde kullanılması gerekmektedir. Ayrıca dinleme, görüntü elde etme ve bilgi sızdırma gibi istihbari faaliyetlerin gerçekleşebilmesi için gerekli yazılımların geliştirilmesine yönelik yeterli bilgi ve beceriye de sahip olunması gerekmektedir.

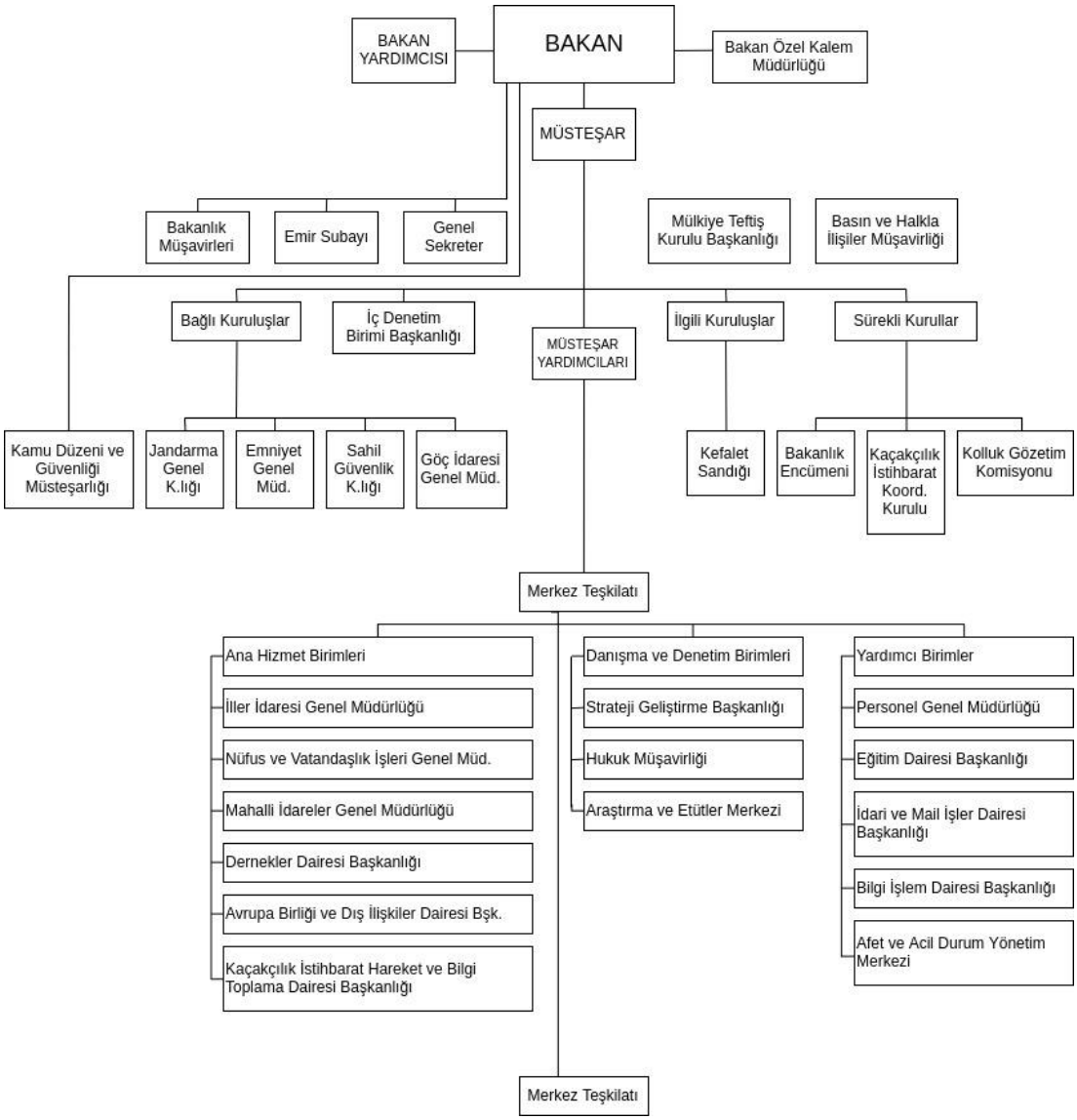
2.7. İçişleri Bakanlığı'nın Örgütsel Yapısı

İçişleri Bakanlığı'nın teşkilat yapısı da yine 3152 sayılı kanunda belirtilmiş olup, her birimin görevleri de tanımlanmıştır. İçişleri Bakanlığı, kendisine bağlı iç güvenlik kuruluşlarını idare etmek suretiyle, ülkenin ve milletin bölünmez bütünlüğünü, ülkenin iç güvenliğini ve asayişini, kamu düzeni ve genel ahlakı ve ayrıca Anayasada yazılı hak ve hürriyetleri korumakla yükümlüdür.

İçişleri Bakanlığı Teşkilatı; merkez, taşra ve yurtdışı teşkilatı ile bağlı kuruluşlardan meydana gelmektedir. Bakanlık ayrıca, 13/12/1983 tarihli ve 189 sayılı Kamu Kurum ve Kuruluşlarının Yurtdışı Teşkilatı Hakkında Kanun Hükmünde Kararname esaslarına uygun olarak, yurtdışı teşkilatı kurmaya da yetkilidir[15]. İçişleri Bakanlığı Merkez Örgütü yapısı, Çizelge 3'teki gibidir.

[15] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.3152.pdf

Çizelge 3: İçişleri Bakanlığı Merkez Örgütü



Kaynak: https://www.icisleri.gov.tr/teskilat-semasi7, Erişim tarihi: 18 Aralık 2017.

2.7.1. İçişleri Bakanı, Müsteşar ve Müsteşar Yardımcıları

3152 sayılı kanunun 5. maddesinde ifade edildiği üzere İçişleri Bakanı, Bakanlık kuruluşunun en üst amiridir. Diğer tüm bakanlar gibi İçişleri Bakanı da Başbakana karşı sorumludur. Bakanlık hizmetlerinin mevzuata, milli güvenlik siyasetine, hükümetin genel politakasına, kalkınma planlarına ve yıllık programlara uygun bir

şekilde yürütmekle görevlidir. Ayrıca Bakanlığın çalışma alanına giren konularla ilgili olarak, diğer bakanlıklarla işbirliği ve koordinasyonu da sağlamakla görevlidir.

Müsteşar, 3152 sayılı Kanunun 6. maddesine göre, Bakan adına ve Bakanın direktif ve emirleri yönünde Bakanlık hizmetlerini yürütmektedir. Müsteşar, Bakanın emrindedir ve onun yardımcısıdır. Bakanlığın amaç ve politikalarını, kalkınma planları ve yıllık programlara, mevzuat hükümlerine uygun bir şekilde düzenler ve yürütür. Bakanlığın kuruluşlarına, gerekli talimatları verir ve bu talimatların uygulanmasını takip ve temin eder. Müsteşar, tüm bu hizmetlerin yürütülmesiyle ilgili olarak, Bakana karşı sorumludur.

3152 sayılı Kanunun 7. maddesine göre, İçişleri Bakanlığı bünyesinde, anahizmet birimleriyle danışma ve denetim birimlerinin yönetim ve koordinasyonunda, Müsteşara yardımcı olmak üzere, Müsteşar Yardımcıları görevlendirilebilir. Daha önce dört olan Müsteşar Yardımcısı sayısı, 15/8/2016 tarihli ve 674 sayılı KHK'nin 34. maddesiyle beş olarak değiştirilmiş olup, daha sonra 10/11/2016 tarihli ve 6758 sayılı Kanun'un 30. maddesiyle bu hüküm aynen kabul edilerek kanunlaşmıştır. Buna göre Bakanlık bünyesinde beş adet Müsteşar Yardımcısı görevlendirilebilmektedir.

2.7.2. Merkez Valileri

Merkez Valiliği, 5442 sayılı İl İdaresi Kanunu'nda yapılan düzenlemeyle girmiş olup, Valilerin çeşitli sebeplerle merkeze alınarak, merkezde görev yapmalarına imkan tanımaktadır. İlgili yasanın 6. maddesi, Valilerin, gerek görüldüğü hallerde, merkeze alınarak Bakan'ın uygun gördüğü görevleri yapacakları belirtilmiştir.

3152 sayılı Kanun'a göre Merkezde görevlendirilen Valiler, Bakan tarafından İçişleri Bakanlığı Müsteşarlığı, Müsteşar Yardımcılığı, Genel Müdürlük, Kurul Başkanlığı, Bakanlık 1'inci Hukuk Müşavirliğinde; ya da inceleme, araştırma, soruşturma ve eğitim işlerinde; Başbakanlığın isteği üzerine, Başbakanlık ve diğer bakanlıkların, Müsteşar, Müsteşar Yardımcısı, Genel Müdürlük ve bu görevlere eşdeğer diğer üst kademe yöneticiliklerinde; unvan ve özlük hakları saklı kalmak kaydı ile görevlendirilebilmektedir.

2.8. İçişleri Bakanlığının Taşra (İl ve İlçe) Yapılanması

Bu başlığın alt başlıklarında; İçişleri Bakanlığı'nın 5442 Sayılı Kanununa göre oluşturulan il ve ilçe uzantıları (valilikler ve kaymakamlıklar) özetle açıklanacaktır.

2.8.1. Vali ve İl Yönetim Kurulu

İl Valileri, 5442 sayılı İl İdaresi Kanunu 6. maddesine göre, İçişleri Bakanlığı'nın önerisi, Bakanlar Kurulu'nun kararı ve Cumhurbaşkanı'nın tasdiki ile görevlendirilmektedir. Vali, görevli olduğu ilin sınırları içinde devleti, hükümeti, bakanlıkları ve ilde birimi bulunan kamu kuruluşunu temsil etmektedir. Valiler, başta güvenlik olmak üzere, tüm kamu hizmetlerinden sorumludur. Bu sebeple de İl İdaresi Kanunu'na göre oldukça geniş yetkilere sahiptir (Öztekin, 2012, s.338).

Valiler ayrıca, il sınırları içindeki güvenlikten sorumlu mülki idare amiri olduklarından, kamu düzenini sağlamak için kendisine doğrudan bağlı olan il emniyet müdürlüğü, il jandarma alay komutanlığı ve varsa konuşlanmış sahil güvenlik bölge ya da grup komutanlığı vasıtasıyla güvenliği sağlayamaması durumunda, kendi il sınırları içinde ya da en yakın ildeki silahlı kuvvetler örgütlerinden yardım talep edebilmektedir. Valinin bu talebi, hemen yerine getirilmektedir. Acil durumlarda bu talep, sonradan yazılı şekle dönüştürülmek kaydıyla, sözlü olarak yapılabilmektedir.

Her ilde valiye danışmanlık yapan ve İl İdaresi Kanunu'na göre çeşitli yönetim görevlerini yürüten "İl Yönetim Kurulu" bulunmaktadır. İlgili kanuna göre oluşturulan İl Yönetim Kurulu, Vali başkanlığında Hukuk İşleri Müdürü, Defterdar, İl Milli Eğitim Müdürü, Çevre ve Şehircilik Müdürü, İl Sağlık Müdürü ve Gıda, Tarım ve Hayvancılık İl Müdürü'nden meydana gelmektedir. Gerekli hallerde İl Yönetim Kurulu, Vali Yardımcısı'nın başkanlığında da toplanabilmektedir.

2.8.2. Kaymakam ve İlçe Yönetim Kurulu

Kaymakam, Valinin astı olarak Türkiye Cumhuriyeti Hükümetini temsil etmektedir. Hükümet, devletin ve toplumun yönetiminden sorumludur. Dolayısıyla ilçenin merkez ve merkez dışı sınırlarından kaymakam sorumludur. Kaymakam, ilçenin en büyük mülki idare amiridir. Kaymakamlar, Valilerden farklı olarak, kariyer

mesleğinden gelmektedirler. Bu sebeple Kaymakamların seçilmeleri, yetiştirimeleri, atanmaları ve yer değiştirmeleri belirli kurallara tabidir (Öztekin, 2012, s.346). Kaymakamlar, Valilerden farklı olarak, devleti temsil etmemektedir. Bu anlamda, büyük ölçüde valilere bağımlı görünmektedirler.

Tıpkı illerde olduğu gibi, ilçelerde de kaymakama danışmanlık yapan, "İlçe Yönetim Kurulları" bulunmaktadır. İlçe Yönetim Kurulları, Kaymakam başkanlığında, Yazı İşleri Müdürü, Mal Müdürü, Sağlık Grup Başkanı, İlçe Milli Eğitim Müdürü, İlçe Gıda, Tarım ve Hayvancılık Müdürü'nden oluşmaktadır. Kaymakam da görevli olduğu ilçenin güvenliğinden sorumlu mülki idare amiridir. İlçenin güvenliğini sağlamak için İlçe Jandarma Komutanlığı, Emniyet Müdürlüğü ve Sahil Güvenlik Komutanlığı, kaymakama yardımcı olmaktadır.

2.9. İçişleri Bakanlığı'nın Kamu Güvenliğinden Sorumlu Birimleri

Türkiye Cumhuriyeti'nin kamu düzeni ve güvenliğinin sağlanması, kolluk kuvvetlerinin görevidir. İçişleri Bakanlığı'na bağlı olarak Emniyet Genel Müdürlüğü, Jandarma Genel Komutanlığı ve Sahil Güvenlik Komutanlığı genel kolluk kuvveti hizmeti vermektedir. Gümrük Muhafaza, Orman Muhafaza ve belediyelere bağlı Zabıta da kendilerine verilen yetki ve görev çerçevesinde, sorumluluk alanlarındaki potansiyel tehlike ya da suç işlenmesini önleyici faaliyetlerde bulunmaktadır. Bu faaliyetlerinden ötürü adı geçen kurum ve birimler de kolluk kuvveti olarak tanımlanmaktadır.

İstihbaratın modernleşmesiyle birlikte, insana dayalı istihbarat ve teknik istihbarat birbirini desteklemiş, böylelikle daha hızlı ve etkin bir istihbarat oluşturulabilmiştir. Gerek insani ve teknik istihbaratın birlikte kullanılabilmesi gerekse de istihbarat örgütlerinin başarılı faaliyetler yürütebilmesi için koordinasyon ve bilgi paylaşımı modern istihbaratın gerekliliği haline gelmiştir. Günümüzde, bir ülkenin istihbarat teşkilatlarının kendi aralarındaki koordinasyonundan öte, özellikle terörle mücadele açısından ülkeler arası istihbarat paylaşımı ve koordinasyona yönelik çalışmalar, düzenlemeler yapılmaktadır. Türkiye'de istihbarat hizmetlerinden sorumlu, farklı yetki, sorumluluk ve görevlere sahip kurumlar bulunmaktadır. Bu kurumlar arasındaki

koordinasyonun sağlanması, 2937 sayılı kanun ile Milli İstihbarat Teşkilatı'na verilmiştir (m.5). Milli İstihbarat Teşkilatı'ndan başka istihbarat hizmetlerinden sorumlu kamu kurum ve kuruluşları şu şekildedir:

- Genelkurmay Başkanlığı
- Kara Kuvvetleri Komutanlığı
- Deniz Kuvvetleri Komutanlığı
- Hava Kuvvetleri Komutanlığı
- Jandarma Komutanlığı
- Sahil Güvenlik Komutanlığı
- Emniyet Genel Müdürlüğü
- Kamu Düzeni ve Güvenliği Müsteşarlığı

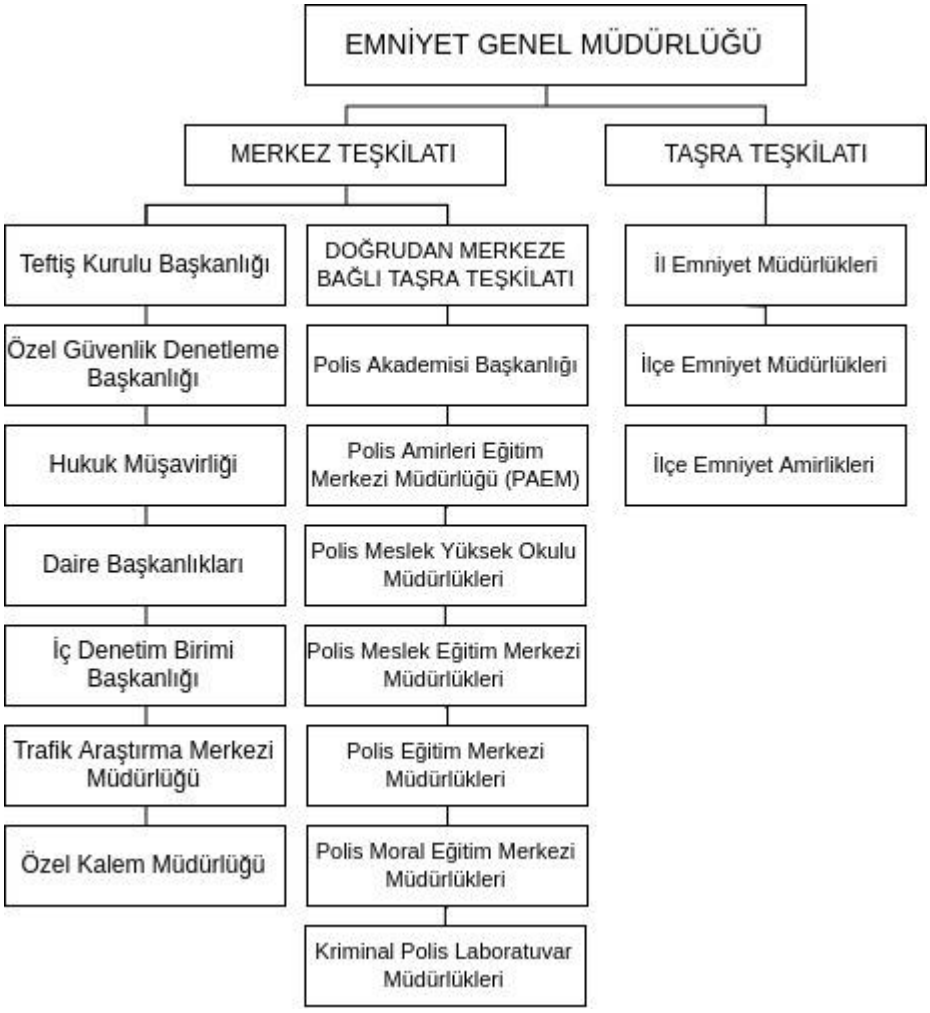
2.9.1. Emniyet Genel Müdürlüğü

Antik Yunan'da polis "kent, devlet" anlamlarına gelmektedir. Latince politia, "devlet düzeni" anlamında kullanılmaktadır. Zamanla kent ve devlet anlamında kullanılmaktan çıkıp, devlet düzeni şeklinde kullanılan polis kelimesi, Türkçe'ye ise Fransızca "kamu düzeni" ve "polis teşkilatı" anlamlarında kullanılan "police" kelimesinden geçmiştir. Güncel Türkçe Sözlük'te ise polis, "şehirde kamu düzeni, huzur ve güvenliği sağlayan kuruluş, kolluk, zabıta" anlamına gelmektedir.

Polis ayrıca, emniyet teşkilatında görevli kişi anlamında da kullanılmaktadır. 2559 sayılı Polis Vazife ve Salahiyet Kanunu'nda ifade edildiği üzere polis, toplumu, şahısları ve meskenleri korumakla görevlidir. Polis ayrıca halkın ırzı, canı ve malını da korumakla görevlendirilmiştir. Osmanlı Devleti'nde 10 Nisan 1845 tarihine kadar iç güvenlik, askeri teşkilatlar tarafından sağlanmaktayken, İstanbul'da polis teşkilatının kurulmasıyla birlikte iç güvenlikten sorumlu kurum, Polis Teşkilatı, bugünkü adıyla Emniyet Genel Müdürlüğü olmuştur. Modern toplumlarda, kamu düzeni ve güvenliğinin sağlanması için polisin ve polis teşkilatının olması zaruridir. Ancak bu teşkilat içinde görevli olan kimselerin yetki ve görevlerinin, kanunlarla belirlenmiş olması gerekmektedir. Polis Vazife ve Salahiyet Kanunu 2. maddesine göre polis, kamu düzeni ve kamu güvenliğinin sağlanmasından sorumludur.

3201 Sayılı Emniyet Teşkilatı Kanunu'nun 8. maddesine göre polis; İdari, siyasi ve adli olarak üçe ayrılmıştır. İdari polis, toplumsal ve genel güvenliği temin etmekle görevlidir. Siyasi polis, devletin genel güvenliğiyle ilgili faaliyetler yürütmektedir. Adli polis ise, asgari tam teşekküllü bir polis karakolu bulunan yerlerde, adli işlerle uğraşmak üzere Emniyet Genel Müdürlüğünce kadrodan ayrılan bir kısımdır. 3201 Sayılı Emniyet Teşkilatı Kanunu'nun 16. maddesine göre Emniyet Genel Müdürlüğü, merkez ve taşra teşkilatlarından oluşmaktadır. EGM teşkilat yapısı aşağıdaki gibidir:

Çizelge 4: Emniyet Genel Müdürlüğü Teşkilat Şeması



Kaynak: https://www.egm.gov.tr/sayfalar/organizasyon-yapisi.aspx, Erişim tarihi: 18 Aralık 2017.

Türkiye Cumhuriyeti'nin kurulmasıyla birlikte, modern bir istihbarat ve karşı istihbarat teşkilatlarına olan ihtiyaç da artmış, konuya ilişkin kurum ve kuruluşların oluşturulması çalışmaları başlatılmıştır. 4 Haziran 1937 tarihinde, ajanlarla ilgili iş ve işlemlerin yapılması, genel müdürün verdiği özel görevleri yapmakla görevlendirilmiş "Önemli İşler Müdürlüğü" kurulmuş ve bugünkü İstihbarat Daire Başkanlığı'nın temelleri atılmıştır. 1951 yılında doğrudan Emniyet Genel Müdürü'ne bağlı olarak, ideolojik akımlar, karşı casusluk ve her türlü kaçakçılıkla ilgili haber toplamak üzere "Özel Büro" kurulmuş ve çeşitli illerde bu büroya bağlı birimler çalışmalara başlamıştır.

Zaman içerisinde istihbarat elemanları eğitilmiş, ilgili birimlere personel alımı yapılmış ve buna bağlı olarak teşkilatın imkan ve kabiliyetleri geliştirilmiştir. 27 Mayıs 1960 tarihinde taşra birimlerinde de İstihbarat Kısmı ya da İstihbarat Büroları kurulmuştur. 1963 yılında, Önemli İşler Müdürlüğü'nün gelişmiş bir istihbarat örgütü olma niteliği kazanmasıyla birlikte, iç güvenlikle ilgili istihbarat faaliyetleri günün çağına uygun şekillerde yapılmaya başlanmıştır.

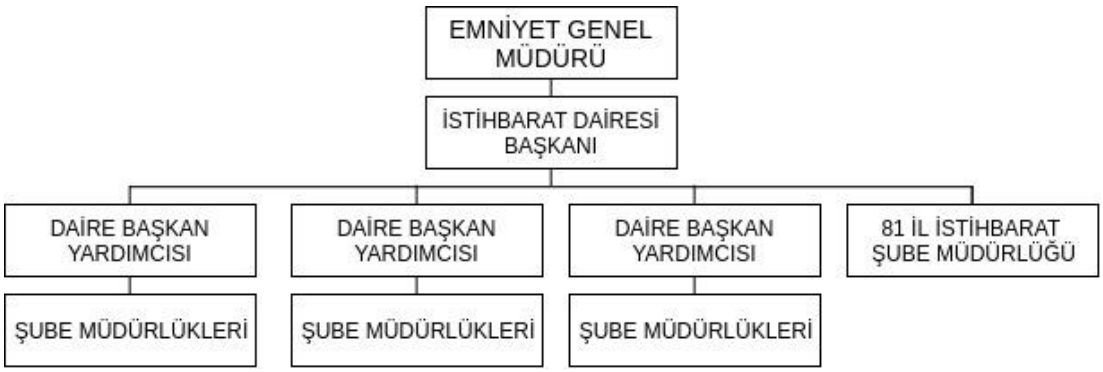
1970'li yıllarda Türkiye'deki ideolojik olayların artmasıyla birlikte, Önemli İşler Müdürlüğü, 1971 yılında dönemin İçişleri Bakanı'nın onayı üzerine, Daire Başkanlığı statüsüne geçirilmiştir. Bu gelişmeyle birlikte teşkilat, Önemli İşler Daire Başkanlığı adını almıştır. 1975 yılında, Önemli İşler Daire Başkanlığı'nın ismi, İstihbarat Başkanlığı'na çevrilmiştir. Böylelikle teşkilatın ismine, görevine matuf "istihbarat" kelimesi eklenmiştir. 1983 yılındaysa İstihbarat Daire Başkanlığı adını almış ve tüm illerde Emniyet Müdürlükleri bünyesinde, istihbarat birimleri oluşturulmuştur.

İstihbarat Dairesi Başkanlığı, kendisine özgü ilk kanun maddesine 1985 yılında PVSK'ya eklenen Ek-7. Madde ile kavuşmuştur. İstihbarat Daire Başkanlığı, 3201 sayılı Emniyet Teşkilatı Kanunu'na göre düzenlenmiş ve 13 Şubat 1989 tarihinde çıkartılan Yönetmelik hükümlerine uygun olarak teşkilatlandırılmıştır. Ek-7 ile birlikte teşkilat, kolluk görevleri sınırlaması olmaksızın, istihbarat faaliyetleri yapmakla da yetkilendirilmiştir. Dönemin Başbakanı Turgut Özal'ın girişimi sayesinde İstihbarat

Daire Başkanlığı, MİT'e alternatif olarak iç istihbarat teşkilatı halini almıştır[16]. İstihbarat Daire Başkanlığı, Atatürk ilke ve inkılaplarına bağlı olarak, kanunlara dayalı yetkiler çerçevesinde, Devletin ülkesi ve milletiyle bölünmez bütünlüğüne, anayasal düzenine ve genel güvenliğine dair koruyucu ve önleyici tedbirler almakla görevlendirilmiştir.

Ayrıca, emniyetin ve asayişin sağlanması için, iç ve dış tehdit oluşturan faaliyetlere karşı, ülke seviyesinde istihbarat faaliyetlerinde bulunmak ve bu maksatla elde edilen bilgilerin hızlı, etkin ve güvenilir bir şekilde değerlendirilmesi, ilgili makam, kurum ve kuruluşlara ulaştırılması görevlerine de sahiptir[17]. İstihbarat Daire Başkanlığı'nın teşkilat yapısı Çizelge 5'teki gibidir.

Çizelge 5: EGM İstihbarat Daire Başkanlığı Teşkilat Yapısı



Kaynak: http://www.istihbarat.pol.tr/Sayfalar/Teskilat-Yapilanmasi.aspx, Erişim tarihi: 18 Aralık 2017.

2.9.2. Jandarma Genel Komutanlığı

Etimolojik olarak Fransızca "gens d'armes", yani silahlı insanlar anlamına gelen "gendarme" kelimesinden Türkçe'ye geçmiş olan jandarma, TDK'daki tanımına göre ülke içindeki kamu düzenini ve genel güvenliği korumakla görevli, kanun ve düzenlerin koyduğu hükümlerin yerine getirilmesi ve bunlara bağlı olarak, hükümetin

[16] http://www.istihbarat.pol.tr/Sayfalar/Tarihce.aspx, Erişim tarihi: 18 Aralık 2017.
[17] http://www.istihbarat.pol.tr/Sayfalar/Misyon-ve-Vizyonumuz.aspx, Erişim tarihi: 18 Aralık 2017.

emirlerini yerine getirmeyi sağlayan, silahlı askeri kuvvettir[18]. Türkçe sözlüğe göre ayrıca, bu görevi yerine getiren kimselere de jandarma denilmektedir. 15 Temmuz Darbe Girişimi'nden önce TSK'nın bir parçası olarak Silahlı Kuvvetlerle ilgili görevleri, eğitim ve öğrenimi bakımından Genelkurmay Başkanlığı'na bağlı olan Jandarma Genel Komutanlığı, emniyet ve asayiş işleriyle diğer görev ve hizmetlerinin yürütülmesi bakımından İçişleri Bakanlığı'na bağlı olarak görev yapmaktaydı.

Genelkurmay Başkanlığı'nın gerek gördüğü hallerle birlikte sıkıyönetim, seferberlik ve savaş hallerinde gerekli olan bölümü Kuvvet Komutanlıkları emrine girmiş, diğer kalan bölümler Jandarma Genel Komutanlığı emrindeki görevlerine devam etmiştir[19]. 25 Temmuz 2016 tarihli ve 668 sayılı Kanun Hükmünde Kararname ile Jandarma Genel Komutanlığı, sivilleştirilerek tamamen İçişleri Bakanlığı'na bağlanmıştır. İlgili KHK ile birlikte Jandarma Teşkilatı, Seferberlik ve savaş hallerinde Komutanlığın, Genelkurmay Başkanlığı'nın görüşü alınarak, Bakanlar Kurulu tarafından verilecek karar neticesinde belirlenecek bölümleri, Kara Kuvvetleri Komutanlığı emrine girmektedir.

Jandarma, 2803 sayılı Jandarma Teşkilat, Görev Yetkileri Kanunu'nunun üçüncü maddesine göre, "emniyet ve asayiş ile kamu düzeninin korunmasını sağlayan ve diğer kanunların verdiği görevleri yerine getiren silahlı genel kolluk kuvvetidir"[20]. Jandarma Genel Komutanlığı'nın resmi sitesinde belirtildiği üzere Jandarmanın görevleri mülki görevler, adli görevler ve askeri görevler olarak üçe ayrılmaktadır. Jandarmanın mülki görevleri arasında emniyet ve asayişle kamu düzenini sağlamak, korumak ve kollamak yer almaktadır. Bunun dışında jandarma, kaçakçılıkla mücadele etmek, suç işlemesini önlemek için gerekli tedbirleri almak ve uygulamak, ceza infaz kurumları ve ceza evlerinin dış korunmalarını sağlamak gibi görevleri de yerine getirmektedir.

[18] http://www.tdk.gov.tr/index.php?option=com_yanlis&view=yanlis&kelimez=83, Erişim tarihi: 19 Aralık 2017.
[19] http://www.jandarma.gov.tr/ust_menu/tarihce.htm, Erişim tarihi: 19 Aralık 2017.
[20] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2803.pdf, Erişim tarihi: 19 Aralık 2017.

Jandarma ayrıca, adli ve askeri görevler dışında kalan ve diğer kanun ve hükümlerin uygulanması için ilgili emir ve kararlara bağlı olarak, kendisine verilen görevleri yapmakla yükümlüdür. Jandarmanın adli görevleri arasındaysa, işlenmiş suçlara istinaden, kanunlarda belirtilen işlemleri yapmak ve bunlara bağlı adli hizmetleri yerine getirmek bulunmaktadır. Jandarmanın askeri göreviyse; kanunlarla kendisine verilen askeri hizmetleri yerine getirmektir[21].

Jandarma Teşkilat, Görev ve Yetkileri Yönetmeliği'nin üçüncü maddesine göre, Jandarma asayiş komando birlikleri, gerektiğinde bağlı olduğu il jandarma komutanlığının diğer birliklerini takviye etmek, her türlü toplumsal olaylara süratle müdahale etmek, terörle mücadele çalışmalarını sürdürmek, takip ve tenkil harekatını yürütmek maksadıyla İçişleri Bakanlığı tarafından gerek görülecek yerlerde konuşlandırılmakta ve görevlendirilmektedir.

Jandarma kriminal birimleri, Jandarma kriminal daire başkanlığı, Jandarma kriminal laboratuvar amirlikleri, olay yeri inceleme timleri, patlayıcı madde imha timleri ve kriminal alanda görev yapmaktadır. Jandarma komando birlikleriyse, gerekli hallerde mahalli jandarma birliklerinin gücü dışına çıkan toplumsal olaylara müdahale etmek ve terörle mücadele çalışmalarını sürdürmek amacıyla Bakanlıkça gerek görülen yerlerde konuşlandırılmakta ve görevlendirilmektedir.

Jandarma ayrıca, İstihbarat Daire Başkanlığı bünyesinde, emniyet ve asayişin sağlanması, suçların ortaya çıkarılması, işlenmiş suçlarda suçluların tespit edilmesi ve yakalanması amacıyla istihbarat toplamaktadır. Ayrıca topladığı istihbaratı, diğer istihbarat ve kolluk birimleriyle paylaşmakta ve onlarla işbirliği yapmaktadır. Jandarma topladığı istihbaratı ayrıca yetkili mercilere ulaştırmakla da görevlidir. İlgili yönetmeliğin, yedinci kısmında açıkça ifade edildiği üzere Jandarma birimlerinde, emniyet ve asayişle ilgili görev alan personelin, resmi kıyafetle görev yapması esastır.

Ancak istihbarat faaliyetlerinin doğası gereği, suç ve suçluların gizli olarak takip edilmesi, yakalanması ve istihbarat, kaçakçılık ve terörle mücadele hizmetleri için,

[21] https://www.jandarma.gov.tr/gorev/gorev_guncel/goreviindex.htm, Erişim tarihi: 19 Aralık 2017.

mülki amir ya da il jandarma komutanının izniyle görevin icap ettirdiği kılık ve kıyafetle hizmet yürütülebilmektedir. Jandarma personeli, bu görevlerin yerine getirilmesi amacıyla, görevin gerektirdiği araç, gereç, donanım, iletişim aracı ve silah kullanabilmektedir[22].

Jandarma, Kanunun 7. maddesinin (a) bendine ilişkin görevlerini yerine getirirken, önleyici ve koruyucu önlemleri almak üzere, sadece kendi sorumluluk alanında Ceza Muhakamesi Kanunu'nun, casusluk suçları hariç, 25. maddesinin birinci fıkrasının (a), (b) ve (c) bentlerinde yazılı suçların işlenmesini önlemek amacıyla, hakim kararı ya da gecikmesinde sakınca bulunan hallerde Jandarma Genel Komutanı ya da İstihbarat Başkanı'nın yazılı emriyle, telekomünikasyon yoluyla yapılan iletişimi tespit edebilme, sinyal bilgilerini değerlendirme ve kayda alma yetkisine sahiptir.

Ayrıca Jandarma, CMK kapsamında, soruşturma konusu suçun işlendiğine dair kuvvetli şüphe ve sebeplerinin bulunması ve başka halde delil elde edilememesi halinde, hakim ya da gecikmesinde sakınca bulunan hallerde Cumhuriyet savcısı kararıyla istihbari faaliyetlerde bulunabilmektedir (Seyrek, 2013, s.155).

2.9.3. Sahil Güvenlik Komutanlığı

13 Temmuz 1982 tarihinde 2692 sayılı Kanun ile kabul edilen ve kurulan Sahil Güvenlik Komutanlığı, 1 Ocak 1985 tarihine kadar JGK'ya bağlı olarak görev yapmıştır. İçişleri Bakanlığı'na bağlı olarak görev yapan Sahil Güvenlik Komutanlığı, 24 Haziran 2003 tarihinde yayınlanan Resmi Gazete'ye belirtilen kanun değişikliği ile müstakil bir yapıya kavuşmuştur[23]. Sahil Güvenlik Komutanlığı da 15 Temmuz Darbe Girişimi'nin ardından İçişleri Bakanlığı'na bağlanmış bir silahlı genel kolluk kuvvetidir.

2016 yılında yürürlüğe giren 668 sayılı KHK gereğince sivilleştirilen Sahil Güvenlik Komutanlığı'nın belirlenen bölümleri seferberlik ve savaş hallerinde, Bakanlar Kurulu kararıyla Deniz Kuvvetleri Komutanlığı emrine girmektedir. Kalan

[22] http://www.resmigazete.gov.tr/eskiler/2017/01/20170121-8.pdf, Erişim tarihi: 19 Aralık 2017.
[23] http://www.sahilguvenlik.gov.tr/baskanliklar/genel_sekreterlik/tarihce/tarihce.asp, Erişim tarihi: 20 Aralık 2017.

bölümlerse normal görevlerine devam etmektedir. Sahil Güvenlik Komutanlığı'nın görev alanları, üsleri ile kadrolarıyla yerleşme yerleri, İçişleri Bakanlığı tarafından düzenlenmektedir. 668 sayılı KHK gereğince seferberlik ve savaş hallerinde, DKK emrine girecek birliklerin kuruluş ve kadrolarıyla konuş yerlerinin düzenlenmesinde Genelkurmay Başkanlığı'nın görüşü alınmaktadır.

Sahil Güvenlik Komutanlığı, 2692 sayılı Kanun'un 4. maddesinde belirtilen kanunlara dayalı olarak, Türk karasuları ile birlikte iç suları olan Marmara Denizi ile İstanbul ve Çanakkale Boğazları, liman ve körfezleri, münhasır ekonomik bölgesiyle ulusal ve uluslararası hukuk kurallarına göre egemenlik ve denetimi altında bulunan deniz alanlarında kendisine verilen görevleri uygulamak ve yetkileri kullanmakla yükümlüdür.

2692 sayılı Kanun gereğince, kendilerine verilen görevlerin yerine getirilmesi için Sahil Güvenlik Komutanlığı mensuplarına bir takım yetkiler verilmiştir. Buna göre liman sınırları dışında Türk Kanunları'na göre cezalandırılması icap eden eylemlere, ilgili kanun ve uluslararası andlaşmalarda yer alan hükümlere göre elkoyma yetkisine sahiptirler.

SGK personeli ayrıca suçun denizde başlayıp karada devam etmesi veya suçluların karaya geçmesi hallerinde, yetkili güvenlik kuvvetinin olaya elkoymasına kadarki süreçte, suç delillerinin kaybolması ve suçluların kaçmasını önlemek amacıyla, kendilerine verilen yetkileri karada da sürdürebilmektedir. Böyle bir durumun mevcudiyetinde, en kısa sürede mülki amir durumdan haberdar edilmektedir[24].

2.9.4. Kamu Düzeni ve Güvenliği Müsteşarlığı

Türkiye'nin uzun yıllardır sürdürmekte olan terörle mücadele geçmişinde, bütüncül bir stratejinin bulunmadığı ve terör sorununa sivil bir açıdan bakan bir kurumun olmadığına ilişkin ciddi bir eksiklik olduğu dile getirilmiştir. KDGM bu eksikliğin ortadan kaldırılması amacıyla, terörle mücadeleye ilişkin politikaların ve

[24] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.2692.pdf, Erişim tarihi: 20 Aralık 2017.

stratejilerin geliştirilmesi ve bu konuda ilgili kurum ve kuruluşlar arasında koordinasyonu sağlamak üzere, 5982 sayılı "Kamu Düzeni ve Güvenliği Müsteşarlığının Teşkilat ve Görevleri Hakkında Kanun" ile İçişleri Bakanlığı'na bağlı olarak kurulmuştur. Müsteşarlık, daha sonra 08.07.2011 tarihinde yapılan değişiklikle Başbakanlık'a bağlanmıştır. 03.09.2014 tarihli Resmi Gazete'de yayımlanarak yürürlüğe giren düzenlemeyle birlikte Müsteşarlık, tekrar İçişleri Bakanlığı'na bağlanmış olup, çalışmalarını bakanlık bünyesinde yürütmeye devam etmektedir.

Müsteşarlık, ilgili kanunla kendisine verilen görevleri yürütmektedir ancak güvenlikle ilgili operasyonel bir görevi bulunmamaktadır[25]. KDGM bünyesinde terörle mücadele alanında, güvenlik kuruluşları ve ilgili kurumlar arasındaki gerekli koordinasyonun sağlanması, bu alandaki politika ve uygulamaların değerlendirilmesi için Terörle Mücadele Koordinasyon Kurulu kurulmuştur. Kurul, İçişleri Bakanı başkanlığında, Genelkurmay İkinci Başkanı, Jandarma Genel Komutanı, MİT Müsteşarı, KDGM Müsteşarı, Emniyet Genel Müdürü ve Sahil Güvenlik Komutanı'ndan oluşmaktadır.

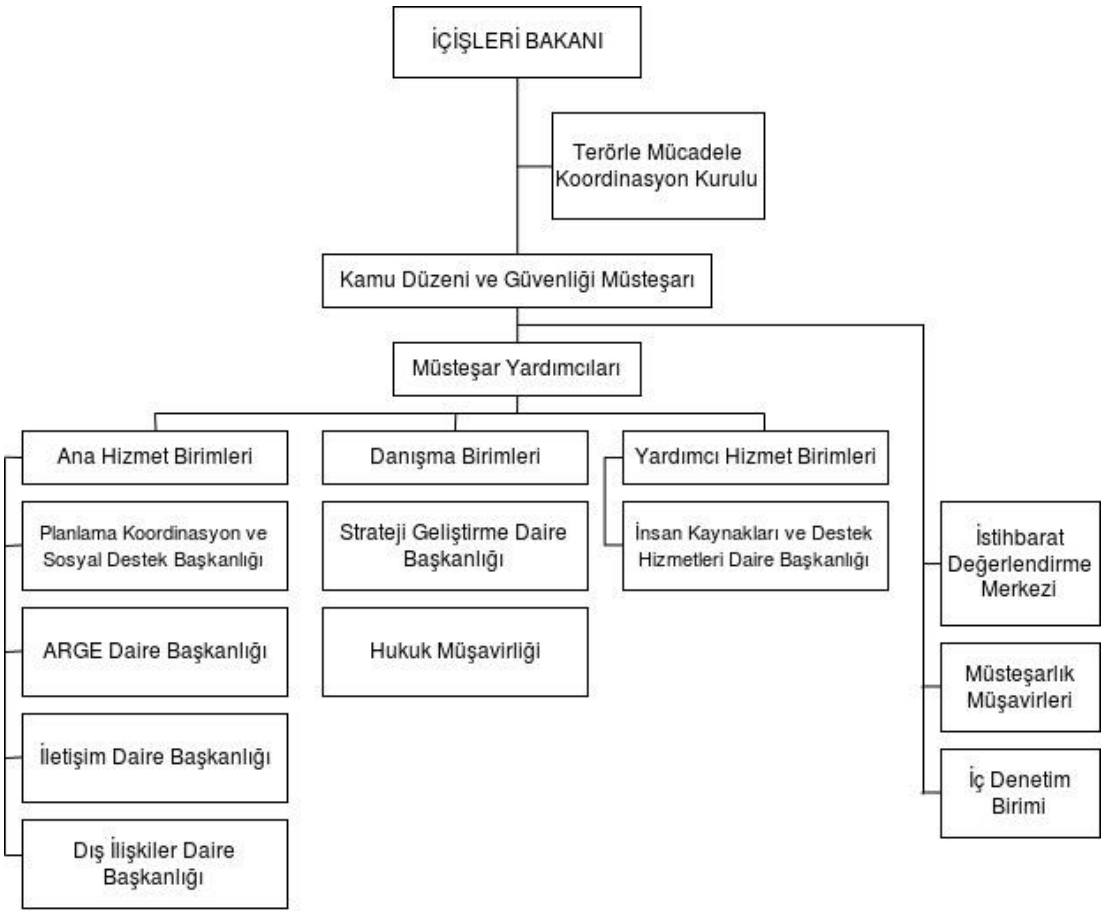
Gerekli durumlarda, gündemle ilgili diğer kurum ve kuruluşların temsilcileri de toplantıya davet edilebilmektedir. Kurul, İçişleri Bakanı'nın daveti üzerine toplanmaktadır. Toplantı gündemi, Kurul üyelerinin görüşleri alınarak, İçişleri Bakanı tarafından belirlenmektedir. KDGM, Müsteşar, müsteşar yardımcıları ile ana hizmet, danışma ve yardımcı hizmet birimlerinden oluşmaktadır. Gerekli görülmesi halinde, görev ve hizmet süreleri belirtilmek suretiyle, Müsteşarın teklifi ve İçişleri Bakanı'nın onayı ile özel uzmanlık ve araştırma komisyonları kurulabilmektedir.

KDGM bünyesinde yer alan İstihbarat Değerlendirme Merkezi, doğrudan Müsteşara bağlı olarak terörle mücadele kapsamında ilgili birimlerden stratejik istihbaratın alınması ve değerlendirilmesi faaliyetlerini yürütmektedir. Güvenlik kuruluşları ve istihbarat birimleriyle Dışişleri Bakanlığı tarafından elde edilecek stratejik bilgi ve istihbarat, bu merkezde değerlendirilmektedir.

[25] http://www.kdgm.gov.tr/tarihcemiz, Erişim tarihi: 20 Aralık 2017.

Terörle mücadeleye yönelik strateji belirlemek amacıyla ihtiyaç duyulan istihbari bilgiler; Genelkurmay Başkanlığı, Dışişleri Bakanlığı, MİT, Jandarma Genel Komutanlığı, Emniyet Genel Müdürlüğü ve Sahil Güvenlik Komutanlığı tarafından KDGM'ye verilmektedir. Bu bilgiler eşliğinde yapılacak analiz ve değerlendirmeler, ilgili birimlerle paylaşılmaktadır[26]. Kamu Düzeni ve Güvenliği Müsteşarlığı'nın teşkilat yapısı Çizelge 6'daki gibidir.

Çizelge 6: Kamu Düzeni ve Güvenliği Müsteşarlığı Teşkilat Yapısı



Kaynak: http://www.kdgm.gov.tr/teskilat, Erişim tarihi: 21 Aralık 2017.

[26] http://www.mevzuat.gov.tr/MevzuatMetin/1.5.5952.pdf, Erişim tarihi: 21 Aralık 2017.

2.9.5. Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Dairesi Başkanlığı ve Örgütsel Yapısı

Türkiye'de kaçakçılıkla ilgili istihbaratın bir merkezde toplanması ve değerlendirilmesine ilişkin çalışmalar, 21 Kasım 1978 gün ve 237 sayılı Milli Güvenlik Kurulu kararı ile birlikte başlatılmış olup, 1981 yılında İçişleri Bakanlığı bünyesinde, Kaçakçılık İstihbarat ve Harekat Merkezi kurulmuştur. Buna göre teşkilat, kaçakçılık istihbaratıyla ilgili kurumların, uyum ve işbirliği içinde çalışmalarına yönelik faaliyetler yürütmekle görevlendirilmiştir.

Teşkilat, daha sonra Jandarma Genel Komutanlığı ve Emniyet Genel Müdürlüğü'nün ortak teklifiyle, daha önce işlediği suçtan dolayı tüm ülkede aranan, ancak ele geçirilmemiş, kimliği belirlenmiş kişilerle; çalıntı motorlu taşıt, çalınan veya kaybedilen ateşli silahlar ve her türlü kimlik bilgilerini bulmak ve ele geçirmek, bu konuda iller seviyesinde tasnif edilecek bilgilerin bir merkezde toplanmasını sağlamak, bu bilgilerin ilgili kişi ve mercilere doğru gönderilmesini sağlayarak, genel kolluk kuvvetlerinin adli ve idari soruşturmalarına hız ve netlik kazandırmakla görevlendirilmiştir.

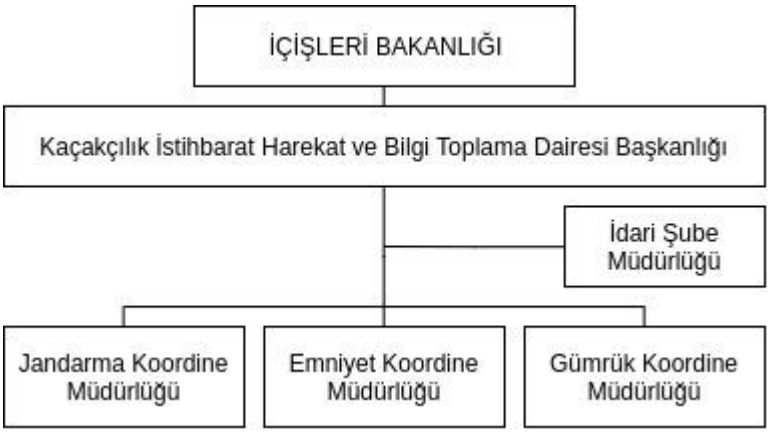
İçişleri Bakanlığı Teşkilatının Yeniden Düzenlenmesine İlişkin 13.12.1983 Tarih ve 176 Sayılı Kanun Hükmünde Kararname ve bu kararnamenin değiştirilerek kabul edilmesiyle kesinleşen 14.02.1985 Tarih ve 3152 Sayılı İçişleri Bakanlığı Teşkilat ve Görevleri Hakkındaki Kanun İle; Kaçakçılık, İstihbarat, Harekat ve Bilgi Toplama Daire Başkanlığı haline getirilmiştir[27].

Kaçakçılık, İstihbarat, Harekat ve Bilgi Toplama Dairesi Başkanlığı'nın görevleri, öncelikli olarak kaçakçılık istihbaratının yapılması ve planlanarak yönlendirilmesi, koordine edilmesidir. Bununla birlikte başkanlıkça yapılacak görevler, İçişleri Bakanlığı Müsteşarı veya Yardımcısı başkanlığında toplanan Kaçakçılık İstihbarat Koordinasyon Kurulunca belirlenir. KİKK, başkanlığın en üst düzeydeki kuruludur. Kurul, yurt içi ve yurt dışında, Türkiye Cumhuriyeti'ne yönelik yapılan kaçakçılık faaliyetlerini değerlendirmektedir ve tespit edilen kaçakçılıkla, nasıl mücadelede

[27] http://www.kihbi.gov.tr/tarihe, Erişim tarihi: 21 Aralık 2017.

edileceği konusunda alınacak tedbirler belirlenmektedir. KİHBİ Daire Başkanlığı'nın teşkilat yapısı Çizelge 7'deki gibidir.

Çizelge 7: Kaçakçılık İstihbarat Harekat ve Bilgi Toplama Dairesi Başkanlığı Teşkilat Yapısı



Kaynak: http://www.kihbi.gov.tr/sema, Erişim tarihi: 21 Aralık 2017.

2.10. Milli İstihbarat Teşkilatı

İçişleri Bakanlığı bünyesinde olmamasına rağmen, dış istihbarattan başka, kamu güvenliği açısından iç istihbarat faaliyetleri yürütmekte olan bir diğer önemli kurum da Milli İstihbarat Teşkilatı'dır. Devlet çapında istihbarat oluşturmakla görevli olan MİT, 19 Aralık 1926 tarihli ve "Gazi Mustafa Kemal" onaylı gizli kararnamesi ile resmiyet kazandırılmış olan Milli Emniyet Hizmeti Riyaseti'nin zaman içerisinde çeşitli gelişim ve değişimlere uğramasıyla birlikte, 22 Temmuz 1965 tarihinde yayınlanan 644 sayılı Milli İstihbarat Teşkilatı Kanunu ile birlikte resmen hizmete girmiştir[28]. 1983 yılında çıkarılan 2937 sayılı Kanun ile MİT'in bugünkü görev ve sorumlulukları belirlenmiştir. Buna göre MİT'in görevleri şu şekildedir:

■ Türkiye Cumhuriyetinin ülkesi ve milleti ile bütünlüğüne, varlığına, bağımsızlığına, güvenligine, Anayasal düzenine ve milli gücünü meydana getiren bütün unsurlarına karşı içten ve dıştan yöneltilen mevcut ve muhtemel faaliyetler

[28] http://www.mit.gov.tr/tarih_index.html, Erişim tarihi: 22 Aralık 2017.

hakkında milli güvenlik istihbaratını Devlet çapında oluşturmak ve bu istihbaratı Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile gerekli kuruluşlara ulaştırmak.

■ Devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamak.

■ Kamu kurum ve kuruluşlarının istihbarat faaliyetlerinin yönlendirilmesi için Cumhurbaşkanı, Başbakan ve Milli Güvenlik Kuruluna tekliflerde bulunmak.

■ Kamu kurum ve kuruluşlarının istihbarat ve istihbarata karşı koyma faaliyetlerine teknik konularda müşavirlik yapmak ve koordinasyonun sağlanmasında yardımcı olmak.

■ Genelkurmay Başkanlığınca Silahlı Kuvvetler için lüzum görülecek haber ve istihbaratı, yapılacak protokole göre Genelkurmay Başkanlığına ulaştırmak.

■ Milli Güvenlik Kurulunda belirlenecek diğer görevleri yapmak.

■ İstihbarata karşı koymak,

■ Dış güvenlik, terörle mücadele ve millî güvenliğe ilişkin konularda Cumhurbaşkanınca veya Bakanlar Kurulunca verilen görevleri yerine getirmek.

■ Dış istihbarat, millî savunma, terörle mücadele ve uluslararası suçlar ile siber güvenlik konularında her türlü teknik istihbarat ve insan istihbaratı usul, araç ve sistemlerini kullanmak suretiyle bilgi, belge, haber ve veri toplamak, kaydetmek, analiz etmek ve üretilen istihbaratı gerekli kuruluşlara ulaştırmak.

■ İstihbarat kapasitesini, niteliğini ve etkinliğini artırmak amacıyla çağdaş istihbarat usul ve yöntemlerini araştırmak, teknolojik gelişmeleri takip etmek ve uygun görülenleri temin etmek.

17/4/2014 tarihli 6532 sayılı Kanun'un 1. maddesinde ifade edildiği üzere, MİT'e yukarıda yer alan bu görevler dışında başka görev verilememektedir. Türkiye'nin jeo-stratejik konumu, bölgesel ve uluslararası sorunlarla çıkar çatışmaları, siyasi, ekonomik, askeri ve güvenlik konularının girift yapısı sebebiyle, haber toplama ve değerlendirme faaliyetleri bakımından iç ve dış tehditlere bir bütün olarak yaklaşmak gerekmektedir. Buna göre MİT, kanun gereği iç ve dış kaynaklarca sağlanacak istihbaratı, devlet çapında oluşturmakla görevlidir[29].

İlgili kanunun 4. maddesine göre Milli İstihbarat Teşkilatı, devletin milli güvenlik siyasetiyle ilgili planların hazırlanması ve yürütülmesinde; 2937 sayılı kanunun 4 üncü maddesine göre MİT Müsteşarlığı devletin milli güvenlik siyaseti ile ilgili planların hazırlanması ve yürütülmesinde; Cumhurbaşkanı, Başbakan, Genelkurmay Başkanı, Milli Güvenlik Kurulu Genel Sekreteri ile ilgili bakanlıkların istihbarat istek ve ihtiyaçlarını karşılamaktadır[30]. MİT'in teşkilat yapısı Çizelge 8'deki gibidir.

Çizelge 8: MİT Teşkilat Yapısı

Kaynak: http://www.mit.gov.tr/teskilat.html, Erişim tarihi: 22 Aralık 2017.

■ Stratejik Analiz Başkanlığı; Türkiye'nin stratejik istihbarat ihtiyacını karşılamak için, kısa, orta ve uzun vadeli stratejik analiz üretmekle görevli başkanlıktır. Başkanlık, bu amaçla bölgesel ve küresel gelişmeleri yakından takip ederek, toplumsal dinamikleri çözümlemekte, birbirinden bağımsız görünen olaylar arasındaki nedensellik bağını ortaya çıkarmakta ve öngörüde bulunmaktadır.

[29] http://www.mit.gov.tr/me_diger.html, Erişim tarihi: 22 Aralık 2017.
[30] https://www.mit.gov.tr/2937.pdf, Erişim tarihi: 22 Aralık 2017.

■ İstihbarata Karşı Koyma Başkanlığı; yabancı devlet, gizli servis, kurum/kuruluş ve kişilerin Türkiye'ye yönelik casusluk faaliyetlerinin tespiti ve engellenmesiyle görevlidir. Başkanlık, bu amaçla karşı casusluk faaliyetleri yürütmekte, casusluk faaliyetlerinin hedefi olan kamu ve özel sektör kurum/kuruluşları ile işbirliği ve koordinasyon çalışmalarını sürdürmektedir.

■ Dış Operasyonlar Başkanlığı; Türkiye'nin stratejik çıkarlarının korunması ve geliştirilmesiyle görevli başkanlıktır. Başkanlık, yurt içi ve yurt dışı birimlerle birlikte çalışmalar yapmaktadır. Türkiye'nin Milli Güvenlik Stratejisini destekleyen çizgide ve siyasi gelişmelere paralel bir şekilde faaliyetlerini sürdürmektedir.

■ Güvenlik İstihbaratı Başkanlığı; öncelikli olarak terör örgütleri ve terörist faaliyetler olmak üzere, Türkiye'nin milli gücüne yönelik tehditlere karşı güvenlik istihbaratı toplamakla görevli başkanlıktır. Başkanlık tarafından yurt içinde ve yurt dışında toplanan istihbarat, güvenlik önlemlerinin alınması ve tehdidin yok edilmesi için kullanılmaktadır.

■ Elektronik-Teknik İstihbarat Başkanlığı; devlet sırrının açığa çıkarılmasının tespit edilmesi ve terörist faaliyetlerin önlenmesi için telekomünikasyon yoluyla yapılan iletişimi tespit etmek ve dinlemek, sinyal bilgilerini değerlendirerek kaydetmekle görevli başkanlıktır. Başkanlık, ses ve görüntü analizi yapmakta, görüntü istihbaratı (IMINT) üretmekte, şifreli verileri çözmekte ve siber tehdit unsurlarına karşı çalışmalar yürütmektedir.

■ Sinyal İstihbarat Başkanlığı; muhabere ve muhabere dışı sinyalleri kullanarak erken ihbar ve uyarı bilgileri dahil olmak üzere sinyal istihbaratı üretmekle görevli başkanlıktır. Başkanlık, bu amaçla haberleşme ve radar sinyallerini yakalayarak, elde edilen bu sinyalleri analiz etmekte ve istihbarata dönüştürmektedir[31].

[31] http://www.mit.gov.tr/teskilat.html, Erişim tarihi: 24 Aralık 2017.

ÜÇÜNCÜ BÖLÜM

3. SİBER İSTİHBARATIN KAMU GÜVENLİĞİ İÇİN ROLÜ VE ÖNEMİ

3.1 Sibernetiğe İlişkin Temel Kavramlar

Siber istihbarat ve siber güvenlik ile ilgili konulara değinmeden önce, sibernetik içinde yer alan kavramların açıklanması faydalı olmaktadır. Bu kavramların Türkiye'de ne yazık ki henüz oturmamış olması sebebiyle, yapılan çalışmalarda da eksiklikler ve hatalar olduğu gözlemlenmektedir. Siber istihbarat ve siber güvenlik gibi konular, uzun bir çalışma, yüksek tecrübe, gelişmiş analitik düşünme gücü ile birlikte, bu konulara ilişkin kavramların doğru kullanılmasını da gerektirmektedir.

3.1.1. Sibernetik

Bugün, siber olarak kısaltılmış olan sibernetik terimi, ilk olarak ABD'li bir bilim insanı olan Norbert Weiner tarafından 1948 yılında, "hayvanlarda ve makinelerde iletişim ve kontrol bilimi" anlamında kullanılmıştır (Glaserfeld, 2002, s.3). Bu tanımla birlikte ilerleyen yıllarda, hayvanlardaki sinir ağlarının makinelere entegrasyonuyla ilgili çeşitli çalışmalar yapılmaya başlanmıştır.

Yapay sinir ağları ve yapay zeka gibi kavramların ortaya çıkmasıyla birlikte, sibernetik olarak tabir edilen kavram, bugünkü haline iyice yaklaşmıştır. Sibernetik kavramının Türkçe'de çok yaygın olarak kullanılmadığı, özellikle son yıllarda artan

siber saldırılar ve buna bağlı olarak yaygınlaşan siber güvenlik kavramıyla birlikte tekrar gün yüzüne çıktığı görülmektedir.

Bugüne kadar Türkçe'de sibernetik yerine kullanılan en yakın tanımın "bilişim" olduğu görülmektedir. TDK'ya göre bilişim, "İnsanlar tarafından teknik, ekonomik ve toplumsal alanlarda iletişim için kullanılan ve bilimin dayanağı olan bilginin, bilhassa elektronik makineler vasıtasıyla düzenli ve akla uygun bir şekilde işlenmesi bilimidir"[32]. Bilişim yerine ayrıca Fransızca "informatique" sözcüğünden gelen ve Türkçe'ye de "enformatik" olarak geçen ifade de kullanılmaktadır.

Enformatik ise insan hayatının vazgeçilmez bir parçası olan bilginin nasıl üretildiğini, iletildiğini ve kullanıldığını inceleyen bilim dalıdır. Görseller, videolar, metinler ve istatistikler vb. çeşitli biçimlerdeki bilginin doğasını ve fikirle ilişkisini incelemektedir. Bilginin elde edilmesi, tasnif edilmesi, depolanması vb. konularla, gerektiği hallerde kullanılmak üzere ilgili sistem ve teknolojilerle ilgili uygulama ve araştırmalar yapan bir bilim dalıdır[33].

Görüldüğü gibi bilişim ve enformatik tanımlarında bilgiden sıkça söz edilmektedir. Dolayısıyla siber kavramıyla ağlar ile birbirine bağlı cihazlar ve cihazların bağlı olduğu sistemlerden oluşan ortam ifade edilmekeyken, bilişim ve enformatik tanımıyla bu ortamdan etkin bir şekilde faydalanmak veya bu ortamın kullanılarak bilgi üretilmesi ve iletilmesi ifade edilmektedir.

3.1.2. Siber Uzay

Türkçe'de sanal ortam, sanal alem veya siber alem gibi farklı şekillerde de ifade edilen, ancak bugünkü tam karşılığı siber uzay (cyberspace) olan kavram, ilk olarak Kanadalı ünlü bilim kurgu yazarı William Gibson tarafından, önce 1982 yılında "Burning Chrome" isimli romanında, daha sonra da 1984 yılında bir bilgisayar korsanının "Matrix" adı verilen bir bilgisayar sistemi içinde yaşadıklarını anlatan "Neuromancer" isimli romanında kullanılmıştır. Aslında bu roman sadece siber uzayın

[32] http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&kelime=bilişim, Erişim tarihi: 24 Aralık 2017.
[33] http://enformatik.aku.edu.tr/bolum-hakkinda-2/enformatik-nedir, Erişim tarihi: 24 Aralık 2017.

değil, aynı zamanda sanal gerçeklik, yapay zeka ve genetik mühendisliği gibi kavramların da ilk olarak ele alındığı eser olarak nitelendirilmektedir (Keleştemur, 2015, s.133).

Siber uzay, ABD Genelkurmay Başkanlığı tarafından yapılan tanıma göre "İnternet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve kontrol birimlerini içeren, birbirine karşılıklı olarak bağımlı olan, bilgi teknolojileri altyapıları tarafından oluşturulan küresel alandır[34]. NATO'nun siber güvenlik terimleri sözlüğünde yer alan tanıma göreyse siber uzay, insanların, yazılım ve servislerin cihazlar ve ağlar üzerinden birbirleriyle etkileşimde bulunduğu, fiziksel bir biçimi bulunmayan, karmaşık bir ortamdır[35].

NATO'nun tanımında, insanlara da yer verilmektedir. Dolayısıyla siber uzay için sadece bilgisayar sistemlerinden ya da birbirlerine bağlı cihazlardan bahsetmek doğru değildir. Bu sistem ve cihazlarla birlikte, sibernetik ve/veya enformatik teknolojilerini kullanan insanlar da siber uzayın birer parçası haline gelmektedir. Bir başka ifadeyle iletişim ağları, bilgi sistem teknolojileri, askeri ağlar, enerji dağıtım ağları, mobil cihazlar, IoT cihazlar, elektronik komuta sistemleri, uydu sistemleri, İHA'lar, telsizler, SCADA sistemler vb. siber uzayı meydana getirmektedir.

Siber uzayın uluslararası ilişkilerdeki yeri de günden güne farklılık göstermektedir. Günümüzde halen bilişim hukukuna yönelik çeşitli gelişmeler, yenilikler yaşanmaktadır. Siber uzayın aktörlerinin, geniş bir coğrafyaya hızlı ve anonim olarak erişme imkanı sunmasından dolayı, özellikle saldırılar bakımından büyük bir kolaylık sağladığı görülmektedir. Gerekli teknik bilgi ve beceriye sahip kimselerin, kolaylıkla dünyanın herhangi bir yerindeki ağ bağlantısına ya da bu ağa bağlı sistemlere saldırabildiği bilinmektedir.

Siber saldırılara karşı, yerel ağların ya da internete bağlı olmayan sistemlerin, korunaklı olduğuna ilişkin yorumlar olmasına karşın, bu ifadeler günümüz saldırı

[34] https://fas.org/irp/doddir/dod/jp1_02.pdf, Erişim tarihi: 25 Aralık 2017.
[35] https://ccdcoe.org/cyber-definitions.html, Erişim tarihi: 25 Aralık 2017.

yöntemleri karşısında geçersiz olmaktadır. Bugün hava boşluklu, ağ bağlantısı bulunmayan sistemler üzerinden dahi bilgi hırsızlığı yapıldığı görülmektedir[36]. Tüm bu durum siber uzayı, saldırılar için etkin ve hassas bir ortam haline getirmektedir.

3.1.3. Siber Saldırı

Basit bir ifadeyle siber uzay üzerinden gerçekleştirilen her türlü saldırıya siber saldırı denilmektedir. Sibr saldırılar verilere ya da sistemlere yönelik olmak üzere iki farklı şekilde gerçekleştirilmektedir. Verilere yapılan siber saldırılar, bilgi güvenliğini bütünlük ve kullanılabilirlik ögelerini tehdit etmektedir. Sistemlere yönelik saldırılar ise bilgi güvenliğinin erişilebilirlik ögesini tehdit etmektedir. Ancak çoğu siber saldırının bu üç ögeyi birden tehdit ettiği görülmektedir. Verilerin ele geçirilmesi ya da değiştirilmesi, verilere yönelik saldırılara örnek verilebilmektedir.

Sunuculara yapılan DDoS saldırıları neticesinde, bir web sitesinin erişilemez hale getirilmesiyse sistemlere yönelik saldırılara örnek olarak gösterilebilir. 2010 yılı öncesine kadar saldırılar genellikle DDoS ile hedef sistemin hizmet veremez hale getirilmesi ya da web sunucularına indeks atılması gibi faaliyetler üzerine kuruluyken, 2010 yılından itibaren özellikle APT (Advanced Persistent Threat – Gelişmiş Kalıcı Tehdit) saldırılarının gelişmesiyle birlikte evrilmiş, daha komplike bir hale gelmiştir. APT saldırılarına örnek olarak Stuxnet vakası gösterilebilmektedir.

Bunun dışında siber uzayda saldırı yöntemi olarak kullanılan sosyal mühendislik ve sosyal medya saldırıları da bulunmaktadır. Gelmiş geçmiş en büyük hacker'lardan biri olan Kevin Mitnick'in en çok kullandığı yöntem olan sosyal mühendislik, bugün bile en başarılı yöntemler arasındadır. Sosyal mühendislik yoluyla, hedef kişiye sanki bir arkadaş, akraba, güvenlik uzmanı ya da bir firma temsilcisi gibi yaklaşarak, istenilen bilgiye erişilebilmektedir. Bu bilgiler daha sonra toplanarak, biyografik istihbarat oluşturulabilmektedir. Ayrıca kimlik bilgisi ya da kredi kartı vb. ele geçirilmesiyle ekonomik saldırılar da düzenlenebilmektedir.

[36] https://www.insidescience.org/news/computers-can-be-hacked-using-high-frequency-sound, Erişim tarihi: 26 Aralık 2017.

Sosyal medya bugün insanların sosyalleşebilmesi, sevdikleriyle birlikte sohbet edebilmesi ve paylaşım yapabilmesi için en çok kullanılan platform haline gelmiştir. Daha önceleri forum, haber grupları ve sohbet odaları varken, bugün sosyal medya üzerinden hepsi bir arada etkileşim içine girmek mümkündür.

Facebook, Twitter, YouTube, Google Plus, MySpace, Instagram, Vine gibi pek çok paylaşım platformu sayesinde sadece kişiler arası iletişim değil, haber paylaşımı da yapılabilmektedir. Ancak burada dikkat edilmesi gereken en önemli konu, özellikle sosyal medya üzerinden paylaşılan haberlerin propaganda ve manüpilasyon aracı olarak kullanılabildikleridir.

Toplumsal olayların birçoğunda paylaşılan haberlerin bazılarının yanlış, manüpilatif olduğu gözlemlenmiştir. Çeşitli görseller üzerinde oynama yapılarak, yapılan yorumların sosyal medya kullanıcıları üzerinde etki yarattığı görülmüş, çeşitli örgütler ve hatta istihbarat servisleri tarafından sosyal medya etkin bir şekilde kullanılmaya başlanmıştır. Sosyal medya ya da sohbet ortamları üzerinden paylaşılan fotoğraflar oldukça önemlidir.

Yapılan yanlış paylaşımlar sebebiyle, tehdit ve şantaja maruz kalan internet kullanıcılarının intihara sürüklediği görülmüştür[37]. Siber saldırı, siber korsanlar tarafından yapılabileceği gibi, devletlerin ilgili kurum ve kuruluşlarında görevli kişiler tarafından da gerçekleştirilebilmektedir. Dolayısıyla siber saldırı gerek yasal anlamda gerekse de teknik anlamda farklılıklar gösterebilmektedir. Siber saldırı yöntemleri gün geçtikçe değişmekte çeşitlenmektedir.

APT (Gelişmiş Kalıcı Tehdit) saldırıları sayesinde, hedefin haberi olmadan, arka planda bilgi elde etmek, tüm sistemi ele geçirmek, kullanılamaz hale getirmek ve hatta fiziksel etki oluşturmak mümkündür. Ancak sadece APT saldırıları değil, aynı zamanda AET (Gelişmiş Atlatma Teknikleri) saldırılarına karşılık verebilmek için de gerekli güvenlik sistemleri oluşturulmalıdır. Siber saldırılar, siber uzayda koşmakta

[37] https://www.theguardian.com/commentisfree/2012/oct/26/amanda-todd-suicide-social-media-sexualisation, Erişim tarihi: 26 Aralık 2017.

olan yazılım, donanım ve altyapıları hedef almaktadır. Siber saldırıların amaçları, saldırı şekilleri ve etkileri farklılık göstermektedir.

Siber saldırıların sebepleri arasında en temel olanları siyasi ve politik sebepler, ekonomik nedenler, dini inançlar, ego, intikam alma ya da merak olabilmektedir. Saldırı amaçları ideoliji empoze etme, bilgi hırsızlığı, hedef sistemi çökertmek gibi çeşitliklik arz etmektedir.

Buradaki amaç, kurum ya da devletin siyasi stratejisi ile de orantılıdır. Saldırılar temel olarak, aktif ve pasif saldırı olarak ikiye ayrılmaktadır. Aktif saldırılar, doğrudan hedefteki bilgiyi ele geçirmek, sisteme zarar vermek ya da devre dışı bırakmak gibi faaliyetlerdir. Pasif saldırılar ise sistem üzerindeki bilgi akışını ve davranışları gözlemleme üzerine yapılmaktadır. Siber saldırılar şu süreçleri izlemektedir:

1) Bilgi Toplama (Reconnaissance)
2) Tarama (Scanning)
3) Erişim ve Yetki Yükseltme (Access and Escalation)
4) Erişimi Sürdürme (Maintaining Access)
5) İzleri Silme (Covering Tracks)

Siber saldırının etkisi, hedefe göre değişiklik göstermektedir. Bugün gelişmiş olan saldırı şekilleri sayesinde tüm sistemi, hatta sisteme bağlı ne varsa tamamen çalışılmaz hale getirmek mümkün olmaktadır. Siber uzay üzerinden yapılan saldırılar neticesinde yangına ve hatta patlamaya varacak tesirler oluşturmak mümkündür.

Siber saldırı türlerinin en önemli olanları aşağıda verilmiştir. Bu saldırı türleri, kendi aralarında da alt kategorilere ayrılmakla birlikte, farklı yöntemlere sahip olabilmektedir. Listede yer alan yöntemler alfabetik sıraya göre dizilmiştir. Bu yöntemlerden başka yöntemler de bulunmaktadır.

- Arka kapı
- Açık mikrofon dinleme
- GSM / VoIP vb. Dinleme

- Ağ dinleme
- Ağ tarama ve haritalama
- Hizmet dışı bırakma
- IP aldatmacası
- DNS aldatmacası
- İnternet servis saldırıları
- Kabloya saplama yapma
- Kriptografik saldırılar
- Oturum çalma
- Sosyal mühendislik
- Trafik analizi
- Yemleme
- Yerine geçme
- Yığın e-posta gönderme
- Zamanlama saldırıları
- Zararlı yazılım

3.1.4. Siber Suç

Siber suç, yine en çok karıştırılan kavramların başında gelmektedir. Siber uzay üzerinden yapılan ve suç unsuru teşkil eden her suç, siber suç değildir. Konuyla ilgili daha fazla ayrıntı vermeden önce, siber suç kavramına değinmek gerekmektedir. Siber Suç, bilişim sistemi kullanılarak, bir bilişim sisteminin güvenliğini ya da buna bağlı verileri hedef alan suçlardır. Dolayısıyla siber suçun işlenmiş olması için, bir bilişim sistemine hukuka aykırı bir şekilde girilmiş olması gerekmektedir.

Siber suçlara örnek olarak bir sisteme izinsiz girmek, sisteme ya da verilere zarar vermek, verileri silmek, şifrelemek, veri eklemek veya sistemin kullanımını engellemek gösterilebilir. Ayrıca özel hayatın gizliliğine müdahalede bulunmak,

iletişimi engellemek ve iletişimi izinsiz izlemek ya da kaydetmek gibi eylemler de siber suç kategorisinde değerlendirilmektedir[38].

Siber suçlar için dijital suçlar, internet suçları ya da ileri teknoloji suçları gibi ifadeler de kullanılmaktadır. Ancak bu ifadeler arasında en doğru olanı kuşkusuz siber suçtur. Siber suçlarla ilgili çeşitli düzenlemeler yapılmaktadır. Bunlardan en kapsamlısı Avrupa Konseyi tarafından oluşturulan Avrupa Siber Suç Sözleşmesi'dir. İlgili sözleşme, Avrupa Konseyi Bakanlar Komitesi'nce kabul edilmiş olup, Budapeşte'de düzenlenen Siber Suçlar Uluslararası Konferansı'nda imzalanmıştır. Bu sözleşmenin ikinci bölümüne göre siber suçlar şu şekilde sınıflandırılmıştır[39]:

- Bilgi güvenliğinin gizlilik, erişilebilirlik ve bütünlük unsurlarını hedef alan, bilgisayar sistemleri ve verilerine yasadışı erişim, yasadışı durdurma, değiştirme, cihazların kötüye kullanımı,
- Bilgisayarlarla ilgili sahtecilik ve bilgisayarlarla ilgili dolandırıcılık,
- İçerikle ilgili olarak, çocuk pornografisi ile ilgili suçlar,
- Telif hakları ve benzer hakların ihlal edilmesiyle ilgili suçlar,

Sözleşmeye göre; suça iştirak, azmettirme ve yardım etme de siber suçlar kapsamında ele alınmaktadır. Konuya ilişkin her ülke, çeşitli cezai müeyyideler uygulamakta, kanunlarını buna uygun düzenlemektedir. Özellikle SCADA sistemler başta olmak üzere, siber uzay içindeki cihaz ve sistemlerin, fiziksel olarak etkilenmesine yönelik gerçekleştirilen siber saldırılar ile doğrudan fizilsel saldırılar da siber suç kapsamına girebilmektedir.

[38] http://www.istanbul.pol.tr/sibersuclarlamucadele/Sayfalar/Siber_Suclar.aspx, Erişim tarihi: 28 Aralık 2017.
[39] https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561, Erişim tarihi: 28 Aralık 2017.

Ne yazık ki günümüzde, Türk internet kullanıcısı siber uzay üzerinden gerçekleştirilen asayiş suçlarını da siber suç olarak nitelendirmektedir. Siber suç olmayan, internet üzerinden işlenen asayiş suçları şu şekildedir[40]:

- İntihara yönlendirme (TCK Madde 84)
- Cinsel taciz (TCK Madde 105)
- Tehdit (TCK Madde 106)
- Şantaj (TCK Madde 107)
- Hakaret (TCK Madde 125/2)
- Fuhuşa teşvik ya da aracılık (TCK Madde 227)
- Müstehcenlik (TCK Madde 226)

3.1.5. Siber Terörizm

Terör, kelime anlamı olarak Latince "terrere" kelimesinden türetilmiştir ve "korkutmak" anlamına gelmektedir. Terörle ilgili tanımlar farklılık göstermektedir. Bunun en büyük sebebi olarak, devletlerin, kendi çıkarları doğrultusunda terör unsurlarını kullanması gösterilebilir.

Kimi devlet için bir örgütün yaptığı faaliyetler terör faaliyetleri olarak nitelendirilmekteyken, kimine göreyse bu bir direniş ya da özgürlük hareketi olarak adlandırılabilmektedir. Ancak yine de terörün bilimsel tanımı yapılabilmektedir. Basitçe tanımlamak gerekirse terör, hukuk dışı güç kullanarak, amaca ulaşmak için yapılan her türlü eylemdir (Çakmak, 2008, s.29-30).

Terörizm "genellikle yasadışı örgütler tarafından güvensiz bir ortam oluşturma, rejimi zayıflatma ya da bir baskı sistemini başarısızlığa uğratma amacıyla gerçekleştirilen şiddet eylemleridir" (Winock, 2001, s.76). Bundan hareketle, siber terörizm ise siber uzay üzerinden, bilgisayar ağlarını ya da ağlara bağlı cihazları kullanılamaz hale getirmek ya da doğrudan bu sistemleri kullanmakta olan şahısları korkutmak veya zarar vermeye yönelik gerçekleştirilen terör faaliyetleridir. Bu

[40] http://www.asayis.pol.tr/Sayfalar/bilisim_suclari.aspx, 02 Ocak 2018.

noktada devreye kritik altyapılar girmektedir. Terör örgütlerinin hedefleri arasında yer alan kritik altyapılar, gerekli siber güvenlik önlemlerinin alınmaması halinde, saldırılara açık olmaktadır.

Bir terörist faaliyeti tanımlamak için genellikle geniş kitleler halindeki sivillere atılan bombalar, intihar saldırıları, silahla ateş, adam kaçırma gibi fiziksel şiddet içeren aktiviteler akla gelmektedir. Ancak terörizm, daha önce de yapılan tanımlarda olduğu gibi her zaman fiziksel bir şiddet içermek zorunda değildir. Halkı korkutmaya yönelik çalışmalar da terörizm kapsamına girmektedir. Wilkinson'a göre terörizm sistematik olarak kullanılan bir yöntemdir ve aşağıdaki karakteristik özelliklere sahiptir (Wilkinson, 2011, s.4):

- Önceden planlanmıştır/tasarlanmıştır ve şiddetli bir korku iklimi oluşturmaktadır,
- Etkilediği ilk kurbanlardan çok daha geniş bir hedef kitleye yönlenmiştir,
- Sivilleri de kapsayan, rastgele ya da sembolik hedefleri içermektedir,
- Birincil olarak hükümetlerin, toplulukların ya da belirli sosyal grupların siyasi davranışlarını etkilemek için kullanılmaktadır.

İnternet, doğası gereği kolay erişim, kaotik bir yapı, anonimlik ve uluslararası bir karakter olma imkanı sunduğu için, terör örgütlerinin de faaliyetlerini daha düşük bütçeyle yapmasını sağlamaktadır. İnternet üzerinden gerçekleştirilen terör faaliyetleri, geleneksel terör eylemlerine göre daha kolaydır. Terör örgütünün hedeflediği kitle sayısı ve çeşidi daha fazladır. Ayrıca siber terör faaliyetleri uzak bir mesafeden gerçekleştirilebilir ve tesiri de ışık hızındadır.

Diğer taraftan, özellikle son yıllarda sosyal medyanın gelişmesi ve kullanımının artmasıyla birlikte terör örgütlerinin gözü, sosyal medya kullanıcılarına çevrilmiştir. Teknolojiyi ve siber uzayı, propaganda yapmak amacıyla etkin bir şekilde kullanan

terör örgütleri, mevcut sosyal medya platformları dışında, kendi sosyal medya ağları ve uygulamalarını da geliştirmeye başlamıştır[41].

İnternet üzerinde faaliyet gerçekleştirmekte olan çok fazla terör örgütü bulunmaktadır. Bunladan bazıları Filistin Kurtuluş Örgütü (FKÖ), Filistin Halk Kurtuluş Cephesi (FHKC), Tupak-Amaru (MRTA), Bask Ayrılıkçı Hareketi (ETA), İrlanda Cumhuriyet (İRA), Aum Shinrikyo, Kolombiya Ulusal Kurtuluş Ordusu (ELN-Colombia), Tamil Elam Kurtuluş Kaplanları (LTTE), Devrimci Halk Kurtuluş Partisi- Cephesi (DHKP-C), Japon Kızıl Ordusu (JRA), Kürdistan İşçi Partisi (PKK), Zapasita Ulusal Kurtuluş Ordusu (EZLN), Özbekistan İslami Hareketi, Irak ve Şam İslam Devleti (IŞİD) gibi örgütlerdir. Coğrafi olarak bakıldığında, bu örgütlerin büyük bir çoğunun Ortadoğu'da konuşlandığı görülmektedir (Tsfati ve Weimann, 2002, s.320-321).

Siber uzayda, gerekli teknik faaliyetlerin gerçekleştirimesi halinde saldırıların ki ya da kimler tarafından yapıldığını tespit etmek neredeyse imkansızdır. Bu durum, terör örgütleri ve organize suç örgütlerinin ilgisini çekmektedir. İnternet üzerinden, özellikle sosyal medya kullanımı sayesinde propaganda, algı yönetimi, dezenformasyon ve manipülasyon gibi faaliyetlerde bulunarak, halkı korkutmak ya da infiale sürüklemek gibi eylemler gerçekleştirilebilmektedir.

Konuyla ilgili olarak IŞİD'in sosyal medyayı oldukça başarılı bir şekilde kullandığı, bu sayede de kendilerine çok fazla sempatizan kazandırdıkları ve hatta üye devşirdikleri ifade edilmektedir. Dahası, paylaştıkları şiddet içerikli videolarla, Batılı gençleri dahi kendilerine çekebilmişilerdir (Blaker, 2015, s.1).

Siber uzayın, kısa bir sürede milyonlarca kişiye ulaşılmasına imkan tanıması, kimlik tespitinin imkansızlaştırılmasını sağlayan yöntemler ve internette bulunan zafiyetler sebebiyle terör örgütleri günümüzde sosyal medya başta olmak üzere siber uzaydaki tüm ögeleri etkin bir şekilde kullanmaktadır. Bir başka terör örgütü El

[41] https://www.engadget.com/2017/05/04/isis-created-its-own-social-network-to-spread-propaganda, Erişim tarihi: 03 Ocak 2018.

Kaide'nin finansal kaynağının da internet kullanıcılarına ait kredi kartı bilgilerinin ele geçirilmesi faaliyetleri olduğu görülmüştür (Lormel, 2007, s.14).

Terör örgütleri kimi zaman da bir devletin kamu kurum ve kuruluşlarına karşı siber saldırılar düzenleyerek, çeşitli kişisel bilgi ve belgelerle birlikte, devlete ait önemli bilgilere de ulaşmayı hedefleyebilmektedir. Bununla ilgili olarak Diyarbakır'da yakalanmış olan, PKK terör örgütüne bilgi sağladığı mahkeme kararıyla tespit edilmiş bilgisayar korsanının, MİT, Genelkurmay Başkanlığı, Jandarma Genel Komutanlığı ve sair askeri birlikler ile emniyet müdürlüklerine ait bilgi ve yerleşim krokilerini sızdırması gösterilebilir[42].

Siber terörizm ve siber suç iki farklı kavram olup, genellikle karıştırılma potansiyeli bulunmaktadır. Her ikisi de benzer sistemler ve yöntemler üzerinden gerçekleştirilmiş olsa da aradaki farkı anlayabilmek için saiklerin motiflerine bakmak gerekmektedir. Yapılan siber eylemler, belli bir kişi ya da grubu hedef almaktaysa ve genellikle maddi çıkar elde etmek, ego, kendini ispat ya da intikam gibi duygulardan oluşmaktaysa, siber suç olarak nitelendirilmektedir.

Ancak eylem, daha geniş kitleleri kapsıyor ve halkı korkuya sürükleyecek, geleneksel terör eylemlerinin, siber uzaydaki izdüşümü şeklinde nitelendirilecek bir yapıya sahipse, eylemi gerçekleştirenlerin motifleri, bölücü ve yıkıcı ideolojilere dayanıyorsa, bu durumda siber terör tanımı yapmak daha uygun olabilmektedir.

3.1.6. Siber İstihbarat

Siber istihbarat, öneminin artmasıyla birlikte özellikle son dönemde sıkça adından söz edilen bir istihbarat disiplinidir. Siber istihbarat, hem bir haber toplama yöntemi hem de bir disiplindir. Dolayısıyla siber istihbaratın tanımını yaparken dikkat etmek gerekmektedir. Günümüzde birçok siber güvenlik firması, siber istihbarat ile siber tehdit istihbaratı kavramlarını karıştırmaktadır. Geliştirmekte oldukları yazılım, sundukları çözümleri siber istihbarat çatısı altında değerlendirmektedir. Siber

[42] http://www.hurriyet.com.tr/pkknin-en-onemli-hackeri-yakalandi-10393202, Erişim tarihi: 04 Ocak 2018.

istihbaratın anlaşılabilmesi için sibernetik ve siber uzay gibi kavramları bilmek gerekmektedir. Bu kavramlara ayrıntılı bir şekilde bu bölümde değinilmektedir. Siber İstihbarat, siber uzay üzerinden istihbarat oluşturma faaliyetleridir. Bu faaliyetler hedef sistemlere izinsiz erişim sağlayarak, casusluk faaliyetleri yürütmek şeklinde olabileceği gibi, siber uzaydaki açık kaynakları kullanarak istihbarat oluşturmak şeklinde de gerçekleşebilmektedir. Siber istihbarat oluşturmak için, sosyal mühendislik, psikolojik savaş ve diğer ögeler kullanılabilmektedir.

İstihbarat teşkilatı için çalışan, hedef örgütte görevli kişilerin, fiziksel olarak sisteme girmesi, truva atı, casus yazılım, virüs vb. zararlı yazılımları sızdırması ya da hassas verilerin bulunduğu dizüstü bilgisayar, harici disk, sabit disk vb. depolama alanlarını izinsiz ele geçirmesi de siber istihbarat faaliyetleri arasında değerlendirilebilmektedir. Siber uzay, "tradecraft" olarak adlandırılan, istihbarat yöntemlerinin farklı şekillerde kullanılabileceği bir alan haline gelmiştir. İnternetin, yabancı devletler ve potansiyel düşmanlar için hızla gelişmekte olan bir istihbarat toplama alanı olduğu ifade edilmektedir (Wettering, 2001, s.342).

Hedef devletin kurumlarında yer alan veri tabanlarındaki bilgilerin, hacking yöntemleri sayesinde elde edilmesi mümkün olmaktadır. Gerekli önlemlerin alınmaması halinde, siber uzay üzerinden hassas bilgileri ele geçirmek, bunları istihbari amaçla kullanmak ve oluşturulan istihbaratı karar alıcılara iletmek, geleneksel istihbarat yöntemlerine göre daha hızlıdır ve daha az bütçe gerektirmektedir. Bugün, siber uzayda yer alan her cihaz, istihbarat teşkilatları için potansiyel birer hedeftir.

Ayrıca Internet başta olmak üzere, sibernetik içindeki ağlara bağlı kullanıcının nerede olduğu, kiminle görüştüğü, ne konuştuğu, arkadaşları ve akrabalarının kimler olduğu, siyasi görüşü, dini inancı vb. bilgi elde etmek mümkündür. Siber istihbarat faaliyetleri, sadece bilgi elde etmek amacıyla yapılmamaktadır. Bir ülkenin e-devlet altyapılarının hizmet dışı bırakılması, kurumlarına ait web sitelerinin erişilemez hale getirilmesi, e-ticaret siteleri ya da bankacılık altyapılarına saldırı gerçekleştirerek ekonomik zarar vermek gibi faaliyetler de siber istihbarat kapsamında yer almaktadır.

3.1.7. Siber Savaş

Harbin kara, deniz, hava ve uzaydan sonra beşinci boyutu olarak adlandırılan siber uzay, sadece bilgi paylaşımının yapıldığı bir alan olmaktan çıkmıştır. Dahası geleneksel savaşlarla paralel olarak operasyonların düzenlendiği ve hatta tamamen bağımsız olarak savaşların yapıldığı bir alan haline gelmiştir. İsrail Eski Başbakanı Benjamin Netanyahu'nun Siber Güvenlik danışmanı Itzhak Ben-Israel, yaptığı bir açıklamada "Siber Savaşlar konvansiyonel savaşlardaki gibi bir etki verebilecek türdedir. Bir ülkeyi vurmak istiyorsanız, o ülkenin enerji ve su kaynaklarına karşı siber saldırılar düzenlemek gerekmektedir. Siber teknoloji bunu tek mermi kullanmadan yapabilme yeteneğine sahiptir." demiştir[43].

Daha önceleri önem arz eden "toprak", iş gücü" ve "sermaye" gibi üretim faktörlerinin yerini artık daha değerli olarak "bilgi" almıştır. Bilişim teknolojilerinin sağladığı imkan ve kolaylıklardan ziyade siber suçlar, siber saldırılar ve siber savaş gibi konular konuşulur olmuştur. Tüm bu gelişmeler ışığında bilgi ve iletişim sistemlerinin ve yapılarının siber saldırılara karşı korunmasının, yani siber güvenliğin sağlanmasının yolları aranır olmuştur (Şenol, 2016, s.10-17).

Siber Savaş, bir devletin başka bir devlete ait siber uzayda yer alan varlıklarına zarar vermek, manipüle etmek, çıkarları çerçevesinde kullanmak, kesinti yaratmak veya tamamen hizmet veremez duruma getirmek üzere gerçekleştirilen saldırı faaliyetlerinin tümüdür. Siber savaşta çok fazla sayıda yöntem kullanarak, hedefe kimi durumda fiziksel hasar dahi verilebilmektedir (Keleştemur, 2015, s.120-133).

Siber Savaş, dünyadaki tüm bilgisayar ve birbiriyle bağlantı kurabilen cihazlarıla bunların kontrol ettiği tüm ögeleri kapsayan siber uzay üzerinden gerçekleşmektedir. Siber uzay, sadece Internet'ten ibaret değildir. Internet'teki herhangi bir ağdan, Internet'e bağlı başka ağlardan herhangi birinde bulunan bir bilgisayarla iletişim kurulabilmektedir. Siber savaş, Internet artı Internet'ten girilemeyen bir sürü başka bilgisayar ağının bulduğu oldukça geniş bir alanda yapılmaktadır (Clarke ve Knake,

[43] http://www.timesofisrael.com/israel-fights-off-1000-cyber-attack-hits-a-minute, Erişim Tarihi: 04 Ocak 2018.

2011, s.44). Konvensiyonel Savaş ile Siber Savaş arasındaki temel farklar Tablo 4'te ayrıntılı bir şekilde verilmiştir.

Tablo 4: Konvansiyonel Savaş ve Siber Savaş Arasındaki Farklar

	Konvansiyonel Savaş	**Siber Savaş**
Saldırının Kaynağı	Saldırı kaynağının bulunması, teknoloji sayesinde kolaydır.	Saldırının nereden geldiğini tespit etmek zordur. Kimi zaman da ispat edilememektedir.
Hızı	Kullanılmakta olan uçak, tank, gemi, füze vb. ögelerin hızı kadardır.	İnternet hızındadır
Etkisi	Fiziksel alanda etkisi büyüktür.	Genellikle bilgi ve iletişim sistemlerinde etkilidir. Ancak nükleer santraller vb. fiziksel etki de yaratabilmektedir.
Savaşçıları	İki veya daha fazla ülkenin orduları savaşmaktadır.	Tek bir kişi, bir grup, bir örgüt ya da devlet savaşmaktadır.
Maliyeti	Kullanılan askeri silahların maliyetine bağlıdır ve genellikle oldukça pahalıdır.	Kimi zaman tek bir bilgisayar ile etkili olunabilmektedir. Maliyeti ucuzdur.
Silahları	Füze, bomba, top tabanca, tüfek, tank, uçak, gemi, radar vb.	Bilgisayarlar, çipler, yazılımlar, donanımlar.
Teknolojisi	İleri – askeri harp teknolojileri.	Yüksek teknoloji ve bilgi ihtiyacı bulunmaktadır.
Saldırı Belirtileri	Saldırının farkına, intikal ve saldırı sırsaında varılmaktadır.	Saldırının farkına varılmayabilir.
Hasarın Tespiti	Etkiler fiziksel olduğundan dolayı, daha kolay bir şekilde hasar tespiti yapılmaktadır.	Fiziksel bir tahribat olmadığı sürece, nerede hasar olduğunu tesit etmek çok zor; kimi zaman imkansızdır.

Kaynak: Çifci, 2013, s.20.

3.2. Siber Savaştaki Kritik Altyapılar

Siber savaş artık çok daha güçlü etkiler yaratabilecek seviyededir. Bu anlamda, konuyla ilgili olarak her devletin gerekli aksiyonu harekete geçirmesi gerekmektedir. Yakın bir geçmişe kadar fidye yazılımlar küçük çapta özel kurumları etkilemekteyken, bugün devlet çapında ekonomik zararlar verebilmektedir. WannaCry isimli fidye yazılımın, İngiltere'deki hastanelerin altyapılarını vurması ve hastanelerin bir süre yeterli hizmeti verememesi bu duruma örnek gösterilebilir[44].

Dünya üzerinde yaşanan herhangi bir siber saldırı, yine WannaCry örneğinde olduğu gibi birden fazla ülkeyi aynı anda etkisi altına alabilmektedir. Bu da siber savaşın, küresel olma özelliğini ortaya çıkarmaktadır. Kritik altyapılara yapılacak saldırılar sonucunda, sadece devletler değil, siviller de olumsuz etkilenebilmektedir. Dolayısıyla kritik altyapıların etkin bir şekilde korunması çok önemlidir. Avrupa Birliği ve ABD'nin en önemli 10 kritik altyapı listeleri Tablo 5'teki gibidir.

Tablo 5: AB ve ABD İçin En Önemli 10 Kritik Altyapı

Avrupa Birliği	**Amerika Birleşik Devletleri**
Su	Su
Gıda	Enerji
Sağlık	Ulaşım
Enerji	Tarım ve Gıda
Finans	Kolluk Hizmetleri
Ulaşım	Bilgi ve İletişim
Sivil Yönetim	Bankacılık ve Finans
Uzay Araştırmaları	Bayındırlık Hizmetleri
Kimyasal ve Nükleer Endüstri	Federal ve Yerel Hizmetler
Kamu Düzeni ve Güvenlik Alanı	Acil Hizmetler

Kaynak: Keleştemur, 2015, s.137.

[44] https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin, Erişim Tarihi: 05 Ocak 2018.

Bugün, özellikle internetin tüm dünyaya yayılmasıyla birlikte, siber savaş da küreselleşmiş durumdadır. Dünya üzerinde yaşanan herhangi bir siber saldırı, diğer ülkeleri de etkilemektedir. Bu da siber savaşın, küresel bir hale gelmesine sebep olmaktadır. Kritik altyapılara yapılacak saldırılar neticesinde, sadece devletler değil, siviller de olumsuz etkilenebilmektedir. Dolayısıyla kritik altyapıların efektif bir şekilde korunması büyük bir önem arz etmektedir.

Tablo 6: Siber Suç, Siber Terör ve Siber Savaşın Temel Özellikleri

	Siber Suç	**Siber Terör**	**Siber Savaş**
Niteliği	Doğrudan	Sembolik	- Doğrudan - Sembolik
Şiddeti	Az yoğun	Yoğun	En yoğun
Motivasyonu	Kişisel kazanç	Siyasi	- Siyasi - Doğrudan savaş kabiliyetini azaltmak - Casusluk
Failleri	- Bireyler Organize suç örgütleri - Anonim	- Terörist örgütler - Hangi örgüt olduğu tahmin edilebilir	Failin kim olduğu tam olarak bilinmese de kaynaklandığı devletler bilinir
Hedefleri	Kazanç sağlanacak hedefler	- Kritik tesisler - Güvenlik birimleri - Hükümet temsilcilikleri	- Kritik tesisler Ekonimik ve endüstriyel altyapılar - Güvenlik birimleri - Hükümet temsilcilikleri - Askeri altyapılar
Kaynağı	Ülke içinden ya da dışından	Ülke içinden ya da dışından	Ülke dışından

Siber suç, siber terör ve siber savaş kavramları incelendiğinde, temel özelliklerinin yukarıda yer alan tablodaki gibi olduğu görülmektedir. Bu tabloda yer alan kavramlara ait siber saldırı yöntemleri ve kullanılan teknolojiler, genel olarak aynı olup, motivasyon farkı ve etki alanı gibi ögeler sebebiyle farklı isimler almaktadır. Saldırı yöntemleri ve teknolojilerin aynı olması, uygulanması gereken savunma yöntemlerinin de standartlaşmasına imkan tanımaktadır.

3.3. Ülkelerin Siber Savaş Kapasiteleri

Bir ülkenin savaşma kapasitesi, sahip olduğu asker sayısı, askerlerin askeri eğitim düzeyi, askeri sistem ve silahlarının gücü, bu sistem ve silahların savaş ve barış ortamlarında üretilebilme, kullanılabilme kabiliyetleri ile birlikte milli güç unsurları (teknoloji, ekonomi, sosyal durum, nüfus, coğrafya, politika) vb. kriterlerle ölçülmektedir. Burada bir diğer önemli unsur da milli duygular ve milli menfaatlerdir. Siber savaş kapasitesini ölçmek içinse farklı kriterler devreye girmektedir. Bu kriterler de devlet kurumları ve özel kurumlar olmak üzere ikiye ayrılmaktadır.

Siber savaş kapasitesini belirlerken, ülkenin teknolojik altyapısının genişliği, aynı zamanda saldırıya karşı da büyük bir hedef olduğu anlamına gelmektedir. Dolayısıyla internet teknolojilerinin ve altyapının gelişmiş olması, kimi zaman ters yönde bir etki yaratabilmektedir. Siber savaş gücünün saldırıdan ziyade, savunma gücü olduğu burada tekrar ön plana çıkmaktadır.

3.4. Olası Siber Savaş Senaryoları

Siber savaş, tek bir yöntemle değil, birden fazla unsur kullanılarak gerçekleştirilmektedir. Bir siber savaş esnasında aşağıdaki gibi durumlar meydana gelebilmektedir:

- Bir ülkeye ait tüm vatandaşların bilgileri ele geçirilebilir, değiştirilebilir, silinebilir veya e-devlet sistemleri çökebilir,

- Devlete ait önem arz eden tüm bilgilerin saklandığı sunuculara sızılabilir, bu belgeler yabancı devlet veya örgütlerin eline geçebilir,

- Nükleer tesislerde, petrol ve doğalgaz hatlarında sorun çıkabilir, dahası bu tesisler patlatılabilir,

■ Tüm elektronik bankacılık hizmetleri durdurulabilir, ekonomiye zarar verilebilir,

■ Banka hesaplarından yurt dışına para transferi yapılabilir,

■ Metro, tren ve kara trafik sinyalizasyon sistemlerinin çökertilmesiyle, trafikte tıkanmalar ve kazalar meydana gelebilir,

■ Tüm elektrik şebekesi durdurulabilir, ülkede elektrikle çalışan hiçbir makine yahut alet kullanılamaz hale gelebilir,

■ Hastane sistemleri ele geçirilebilir, sağlık hizmetleri durdurulabilir,

■ Uydu sistemleri ele geçirilebilir ve meteoroloji, seyrüsefer, iletişim uyduları ve diğer uydular düşürülebilir ya da yörünlerinden saptırılıp kullanılamaz hale getirilebilir,

■ Bir ülkenin internet hizmetleri tamamen durdurulabilir,

■ Su ve baraj sistemlerine zarar verilebilir, baraj kapakları açılarak yaşamsal zararlar verilebilir.

Siber savaş artık yadırganamayacak kadar büyük öneme sahiptir ve bugüne kadar olanlardan çok daha kötü senaryolarla karşılaşılması mümkündür. Bir başka deyişle, eğer ülkeler yeterli önlem almazlarsa, devasa büyüklükte siber saldırılara maruz kalabilir, hatta yıkılışlarına tanıklık edebilirler.

3.5. Yaşanmış Siber Savaş Olayları

Bu başlığın alt başlıklarında; Siber İstihbaratın kamu güvenliği için ne kadar önemli olduğuna vurgulamaya yönelik, Solar Sunrise, Çin Büyükelçiliği'nin Bombalanması, Hainan Adası Olayı, Titan Rain, İsrail Sitelerine Saldırı, Körfez Savaşı, Estonya Siber Savaşı, Operation Orchard, Gürcistan'ın Güney Osetya Saldırısı, Conficker, Cast Lead Harekatı, Operation Aurora, Ghostnet, Stuxnet, Night Dragon ve WikiLeaks vakaları anlatılmaya çalışılacaktır.

3.5.1. Solar Sunrise

Siber Savaş ifadesinin ilk kez kullanılmasına sebep olan Solar Sunrise, 1998 yılında ABD Savunma Bakanlığı'nın ağına yapılan saldırıların tespit edilmesiyle birlikte ortaya çıkmıştır. Saldırılar Pentagon'dan sonra ABD Hava Kuvvetleri

Komutanlığı ile Deniz Kuvvetleri Komutanlığı'na sıçramıştır. Yaklaşık 24 saat süren acil durum çağrısının ardından gerekli müdahaleler yapılmış ve saldırılar kontrol altına alınabilmiştir[45].

İlk önceleri saldırıyı yapanların yabancı devletler ya da terör örgütleri olduğu düşünülse de yapılan araştırmalar sonucu faillerin, Kaliforniya'da yaşamakta olan iki genç olduğu ortaya çıkmıştır. Bu olayın atlatılmasından kısa bir süre sonra Rusya tarafından seri saldırılar düzenlenmeye başlanmıştır. Her ne kadar, bu saldırıları Rus hükümeti kabul etmese de ABD gizli servisleri tarafından yapılan araştırmalar, tüm saldırıların tek bir noktadan, Rusya'dan meydana geldiğini ortaya koymuştur. Saldırılar, ABD'nin Irak'a müdahale yapacağına ilişkin haberlerin yayılmasıyla birlikte şiddetlenmiştir.

3.5.2. Çin Büyükelçiliği'nin Bombalanması ve Hainan Adası Olayı

Çin'in uydu üzerinden Belgrad'a NATO operasyonu hakkında bilgi aktardığı iddia edildiği sıralarda, NATO'ya ait jetlerin Belgrad'daki Çin büyük elçiliğini yanlışlıkla bombalaması kuşku ile karşılanmıştır. Mayıs 1999'da gerçekleşen bombalama olayı sonucu 4 kişinin yaşamını yitirdiği, en az 20 kişinin yaralandığı, 2 kişinin de kaybolduğu açıklanmıştır. Olayın ardından Çin Kızıl Korsanlar Birliği, ABD devlet sitelerine saldırılar düzenlemiş, bu saldırılar karşısında ABD'nin birçok kurum sitesi hizmet veremez hale getirilmiştir.

ABD ile Çin arasındaki gerginliğin yükseldiği dönemde, 1 Nisan 2001 tarihinde bir Çin savaş uçağı ile ABD casus uçağı Güney Çin Denizi üzerinde çarpışmıştır. Çarpışmanın ardından Çin uçağı düşmüş, ABD uçağı da ağır hasar almış ve Hainan Adası'na zorunlu iniş yapmıştır. Olayın ardından 80.000'in üzerinde bilgisayar korsanı ABD'ye siber saldırı düzenlemiştir. Bunun üzerine ABD menşeli gazeteler World Wide Web War I gibi başlıklar atarak, artık siber savaş dönemine geçildiğini ifade etmişlerdir (Keleştemur, 2015, s.141).

[45] https://www.globalsecurity.org/military/ops/solar-sunrise.htm

3.5.3. Titan Rain ve İsrail Sitelerine Saldırı

2002 yılından itibaren artık Çin de siber saldırılara başlamış, adeta yağmur gibi yağmaya başlayan bu saldırılar sonucu siber istihbarat kavramı ortaya çıkmıştır. Bu olayın ardından Advance Persistent Threat (APT) yani Gelişmiş Kalıcı Tehdit terimi de ortaya çıkmıştır. Titan Yağmuru vakası sonucu NASA ile birlikte ABD askeri kurum ve firmalarına ait bilgisayarlara siber saldırılar düzenlenmiş ve bu sayede 10 ile 20 TB arasında gizli dosya ele geçirilmiştir. Saldırılar üç sene boyunca devam etmiştir. Yapılan araştırmalar, saldırıların Çin'in Guangdong şehrinden geldiğini, çalınan bilgilerin Güney Kore, Hong Kong ve Tayvan üzerinden Çin'e ulaştığını göstermektedir (Çifci, 2013, s.164).

Eylül 2000'de Filistin'de ikinci başkaldırış meydana gelmiş, İsrail yönetimi 6 Kasım 2000 tarihinde üç İsrail askerinin Hizbullah tarafından kaçırılmasının ardından, Hizbullah ve Hamas'ın İnternet sitelerine yoğun bir şekilde DDoS saldırıları düzenlemiştir. Bu saldırılara cevap olarak Filistin sempatizanı bilgisayar korsanları da İsrail savunma güçleri ile birlikte Dışişleri Bakanlığı, Tel Aviv Borsası ve Merkez Bankası'nın web sitelerine yönelik saldırılarda bulunmuştur.

Yine aynı şekilde 2008'in Aralık ayında Gazze ablukası sırasında binin üzerinde sivilin hayatını kaybetmesinin ardından, İsrail sitelerine yönelik saldırılar düzenlenmiş ve 10 binin üzerinde web sitesi ya içerik değişikliğine uğramış, ya da erişim dışı bırakılmıştır (Keleştemur, 2015, s.143).

3.5.4. Körfez Savaşı ve Estonya Siber Savaşı

2003 yılında ABD'nin Irak'ı işgal etmesinden önce, siber ordu tarafından Irak'ın kapalı devre bilgisayar ağına sızdığı ve Irak Savunma Bakanlığı e-posta sistemi üzerinden Iraklı subaylara, savaşa girmeden teslim olmaları için çeşitli e-posta mesajları gönderdiği ifade edilmektedir. Bu e-postaları alan birçok Iraklı subayın silah bırakarak, savaştan çekildiği de öne sürülmektedir. Siber savaşın, konvansiyonel savaş ile birlikte kullanıldığı ilk savaş olarak nitelendirilen Körfez Savaşı, yapılan siber saldırılar sonucunda Irak askeri birliklerinin zayıflatılmasıyla birlikte ABD'nin zaferiyle sonlanmıştır. 2007 yılına gelindiğindeyse Rus hükümetiyle bağlantısı olduğu

tahmin edilen bir hacker grubunun Estonya parlemanto web sitesi, bankalar, bakanlıklar, gazeteler ve birçok yayın kuruluşunun resmi sitelerini hacklediği haberleri tüm dünyada geniş yankı uyandırmıştır.

Estonya hükümeti bu durum karşısında çaresiz kalmış, NATO'yu gerekli müdahalenin yapılması hususunda göreve çağırmıştır. Bu olaydan tam bir sene sonra aynı durum, Gürcistan'ın başına gelmiştir. Gözler yine Rusya'ya çevrilmiş ancak yine herhangi bir kanıt sunulamadığı için saldırıların Rusya'dan geldiği ile ilgili haberler iddiadan öteye gidememiştir.

Estonya Siber Savaşı olarak da bilinen bu olayın temeli ise aslında İkinci Dünya Savaşı'na kadar dayanmaktadır. İkinci Dünya Savaşı sırasında Estonya, Sovyetler Birliği ile birlikte Almanya'ya karşı savaşmış, savaşın sona ermesiyle birlikte de Bronz Asker Anıtı dikilmiştir. Bu heykel, Estonya'nın Nazi istilasından korunması amacıyla, Sovyetler Birliği'nin verdiği kahramanca mücadeleyi sembolize etmektedir.

26 Nisan 2007'de Estonya, Kızıl Ordu Anıtı'nı yerinden kaldırmak istemiş, bu durum karşısında Rusya, ertesi gün bu kararı kınamıştır. Ülkede çeşitli ayaklanmalar yayınlanmış ve Rusya yanlısı gösteriler yapılmaya başlanmıştır. Özellikle başkent Tallin'deki ayaklanmalar oldukça büyük boyutlara ulaşmış ve 27-29 Nisan 2007 tarihinde devletin internet sitelerinin ele geçirilmesi sebebiyle ulusal bilgi sistemleri çökmüş, internet hizmet sağlayıcıları ve bankalara büyük zarar verilmiştir (Çifci, 2013, s.165-166).

3.5.5. Operation Orchyard ve Gürcistan'ın Güney Osetya Saldırısı

6 Eylül 2007'de Suriye topraklarında, nükleer silah geliştirdiği iddiası ile şüpheli bir tesis, gece saatlerinde İsrail savaş uçakları tarafından imha edilmiştir. "Operation Orchard" olarak adlandırılan operasyon, siber saldırılar sonucunda hava savunma sistemlerine sızılması ile birlikte çok daha etkili sonuçlar vermiştir. Uçakların radarlara yakalanmadan saldırıyı gerçekleştirebilmesi üzerine ortaya çıkan iddialar şu şekildedir:

■ İsrail, Suriye hava savunma sisteminin üzerine bir İHA göndermiş, özel boya kullanarak İHA'nın radara yakalanmasını engellemiştir.

■ Suriye'nin kullandığı Rus yapımı sistemlerde kullanılan bilgisayar programlarına, İsrail adına çalışan bir ajan tarafından truva atı yüklenmiş, böylelikle sisteme uzaktan erişilerek gerekli önlemler alınmıştır.

■ İsrail ajanları, Suriye'deki fiber optik kabloları kesmiş ve hava savunma sistemine kendi kablosunu saplamıştır (Çifci, 2013, s.167).

Takvimler bu kez 8 Ağustos 2008'i gösterdiğinde, Gürcü kuvvetler, Güney Osetya topraklarına operasyon düzenlemişti. Rusya bu olay karşısında harekete geçmiş ve 11 Ağustos 2008 tarihinde Gürcistan'a savaş açmıştı. Aslında bu savaşın başlamasından hemen önce siber saldırılar düzenlenmeye başlanmış, Gürcistan Devlet Başkanı Mihail Saakaşvili'nin internet sitesi ele geçirilmişti.

Bu saldırıların başını çeken DDoS saldırıları gittikçe popülerleşmeye başlamıştır. Bu saldırılar fiziksel bir zarar vermemesine rağmen, Gürcistan hükümetinin zayıf düşmesine sebep olmuştur. Özellikle birçok web sitesi üzerinden yapılan yayınlar sayesinde, Rusya'nın Gürcistan ile mücadelesinde haklı olduğu dünya kamuoyuna psikolojik bir harekat sayesinde empoze edilmiştir (Keleştemur, 2015, s.144).

3.5.6. Conficker ve Cast Lead Harekatı

Microsoft işletim sistemlerini hedef alan Conficker isimli solucan ilk olarak Kasım 2008 yılında tespit edilmiştir. Solucan, Windows işletim sistemlerindeki zafiyetleri kullanarak yönetici hesabına "sözlük saldırılar" düzenlemeye imkan kılmıştır.

Hızlı bir şekilde diğer bilgisayarlara da bulaşan solucan, kısa bir süre içinde dünya genelinde milyonlarca bilgisayara bulaşmıştır. Solucan, sadece askeri ve devlete ait bilgisayarları değil, ev kullanıcılarını da etkilemiştir. Solucanın Atatürk Havalimanı'ndaki bilgisayarlara bulaşmasıyla birlikte 30 Ocak 2009 tarihinde bilet ve bagaj işlemleri elle yapılmıştır.

2008'in Aralık ayının sonlarına doğru İsrail, Gazze Savaşı sırasında Filistin'e "Cast Lead" isimli bir harekat başlatmıştır. İsrail savunma güçleri, Hamas'a ait Al Aqsa kanalını hacklemesinin ardından, Hamas liderinin öldürüldüğünü gösteren Arapça "Zaman Tükeniyor" isimli bir çizgi film yayınlamış, bu olayın ardından Filistinli siber korsanlar İsrail'e ait birçok web sitesine saldırmıştır. Ele geçirilen web sitelerinin büyük bir kısmında İsrail aleyhine yazılar ve görseller yayınlanmıştır (Keleştemur, 2015, s.145).

3.5.7. Operation Aurora ve GhostNet

2009 yılında yaşanan Operation Aurora hadisesi, bir anda Siber Savaş'ın sadece ülkeler arasında değil, aynı zamanda firmalar arasında olduğunu da gözler önüne sermiştir. Aralarında Google gibi internet devlerinin de bulunduğu toplam 34 teknoloji firması saldırılara maruz kalmıştır. Saldırıların Çin menşeli olduğu ve Microsoft'un web tarayıcısı Internet Explorer'da bulunan ve antivirüs yazılımları tarafından tespit edilemeyen, sıfırınca gün (zero day) açığı sayesinde gerçekleşmiş olduğu ortaya çıkmıştır. Saldırganlar, firmaların ağlarına sızmış, çeşitli hassas bilgileri ele geçirmiştir[46].

Aynı yıl ortaya çıkan bir diğer önemli siber saldırı da GhostNet'dir. Özellikle büyükelçilikler, dışişleri bakanlıkları gibi devletler arası ilişkilerin yönetildiği makamların hedef alındığı bu operasyonda dünyanın 103 ülkesi saldırıya uğramıştır. Yine saldırı merkezinin Çin olduğu yaklaşık 10 aylık bir çalışma sonucunda tespit edilmiştir. Faaliyetlerin Çin üzerinden gerçekleşmiş olmasına rağmen, Çin hükümeti bu saldırıların yürütüldüğünden haberdar olmadığını belirtmiş, suçlamaları reddetmiştir (Keleştemur, 2015, s.146).

3.5.8. Stuxnet ve Night Dragon

Dünyayı sarsan en büyük siber istihbarat operasyonlarından biri de Stuxnet'dir. İran'ın nükleer projelerini tamamen alt üst eden bu solucan, neredeyse ABD ve İran arasında savaşın çıkmasına sebep olmuştur. Aslında basit gibi görünen, ancak

[46] https://www.wired.com/2010/01/operation-aurora, Erişim Tarihi: 08 Ocak 2018.

karmaşık kodlardan oluşan solucan sayesinde, ABD büyük bir bütçe ayırmaya gerek kalmadan ve askerlerlerini riske atmadan, İran hükümetine ve projelerine maddi anlamda büyük zarar vermiştir. Dünya basını Stuxnet'in İran'ın Buşehr ve Natanz nükleer tesislerini etkilediğini ileri sürmüştür; ancak İran açıklama yaparak sadece nükleer tesis çalışanlarına ait bilgisayarların etkilendiğini belirtmiştir.

2011 yılına gelindiğinde ise iki büyük saldırı daha gerçekleşmiştir. Bunlardan birincisi Night Dragon adı verilen enerji raporunun sızdırılmasına yöneliktir. Bu rapor, Çin'in casusluk çalışmaları sayesinde enerji piyasasında üstünlük sağlama planlarını ortaya koymuştur. İkinci saldırı ise RSA saldırısı olarak adını duyurmuştur.

Bu saldırı sayesinde istenilen bilgiler elde edildikten sonra, hiçbir şey olmamış gibi yeniden aynı verileri, eski hallerine geri getirmek mümkün kılınmıştır. Böylelikle, ABD'nin internet alt yapısını kullanan tüm verilere ulaşmak, hepsine zarar vermek basit bir işlem haline gelmiştir. Kısa süreli bir çalışmanın ardından ABD'li siber güvenlik uzmanları tüm açıkları kapatarak bu saldırıyı savuşturabilmiştir (Keleştemur, 2015, s.147).

3.5.9. Wikileaks Vakası

Amerikan büyükelçilikleri tarafından 1968-2010 yılları arasında yapılan yaklaşık 250.000 yazışmanın internete sızdırılması ve bunun duyurulmasını engellemek için Wikileaks sitesine karşı DDoS saldırıları düzenlenmiştir. Bu saldırılarla birlikte gündem bir anda değişmiş, çeşitli hacking grupları desteklerini duyurmuştur. Anonymous adlı haktivist grup ise Wikileaks'e destek vermek amacıyla Mastercard, Paypal, Visa ve çeşitli devlet kurumlarının sitelerini hedef alan, karşı bir saldırı başlattığını açıklamıştır. Anonymous, gönüllü olarak herkesin bu saldırıları desteklemesini istemiştir.

Anonymous'un internette örgütlenerek protesto amaçlı olarak devlet kurumlarını, ticari firmaları hedef almasından hemen sonra ortaya çıkan LulzSec adlı bilgisayar korsanlığı grubu da şirketler ve ülkelerin önemli kurumlarına saldırı düzenlemiştir. "Halk ya da tüketiciler aleyhine çalışmalar yaptığı" iddiasıyla birçok saldırı

düzenleyen LulzSec de bugüne kadar Sony, Nintendo ve Fox gibi önemli şirketlerin sistemlerini hacklemiş ve verilerini yayınlamıştır.[47]

3.6. Siber Silahlar

Savunma ya da saldırı amaçlı kullanılan her türlü araca silah denilmektedir[48]. Burada önemli olan, kullanılan silahın üretim amacının ne olduğu değil, hangi maksatla kullanıldığıdır. Bir çekiç, çivi çakmak ya da madenleri dövmek gibi işler için üretilen bir aletken, kimi zaman saldırı amacıyla da kullanılabilmektedir. Dolayısıyla çekiç burada bir iş aleti olmak yerine silaha dönüşmüştür.

Bir başka deyişle silah; yapıları, sistemleri ya da canlıları tehdit etmek ve/veya fiziksel, fonksiyonel ya da mental zarar vermek için tasarlanmış ya da kullanılmakta olan aletlerdir. Bundan hareketle, siber silahlar için "siber uzayda, saldırı ya da savunma saikleriyle kullanılmakta olan yazılım ve donanımlardır" ifadesi kullanılabilmektedir.

Siber silahları düşük potanesiyelli ve yüksek potansiyelli olmak üzere iki farklı gruba ayırmak mümkündür. Düşük potansiyelli siber silahlar, bir sisteme teknik olarak doğrudan zarar verme yeteneği olmayan, ancak dolaylı yollardan sızması halinde etkileşimde bulunarak amaca yönelik faaliyetlerde bulunan yazılımlardır. Yüksek potansiyelli siber silahlar ise bir istihbarat görevlisi gibi, korunaklı ve hatta fiziksel olarak izole sistemlere dahi sızabilen ve doğrudan bu sistemler üzerinde istihbarat faaliyetlerinde bulunabilen yazılımlardır (Rid ve McBurney, 2012, s.8).

Düşük potansiyelli siber silahlara CryptoLocker, WannaCry, Petya ya da çok daha eski olan ILOVEYOU gibi zararlı yazılımlar örnek gösterilebilir. Zira bu yazılımlar, kullanıcı hatası ya da protokoldeki bir açıktan dolayı aktifleşmektedir. Diğer taraftan Stuxnet, Duqu, Gauss ve Flame gibi yazılımlar ise yüksek potansiyelli siber silahlara örnek teşkil etmektedir ve doğrudan belli bir amaç ve hedefe yönelik olarak

[47] https://www.theatlantic.com/technology/archive/2011/09/lulzsecs-sony-hack-really-was-simple-it-claimed/335527/, Erişim tarihi: 09 Ocak 2018.
[48] http://www.tdk.gov.tr/index.php?option=com_gts&kelime=SİLAH, Erişim Tarihi: 09 Ocak 2018.

geliştirilmiştir. Bugün, siber silah olarak kullanılabilen zararlı yazılım türlerinden bazıları aşağıda açıklanmaktadır.

3.6.1. Virüs

Bilgisayar virüsleri çalışma prensibi olarak biyolojik virüslere benzemektedir. Sisteme sızdıktan sonra çalışmaya başlayan virüsler, geliştirilme biçimine göre farklılık gösterse de temel olarak sistemi kullanılamaz hale getirmektedir. Virüsler, mevcut sistem içerisinde kendini çoğaltabildiği için, ev sahibini taşıyıcı olarak da kullanabilmektedir.

Genellikle, içine gizlendiği programın çalıştırılması ya da sistem içerisindeki bir aksiyonun devreye girmesi sonucu çalışmaya ve yayılmaya başlamaktadır. Kimi virüs, kendini kopyalamak için internet ve yerel ağları kullanabileceği gibi, kimisi USB diskler, CD ve DVD'ler gibi depolama medya ve aygıtlarını kullanmaktadır.

Virüsler genellikle uygulama dosyaları olarak karşımıza çıkmaktadır. Bazı virüsler çalışmak için, kullanıcı tarafından çalıştırılarak tetiklenmek ihtiyacında olabileceği gibi, bazı virüslerse doğrudan sisteme kendini tetikletebilmektedir. Virüslerin ne kadar tehlikeli bir silah olabileceği, kendisini geliştirmekte olan yazılımcının niyetine ve zekasına bağlıdır.

Bazı virüsler ekranda bir mesaj gösterirken, bazı virüsler bulundukları sistem ve sistemleri tamamen kullanılamaz hale getirebilmektedir. Günümüzde, çeşitli donanımlara fiziksel zarar verebilen virüsler de bulunmaktadır. Virüsler, fark edilmeden sistemlere girmek ve sistem üzerindeki faaliyetlerini sürdürmek zorundadırlar (Keleştemur, 2015, s.222). Bu sebeple, gittikçe gelişmiş ve karmaşık yapılarda virüsler geliştirilmeye başlanmıştır. Virüsler ayrıca, yapılarına göre de farklı şekillerde gruplandırılabilmektedir:

- Yerleşik virüsler
- Ön yükleme virüsleri
- Makro virüsleri
- E-posta virüsleri

- Gözcü virüsleri
- Taklitçi virüsler
- Dosya virüsleri
- Betik virüsleri

3.6.2. Truva Atı

Trojan olarak da adlandırılan Truva atları, tıpkı tarihte olduğu gibi iyi niyetli, zararsız gibi kendini gösterip sisteme girerler ancak arkaplanda sistem yöneticisinin izni ve bilgisi olmadan, işlemler gerçekleştirmektedir. Bu zararlı yazılım türünün ismi, Yunanlar tarafından Truva'ya hediye olarak gönderilen tahtadan inşa edilmiş at figüründen gelmektedir. Genellikle hedef sistemi, zombi bilgisayara çevirmek için geliştirilmiş yazılımlardır. Truva atları sayesinde, hedef sistem, saldırganın emri altına girmektedir. Bu yazılımın amaçlarından biri, sızdığı sistemde fark edilmeden, uzaktan saldırılar düzenlenmesine imkan tanımaktır.

Saldırganlar bazı durumlarda, kimliğin ya da saldırının ortaya çıkmasını önlemek amacıyla, hedefine doğrudan saldırmak yerine, kendini gizlemek için ön çalışmalar yapmaktadır. Gizleme işlemi sırasında ne kadar çok katman kullanılırsa, saldırganın tespit edilmesi de o kadar zor olmaktadır. Bu gizleme katmanlarının en önemlilerinden biri de zombi bilgisayarlardır.

Zombi bilgisayarlar ise genellikle iki farklı amaç için kullanılmaktadır. Bunlardan ilki, doğrudan zombi bilgisayar üzerinde saldırı gerçekleştirmektir. İkincisiyse, zombi bilgisayardan koca bir ordu oluşturup, bu ordunun gücünü kullanarak DDoS saldırıları gerçekleştirmektir (Çıtak, 2016, s.149). Truva atları da kendi aralarında çeşitli sınıflara ayrılmaktadır.

- Şifre çalar truva atları,
- Arkakapı açan truva atları,
- Ajan truva atları,
- Aracı truva atları.

3.6.3. Botnet ve Zombi Bilgisayarlar

Uzaktan kontrol edilebilen ve saldırganın istediği tüm amaçları yerine getirmek için kullanılan bilgisayarlara zombi bilgisayar denilmektedir. Zombi bilgisayar ayrıca köle bilgisayar olarak da adlandırılmaktadır. Hedef sisteme gizlice yüklenen uygulamalar, sistem üzerinde ne gibi faaliyetler yapacağı belirlendikten sonra harekete geçmektedir. Zombi bilgisayarlar da bu yazılımlar aracılığıyla kontrol edilmektedir.

Zombi bilgisayar, her ne kadar artık literatürde bu şekilde anılsa da özellikle son dönemde gittikçe popülerleşen IoT cihazlar da aynı amaçla kullanılması halinde, bu şekilde isimlendirilebilmektedir. Kullanıcının haberi olmadan, uzaktan kontrol edilen bu cihazlar, botlar sayesinde birer saldırı makinesine dönüşmektedir. Botlar, yazılan kodlar doğrultusunda otomatik işlemler yapan ve birtakım yönetimsel araçları ele geçiren yazılımlardır.

Botlar sistemlere zarar vermek yerine, çalışmalarını engellemek ya da sistemi yavaşlatmak amacıyla kullanılmaktadır. Zombi bilgisayarlar tarafından, birer saldırı silahı olarak kullanılan botlar, günümüzde ayrıca web sitelerinden otomatik olarak zararlı yazılım indirilmesi şeklinde kod topluluğu halinde de görev almaktadır. Botnet, zombi bilgisayardan oluşturulmuş büyük bir ordu olarak düşünülebilir. Botnet'ler genellikle DDoS saldırıları için kullanılmaktadır (Keleştemur, 2015, s.228).

3.6.4. Tuş Dinleyici

Keylogger olarak da bilinen tuş dinleyiciler, temel olarak hedef sisteme yerleştikten sonra, kurbanın klavyede bastığı tuşları, sürekli olarak kayıt etmekte ve bunları belli bir metin dizesi haline getirerek, ağ üzerinden saldırgana iletmektedir. Tuş dinleyiciler, özellikle siber istihbaratçılar tarafından etkin bir şekilde kullanılmaktadır. Tuş dinleyicilerin, klavyede hangi tuşa basıldığını iletmesi için, hedef sistemin bir ağa bağlı olması gerekmektedir. Ancak havaboşluğunda tesis edilmiş bilgisayarlara da fiziksel olarak erişerek bir harici depolama aygıtına kayıt metni kaydedilebilmektedir.

Günümüzde artık yüksek frekans kullanılarak, belirli bir mesafeye kadar herhangi bir ağ bağlantısı olmaksızın, arada beton ya da metal bir engel olsa dahi uzaktan iletim gerçekleştirilebilmektedir. Tuş dinleyiciler, gömülü olarak donanımlarla birlikte de gelebilmektedir. Donanım ile gelen tuş dinleyiciler, genellikle bilgisayarın ana kartına gizlice yerleştirilmiştir ve oldukça zor tespit edilmektedir. Bu tür donanımlar, sıradan kullanıcıların evlerinde bulundurduğu donanımlar gibi çalışmamaktadır. Yazılımsal olarak çalışmakta olan tuş dinleyiciler ise kendini belli etmemektedir.

Bilindik, popüler tuş dinleyici uygulamalar dışında, saldırganların kendi yazdıkları tuş dinleyici uygulamalar çoğunlukla güvenlik uygulamaları tarafından tespit edilmesi zor, karmaşık kodlardan oluşmaktadır. Bu uygulamalar, esas itibariyle kullanıcıların bastıkları tuşları kaydederek, kullanıcı adı ve parola gibi hassas verilerin ele geçirilmesini sağlamaktadır. Günümüz tuş dinleyicileri sadece metin değil, aynı zamanda simültane olarak çektiği ekran görüntüleri ve video kayıtlarını da saldırgana gönderebilmektedir (Keleştemur, 2015, s.224-225).

3.6.5. Rootkitler

Rootkitler, temel olarak hedef sistemde bulunan dosya ve dizinleri, sistem bilgileri ile çalışmakta olan işlemleri gizleyen, böylelikle de onları etkisiz hale getiren yazılımlardır (Elbahadır, 2014, s.237). İlk nesil rootkitler, salgırganınn yönetici haklarına sahip olabilmek, yönetim uygulamaları ile sistem bilgilerine ulaşabilmek ve bunları gizlemek için geliştirilmiştir. Günümüzde kullanılmakta olan yeni nesil rootkitler ise hedef sisteme sızmış olan diğer zararı yazılımların, sistem yöneticileri tarafından fark edilmeden rahat çalışmalarını sağlamak için kullanılmaktadır.

Rootkitler, genellikle işletim sistemlerinin çekirdek düzeyinde çalışmaktadır. Bu sebeple de tespit edilmeleri ve sistemden kaldırılmaları oldukça zordur. Rootkitler, kaynağı belli olmayan yazılımların sisteme kurulmasıyla birlikte sızabilmektedir. Kimi zaman özgür yazılım içindeki kodlarla da sızabilen bu yazılımların, sisteme enfekte olmasını önlemek için Unix/Linux işletim sistemlerinde dağıtımların resmi depolarından indirilerek kurulması gerekmektedir.

3.6.6. Casus Yazılım

Spyware olarak da adlandırılan casus yazılımlar, isminden de anlaşılacağı gibi genellikle siber casusluk faaliyetleri için kullanılan uygulamalardır. Ancak özellikle çeşitli firmaların reklam verme, istenmeyen mesaj gönderme gibi pazarlamaya yönelik çalışmaları için de geliştirilmiş modelleri bulunmaktadır. Casus yazılımlar, geliştirici tarafından tanımlanan görevleri yerine getirmektedir.

Bir casus yazılım, hedef sistemde yer alan mikrofon ve webcam gibi donanımları otomatik olarak aktifleştirerek, buradan veri transferi yapabilmektedir. Bu yazılımlar ayrıca, web formlarında yer alan kullanıcı adı ve parola gibi ikili metinlerde girilen verileri de ele geçirebilmektedir. Arkaplanda çalışması sırasında, ziyaret edilmek istenen web sitesi yerine, kullanıcıyı sahte olanlarına yönlendirebilmektedir.

Bu sayede sosyal mühendislik yöntemleri kullanılarak, kullanıcı adı ve parola ile kredi kartı gibi pek çok önemli bilgi istenmeyen kişilerin eline geçebilmektedir. Casus yazılımlar ayrıca, ziyaret edilen web sitelerini kayıt altına almaktadır. Böylelikle kurbanın ilgi alanlarının tespit edilmesi kolaylaşmaktadır. Sosyal medyada yapılan yorumlar vb. da yine casus yazılımlar tarafından tespit edilebilmektedir (Keleştemur, 2015, s.226).

3.6.7. Solucan ve Bakteri

İngilizce worm adıyla da anılan solucanlar, virüslerin bir alt dalı olarak nitelendirilebilmektedir. Tıpkı virüsler gibi, kendilerini sürekli olarak farklı cihazlara kopyalamaktadır. Hedef cihaza takılan aygıtlara, cihazın bağlı olduğu ağdaki aygıtlara vb. hızlıca bulaşabilmektedir. Solucanların virüs ve truva atlarından farkı, kendini çalıştıracak bir programa ihtiyaç duymamasıdır. Virüs ya da truva atları, taşıyıcı yazılımların çalışmasına ihtiyaç duymaktadır (Çıtak, 2016, s.150).

Bakteriler de solucanlar gibi bağımsız olarak, kendi kendilerine çoğalabilmektedir. Bakteriler, hedef sistemde sürekli kendini çoğaltmakta, farklı versiyonlarını oluşturmaktadır. Oluşan her yeni versiyon, disk üzerinde daha fazla alan işgal etmektedir. Bu da işletim sisteminde devamlı surette, sistem kaynaklarının

kullanılmasına sebep olmaktadır. Bakterinin çoğalması işlemi, hedef sistemin depolama alanı dolduğunda sonlanmaktadır (Keleştemur, 2015, s.227).

3.6.8. Diğer Siber Saldırı Silahları

- Kinetik Enerji Silahları,
- Yönlendirilmiş Enerji Silahları,
- RF Enerji Silahları
- Yüksek Enerji Lazar Silahları,
- Mikrodalga Silahlar,
- Enerji Atımlı Mermiler,
- Enerji Yüklü Parçacıklar,
- EMP Bombaları

3.7. Siber Saldırı Yöntemleri

Siber saldırı yöntemleri, özellikle internet teknolojilerinin gelişmesiyle birlikte paralel olarak gelişim göstermektedir. Siber saldırı yöntemleri, kendi aralarında da alt kategorilere ayrılmaktadır. Listede yer alan yöntemler, alfabetik sıraya göre dizilmiş olup, siber saldırı ve siber istihbarat faaliyetlerine yönelik kullanılmaktadır.

- Arka kapı (trapdoor)
- Açık mikrofon dinleme
- GSM / VoIP vb. dinleme
- Ağ dinleme (Network sniffing)
- Ağ tarama ve haritalama (Network scanning and Network mapping)
- Hizmet dışı bırakma (denial of service)
- IP aldatmacası (IP spoofing)
- DNS aldatmacası (DNS spoofing)
- İnternet servis saldırıları
- Kabloya saplama yapma
- Kriptografik saldırılar
- Oturum çalma

- Sosyal mühendislik (Social engineering)
- Trafik analizi
- Yemleme (Phishing)
- Yerine geçme (Masquerading)
- Yığın e-posta gönderme (Spam)
- Zamanlama saldırıları
- Zararlı yazılım (Virüs, truva atı, solucan vb.)

3.7.1. Arka Kapı

Arka kapılar da truva atlarına benzer bir yapıya sahiptir; ancak birbirlerinden ayıran keskin bir çizgi vardır. Truva atları bilgisayara kullanıcının izni olmaksızın bulaşmaktadır. Arka kapılar ise kimi zaman hedefe sızan hacker tarafından yazılan bir kod parçacığı ile kimi zamansa kullanıcının kendi rızasıyla kurduğu bir yazılım tarafından oluşmaktadır. Bu sebeple bilinmedik, güvenilmedik uygulamaların sisteme kurulmasından kaçınmak gerekmektedir. Son dönemde ortaya çıkan CIA'ye ait Vault 7 belgelerinde de görüldüğü üzere, açık kaynak uygulamalarda dahi bulunan zafiyetler sebebiyle, arka kapılar oluşturulabilmektedir[49].

Kimi zaman yazılım geliştirme esnasında, geliştiriciler hatalı kod yazabilmekte ya da güvenli yazılım geliştirme standartlarına uymamaktadır. Ayrıca yazılım geliştirme sırasında oluşturulan test kullanıcılarından dolayı da güvenlik açıkları oluşabilmektedir (Çıtak, 2016, s.153). Bu sebeplerden ötürü, gerek açık kaynak gerekse de ticari olarak satın alınan uygulamaların, sisteme kurulmadan önce kaynak kodlarının incelenmesi gerekmektedir. Kapalı kaynak uygulamaların, özellikle kamu kurumlarındaki sistemlere kurulmadan önce, çeşitli protokoller aracılığıyla incelenmesi gerekmektedir. Bu işlem, ayrı bir uzmanlık gerektirdiğinden güvenli uygulama geliştirme bilgi ve becerisine sahip kişiler tarafından yapılmalıdır.

[49] https://betanews.com/2017/03/09/vault-7-the-cia-weaponized-these-popular-programs-to-spy-on-people, Erişim Tarihi: 11 Ocak 2018.

3.7.2. Açık Mikrofon Dinleme

Klasik istihbarat yöntemlerinden biri olan açık mikrofon dinleme, teknolojik gelişmelere de ayak uydurmaktadır. Çeşitli istihbarat örgütlerinin açık mikforon dinleme yapabilmek için yeni birimler oluşturduğu ve yeni teknolojiler geliştirdiği görülmüştür. Eskiden telefon ahizelerine yerleştirilen mikrofonlar sayesinde dinleme yapılmaktayken, bugün casus yazılımlar kullanılarak, sahibinin haberi olmadan bilgisayarlarının veya cep telefonlarının mikrofonları vasıtasıyla da canlı dinleme veya ortam dinlemesi yapılabilmektedir.

Aynı şekilde bilgisayarların mikrofon ve kameralarının kullanılmasıyla gizli kayıtlar alınabilmektedir. 2009 yılında ortaya çıkan GhostNet isimli sistemin, 103 ülkeden çok sayıda bilgisayardaki mikrofon ve kameraları çalıştırarak ses ve video kaydı aldığı ve bunların Çin'e gönderdiği öne sürülmektedir. GhostNet'den en çok etkilenen sistemlerin devlet kurumları ve elçilikler olduğu ifade edilmiştir.

Akıllı telefonlar da birer mikrofona dönüştürülebilmektedir. Akıllı telefonların arkaplanında çalıştırdığı pek çok yazılım, mikrofonları etkinleştirerek, ortamdaki sesin dinlenmesine olanak sağlamaktadır. Ortam dinlemesinin yapılabilmesi için iki farklı seçenek bulunmaktadır. Bunlardan biri uzaktan erişilebilen sistem ve cihazların kullanılması, bir diğeri de fiziksel erişimdir. Uzaktan erişilen sistemlerde dinleme yapabilmek için, hedef cihazın herhangi bir ağa bağlı olması yeterlidir. Ağa bağlı olan cihaza erişim için de çeşitli yöntemler ve cihazlar bulunmaktadır.

Fiziksel erişim denildiğinde ise akla hedef bilgisayar ya da akıllı telefona, doğrudan casus yazılım yüklenmesi gelmektedir. Yüklenen bu programlar, uzaktan erişim sayesinde istendiği zaman, mikrofonu devreye sokmakta ve eş zamanlı olarak sesi doğrudan bir başka yere aktarmaktadır. Bazı IP telefonların da mevcut açıklar sayesinde dinlendiği tespit edilmiştir. Bunun dışında, Smart TV'ler üzerinden de casusluk yapıldığı kamuoyuna yansımıştır[50].

[50] http://www.telegraph.co.uk/technology/2017/03/08/smart-tv-perfect-way-spy, Erişim Tarihi: 12 Ocak 2018.

3.7.3. Ağ Tarama

Ağ tarama, iletişim ağından geçen verilerin, gerek saldırmak gerekse de sistemdeki zafiyetin tespit edilmesi amacıyla gözlenmesidir. Yapılan tarama sonucunda hedef sistem hakkında ayrıntılı bilgi edinilebilmektedir. Sistemde yer alan sunucular, yönlendiriciler, işletim sistemleri, çalışan uygulamalar ya da servisler zafiyet taraması yapıldıktan sonra saldırı gerçekleştirilebilmektedir.

Ağ tarama, siber saldırı öncesinde hedef sistemle ilgili bilgi toplamak için en çok kullanılan yöntemlerden biridir. Nmap, Zenmap ve Wireshark gibi pek çok uygulama ile ağ taraması yapılabilmektedir. Ağ tarama bir siber saldırıya yön veren en önemli evrelerden biridir. Bu evrede elde edilen verler ışığında siber saldırının senaryosu belirlenmekte ve saldırı buna göre gerçekleşmektedir. En çok kullanılan ağ tarama uygulamalarından Nmap'in tarama türleri aşağıdaki gibidir (Çıtak, 2016, s.91-94).

- TCP Syn Scan
- TCP Connect Scan
- FIN Scan
- Xmas (Christmas) Scan
- Null Scan
- Ping Scan
- UDP Scan
- IP Protocol Scan
- ACK Scan
- Window Scan

3.7.4. Hizmet Dışı Bırakma ve Dağıtık Hizmet Dışı Bırakma

Hizmet Dışı Bırakma yani (DoS) hedeflediği sistemin işleyişini engellemeye yönelik bir saldırı türüdür. Bu saldırıların daha etkili olması için Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service – DDoS) saldırıları yapılmaktadır. Bir başka deyişle DDoS, birden fazla kaynak üzerinden tek bir hedefe yapılan saldırılardır. Bu saldırı türünde saldırılar yüzlerce hatta binlerce makineden tek bir hedefe yönelik olabilmektedir.

Saldırgan, DDoS saldırısı yapabilmek için birden fazla bilgisayarı ele geçirebileceği gibi, doğrudan anlaşmalı olan makinelerle de bu saldırıyı gerçekleştirebilmektedir. DDoS saldırıları sayesinde hedef sunucunun çalışması engellenebilmektedir. Yapılan bu saldırılar sonucunda, eğer sunucuda birden fazla web sitesi bulunuyorsa, tüm web siteleri hizmet dışı kalmaktadır.

DoS saldırılarının çalışma prensibi büyük veri paketlerinin sunucuya gönderilmesi üzerinedir. Hedef sisteme gönderilen karmaşık paketler, sunucudan yanıt beklemektedir. Sunucu, gönderilen paketlerin işlemci, bellek ve bant genişliği gibi sistem kaynaklarını tüketmesinden ötürü çalışamaz hale gelmektedir.

Bunun dışında, sistem üzerinde tespit edilen bir zafiyet olması halinde, bu noktaya yapılan saldırılar neticesinde sistemin çökmesi de sağlanabilmektedir. DDoS saldırıları sonucunda hedef sistem hizmet veremez hale gelmektedir. Günümüzde en çok kullanılan DoS saldırı türleri aşağıdaki gibidir (Çıtak, 2016, s.195-197):

- SYN Flood
- Land Flood
- UDP Flood
- Smurf

DDoS saldırılarından başka bir diğer önemli saldırı yöntemi de PDoS'tur. PDoS saldırılar hedefteki sisteme büyük zarar verebilmektedir. PDoS saldırıları sonucunda, hedef sisteme ait donanımın ya değiştirilmesi ya da yeniden kurulması gerekmektedir. Bu saldırı türünde sunucularda çalışmakta olan uygulama ve servisler yerine yönlendirici, yazıcı veya ağdaki herhangi bir donanım hedef alınmaktadır. Temel olarak amaç donanımın firmware'ini değiştirmek, bozmak veya silmektir. PDoS saldırıları, donanımın yönetimsel arayüzüne yerişmeyi sağlayan güvenlik açıkları üzerine kurulmuştur (Keleştemur, 2015, s.297).

3.7.5. IP Aldatmacası

IP aldatmacası aynı zamanda IP spoofing olarak da bilinmektedir. Bu yöntem sayesinde saldırganın gerçek IP adresi değiştirilmekte, bir başka deyişle gizlenmektedir. IP aldatmacası, özellikle hizmet dışı bırakma saldırılarında sıkça kullanılmaktadır. Bunun dışında IP adresine dayalı kimlik doğrulama sistemlerinde de hedef bilgisayarı aldatmak için kullanılabilmektedir. IP aldatmacası temel olarak iki yöntemle yapılmaktadır.

1. Proxy & Socks kullanımı
2. IP paketlerinin düzenlenmesi

Söz konusu yöntemlerden basit olanı şüphesiz ki Proxy & Socks kullanmaktadır. İnternette ücretli/ücretsiz pek çok vekil sunucu bulunmaktadır. Bu sunucuların listesine arama motorlarında basit bir arama yaparak ulaşmak mümkündür. Proxy sunucuya bağlandıktan sonra, ziyaret edilen sunucular artık orijinal IP adresini değil, proxy sunucu tarafından tayin edilen yeni IP adresini görmektedir.

Bu yöntemle, IP adresleri gizlenebilmektedir. Bunun dışında özellikle son yıllarda internet sansürüne karşı kullanılmakta olan VPN servisleri de IP adreslerini değiştirmek için kullanılabilmektedir. Dahası, VPN kullanarak şifrelenmiş veri transferi yapmak mümkündür. Bir başka yöntem de IP paketlerinin düzenlenmesidir. Ancak bu tekniğin uygulanabilmesi için iyi derecede TCP/IP bilgisinin olması gerekmektedir (Keleştemur, 2015, s.299-300).

3.7.6. İnternet Servis Saldırıları

İnternet üzerinde yer alan tüm cihazlar, birbirleriyle konuşabilmektedir. Bu bağlantının oluşması içinse arada, ihtiyaçlara göre farklı hizmetler veren bilgisayarlar bulunmaktadır. Bir başka deyişle, internetteki bilgisayarlar çeşitli protokol ve servisler sayesinde birbirine bağlanmakta ve iletişim kurmaktadırlar. Bu protokol ve hizmetlerin de zafiyetleri bulunmaktadır. Saldırganlar kimi zaman doğrudan protokoldeki zafiyeti, kimi zamansa protokollerin çalışmalarını sağlayan yazılımlardaki açıkları kullanarak saldırı düzenlemektedir (Çifci, 2013, s.143).

İnternette en çok kullanılan protokollerden bazıları aşağıda alfabetik sıra ile listelenmiştir:

- BGP (Border Gateway Protocol)
- DHCP (Dynamic Host Configuration Protocol)
- DNS (Domain Name System)
- FTP (File Transfer Protocol)
- HTTP (Hyper Text Transfer Protocol)
- IMAP (Internet Message Acces Protocol)
- POP3 (Post Office Protocol 3)
- SMTP (Simple Mail Transfer Protocol)
- TCP/IP (Transmission Control Protocol)
- Telnet

Bu servis/protokollerin, özellikle eski yapılara sahip olmasından ötürü çeşitli zafiyetleri bulunmaktadır. Saldırganlar, bu zafiyetlerin, farklı yöntemler aracılığıyla kullanılmasıyla, gelişmiş siber saldırılar düzenleyebilmektedir. Günümüzde, güvenliğe daha fazla önem verilmesiyle birlikte listede yer alan protokollerden bazılarıyla ilgili çeşitli yeni güvenlik teknolojileri oluşturulmuştur. Ancak yine de halen dahi bu zafiyetler saldırganların hedefi arasında yer almaktadır.

3.7.7. Kabloya Saplama Yapma

Kabloya saplama yapma, konvansiyonel istihbarat faaliyetlerinden birisidir. Güvenli olmayan, sıradan iletişim ağ kablolarına, çeşitli teçhizatların kullanılmasıyla, fiziksel olarak saplama yapılması ve bağlantı kurulmasını ifade etmektedir. Kabloya saplama yapılması durumunda, iletişim trafiğini ele geçirmek mümkündür. Eskiden sadece telefon trafiğinin dinlenebildiği bu yöntemle, bugün bilgisayar sistemleri arasındaki trafik de dinlenebilmektedir.

Günümüzde sahip olduğumuz gelişmiş teknoloji sayesinde, sadece internet ve ev telefonları değil, aynı zamanda VoIP telefonlar ve mobil telefonlar için de benzer işlemler uygulanabilmektedir. İngiltere ve ABD gibi ülkelerdeki istihbarat

teşkilatlarının, fiber kablolara saplama yaparak, tüm ağ trafiğini dinlediğine dair iddialar ortaya atılmıştır[51].

3.7.8. Kriptografik Saldırılar

Kripgotrafik saldırılar da eski bir istihbari faaliyettir. Özellikle I. Dünya Savaşı ve II. Dünya Savaşı yıllarında büyük bir önem verilmiş olan bu saldırılar sayesinde, düşmana ait birçok hassas bilgi elde edilmiş ve bu sayede savaşın seyrini değiştiren operasyonlar düzenlenmiştir. Kriptografik saldırılar, şifrelenmiş mesaj ya da verilerin okunabilmesi için, şifrenin çözülmesi amacıyla yapılan saldırılardır. Bu saldırılar sırasında kullanılan kriptografik sistem araştırılmaktadır. Daha sonra bu sistemin zayıf yönleri irdelenerek şifre çözülmeye çalışılmaktadır.

Kripto analiz sayesinde bilinmeyen kripto sistemler çözümlenebilmekte ve bilinen kripto sistemlerin anahtarı tahmin edilebilmektedir. Saldırılar genellikle anahtar değişkenleri oluşturan üreticiler ve dağıtıcılara yapılmaktadır. Bu sistemlerde herhangi bir zafiyet bulunması sonucunda saldırgan, anahtar tahmini yapabilmektedir. Bunun dışında rastgele sayı üreticilerinin tekrarlanan karakteristiğinin belirlenmesi durumunda da anahtar tahmin etmek mümkün olmaktadır. Kimi zaman da karşı tarafa ait bir mesajın ele geçirilmesi halinde, anahtar elde edilebilmektedir (Keleştemur, 2015, s.304).

3.7.9. Web Uygulama Saldırıları

İnternette yer alan bilgilerin büyük bir kısmına web siteleri üzerinden erişmek mümkündür. Kimi zaman doğrudan web sitelerine, kimi zamansa web sitelerinin bağlı olduğu veritabanları ve hatta bu veritabanlarının da konuşlandığı sunuculara saldırılar düzenleyerek, bilgi hırsızlığı yapılabilmektedir. Genellikle bu tür durumlarda saldırılar, uygulama katmanı üzerinden gerçekleşmektedir. Bir başka deyişle, web uygulamalarına saldırılar düzenleyerek, veritabanına ulaşmak ve hatta site üzerindeki verilerde manipülasyon yapmak mümkündür.

[51] https://www.theguardian.com/uk/2013/jun/21/gchq-cables-secret-world-communications-nsa, Erişim Tarihi: 13 Ocak 2018.

Cross-Site Scripting (XSS) açığı, kullanıcıdan alınan değerler, gerekli HTML ve JavaScript filtrelerinden geçmediği takdirde oluşmaktadır. Ziyaretçinin, sisteme doğrudan zarar verebilecek zararlı kodları çalıştırmasına imkan tanıyan XSS açığı, Reflected XSS, Dom-Based XSS ve Stored XSS olmak üzere üç türe ayrılmaktadır (Çıtak, 2016, s.211). Web uygulamalarında rastlanılan bir diğer önemli zafiyet de Cross-site Request Forgery (CSRF) açığıdır. Bir sistem üzerinde herhangi bir işlem yapmaya yetkisi olmayan saldırganın, bu işlemi yapmaya yetkisi olan bir kullanıcıya istediği işlemi yaptırmaya dayalı bir zafiyettir. CSRF saldırıları, daha basit bir ifadeyle güven sömürüsüne dayanmaktadır (Elbahadır, 2014, s.168).

Bir başka önemli web zafiyeti de SQL Enjeksiyonudur. SQL, veritabanına erişmek ve yönetmek için kullanılan standart bir yapıdır. Veritabanına kayıt eklemek, mevcut kaydı değiştirmek ya da silmek gibi işlemlerin yapılmasını sağlamaktadır. SQL Enjeksiyonu ise bir takım SQL ifadelerinin kullanılarak, sistemdeki açıktan faydalanmak suretiyle veritabanına izinsiz erişimi ifade etmektedir.

Uygulamalara güvenilir olmayan kaynaklardan gelen girdilerin, kontrol edilmeden SQL sorgusunu oluşturan cümlecik içinde kullanılmasından kaynaklanmaktadır (Demir, 2015, s.298). SQL Injection, SQL cümleciklerinin arasına dışarıdan girdi yapılarak, SQL'i istenilen şekilde manipüle etmeye yarayan bir zafiyettir[52].

3.7.10. Sosyal Mühendislik

Siber saldırganların en büyük silahları teknik bilgilerinden ziyade zekalarıdır ve sosyal mühendislik bu konuda zekanın önemini en çok vurgulayan yöntemlerden biridir. Elbahadır'a göre sosyal mühendislik, sıradan kullanıcı yetkileriyle, hedef sistem hakkında elde edilemeyecek bilgilerin; ikna etme, etkileme, aldatma gibi faktörlerin kullanılarak ele geçirilmesidir (Elbahadır, 2014, s.197).

[52] https://ferruh.mavituna.com/sql-injection-a-giris-ve-sql-injection-nedir-oku, Erişim Tarihi: 13 Ocak 2018.

Yeterli teknik bilgiye sahip olmadan, etkin bir sosyal mühendislik sayesinde başarılı saldırılar düzenlemek mümkündür. İyi bir saldırgan insan psikolojisini ve kurum yapısını çözümleyebilmelidir. Sadece bu yeteneği ile zeki bir saldırgan, hedef kurumun içine sızabilmektedir. Saldırgan, hedef kişi ya da kuruma saldırı yapmak için farklı kimliklere bürünebilmektedir:

- Kurum personeli
- Yetkili personel
- Müşteri
- Müşteri temsilcisi

En sık kullanılan sosyal mühendislik yöntemleri ise şu şekildedir:

- Hedefe, güvenilir bir kişi gibi yaklaşmak ve onu bu yönde ikna etmek,
- Herhangi bir teknik sorun yaşayan kişi ya da kuruma yardım sever bir tavır sergilemek. Kimi zaman saldırgann kendisi gizli bir şekilde zor durum oluşturabilmektedir,
- Şirket çalışanları ile aynı ilgi alanları olduğunu belirtmek ve bu yolla iletişim kurmak,
- Şirket çalışanlarını sosyal medya üzerinden takip etmek. Önce arkadaşları ile yakınlık kurmak. Ardından da ortak tanıdıklar üzerinden yakınlık kurmak,
- Başka bir kişiyi taklit etmek. E-posta ya da telefon aracılığıyla sanki bu kişiymiş gibi iletişim kurmak,
- Hedef kurumun çöplerini, eski donanımlarını vs. incelemek.

Sosyal mühendislik aracılığıyla hedefini kandıran bir kişi, hedef sistemle ilgili tüm yetkilere sahip olabilmektedir. Yapılacak saldırı sonucunda, sadece kuruma ait veriler değil, kurumla çözüm ortaklığı ya da tedarikçilik vb. yapan üçüncü partiler ve kullanıcılar da etkilenebilmektedir (Keleştemur, 2015, s.307).

3.7.11. Trafik Analizi

Trafik analizi genellikle ağ tarama ile karıştırılan bir yöntemdir. Trafik analizi sayesinde hedefin eylemleri hakkında bilgi toplanabilmektedir. Ağa yapılan bir saldırı sonucunda, siber olaylara müdahale ekipleri ya da adli bilişim uzmanları tarafından yapılan trafik analizleri sayesinde, hedefe yönelik ne gibi saldırıların bulunduğu ve potansiyel tehlikeler hakkında bilgi edinilebilmektedir.

Trafiğin fazla olduğu noktalar tespit edilerek, herhangi bir eylem aşamasına geçilebileceği analiz edilebilmektedir. Trafik analizi ayrıca, ağ üzerinde herhangi bir anormallik olup olmadığının kontrol edilmesine de imkan tanımaktadır[53]. Özellikle insider threat olarak adlandırılan ve şirket çalışanlarının, çeşitli motifler doğrultusunda firmaya ait bilgileri bir başka kişi ya da kuruma izinsiz olarak iletmesi gibi durumların ortaya çıkmasında da etkilidir.

Sosyal medya üzerinden paylaşılmış olan bir videonun, orijinaline ulaşılması ve bu dosyanın incelenerek boyutunun tespit edilmesi halinde, belli zaman aralığında, aynı boyuttaki upload trafiğinin hangi IP adreslerinden yapıldığı incelenerek, ilgili dosyanın internete yüklenmesini kim ya da kimlerin yaptığı tespit edilebilmektedir.

Trafik analizi ayrıca, kimin kimle hangi saatte, ne kadar süre konuştuğuna ve hatta ne konuştuğuna kadar farklı konularda bilgi edinilmesine imkan tanımaktadır. İki kişinin, birbiriyle siber uzay üzerinden yapmakta olduğu mesajlaşma ya da sesli/görüntülü konuşma trafik analizi sayesinde ele geçirilebilmektedir.

3.7.12. Yemleme

Yemleme, yani Phishing sayesinde çok büyük istihbari operasyonlar düzenlenebileceği gibi, sıradan kullanıcılara ekonomik yönden zarar da verilebilmektedir. Yemleme kısaca, bir web sitesinin, birebir benzerinin yapılarak, kurbanın sanki orijinal siteyi ziyaret ediyormuş gibi yönlendirilerek, kullanıcı adı, parola, kredi kartı gibi bilgileri girmesini sağlama ve böylelikle bu bilgileri elde etme

[53] https://www.sans.edu/cyber-research/security-laboratory/article/traffic-analysis, Erişim Tarihi: 14 Ocak 2018.

yöntemidir. Yemleme için genellikle orijinal banka siteleri, alışveriş siteleri, açık artırma siteleri, sosyal ağ vb. web sitelerinin benzerleri yapılmaktadır.

Yemleme yapılabilmesi için sadece websitelerinin taklitlerininin geliştirilmesi yeterli olmamaktadır. Benzer site yapıldıktan sonra, kurbanı yemleyebilmek için onun ilgisini çekecek içeriğin kendisine gönderilerek, bu siteyi ziyaret etmesi sağlanmalıdır. Bu işlem genellikle kurbana e-posta gönderilerek yapılmaktadır. E-postanın içinde bulunan linke tıklanılması halinde de kurban orijinal site yerine, sahte siteye yönlendirilmektedir. WannaCry ve CyrptoLocker gibi fidye yazılımlar da yemleme yöntemiyle hedef sisteme sızmıştır[54].

3.7.13. Yerine Geçme

Masquarede olarak da adlandırılan bu saldırı türünde sahte bir kimlik kullanarak hedef bilgisayara izinsiz erişim sağlanmaktadır. Bu erişimin sağlanması için ağ üzerindeki başka bir bilgisayara ait bilgiler girilmektedir. Yerine geçme eylemi, dahili ağda bulunan bir bilgisayar kullanıcısının, bir başka bilgisayar üzerinden internete bağlanabilmek için yapılabileceği gibi, tamamen içeriden düzenlenecek saldırılar aracılığıyla, ağa bağlı bilgisayarlardaki hassas bilgilere izinsiz erişmek amacıyla da yapılabilmektedir (Çifci, 2013, s.148).

Ağ içinde yer alan bilgisayarların etkin bir şekilde korunmaması ya da etkin bir onaylama sisteminin bulunmaması halinde, yerine geçme saldırılarına karşı büyük bir zafiyet var demektir. Yerine geçme saldırıları genellikle ele geçirilmiş kullanıcı adı ve parolalar aracılığıyla yapılmaktadır. Yerine geçme saldırısına başlamadan önce, çeşitli hazırlıklar yapılabilmektedir. Saldırı içeriden gerçekleşecekse, bilgisayarlara tuş dinleyici kurularak, kullanıcıların giriş bilgileri elde edilmektedir. Bunun dışında omuz sörfü, yakından takip ya da çeşitli sosyal mühendislik yöntemleri de uygulanabilmektedir.

[54] https://www.us-cert.gov/ncas/alerts/TA13-309A, Erişim Tarihi: 15 Ocak 2018.

3.7.14. Yığın E-posta Gönderme

Yığın e-posta'lar aslında neredeyse tüm internet kullanıcılarının, hemen hemen hergün karşılaştığı ve spam posta olarak adlandırılan e-postalardır. Yığın e-postalar; istenmeyen e-posta, junk mail, spam mail, bulk mail gibi farklı isimlerle de anılmaktadır. Yığın e-posta göndermek için, binlerce hatta yüzbinlerce e-posta adresini web sitelerinden, müşteri listelerinden, elektronik bültenlerden, haber gruplarından, sosyal medyadan vb. toplayıp satan firmalardan veritabanı satın alınmaktadır. Daha sonra genellikle reklam amaçlı olmak üzere veritabanındaki kullanıcılara toplu e-posta gönderimi yapılmaktadır.

Yığın e-posta göndermek için internette pek çok çevrimiçi servis bulunmaktadır. Bunun dışında ücretli/ücretsiz uygulamalar sayesinde de hızlı bir şekilde yığın e-posta göndermek mümkündür. Yığın e-postalar, I. Körfez Savaşı sırasında ABD ordusu tarafından etkin bir şekilde kullanılarak, düşman subayların savaş öncesi ve savaş sırasında morallerini bozmaya yönelik çalışmalar yapılmıştır[55].

3.7.15. Zamanlama Saldırıları

Zamanlama saldırıları özel bir kriptografik saldırı türüdür. Bu saldırı türü aracılığıyla saldırgan, çeşitli kriptografik algoritmaların çalışması için geçen süreyi analiz ederek kriptosistem çözümlenmektedir. Bilgisayar üzerinde gerçekleşen her işlemin çalışması için belirli bir süre gerekmektedir. Saldırgan, bu süreleri tespit ederek kullanılmakta olan kriptosistem hakkında bilgi sahibi olabilmektedir.

Zamanlama saldırılarının kullanılabilmesi için kripto sistem tasarımı, CPU tasarımı ve sistem üzerindeki çalışma prensibi, kullanılmakta olan algoritmalar, zamanlama ölçümleri gibi konularda bilgi sahibi olmak gerekmektedir. Hassas süre ölçümü yapılarak, kriptosistemin özelliklerine ulaşılabilmektedir. Zamanlama saldırıları veriye bağlı zamanlama özelliğine sahip tüm algoritmalarda kullanılabilmektedir. Kimi durumda zamanlama saldırıları kullanılarak, bilinen bir düz metin ya da şifrelenmiş bir metin parçasını deşifre etmek, kripto analiz yöntemlerine

[55] http://edition.cnn.com/2003/WORLD/meast/01/11/sproject.irq.email/index.html, Erişim Tarihi: 15 Ocak 2018.

göre çok daha kolay olabilmektedir. Bazı hallerde ise her iki sistem kombine kullanılarak daha kesin sonuçlar elde edilebilmektedir (Keleştemur, 2015, s.311).

3.8. Diğer Ülkelerin Siber İstihbarat Faaliyetleri

Bu başlığın alt başlıklarında; ABD, Çin, Rusya Federasyonu, İngiltere ve İsrail'deki siber istihbarat faaliyetleri konularında özet bilgiler verilecektir.

3.8.1. ABD'de Siber İstihbarat Faaliyetleri

ABD için siber istihbarat ve siber güvenlik oldukça önemli konulardır. ABD'de, siber uzay harbin beşinci boyutu olarak kabul edilmektedir ve NSA'nın başındaki isim Michael S. Rogers aynı zamanda USCYBERCOM'un da komutanı olarak görev yapmaktadır.

ABD Savunma Bakanlığı Siber Komutanlığı'nın tam yetkili operasyonel kabiliyeti bulunmaktadır. Böylelikle siber savaş ortamında gerektiğinde harekat icra edebilecek bir yapıya sahiptir. Komutanlık, düşman iletişim ağlarına, komuta kontrol sistemlerine ve bilgisayarlarına sızmak, veri çalmak/değiştirmek ve kullanılamaz hale getirmek gibi faaliyetler gerçekleştirmektedir.

Komutanlığın görevi; Savunma Bakanlığı'nın bilgi ağının korunması ve savunmasına önderlik etmek, Savunma Bakanlığı'nın askeri harekatlarına destek sağlanmasını koordine etmek, tüm askeri siber ortam harekatlarına hazırlık yapmak ve gerektiğinde bu harekatları yönetmek, ABD ve müttefiklerinin siber ortamda serbest bir şekilde faaliyet göstermesi ve ABD düşmanlarının siber ortamda faaliyet göstermesinin engellenmesi amaçlarına yönelik aktiviteleri planlamak, koordine etmek, entegre olmak, senkronize etmek ve yönetmektir. Siber Komutanlık, muharip kuvvetlerde olduğu gibi savunma ve saldırı kabiliyetlerine sahiptir. Son senelerde özellikle saldırı konusunda büyük çalışmalar başlatılmıştır.

Siber Komutanlık, ABD Stratejik Komutanlığı'na bağlıdır. Stratejik Komutanlık ise uzay harekatı, bilgi harekatı, füze savunması, komuta kontrol, istihbarat, keşif ve gözetleme ile nükleer silahlardan sorumlu bir komutanlıktır. ABD Siber Komutanlık ise kendi içinde dört bölüme ayrılmıştır:

- Kara Kuvvetleri Siber Komutanlığı/2'nci Ordu
- Donanma Siber Komutanlığı/Deniz Kuvvetleri 10'uncu Filosu
- Hava Kuvvetleri Siber Komutanlığı/24'üncü Hava Kuvveti Komutanlığı
- Deniz Piyadeleri Siber Komuntalığı

ABD gizli servisi NSA de siber istihbarat konusunda dünyanın en önde gelen isimlerinden biridir. Zira Snowden tarafından sızdırılmış olan bilgi ve belgeler ışığında, NSA'in tüm dünyayı dinlediği ortaya çıkmıştır. NSA, ABD Savunma Bakanlığı ve ABD İstihbarat Topluluğu'nun (U.S. Intelligence Community) üyesi olarak görev yapmaktadır. Dış siber tehdit istihbaratını yürütmekle yükümlü olan teşkilat, milli güvenlik sistemlerinin savunulması konusunda da gerekli çalışmaları yürütmektedir.

ABD siber alanının korunması için İç Güvenlik Bakanlığı'na istihbarat desteği sağlamaktadır. ABD Savunma Bakanlığı'nın kriptografik istihbarat birimi olan NSA, ülke sınırları dışındaki iletişim ve sinyal istihbaratından da sorumludur. Dünyada en fazla matematikçi istihdam eden istihbarat teşkilatı olarak da dikkat çeken NSA, uzun yıllar kamuoyundan saklı tutulmuş, çok gizli bir servis olarak görev yapmıştır.

Bu yüzden NSA için ayrıca "No Such Agency" ifadesi de kullanılmaktadır. Küresel kriptolojide en üstün kurum olma stratejisi içerisinde olan NSA için, bu anlamda yurtdışındaki tüm kriptoları çözebilecek kabiliyeti sahip olduğu ifade edilmektedir. NSA terör örgütleri, bunlarla iletişimde olan ya da potansiyel olarak olabilecek şahısların, telefon aramaları ve tüm internet iletişimini dinlemektedir.

Siber istihbarat faaliyetleri yürütmekte olan bir diğer ABD gizli servisi de FBI'dır. FBI, ABD sınırları içindeki suç ve istihbarat karşı koyma faaliyetlerinde bulunmaktadır. Son yıllarda siber faaliyetlerin öneminin artmasıyla birlikte, siber olayların araştırılması ve engellenmesinden de sorumlu hale getirilmiştir. Ülke içi siber tehditlere karşı istihbarat sağlamak ve bunları karar alıcılara sunmakla görevlendirilmiştir. Bu anlamda ABD İstihbarat Topluluğu'na karşı doğrudan

sorumludur. FBI, ayrıca siber güvenlik ve siber istihbarat konularında İç Güvenlik Bakanlığı'na bilgi ve destek sunmaktadır (Keleştemur, 2015, s.178-184).

3.8.2. Çin'de Siber İstihbarat Faaliyetleri

Çin, bugün belki de siber istihbarat konusunda faaliyet gösteren en önemli ülkeler arasında yer almaktadır. Son dönemde siber savaş ve siber istihbarat konularına önem veren Çin, bu anlamda çeşitli projeler geliştirmekte ve diğer ülkelerin siber uzay üzerinden gerçekleştirmekte olduğu istihbarat faaliyetlerine karşı koymaktadır.

Çin'in, vatandaşları arasından yetiştirdiği birçok siber savaşçıyı, ayrı hacker grupları altında birleştirdiği ve faaliyetlerini buna göre gerçekleştirdiği iddia edilmektedir. Böylelikle, yapılan saldırılar Çin hükümetinden bağımsız olarak dışarıya servis edilmektedir. Çin ayrıca ABD menşeli yazılım ve donanımlardan uzak kalarak, kendi yazılım ve donanımlarını geliştirmeye başlamıştır.

Diğer taraftan Çin'in ABD menşeli altyapılara siber saldırılar düzenleyerek, önemli ölçüde istihbarat elde ettiği de düşünülmektedir. Kurduğu siber ordu ile siber savaşa hazır olduğunu tüm dünyaya göstermiş, hatta büyük ölçüde tehdit oluşturmaya da başlamıştır. Çin, geliştirdiği siber strateji sayesinde özellikle hacker grupları ile büyük bir hareket içerisinde bulunmaktadır. Yapılan araştırmalara göre ülkede yaklaşık 250 adet hacker grubu olduğu belirtilmektedir (Fritz, 2017, s.44).

Çin, siber uzayda savunmayla birlikte saldırıya yönelik bir gelişme planı uygulamaktadır. Bu anlamda Tayvan ile Çin arasındaki gerilime ABD'nin müdahil olmaya çalışması sebebiyle ABD'nin elektrik şebekesini çökertebileceğini ispatlayan çeşitli eylemlerde bulunmuştur. İnterneti propaganda aracı olarak da kullanan Çin, bu amaçla siber uzayda manilülatif, dezenformatif bilgiler de yayınlamaktadır. Ayrıca ağ verilerini değiştirebilme, ağ casus istasyonları kurabilme gibi yeteneklere de sahiptir. Çin Ordusu da tıpkı ABD gibi, konvansiyonel savaşları desteklemek amacıyla siber alanda faaliyetlerini genişletmekte, araç ve personelinin eğitim kapasitesini artırmaktadır.

Çin Genelkurmay 3. Dairesi, yabancı askeri güçlerin iletişimlerini kontrol etme, sinyal istihbaratı ve siber güvenlikle ilgili çalışmaların yapıldığı birimdir. Çin'de farklı bölgelerde bulunan komutanlıklar ile birlikte sinyal istihbaratını toplamakta ve yorumlamaktadır. Tıpkı ABD'nin NSA kurumundaki gibi ülke dışındaki sinyalin toplanması, ele geçirilmesi ve analiz edilmesi görevlerinden de sorumludur.

Çin'in Asya-Pasifik bölgesinde en fazla SIGINT trafiğine sahip olmasını sağlayan kurum olarak da adını duyurmuştur. HUMINT elde etmekte olan Genelkurmay 2. Dairesi ile de koordinasyon içerisindedir. Genelkurmay 4. Dairesi ise Elektronik istihbarat (ELINT) elde etmekle yükümlü kurumdur. Elektronik karşı tedbirler ve radar unsurlarından oluşan faaliyetler yürütmektedir. SIGINT elde etme özelliğine de sahip olduğundan, bir başka deyişle Genelkurmay 3. Dairesi'ne de yardımcı olmaktadır (Keleştemur, 2015, s.185-186).

3.8.3. Rusya Federasyonu'nda Siber İstihbarat Faaliyetleri

Siber savaşın bir diğer önemli ismi de kuşkusuz Rusya'dır. Daha önce, ABD ile girmiş olduğu mücadeleden teknik anlamda galip gelememiş olmasına rağmen, günümüzde siber güvenlik ve siber istihbarat açısından öncül ülkeler arasına girmeyi başarmıştır. Rusya, 1999 yılında Vladimir Putin'in göreve gelmesiyle birlikte siber savaşa hazır bir diğer ülke olarak gelişim göstermiştir.

Siber uzay'da ABD ve Avrupa'nın en büyük tehditi haline gelen Çin'den sonra Rusya da benzer şekilde güç anlamında büyük bir tehdit haline gelmektedir. Çeşitli siber güvenlik uzmanları Rusya'nın Çin'den siber savaş konusunda çok daha iyi olduğunu belirtmektedir. Rusya da son dönemde milli işletim sistemi ve antivirüs gibi projelerle bu anlamda büyük yol kat etmiş, ülkenin alt yapısını tamamen milli ürünlerle oluşturmaya başlamıştır.

Rusya hükümetinin de tıpkı Çin'de olduğu gibi hükümetle bağlantısı bulunmayan hacker grupları ile iş birliği içine girdiği iddia edilmektedir. Daha önce, Estonya ve Gürcistan gibi ülkelere bu gruplar aracılığıyla çeşitli saldırılar düzenlemiştir. Önceki yıllarda KGB olarak bilinen, bugünse FSB adıyla hizmet veren Rus istihbarat servisi

de siber uzayda gerçekleşen gelişmeleri yakından takip etmektedir. Bunun dışında tıpkı NSA gibi çalışmakta olan FAPSI (Devlet İletişim ve Bilişim Federal Teşkilatı) isimli teşkilat da siber uzayda istihbari çalışmalar yapmakta, ülkeye karşı gerçekleşecek tehditleri önceden kestirmekte ve gerekli önlemleri almaktadır.

FAPSI kod kırma, telefon dinleme, zararlı yazılım geliştirme gibi önemli çalışmalar yapmaktadır. Ortaya atılan iddialara göre 2003 yılında imzalanan bir protokolle birlikte FAPSI, dünyanın en büyük hacker okulu olarak da gizli bir misyon edinmiş, bu anlamda Rusya'da hükümet için çalışan hacker'lar geliştirmeye başlamıştır. Ayrıca aynı yıl birimin ismi "Özel İletişim ve Bilişim Servisi" olarak değiştirilmiştir.

FSB, Rusya Federasyonu'nun iç güvenliğinden sorumlu teşkilattır. Rusya Devlet Başkanı'na doğrudan bağlı olan kurum, istihbarata karşı koyma, iç güvenlik, sınır güvenliği ve terörle mücadeleden sorumludur. Siber uzayda ise FSB iletişim ağları dahil, kritik altyapıların korunmasından sorumludur. FSB Kanunu'na göre Rusya'da hizmet etmekte olan tüm telekomünikasyon hizmeti veren birey ve kurumlar, FSB'nin ek yazılım ve donanımlarına müsade etmek zorundadır.

Rusyanın 5. Boyut Siber Ordusu, Savunma Bakanlığı'na bağlı Elektronik Harp Birlikleri ile profesyonel siber korsanlık eğitimi veren kurumların yetiştirdiği kişilerden oluşmaktadır. Resmi olarak bu bilgiler tam olarak kamuoyu ile paylaşılmıyorsa da kriptografi, bilgisayar güvenliği, gelişmiş dinamik keşif kapasitelerinin artırılması, kablosuz veri iletişim jammerlarının geliştirilmesi, elektromanyetik dalga silahlarının üretilmesi, siber mantık bombaları, virüs ve solucanların yazılması ve DDoS ve istihbarat maksatlı gelişmiş, büyük Botnet oluşturulması gibi hususlarda çalışmalar yaptığı öne sürülmektedir. 5. Boyut Siber Ordu bünyesinde 7500'den fazla personel görev almaktadır (Keleştemur, 2015, s.187-188).

3.8.4. İngiltere'de Siber İstihbarat Faaliyetleri

İngiltere de özellikle GCHQ ile birlikte siber savaş ve siber istihbarat konularında önemli faaliyetler gerçekleştirmekte olan bir başka ülkedir. GCHQ, Snowden tarafından sızdırılan belgelerde adı en çok geçen kurumlar arasındadır. İngiltere'de Haziran 2009'da Milli Güvenlik Stratejisi kapsamında ilk kez siber güvenlik konularının ele alınmasıyla birlikte, ülke çapında siber güvenlik ve siber saldırı konularında önemli adımlar atılmıştır. GCHQ'nun da NSA gibi, uluslararası dinlemeler yaptığı, internet trafiğini analiz ettiği görülmektedir. GHCQ, iç güvenlik servisi MI5 ve dış istihbarat servisi MI6 ile birlikte ulusal güvenlikten sorumlu üç teşkilatından biridir.

Siber Güvenlik ve Bilgi Güvencesi Ofisi (OCSIA) İngiltere'deki siber uzayın güvenliğinden sorumlu olarak, önceliklerin belirlenmesini sağlamaktadır. Ayrıca ülkenin siber güvenlik ve bilgi güvenliğinin sağlanmasıyla ilgili stratejik yönlendirmeler ve koordinasyon da yine bu kurum tarafından yapılmaktadır. Siber Güvenlik Harekat Merkezi (CSOC) ise siber uzaydaki gelişmelerin takip edilmesi, siber olaylara karşı müdahale işlemlerinin koordinasyonundan sorumlu olan kurumdur. 12 Mart 2010 tarihinde faaliyete geçen kurumun binası, GCHQ ile aynı yerleşke içerisinde bulunmaktadır.

İngiltere'nin siber uzay üzerindeki güvenliği ve siber İKK faaliyetleri bakımından bir diğer önemli kurumu da Milli Altyapıları Koruma Merkezi'dir. (CPNI) CPNI, İngiltere'nin milli altyapılarını terörizm ve casusluk gibi tehditlere karşı korumakla yüklümlü olan kurumdur. Ayrıca sistemde bulunan zafiyetlerin azaltılması, kapatılmasıyla ilgili olarak da tavsiye otoritesi olarak da kabul görmektedir.

Tavsiyeler neticesinde personelin eğitiminden, bilgi güvenliği için kullanılması gereken yöntemlere kadar farklı işlemler gerçekleşebilmektedir. Kamu Bilgisayar Olaylarına Acil Müdahale Ekibi (GovCertUK) ise CPNI ile oldukça yakın bir çalışma içerisindedir. Devlete hizmet etmekte olan kamu bilgisayarlarına karşı gerçekleşebilecek tehditlerin azaltılması ile ilgili çalışmalarda ve tavsiyelerde bulunmaktadır (Keleştemur, 2015, s.188-190).

3.8.5. İsrail'de Siber İstihbarat Faaliyetleri

İsrail, birçok Avrupa ülkesinin aksine siber savaş ve siber istihbarat alanlarında ki faaliyetlerine çok daha önceden başlamıştır. Bu anlamda oldukça yüksek bilgi ve beceriye sahip olan kurumlar, konvensiyonel askeri operasyonlarda da siber savaş ögelerinden istifade etmektedir. Bununla birlikte, 2002 yılında kurulmuş olan siber saldırılara karşı savunma özelliği bulunan bir özel tim, İsrail Güvenlik Teşkilatı (Shin Bet) çatısı altında faaliyetlerine başlamıştır.

İsrail, diğer ülkelerdeki siber savaşçılarda aranmayan bir özelliği de kriterleri arasına eklemiştir. Tıpkı konvansiyonel savaşlarda aranan komandolar gibi, siber savaşçılardan da bir takım fiziki özellikler talep edilmektedir. İsrailli siber savaşçılar, hem siber hem de fiziksel tahribat yapabilme yeteneğine sahiptirler. Bu anlamda, İsrail'e ait siber saldırı kuvvetleri, Ortadoğu'nun en tehlikeli siber savaşçılarıdır denilebilir.

İsrail'e bağlı Milli Sibernetik Görev Gücü, İsrail'in kritik ağlarını savunmak, özel kuruluşları sanayi casusluğuna karşı korumak ve İsrail'i bir bilgi merkezi haline getirmekle görevlidir. Yapısal olarak ABD'nin Siber Komutanlığı'na benzemektedir. Unit 8200 ise İsrail'in sinyal istihbarat ve şifre çözme teşkilatıdır. Yeni dünya düzenine uyum sağlayan kurum, siber faaliyetler için de önemli çalışmalar yapmaktadır. Bir başka önemli birim, C41 Tugayı da askeri ağları siber saldırılardan korumakla görevlendirilmiştir. Ayrıca komuta, kontrol, muhabere ve bilgisayarlarla ilgili faaliyetlerin tamamından askeri anlamda sorumlu olan birimdir (Keleştemur, 2015, s.191-192).

3.9. Siber İstihbarat ve Kamu Güvenliği İlişkisi

Soğuk Savaş dönemindeki iki kutuplu güvenlik anlayışı, bugün yerini küresel güvenliğe bırakmıştır. 20. yüzyılda özellikle nükleer silahlar başta olmak üzere, konvensiyonel silahlar ve buna bağlı gerçekleştirilmesi muhtemel terör eylemleri en büyük güvenlik problemini oluşturmaktayken, günümüzde KİS'ler ve siber saldırılar öncelikli tehlikeler arasına girmiştir. Konuyla ilgili olarak NATO ve AB gibi örgütler, siber savaş ve siber istihbarat unsurlarının önemine değinmektedir. Bu örgütler, üye

devletlerin altyapılarının güçlendirilmesi ve teknokratların konuya ilişkin bilgi ve becerilerinin artırılması için çalışmalar yapmaktadır. Türkiye de NATO üyesi bir devlet olarak, siber güvenlikle ilgili olarak gerekli çalışmalarını sürdürmektedir.

Siber uzayın her geçen gün genişlemesi ve bu sistem içinde yer alan cihazlar ve kullanılan protokollerdeki gelişmelere bağlı olarak, siber tehditler de nitelik ve nicelik bakımından artış göstermektedir. Bu saldırılar kimi zaman yeni bir silahın ortaya çıkması kimi zamansa tespit edilen yeni zafiyetlere bağlı olarak geliştirilen yöntemlere bağlı olarak farklı yapılarda karşımıza çıkmaktadır.

Yeni çıkan saldırılar ya da sıfırıncı gün zafiyeti olarak adlandırılan, henüz tespit edilmemiş ancak mevcut sistemlerde var olan zafiyetlere bağlı siber tehditin önceden algılanması ve analiz edilmesi gerekmektedir. Bunun için de devletlerin gerek özel siber güvenlik firmalarından alacağı profesyonel danışmanlık hizmetleri gerekse de kamu hizmeti veren siber olaylara müdahale merkezleri aracılığıyla etkin bir siber tehdit istihbaratı oluşturması gerekmektedir.

Günümüzde ABD gibi birçok gelişmiş ülke, kritik altyapılarının korunması ve siber saldırılara karşı mücadele eden ya da ülke menfaatleri için yapılmakta olan siber saldırıların oluşturulmasında etkin rol oynayan personelin yetiştirilmesi konusunda özel firmalardan danışmanlık hizmeti almaktadır. Tüm dünyayı sarsan açıklamalarıyla bir anda gündem yaratan Edward Snowden de ABD gizli servisinde çalışmaya başlamadan önce Booz Allen Hamilton firmasında çalışmıştır. BAH ve benzer yapıdaki firmalar, personel ve hizmet konularında danışmanlık hizmeti vermesinden ötürü, gizli servislerin arka bahçesi olarak da adlandırılmaktadır.

Günümüz bilgi teknolojilerinde yaşanan gelişmeler, internetin yaygın kullanımı, sosyal medya vb. platformların hızla yayılması ve üretilmekte olan cihazların donanımsal güçlerinin artmasıyla birlikte kamu ve özel sektör alanlarındaki çalışma yöntemlerinde de büyük değişimler yaşanmaktadır. Bundan yıllar önce çevrimdışı, matbu belgeler üzerinden, günler hatta haftalar süren devlet işlemleri

yürütülmekteyken, bugün tek bir tıkla, internete bağlı herhangi bir cihaz üzerinden anında tüm devlet işleri yapılabilir hale gelmiştir.

Bir başka deyişle devletler ve vatandaşlar, bilgi teknolojileri ve bilgi altyapılarına bağımlı haldedir. Dolayısıyla da devletlerin artık siber saldırılara karşı çok daha hassas olduğunu söylemek mümkündür. Devletler, gerek vatandaşlarının bilgileri ve kritik altyapılarını korumak gerekse de kamu kurumlarında bulunan hassas bilgilerin diğer devletler ya da terör örgütlerinin eline geçmesini engellemek için siber uzay üzerinden gerekli faaliyetleri yürütmelidir.

Bilgi Çağı'ndan önce devletler, birbirlerine karşı üstünlük kurmak ve diğer ülkere karşı caydırıcı olması amacıyla konvensiyonel silah teknolojilerine yatırım yapmaktayken, günümüzde siber silahlar, siber güvenlik, siber savaş ve siber istihbarat gibi kavramlar üzerine eğilmekte ve bu konuda yatırımlar yapmaktadır. Diğer taraftan, vatandaşların dijital kimliklerinin korunması için de gerekli tedbirleri almaktadır. Ne yazık ki bu konuda oldukça geç davranan ülkemizde, milyonlarca vatandaşın kimlik bilgileri internete sızmış, anne-baba adı, T.C. kimlik numarası ve açık adresi gibi bilgiler kötü amaçlı kimseler tarafından rahatça ulaşılabilmiştir.

Buradaki hataların başında, geliştirilen sistemlerin güvenlik standartlarına uygun olmaması gelmektedir. Veritabanındaki kimlik bilgileri şifrelenmek yerine, düz metin halinde saklanmıştır. Verilerin kolayca elde edilmesini engellemek için shifting adı verilen bir yöntem kullanılmıştır. Ancak bu yöntem, herhangi bir şifreleme yöntemi olmadığından basitçe çözümlenmiş ve veriler düz metin haline getirilmiştir. Günümüzde, evlere telefon açarak, kurbanın kimlik bilgilerini verdikten sonra, güven kazanmak ya da korkutmak gibi psikolojik faaliyetlerin ardından gerçekleştirilen dolandırıcılık faaliyetlerinin büyük bir kısmı, bahsi geçen kimlik sızdırma vakası sebebiyle meydana gelmektedir.

İnternetin gelişmesiyle birlikte ortaya çıkan e-devlet kavramı, vatandaş-devlet arasındaki bağın güçlenmesine ve hızlanmasına imkan tanırken, zafiyetleri de beraberinde getirmektedir. Ancak burada söz konusu olan, zafiyetlerin kendisi değil,

aslında bu sistemleri koruyacak bilgi ve beceriye sahip teknokratların eksikliğidir. Siber uzaydaki sistemlerde sürekli olarak zafiyetler tespit edilmekte ve çeşitli web siteleri, forumlar vb. üzerinden paylaşılmaktadır.

Dahası bugün, gelişmiş antivirüs ve siber güvenlik firmalarının dahi hacklendiği görülmektedir. Dolayısıyla kamu kurumları bünyesinde yaşanan olayların da sıradışı olmadığını söylemek mümkündür. Ancak kamu kurumları, devlet hizmeti verdiğinden, kamu güvenliğini tehdit edebilmektedir. Bu sebeple de devlet bünyesinde gerçekleştirelen e-hizmetlerin standartlara uygun ve yetkin kişiler tarafından verilmesi gerektiği artık kaçınılmaz bir gerçektir.

E-devlet çalışmalarının İngiltere ve Kanada'da 1990'lı yılların ortasında başladığı görülmüştür. Microsoft'un katkılarıyla gerçekleştirilmiş olan Birleşik Krallık Geçit Projesi ile 200 merkezde bulunan 482 adet devlete bağlı kurum ve kuruluşun birbirine bağlanması sağlanmıştır. Bu projenin bir diğer amacı da kamu görevlilerinin, çalışmalarını elektronik ortama taşımaktır. Taşınma işlemiyle birlikte işlemlerin hızında artış sağlanmıştır. Arjantin'de sürücü belgelerinin akıllı karta dönüştürülmesi işlemi ise 1995 yılında başlamıştır.

Dört yıl süren bir çalışmanın ardından sürücü belgesi, araç ruhsatı ve araç vergisiyle ilgili bilgiler tek bir akıllı kart üzerinde birleştirilmiştir. Finlandiya'da da aynı yıl benzer bir çalışma yapılmış olup, vatandaşların akıllı kimlik kartı uygulaması sayesinde dijital imza, internet ve bürokratik işlemleri kolayca yapmalarına imkan tanınmıştır. İspanya da vergi matrahının internetten öğrenilip, ilgili formların çevrimiçi doldurularak, ödemenin de internet üzerinden yapılmasına imkan tanıyan bir sistem geliştirmiştir. Bu uygulama sayesinde İspanya'da bürokratik engeller aşılmış, vergi ödeme işlemi hızlandırılmıştır.

Singapur da 1997 yılından beri e-vatandaş geçit kapısıyla vatandaşlarına aralarında eğitim, sağlık, ulaşım ve seyahat, iş bulma, barınma gibi konularla ilgili olarak 150 farklı birimde hizmet verebilmektedir. ABD'deyse e-devlet çalışmalarının daha çok yerel yönetimler tarafından desteklendiği görülmektedir. E-öğrenme de

ABD'nin üzerinde durduğu bir başka önemli konudur. Bu konu kapsamında sanal kampüslerde 2002 yılından beri devlet görevlilerine eğitim verildiği görülmektedir. Liberya da ilginç bir diğer örnek olarak karşımıza çıkmaktadır.

Ülkede 2000 yılından beri vatandaşa kaliteli ve hızlı hizmet sunmak amacıyla geliştirilmiş olan e-devlet projesi ile halkın refahı artırılmaktadır. Bu hizmet ayrıca, devletin sahibi olduğu bir online kumarhanenin işletilmesi için de kullanılmaktadır. Bu örneklerden açıkça görüldüğü üzere, 1990'lı yıllardan beri devletlerin siber uzaydaki varlıkları ve faaliyetleri gelişim göstermektedir. Bu gelişmelere ayak uyduramayan devletler, siber savaşlardan mağlup gelmek ve hatta yıkılmaya mahkumdurlar (Çakmak ve Altunok, 2009, s.142-143).

Türkiye Cumhuriyeti Devleti de vatadanşlarına kolay, hızlı ve kaliteli hizmet verebilmek için e-devlet uygulamaları geliştirmiştir. Oldukça başarılı olan e-devlet sistemi sayesinde birçok işlem artık anında yapılabilmektedir. İnternet erişiminin olduğu her an, her noktadan vatandaşlaık hizmetleri almak mümkündür. Ancak; vatandaşa daha iyi ve hızlı hizmet vermek için geliştirilmiş olan e-devlet uygulamaları, tehlikeleri de beraberinde getirmektedir.

E-devlet altyapılarına yapılacak saldırılar neticesinde vatandaşların bilgilerine ulaşılabileceği gibi, bu sistemlerin tamamen yok edilmesi veya verilerin değiştirilmesi gibi faaliyetler sonucu kamu düzeninde bozulma gibi sonuçlarla karşılaşılabilir. Daha önce sözünü ettiğimiz, vatandaşlara ait T.C. Kimlik numaralarının sızdırıldığı veritabanında, belli adreslere yönelik yapılan aramalar neticesinde, sızdırma operasyonun gerçekleştiği dönemde devlete ait kolluk kuvvetleri ile istihbarat teşkilatlarındaki çalışanlar ve hatta ailelerinin isimlerine kadar ulaşılabilmektedir. Bu basit arama ile elde edilecek bilgiler dahi istihbarata karşı koyma faaliyetleri açısından büyük bir sorun teşkil etmektedir. İstihbarat personelinin kendi bilgilerinin korunamadığı bir sistemde, vatandaşın güvenliğinin sağlanması beraberinde soru işaretlerini de getirmektedir.

Siber istihbarat ve siber istihbarata karşı koyma faaliyetleri, geleneksel istihbarat faaliyetleriyle çeşitli konularda benzerlik göstermektedir. Yabancı devletlerin operasyonlarında görüldüğü üzere kimi zaman yardımcı unsur kimi zamansa birincil unsur olarak kullanılmaktadır. Siber uzay üzerinden örtülü operasyonlar düzenlemek, sosyal medya aracılığıyla propaganda yapmak, istihbarat toplamak ve siber saldırılar düzenleyerek yetkisiz erişim sağlayarak gizli bilgilere ulaşmak mümkündür.

Bu faaliyetlerin etkin kullanılması halinde, potansiyel terör faaliyetlerin önüne de geçilebilmektedir. Potansiyel ya da tespit edilmiş örgüt elemanlarının internet trafiklerinin dinlenmesi, bilgisayar ya da mobil cihazlarına hacking faaliyetleriyle sızmak ve buna bağlı olarak sistemdeki verileri elde etmek, analiz etmek suratiyle istihbarat toplamak önleyici faaliyetler kapsamında değerlendirilebilmektedir.

Son dönemde gizli servislerin önem verdiği konulardan biri de TOR vb. sistemlerle birlikte VPN kullanımıdır. Terör örgütleri, şifreli haberleşme yaptıklarından, kolluk kuvvetleri ya da istihbarat teşkilatlarının bu haberleşmeyi dinlemeleri neredeyse imkansız hale gelmektedir. Diğer taraftan, kullanılmakta olan anında mesajlaşma uygulamalarının da uçtan uca şifreleme desteği sunması, yine trafiğin dinlenmesi konusunda engel oluşturmaktadır. Ancak yine de bunların üstesinden gelmek mümkündür. Haberleşmenin sürekli olarak yetkili birimler tarafından dinlenmesi, gözlemlenmesi potansiyel tehlikelerin önüne geçme konusunda büyük önem arz etmektedir.

Diğer taraftan, sosyal medyanın takip edilerek, gerekli analiz araçlarının kullanılması halinde de mevcut olarak internetteki gelişmelerden ya da belirli bir konudaki yorumlardan, plan ve politika geliştirmek mümkün olmaktadır. Yaşanan güncel bir siyasi olayın ardından, sosyal medya üzerindeki yorumların incelenmesi, oluşabilecek toplumsal olayların önüne geçme konusunda yardımcı olmaktadır.

Halka infiale sürükleyecek yorumların kimler tarafından yapıldığını tespit etmek de yine siber istihbarat faaliyetleri kapsamında yer almaktadır. Gerçek hayatta karşılaşılan potansiyel tehlikeler ve bunların kimler tarafından yapıldığının tespiti,

siber uzayda da aynı kolluk kuvvetleri ve istihbarat teşkilatları tarafından gerçekleştirilmektedir. Bu sebeple, ilgili birimlerde çalışan personelin istihbarat, istihbarata karşı koyma ve siber güvenlik konularında yeterli bilgi ve beceriye sahip olması gerekmektedir.

Gizli haberleşmenin önemli ögelerinden biri olan şifreleme, terör örgütleri tarafından da etkin bir şekilde kullanılmaktadır[56]. Şifreleme desteği, bugün artık birçok anlık mesajlaşma uygulamalarıyla öntanımlı olarak gelmektedir. Dünyanın en çok kullanılan anında mesajlaşma uygulamalarından Whatsapp da Open Whisper Systems ile birlikte yaptığı çalışmayla birlikte, uçtan uca şifreleme desteği sunmaya başladı[57]. Bir başka deyişle, günümüzde sıradan mesajlaşma uygulamalarıyla dahi yapılan iletişim, eskisi kadar kolay ele geçirilememektedir. Çeşitli siber saldırı yöntemleriyle, mesajlaşmanın yapıldığı trafik dinlense dahi, veri şifrelenmiş olduğundan, elde edilen verinin ayrıca deşifre edilmesi gerekmektedir.

NSA ve GCHQ gibi istihbarat teşkilatları, kriptografi uzmanları ve süper bilgisayar aracılığıyla bu tür şifreleri kırabilmektedir. Dolayısıyla bu tür kurumların, şifreleme desteği bulunan Telegram, Signal, WhatsApp vb. uygulamalar üzerinden gerçekleştirilen iletişimi deşifre ettiği düşünülmektedir. Ancak yine de bu kurumların da çoğu noktada çaresiz kaldığı görülmektedir. Özellikle TOR ağları üzerinden gerçekleştirilen iletişimin dinlenmesi konusunda büyük sorunlar yaşanmaktadır.

İstihbarat teşkilatları tarafından düzenlenen raporlarda, çeşitli terör örgütlerinin, saldırı planları ve yönetimini siber uzay üzerinden, benzer şifreleme yöntemlerini kullanarak gerçekleştiği yer almaktadır[58]. Siber istihbarat konusunda gelişme gösterememiş ülkelerin istihbarat teşkilatları, bu konuda büyük sorun yaşamaktadır. Son yıllarda ABD ve Avrupa ülkelerine karşı düzenlenen terör eylemlerinin,

[56] http://edition.cnn.com/2015/12/17/politics/paris-attacks-terrorists-encryption, Erişim Tarihi: 18 Ocak 2018.
[57] https://whispersystems.org/blog/whatsapp-complete, Erişim Tarihi: 18 Ocak 2018.
[58] https://www.ft.com/content/965b3104-8cce-11e5-8be4-3506bf20cc2b, Erişim Tarihi: 18 Ocak 2018.

şifrelenmiş sistemler üzerinden planlanması ve yönlendirilmesi, siber istihbarat konusunun önemini bir kez daha gözler önüne sermektedir.

Bu noktada devreye teknik bilgi ve beceri dışında, hukuki boyut da girmektedir. Zira özel hayatın gizliliği, kişisel verilerin korunması gibi hukuksal kavramlar nedeniyle, bazı istihbarat teşkilatlarının, mahkeme kararı olmaksızın kişi dinleme, hackleme gibi bir yetkisi bulunmamaktadır. ABD gibi ülkeler, zamanın büyük önem teşkil ettiği bu gibi durumlara karşı e-posta, anında mesajlaşma, sosyal medya vb. hizmetler veren firmalarla anlaşarak, bu sistemler üzerinden geçen her türlü veriyi dinleyebilmektedir. Bu gibi anlaşmalar, kamu güvenliği açısından büyük önem arz etmektedir ve bu sebeple de konuya ilişkin kanunlar hazırlanmıştır. Tüm bu anlaşmalar, önleyici güvenlik faaliyeti çatısı altında hukuki boyuta dayandırılabilmektedir.

Şifreleme konusundaki bir diğer önemli konu da PGP'dir. Düz metin halinde yazılan mesaj veya dosyaları, şifreleyebilen PGP sayesinde özellikle e-posta mesajlaşmaları olmak üzere, tüm iletişim mesajları şifrelenebilmektedir. PGP, Edward Snowden'in bilgi sızdırdığı gazeteciyle, iletişim kurduğu zaman kullandığı şifreleme yöntemidir. Buradan hareketle, çoğu zaman NSA gibi gelişmiş kurumların dahi şifreleme kullanılarak gerçekleştirilen iletişimi çözme konusunda geciktiği ya da kimi zaman yetersiz kaldığı yorumları yapılabilir.

El Kaide'nin Inspire isimli dergisinde de PGP şifreleme kullanılmaktadır. Dergiye makale göndermek isteyenlerin, dergi tarafından yayınlanan genel anahtarı kullanarak PGP ile şifreleme yapması istenmektedir. Dolayısıyla dergiye gönderilecek olan makalenin önce şifrelenmesi daha sonra gönderilmesi gerekmektedir. Son yıllarda istihbarat teşkilatlarının meşgul olduğu bir başka konu da tam cihaz şifrelemedir. Cihazların gömülü şifreleme desteği, kaybolma ya da çalınma gibi durumlarda verilerin güvenli bir şekilde korunmasını sağlamaktadır. FBI'ın Apple ile yaşadığı sorunun en büyük sebebi tam cihaz şifrelemedir[59]. Tam cihaz şifreleme desteğine sahip

[59] http://www.imore.com/faq-everything-you-need-know-about-apple-encryption-and-fbi, Erişim Tarihi: 18 Ocak 2018.

telefonlarda yer alan veriler, doğrudan telefon donanımıyla kombine olarak şifrelendiğinden, klonlanamamaktadır. İstihbarat teşkilatları, internette anonimlik sebebiyle de zor durumda kalabilmektedir.

Snowden tarafından yapılan sızdırmalara göre, NSA'in her ne kadar ABD vatandaşlarını dinlenmediği savunulsa da metadata'nın toplandığı, bir başka deyişle kimin kimle görüştüğü, görüşmeni süresi gibi bilgilerin tasnif edildiği belirtilmektedir[60]. Metadata'nın toplanmasını önlemek içinse terör örgütleri TOR ve benzeri servisleri kullanmaktadır. Bu servisler aracılığıyla anonimleşen örgüt üyelerinin yakalanması da zorlaşmaktadır. Trafiğin şifrelenmiş bir şekilde birden fazla vekil sunucu üzerinden akışını sağlayan bu sistem sayesinde, sadece veriler değil, aynı zamanda metadata da analiz edilememektedir.

TOR ve benzer servislerin kullanılması, kaynak ve hedef hakkında bilgi almayı neredeyse imkansızlaştırmaktadır. FBI daha önce Stratfor sunucularını hacklediği için Jeremy Hammond hakkında soruşturma başlattığında tüm internet trafiği incelenmişti. Bu inceleme sonucunda FBI, elde ettiği verileri analiz ederek, Hammand'un yaptığı sohbet sırasında meydana gelen trafikle karşılaştırarak faili tespit etmiş ve yakalama kararı almıştır. Terör örgütlerinin aktif olarak kullandığı bir diğer haberleşme aracı da "burner phone" olarak adlandırılan, konuşma bittikten sonra mesaj ve dosyaların otomatik olarak silindiği, iz bırakmayan telefonlardır.

Bu telefonlarla birlikte kullanılan uygulamalar, underground forumlarda bulunan geliştiriciler tarafından özel olarak geliştirilmektedir. Bu uygulamalar, müşterinin ihtiyaçlarına göre değişiklik göstermektedir. Paris saldırıları sırasında da bu telefonların kullanıldığı, Fransız istihbarat servisleri tarafından ortaya çıkarılmış durumdadır[61].

[60] https://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document, Erişim Tarihi: 19 Ocak 2018.
[61] http://arstechnica.com/tech-policy/2016/03/paris-terrorist-attacks-burner-phones-not-encryption, Erişim Tarihi: 19 Ocak 2018.

Bunun önüne geçebilmek içinse devlet destekli VPN ve benzeri uygulamaların halk seviyesine indirgenmesi faydalı olmaktadır. Snowden'in sızdırdığı raporlarda da görüldüğü üzere, ABD ve İngiliz gizli servisleri hedef sistemleri sürekli olarak hacklemek yerine, doğrudan halkın indirdiği, kurduğu yazılımlara entegre ettiği arka kapılar aracılığıyla dinleme faaliyetleri yapmaktadır. Bu sayede sistem üzerindeki tüm haberleşme, doğrudan komuta merkezi üzerinden rahatlıkla dinlenebilmektedir. Bu tür sistemlerin devlet desteği ile çeşitli hacking grupları ve sivil toplum örgütleri aracılığıyla yapması faydalı olacaktır. Aksi taktirde internet kullanıcılarının güveninin kazanılması zor olmaktadır.

3.10. Siber Terörizmle İlgili Uluslararası Hukuki Düzenlemeler

Siber terörizm sadece siber uzaydaki iletişim sistemleri ile bilgi teknolojileri altyapılarıyla sınırlandırılmamaktadır. Siber uzay üzerinden yapılan, insan hayatı da dahil olmak üzere tüm altyapıları ve sistemleri tehlikeye sokan, yasalara aykırı faaliyetlerdir. Bu faaliyetleri yapmak dışında, yapan kişilere yardım ve yataklık etmek, terörizmi kışkırtmak, reklamını yapmak, finans sağlamak, terörist faaliyetlerinde bulunan ya da bulunacak kişileri eğitmek ve bu konularla ilgili olarak yasadışı yayın yapmak da siber terörizm kapsamında yer almaktadır.

Siber terörizm, gelişmiş ülkeler ve çeşitli örgütler tarafından ele alınmış ve konuya ilişkin kanuni düzenlemeler yapılmıştır. Siber terörizm, Birleşmiş Milletler Sözleşmesi'nin 41. maddesinde yer alan "Telli iletişimin diğer araçlarla kesilmesi" ifadesi dayandırılarak suç oluşturduğu yorumu yapılmaktadır. Birleşmiş Milletler Güvenlik Konseyi'nin dünyadaki barış ve güvenliği tehdit eden terörist faaliyetlerle mücadele yapılmasını öngören 1373 sayılı kararı da hukuki dayanak olarak nitelendirilebilmektedir (Çakmak ve Altunok, 2009, s.191-192).

Siber terörizmle ilgili olarak Avrupa Konseyi'nde terörizmle ilgili birim olan Avrupa Konseyi Terörizm Uzmanlar Komitesi, 2003'te 2. Avrupa Adalet Bakanları toplantısında kurulmuştur ve 16.05.2005 tarihli "Avrupa Konseyi Terörizmin Önlenmesi Konvansiyonu" oluşturulmuştur. Konvensiyonun Terör Suçu İşlemeye Yönelik Halkın Provokasyonu başlığında yer alan 5. maddeye göre, terör suçu işlemek

için halkın provokasyonu, bir mesajın halka dağıtılması ya da bir başka deyişle hazır olmasının sağlanması, terör suçlarını doğrudan ya da dolaylı olarak destekler yapıdaki hareketler olarak ifade edilmektedir[62].

Avrupa Konseyi'nin 13/06/2002 tarihli 2002/475/JHA Terörizmle Mücadele Konsey Çerçeve Kararı bulunmaktadır[63]. Bu kararda, terörizmle mücadele kapsamında siber tehditler de tanımlanmıştır. Buna göre halkı korkutmaya yönelik, hükümet ya da uluslararası örgütün çalışmalarını zorlaştırmak ya da faaliyetlerini durdurmaya yönelik faaliyetlerle, bir ülkenin ya da uluslararası örgütün siyasi, hukuki, ekonomik ya da sosyal yapılarını ciddi bir biçimde istikrarsızlaştıran ya da altyapılarına zarar vermeye yönelik faaliyetler olarak tanımlanmaktadır. Konseyin ayrıca 24/02/2005 tarihli 2005/222/JHA Bilgi Sistemlerine Karşı Saldırılarla İlgili Konsey Çerçeve Kararı da bulunmaktadır[64].

Siber terörizmin tanımlanması yolunda bir adım olan bu düzenleme yanında 24 Şubat 2005 tarihli 2005/222/JHA Bilgi Sistemlerine Karşı saldırılarla ilgili konsey çerçeve kararında madde 2 ile bilgi sitemlerine yasadışı erişim madde 3 ile yasdışı sistem müdaheles, madde 4 ile yasadışı veri müdahalesi düzenlenmektedir. NATO, siber suçlarla mücadele kapsamında Bilgisayar Olayları Mukabele Gücü'nü kurmuş, 11 Eylül sonrasında önemli altyapıların korunmasıyla ilgili çalışmalar başlatılmıştır. NATO, siber güvenlikle ilgili olarak iletişim bilgi sistemleri altyapı bileşenlerinin korunmasına yönelik gerekli güvenlik önlemlerinin alınmasını sağlamıştır. Siber Savunma Politikası hedefi altında NATO, siber saldırılara karşı önem arz eden tüm iletişim ve bilgi sistemlerinin korunmasını, ittifak üyelerine sağlamak için NATO yeteneğinin kuvvetlendirilmesi konusunda müdahalelerde bulunmuştur. NATO'nun en üst karar organı olan Kuzey Atlantik Konseyi, Siber Savunma Programı'nı desteklemektedir. Bu anlamda üye ülkelere gerekli personel ve bilginin sağlanmasıyla

[62] https://rm.coe.int/168008371c, Erişim Tarihi: 19 Ocak 2018.
[63] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=LEGISSUM%3Al33168, Erişim Tarihi: 20 Ocak 2018.
[64] http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32013L0040, Erişim Tarihi: 20 Ocak 2018.

ilgili de çalışmalar düzenlenmektedir. NATO ayrıca çeşitli dönemlerde siber güvenlikle ilgili stratejiler geliştirmektedir[65].

3.11. Türkiye'de Siber Güvenlik Firmalarına İlişkin Bulgular

Türkiye'de, siber güvenlik ya da siber istihbarat gibi konulara ilişkin çalışmalar aslında uzun yıllardır yapılmaktadır. Henüz ilgili kamu kurumları kurulmamış, personel istihdam edilmemişken, internetin Türkiye'de yaygınlaştığı yıllardan beri siber güvenlikle ilgili uzmanlar, çalışmalar yapılmaktadır. Bu uzmanlardan bazıları, uluslararası arenada isim yapmış, önemli sistem açıkları keşfetmiş ve siber güvenlikle ilgili düzenlenen yarışmalarda derecelere girmiş kişilerdir.

Çalışmada, sözü edilen kişilerin yönetici olduğu firmalarla anket yapılarak, siber güvenlikle ilgili personel yapısının, özel sektörde nasıl olduğu incelenmiştir. Uzun yıllardır elde edilen bilgi birikimi ve tecrübenin yanısıra, yurt dışındaki siber güvenlik firmalarının yapılarını da inceleme şansı bulmuş bu kişilerin oluşturduğu sistemin bir benzerinin, kamu sektörüne de uygulanabilmesi halinde, devlet çapında siber güvenlik ve siber istihbarat faaliyetlerinin daha etkin bir şekilde yapılacağı düşünülebilir.

Çalışmada kamu kurum ve kuruluşlarına siber güvenlikle ilgili danışmanlık hizmeti vermekle birlikte, görevli personelin eğitimini gerçekleştirmiş ya da gerçekleştirmekte olan kişilerle anket yapılmıştır. Türkiye'de siber güvenlik ve buna bağlı olarak siber istihbarat gibi konulara ilişkin çalışmalar yapmakta olan firma sayısı henüz oldukça az olduğundan, ankete alanında başarılı, on farklı firmadan yöneticiler katılım sağlamıştır. Ankete katılan yöneticilerin bağlı olduğu bu on firma, sektörün en iyileri arasında yer almaktadır.

Katılım gösteren firma ve yönetici isimlerinin paylaşılması, güvenlik açısından sakıncalı olduğundan, bu çalışmada gizli tutulmuştur.

[65] https://ccdcoe.org/cyber-security-strategy-documents.html, Erişim Tarihi: 20 Ocak 2018.

Tablo 7: Firmalarda Görevli Siber Güvenlik Uzmanı Sayısı

Görevli Uzman Sayısı	**Yüzde (%)**
1-5	45.5
6-10	36.4
10'dan fazla	18.2

Tablo'ya göre siber güvenlik firmalarında görev alan uzman sayısı %45 oranında 1 ila 5, %36.4 oranında 6-10 ve %18.2 oranında 10'dan fazladır. Siber güvenlik konusunda önemli olan, temel olarak nicelikten ziyade nitelik olmakla birlikte, diğer birimlerde çalışan personel sayısının fazla olması, siber tehdit unsurlarının her geçen gün gelişmesi ve saldırıların artması gibi sebeplerden ötürü, siber güvenlik uzmanı sayısının da artması gerekmektedir.

Mevcut olan siber güvenlik uzmanlarının, genel anlamda %45'lik dilim içinde yer almasının sebebi, ülkedeki siber güvenlik uzman sayısının düşük olması gösterilebilir. Yeterli sayıda uzman olmaması sebebiyle, ilgili birimlerdeki görevli personel sayısı da buna bağlı olarak düşük olmaktadır.

İlerleyen günlerde, özellikle AB üyesi ülkeler başta olmak üzere, çeşitli ülkelerdeki bilgi güvenliğine ilişkin regülasyonların zaruret haline gelmesiyle birlikte, ülkemizde de benzer çalışmalar ışığında, siber güvenlik uzmanına olan ihtiyaçta artış görülecektir.

Diğer taraftan, ankete katılan uzmanların nitelikleri, sektörde yer alan birçok siber güvenlik çalışanına göre kıyaslanamayacak kadar yüksek olup, bu kurumlarda çalışmak üzere görevlendirilen yeni siber güvenlik araştırmacılarının, kıdemli uzmanlarca eğitilecek olması da önümüzdeki günler için bir umut niteliği taşımaktadır. Ancak mevcut duruma bakıldığında, gerek özel sektör gerekse de kamudaki siber güvenlik uzmanı ihtiyacının karşılanabilmesi için sıkı bir eğitim programının uygulanması, bu konuda devletin özellikle gerekli desteği göstermesi gerekmektedir.

Tablo 8: İşe Alım Sırasında Özel Test Uygulaması

İşe Alım İçin Özel Test Uygulaması	**Yüzde (%)**
Çoktan seçmeli test	9.1
CTF (Capture the Flag)	18.2
Hem Test hem CTF	36.4
Sınav yapılmamaktadır	36.4

Tablo'ya göre, firmalarda işe alım süreçlerinde çeşitli sınavların uygulandığı görülmektedir. Buna göre ankete katılan firmalardan %9.1'i personel alımı sırasında, çoktan seçmeli test, %18.2'si tatbiki sınava dayalı CTF (Capture the Flag) yarışması, %36.4'ü de hem test hem CTF aşamaları uygulamaktadır.

Geri kalan %36.4 ise herhangi bir sınav yapmamakla birlikte, adayın iş tecrübesine bakmaktadır. Siber güvenlik, ülkemizde henüz ilgi duyulmaya, dahası gerektiği önemi görmeye başlayan bir alan olduğundan, az önce de değinildiği üzere yeterli sayıda siber güvenlik uzmanı bulunmamaktadır.

Bu sebeple firmalar, adaylarda olması gereken bir takım özellikleri göz ardı edebilmektetir. Dolayısıyla da yükün büyük bir kısmı yine sözü edilen siber güvenlik uzmanlarına düşmektedir. ABD gibi ülkelerde, devletin ilgili kurumlarında çalıştırılacak personelin, CTF gibi sınavlara girdiği görülmektedir.

Bu sınavlar, başvuran kişinin gerekli bilgi ve beceriye sahip olup olmadığını büyük oranda gösterebilmektedir. Kimi zaman yazılı sınavlar, özellikle liyakat sistemine dayalı olmayan örgütlerde, iktidara yakın kimselerin ya da bu kimselerin tanıdıklarının kuruma girmesine yönelik prosedürlerden ibaret olduğundan, CTF gibi beceriye dayalı sınavlar, bu sistemin de otomatik olarak çökmesini, personel alımlarının tamamen liyakat sistemine dayanmasını sağlamaktadır.

Adayın bilgi ve beceri seviyesinin tespitine matuf gerçekleştirilen bu testlerle birlikte, kritik altyapıların emanet edildiği kimselerin, bilhassa kamuya hizmet veren

özel siber güvenlik firmalarında çalışması halinde bir takım güvenlik tahkikatlarından geçmesi faydalı olacaktır. Zira bu kimselerin, iç hulul tehditi oluşturabilme potansiyeli yüksek olup, bu tehdidin tespit edilmesi de diğer siber güvenlik zafiyetlerine göre de daha zor olmaktadır.

ABD gibi ülkelerin, siber istihbarat faaliyetlerini etkin bir şekilde gerçekleştirebilmesinin en önemli sebebi budur. Bu tip ülkelerde ayrıca, devletin gizli servislerinde çalışan kişilerin, daha önce çeşitli danışmanlık firmalarında görev yaparak alanındaki uzmanlığını ispatladığı ve geliştirdiği görülmektedir. Bu konuyla ilgili olarak en başarılı örneklerden biri Edward Snowden gösterilebilir.

Tablo 9: Siber Saldırı ve İstihbarat Faaliyetleri

Siber Saldırı/İstihbarat Uygulaması	**Yüzde (%)**
Etik hacking	74.7
Laboratuvar ortamı	27.3

Bu kurumlarda görevli personelin, sadece siber güvenlik değil, aynı zamanda etkin bir şekilde siber saldırı ve siber istihbarat faaliyetleri yapabildikleri de görülmektedir. Bu kişiler, siyah şapkalı bir hacker'ın gerçekleştirebileceği tüm faaliyetleri, yasal zemin çerçevesinde uygulayabilmektedir. Ancak tabloda da görüldüğü üzere firma içinde doğrudan saldırı faaliyetlerinin gerçekleştirilmesi yasak olup, %27.3 oranında sadece laboratuvar ortamında saldırı yapılmaktayken, %74.7 oranında etik hacking kapsamında saldırılar gerçekleştirilmektedir.

Siber istihbarat faaliyetlerinin gerçekleştirilebilmesi için, siber saldırı yöntemlerinin iyi bilinmesi ve uygulanması gerekmektedir. Aksi takdirde istihbarat oluşturmaya yönelik, hedef sisteme sızma gibi konularda başarısız olunacaktır. Siber istihbaratın önemli ögelerinden biri de HACKINT'tir.

Hedef sistemi hacklemeye yönelik gerçekleştirilen bu istihbarat faaliyetleri, bugün ABD dahil, siber saldırı konusunda nitelikli personele sahip devletler

tarafından, aktif bir istihbarat oluşturma kapsamında yer almaktadır. Konuya ilişkin, son dönemde sızdırılan Vault 7 belgeleri, hedef sisteme sızmak, sistem üzerinde kalıcı yetkiye sahip olmak, izleri silmek ve uzaktan erişimle istenilen bilgiye ulaşmak gibi çalışmaların, ne derece önemli ve yaygın olduğunu göstermektedir.

Tablo 10: Mavi Takım – Kırmızı Takım Başarı Oranı

Takım Türü	**Yüzde (%)**
Mavi takım	70.6
Kırmızı takım	29.4

Ankete katılan firmaların %36.4'ünde mavi takım - kırmızı takım ayrımı bulunmamaktadır. Geri kalan %36.4'ünde ise bu ayrımı gerçekleştirebilecek bir test ortamı kurulmamıştır. Firmalardan %27.3'üyse saldırı ve savunma takımları oluşturmuş olup, bu takımların içinde aktif rol oynayan personelin %70.6'sının mavi takımda, %29,4'ününse kırmızı takımda daha başarılı olduğu görülmektedir.

Siber güvenlikle ilgili çalışmalar yapan kişiler genellikle savunmaya yönelik beceri geliştirmektedir. Bu durum, yanlış olmamakla birlikte büyük bir eksiklik olarak nitelendirilebilir. Zira, sürekli vurgulandığı gibi, başarılı bir siber istihbarat için, siber saldırıların da aynı oranda etkin bir şekilde gerçekleştirilmesi gerekmektedir. Siber saldırıların anatomisi, temel olarak aynı gibi görünse de hedef sistemin altyapısına göre değişiklik göstermektedir.

Hedef ne olursa olsun, doğru saldırıların yapılmaması halinde, istihbarat faaliyetlerinde de başarı beklemek yanlış olacaktır. Diğer taraftan, en iyi savunmanın saldırı olduğunu hatırlayarak, bir siyah şapkalı hacker gibi düşünmek de siber güvenlik çalışmalarında önemli fayda sağlayacaktır. Bu bağlamda, siber güvenlik birimlerinde belli periyotlarda, rotasyon sistemine dayalı, mavi-kırmızı takım ayrımı yapılmalı ve saldırı-savunma senaryoları üzerinden tatbikatlar gerçekleştirilmelidir.

Tablo 11: Personelin İş Tecrübesi

Toplam Çalışma Süresi	**Yüzde (%)**
1-2 yıl	9.1
3-5 yıl	36.4
6-10 yıl	54.5

Firmalarda görevli siber güvenlik personelinin yıla göre iş tecrübelerinin dağılımı ise şu şekildedir. %9.1 oranında 1-2 yıllık tecrübeye sahip personel, %36.4 oranında 3-5 yıllık tecrübeye sahip personel, %54.5 oranında 6-10 yıllık tecrübeye sahip personel, aktif görev almaktadır.

Ankete katılan siber güvenlik uzmanlarının büyük bir kısmının, alanında on yıldan fazla tecrübesi bulunmaktadır. Proje yönetimi, güvenlik mimarisinin oluşturulmlası, personelin eğitimi gibi konularda aktif rol oynayan bu uzmanlar, uzun yıllar elde ettikleri bilgi birikimi sayesinde, siber olaylara anında müdahale etme yeteneğine sahiptir.

Bu yeteneğin, takım liderinden başka, diğer personelde de olması gerektiğinden, takım içerisinde mümkün olduğunda fazla tecrübeli personelin olması, çalışmaların da verimini artırmaktadır. Bu kapsamda, sözünü ettiğimiz siber güvenlik uzmanı açığının bir an önce en aza indirilmesi, gerçekleştirilecek saldırı ve savunma tatbikatlarıyla, tecrübe açığının kapatılması gerekmektedir.

Tablo 12: Personelin Sahip Olduğu Yeterlikler

Ek Yeterlilik	**Yüzde (%)**
Yabancı dil bilgisi	90.9
En az lisans diploması	9.1
İlgili bölüm mezuniyeti	18.2

Görevli siber güvenlik personelinin, sadece mesleki becerisi değil, aynı zamanda özellikle yabancı dil başta olmak üzere farklı özelliklere de sahip olması beklenmektedir. Buna göre, firmalarda görev yapan siber güvenlik personelinin %90.9'u yabancı dil bilmektedir. %9.1'i en az lisans diplomasına sahipken, %18.2'si ilgili bölümden mezundur.

Yabancı dil gereksinimi, teknik dokümanları okuyup anlayabilecek kadar olup, daha fazlası, özellikle yabancı yayınların takip edilmesi anlamında büyük kolaylık sağlayacaktır. Siber uzaydaki teknolojilerin ve buna bağlı olarak meydana gelen siber saldırı ve savunma metodolojileri, hızlı bir şekilde değişim göstermektedir. Bu değişime ayak uydurabilmek için ilgili personelin, siber tehdit istihbaratı raporlarını inceleyebilmesi, raporlarda yer alan tüm bilgi ve bulguları en ince ayrıntısına kadar anlayabilmesi gerekmektedir.

Gerek beyaz şapkalı gerekse de siyah şapkalı hacker unvanına sahip, Türkiye'de siber güvenlik konusuna ilişkin uzun yıllardır aktif rol oynayan kişilerin büyük kısmı, ilgili bölüm mezunu değildir. Dahası, bu kişiler arasında lisans derecesine sahip olmayanlar da yer almaktadır. Dolayısıyla, siber güvenlik uzmanı olmak için ilgili bölüm mezunu olmak gerekmemektedir.

Siber güvenlik ve benzeri konulara ilişkin, Türkiye'deki üniversitelerde sözünü ettiğimiz kırmızı takım-mavi takım çalışmalarıyla CTF'ler düzenlenmediği takdirde, verilen eğitim teoriden öteye geçmeyecektir. Personelin lisans ve üzeri eğitime sahip olması ancak sahada karşılaşacağı senaryolara ilişkin pratik bilgiyi de alması oldukça önemlidir.

Tablo 13: Personelin Periyodik Eğitimi

Eğitim Aralığı	**Yüzde (%)**
6 ayda bir	54.5
Yılda bir	36.4
Hiç	9.1

Siber güvenlik firmaları, düzenli aralıklarla personeline eğitimler sunmaktadır. Masraflarının çoğunlukla firma tarafından karşılandığı bu eğitimlerle, personelin bilgi ve becersinin artmasını amaçlamaktadır. Buna göre, ankete katılan firmaların %54.5'i personelini 6 ayda bir, %36.4'üyse yılda bir eğitime göndermektedir. Kalan %9.1 ise personelini eğitime göndermemektedir. Bu eğitimlerden bir kısmı dış kaynaklı, bir kısmı iç kaynaklı yapılmaktadır.

Daha önce de vurgulandığı üzere, siber güvenlik sürekli olarak gelişim gösterdiğinden, konuya ilişkin farklı görevlerde bulunan personelin, bir diğerinin çalışma alanına müdahale etmeksizin, teorik bilgiye sahip olmasıyla birlikte, kendi alanındaki yeniliklere yönelik eğitimleri alması da personelin gelişimi açısından önem arz etmektedir.

Bazı siber güvenlik firmaları, belirli aralıklarla konusunda uzman personelini, diğer personelin bu uzmanlık alanına ilişkin bilgiye sahip olması açısından eğitmen olarak tayin etmektedir. Belli bir rotasyon üzerinden gerçekleşen bu iç eğitimler sayesinde personelin, kendi uzmanlık alanı dışındaki farklı konularda da bilgi ve tecrübe sahibi olması amaçlanmaktadır.

Tablo 14: İç ve Dış Denetim

Denetim	**Yüzde (%)**
İç denetim	27.3
Dış denetim	0.0
Hem iç hem dış denetim	54.5
Denetim yok	18.2

Bilgi güvenliği ve siber güvenlik gibi kavramların olduğu her yerde denetim de olmak zorundadır. Buna göre, ankete katılan firmaların %27.3'ü iç denetim gerçekleştirmektedir. Bu firmaların %54.5'iyse hem iç hem dış denetim gerçekleştirmektedir. Sadece dış denetime tabi olan firma yokken, hiç denetim yapmayan firma oranı ise %18.2'dir.

Dış denetim, örgütün kendi yapısı dışındaki başka örgütlerce denetlenmesini ifade etmektedir. İç denetim ise örgütün planlanan, belirlenen, hedeflenen amaçlara ulaşıp ulaşmadığını, ne ölçüde ulaştığını ortaya çıkarmak için örgütün kendi bünyesi içinde denetlenmesidir (Öztekin, 2012, s.231-232). Siber güvenlik, bilgi güvenliği gibi konularda da çeşitli denetimler gerçekleşmektedir. Bu denetimlerden bir kısmı yavaş yavaş kurallara bağlanıp, zorunluluk haline gelmektedir. Ancak genellikle siber güvenlik firmaları, kendi isteklerine bağlı olarak bu denetimlerin yapılmasını sağlamaktadır.

Bilgi güvenliğinin sağlanması, siber güvenlik faaliyetlerinin gerektiği şekilde yapılması için, iç ve dış denetim büyük önem erz etmektedir. Ankete katılan firmalar, sadece dış denetim yapmaktan kaçınırken, hem iç hem dış denetimin yapılmasından rahatsızlık duymayıp, aksine güvenlik için bir başka örgütün denetim gerçekleştirmesine rıza göstermektedir.

Buradan hareketle, kamu kurum ve kuruluşlarının da bilgi güvenliği başta olmak üzere, siber uzaydaki faaliyetlere ilişkin iç ve dış denetime tabi tutulması da zorunluluk haline getirilmeli, bu denetimi yapacak yetkin kuruluşların sayısının artırılması ve desteklenmesi gerekmektedir. Ancak bu şekilde atıl bir siber güvenlik yapısından kurtulmak mümkün görünmektedir.

Tablo 15: Personelin Eğitim Dağılımı

Eğitim Derecesi	**Yüzde (%)**
Lise	5.3
Ön lisans	29,4
Lisans	50.6
Yüksek lisans	9.6
Doktora	5.1

Ankette yer alan firmalardaki görevli personelin, farklı eğitim derecelerine sahip oldukları görülmektedir. Yöneticilerle yapılan mülakatlar neticesinde, birincil olarak personelin bilgi ve becerisine bakıldığı, ikincil olarak da diploma ya da sertifikasının ele alındığı belirtilmiştir. Görevli personelin büyük bir kısmında CEH, CPTE, CPEH, GPEN, CISSP, OSCP gibi uluslararası sertifikalar bulunmaktadır.

Bu sertifikalar, belli bir bilgi birikimi ve daha önce sözünü ettiğimiz İngilizce gibi yabancı dillerin bilinmesi halinde alınabilecek, sınavları yetkili kuruluşlarca yapılan ve uluslararası geçirliliğe sahip belgelerdir. Dolayısıyla, bilgi güvenliği ve siber güvenlik gibi konulara ilişkin uluslararası sertifikalar, dünyanın her yerinde kabul görmektedir. Bu sertifikalara sahip kişiler, ilgili konularda sahip olduğu bilgi ve beceriyi kanıtlayabilmiş, uzmanlık unvanını resmiyete dökebilmiştir.

Buradan hareketle, devletin siber güvenlik ve siber istihbaratla ilgili kuruluşlarında görevli personelin, en azından takım ya da proje yöneticisi olacakların, sertifika programlarına katılarak, resmi unvana sahip olması fayda gösterecektir. Zira bu sertifikalar belli bir süre geçerliliğe sahip olduğundan, yenilenmesi için de güncel mevzuatın takip edilmesini zorunlu kılmaktadır.

SONUÇ VE ÖNERİLER

Bilişim teknolojilerinin gelişmesi ve internetin yaygın olarak kullanılmasıyla birlikte devletler de bu gelişime ayak uydurarak, vatandaşlarına e-devlet hizmetleri vermeye başlamış, kıymetlendirilmiş belgelerini siber uzaya aktarmış ve tüm bunlar neticesinde de siber saldırıların hedefi haline gelmiştir. Siber savaş ve siber istihbarat faaliyetleri çatısı altında devletler, birbirlerine karşı üstünlük mücadelesi kurmaya çalışmaktadır. Çalışmada yer verilen yaşanmış olaylar, artık siber saldırıların konvansiyonel savaşlarda da kullanılmakta olduğunu, dahası birçok gizli bilgi ve belgeye siber istihbarat faaliyetleriyle erişilebildiğini göstermektedir.

1. İçinde bulunduğumuz bilgi çağında, devletin bekası ve kamu güvenliğinin sağlanabilmesi için siber uzayda da gerekli tedbirlerin alınması gerekmektedir. Bu tedbirlerin alınması, ülkenin kritik altyapılarına yapılacak saldırıların savuşturulması, vatandaşlara ve devlete ait hassas bilgilerin ele geçirilmesi ve ekonomik kayıpların önlenmesinde etkili olmaktadır. Bunun dışında, ABD, İngiltere, Rusya ve İsrail örneklerinde olduğu gibi, siber güvenlik ve siber savaş konularında yetenekli ülkeler, ışık hızında istihbarat elde edebilmektedir. Gerek bu istihbari faaliyetlere karşı etkin bir İKK (İstihbarata Karşı Koyma) çalışması için, gerekse de potansiyel terör faaliyetlerinin önceden tespit edilmesi ve mevcut teröristlerin teşhisi için başarılı bir siber istihbarat gücüne sahip olmak gerekmektedir.

2. Bu güç, ülkenin kritik altyapıları, siber güvenlik konusunda vatandaşın sahip olduğu farkındalık, kolluk kuvvetleri ve istihbarat teşkilatlarındaki ilgili birimlerde

görevli personelin bilgi ve becerisi gibi faktörlere bağlı olarak değişim göstermektedir. Bu noktada dikkat edilmesi gereken bir diğer önemli nokta da bu imkan ve kabiliyete sahip personelin, siber istihbarat konusunda gerekli yasal izne sahip olup olmadığıdır. Siber istihbarat faaliyetleri içerisinde yer alan yöntemlerden bazıları bilişim hukukuna bazılarıysa, mevcut istihbarat servislerinin sıkça karşılaştığı hukuksal engellere takılmaktadır. İstihbarat teşkilatları ve bu kurumlara bağlı çalışmakta olan personelin, çeşitli kanunlarla özel hakları bulunmaktadır. Yapılan yeni düzenlemelerle birlikte, istihbarat teşkilatları özellikle kamu güvenliğinin sağlanmasına ilişkin, yapılacak faaliyetlere yönelik ek yetkilere sahip olmuşlardır.

Siber güvenlik, siber saldırı, siber savaş, siber istihbarat ve siber terörizm gibi kavramların ortaya çıkmasıyla birlikte, NATO başta olmak üzere birçok uluslararası örgüt, üye ülkelere konuya ilişkin kendi yasal düzenlemelerini yapmaları konusunda tavsiyede bulunmuştur. Siber uzayda çalışmalar yapmakta olan devletler de kendilerine özgü yasalarını düzenleyerek, bilişim hukuku ve terörizmle mücadele gibi konularda gerekli direnci gösterebilecek güce sahip olmuşlardır.

3. Siber istihbarat kapsamında yapılacak olan hacking faaliyetleri ile hedef sistem ya da bu sistemi kullanmakta olan kişi/kişilerin dinlenmesi gibi çalışmalar için de gerekli hukuki düzenlemelerin yapılması gerekmektedir. İstihbarat teşkilatlarının, kamu güvenliğinin sağlanması amacıyla yapacağı bu çalışmalar, özellikle içinde bulunduğumuz terörizm ve siber saldırıların şiddetli bir şekilde tezahür ettiği bu dönemde, büyük önem arz etmektedir. Bu sebeple, ilgili birimlerin görüş ve önerileri doğrultusunda, gerekli yasal düzenlemelerin ivedilikle yapılması gerekmektedir.

4. Türkiye'de son yıllarda siber güvenlik konusunda önemli çalışmalar yapıldığı görülmektedir. Bu çalışmalara paralel olarak, kolluk kuvvetleri ve istihbarat teşkilatları başta olmak üzere, çeşitli kamu kurumlarında ilgili birimler oluşturulmaya başlanmıştır. Diğer taraftan, yıllardır siber güvenlik konusunda hizmet vermekte olan özel sektörde çalışan siber güvenlik uzmanları da gerek kamu kurumlarındaki ilgili personele verdikleri eğitimler gerekse de zafiyet taraması, sızma testi gibi siber

güvenliğe ilişkin hizmetlerle kamu güvenliği konusunda gerekli çalışmaların yürütülmesine destek olmaktadır.

5. Çalışmada, istihbarat seksiyonunda yer alan kavramlara ve mevcut siber saldırı silahları ve yöntemlerine yer verilerek, istihbarat ve siber güvenlik kavramlarının aslında girift bir yapıda olduğu vurgulanmıştır. Bir başka deyişle, etkin bir siber istihbrat ve siber İKK faaliyeti için, ilgili birimlerdeki personelin istihbarat ve İKK disiplinine sahip olması, bunun yanında da siber güvenlik konusundaki gerekli bilgi ve beceriyi kullanabilmesi gerektiğine değinilmiştir. Personelin sahip olduğu siber güvenlikle ilgili bilgi ve beceri, özel sektörde yıllardır hizmet vermekte olan, yüksek tecrübeye sahip uzmanlar tarafından eğitilmeli ve eğitim sonunda başarılı olan personel, uluslararası sertifikasyonlarla tescillenmelidir.

6. Ülkemizde, siber güvenlik sertifikalarına ilişkin bilinç henüz yeni yeni oluşmaktadır. Dolayısıyla kamu kurumlarında, siber güvenlik veya siber istihbaratla ilgili görevlerde bulunacak personelin, bu sertifikalardan en az birine sahip olması şartı koşulmalıdır. Bunun dışında, bu belgelere sahip kimselerin, ayrıca kuruma girmeden önce çeşitli tatbiki ve yazılı sınavlara girmesi de personelin bilgi ve becerisinin ne düzeyde olduğunu ispatlayacağından, artık kritik altyapıları koruyacak ya da siber istihbarat faaliyeti yapacak personelde zorunluluk haline getirilmelidir.

7. Siber güvenlik ve siber istihbarat kavramları oldukça geniş olup, içinde birçok önemli ögeyi barındırmaktadır. Siber güvenlik uzmanı olabilmek için ağ yönetimi, Linux işletim sistemi, Windows işletim sistemi, güvenlik yazılım ve donanımları, veritabanı, programlama vb. konularda bilgi ve tecrübe sahibi olmak gerekmektedir. Dahası, sözü edilen konulardan bir ya da birkaçında uzmanlık şartı da aranmaktadır. Aksi takdirde bu yeterliğe sahip olmayan kimselerin siber güvenlik uzmanı olmaları mümkün değildir.

8. Kamu personelinin, siber güvenlik uzmanı olabilmesi için devlet destekli olarak, konusunda uzman kişiler tarafından, yetkili eğitim merkezlerince eğitimden geçirilmesi de oldukça önemlidir. Günümüzde Türkiye'de 30.000'den fazla siber

güvenlik uzmanı açığı bulunduğu ifade edilmektedir. Bu açığın kapatılabilmesi için konuyla ilgili kimselerin siber güvenlik eğitimi alarak uzmanlaşması, sertifika kazandırılması sağlanmalıdır. Tüm bu sürecin ardından liyakat sistemine dayalı bir yapıyla, siber güvenlik ile ilgili pozisyonlarda personel istiham edilmelidir.

9. Siber güvenlikle ilgili uluslararası sertifikalar bugün yurtdışındaki özel kurumlarda büyük bir öneme sahiptir. Bu sertifikaların kazanılması oldukça zordur ve İngilizce bilgisi de gerektirmektedir. Dolayısıyla yeterli seviyede yabancı dil bilgisi olmayan kimselerin de siber güvenlik uzmanı olması, ileride karşılaşılabilecek saldırı yöntemleri ve zafiyetlere karşı etkin bir mücadele verme konusunda sorun oluşturabilecektir.

Bu sebeple, personel seçimlerinde yabancı dil bilgisi kriteri de oldukça önemlidir. Siber güvenlik sektörü, sürekli olarak gelişim gösterdiğinden, personelin, takım çalışmasına yatkınlık, analitik zeka, esnek çalışma saatleri gibi faktörler dışında, kendini geliştirme ve literatürü takip edebilme gibi özelliklere sahip olması gerekmektedir.

10. Siber güvenlik ve siber istihbarat gibi çalışmalar, Türkiye'de diğer ülkelere nazaran henüz yeni hayata geçmeye başladığından, bu konulara ilişkin bilgi ve tecrübe eksiği çok fazladır. İlgili kurumlarda görevli personelin, kendini geliştirmek için bireysel olarak mücadele ettiği bu dönemde devletin, personelin eğitimine ilişkin daha fazla destek sunması gerekmektedir.

Üniversitelerde açılan bölümlerde, konuya ilişkin eğitim veren kimselerin büyük çoğunluğunun saha tecrübesi bulunmaması sebebiyle, mezun öğrencilerin de siber güvenlik konusunda aktif rol oynaması şu aşamada pek mümkün görünmemektedir.

Bundan hareketle, gerek devletin bilgi güvenliği konusunda, gerek siber güvenlik ve siber istihbarat konularında etkin bir çalışma yapabilmesi için, öncelikli olarak uzun yıllardır bu alanda savunma ve saldırı metodolojilerini teorik ve pratik anlamda en üst seviyede bilen kişilerden destek alması, kurumsal

yapıları özel sektördeki siber güvenlik firmalarından örnek alarak hayata geçirmesi, kısa ve uzun vadede etkili olacaktır.

Hacking faaliyetleriyle uğraşan kimselerin, genellikle memur mantığından çok uzak, farklı düşünce ve hayatlara sahip olduğundan hareketle, bu kimselere çeşitli konularda, en azından bağlı bulunduğu birimlerde, özellikle kılık kıyafet başta olmak üzere bir takım ayrıcalıkların tanınması da cezbedici olacaktır.

Underground olarak tabir edilen, siber uzayın karanlık yüzünde uzun yıllar hacking faaliyetlerinde bulunmuş, çeşitli hack gruplarını yönetmiş ve hatta uluslararası üne kavuşmuş kimselerden istifade edilebilmesi için, çalışma saatleri konusunda da esnek olunması fayda sağlayacaktır. Bu kişiler, kimi zaman gece çalışmalarında daha verimli olabilmektedir. Dolayısıyla bu kriterin de göz önünde bulundurulması önem arz etmektedir. Siber saldırılarılara karşı hızlı cevap verebilmek için, vardiyalı çalışma sisteminin de geliştirilmesi gerekmektedir.

Siber güvenlik ve siber istihbarat gibi konularda topyekün mücadele ve gelişim gösterebilmek için tüm bu konular üzerinde hassasiyetle durulmalı, özel sektörde hizmet veren siber güvenlik firmaları, model olarak örnek alınmalıdır.

KAYNAKLAR

Aid, M. M. ve Wiebes, C., *Secrets of Signals Intelligence During The Cold War and Beyond*, Franks Caas, Londra, 2001.

Aydın, A. H., *Kamu Yönetimine Giriş*, 2. Basım, Seçin Yayıncılık, Ankara, 2013.

Aygün, Z., *Daima Başarı ve İstikrar İçin Kamu Yönetimi*, Kum Saati Yayın Dağıtım, İstanbul, 2008.

Ayhan, U., *Metropol Alanlarda Kamu Güvenliği*, Kripto Kitaplar, Ankara, 2008.

Blaker, L., *The Islamic State's Use of Online Social Media*, The Journal of The Military Cyber Professionals Association, Volume 1, Issue 1, 2015.

Çakmak, H. *Terörizm*, Platin Kitabevi, Ankara, 2008.

Çakmak, H. ve Altunok, T., *Suç, Terör ve Savaş Üçgeninde Siber Dünya*, Barış Platin Kitabevi, Ankara, 2009.

Churchouse, R., *Codes and Ciphers*, Cambridge University Press, Cambridge, 2002.

Çınar, B., *Devlet Güvenliği*, İstihbarat ve Terör, Sam Yayınları, Ankara, 1997.

Çıtak, Ö., *Ethical Hacking Offensive & Defensive*, Level Kitap, Kocaeli, 2016.

Çifci, H., Her Yönüyle Siber Savaş, Tübitak Popüler Bilim Kitapları, Ankara, 2013.

Clarke, R. A. ve Knake, R. K, *Siber Savaş*, İKÜ Yayınevi, İstanbul, 2011.

Clausewitz, C., *On War, Princeton University Press*, New Jersey, 1984.

Demir, B., *Yazılım Güvenliği Saldırı ve Savunma*, 2. Basım, Dikeyeksen Yayın Dağıtım, İstanbul, 2015.

Demir, T., *İstihbarat Dünyası*, Kripto Yayınları, Ankara, 2015.

Duthel, H., *Global Secret and Intelligence Service*s, 3. Basım, BoD-Books, Norderstedt, 2014.

Ehrman, J., *What Are We Talking About When We Talk About CounterIntelligence?*, Studies in Intelligence, vol. 53, No 2, 2009

Elbahadır, H., *Hacking Interface*, 8. Basım, Kodlab, İstanbul, 2014.

Eryılmaz, B., *Kamu Yönetimi*, Der Yayınları, İstanbul, 2000.

Fritz, J. R., *China's Cyber Warefare: The Evolution of Strategic Doctrine*, Lexington Books, Maryland, 2017

Gill, P., *What is Intelligence Theory?*, Toward a Theory of Intelligence Workshop Report, 2006.

Glasersfeld, E., *Cybernetics and the Theory of Knowledge*, Section on System Science and Cybernetics, 2002.

Güven, E. ve Yılmaz, S.(Ed.), *İstihbarat Bilimi*, Kripto Basım Yayın, Ankara, 2013.

Heywood, A., *Siyaset*, 16. Basım, Adres Yayınları, Ankara, 2015.

Hirschman, A. O., *National Power and the Structure of Foreign Trade*, University of California Press, Kaliforniya 1992.

Kartal, A. ve Yılmaz, S.(Ed.), *İstihbarat Dünyası*, Kripto Basım Yayın, Ankara, 2015.

Keleştemur, A, *Siber İstihbarat*, Level Kitap, Kocaeli, 2015.

Köseli, M., *İstihbarat: Temel Hususlar ve Güncel Konular*, Adalet Yayınevi, Ankara 2011.

Kösereli, V., *İstihbarat Hukukuna Giriş*, Ekin Yayınevi, Bursa, 2015.

Lormel, D. M., *Terrorism and Credit Card Information Theft*, Shift 4 Secure Payment Processing, 2007.

Lowenthal, M. M., *Intelligence: From Secrets to Policy*, 5. Basım, Sage Publishing, Londra, 2012.

Macrakis, K., *Technophilic Hubris and Espionage Styles during the Cold War*, ISIS A Journal of the History of Science Society,101,2: 378-385, 2010.

NATO, *Open Source Intelligence Handbook*, 2011.

Nicholls, D., *Napoleon: A Biographical Companion*, ABC-CLIO, 1999.

OPSEC Support Staff, *Intelligence Threat Book*, Diane Publishing, Collingdale, 1996.

Özdağ, Ü., *İstihbarat Teorisi*, Kripto Yayınları, Ankara, 2013.

Özkan, T., *MİT'in Gizli Tarihi*, Alfa Yayınları, 19. Basım, İstanbul, 2005.

Öztekin, A., *Siyaset Bilimine Giriş*, 9. Basım, Siyasal Yayınevi, Ankara, 2014.

Öztekin, A., *Yönetim Bilimi*, 5. Basım, Siyasal Yayınevi, Ankara, 2012.

Pamukoğlu, O., *Savaş Sanatı*, İnkılap Yayınevi, İstanbul, 2014.

Rid, T. ve McBurney, P., *Cyber-Weapons*, The RUSI Journal, 2012.

Seyrek, Ö., Ziya, Ö.(Ed.), *Jandarmanın Görev ve Yetkileri-I*, Anadolu Üniversitesi, Eskişehir, 2013.

Smith, R., *A Call For The Integration of "Biographical Intelligence" Into The National Intelligence*, Policing: A Journal of Policy and Practice, Volume3, Issue2,191-199, 2009.

Şenol, M., *Siber Güçle Caydırıcılık Ama Nasıl?*, Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 2(2):10, 2016.

Tsfati, Y. ve Weimann, G., *www.terrorism.com: Terror on the Internet, Studies in Conflict & Terrorism*, 25:317-332, 2002.

Tzu, S., *Savaş Sanatı*, 3. Basım, Çev: Demir, A., Kastaş Yayınevi, İstanbul, 2008.

Wafe, T. W., *Inside CIA's Private World Declassified Articles from The Agency's Internal Journal 1955-92*, Yale University Press, Londra, 1995

Warner, M., *Wanted: A Definition of "Intelligence*", Studies in Intelligence, Vol46, No3, 2002.

Weir, A. Henry VIII*, The King and His Court*, Ballantine Books, New York, 2008.

Wettering, F. L., *The Internet and the Spy Business*, International Journal of Intelligence and CounterIntelligence, 14:342, 2001.

Wilkinson, P., *Terrorism versus Democracy*, 3. Basım, Routledge, New York, 2011.

Winock, M., *Terrorism, l'histoire d'un mot*, L'Histoire, no259/11, 2001.

Yayla, Y., *İdare Hukuku*, 2. Basım, Beta Basım, İstanbul, 2009.

EKLER

EK 1. ANKET FORMU

Değerli katılımcı,

Bu anketin amacı, kamu kurum ve kuruluşlarına, eğitim ve danışmanlık hizmetleri vermekte olan özel siber güvenlik firmalarının, örgütsel yapısını ve personel özelliklerini incelemektir. Anket uygulaması sonucu elde edilecek veriler, İstanbul Gedik Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Yüksek Lisans Programı tez çalışmasında kullanılacaktır.

Ankete vereceğiniz doğru cevaplar, kamu kurum ve kuruluşlarında siber güvenlik ve siber istihbarat faaliyetlerinin daha etkin olması konusunda fayda sağlayacaktır. Vermiş olduğunuz cevaplar, akademik bir çalışmada kullanılacak olup, verilen bilgiler kesinlikle gizli tutulacaktır. Göstermiş olduğunuz ilgiye teşekkür ederim.

Saim Atalay Keleştemur
İstanbul Gedik Üniversitesi Sosyal Bilimler Enstitüsü
Siyaset Bilimi ve Kamu Yönetimi
sakelestemur@gmail.com

İsim Soyisim :

E-posta Adresi :

Çalışmakta olduğunuz kurum :

Görev aldığınız pozisyon ve unvanınız :

1. Biriminizde görevli siber güvenlik uzmanı sayısı kaçtır?

a) ☐ Hiç yok b) ☐ 1-5 c) ☐ 6-10 d) ☐ 10'dan fazla

2. Bu görevlilerin kaçı uluslararası sertifikaya sahiptir?

Sayı: …….. Yüzde: ……..

3. Kurum içinde kabul gören uluslararası sertifikalar hangileridir?

a) ☐ CEH b) ☐ CISSP c) ☐ CPEH d) ☐ GPEN e) ☐ OSCP

f) ☐ CPTE g) ☐ Diğer

4. Personel, işe alım sırasında herhangi bir özel test ve CTF (Capture the Flag / Bayrağı Yakala) aşamalarından geçmekte midir?

a) ☐ Çoktan seçmeli test b) ☐ CTF c) ☐ Test yapılmamaktadır

5. Personel siber güvenlik dışında, siber saldırı becerisine de sahip midir?

a) ☐ Evet, ethical hacking kapsamında her şeyi yapabilir

b) ☐ Sadece laboratuvar ortamında yapabilir

c) ☐ Hayır, sadece siber güvenlik çalışmaları yapabilir

6. Kurum içinde kırmızı takım ve mavi takım çalışmaları yapılmakta mıdır? Yapıyorlarsa bu takımların başarı oranlarını yazınız.

a) ☐ Evet yapılmaktadır b) ☐ Hayır yapılmamaktadır

…….

7. Personelin siber güvenlik/siber istihbaratla ilgili iş tecrübesi kaç yıldır?

a) ☐ 1-2 b) ☐ 3-5 c) ☐ 6-10 d) ☐ 10 yıl ve üzeri

8. Bilgi güvenliği / Siber güvenlik ile ilgili birimlerde çalışan personelde başka hangi yeterlilikler aranmaktadır?

a) ☐ Yabancı dil b) ☐ Lisans ve üzeri diploma

c) ☐ İlgili bölümden mezuniyet c) ☐ Diğer

…….

9. Personelin konuya ilişkin eğitimleri hangi aralıklarla yapılmaktadır?

a) ☐ 6 ayda bir b) ☐ Yılda bir c) ☐ Hiç

10. Kurum ve personel iç ve dış denetimlerden geçmekte midir?

a) ☐ İç denetim b) ☐ Dış denetim c) ☐ İç ve Dış denetim d) ☐ Denetim yok

11. Personelin çalışma saatleri hakkında bilgi verir misiniz? Proaktif bir siber güvenlik için çalışma saatlerinde herhangi bir esneklik bulunmakta mıdır?

…….

12. Personelin yaş dağılımı ne şekildedir? Yanlarına sayı ve yüzdelerini yazınız.

a) 18-25 :
b) 26-35 :
c) 36-45 :
d) 46 ve üzeri :

13. Personelin eğitim dağılımları ne şekildedir? Yanlarına sayı ve yüzdelerini yazınız.

a) Lise :
b) Önlisans :
c) Lisans :
d) Lisans üstü :
e) Doktora :

14. Biriminizde daha iyi görev yapılabilmesi için sizce nasıl bir örgütlenme modeli gerekir?

a) ☐ Merkeziyetçi yönetim b) ☐ Adem-i merkeziyetçi yönetim

c) ☐ Karma Yönetim d) ☐ Diğer

…….

15. Biriminizde daha iyi görev yapılabilmesi için sizce istenilen personel özellikleri nasıl olmalıdır?

a) ☐ Aldığı emri tartışmadan uygulayan b) ☐ Aldığı emir sorgulayan, tartışan

c) ☐ Aldığı emir zamana (günlere) yayarak uygulayan d) ☐ Diğer

…….

16. Etkin bir siber istihbarat için sizce ne gibi değişikliklerin yapılması gerekmektedir?

a) ☐ Örgütsel yapıda değişiklik yapılmalıdır

b) ☐ Personel sisteminde değişiklik yapılmalıdır

c) ☐ Her iki sistemde de değişiklik yapılmalıdır

d) ☐ Diğer

…….

17. Siber güvenlik ve siber istihbarat faaliyetleri için mevcut personel sayısı yeterli midir? (Değilse kaç olmalıdır?)

a) ☐ Yeterlidir b) ☐ Yetersizdir

…….

18. Kamu güvenliği açısından, konuya ilişkin varsa diğer önerilerinizi yazınız.

…….

…….

…….

…….

…….

İlgi gösterdiğiniz ve zaman ayırdığınız için teşekkür ederim.