T.C.

HASAN KALYONCU ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER TEZLİ YÜKSEK LİSANS PROGRAMI

TERÖRİST YAPILARIN MARJİNALLEŞTİRMESİNDE SİBER İSTİHBARAT: DAEŞ ÖRNEĞİ

YÜKSEK LİSANS TEZİ

HAZIRLAYAN

SERKAN GÖKÇE

GAZİANTEP – 2022

T.C.

HASAN KALYONCU ÜNİVERSİTESİ

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ

SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER TEZLİ YÜKSEK LİSANS PROGRAMI

TERÖRİST YAPILARIN MARJİNALLEŞTİRMESİNDE SİBER İSTİHBARAT: DAEŞ ÖRNEĞİ

YÜKSEK LİSANS TEZİ

HAZIRLAYAN

SERKAN GÖKÇE

TEZ DANIŞMANI

DR. ÖĞR. ÜYESİ MURAT ASLAN

GAZİANTEP – 2022

LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ MÜDÜRLÜĞÜNE
YÜKSEK LİSANS KABUL VE ONAY FORMU

Siyaset Bilimi ve Uluslararası İlişkiler Anabilim Dalı **Siyaset Bilimi ve Uluslararası İlişkiler** Tezli Yüksek Lisans Programı öğrencisi **Serkan GÖKÇE** tarafından hazırlanan **"Terörist Yapıların Marjinalleştirmesinde Siber İstihbarat: DAEŞ Örneği"** başlıklı tez,
04 / 01 / 2022 tarihinde yapılan savunma sınavı sonucu **başarılı** bulunarak jürimiz tarafından **Yüksek Lisans Tezi** olarak kabul edilmiştir.

Görevi	**Unvanı, Adı ve Soyadı** **Kurumu/Üniversitesi**	**İmzası:**
Jüri Başkanı	Dr. Öğr. Üyesi Bilal ULUSOY Hasan Kalyoncu Üniversitesi	
Tez Danışmanı	Dr. Öğr. Üyesi Murat ASLAN İstanbul Sabahattin Zaim Üniversitesi	
Jüri Üyesi	Dr. Öğr. Üyesi Mesut ŞÖHRET Gaziantep Üniversitesi	

Bu tez Enstitü Yönetim Kurulunca belirlenen yukarıdaki jüri üyeleri tarafından uygun görülmüş ve Enstitü Yönetim Kurulu kararı ile onaylanmıştır.

Prof. Dr. İbrahim Halil GÜZELBEY
Enstitü Müdürü

TEZ ETİK VE BİLDİRİM SAYFASI

Yüksek Lisans Tezi olarak sunduğum **‘‘Terörist Yapıların Marjinalleştirmesinde Siber İstihbarat: DAEŞ Örneği’’** başlıklı çalışmamın tarafımca, bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın yazıldığını ve yararlandığım eserlerin kaynakçada gösterilenlerden oluştuğunu ve bunlara atıf yapılarak yararlanmış olduğumu belirtir ve onurumla doğrularım. 04 / 01 / 2022

Serkan GÖKÇE

ÖNSÖZ

Son yıllarda internet ve bilgi teknolojilerindeki yaşanan gelişmeler, siber uzay denilen sanal bir dünyanın ortaya çıkarak hızla yayılmasına neden olmuştur. Yaşanan hızla yayılım siber uzayın sağladığı imkân ve kabiliyetlerin etkisiyle, hayatın içinde var olan diğer tüm alanları kısa bir sürede siber uzaya bağımlı hale getirmiştir. Ortaya çıkan bağımlılık, sağladığı imkân ve kabiliyetlerle birleşince, hem (siber terörizm adı verilen) terörist yapılanmaların faaliyetlerinin siber uzaya kaymasına hem de teröristle mücadele noktasında ihtiyaç duyulan istihbaratın siber uzay üzerinden sağlanmasına neden olmuştur. Bu sonuç istihbaratın gerek siber uzayın sağladığı imkân ve kabiliyetler ölçüsünde gerekse siber terörizmle mücadeleye yönelik etkileşimsel bir dönüşüm sürecinden geçmesiyle, siber istihbarat adı verilen yeni bir alanının oluşturulmasını sağlamıştır. Bu doğrultuda çalışmada, terörist yapılanmaların siber istihbarat taktik, teknik ve yöntemleri özelinde yapılabilecek faaliyetlerle nasıl bir konuma getirilebileceği anlatılmaya çalışılmıştır.

Bu çalışmayı sonuçlandırmamda öncelikle çalışmamın her safhasında beni yönlendiren ve desteğini esirgemeyip yoğun çalışma temposu içinde kıymetli vakitlerini ayırarak görüşleri ile katkıda bulunan değerli hocam Dr. Öğr. Üyesi Murat ASLAN'a; akabinde de rahat bir çalışma ortamına sahip olmamı sağlayan ve gösterdiği fedakârlık ve manevi destekle daima yanımda olan değerli eşime çok teşekkür eder, çalışmamın tüm ilgililere yararlı olmasını dilerim.

Gaziantep 2022 Serkan GÖKÇE

ÖZET

Bu çalışma, terörle mücadeleye yönelik ilgililere bakış açısı kazandırması amacıyla, siber istihbaratın teröristle mücadelede oynayacağı rolün ortaya koyabileceği sonuçlarını gerek kavramsal gerekse yapısal olarak araştırmaktadır. İstihbarat ve terörizmin siber uzay boyutlarına odaklanmak suretiyle tarihsel bir bağlamda ele almakta ve tahlil etmektedir. Bu doğrultuda ilk olarak istihbarat ve terörizmin tarihsel serüveni incelenerek siber uzaya bağlı değişim ve dönüşümü ele alınmaktadır. Devamında ise siber istihbaratın teröristle mücadele ve yürütülen istihbarat faaliyetleri kapsamında yeterli düzeyde kavramsallaştırılabilmesinin etkileri değerlendirilmektedir. İkinci olarak siber istihbaratın mevcut durumunun uygulamalarla resmedilerek teröristle mücadelede belirlenmiş (doğruluk, isabet ve devamlılık) parametrelerle ölçülmesi sonrasında, kavramlarla ulaşılmak istenen nihai duruma katkısı (kuvvet çarpanı, maliyet etkin teröristle mücadele ve sert mücadeleye katkı) ölçülmeye çalışılmaktadır. Üçüncü ve son olarak da mevcut durumun incelenmesi esnasında tespit edilen parametreler, DAEŞ'in bir vaka olarak ele alınmasıyla ulaşılmak istenen nihai duruma katkısı sorusuna cevap aranmaktadır.

Anahtar Kelimeler: Terörist Yapılar, Teröristle Mücadele, Siber İstihbarat, DAEŞ

ABSTRACT

This study explores, both conceptually and structurally, the implications of cyber intelligence's role in the fight against terrorism in order to give a perspective to those involved in the fight against terrorism. It scrutinizes and analyzes in a historical context by focusing on the dimensions of cyberspace of intelligence and terrorism. In this sense, first, the historical process of intelligence and terrorism is examined, and the change and transformation related to cyberspace are discussed afterwards. Furthermore, the effects of adequate conceptualization of ISI cyber intelligence within the scope of counterterrorism and intelligence activities are evaluated. Secondly, after the current situation of cyber intelligence is illustrated by applications and measured with the specified parameters in the fight against terrorism (accuracy, accuracy and continuity), its contribution to the final situation (force multiplier, cost-effective counterterrorism and hard fight) is measured. Finally, the parameters are identified during the examination of the current situation are sought to answer the question of the DAESH's capacity within its input to the states of cyber intelligence.

Keywords: Terrorist Structures, Counterterrorism, Cyber Intelligence, DAESH

İÇİNDEKİLER

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

ABD : Amerika Birleşik Devletleri

ANS : Advanced Network Service (Gelişmiş Ağ Hizmeti)

ARPA : Advanced Research Project Agency (İleri Araştırma Proje Ajansı)

ARPANET : Advanced Research Projects Agency Network (İleri Araştırma Projesi Ajansı Ağı)

ATM : Automated Teller Machine (Otomatik Vezne Makinesi)

DAEŞ : Devlet'ül Irak ve's Şam (Irak – Şam İslam Devleti) (DEAŞ-İŞİD-ISIS)

DDOS : Distrubuted Denial Of Service (Dağıtılmış Ağ Saldırısı\Hizmet Reddi)

DNA : Deoksiribo Nükleik Asit

DNS : Domain Name System (Alan Adı sistemi)

EMP : Electromagnetic Pulse (Elektromanyetik Darbe)

GPS : Global Positioning System (Küresel Konumlama Sistemi

İHA : İnsansız Hava Araçları

İKK : İstihbarata Karşı Koyma

IİD : Irak İslam Devleti

IP : Internet Protokol

IŞİD : Irak Şam İslam Devleti

MİT : Millî İstihbarat Teşkilâtı

NSFNET : National Science Foundation Network (Ulusal Bilim Kurumu Ağı)

NATO : North Atlantic Treaty Organization (Kuzey Atlantik Antlaşması)

OSINT : Open Source Intelligence (Açık Kaynak İstihbaratı)

RF : Radyo Frekans

SOCMINT : Soial Madia Intelligence (Sosyal Medya İstihbaratı)

SSCB	**:**	Sovyet Sosyalist Cumhuriyetler Birliği
TBB	**:**	Türkiye Barolar Birliği
TCP	**:**	Transmission Control Protocol (Geçiş Kontrol Protokolü)
TC	**:**	Türkiye Cumhuriyeti
TDK	**:**	Türk Dil Kurumu
UAB	**:**	Ulaştırma ve Altyapı Bakanlığı
WEB/WWW	**:**	World Wide Web (Dünya Çapında Ağ)
WI-FI	**:**	Wireless Fidelity (Kablosuz Bağlantı Alanı)

BİRİNCİ BÖLÜM

GİRİŞ

II. Dünya Savaşı'nın bitimiyle ortaya çıkan Soğuk Savaş Dönemi ve beraberinde getirdiği nükleer silahlanma yarışı, ABD ve Sovyet Rusya arasındaki rekabeti uzaya kadar ulaştırmıştır. Uzayda yaşanan rekabet, bilgi ve iletişim teknolojilerine olan ilgiyi daha da artırmıştır. Artan ilgi, yeni gereksinimleri de beraberinde getirmiştir. Bu çerçevede, iletişimin sürdürülebilirliğine olan ihtiyaç ortaya çıkmış ve olası bir iletişim kopukluğunu önleyebilmek amacıyla siber uzayın temelini oluşturan, internet adı verilen önemli bir haberleşme sistemi kurulmuştur. Böylece coğrafi uzaklık izafi olarak ortadan kalkmış ve dünyanın bir diğer ucuyla haberleşmek mümkün hale gelmiştir. Sağladığı pratiklik ve kolaylığın etkisiyle de hızla yayılarak toplumun bütün katmanlarını kapsamıştır.

İnternet kullanımının yaygınlaşması ve siber uzayın ortaya çıkmasıyla birlikte sanal ile gerçeklik iç içe geçmiştir. Soyut ve düşünce düzeyindeki olgular, somutlaştırılabilme imkânına kavuşmuştur. Sağladığı bu kolaylık sayesinde de sağlıktan ekonomiye, savunma sistemlerinden yaşamsal kaynaklara kadar hayatın için de var olan tüm alanlar dönüşüm geçirerek siber sanal dünyaya entegre edilmiştir. Siber sanal dünyanın yaratmış olduğu bu etkileşimsel dönüşüm süreci, istihbarat konseptlerinde de devrimsel bir gelişime yön vermiştir. Bugüne kadar bilinen tüm istihbarat teknik ve taktikleri, siber uzaya taşınarak yeni bir boyut kazanmıştır. Bu boyutuyla da istihbarat, siber istihbarat olarak adlandırılan ve diğer tüm teknik ve taktikleri bünyesinde barındıran kapsamlı bir yapıya dönüşmüştür.

İstihbarat ise, teröristle mücadelede ihmal edilmemesi gereken önemli bir faaliyet alanıdır. Bu mücadelede, doğru zamanda doğru bilgiye ulaşabilmek büyük önem taşımaktadır. Bunun içinde aktif, doğru ve eş zamanlı bir istihbarat anlayışı gereklidir. Gelecekte de bu anlayışı, hiç kuşkusuz siber istihbaratla sürdürebilmek mümkün olacaktır. Bu çerçevede, terörle mücadelenin geleceği açısından siber istihbaratın öneminin, yönteminin ve yapısının incelenmesi ve analiz edilmesi büyük önem taşıyacaktır.

1.1.Problem Durumu

Konvansiyonel anlamda icra edilen istihbarat faaliyetleri, teröristle mücadelede teksif edilen gayretlere olumlu katkı sağlarken zaman, konum, terkip ve faaliyet bağlamında teyit veya tekzip sürecine katkı sağlayamamaktadır. Arzu edilen katkının alınamaması niteliği

gelenekselleştirilmiş istihbarat yapı ve algılarının sorgulanmasına neden olmakta ve istihbaratı yeni arayışlara yönlendirmektedir. Tam da bu noktada siber sanal dünya, doğru zamanda doğru bilgiye ulaşmada isabet ve devamlılık sağlanabilmesi gayretleriyle sürdürülen arayışların ilgi odağı haline gelmiştir.

Son yıllarda ortaya çıkan siber tabanlı istihbarat gayretlerinin ise teröristle mücadelede; doğruluk, isabet ve devamlılık parametreleri dâhilinde hassas ve nihai maksada matuf bir şekle büründüğü görülmektedir. Bu durum siber uzayın bilgiye ulaşmayı kolay, hızlı ve ekonomik kılmasıyla ilintilidir. Yapısı itibariyle siber uzay, faaliyet alanları ve konularına göre istihbaratın ihtiyaç duyduğu askerî, siyasi, ekonomik, coğrafi, sosyal, biyografik, teknolojik, bilimsel ve teknik gibi bilgileri bünyesinde barındırmaktadır. Bu özelliği sayesinde de istenen zamanda doğru bilgiye süratle ulaşılarak güvenlik odaklı faaliyetlerin çıktılarında isabet sağlanabilmesi mümkün gözükmektedir. Böylelikle teröristle mücadelede arzu edilen nihai maksada matuf sonuçlara ulaşılabilecektir.

Belirtilen hususlar dâhilinde bu araştırmanın önermesi, teröristle mücadelede siber istihbaratın çarpan etkisi yaratarak maliyet etkin 'sert' mücadele yöntemlerini mümkün kılacağı hususudur.

1.1.1. Problem Cümlesi

Siber istihbarat, terörist yapıların marjinalleştirmesinde önemli bir rol oynamaktadır. Siber istihbarat aracılığıyla teröristle mücadele ederken maliyet etkin bir mücadele ortaya koymak gerekmektedir. Bu çerçevede teröristle mücadelede siber istihbaratın belirlenmiş parametreler dâhilinde amaçlanan operasyonel sonuçların elde edilmesinde terörist örgütlerin marjinal hale getirilmesi sorunsalı araştırmanın problemi olarak tespit edilmiştir.

1.1.2. Alt Problemler

Giriş, yöntem ve sonuç bölümü de dâhil olmak üzere, toplam altı bölümden oluşan çalışmada alt problemler şu şekilde kurgulanmıştır.

1. Kavramsal çerçeveyi oluşturan ikinci bölümde cevap aranan problem; "siber istihbarat, teröristle mücadele ve yürütülen istihbarat faaliyetleri kapsamında yeterli düzeyde kavramsallaştırılmış mıdır?" şeklinde tespit edilmişti. Böylece kavramsal belirsizlikler ön plana çıkartılarak araştırma problemine neden olan bilgi boşlukları ile tartışılan parametreler dâhilinde araştırmanın önermesinin ölçütleri tespit edilebilecektir.
2. Siber istihbaratın mevcut durumunun uygulamalar çerçevesinde ele alındığı dördüncü bölümde problem; "siber istihbarat, teröristle mücadelede belirlenmiş parametrelerle

ölçülmesi sonrasında kavramlarla ulaşılmak istenen nihai duruma katkı sağlamış mıdır?" şeklinde belirlenmiştir. Böylece kavramsal tespitlerin uygulama ile karşılaştırılması hedeflenmiştir. Ayrıca parametreler şeklinde tespit edilen kavramsal çerçevenin geçerliliği tartışılacaktır.

3. DAEŞ'in bir vaka olarak ele alındığı beşinci bölümde problem; "farklı devletlerin ortak bir tehdit olarak algıladıkları DAEŞ'e yönelik icra edilen siber istihbarat gayretleri, mevcut durumun incelenmesi esnasında tespit edilen parametreler çerçevesinde ulaşılmak istenen nihai duruma katkı sağlayabilir mi?" minvalinde ortaya konmuştur. Kavram ve uygulama mukayesesi sonrasında DAEŞ vakasının ulaşılan sonuçlar için geçerlilik testi olarak tartışılması amaçlanmıştır.

1.2.Araştırmanın Amacı

Çalışmada, siber istihbarat ile ilintili parametreler üretilmesi ve vakaların etkinliği bağlamında ölçülmesi yoluyla devletlerin teröristle mücadeledeki yöntem çeşitliliğini geliştirmek amaçlanmaktadır. Bu amaçtan hareketle siber istihbaratın teröristle mücadelede oynayacağı rolün ortaya koyabileceği sonuçlarının gerek kavramsal gerekse yapısal olarak iyi anlaşılması ve terörle mücadeleye yönelik ilgililere bakış açısı kazandırılması hedeflenmiştir. Bu çerçevede de ikinci bölümde, teröristle mücadelede istihbarat yöntemlerinden 'siber istihbaratın' kavramsal çerçevesi literatür taranarak ortaya konmaya çalışılmıştır.

Üçüncü bölümde, 'araştırmanın yöntem bağlamında nasıl icra edileceği' ortaya konmuştur. Araştırmanın modeli, veri toplama araçları, evreni ve örneklemi açıklanmıştır. Bu sayede de araştırmanın geçerlik ve güvenilirliğine dair kanaat oluşturulmak istenmiştir.

Dördüncü bölümde, ortaya konan kavramsal çerçeveden hareketle siber istihbarat uygulamalarının mevcut durumu farkındalık yaratma anlamında resmedilmeye çalışılmıştır. Buna bağlı olarak da siber istihbaratın unsurları, yöntemleri teknik ve taktikleri derinlemesine incelenerek etkinliğe yönelik temel bilgiler ortaya konmak istenmiştir. Böylelikle siber istihbaratın teröristle mücadelede bir yöntem olarak resmi çekilmiş, etkinlik parametreleri ortaya konulmuştur. Esasen bu husus, tezin bilime katkısı olarak ortaya çıkmaktadır.

Beşinci bölümde ise kavramsal çerçeveden yola çıkarak resmedilmeye çalışılan mevcut durum, güncel ve geçerli bir bakış açısı kazandırılması maksadıyla DAEŞ vakasının ele alınmasıyla aktarılmaya çalışılmıştır. Gerçekleşmiş veya gerçekleşebilecek olası siber istihbarat vaka örneklerine değinilerek konunun daha iyi anlaşılabilmesi istenmiştir. Bu sonuçla da

kavramsal tartışma sonrası tespit edilen parametreler üzerinden vakanın analizi yapılmaya çalışılmıştır.

1.3.Araştırmanın Önemi

Yapılan araştırmada, siber istihbaratın terör örgütlerinin marjinalleştirmesinde bir araç olarak oynayabileceği rolün tartışılması suretiyle teröristle mücadeleye katkısı ortaya konacaktır. Daha önce siber istihbarat ve teröristle mücadele üzerine yapılan çalışmaların mikro ve mezo düzeyde teknik analizler olduğu dikkate alındığında, bu araştırmayla siber istihbaratın makro etkileri üzerinde durulacak ve akademik mecraya katkıda bulunulacaktır. Böylece teröristle mücadele yöntemlerinde, siber istihbarat ile ilgili akademik nitelikte ölçüt tespit edilebilecek ve etkinlik analizi yapılabilecektir.

1.4.Araştırmanın Varsayımları

Doğruluğundan büyük ölçüde emin olunduğu için denenmeyen veya denenemeyen ve bu nedenle araştırmayı etkileyebileceği düşünülen varsayım terörist örgütlerin tamamen etkisiz hale getirilmesinden ziyade, marjinalleştirilerek görünürlük ve propaganda kabiliyetlerinin düşük profile indirgenebileceği şeklindedir. Dolayısıyla siber istihbarat aslî teröristle mücadele gayretlerinin tamamlayıcı ve kimi zamanda başat unsuru olarak değerlendirilmiştir.

1.5.Araştırmanın Sınırlılıkları

Literatürde terör, terörizm, terörle mücadele, siber terörizm, siber istihbarat gibi konularda çok sayıda çalışma bulunurken, terörle mücadelede siber istihbaratın incelendiği çalışmalar yeterli düzeyde değildir. Nitekim istihbarat alanında ketumiyet olgusunun bir tahdit olarak ortaya çıkması yanında siber istihbaratın kendine has gizliliği önemli bir sınırlılıktır. Bu nedenle, araştırma kavramsal çerçevesi bakımından siber istihbarat çalışmalarını zenginleştirmiş, ancak konusu bakımından verilen örneklerin alanını kısıtlamıştır. Ayrıca siber istihbaratın, özellikle terörle mücadeledeki uygulamasının ulusal ve uluslararası istihbarat servislerince yapılıyor oluşu, istatistiki verilere ulaşmada imkânsızlık yaratmıştır. Bu sonuçtan hareketle, açık kaynaklardan istifade edilerek çalışmaya zenginlik kazandırılmaya çalışılmıştır.

Çalışmada zaman, mekân, ulaşım, ekonomik, teknik ve teknolojik imkânların etkisi göz ardı edilmemiştir. Eldeki imkân, bilgi, beceri ve olanaklar göz önünde bulundurularak sistemli bir yol izlemeye çalışılmıştır. Bu çerçevede konunun daha iyi anlaşılabilmesi açısından, terör örgütü olduğuna yönelik üzerinde uluslararası uzlaşı sağlanmış ve üzerinde çok sayıda araştırma yapılmış DAEŞ terör örgütü üzerinden vaka incelemesi yapılmıştır.

1.6.Tanımlar

Çalışmada yer alan ve bilinmesinin önem arz ettiği değerlendirilen, araştırmaya özgü bazı terimler ve kavramlar şunlardır.

Terörist: Türk Dil Kurumuna göre "yıldırıcı" anlamına gelen terörist kelimesi, "siyasi nitelikteki bir davayı zorla kabul ettirebilmek amacıyla, karşı tarafa korku ve endişe salarak cana ve mala kastedebilecek davranışlar sergileyen kimse" şeklinde tanımlanmaktadır (TDK).

Terörist Yapılar: Türk Dil Kurumu'nun terörist tanımından ve Prof. Dr. Abdulkadir BAHARÇİÇEK'in terörün amacına yönelik açıklamalarının bulunduğu çalışmasından hareketle, "siyasi nitelikli davalarını zorla kabul ettirebilmek amacıyla bir araya gelmiş ve bu amaçla da acımasızca eylemler gerçekleştirerek toplumda ve kişilerde korku iklimi yaratmayı, devlete olan güveni sarsmayı, sosyal bütünlüğü bozmayı, anayasal ve toplumsal düzeni yıkmayı hedeflemiş örgütlü hiyerarşik yapılar" olarak tanımlanmaktadır (TDK; Baharçiçek, 2000:13).

İstihbarat: Türk Dil Kurumuna göre "bilgi toplama" ve "haber alma" anlamına gelen istihbarat kelimesi, Milli İstihbarat Teşkilatı'na göre, "belirlenmiş ihtiyaçları karşılamak amacıyla farklı kaynaklardan toplanmış olan haber, bilgi, belge ve doküman gibi verilerin belirli bir sistematik içerisinde işlenerek hedefe yönelik ürün haline getirilmesini" ifade etmektedir (TDK; MİT).

Siber İstihbarat: Keleştemur ve Bayraktar'ın çalışmalarından yola çıkarak "istihbaratın siber uzayda gerçekleştirilmesi" kavramı çerçevesinde tanımlanmaktadır (Keleştemur, 2018:76; Bayraktar, 2010:12).

Siber Uzay: Ulaştırma ve Altyapı Bakanlığınca yayınlanmış olan 2016 -2019 ve 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'ndan hareketle, "tüm dünyaya ve de uzaya yayılmış durumda bulunan doğrudan ya da dolaylı olarak internete, bilgisayar ağlarına, elektronik haberleşme sistemlerine bağlı, bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan veya bağımsız bilgi sistemlerinden oluşan sanal dijital ortam" olarak tanımlanmıştır (UAB, 2013:7; 2020:10).

İKİNCİ BÖLÜM

KAVRAMSAL ÇERÇEVE

2.1. Terör, Terörizm ve Terörle Mücadele

Terör ve terörizm kavramları toplum tarafından sıkça birbirinin yerine kullanılan kelimeler olarak karşımıza çıkmaktadır. Ancak pek tabi bu kelimeler birbirini tamamlayan birer olgu olsalar bile farklı iki kavramı ifade etmektedir. Bu farklılık ise daha çok iki kavramın yapısından kaynaklanmaktadır. Terör yapısı itibarıyla daha çok sistemli bir stratejiyle sürdürülen bir eylem biçimini veya bir eylem silahını ifade etmektedir (Cin, 1987:55). Terörizm ise bu eylem biçiminin ya da diğer bir deyişle bu eylem silahının ideolojik bir örgütlenmeyle sürekli olarak siyasi veya politik sonuçları elde etme amaçlı bir yöntem olarak kullanılmasıdır (Çakmak, 2008:29). Yani terör daha çok bir yöntem, eylem biçimi veya silahken terörizm, belirli bir ideoloji çerçevesinde terörün siyasi, politik kazanımları elde etmede sürekli hale getirilmesidir.

Bu farklılıktan hareketle çalışmanın bu bölümünde ilk olarak iki ayrı başlık altında terör ve terörizmin kavram tartışması yapılmıştır. İkinci olarak terörle mücadele kavramı incelenmiştir. Son olarak da tarihsel süreç içerisinde terör ve terörizmin değişim ve dönüşüm süreci özetlenmiştir.

2.1.1. Terör Kavramı

Terör kelimesi etimolojik olarak "korkudan titreme" ya da diğer bir ifadeyle "titremeye sebep olma" anlamına gelen Latince "terrere" kelimesinden türetilmiştir (Wilkinson, 1974: 9). Türk Dil Kurumunun Yabancı Sözlere Karşılıklar Kılavuzu'nda ise "yıldırma, cana kıyma ve malı yakıp yıkma" anlamına gelen Fransızca "terreur" kelimesinin karşılığı olduğu görülmektedir (TDK). Ancak ne korkudan titreme veya titremeye sebep olma anlamıyla ne de yıldırma, cana kıyma ve malı yakıp yıkma anlamlarıyla terör kelimesini açıklamak yanıltıcı bir yaklaşımdır. Çünkü bu kavramlar tek başına veya bir arada kullanıldıklarında bir şeyden korkma, birtakım şeylere zorlanma, can ve mal kaybına uğrama gibi anlamlar çağrıştırabileceğinden terör kavramını hafifletmektedir (Kartal, 2014:2). Bu durumu ortadan kaldırmak adına da terör kavramının 'terör' kelimesi üzerinden kavramsallaştırılarak ortak bir algı oluşturulması gerekir. Böylelikle terör kelimesi, karşı tarafta uyandırabileceği algı bağlamında kavramsallaştırılabilecektir.

Fransızca Petit Robert Sözlüğünde terör, ‘‘bir toplumda belirli bir grubun, halkın direnişini ve cesaretini kırmak için yaratmış olduğu ortak korku’’ olarak tanımlanmıştır (Bilir, 2009:28). Büyük Larousse Sözlük ve Ansiklopedisi yine benzeri bir tanımla terörün ‘‘bir topluluk üzerinde toplum direncini ortadan kaldırmak amacıyla yaratılmış olan kolektif korku’’ olduğunu belirtmiştir (Köşüş, 2019:9). Siyasi Terimler ve Örgütler Sözlüğü’nde ise terör ‘‘kamu otoritesini ya da toplumun yapısını yıkmak veya ortadan kaldırmak için girişilmiş olan, aynı zamanda da korku ve yılgınlık saçan şiddet hareketleri’’ şeklinde tanımlanarak biraz daha kapsamlı ifade edilmeye çalışılmıştır (Akmaral, 2013:33).

İoanna Kuçuradi terörü ‘‘insan haklarını hiçe sayan bir eylem biçimi’’ olarak nitelendirirken Gus Martin ‘‘bilinçli seçilmiş bir strateji’’ olduğunu vurgulamıştır (Kuçuradi, 1980; Martin, 2007). Gerard Chaliand ve Arnaud Blin ise terörün bir araç olarak ele aldığında ‘‘stratejik ilkelere dayalı olarak hasmın direnme kapasitesini etkilemek ve de iradesine baş eğdirmek’’ amaçlı kullanıldığını belirtmişlerdir (Chaliand ve Blind, 2016:19).

Bu kavramlardan yola çıkarak terörün, bir yandan bir araç olarak şiddet eylemini diğer bir yandan da eylem sonucunda oluşan korku ortamını belirtmekte olduğu görülmektedir. Bu durum terörün uzun süreli ve yoğun niteliğe sahip bir eylem biçimi olduğunun bir nevi göstergesidir. Bu doğrultuda da terörü, ‘hedeflenen sonuçlara ulaşmak için kişilerin veya toplumların korkutulması, caydırılması, yıldırılması, sindirilmesi, boyun eğdirilmesi ve ortadan kaldırılması stratejisiyle her türlü tehdidin, saldırının ve de eylemin gerçekleştirildiği acımasız bir şiddet biçimi ya da diğer bir ifadeyle şiddet silahı’ olarak adlandırmak daha doğru bir yaklaşım olacaktır.

2.1.2. Terörizm Kavramı

Terörizm kelimesi, terörün sistematik bir şiddet politikası olarak uygulanmaya başlamasıyla ortaya çıkmıştır (Saraçlı, 2007:4). Burada şiddetten kastedilen olgunun terör olduğunu ayrıca açıklamaya gerek yoktur. Terör yapısı itibariyle başlı başına bir dehşet durumudur. Terörizm ise bu durumun bir yöntem olarak benimsendiği strateji biçimidir. Terörün daha çok genel bir korku ve yılgınlık durumunu ifade ettiğini söylemek mümkündür. Ancak terörizmin teröre göre daha komplike bir durum olduğu da bir gerçektir.

İlhan Bal, terörü ‘‘silahlı şiddet eylemi ile davanın duyurulması’’ olarak nitelendirirken terörizmi, ‘‘terörün gerçekleştirilmesinin arkasında yatan bir amaç, düşünsel bir altyapı ve bir nevi strateji’’ olarak nitelendirmiştir (Bal, 2006:8). Yani terörü daha çok bir eylem durumu olarak görürken terörizmi, stratejik bir söylem biçimi olarak görmüştür. Yılmaz Altuğ ise bu

farklılığı terörün ‘‘gayri iradi olarak ortaya çıkan bir olgu’’ olduğunu terörizmin ise ‘‘bu olguyu siyasi maksatla iradi olarak ortaya çıkardığı’’ sözleriyle açıklamıştır (Altuğ, 1995:18). Bu yönüyle terörün içinde bulunulan durumdan hareketle kendiliğinden de ortaya çıkabileceğini belirtirken terörizmin daha çok terörün sistemli ve hesaplı olarak bir felsefeye, teoriye veya ideolojiye dayandırılarak uygulanmakta olduğunu belirtmiştir.

Terörizm kavramını kendi başına ele aldığımızda ise birçok tanımının bulunduğu görülmektedir. Genel kabul görmüş tanımlamaların ortak noktasında da “şiddet, örgüt ve ideoloji” kavramları bulunmaktadır (Şen, 2019:8). Bu kavramlar aynı zamanda terörizmin ana unsurlarındandır (TBB, 2006:205-211). Bu nedenle terörizmden bahsedebilmek için aynı ideoloji etrafında toplanmış örgütsel bir yapının var olması ve bu yapı tarafından şiddet içerikli bir eylemin gerçekleştiriliyor olması gerekmektedir.

Temel Britannica Ansiklopedisi’ndeki terörizm tanımına baktığımızda bu üç unsurun varlığı görülebilmektedir. Buradaki tanıma göre terörizm; ‘‘bireylerin, grupların veya devletlerin siyasi bir amaca yönelik olarak kişi ya da gruplara karşı savaş dışı şiddet eylemlerinde bulunma’’ anlamına gelmektedir (Hürriyet, 1993:159). Burada ‘bireyler, gruplar veya devletler’ sözleriyle kastedilen olgunun örgüt unsuru olduğu açıktır. Siyasi bir amacın varlığının ise bir ideoloji olduğu herkesçe malumdur. Şiddet eylemi ise zaten başlı başına terör yapısının bir ürünüdür.

Paul Wilkinson, bir benzeri açıklamasıyla terörizmi ‘‘teröristlerin siyasi taleplerine ödün verilmesi için bireylere, gruplara, toplumlara ya da devletlere karşı korku ve dehşet salacak şekilde sistemli şiddet eylemleri gerçekleştirmesi veya bu eylemleri gerçekleştirebilme tehdidi’’ olarak vurgulamıştır (Wilkinson, 2002:144). Bruce Hoffman ise bir başka ifadeyle terörizmin, amacı ve gerekçesi itibariyle politik olduğunu, kapsamlı bir psikolojik yankı uyandırmak amaçlı şiddet veya eşiti sayılabilecek şiddet tehdidi kullandığını ve de tüm bunların bir organizasyon ya da belirlenebilir bir komuta zinciri yapısıyla yürütüldüğünü belirtmiştir (Hoffman, 1998:43).

Ted Robert Gurr, terörizmi ‘‘siyasi ya da sosyal amaçlar doğrultusunda insanları yıldırmak veya zorlamak için beklenmedik şiddet kullanma’’ olarak tanımlarken Jack P. Gibss, terörizmde insanın yanında insan dışı nesnelere yönelik olarak da yasa dışı şiddetin veya şiddet tehdidinin var olduğundan bahsetmiştir (Gurr’dan [1989] aktaran Martin, 2017:32; Gibbs, 1989:329). Yonah Alexander ise terörizmin, ‘‘organize bir grubun şiddet kullanarak gerçek ve hayali hedefleri ele geçirmek üzere geniş bir korku iklimi oluşturmak’’ amaçlı kullanıldığını

söylerken Paul Johnson, ‘‘her çeşit siyasi eyleme karşı bilinçli ve soğukkanlı şiddet gösterisi’’ olarak kullanıldığını söylemiştir (Alexander, 1979:11; Johnson, 1980:15).

Terörizme karşı büyük savaşlar veren başat ülkelerin resmi terörizm tanımlamaları karşılaştırıldığında, benzeri tanımlamalar göze çarpmaktadır. Bu doğrultuda Türkiye’nin Terörle Mücadele Kanunu’ndaki terör tanımına bakıldığında terörizmin, ‘‘bir örgüte mensup kişi veya kişilerin baskı, korkutma, yıldırma, sindirme veya tehdit yöntemiyle anayasada belirtili cumhuriyetin nitelikleri ile siyasi, hukuki, sosyal, laik ve ekonomik düzeni değiştirmek, devletin ülkesi ile milletin bölünmez bütünlüğünü, kamu düzeni ile genel sağlığını bozmak, devletin ve cumhuriyetin varlığını tehlikeye düşürmek, devlet otoritesini zaafa uğratmak, devleti yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek amacıyla cebir ve şiddete başvurmaları’’ olarak tanımlandığı görülmektedir (Terörle Mücadele Kanunu, 1991). Öte yandan İngiltere’nin Terörle Mücadele Kanunu’nda terörizmin tanımının, ‘‘siyasi, dini veya ideolojik hedefe ulaşabilmek amaçlı, kişiye veya mülkiyete karşı, toplumu veya toplumun çeşitli kesimlerini korku içinde bırakacak ciddi şiddet içeren eylemde veya eylem tehdidinde bulunma’’ şeklinde yapıldığı görülmektedir (Martin, 2017:32; Kazan, 2012:7). Fransız Ceza Kanunu’nda bakıldığında da terörizmin ‘‘baskı, tehdit, sindirme ya da terör yöntemleriyle mevcut kamu düzenini bozmak için gerçekleştirilen bireysel veya kolektif şiddet girişimi’’ olarak algılandığı gözlemlenmektedir (Kazan, 2012:7; Karaağaç, 2019:3). Yine ABD yasasına göre terörizmin ‘‘politik veya sosyal hedeflere ulaşmak amacıyla sivil nüfusa ya da bir hükümete gözdağı vermek, onu zorlamak, yıldırmak, baskı altına almak, suikast veya kaçırma eylemlerinde bulunmak için gayri meşru şiddet kullanımı’’ olarak görüldüğünü söylemek mümkünken Almanya’nın, Anayasanın Korunması Bürosuna göre terörizmi, ‘‘elde edilmek istenen siyasi hedeflere ulaşılabilmek için, kişilerin yaşamlarına ve mülklerine yönelik olarak şiddetli suçların özellikle saldırı niteliğinde kullanıldığı mücadele biçimi’’ olarak nitelendirildiği söylenebilmektedir (Martin, 2017:32-33).

Buraya kadar aktarılanlardan terörizmin evrensel olarak eylemle propagandayı öne çıkaran bir kavram olduğu anlaşılabilmektedir. Ancak uluslararası kamuoyunda devletlerin hemfikir olduğu ortak bir terörizm algılaması bulunmamaktadır (Çomak vd., 2016:137). Devletler terörizm algılamalarını kendi bakış açılarına göre yapmakta ve terör örgütlerini de bu bakış açılarına göre değerlendirmektedir (Yenal ve Begenirbaş, 2019:3). Devletlerin çıkar odaklı yaklaşımının sonucu olarak karşımıza çıkan bu durum, kiminin teröristinin kimine göre özgürlük savaşçısı olduğu sorunsalını ortaya çıkarmaktadır.

2.1.3. Terörle Mücadele Kavramı

Terörle mücadelenin genel anlamda devletlerin, teröristlerin talep, hedef, amaç ve eylemlerine karşı kendini savunma çabası olduğu söylenebilir (Sönmez, 2013:25). Bu çabaların da ortaya çıkan şiddet eyleminin dozuna ve bu eylemlerin toplumdaki yansımalarına göre çeşitlilik gösterdiği görülmektedir. Sorunun çözümü adına ortaya çıkan bu çeşitlilik, demokratik toplumlarda öncelikli olarak sosyo-ekonomik ve klasik asayiş tedbirlerinin ön planda tutulduğunu, sonuç alınamadığında ise askerî tedbirlerin devreye sokulduğunu bizlere göstermektedir. Burada mücadele, askeri tedbirlerle çözüme kavuşturulmak istenebileceği gibi askeri güç kullanımı ile paralel de yürütülebilmek istenebilir. Anti demokratik toplumlara bakıldığında ise sorunun çözümünde doğrudan silahlı kuvvetlerin devreye sokulduğu gözlemlenir. Buradaki mücadelede, sorunun ortaya çıkma nedenlerinden ziyade tamamen ortadan kaldırılması istenmektedir.

Devletlerin savunma reflekslerinden kaynaklanan bu farklılıklar iki bakış açısıyla sınırlı değildir. Son derece geniş perspektifte ele alınan terörle mücadele, çok çeşitli taktik ve tekniklerin uygulandığı geniş bir yelpazede uygulama alanı bulabilmektedir (Sönmez, 2013:25). Teknolojiden yararlanma, yoğun istihbarat faaliyetlerinde bulunma, karşılık verme, gizli operasyonlar yürütme, grup içerisine sızma gibi yöntemler bunlardan sadece birkaçıdır (Öğreten, 2014:25-27). Bu yöntemler sayesinde terörizm tehdidi tamamen ortadan kaldırılamasa bile kontrol altına alınarak etkisizleştirilebilir ve böylece terörizm tehdidi baş edilebilir bir noktaya getirilebilir.

Bunu yaparken de uluslararası terörizmle stratejik olarak baş etmeye ilişkin politika yapıcılarının ortaya koyduğu dört temel yaklaşımı uygulamak elzemdir (Viotti ve Kauppi, 2014:353-359). Bu yaklaşımlardan ilki, alta yatan nedenlere eğilerek onları ortadan kaldırmaktır. Böylece problemin kaynağında yatan sıkıntılar tespit edilerek bir çözüm yolu bulunabilecektir. İkincisi, askeri güç kullanılarak karşı saldırıda bulunmaktır. Saldırı neticesinde ceza ve adalet talepleri tatmin edilerek teröristler yok edilebilecek ve tüm planları bozulabilecektir. Üçüncüsü, hukukun üstünlüğü ilkesini uygulayarak mücadelenin haklılığını ve de gerekliliğini ortaya koymaktır. Haklı mücadele, terör örgütlerinde çözülmelere neden olabileceği gibi, eleman temin etmelerinde de zorluklar çıkartacaktır. Dördüncü ve son olarak ise tam manasıyla küresel ölçekte uluslararası bir iş birliğine gidilmesidir. Bu iş birliğiyle teröristler, başka devletlerden destek alamadıkları gibi, başka ülke topraklarında da barınamayacaklardır. Böylelikle teröristler, her anlamda uzlaşı sağlanmış sert ve kapsamlı bir terörle mücadele çemberinin arasında kalarak sıkışacak ve zamanla da yok olacaklardır.

Terörle mücadelede tüm bu teknik, taktik veya yöntemleri uygularken, terör ve terörizmin doğasının anlaşılması da arzu edilen başarıya ulaşılmasında önemli bir gereksinimdir. Çünkü terör ve terörizmin doğasını derinlemesine incelemeden ve analiz etmeden etkin bir terörle mücadele politikası tesis etmek etkili bir çözüm yolu sunmayacaktır. Bu perspektiften hareketle, tarihsel süreç içerisinde terör ve terörizmin değişim ve dönüşümünün incelenerek analiz edilmesi, terörle mücadele noktasında çok ciddi kazanımlar sağlayacaktır.

2.1.4. Terör ve Terörizmin Değişim ve Dönüşüm Süreci

Terörizm olgusu, Gus Martin'in de dediği gibi, 'ilk tarihi kayıtlardan bugüne insan davranışlarının karanlık bir özelliği' olarak karşımıza çıkmıştır (Martin, 2017:49). Siyasi bir boşluktan kaynaklanmadığı gibi süreç içerisinde uzun ve köklü bir serüvene de sahiptir. Tarihsel perspektif içinde de değişim ve dönüşüm geçirerek kavramsal olarak genişlemiştir.

Bunu ortaya koyabilmek ve anlamlandırabilmek adına, konuyu belirli bir sistematik içerisinde ele almak gerekmektedir. Bunun için de bu süreci dönemsel olarak irdelemek daha doğru bir yaklaşım olacaktır. Böylece insan zihnindeki terörizme yönelik boşluklar doldurulabilecek ve terörizmin tekâmül eden tarihsel bir fenomen olduğu anlaşılabilecektir.

2.1.4.1. İlk Terör Hareketleri

Şiddeti asıl amaca ulaşmada bir eylem aracı olarak gördüğümüzde, terörizmin insanlık tarihi kadar eski olduğunu söylemek mümkündür (Kanat vd., 2016:4). Öyle ki güvende olma isteğiyle ortaya çıkan toplum bilinci dahi bizlere, bir toplumun başka bir toplumu imha ettiği birçok insanlık dışı örnekler sunmuştur. Halkların daha büyük bir iyiliği savunmak adına toptan kılıçtan geçirilmesi ya da otoriteye boyun eğmeleri için acımasızca davranılması, büyük liderlerin ortadan kaldırılması ve tanrıları memnun etme adına tiranların katledilmesi bu örneklerin en bilindikleridir. Ancak pek tabi bu örneklerin bugün bildiğimiz terörist eylemleriyle bir benzerliği bulunmamaktadır. Bu örneklerin daha çok terörün içinde var olan şiddet eyleminin bir ön gösterimi olduğu söylenebilir. Dolayısıyla bugün bildiğimiz anlama yakın bir terörizmden bahsedebilmek için konunun bilimsel açıdan irdelenmesi gerekir.

Walter Laqueur'e göre hakkında bilgi ve belge toplanabilen ilk terörist gruplarından birinin, bugünkü Filistin toprakları üzerinde M.Ö. 73-66 yılları arasında yaşamış, katı ve fanatik Yahudilerden oluşan Sicariiler (bir diğer adıyla Zelotlar) olduğu söylenebilir (Laqueur. 1977: 7). Adını acımasızca gerçekleştirmiş oldukları suikastlarda kullandıkları 'sica' adı verilen kavisli, kısa, gizlemesi ve taşıması kolay hançerlerinden alan Sicariler; birinci yüzyılda

dönemin kudretli savaşçılarına sahip olan Roma İmparatorluğu'na asla boyun eğmeyen nadir gruplardandır (Özman ve Açıl, 2019:2). Ancak tam da bu noktada onları diğerlerinden ayıran en önemli özellik, Roma hâkimiyetini reddetmelerinden ziyade, tıpkı günümüz radikal dini terörist grupları gibi tanrı dışındaki tüm otoriteyi de reddetmeleri olmuştur (Chaliand ve Blin, 2016:13). Bu doğrultuda kurulu düzeni yıkmak ve kendilerine tanrı tarafından vaat edildiğine inandıkları kutsal toprakları bütün kirletenlerden temizlemek için, din, dil, ırk ve statü gibi ayrımları gözetmeden düşman ve işbirlikçi olarak nitelendirdikleri herkesi vahşice yöntemler kullanarak ortadan kaldırmaya çalışmışlardır.

Laqueur'ün belirtiği bir diğer ikinci en eski terör örgütü örneği ise Haşşaşinlerdir (Laqueur. 1977: 7). Sicariilerden yaklaşık bin yıl sonra ortaya çıkan bu örgüt, tıpkı Sicariiler gibi Ortadoğu'da ortaya çıkmış ve mücadelesini radikal dini motivasyonla sürdürmüştür (Kanat vd., 2016:4). Bu motivasyonunu da günümüzde bile hala sürdürülmekte olan İslam dünyasının Sünni-Şii çatışmasından almıştır (Chaliand ve Blin, 2016:73-77). Yaşanan bu çatışma, İslami gelenekleri daha doğru muhafaza ettiklerini savunan Sünnilere karşıt olarak, farklı gelenekleri izleyerek dini ve politik lider olan imamların Peygamber soyundan gelmesi gerektiğini savunan Şiiler arasında yaşanmıştır (Yönem, 2013). Klasik bir iktidar mücadelesi olarak başlayan çatışmalar zamanla daha da şiddetlenmiştir. Bir süre sonra da derin ayrışmalara yol açarak ideolojik bir kisveye bürünmüştür. Çok geçmeden de Şii hareketinin içinden küçük ve marjinal bir mezhep olan İsmaili tarikatını ortaya çıkarmıştır (Ay, 2013:3). İlerleyen dönemlerde de bu tarikatın içinden çıkan Hasan bin Sabbah, kendisini İmam'dan sonra gelen kişi olarak ilan etmiştir. Kısa süre sonrada, kendi taraftarlarını yanına alarak bugünkü İran toprakları üzerinde bulunan Alamut Kalesi'nde Haşhaşiler adı verilen tarikatını kurmuştur (Ay, 2013:9). Örgütlenmesini tamamladıktan sonra da dönemin en güçlü Sünni devleti olan Büyük Selçuklu İmparatorluğunu hedef almıştır. Her anlamda iyi yetiştirilmiş gizli, hızlı, disiplinli, gözü kara ve itaatkâr fedaileri aracılığıyla da uzun vadeli bir terör kampanyası başlatarak siyasi kazanımlar elde etmek istemiştir (Zafer, 1996:10; Aydın, 2006:27). Bu doğrultuda Selçuklu yöneticilerini, askerlerini, kadılarını ve alimlerini hedef alarak gelecek dönemleri etkileyen acımasız bir konsept ortaya çıkarmıştır. En sansasyonel eylemini de bin yıl Müslüman dünyasının devlet teşkilatlanmasına öncülük edecek olan yapılanmanın mimarı, Büyük Selçuklu İmparatorluğu'nun Baş Veziri Nizamülmülk'ü öldürtmeleri olmuştur. Nizamülmilk'ün öldürülmesiyle adeta dönemin 11 Eylül'ü yaşanmış ve gelecek terör kavramına teşkilatlanma, örgütsel yapılanma, uyuyan hücre sızdırma, örtülü kimlik kullanarak

etkili ve sarsıcı eylemler yapma anlamında esin kaynağı olabilecek örnekler girmiştir (Chaliand ve Blin, 2016:79).

2.1.4.2. Modern Terörizm Dönemi

Sicarii ve Haşhaşiler'in ardından, dünyanın çeşitli bölgelerinde terörist nitelikli hareketler ortaya çıkmıştır. Ancak dünyanın modern anlamdaki terörizmle tanışması Fransız Devrimi ile olmuştur (Martin, 2017:51). Zira devrim sonrası kurulan cumhuriyet rejimi, Maximillien Robespierre ve yakın arkadaşlarının yani Jakobenlerin (1793-1794 arası) mutlak iktidarını kanlı katliamlarla tesis ettiği acımasız bir dönemi sahnelemiştir (Sander, 2000:164). Radikal Jakoben hükümetinin öncülük ettiği bu döneme de 'Terör İktidarı' ya da 'Terör Rejimi' denilmiştir (Yayla, 1990: 10). Modern terörizmin doğuşu olarak kabul edilen bu dönemde, Jakoben diktatörlüğüne muhalif binlerce kişi sadece yeni devrimci cumhuriyetin düşmanları oldukları gerekçesiyle tutuklanmıştır (Martin, 2017:51). Devrim Mahkemelerinde yargılanan bu tutukluların bir kısmı, giyotin ile idam edilirken bir kısmı da atılmış oldukları siyasi hapishanelerde hastalık ve açlıktan ölmüştür. Toplam 500 bini bulan bu sayı, 25 milyonluk Fransa'yı terörle susturmayı başarmış ve Fransa adeta terörle teslim alınmıştır (Yayla, 1990: 10).

Bu dönemde terörün yönetim tarafından doğal ve yararlı bir araç olarak kullanılmasıyla devrimci bir ideolojinin hedefleri daha da ileriye götürülmek istenmiştir. Öyle ki Maximillien Robespierre'in ''Terörsüz erdem acizdir; erdemsiz terör zararlıdır'' sözü, bu durumu özetlemek için en uygun cümledir (Herbst, 2003:164). Ancak zorbalıkla geçen süreç korku ve güvensizlik ortamına neden olmuştur. Artan şiddet, Rebespierre'in düşmanlarının ve onun hışmından korkanların birleşmesiyle ve çok geçmeden ortak bir harekete dönüşerek onun ve 20 arkadaşının kendi silahları olan giyotinle idam edilmesiyle neticelenmiştir (Gaxotte, 1961:281).

Fransız devriminin ardından terörizm, anarşizmden aldığı ilhamla en kanlı ve en etkili silah olmuştur. Özellikle Johan Caspar Schmidt (1806-1856), Pierre Joseph Proudhon (1809-1864), Mihail Bakunin (1814-1876) ve Peter Kropotkin (1842-1921) gibi başlıca anarşist düşünürlerin savunduğu ''kişilerin hürleştirilmesi için her türlü otoriteye ve kuruma saldırılması ve de bunların yok edilmesi'' inancı, bu dönemin en önemli esin kaynağıdır (Yayla, 1990:11). Dönemin şartlarının yarattığı yoksulluk, sınıf ayrımı gibi durumların da etkisiyle bu düşünceler, hızla yayılmıştır. Yayılan düşünceler başta Fransa olmak üzere, Güney Avrupa ve Rusya gibi krize batmış toplumlarda farklı ideolojileri savunan grupları ortaya çıkarmıştır. Ortaya çıkan bu gruplar 'eylemle propagandayı' öne çıkararak tüm dünyayı etkisi altına almıştır

(Chaliand ve Blin, 2016:117). Bu noktadan sonra da artık terörizm, hem otoriteye karşı mücadele eden grupların kullandıkları bir silah, hem de otoritenin mutlak iktidarını güçlendirmek ve muhalefeti sindirmek amaçlı kullandığı bir araca dönüşerek tüm dünyada yaygın olan bir fenomen haline gelmiştir (Kanat vd., 2016:5).

Özellikle Rusya'da kurulan Norodnaya Volya yani Halkın İradesi adlı grup, terörü "Ölümle Propaganda"ya[1] dönüştürerek sapkın bir politika izlemiştir (Laqueur, 2002). Ardından Norodnaya Volya'yın ölümü propaganda aracına dönüştürmesini esin alan İspanya, Fransa, İtalya, Almanya ve ABD'li anarşist gruplar, sanayi devriminin getirdiği askerî ve kimyevi alandaki teknolojik gelişmelerle acımasız saldırılar düzenlemiştir. "Bomba Felsefesi"[2] olarak da adlandırılan bu saldırılarda önemli liderlerden politikacılara, sanatçılardan halka kadar sayısız insan yaşamını yitirmiştir (Laqueur, 2002).

Narodnaya Volya'nın dağılmasının hemen ardında kurulan Sosyal Devrimci Parti'yle Rusya'da ikinci bir terör dalgası başlamıştır (Yayla, 1990:14). Bir nevi Narodnaya devamı niteliği taşıyan bu oluşum, Karl Marx ve Friedrich Engels'in fikirlerinin de etkisiyle burjuva devleti olarak gördükleri Çarlık Rusya'yı yıkmak ve yerine proleter devlet dedikleri Komünist Rusya'yı kurmak istemişlerdir (Lenin, 2009:21). Nitekim 25 Ekim 1917'de Vladimir İlyiç Ulyanov, yani bilinen adıyla Lenin önderliğinde bu devrimi gerçekleştirmeyi başarmışlardır. Böylece iktidara gelen Bolşevikler, sistemli bir terör politikasıyla gerçekleştirdikleri bu devrimi, yine sistemli bir terör politikasıyla muhafaza etmiştir.

Rus Devrimiyle başlayan totalitarizm ve devlet terörizmi, 20 yüzyılın ikinci çeyreğinde Marksizm-Leninizm'den Sosyalizme doğru evrilirken, Batı Avrupa'yı da köklerini 1776 Amerikan Devrimi'nden alan özgürlük ve Liberal Demokrasi kutbuna doğru itmiştir (Chaliand ve Blin, 2016:119). Bu iki kutup arasında kalan Fransız Devrimi ise self determinasyon ve milliyetçilik akımından yola çıkarak kendisini Faşizme yöneltmiştir. Bu noktada Alman nasyonal sosyalizminin ortaya çıkmasıyla da dünya, çok çeşitli terör uygulamalarının yaşandığı savaş alanını olmuştur. İkinci Dünya Savaşıyla biten bu süreci, savaştan güçlü çıkan Liberal Amerika ile Sosyalist Sovyetler Birliği arasındaki güç dengesi izlemiştir.

[1] Ölümün dava uğruna kutsallaştırılarak ideolojik bir propaganda aracına dönüştürülmesidir. 19.uncu yüzyılın sonlarına doğru anarşistlerin öncülüğünde ortaya çıkmıştır. Bu dönemde anarşistler, kutsal olarak gördükleri hedeflerini gerçekleştirmek için acımasızca eylemler gerçekleştirmişlerdir. Binlerce insanın ölümüne neden olan eylemleri sonucunda da birçoğu yakalanarak yargılanmış ve idam edilmiştir. Ancak idam edilmeleri istenen sonucu vermediği gibi ideolojik fikirlerinin daha da geniş kitlelere yayılmasına neden olmuştur.

[2] Devrimin gerçekleştirilmesi ve kutsal olarak görülen amaçlara ulaşılması için teknolojiden yararlanılarak yeni patlayıcılar bulunması, geliştirilmesi ve etki alanının büyütülerek acımasızca kullanılmasıdır.

2.1.4.3. Dini Motifli Dalga: Yeni Terörizm

II. Dünya Savaşı'nın bitimiyle birlikte başlayan iki blok veya bloklar arası oluşan nükleer denge, uluslararası diplomaside, olası bir sıcak savaşı olabildiğince tercih edilemez bir konuma getirmiştir. Topyekûn savaşın muhtemel sonuçlarını iyi hesap eden Amerika Birleşik Devletleri ve Sovyet Sosyalist Cumhuriyetler Birliği, iki büyük baş aktör ve rakip olarak terörizmi uluslararası diplomaside bir araç olarak kullanmışlardır. Böylece gerek düşman olarak gördükleri devletleri zayıflatmak gerekse rakip bloktan uzaklaştırarak kendi saflarına çekebilmek adına mücadele etmişlerdir. Adeta işbirlikçi, taşeron veya kiralık örgütlerin savaştırıldığı devlet destekli bir terörizm kisvesi altında yürütülen mücadeleler, Soğuk Savaş dönemi boyunca hiç durmadan sürdürülmüştür (Bal, 2003:51).

Literatürde 'Dehşet Dengesi' olarak da adlandırılan bu dönemde terörizm, sırasıyla 1950-1953 Kore Savaşı, 1955-1975 Vietnam Savaşı, 1962 Küba Füze Krizi etkisiyle, bilhassa sömürgeci devletlere karşı bağımsızlık mücadelesi veren gruplarca en geçerli kurtuluş yolu olarak görülmüştür. Özellikle 1950'de başlayan ve 1960'ta Cezayir'in Fransa'dan bağımsızlığını kazanmasıyla neticelenen süreç, bu durumun perçinlenmesinde en önemli olgu olmuştur (Kanat vd., 2016:6). Onu izleyen Filistin Kurtuluş Örgütü üyelerinin 1969 uçak kaçırma eylemleriyle de uluslararası terörist saldırıların fitili ateşlenmiştir (Martin, 2017:51).

Yine bu dönemde Vietnam Savaşı'yla yaşanan ve süreç içerisinde artan karışıklıklar, Avrupa başta olmak üzere Latin Amerika ve Birleşik Devletlerde hızla yayılan Marksist-Leninist ve Maoist siyasi öngörüler doğrultusunda hareket eden 'Yeni Solcu' terörizm dalgasını ortaya çıkarmıştır (Shughart, 2006:21). Sosyal adaleti sağlamak güdüsüyle hareket eden bu gruplar, daha önceden örneklerini gördüğümüz siyasi kaçırmalardan suikastlara, silahlı saldırılardan bombalama eylemlerine varıncaya kadar her türlü terör eylemlerini kararlılıkla ve inançla sürdürmüşlerdir. Özellikle Batı bloğuna karşı sürdürülen bu mücadelenin en büyük destekçisi de Sovyetler Birliği olmuştur.

İlerleyen yıllarda ise asıl en büyük küresel tehdidin temelleri, Sovyetlerin Afganistan'a müdahalesiyle (1979- 1989) başlamıştır. Bu müdahaleler esnasında ABD, SSCB'ye karşı, Arap gönüllülerinden oluşan ve Abdullah Azzam ile Usame bin Ladin gibi liderler tarafından yönetilen Arap Mücahitlerine, her türlü parasal, askerî ve lojistik desteğini vermiştir. Ancak yaklaşık on yıl süren bu mücadele, son yıllına doğru, Sovyetlerin yenilmesi sonrasında derin ikilemleri de beraberinde getirmiştir. Bu ikilemle birlikte yaşanan kırılma, Sovyetlerin

yenilmesinden sonra dahi cihadın devam etmesi gerektiğine inanan radikal İslamcı Mücahitleri, Usame bin Ladin önderliğinde 'El-Kaide' adı altında birleştirmiştir.

Sovyetlerin yenilmesiyle Afganistan'da artan ABD etkisi, rejime yönelik iç karışıklıkların kaynağı olarak görülmüştür. Bunu takip eden Sovyet etkisindeki Irak'ın Kuveyt'i işgali ve Amerikan askerlerinin Suudi Arabistan'a konuşlanması, zaten bölgede hâlihazırda var olan gerilimin daha da tırmandırılmasını sağlamıştır. Artan gerilim Usame bin Ladin önderliğindeki El-Kaide'de, ''esas savaşın Irak'a karşı değil de İslam'a karşı verildiğine'' yönelik inancı ortaya çıkarmıştır (Scheuer, 2012:81). Çok geçmeden de bu inanç, kutsal toprakları tüm kirletenlerden temizlemek gayesiyle radikal bir dönüşüme uğramıştır. Bu sayede de birçok taraftar El-Kaide bünyesinde toplanmıştır.

El-Kaide'nin tam manasıyla harekete geçmesi ise SSCB'nin dağılmasıyla olmuştur. SSCB'nin dağılmasıyla ABD'nin bölgedeki hegemonyası artmış ve bölgeyi kendi politikaları doğrultusunda şekillendirme çabaları hız kazanmıştır. Bu doğrultuda da Batılı müttefikleriyle Irak'a askeri müdahalede bulunmaları bölgesel anlamda büyük tepkileri doğurmuştur. Artan tepkiler ise El-Kaide'yi güçlendirerek harekete geçirmiştir. Yaşanan hareketlilik bölgede aktif olan Mısırlı El Cihat, Pakistanlı Hareket-ül Ensar ve Bangladeşli Hareket-ül Cihat gibi aşırılık yanlısı gurupları El-Kaide önderliğinde birleştirmiştir. Birleşen gruplar ABD'ye karşı eşgüdümlü yeni bir sözde cihadı başlatmışlar ve ABD çıkarlarına karşı olabilecek her türlü silahlı eylemlerde bulunmuşlardır (Migaux, 2016:399). Dünyanın farklı bölgelerinde ABD konsolosluklarından uçak seferlerine, lider ve diplomatlardan turistlere kadar uzanan bu eylemleriyle de tüm dünyayı derinden etkilemiş ve yeni eylemler için de başta Asya, Avrupa ve Kuzey Amerika olmak üzere dünyanın birçok bölgesinde hücre şeklinde teşkilatlanmışlardır. Tarih 11 Eylül 2001'i gösterdiğinde ise tüm dünyayı dehşete düşürecek büyük eylemlerini gerçekleştirmişlerdir.

11 Eylül 2001 sabahı 19 El-Kaide üyesi tarafından 4 uçağın kaçırılmasıyla gerçekleştirilen intihar amaçlı sözde şehadet eyleminde, yaklaşık 3 bin kişi yaşamını yitirmiştir (Martin, 2017:63). Saldırılarda: Boston'dan kalkan iki Los Angeles uçağı, New York'taki Dünya Ticaret Merkezi'nin kuzey ve güney kulelerine, Washington'dan kalkan Los Angeles uçağı, Pentagon'a çarpmıştır (Migaux, 2016:408-409). New York'tan kalkan San Fransisco uçağı ise Pensilvanya, Pittsburgh'un 80 mil güneydoğusunda düşmüştür (Martin, 2017:63). Çarpmaların sonucunda Amerika'nın küresel gücünün en büyük sembolü olan Dünya Ticaret Merkezi'nin iki kulesi çökmüş, Wall Street Borsası kapatılmış ve her terör saldırısında olduğu

gibi binlerce masum insan yaşamını yitirmiştir. Bu saldırıyla birlikte terörün doğası değişerek dünyanın hiçbir yerinde terör tehlikesinin uzağında olmadığı, eylemlerin daha fazla ölümcülleştirildiği ve en fazla tahrifatın yaratıldığı yeni bir terör dalgası başlamıştır (Yenal, 2013:27-28; Bankoff, 2004:377-378). Yeni Terörizm Çağı olarak da adlandırılan bu süreçte terörizm, ulusal boyutun ve hedeflerin ötesine geçerek daha ulus ötesi bir tehdit olarak karşımıza çıkmıştır. Böylece terörizm, daha sembolik hedeflere yönelerek daha çok insanın ölümüne yol açan, âdete savaş benzeri sonuçlar doğuran küresel bir hal almıştır (Yenal ve Begenirbaş, 2019:208).

2.1.4.4. 11 Eylül Sonrası Dönem

11 Eylül saldırıları her ne kadar ABD'yi vurmuş olsa da asıl altında yatan hedefin farklı olduğu söylenebilir. Burada temel hedef, çıkış noktasını batının oluşturduğu küreselleşme sürecine olan tepkidir (Semercioğlu, 2016:11). Bu tepki başta El-Kaide üyeleri olmak üzere dini motifli radikal örgütleri daha da motive etmiş ve El-Kaide'ye karşı özellikle Ortadoğu'da ilgiyi artırmıştır. Artan ilgi, Ortadoğu'nun genel anlamda siyasi, toplumsal ve sosyal durumu göz önüne alındığında büyük endişelere neden olmuştur (İzol ve Zenginoğlu, 2014:3). Endişeler ise zamanla potansiyel tehditleri artırmıştır. Çok geçmeden de ABD öncülüğünde terörizme karşı küresel bir savaşı başlatmıştır.

Kararlılık gösterebilmek adına öncelikli olarak Avrupa Atlantik Ortaklık Konseyi'nin (aynı zamanda 19'u NATO üyesi olan) 46 üyesi, yapılan saldırıları koşulsuz kınadıklarını beyan ederek üzerlerine düşen tüm sorumlulukları üstleneceklerini taahhüt etmişleridir (Yaman, 2006:5). Akabinde de NATO'nun terörizmle mücadelede alacağı önlemlerin genel çerçevesi niteliğindeki 'ortak savunma' anlayışını öngören istihbarat paylaşımı, araç gereç yardımı, güvenliğin sağlanması gibi konularda iş birliğine gidilmesi hususunda uzlaşı sağlamışlardır (Johnson and Zenko, 2002:4). Bu bağlamda da Kartal Yardımı (Eagle Assist) ve Aktif Çaba (Active Endeavor) adı verilen operasyonları başlatarak terörizmle mücadeleye katkıda bulunmak istemişlerdir (Semercioğlu, 2016:12). 21-22 Kasım 2002 tarihinde de Prag'da bir zirve gerçekleştirerek NATO'nun terörizmle mücadeledeki varlığını kararlılıkla devam ettirileceği vurgulanmıştır (Rühle, 2003:6). İlerleyen süreçte de NATO üyeleri, 27-28 Haziran 2004 tarihinde İstanbul'da bir zirve gerçekleştirerek tıpkı Soğuk Savaş döneminde olduğu gibi ''ortak savunma stratejisini'' ''ortak mücadele stratejisine'' dönüştürme kararı almışlardır (Yaman, 2006:8-10). Böylelikle terörizmle mücadelede uluslararası bir konsept yani bir konsorsiyum oluşturulmak istenilmiştir.

Süreç içerisinde ilk olarak 7 Ekim 2001 günü ABD ve Birleşik Krallık öncülüğünde yapılan hava bombardımanı ile Afganistan Savaşı başlamış, akabinde de Afganistan'a asker indirilmiştir. Kısa bir süre sonra, NATO üyesi olan Koalisyon Güçleri de savaşa dâhil olmuştur. Böylelikle El-Kaide lideri Usame bin Ladin'in yakalanmasına ve Afganistan'da güvenliğin sağlanmasına değin sürecek bir savaş yaşanmıştır. Savaşın sonucunda, Taliban Rejimi yenilgiye uğratılmış, birçok El-Kaide kampı yok edilmiş, Usame bin Ladin öldürülmüş, Afganistan İslam Emirliği yıkılmış ve de Afganistan'da ilk demokratik hükümet kurulmuştur. Ancak savaş sonu ortaya çıkan bu tablo, her ne kadar kâğıt üzerinde olumlu gözükse de Afganistan'da güvenlik bir türlü tesis edilememiştir. Taliban kuvvetleri zamanla yeniden toparlanmış ve buna bağlı olarak da bölgede El-Kaide'nin hareketliliği artmıştır. Nihayetinde de ABD, kalıcı barışı tesis edebilmek adına, bölgede asker bulundurma kararı alarak varlığını hissettirmeye devam etmiştir.

İkinci olarak ise yine ABD ve Birleşik Krallık öncülüğünde çok uluslu bir koalisyon gücü oluşturularak 20 Mart 2003'te Irak'a askerî harekât düzenlenmiştir. Bu harekâtta Koalisyon Güçleri, Irak'ın kitle imha silahlarına sahip olduğunu ve Saddam rejiminin El-Kaide'yi desteklediğini iddia etmiştir. Kitle imha silahlarının El-Kaide'nin eline geçme olasılığından bahisle de ortaya çıkabilecek potansiyel tehditleri hesap ederek Irak'ı işgal etmişlerdir. İşgalin başlamasından kısa bir süre sonra Baas Partisi Hükümetini devirerek Saddam rejimini yıkmışlar ve de Saddam Hüseyin'i yakalamışlardır. Akabinde de Irak'ta El-Kaide operasyonlarını başlatmışlardır. İşgalin sonucunda da Saddam Hüseyin'i yargılayarak idam etmişler ve de Irak'ta demokratik yönetime geçişi sağlamışlardır. Ancak sağladıkları demokratik düzen bölgedeki istikrarı bir türlü sağlayamadığı gibi etnik ve mezhepsel ayrışmaları da körüklemiştir. Kısa bir süre içinde de ABD güçlerine karşı, son derece şiddetli bölgesel bir direniş başlamış ve bu direnişten de radikal gruplar kazançlı çıkmıştır.

2001 Afganistan ve 2003 Irak müdahalelerini izleyen süreç, bölgedeki kırılgan yapıyı daha da derinleştirmiştir. Bir türlü tesis edilemeyen istikrar ve güven ortamının da etkisiyle, terörist faaliyet ve yapılanmalar hızla yayılarak gelişmiştir (Pfiffner, 2006:35-52). Son derece ürkütücü sonuçlar içeren bu yeni terörizmin gelişiminde, yapılan terörist eylemlerin karakteri, insanların toplu şekilde öldürülmesi yönünde eğilim göstermiştir. Bunun en büyük göstergesi de teröristlerin, kitle imha silahlarına sahip olabilme ihtimalleri ve eylemlerinde bunları

kullanabilme tehdidinde bulunabilmeleri ya da nükleer terörizm[3], biyoterörizm[4] ve siber terörizm tehdidinin doğuşu olmuştur (Demirci, 2012:3).

Nükleer terörizm ve biyoterörizm, teröristlerin amaç ve hedeflerini göz önüne aldığımızda büyük avantajlar sağlamaktadır. Bu avantajların en büyük göstergesi, nükleer, biyolojik ve kimyasal silahların çok sayıda insana zarar vererek geniş çapta ilgi çekmesidir (Demirci, 2012:3). Dezavantajları ise silahlara ulaşma ve kullanmadaki güçlüklerdir. Ancak yeni bilgi teknolojilerinde yaşanan gelişmelerle, olası güçlüklerin etkisi zamanla azalmaktadır. Özellikle bilgisayar ağları ve internetin gelişimi ve ilerleyen süreçte tüm sistemlerin siber uzaya bağımlı hale getirilmesi, olası güçlükleri ortadan kaldırmada bir nevi fırsatta yaratmaktadır. Bu sebepten siber uzayın hayatın içinde var olan alanlarda yarattığı imkân, kabiliyet ve fırsatların yanında, terörizme yönelik olarak da ne gibi etkiler yarattığı, değişim ve dönüşüm sürecini nasıl etkilediği iyi incelenmelidir.

2.1.4.5. Siber Terörizm

2000'li yıllardan günümüze yaşanan yenilikler, çok kısa bir süre içerisinde internet ve bilgisayar ağlarını yaşamın tüm alanına entegre etmiştir. Bilgisayar ağları ve internet ile birlikte bilgisayar ve mobil teknolojiler yaygınlık kazanmıştır. Bu hızlı yayılım, dijital kodlama sistemleriyle temellenmiş, eşzamanlı ve son derece yoğun kapasiteli olan, aynı zamanda karşılıklı olarak yüksek hızda enformasyon aktarımına olanak sağlayan yeni iletişim modellerini ortaya çıkarmıştır (Avşar, 2017:10-11). Çoklu kaynak işlevi de sağlayan bu modeller sayesinde, mesajların coğrafi olarak dağınık kitlelere anında ulaştırılabilmesi mümkün olmuştur. Günümüzde de terör örgütleri bu imkândan faydalanarak propaganda yapma, destekçi artırma, eğitim, operasyonel kontrol ve komuta gibi konularda gereksinimlerini kolayca karşılamıştır.

Bilgisayar ağları, internet, bilgisayar ve mobil teknolojiler üzerinden yola çıkarak ilerleyen teknoloji, elektronik cihazların birbirine bağlı sistemler ile alt yapı aracılığıyla bilgiyi kullandığı siber uzay denilen operasyonel alanı ortaya çıkarmıştır (Yılmaz, 2020:3). Elektronik olarak kontrol edilebilen her türlü cihaz, sistem ve tesis, siber uzayla birlikte uzaktan komuta

[3] Kısaca terör örgütlerinin nükleer silah üretebilme kapasitesine sahip olabilme veya bu silahları çalarak kullanabilme ihtimaline sahip olmaları ya da nükleer tesislere saldırıda bulunularak büyük alanlara, su kaynaklarına ve doğaya radyasyon yayılmasına sebebiyet vererek birçok canlının yaşamını tehlikeye sokan felaketlere yol açma olasılığı olarak tanımlanmaktadır.

[4] İnsanlar, hayvanlar ve bitkiler gibi canlılarda ciddi hastalık oluşturan veya ölümlere yol açan her türlü bakteriler, virüsler ve bunların yan ürünleri gibi doğal veya genetiğiyle oynanarak sonradan geliştirilmiş mikroorganizmaların biyolojik bir silah olarak terör eylemlerinde kullanılması olarak tanımlanabilir.

edilebilir hale getirilmiştir. Ekonomi, finans, bankacılık, güvenlik, silahlanma gibi yenilikler ile e-ticaret, e-devlet gibi alanların siber uzaya entegrasyonuyla da bu alan, uluslararası güncel meselelerin yer aldığı kara, deniz, hava ve uzay alanı boyutuna yeni bir boyut olarak eklenmiştir (Çelik, 2018:6). Ancak bu durum, sağladığı fayda kadar yeni bir risk ve tehdit olan siber tehditleri de beraberinde getirmiştir. Ortaya çıkan bu yeni siber tehditlerin en tehlikelisi de siber terörizm olmuştur. Siber terörizm tehdidiyle de su, enerji, iletişim, nükleer, askeri, güvenlik, ekonomi, finans, bankacılık, uzay vb. tüm kritik altyapı sistemleri teröristlerin en önemli hedefi haline dönüşmüştür. Böylece tek boyutlu ve simetrik olan riskler çok boyutlu ve asimetrik bir yapıya kavuşmuş, düşman tanımlamalarında ve dünyadaki tehdit algılamalarında değişimler yaşatmıştır.

Siber terörizmi kavramsal olarak ele aldığımızda, ortaya çıkan yeni risk ve tehditleri anlamak daha da kolay olacaktır. Ancak günümüzde tam manasıyla net bir örneğine rastlayamadığımız için üzerinde uzlaşı sağlanmış bir siber terörizm kavramına rastlamak da oldukça zor gözükmektedir. Yine de konunun derinliği açısından belli başlı kavramları inceleyerek bu kavramlar üzerinden sentez bir tanımlama yapmak gerekmektedir.

Siber terörizm kavramı, literatürde yeni bir olgu olarak karşımıza çıkmaktadır. Kişilerde ise ilk olarak terörizme yönelik her türlü faaliyetlerin siber uzayda gerçekleştirilmesi anlamını çağrıştırmaktadır (Yılmaz, 2020:4). Bir diğer bakış açısı olarak da terörist amaçların gerçekleştirilmesine yönelik, bilgisayarların birer silah veya birer yöntem olarak kullanılması algısını uyandırmaktadır (Chomsky vd.'den [1999] aktaran Topal, 2004:22). Konuyu derinlemesine irdelediğimizde de daha geniş bir perspektifte ele alındığı görülmektedir. Bu perspektiften hareketle bazı siber terörizm tanımlarını incelediğimizde; Dorothy Denning'in siber terörizmi, ''kişi, kurum, siyasi ve sosyal mercilere gözdağı vererek üzerlerinde baskı oluşturmak amacıyla resmi kuruluşların bilgisayar, network sistemleri, bilgi ve veri tabanlarına yönelik tehdit ve zarar verici içerikli yapılan saldırı'' olarak tanımladı görülür (Denning'den [2003] aktaran Çokbildik, 2019:55). Denning'in tanımından siber terörizmin, siber boşluk ve terörizmin bileşiminden ortaya çıktığı ve siber terörizm olarak nitelendirilebilmesi için de bireylere ya da mala karşı şiddet eylemini içermesi gerektiği anlaşılır. Ceza hukuku profesörü Marie-Helen Maras ise siber terörizmi, ''terörizmde olduğu gibi ideolojik, dini veya siyasi bir amaç uğruna hükümetlerin korkutulmak ya da baskı altına alınmak için su, enerji, iletişim, nükleer, vb. kritik altyapı sistemlerine saldırıda bulunulması'' olarak tanımlayarak eylemin sonucunda ortaya çıkan tabloyu vurguladığı söylenebilir (Maras'dan [2012] aktaran Nasrat, 2015:17). Maras'ın tanımından bir eylemin siber terörizm olabilmesi için, eylemin sonucunda

ölüm ve büyük ölçekli yıkımların ortaya çıkmasının gerektiği anlaşılır. Maras'a yakın bir görüşle, Dublin City Profesörü Maura Conway, ‘‘bir eylemin siber terörizm sayılası için siyasi amaçlı olması gerektiğini ve eylemin sonucunda da ölüm veya büyük tahribatlar oluşması gerektiği’’ görüşünü aktardığı görülür (Conway, 2002:7). Conway'ın görüşünden siber terörizmin elde edilmesi istenen sonuç ölçeğinde klasik terörizm gibi olduğu kanısına varılabilir. Bir başka görüş olarak Gabriel Weimann, siber terörizmin ‘‘terör örgütleri için takipçilerini artırma ve üyelerini elde tutmalarını kolaylaştırma anlamında geleneksel terörizme göre daha az ölüm ve seyahat riski barındırarak fiziksel eğitimler ve psikolojik yatırımlar hususunda fayda sağladığını’’ belirtir (Weimann, 2004:6). Weimann'ın yaklaşımından siber terörizmin, geleneksel terörizm faaliyetlerine göre daha az maliyet gerektirdiği ve teknolojik bilgiye dayanarak farklı coğrafyalardaki ülkeleri etkileyebilme kapasitesine sahip olduğu söylenebilir.

Yerli tanımlamaları incelediğimizde, siber terörizmin küresel ölçekte olduğu gibi yine benzeri birçok tanımla karşılaşıldığı görülür. Atilla Sandıklı ve Gökhan Yivciger'in siber terörizme yönelik vurgulamalarını incelediğimizde Maras'ın tanımıyla benzer yönleri dikkat çeker. Sandıklı ve Yivciger, ‘‘ülkelerin kritik alt yapı sistemlerine yapılmış olan saldırılarında, yaratmış oldukları etkilerine göre’’ siber terörizm olarak tanımlanabileceğini vurgulayarak Maras'ın söz ettiği gibi eylemin sonucunda ortaya çıkan etkiyi göz önüne alır (Sandıklı ve Yivciger, 2004:5). Süreyya Atasever, İlker Özçelik ve Şeref Sağıroğlu da ‘‘bireylerin veya toplumların can ve mal güvenliğinin riske uğratılması ya da zarara uğratılması kastıyla, etkileşimde bulundukları sayısal teknolojilere veya platformlara gerçekleştirilmiş olan saldırıları’’ siber terörizm olarak nitelendirerek Denning'e yakın bir görüşü ortaya koyar (Atasever vd., 2019:2). Ali Murat Köknar ise tüm bu tanımlamalara ek olarak siber terörizmi ‘‘klasik anlamdaki terör faaliyetlerinin siber uzayın imkân ve kabiliyetlerinden istifade edilerek gerçekleştirilmesi’’ şeklinde tanımlayarak kapsamı ve niteliği üzerinde bir değerlendirme yapar (Köknar, 2001). Yani terör eyleminin siber ortamda gerçekleştirildiğini, ancak eylemin sonucunun gerçek dünyada somut bir etkiyle yarattığını aktarmaya çalışır. Bir başka bakış açısına sahip olan Saim Atalay Keleştemur da siber terörizm kapsamının içerisine ‘‘terörü destekleyen faaliyetlerin sosyal ağlar vasıtasıyla yapılmasını’’ ekleyerek kavramın genişletilmesi fikrini ortaya koyar (Keleştemur, 2015:161). Ortaya koyduğu fikri de gerçek hayatta teröre verilen desteğin bir terörizm faaliyeti olduğu gerçeğinden yola çıkarak savunur. Böylece siber uzayda, teröre yönelik her türlü destek, yardım, propaganda vs. içerikli

eylemlerin siber terörizmin içerisinde bir unsuru olarak ele alınması gerektiğini gözler önüne serer.

Siber terörizme yönelik olarak yapılan tüm bu tanımlamalardan siber terörizmin; terörizmin unsurlarının yanında, terörizme yönelik tüm hedef, amaç veya emelin gerçekleştirilebilmesi için siber uzayın bir yöntem, bir vasıta veya hedefe ulaşmada bir araç olarak kullanılması olduğu kısaca söylenebilir. Yani terör örgütlerinin ideolojik hedeflerine ulaşma, şiddete başvurarak eylem ve propaganda yapma, korku ortamı yaratarak toplumu ve devleti baskı altında tutma anlamında, siber uzayın yaratmış olduğu tüm imkân ve fırsatlarından azami derecede istifade ederek eğitim, iletişim, personel, ekonomik, stratejik, operasyonel, teknik ve taktik ihtiyaçlarını karşılama ve de siyasi, ekonomi, teknoloji, biyoloji, kimyevi, enerji, nükleer, askerî vb. kritik altyapı sistemlerine doğrudan veya dolaylı olarak saldırarak büyük yıkıma sebebiyet vermesi siber terörizmin kapsamı içerisinde yer almaktadır.

Konuyu daha iyi anlamak için siber terörizmi, olası korkutucu senaryolar üzerinden incelediğimizde, akademik olarak ilk örneklerini Barry Collin'in sunmuş olduğu göze çarpmaktadır. Collin 1977 yılında yayımlamış olduğu "Siber Terörizmin Geleceği" başlıklı makalesinde birçok korkutucu senaryolardan bahsetmiştir (Collin'den [1997] aktaran Nasrat, 2015:17). Bu senaryolarda teröristler: Ulusal veya uluslararası bankacılık, finans, borsa vb. sistemlerin alt yapılarına siber saldırı gerçekleştirerek tüm sistemi bozabilir ve bu sayede ekonomik kriz çıkarabilirler. Hava trafik veya demiryolu sistemlerine siber saldırı düzenleyerek iki uçağı ve iki treni birbiri ile çarpıştırabilir ya da 11 Eylül saldırılarına benzer bir saldırı gerçekleştirebilirler. Siber saldırıyla uzaktan ilaç firmasının ilaç formüllerini değiştirerek toplu can kayıplarına neden olabilirler. Yine aynı yöntemle siber saldırı gerçekleştirerek uzaktan gaz hatlarının basıncını, elektrik santrallerinin direncini değiştirerek büyük patlamalar yaratabilirler.

Olası senaryoları değerlendirdiğimizde, siber terörizm tehdidinin ihmal edilmemesinin elzem olduğu görülmektedir. Günümüzde bu senaryoların yanına askeri, güvenlik, savaş teknolojisi ile enerji, uzay, nükleer, biyolojik, kimyasal, radyolojik, robotik ve yapay zekâ teknolojisi gibi kritik alt yapı sistemlerini de eklediğimizde, küresel ölçekte ne denli büyük bir tehditle karşı karşıya olduğumuz daha da iyi anlaşılacaktır. Bu nedenle teröristlerce olası siber terörizm senaryoları gerçekleştirilmeden önce gerekli hazırlıkların yapılması ve ihtimallerin dahi ortadan kaldırılması gerekir. Gerekli hazırlıkların yapılabilmesi ve ihtimallerin ortadan kaldırılabilmesi için de devamlılık arz eden doğru ve isabetli istihbari bilgiye ihtiyaç

duyulacaktır. Bu minvalde tarihte hiç görülmediği kadar kapsamlı, sistemli ve süreklilik arz eden küresel bir iş birliği sağlanmalıdır. Başarıldığı takdirde de olası risk ve tehditleri azaltmada kayda değer sonuçlar alınabilecektir.

2.2. İstihbarat

İstihbarat, tıpkı terörizmde olduğu gibi tarihsel süreç içerisinde birçok değişim ve dönüşümden geçmiş olan ve temelinde de doğru bilgiye, doğru zamanda ve doğru mekânda ulaşma arzusu yatan önemli bir bilim dalıdır. Zaman içerisinde, mevcut yeniliklere ve değişimlere ayak uydurarak farklı alanlara bölünmüştür. Bu alanlar sayesinde, son derece geniş bir faaliyet sahasına sahip olmuştur. Siber dünyada yaşanan gelişmelerle de daha spesifik bir yapı kazanmıştır. Bu yapı sayesinde de kısa bir zaman diliminde finansal, sosyal, çevresel, askerî, kurumsal, kişisel vb. birçok alana yönelik bilgilere ulaşabilmek imkân dâhilinde olmuştur. Günümüzde de bir "güç kaynağı" veya "güç aracı" olarak kullanılmaya başlanmıştır (Seren, 2017:95).

İstihbaratın bu bakış açısı, terörle mücadele açısından önemli bir kazanım olmuştur. Mücadelede gerekli olan doğru, eşzamanlı üretilen ve dağıtılan istihbaratın kapasitesi, bilgi teknolojilerinde yaşanan yeniliklerle artmıştır. Artan kapasitede, mücadelenin başarıya ulaşma şansını bir o kadar yükseltmiştir. Bu minvalde, çalışmanın bu bölümünde ilk olarak istihbaratın kavram tartışması yapılmıştır. İkinci olarak terörle mücadeledeki yeri ve önemi ortaya konmaya çalışılmıştır. Son olarak da istihbaratta yeni bir alan olan siber istihbarat kavramına, ilerleyen bölümlerin daha iyi anlaşılabilmesi açısından açıklık getirilmek istenmiştir. Böylece teröristle mücadelede, istihbarat yöntemlerinden 'siber istihbaratın' kavramsal çerçevesini ortaya koyabilmek amaçlanmıştır.

2.2.1. İstihbarat Kavramı

İstihbarat, kökeni itibariyle Arapça bir kelime olup; anlık veya geniş zamana ait bir bilgiyi tanımlamak için kullanılan kökten "istihbar etmek" ya da "haber almak" anlamı taşımaktadır (Seren, 2017:223). İngilizce ve Fransızcada ise "akıl ve zekâ" anlamına gelen "intelligence" sözcüğüyle ifade edilmektedir (MİT). Türk Dil Kurumunun Güncel Türkçe Sözlüğünde de kelimenin anlam karşılığının "yeni öğrenilen bilgiler, haberler ve duyumlar" ile "bilgi toplama ve haber alma" olduğu görülmektedir (TDK). Ancak bu anlamların tümü, tek başına istihbarat kavramını dolduramamaktadır. Çünkü terminolojide işlenmemiş bilgi olarak ifade edilen haber, ancak ihtiyaca yönelik olarak akıl ve zekâ yoluyla mevcut bilgi ve dokümanlardan da istifade edilerek incelendiğinde kıymet kazanmaktadır. Bu nedenle

istihbarat kavramını ‘istihbarat’ kelimesi üzerinden kavramsallaştırmak gerekir. Böylelikle kavramın anlam bütünlüğü oluşturulabilecektir.

The American Heritage isimli sözlükte istihbarat, “düşmanlar veya düşman olma potansiyeli bulunanlar hakkında elde edilen gizli bilgiler” olarak tanımlanmıştır (The American Heritage Dictionary). International Dictionary of Intelligence isimli sözlükte de “gerçekleşen veya gerçekleşme ihtimali bulunan durumlar ile yerel ve yabancı faaliyetlere yönelik koşullara ilişkin bilgileri toplama ve bu bilgileri işleme sürecinin sonucu” olarak ifade edilmiştir (Carl’dan [1990] aktaran Seren, 2017:223). NATO sözlüğünde ise bilginin ham veriler olduğu açıklanarak istihbaratın, bu ham verilerin işlenmesiyle ortaya çıktığından bahsedilmiştir (Seren, 2017:224). Milli İstihbarat Teşkilatı’nın tanımına baktığımızda da “ihtiyaca yönelik olarak çeşitli kaynaklardan istifade edilerek toplanan haber, bilgi ve dokümanların tasnif, kıymetlendirme ve yorum gibi aşamalardan geçirilerek işlenmesi neticesinde elde edilen ürün” olarak daha kapsamlı tanımlandığı görülmüştür (MİT).

Taylor, istihbaratı hedefe yönelik bilgilerin toplanması, analiz edilmesi, üretilmesi ve kullanılması olarak vurgulamaktadır (Taylor, 2007:250). Köseli bir benzeri tanımlamayla istihbaratı, ham bilginin birtakım vasıtalar yoluyla toplanarak tasnif edilmesi ve devamında da analiz edilerek kullanıma hazır hale getirilmesi olarak nitelendirmektedir (Köseli, 2009:3). Richelson da iç ve dış tehditlere yönelik olarak kullanılabilir tüm bilgilerin toplanması, işlenmesi, entegrasyonu, değerlendirilmesi ve yorumlanması neticesinde elde edilen ürün olarak tanımlayarak ikiye ayırmaktadır (Rechelson, 2012:2). Bu ayrımda, dış tehdit olarak terör örgütleri de dâhil yabancı hükümetleri, grupları ve bu gibi unsurlar ile uzantıları kastetmektedir. İç de ise daha çok ülke ve toplum içindeki tehditlere değinmektedir.

Bu tanımlamalardan da anlaşılacağı üzere, istihbarat kavramına genelde ‘haber alma ve bilgi’ anlamları yüklenilerek bunların ‘analiz edilmesi, derlenmesi ve işlenmesi’ sürecine değinilmiştir. Ancak ortaya konan bu tanımlamalar kadar istihbaratın kapsamına yönelik yaklaşımlarda önemlidir. Çünkü toplanan haberin veya bilginin işlenmesi kadar, o bilgiye bakış açısı ve istihbarata dönüştürürken ki bilgi, birikim, beceri, imkân ve kabiliyetlerde önemlidir. Dolayısıyla istihbaratın kavramının yanında, kapsamına yönelik bazı yaklaşımları da irdelemek gerekir. Böylece istihbaratın kavramsal derinliği daha iyi anlaşılabilecektir.

Bu açıdan akademik literatürden örnekler vermek gerekirse, ünlü İngiliz istihbaratçı Michael Herman, istihbaratın sadece haber ve bilgiden ibaret olmadığını; asıl meselenin haber ve bilgiyi bulma, ona ulaşma ve onu yorumlama olduğunu ileri sürdüğü görülür (Herman,

2001:10). Bu yaklaşımıyla haberi, istihbaratın sadece bir malzemesi olarak gördüğü söylenebilir. İstihbaratın 'bilgi, organizasyon ve faaliyet' olarak üç temel unsurunun bulunduğunu öne süren Sherman Kent, istihbaratın gözlem, araştırma ve analize dayalı bilimsel bir yöntem olarak bilgiye ulaşma gayretiyle sürdürülen bir süreç olduğunu belirtir (Kent, 2003). Philip H. J. Davies, istihbarat sürecine daha çok ülkelerin tarihsel tecrübeleri ile siyasi, kültürel ve hukuksal yapılarından kaynaklı olarak algılamış oldukları tehditlerin ve bunlara yönelik ulusal güvenlik yaklaşımlarının yön verdiğinden bahseder (Davies, 2002:3). David Kahn, istihbaratı ''bilginin en geniş manadaki hali'' olarak nitelendirirken; savaşta yardımcı bir kuvvet olarak saldırıdan ziyade daha çok savunma için zorunlu olduğunu belirtir (Kahn, 2002:8-11). Peter Gill ise Kahn'ın bu yaklaşımına karşı çıkarak istihbaratın yalnız savunma için değil, özellikle terörizmle mücadele gibi durumlarda saldırı içinde önemli bir unsur olduğundan bahseder (Gill, 2009:2010). ABD'nin İç güvenlik eski Bakanlarından Michael Chertoff ise istihbaratın 21. Yüzyılın radarı olduğunu ve bu yönüyle başta terörizm tehdidi olmak üzere düşmanı durdurarak halkın refahını ve özgürlüğünü korumada etkili bir yöntem olabileceği görüşünü savunur (Chertoff, 2006). Bir başka akademisyen John R. Ferris, istihbaratı teorik ve pratik olarak ikiye ayırarak teoride, hedefe yönelik bilgiye ulaşma sürecindeki stratejiden pratikte ise politikaların belirlenmesindeki taktiksel süreci vurgular (Ferris, 2005:103). Böylece istihbaratın stratejiden ziyade taktikleri etkileyerek daha çok operasyonlar ve pazarlıklar için söz konusu olduğunu anlatmaya çalışır.

Tüm bu kavram tanımlaması ve yaklaşımlar göz önüne alındığında, istihbarat kavramına ilişkin bazı spesifik vurguların öne çıktığı görülmektedir. Bu açıdan istihbaratın belirli amaçlar ile kullanıldığı araçlar bakımından belirlenmiş bir olguya yönelik 'onu tanımlama, anlaşılmasını sağlama ve ortaya çıkarma' ile yapılması gerekenlere ilişkin olarak 'planlama yapma, harekete geçme, strateji geliştirme, politika üretme ve tehditleri önleme' gibi unsurları bünyesinde barındırdığı söylenebilir. Bunun yanında, belli başlı araçlar ya da metodoloji ile bilgiyi toplama, toplayana özgü yöntemlerle analiz etme, bu ölçüde değerlendirmeye tabi tutarak eyleme dönüştürmede, yine istihbarat kapsamı içerisinde kendisine yer bulmaktadır. Dolayısıyla tüm bu yönlerini göz önüne aldığımızda, istihbarat kavramının terörle mücadelede her an ihtiyaç duyulan bir olgu olduğu, analizin ön plana çıkarılarak stratejik, taktik ve operasyonel faaliyetler ile yüksek öneme sahip bilginin elde edilmesinde gerekli olduğu düşünülmektedir.

2.2.2. İstihbaratın Terörle Mücadeledeki Yeri ve Önemi

İstihbarat, en basit haliyle terörü ortaya çıkaran neden ve koşulların anlaşılmasında ilk akla gelen yöntemdir. Devamında da teröristlerin organizasyonlarının deşifre edilmesi, yerlerinin belirlenerek irtibatlarının ve planlarının açığa çıkarılması için öncelik verilen bir alandır. Bu alanda, olası bir terör eylemi gerçekleşmeden önce gerekli istihbarata sahip olunarak ön alınması en temel gayedir. Bu gayeyle, yapılan istihbarat çalışmalarında: Terör tehlikesinin kaynağının, niteliğinin ve seviyesinin belirlenerek yeni kaynak ihtiyacının ve güvenlik önlemlerinin stratejik değerlendirmeleri yapılmak istenmekte; terörü önlemek için gerekli bilgiler toplanarak keşif ve gözetleme faaliyetleri yürütülmekte; yasal önlemlerin alınarak teröristlerin yargılanması sağlanmaktadır (Olgunsoy, 2019:77). Bu sayede: terörist faaliyetlere iştirak edenler tespit edilebilmekte; olası terör saldırısı krizlerine karşı karar verme mekanizmaları geliştirilebilmekte; teröristlerin talep ve metot örüntülerini ortaya çıkarmaya yönelik bilgi tabanı yaratılabilmekte; yüksek risk grubunda olan kişilerle mülkiyetler belirlenerek can ve mal kayıplarının önüne geçilebilmekte; aldatıcı karşı saldırılar düzenlenebilmekte; terörist faaliyetlerin desteklenmekte olduğu sığınaklar ile personel, silah, ikmal ve finans kaynakları tespit edilebilmekte; teröristlerin eleman temin etmelerine yönelik karşı propaganda gayretlerine destek verilebilmekte; karşı istihbaratta bulunularak teröristlerin istihbarat faaliyetlerinin bütününe zarar verilebilmekte; yaklaşan saldırılara karşı uyarı verilebilmekte ve bu tarz saldırıların daha gerçekleştirilmeden önlenebilmesi mümkün olabilmekte; mücadeleye yönelik güvenlik güçlerinin kaynaklarına yön verilebilmekte; teröristlerin iletişim ağı sekteye uğratılabilmekte; müttefik kazanmaları engellenerek caydırıcı maksatla bilgi yayılabilmekte; terörle mücadeleye yönelik politik reformların süreci hızlandırılabilmekte ve de bilgi paylaşımında bulunularak yeni bilgiler elde edilebilmektedir (Robertson, 1987:49).

İstihbaratı, sağladığı bu katkılar ve kullanılma amacıyla değerlendirdiğimizde, stratejik olarak terörle mücadelenin merkezinde yer aldığını söyleyebiliriz. Ancak stratejik olarak terörle mücadelenin merkezinde yer aldığını söylerken istihbaratın nasıl üretildiğinin de belirtilmesi gerekecektir. Burada üretilen istihbarat ile kastedilen olgu, istihbarat kurumları tarafından ihtiyaca yönelik olarak toplanan bilginin belli bir disiplin içerisinde işlenmesi ve analiz edilerek yayılması veya kullanılması sürecidir. Bu süreçte bilgi, istihbarat çarkı adı verilen 4 farklı aşamadan geçmektedir. İlk aşamada, istihbarat ihtiyaçları tespit edilerek eldeki imkân ve kaynakların hedefe yönlendirilmesi sağlanır. İkinci aşamada, ihtiyaca yönelik haber ve bilgiler toplanır. Üçüncü aşamada, toplanan haber veya bilgiler hedefe yönelik olarak değerlendirilerek

işlenir. Son aşamada ise hedefe yönelik olarak değerlendirilerek işlenen bilgi, istihbarata dönüştürülür ve ilgili birimlere yayılarak kullanılması sağlanır.

Terörle mücadelede ihtiyaca yönelik bilgiye ise teşhis, tespit ve analizle ulaşmak mümkündür (Bulut, 2019:18). Bu üç yaklaşım her ne kadar geleneksel olarak gözükse de son derece etkilidir. Teşhis sürecinde terör tehditleri kesin olarak gözlemlenerek genel özellikleri belirli bir şablona oturtulmaya çalışılır. Tespit sürecinde ise gözlemlenerek teşhis edilen temel bilgiler, kritik ve stratejik yönleriyle belirlenmiş parametreler ölçüsünde sistemli bir akıl süzgecinden geçirilerek tüm hassas noktalar ile katmanlarının ortaya konulmasını kapsamaktadır. Böylece teröristlerin taktiksel, eylemsel, organizasyonel ve tarihsel yapısı üzerinden ihtiyaca yönelik bilgilere ulaşılabilecektir. Analiz aşamasına gelindiğinde ise tespit edilen bilgiler bilimsel ve rasyonel bir bakış açısıyla ihtiyaca yönelik olarak ayrıştırılma, incelenme ve derlenme işlemine tabi tutulmaktadır. Buradan elde edilen kıymetlendirilmiş bilgilerle de terörle mücadelede oluşturulacak istihbarata ciddi ve önemli kazanımlar sağlanmaktadır.

İstihbaratın yürütülen faaliyetler kapsamında ele aldığında ise temel olarak stratejik ve taktik olmak üzere iki türe ayrıldığı söylenebilir (Yılmaz, 2020:10). Stratejik istihbaratta, hedefe yönelik olarak onun olası güçlü yönleri, zafiyetleri, amaçları, politikaları ve stratejileri tespit edilerek gerekli bilgi üretilir, analiz edilir ve yayımlanarak kullanılır (Çınar:1997:115-118). Ayrıca operasyonel anlamda ileriye dönük bilgiler vererek taktik istihbarata, bir nevi yön tayin eder (Özdağ, 2002:7). Dolayısıyla terör örgütlerinin organizasyonel anlamdaki yapıları, amaçları, hareket tarzları, dış bağlantıları, finansal ve eleman temin kaynakları ile silah, mühimmat, patlayıcı madde gibi sahip olduğu askeri kapasitelerine yönelik bilgilerin ele geçirilmesi bu türün içerisinde yer alır. Taktik istihbaratta ise hedefin farkında olunarak hedef tarafından koordine edilebilecek olası saldırıların zamanı ve mekânını tayin edilebilir (Köseli, 2009:10). Bu yönü onu, stratejik istihbarattan farklı olarak daha kısa vadeli ve hemen kullanılması gereken bir yapıya büründürür (Özdağ, 2002:7). Bu nedenle de başarıya ulaşmak için taktik istihbaratın, geç kalınmadan bir an önce ilgili birimlere yayımlanarak kullanılması gereklidir. Ancak istihbaratın tam zamanlı, etkin ve doğru olarak yayımlana bilmesi için, yürütülen bu iki faaliyet türünün yanında, bu faaliyetlerin hangi alanda ve hangi yöntemler vasıtasıyla toplandığı da önemlidir. Çünkü istihbaratta; askeri, siyasi, sosyal, kültürel, ekonomik, teknolojik, bilim ve teknik alanda yaşanan gelişmelerin etkisi büyüktür (Yılmaz, 2020:10). Bu gelişmeler istihbaratın değişim ve dönüşüm sürecini hızlandırarak yeni istihbarat alan ve yöntemlerini ortaya çıkarmaktadır. Dolayısıyla elde edilmek istenen stratejik ve taktik

seviyedeki istihbaratta, uygun olan istihbarat alanından uygun yöntemler kullanılarak yararlanılması gereklidir. Günümüzde de bu alanın siber uzay olduğu değerlendirilmektedir. İstihbarat gayretleri ve yöntemlerinin bu alana yönlendirilmesiyle de terörist yapılarla mücadelede istenilen nihai maksada matuf sonuçlara ulaşılabilecektir.

Tüm bu açıklamalardan anlaşılacağı üzere istihbarat, sahip olduğu kapasitesiyle orantılı olarak terörle mücadeledeki en kritik konulardan birisidir. Bu nedenle mücadelede, istihbaratın doğru, eşzamanlı üretilen ve de dağıtılan bir kapasiteye ulaştırılması gerekir. Bu kapasiteye ulaşması içinde kesintisiz sürdürülebilen bir istihbarat ağı kurulması elzemdir. Bu ağı kurabilmek içinde, olaylara bilimsel ve politik yaklaşabilen, analiz yeteneği gelişmiş teknik, taktik, teknolojik ve operasyonel imkân ve kabiliyetlere sahip olarak strateji geliştirebilen, tüm alanlarda olduğu gibi siber uzayda yaşanan değişim ve dönüşüme de ayak uydurarak kendisini yenileyebilen ve de uluslararası iş birliğini ön planda tutabilen bir istihbarat biriminin oluşturulması önemlidir. Böylelikle terörle mücadelede arzu edilen hedefe kısa sürede ulaşılabileceğini söylemek ütopik bir bakış açısı olamayacaktır.

2.2.3. Yeni Bir Alan Olarak Siber İstihbarat

İstihbarat alan ve yöntemlerini incelediğimizde, dönemin şartlarına göre değişim ve dönüşüm geçirerek yeni alanların ortaya çıktığı görülmektedir. Özellikle modern dünyaya giderken yaşanan Fransız İhtilali, Sanayi Devrimi, Emperyalizm gibi siyasi ve ekonomik alandaki gelişmeler, askeri unsurların yanı sıra siyasi, ekonomik, sınıfsal, ideolojik ve etnik faktörleri istihbaratın çalışma sahasına dâhil etmiştir. I. Dünya savaşına doğru telgraf, balon ve uçakların icadıyla sinyal istihbaratı ortaya çıkmıştır. Klasik istihbarat anlayışı olarak da adlandırılan bu süreçten soğuk savaşın bitimine kadar geçen sürede, istihbarat faaliyetleri askerî alanda sürdürülmüştür. Soğuk savaş sonrası dönemde bilgi teknolojilerinde ortaya çıkan yeni gelişmeler, kitle imha silahlarının artması ve küresel terörizm tehdidinin doğuşuyla istihbarat gayretleri uzaya yöneltilmiştir. Uzay teknolojisinin kullanılmaya başlanılmasıyla da keşif ve gözetleme sistemlerindeki yeniliklere ağırlık verilmiştir. Bu noktadan sonra da uydu, frekans, yapay zekâ, bilgisayar ağları, internet gibi teknolojiler hızla gelişerek siber uzay adı verilen sanal dünya ortaya çıkmıştır. Böylece istihbarat, değişen dünya düzeninde geleneksel sistemlerin dışına çıkarak bu yeni alanlardaki yerini almıştır.

Siber uzayın yapısı ise zamanla ekonomi, iletişim, eğitim, finans, askeri, sosyal, coğrafi, ulaşım gibi hayatın içinde var olan tüm sektör ve alanları kapsamıştır. Kritik altyapı sistemleri ve buna bağlı olarak internete bağlanabilen her çeşit elektronik eşyanın siber uzaya entegre

edilmesiyle de fiziksel dünyayla birleşmiştir (Yılmaz ve Salcan, 2008:40). Bu sayede de insanların günlük yaşantısı kolaylaşarak en karmaşık ve uzun zaman gerektiren işlemler, anında çözümlenebilme imkânına kavuşmuştur. Siber uzayın bu kadar çok geniş ve kritik alanları kapsayan yapısı, istihbarat açısından da birçok fırsat ve kolaylık sunmuştur. İstihbarat faaliyetleri yeni imkânlar ve kabiliyetler kazanarak son derece hızlı, daha gizli, ekonomik olarak daha ucuz ve geniş bir alanı kapsayacak şekilde yürütülebilecek yeni imkân ve kabiliyetlere sahip olmuştur (Oruç, 2019:5). Böylece hali hazırda var olan istihbarat alan ve türlerinin bir yanı, bir şekilde siber uzayla kesişmeye başlamış ve siber uzayın imkân ve kabiliyetlerinden faydalanmıştır. Bu sonuçla da ortaya, siber istihbarat kavramı çıkarak istihbarat literatüründeki yeni bir alanı oluşturmuştur.

Siber istihbaratın yeni bir alan olarak ortaya çıkması, kesin bir tanımının yapılarak kavramsallaştırılması sorunsalını beraberinde getirmiştir. Yapılan tanımlamaları incelediğimizde ise ortaya çıkan kavram sorununun çerçevesinde iki yaklaşımın bulunduğu görülmüştür. Bu yaklaşımların ilkinde, siber istihbaratın diğer tüm istihbarat alanlarını kapsadığı iddiası yer alırken ikincisinde ise siber istihbaratın diğer istihbarat alanlarıyla kesişen bir yanı olduğundan bahisle, tüm istihbarat alanlarının siber istihbaratın imkân ve kabiliyetlerinden faydalandığı belirtilmiştir (Oruç, 2019:20). Ancak her iki yaklaşımı kendi içinde irdelediğimizde, ilk yaklaşım abartılı olmakla birlikte ikinci yaklaşımında kavramı tam karşılayamadığı düşünülmüştür. Çünkü ilk yaklaşımın, siber istihbaratın istihbarat literatüründe yeni bir alan olduğu fikriyle çeliştiği, ikinci yaklaşımın ise siber istihbaratın istihbarat literatüründe, bir alanımı yoksa bir yöntemimi oluşturduğu düşüncesiyle yeni bir tartışma yaratabileceği ortadadır. Bu sebepten belli başlı siber istihbarat tanımlamalarını irdeleyerek konuya ilişkin bir kavram ortaya koymaya çalışmak yararlı olacaktır.

Saim Atalay Keleştemur, siber istihbaratı ‘‘siber uzay üzerinden istihbarat oluşturma faaliyetleri’’ şeklinde tanımlamıştır (Keleştemur, 2018:76). Hasan Çiftçi ise ‘‘şahısların, rakiplerin, grupların, ülkelerin veya düşmanların iletişim ağlarına ya da bilgisayarlarına kişisel, ekonomik, politik veya askerî avantajlar sağlamak amaçlı yasa dışı sızılarak istenilen bilginin elde edilmesini’’ siber istihbarat olarak açıklayarak siber istihbaratın genel hatlarını ortaya koymak istemiştir (Çiftçi, 2017:329). Yapılan yabancı bir çalışmada da ‘‘potansiyel hısımların ve rakiplerin teknik, taktik, stratejik ya da başka türdeki faaliyetlerini, hedeflerini veya kabiliyetlerini siber uzayda değerlendirme süreci’’ olarak tanımlanarak Keleştemur ve Çiftçi’nin bir nevi sentezi sayılabilecek ölçüde tanımlandığı görülmüştür (INSA, 2015:2). Gökhan Bayraktar’da tüm bu tanımlamalara ek olarak siber istihbarat kavramının içerisine

‘‘siber uzayda tehditlerin engellenebilmesi amacıyla karar vericilere bilgi desteği sağlamak, propaganda, psikolojik harekât gibi örtülü operasyon yöntemleri ile olayları yönetmek ve düşman veya muhtemel düşmanın istihbarat faaliyetlerini engellemek için gerçekleştirilen istihbarat faaliyetlerini’’ dâhil ederek farklı bir bakış açısı ortaya koymuştur (Bayraktar, 2010:12).

Tüm bu yaklaşım ve tanımlamalardan hareketle siber istihbarat kavramını, ‘ihtiyaca yönelik olan her türlü istihbari bilginin, siber uzayın sağladığı imkân ve kabiliyetler dâhilinde, istihbaratın elde edileceği hedeften uygun bir istihbarat yönteminin kullanılarak siber uzaydan elde edilmesi’ şeklinde kısaca tanımlamak doğru bir bakış açısıdır. Bu bakış açısından yola çıkılarak da siber istihbaratın, istihbarat literatüründe bir yöntemden ziyade, istihbarat yöntemlerinin uygulanabileceği bir alan olduğu söylenebilir.

Siber istihbaratı istihbarat yöntemlerinin uygulanabileceği bir alan olarak ele aldığımızda, konumuz açısından siber terörizm kavramı ve istihbaratın terörle mücadeledeki yeri ve önemi başlığı altında aktarılmaya çalışılan durumu da ele alarak incelemek gereklidir. Siber terörizmin teröristlere sağladığı imkân ve fırsatlar sayesindeki risk ve tehdit durumu ne denli büyük olsa da faaliyetlerini siber uzaya kaydırmaları, izlerinin sürülme olasılığını bir o kadar mümkün kılmaktadır. Yani terörizm ve istihbaratın birbirini etkileyen ve dönüştüren yapısı bu noktada da ön plana çıkarak siber terörizme yönelik tüm faaliyetlerin siber istihbaratla önlenebileceği gerçeğini gözler önüne sermektedir (Bulut, 2019: 25). İstihbaratı terörle mücadeledeki yeri ve önemi açısından değerlendirdiğimizde ise sahip olduğu doğru, eşzamanlı üretilen ve dağıtılan kapasitesiyle orantılı olarak ne denli kritik konulardan biri olduğu ortadadır. Bu sebeple terörle mücadelede, siber istihbaratın tüm imkân ve kabiliyetlerinden azami derecede yararlanılması kritik öneme sahiptir.

Terörle mücadeleye yönelik etkin bir siber istihbarat ağı kurulabilmesi için öncelikli olarak gerekli teknolojik alt yapıya sahip olunması veya bu altyapının oluşturulması şarttır. Oluşturulan veya mevcut olan alt yapıyı da siber uzayda yaşanan değişim ve dönüşüme uyarlayarak imkân ve kabiliyetlerini artırmak hatta yeni icatlar ya da buluşlar ortaya koyarak ilerletmek gerekir. Diğer bir gereklilik ise sahip olunan alt yapının kapasitesini bilen, ölçen, analiz eden, kullanan, gelişime, ilerlemeye, değişim ve dönüşüme açık olan, aynı zamanda da yeni buluşlar, icatlar ve sistemler ortaya koyarak imkân ve kabiliyetleri sürekli arttıran alanında uzman ve yetkin personelin varlığıdır. Bu personellerin varlığı sayesinde de siber istihbarata yönelik sahip olunan alt yapı, hedefe yönelik olarak kullanılarak etkinlik anlamında

değerlendirilebilecektir. Son olarak da terörle mücadele ölçeğinde, siber istihbaratta yönelik küresel anlamda iş birliğinin sağlanabilmesi gerekliliği büyük önem arz etmektedir. Siber uzayın küresel fakat çok katmanlı yapısı uluslar, şirketler, kurumlar vs. ölçeğinde içerisinde var olan herkese sahip olduğu hâkimiyet alanları tanımaktadır. Dolayısıyla bu alanlarda, terörle mücadeleye yönelik gerek duyulan istihbarı bilginin alınabilmesi için iş birliğine gidilmesi veya anlaşma sağlanarak erişim yetkisine sahip olunabilmesi gereklidir. Ancak birçok ülkenin siber istihbarata yönelik gerekli alt yapısının olmadığı gibi, alanında uzman ve yetkin personeli de bulunmadığı bilinmektedir. Diğer bir yandan, ülkelerin terör örgütlerine yönelik olarak sübjektif yaklaşımı, terörle mücadelede olduğu gibi terörle mücadeledeki siber istihbaratın elde edilmesindeki iş birliğinin önüne geçerek güçlüklere neden olmaktadır. Bu durum, siber istihbaratın terörle mücadelede istismarına neden olduğu gibi, teröristlere de siber uzayı etkin olarak kullanma imkânı sunarak siber terörizm tehdidini her daim sıcak tutmuştur.

Sonuç olarak siber istihbarat, siber uzayda yaşanan yeni gelişmelere veya ilerlemelere paralel olarak yeni teknik, taktik, imkân ve kabiliyetler kazanmaktadır. Bu yönüyle devletlere, terörle mücadele açısından son derece önemli avantajlar sağlamaktadır. Sağladığı avantajların etkisiyle, siber ortamda terör faaliyetlerinin izi kolaylıkla sürdürülebilmektedir. Yapay zekâ ve algoritmalar sayesinde de erken uyarı sistemleri kurgulanarak teröristler ve eylemleri deşifre edilebilmektedir. Bu nedenle devletlerin, bu alanı ihmal etmeden gerekli tedbirleri alması, küresel ölçekte iş birliğine gitmesi, değişen ve gelişen şartlara uyum sağlayarak terörle mücadelede etkin bir siber istihbarat konsepti ortaya koyması gerekmektedir. Bu çerçevede ilgililere, terörle mücadeleye yönelik bakış açısı kazandırması için siber istihbaratın teröristle mücadelede oynayacağı rolün ve ortaya koyacağı sonuçların gerek kavramsal gerekse yapısal olarak iyi aktarılması önemli olacaktır. Böylece siber istihbarat; doğruluk, isabet ve devamlılık parametreleri ölçüsünde teröristle mücadelede, sert mücadele yöntemlerini mümkün kılarak maliyet etkin bir araca dönüştürülebilecektir.

ÜÇÜNCÜ BÖLÜM

ARAŞTIMANIN YÖNTEMİ

3.1. Araştırma Modeli

Yapılacak araştırma nitel model üzerine kurgulanmıştır. Bu çerçevede çalışmanın konusunu teşkil eden teröristle mücadele, istihbarat ve siber istihbarat alanları öncelikle literatür taraması yoluyla incelenmiş ve mevcut konular ortaya konmuştur. Bu sayede yapılacak araştırmanın referans alınması muhtemel kavramlar üzerinden incelenmesi yapılmış ve siber istihbaratın mevcut pratikte yaygın olarak gözlemlenen ve tekerrür halinde olan uygulamalarla karşılaştırılması suretiyle kavramsal eksikliklerin tespit edilmesine öncelik verilmiştir.

Kavramsal tartışmalarla siber istihbaratın teröristle mücadelede ulaşılması gereken nihai hedefe yönelik girdileri (kuvvet çarpanı, maliyet etkin teröristle mücadele ve sert mücadeleye katkı) ele alınarak katkı düzeyini ölçmek için doğruluk, isabet ve devamlılık parametreleri üzerinden geçerliliği incelenmiştir. Böylece tarif edilen nihai durum ile parametrelerin tespiti tezin orijinalliği bağlamında yöntemsel bir katkı olarak ele alınmıştır.

Öte yandan siber istihbaratın kavramsal çerçeve dâhilinde literatürdeki yeri incelendikten sonra, dördüncü bölümde, siber istihbarat uygulamalarının mevcut durumu ele alınmış, kavramlarla ulaşılmak istenen nihai duruma katkısı ve parametrelerle ölçülmesi sonrasında mevcut durumun eksiklikleri veya ilave çabalar resmedilmeye çalışılmıştır. Bu sonuçla da ikinci bölümde incelenen siber istihbarat kavramının uygulamadaki yapısal durumu ele alınarak kavram eksiklikleri ortaya konmaya çalışılmıştır.

Beşinci bölümde ise DAEŞ'in bir vaka olarak ele alındığı nitel araştırma yapılmıştır. Bu çerçevede farklı devletlerin ortak bir tehdit olarak algıladıkları DAEŞ'e yönelik siber istihbarat çabaları açık kaynaklardan faydalanılarak incelenmiştir. Böylece ikinci bölümde tespit edilen kavramsal eksiklikler dikkate alınarak dördüncü bölümde ifade edilen mevcut durum, ulaşılmak istenen nihai durum ve ortaya konan parametreler dâhilinde DAEŞ vakası esas alınarak analize tabi tutulmuştur.

3.2. Evren ve Örneklem

Terörizm çok boyutlu ve son derece geniş bir kavramdır. Bu kavram içerisinde teröristlerden terör örgütlerine, siyasi unsurlardan kültürel, sosyolojik ve ideolojik unsurlara, terörün finansmanı gibi ekonomik sorunlardan stratejik, operasyonel, teknik, taktik, bölgesel ve

küresel sorunlara kadar uzanan kapsamlı bir oluşum söz konusudur. Bu nedenle çalışmada zaman, mekân, imkân ve maddi kısıtlar göz önüne alınarak ideal evren olarak terörist yapılar ele alınmıştır. Örneklem olarak da üzerinde uluslararası kamuoyunda terör örgütü olduğuna yönelik uzlaşı sağlanmış ve hakkında da çok sayıda araştırma yapılmış DAEŞ terör örgütü seçilmiştir. DAEŞ'in geniş bir coğrafyada aktif unsurlarla eylemlerde bulunması ve karmaşık örtülü yöntemleri tercih etmesi evreni temsiliyet bağlamında uygun bir örneklem olduğuna işaret etmektedir.

3.3. Veri Toplama Araçları

Araştırmada verilerin toplanması sürecinde izlenen adımlar; ilk olarak kavramsal çerçeve bölümünde literatür taramasıyla elde edilmiştir. Yapılan literatür taramasında terör, terörizm, terörizmle mücadele, siber terörizm, istihbarat, terörizmle mücadelede istihbarat ve siber istihbarat konularında ele alınmış kitap, dergi, yayın, makale, tez, akademik çalışma vb. kaynaklar ile resmi beyanatlar, konuyla ilgili rapor, belge ve dokümanlardan derlenen bilgilerden istifade edilmiştir. İkinci olarak siber istihbaratın mevcut yönteminin resmedilmeye çalışıldığı dördüncü bölümde, kavramsal çerçevede olduğu gibi siber istihbarat alanında ele alınmış kitap, dergi, yayın, makale, tez, akademik çalışma vb. kaynaklar ile resmi beyanatlar, konuyla ilgili rapor, belge ve dokümanlardan derlenen bilgilerin yanında internetin açık kaynaklarından da yararlanılmıştır. Üçüncü olarak ise DAEŞ terör örgütünün bir vaka olarak anlatılmaya çalışıldığı beşinci bölümde, siber istihbarat örnekleri kavramsal çerçeve ve dördüncü bölümde olduğu gibi yine aynı tür kaynaklar üzerinden toplanmıştır.

3.4. Verilerin Analizi ve Yorumlanması

Araştırmada toplanan veriler konu başlıklarıyla ilintili olarak nitel veri analizi teknikleriyle yorumlanmıştır. Toplanan veriler detaylı olarak incelenmiş ve araştırma konusuna uygun olmayan veriler ayıklanmıştır. Böylelikle veri azaltma işlemi yapılarak kullanılacak veriler konu başlıklarına göre sınıflandırılmıştır. Sınıflandırılan veriler ise kendi içerisinde araştırma konusuna yönelik olarak irdelenerek gerekli çıkarımlar yapılmış ve yorumlanmıştır. Son aşamada da araştırmada gerek duyulduğu ölçüde kullanılmıştır.

DÖRDÜNCÜ BÖLÜM

SİBER İSTİHBARATIN BİR YÖNTEM OLARAK MEVCUT DURUMU

Terörle mücadele noktasında, devletler için doğru, isabetli ve devamlılık arz eden istihbaratın varlığı her zamankinden daha büyük bir öneme sahiptir. Çünkü doğru, isabetli ve devamlılık arz eden istihbarat ile teröristlerin ne zaman, nerede ve nasıl bir eylemde bulunacağını tespit etmek mümkün olabilmektedir. Tespit edilen istihbaratın eş zamanlı üretilmesi ve dağıtılmasının başarıldığı takdirde de terörist eylemler zamanında önlenebilecektir. Böylece doğru, isabetli ve devamlılık parametreleri ölçüsünde eş zamanlı üretilen ve de dağıtılan istihbaratın varlığıyla teröristle mücadelede maliyet etkin, 'sert' mücadele yöntemlerini mümkün kılabilecek istihbarata ulaşılabilecektir.

Bu çerçeveden yola çıkarak çalışmada, siber istihbaratın teröristle mücadeledeki mevcut durumu uygulamalarla resmedilmeye çalışılacaktır. Siber istihbaratın iyi anlaşılabilmesi maksadıyla da öncelikli olarak siber istihbarat için gerekli olan unsurlar, belirli bir sistematik içerisinde anlatılacaktır. Devamında ise siber istihbaratın yöntemleri, derinlemesine irdelenerek olası sonuçları zihinlerde canlandırılmak istenecektir.

4.1. Siber İstihbaratın Unsurları

Siber istihbarat, yapısal ve yöntemsel olarak birçok unsuru bünyesinde barındırmaktadır. Barındırdığı unsurlar tek tek ele alındığı takdirde de anlam kargaşasına neden olabilmektedir. Dolayısıyla tüm bu unsurları tek tek incelemek yerine, belirli bir sistematik çerçevesinde kategorize ederek incelemek gerekmektedir. Bu sebepten çalışmada, siber istihbaratın unsurları Tablo 1'de görüldüğü üzere siber uzay, siber savaşçılar ve siber silahlar olmak üzere üç ana başlık adı altında toplanmıştır.

Tablo 1. Siber İstihbaratın Unsurları

Kategori Başlığı	Kategori Edilme Nedeni
Siber Uzay	Çok katmanlı yapısıyla gerek duyulan istihbaratın toplandığı sanal dijital ortam olmasıdır.
Siber Savaşçılar	Siber uzayda gerek duyulan istihbaratın toplanmasında insan faktörünü oluşturmasıdır.

Siber Silahlar	Siber savaşçıların, siber uzayda gerek duyulan istihbaratı toplayabilmesi için silah olarak kullanması gerekli olan vasıtaları oluşturmasıdır.

Burada hemen akla, siber istihbaratın unsurlarının neden üç ana başlık altında toplandığı sorusu gelebilir. İlerleyen sayfalarda anlaşılabilecek olsa da bu soruyu cevaplandırmak adına ilk olarak kategori edilme nedeni üzerinde dikkatle düşünülmelidir. İkinci olarak ise aynı kategoriye girebilecek veya siber istihbaratın yöntemi içerisinde yer alabilecek noktaları ayrı bir unsurmuş gibi değerlendirmemek gerekmektedir. Aksi takdirde benzer yapıdaki unsurlar birbirinden bağımsız veya ayrı bir noktayı oluşturuyormuş gibi düşünülerek anlam kargaşasına sebebiyet verebilecektir. Kısa bir örnek göstermek adına birçok çalışmada görülebileceği gibi Özçoban'ın da internet, siber uzay, hacker, siber saldırı gibi kavramları ayrı başlıklar halinde siber istihbaratın unsurları olarak ele aldığı görülmektedir (Özçoban, 2014:46-55). Ancak üzerinde dikkatle düşündüğümüzde internetin yapısı itibariyle siber uzayın içerisinde yer alan önemli bir alan olduğunu, hacker kavramının da siber casuslar gibi insan faktörünü oluşturan siber savaşçıların içerisinde yer aldığını söylemek daha doğrucu bir bakıştır. Siber saldırı kavramının ise siber istihbaratın bir unsurundan ziyade daha çok siber istihbaratın toplanabilmesinde başvurulan bir yöntem olduğu açıktır. Doğal olarak siber istihbaratın Tablo 1'de görüldüğü üzere üç ana başlık altında toplanması daha anlaşılabilir olacaktır.

4.1.1. Siber Uzay

Siber uzay kavramı, ilk olarak 1982 yılında William Gibson'un ''Burning Chrome'' adlı kısa bir hikâyesinde; ''bir bilgisayar tarafından oluşturulan sanal gerçekliği ifade etmek için'' kullanılmıştır (Oruç, 2019:21). Devamında ise yine aynı yazarın 1984 yılında yayınladığı ''Neuromancer'' adlı bilim kurgu romanıyla popülerlik kazanarak ''bilgisayar sistemleri ile doğrudan ilişkilendirilmeye'' başlanmıştır (Sevis ve Seker'den [2016] aktaran Ulutaş, 2018:87). Süreç içerisinde de yeni bilgi teknolojileri, internet ve bilgisayar sistemlerinde yaşanan gelişmelere paralel olarak internet, bilgisayar ağı ve sistemlerini kapsayan elektronik bir ortam algısıyla sanal bir dünya olarak ifade edilmiştir (Oruç, 2019:22). Böylelikle Gibson'un ifade ettiği 'kurgusal matrix'den çıkan siber uzay kavramı, elektronik bir ortamı ifade eden bilimsel bir gerçekliğe dönüşmüştür. Ancak bu dönüşümü açıklarken siber uzayın internet, bilgisayar ağları ve sistemlerinden çok daha fazlası olduğu gerçeği de bilinmeli ve siber uzay bu minvalde değerlendirilmelidir. Çünkü siber uzay internet, bilgisayar ağları ve

sistemleri içerisindeki sosyal etkileşimlerden günlük hayatı etkileyebilecek hizmetlerin sunulduğu her türlü global bilgisayar ağlarına ve sistemlerine, iletişim araç ve gereçlerine etki edebilecek bir ortamı ifade etmektedir. Yani bir yandan sanal bir dünya olarak elektronik ortamı ifade ederken diğer bir yandan bu elektronik ortamla ilişkili olan tüm unsurları da içerisinde barındırmaktadır. Dolayısıyla tüm bu yönleriyle siber uzayı, çok katmanlı bir model olarak algılayarak açıklamak daha gerçekçidir.

Siber uzay, çok katmanlı bir model olarak fiziksel altyapı, mantıksal yapı, bilgi ve insan olmak üzere dört ana unsurdan oluşmaktadır (Clemente, 2015:163-164). Dave Clemente bu dört unsuru Tablo 2'de belirtildiği şekliyle kısaca açıklamaya çalışmıştır.

Tablo 2. Siber Uzayın Dört Temel Unsuru

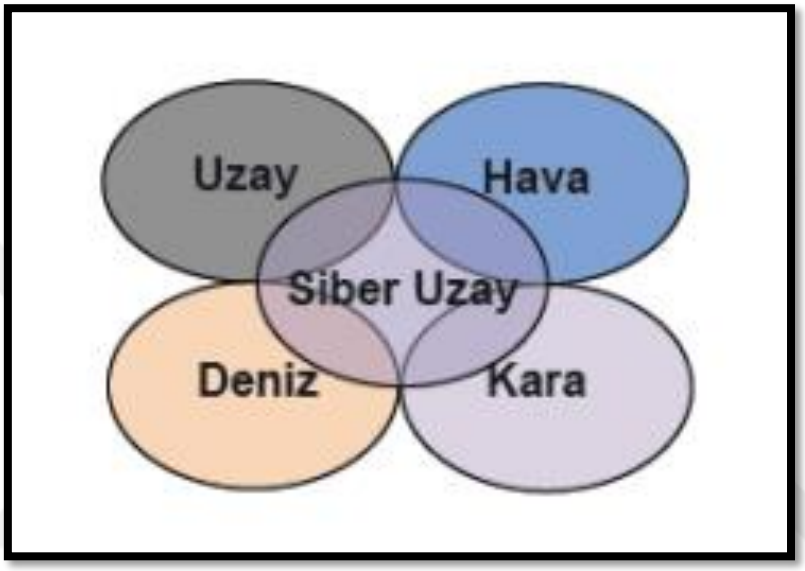
Unsuru	Kapsamı
Fiziksel Altyapı	Siber uzayda fiziksel olarak bulunan tüm kara, denizaltı vb. kabloları ile iletişim yollarını sağlayan uydular gibi bilgileri kendisine yönlendiren yönlendiricilerle birlikte hedefleri kapsamaktadır.
Mantıksal Yapılar	Web tarayıcıları, iletişim kurma ve akıllı telefon uygulamaları ile işletim sistemleri gibi yazılımlarda dâhil olmak üzere siber uzayda bulunan fiziksel altyapıların çalışmasına izin veren sistemleri kapsamaktadır.
Bilgi	İnternet siteleri verileri, sosyal medya gönderileri, metinler, iletiler, finansal transferler, video depolamaları ya da indirmeleri gibi siber alana kalıcı veya geçici olarak bir şekilde verilmiş, aktarılmış ya da depolanmış olan bilgiye yönelik tüm verileri kapsamaktadır.
İnsan	Siber uzayda bulunan bilgiyi kullanan veya manipüle eden, fiziksel ve mantıksal bileşenleri tasarlayarak geliştiren ve de bunlar vasıtasıyla iletişim kuran insanları kapsamaktadır.

Kaynak: Clemente, 2015:163-164.

Tablo 2 incelendiğinde fiziksel altyapı ile kara, deniz, hava ve uzayda tamamen somut bir şekilde yer alarak sistemleri oluşturan fiziksel birimlerin ifade edildiği açıkça görülmektedir. Yani siber uzayda ihtiyaç duyulan her türlü iletişim, telekomünikasyon, internet, bilgisayar ağı vb. teknolojilerine yönelik somut olan kablo, cihaz, yönlendirici, anahtar, modem, bilgisayar, telefon, anten, uydu gibi elektronik sistemler fiziksel altyapıyı oluşturan bileşenlerdir. Mantıksal yapılar ise fiziksel altyapıların çalıştırılabilmesi için gerekli olan yazılımsal sistemlerdir. İnternet, işletim sistemleri, mobil sistemler, web tarayıcıları, cep telefonları ve bilgisayar yazılımları gibi akıllı, aritmetiksel ve mantıksal olarak programlanmış yazılımlar, mantıksal yapılara verilebilecek örnekler arasında yer almaktadır (Ulutaş, 2018:87-88). Dolayısıyla mantıksal yapılar sayesinde fiziksel altyapıyı oluşturan birimlerin kendi aralarında haberleşebilmesi ve görev yapabilmesi olanaklı kılınacaktır. Üçüncü olarak bilgi unsuru, fiziksel altyapılar ile mantıksal yapılar sayesinde siber uzayda o veya bu sebeple var olan ya da bulunmakta olan verilerdir. İnternet, sosyal medya, e-posta, veri depolama alanları, komuta kontrol sistemleri, kritik alt yapı sistemleri gibi siber uzay ortamında yer alan ve akıp giden her türlü yazışma, konuşma, resim, video, ses kaydı, bilgi, belge vb. veriler en basit örneklerdendir. Bu veriler bilgisayarlar, sabit diskler, bellekler, hafıza kartları gibi fiziksel bileşenler içerisinde yer alabileceği gibi bulut bilişim sistemleri, çevrimiçi sistemler, internet gibi mantıksal sistemler içerisinde yer alabilmektedir. Bu nedenle siber uzayda bilginin bulunduğu fiziksel ve mantıksal yapılar siber istihbarat için önemli bir hedef noktasıdır. Son olarak en önemli unsur, hiç kuşkusuz insandır. Çünkü insan, sahip olduğu bilgi sayesinde fiziksel ve mantıksal yapılardan istifade ederek hayal ve kurgularını siber uzayda gerçekleştirebilme kudretine sahip bir varlıktır. Bu sayede siber uzaydaki fiziksel ve mantıksal yapıları tasarlayabileceği gibi burada bulunan tüm bilgiyi üretebilir veya üretilmiş olan bilgileri saklayabilir, iletebilir, değiştirebilir, kullanabilir ve de geliştirebilir.

Clemente'nin bu açıklamalarından siber uzayın ne denli geniş bir alanı kapsadığı açıkça gözlemlenebilmekle birlikte, insan eliyle yapılmış bir alanı işaret ettiği de düşünülebilmektedir. Çünkü insanlar o veya bu sebeplerden ötürü her zaman bilime, teknolojiye, zamanı verimli kullanmak için bilgiye ve iletişime büyük yatırımlar yapmışlardır. İletişime ve doğru bilgiye zamanında ulaşabilme arzusuyla oluşturulan telgraf, telsiz, telefon, internet gibi sistemler bu durumun en basit göstergesidir. Dolayısıyla ilk olarak karada gelişmekte olan insanlık, zaman içerisinde üretkenlik yetisi ve teknoloji üretimi ile birlikte denizlere, havaya, uzaya ve son olarak da siber uzay adı verilen alana uzanabilmiştir (T.C. İçişleri Bakanlığı, 2020:9). Böylelikle siber uzay kavramı kara, deniz, hava ve uzay olarak sınıflandırılan dört büyük

boyutun yanına beşinci bir alan olarak dâhil edilmiştir (Çahmutoğlu, 2020:5). Ancak tam da bu noktada siber uzayı, beşinci büyük boyut olarak değerlendirmeden önce diğer dört büyük boyuttan ayıran en önemli noktasının vurgulanmasında fayda vardır. Uğur Akyazı bu ayrımı Şekil 1'de görüleceği üzere, siber uzayın diğer dört boyuttan farklı olarak her birisi üzerinde birleşim sağlayarak etkinlik sağladığı bir boyut olarak nitelendirerek son derece açık bir şekilde aktarmıştır.



Şekil 1. Beşinci Harekât Alanı Olarak "Siber Uzay"

Kaynak: Akyazı, 2013:216.

Yani siber uzayı bir yandan kara, deniz, hava ve uzay gibi askerî harekât alanları arasında görürken, diğer bir yandan da siber uzayın bu askerî harekât alanlarını bilişsel süreçler ile saklanan, değiştirilen ya da aktarılan verilerin kullanılması yoluyla birbirine bağladığını öne sürmüştür. Böylelikle siber uzayın küresel olarak ne gibi etki alanına sahip olduğunu bizlerin hayal gücüne sunmaya çalışmıştır.

Siber uzay tüm bu etkileyici yapısıyla beşinci büyük harekât alanı olarak dikkate alındığında, insanlığın faydasına birçok hizmeti sunduğu görülmektedir. Kanıt olarak da dünya üzerinde sunulmakta olan her türlü hizmet veya faaliyetlerin siber uzayda da gerçekleştiriliyor olması gösterilebilmektedir (Kara, 2013:4). Ayrıca yine ışık hızında iletişim, internet, coğrafi veya siyasi gibi alanların dışına erişerek harekât imkânı sağlayabilmesi, bir diğer önemli gösterge olarak sunulabilmektedir. Bu durumdan da siber uzayın insanlardan ulusal veya

uluslararası kurum ve kuruluşlara, devletlerden bölgesel, küresel veya ulusüstü örgütlere kadar, içerisinde insan faktörü bulunan hemen hemen her oluşuma yeni fırsat alanları yaratarak sürekli ve hızlı bir şekilde gelişerek yaygınlaştığı çıkarılabilmektedir. Böylelikle siber uzayın bilim, sanat, teknoloji, kimyasal, biyolojik, nükleer, endüstriyel vb. üretim sistemlerinden sağlık, ekonomi, finans gibi sistemlere, güvenlik, savunma ve askeri sistemlerden radar, sinyal, uydu, frekans, uzay ve istihbarat sistemlerine kadar çok geniş ve kritik bir alanı kapsadığı net olarak kavranabilecektir (Oruç, 2019:22).

Siber uzayı tüm katmanlarıyla birlikte net olarak ifade ettikten sonra, ilk olarak içerisinde gerek fiziksel altyapı gerekse mantıksal yapısıyla yer alan internet boyutunu da incelemek gerekmektedir. Çünkü yapısı itibariyle internet, konunun uzmanı olmayan kişilerce siber uzayın kendisiyle karıştırılabilmekte ve hatta siber uzayın kendisiymiş gibi algılanabilmektedir. Oysaki internet ‘‘bilgisayar ağlarının birbirine bağlanmasını sağlayan elektronik iletişim ağını’’ ya da bir başka ifadeyle ‘‘birbirine bağlı sayısız küçük bilgisayar ağlarından oluşan büyük bir bilgisayar ağını’’ ifade etmektedir (Cemalioğlu, 2020; Özkan, 2006:46). Siber uzay ise üst paragraflarda bahsedildiği üzere, internet ve bilgisayar ağı sistemlerini de kapsayan elektronik ortam ve sanal bir dünya olarak internetten çok daha fazlasıdır (Oruç, 2019:22). İkinci olarak ise istihbarat açısından siber uzayda önemli kaynak teşkil edebilecek veya siber istihbaratın siber uzaydaki önemli hedef alanları arasında gösterilebilecek noktalarının vurgulanması gerekmektedir. Böylelikle ihtiyaca yönelik istihbari bilginin kaynağının hangi boyutlarda bulunuyor olabileceği daha çabuk kavranabilecektir.

4.1.1.1. İnternet

Siber uzayın içerisindeki en önemli bileşenlerden birisi olan internet, askeri amaçlı olarak bilgiyi saklama, paylaşma ve ona kolayca ulaşma arzusuyla ortaya çıkmıştır (Özçoban, 2014:47). Temelini ise 1962 yılında Amerikan Savunma Bakanlığı İleri Araştırma Projeleri Ajansı (Advance Research Project Agency-ARPA) tarafından, ‘‘galaktik ağ’’ kavramıyla desteklenen ‘‘ARPANET’’ adlı araştırma ağı projesi oluşturmuştur (Timisi, 2003:122). 1969 yılına gelindiğinde de bu proje kapsamında ilk bağlantı, ana bilgisayarlar arasında iletişim kurularak gerçekleştirilmiştir (Tokgöz, 1994:33-34). 1970’lerde kamu ve özel sektör yardımıyla daha da desteklenerek genişletilmiş ve 1980’li yıllarda NSFNET (National Science Foundation Network – Ulusal Bilim Kurumu Ağı) kurularak bilgisayar araştırma kuruluşları ile üniversitelerde kullanılmaya başlanmıştır (Özkan, 2006:46). Böylelikle sistem içerisinde bilgisayarların birbirine bağlı hale getirilmesi sağlanarak aralarındaki iletişim sağlanabilmiştir. Talebin artması üzerine 1990 yılında NSFNET servis kapasitesini artırarak ANS (Advanced

Network Service – Gelişmiş Ağ Hizmeti) sistemini kurmuş ve de dünya çapındaki binlerce küçük bilgisayar ağlarını NSFNET'e bağlayarak günümüzde kullanılan internetin temellerini oluşturmuştur (Çağıltay, 1997:6-11). 1990 yılı itibariyle de internet adını alarak hızla geliştirilmiş ve dünyaya yayılarak günümüzdeki yapısına ulaşmıştır (Yılmaz ve Salcan, 2008:35-37). Özetle, ABD'de askeri amaçlı iletişimin sağlanabilmesi amacıyla oluşturulan ARPANET, ilk olarak belli başlı Amerikan laboratuvar ve üniversitelerinde kullanılmaya başlanmıştır. Zaman içerisinde, daha da gelişerek hızla yayılmıştır. 1990 yılından itibariyle de internet adını alarak önce ABD üniversitelerinde, devamında ise tüm dünyadaki genel anlamlı kullanıcılara açılarak bugünkü noktasına ulaşmıştır.

İnternetin dünden bugüne uzanan bu dönüşümü, bugünden yarına nasıl bir gelişim ve dönüşüm göstereceği konusunda hayal gücünün sınırlarını zorlamaktadır. Ancak ilk gününden bugününe muazzam bir yayılım gösterdiği de bilinen bir gerçektir. Bu noktada, Tablo 3 son on yıla ait dünyadaki internet kullanıcısı sayılarındaki değişimi göstererek internetin mevcut yayılımını göz önüne sermektedir.

Tablo 3. Son On Yıla Ait Dünyadaki İnternet Kullanıcısı Verileri

Yılı	Dünya Nüfusu	Dünya Üzerindeki İnternet Kullanıcılarının	
		Sayısı	Dünya Nüfusuna Oranı
2021	7.83 Milyar	4.66 Milyar	%59
2020	7.75 Milyar	4.54 Milyar	%59
2019	7.67 Milyar	4.8 Milyar	%56
2018	7.59 Milyar	4.02 Milyar	%53
2017	7.47 Milyar	3.77 Milyar	%50
2016	7.39 Milyar	3.41 Milyar	%46
2015	7.21 Milyar	3.01 Milyar	%42
2014	7.09 Milyar	2.48 Milyar	%35
2013	7.01 Milyar	2.33 Milyar	%33
2012	6.80 Milyar	2.07 Milyar	%30

Kaynak: Hootsuite, 2012; 2013; 2014; 2015; 2016; 2017; 2018; 2019; 2020; 2021.

Tablo 3'den anlaşılacağı üzere; 2021 yılı dünyasında, yaklaşım 4,66 milyar insanın interneti kullandığı görülmektedir. Bu sayı dünya nüfusunun %59'una tekâmül etmektedir. İnternet kullanamayacak olan çocuk, yaşlı ve hastaları da hesaba kattığımızda, bu oran artarak yüksek seviyelere ulaşacaktır. İlerleyen yıllarda da internet kullanmayan insan sayısı internet kullanamayacak durumda olanlarla sınırlı kalacaktır. Böylelikle internet, dünya üzerinde bulunan tüm insanlarca kullanılan ve ihtiyaçlar kategorisinde öncelik arz eden bir noktada olacaktır.

Tüm bu argümanlar göz önüne alındığında, internetin basit olarak fiziksel ya da elle tutulur bir araç olmadığı ve dünya üzerindeki tüm bilgisayar sistemlerini birbirine bağlayarak sürekli olarak büyüdüğü söylenebilmektedir (Özkan, 2006:45). Aynı zamanda bilgisayar ağlarının birbirine bağlanmasıyla ortaya çıktığı ve uluslararası bilgi iletişimi ağı olarak herhangi bir sınırlaması ve yöneticisi olmadan da çalışabildiği vurgulanabilmektedir (TDK). Tercih edilebilirliği konusunda ise bulunulan konumdan bağımsız olunarak bilgiye erişme, iletişim kurma, komuta ve kontrol gibi yüzlerce ihtiyaca yönelik gereksinimleri dünya çapında karşılayabilmesi ve de zaman içerisinde yeni ihtiyaçlara yönelik gereksinimleri giderilebilmesi kanıt olarak sunulabilmektedir. Bu bakış açısıyla da internet, kısaca ‘‘bilgisayar ağlarının birleşiminden oluşan ve onlarca farklı amaç için kullanılan bir bilgisayar ağı’’ olarak tanımlanabilmektedir (TürkNet Sözlük).

4.1.1.2. Siber İstihbaratın Siber Uzaydaki Önemli Hedef Alanları

Siber istihbaratın siber uzaydaki hedef alanlarını genel anlamda nitelendirebilmek oldukça güçtür. Çünkü siber uzayın kendisi sahip olduğu tüm özellikleriyle istihbarata o veya bu minvalde bir alan yaratmaktadır. Diğer bir yandan da sürekli gelişerek genişlemekte ve buna paralel olarak da istihbarata yeni alanlar açmaktadır. Bu sebepten kesin bir ifade kullanmamakla birlikte günümüzde en önemli hedef alanları olabilecek bileşenlerini kısaca belirtmekte yarar vardır. Günümüzde de bu bileşenler veri tabanları, web siteleri, sosyal medya platformları, bulut ortamlar ve mobil teknolojiler olarak seçilmiştir.

4.1.1.2.1. Veri Tabanları

İngilizce "database" anlamına gelen veri tabanları, en basit haliyle yapılandırılmış bilgilerin veya verilerin elektronik olarak depolandığı alanları ifade etmektedir. Herhangi bir konudaki, birbiriyle ilişkili ve düzenli bilgiler ile verilerin bir araya getirilmesiyle oluşturulurlar (Tekeli, 2015:2). Mantıksal olarak da gerçekte var olan ve birbiri arasında ilişki bulunan nesneler ile ilişkileri, kullanım amaçlarına uygun olarak düzenleyerek modelleme işlevi

görürler (Özkan:5). Ayrıca istenilen bilginin, istenilen türde ve istenilen sürede sistemin içerisinde saklanabilmesine de imkân tanırlar. Bu sayede de sistemi oluşturan verilere kolayca erişilerek verileri yönetmek, değiştirmek, güncellemek, kontrol ve organize etmek olanaklı hale gelir.

Veri tabanları olmadan herhangi bir sistemde bilgilerin veya verilerin kalıcı olarak saklanması oldukça zordur. Çünkü sistem, birbiri ile ilişkili verileri sistemli ve bağlantılı bir düzenleme biçimiyle saklamak veya dizayn etmek üzerine kurulmuştur. Dolayısıyla tutulan verilere erişim, geleneksel dosya sistemlerine göre daha kolay ve daha hızlı gerçekleşir. Kaybolma riski daha aza indirgenerek ulaşımda mekân kavramı ortadan kaldırılır. Sağladığı imkân ve kolaylıklar neticesinde de hızla yayılarak tüm alanlarda belirli bir sistem çerçevesinde kullanılmakta ve her geçen gün daha da gelişmektedir.

Veri tabanları günümüzde, bankacılık sektöründen otomotiv sanayisine, sağlık ve eğitim sistemlerinden kurum, kuruluş ve şirketlerin yönetim sistemlerine, telekomünikasyon ve iletişim sistemlerinden hava taşımacılığı gibi ulaşım sistemlerine, çok geniş alanlarda kullanılmakta olan bilişim sistemlerinin alt yapısını oluşturmaktadır. Ayrıca isimlendirilerek kategorize edilmiş klasörler ve içerisinde barındırılan dosyalar, arşivlenmiş metin, resim, müzik, video vb. veriler, oyun dosyaları, şirket çalışan bilgisi veya muhasebe verileri ya da telefon rehberi, web sitelerine ait veriler gibi tüm kayıtlarda yine veri tabanlarının günümüzdeki en basit örneklerindendir. Tüm bu örneklerin içerisinde de kullanıcıları açısından son derece önemli ve gizli bilgiler yer almaktadır. Doğal olarak veri tabanlarının içerisinde yer alan bilgileri, istihbari açıdan değerlendirdiğimizde çok önemli veriler olabileceği açıktır. Bu gerekçeyle veri tabanlarını istihbari açıdan kıymetli bir hazine olarak düşünmek mantıklı ve makul bir bakıştır.

4.1.1.2.2. Web Siteleri (İnternet Üzerindeki Sayfalar)

Türkçe karşılığı "dünya çapında ağ" olan ve kısaca "web" veya "www" olarak adlandırılan "world wide web", internet üzerinde birbirleri ile bağlantılı olarak yayınlanmakta olan hiper-metin dokümanlarıyla oluşturulmuş bir nevi bilgi sistemidir (Sözcü, 2019). Sistemi oluşturan dokümanların her birisine, world wide web sayfası veya bir diğer adıyla web sitesi adı verilir (Hürriyet, 2020). World wide web tarayıcısı adı verilen bilgisayar programları aracılığıyla da bu sayfalara, internet üzerinden erişim sağlanır (CNNTürk, 2019). Bu sonuçla birlikte, internet üzerinde yer alan web sayfalarında özgürce dolaşılarak her türlü metin, imaj,

resim, video ve diğer multimedya öğelerine ulaşılır ve de hiper bağlantılar gerçekleştirilerek diğer web siteleri arasında kolayca geçiş yapılır.

Web sitelerinin birçok farklı türü vardır. Online satış siteleri, haber siteleri, oyun siteleri, tanıtım siteleri, blog siteleri, paylaşım siteleri, forum siteleri, kişisel ve kurumsal web siteleri ile sağlıktan ekonomiye her türlü hizmet siteleri en bilindik örnekleridir. Sahip olduğu farklı türlerdeki yapısıyla bir yandan çok geniş alanlarda hizmet vererek satış, tanıtım, öğrenim, öğretim, etkileşim, paylaşım ve haberleşme gibi ihtiyaçlara cevap vermekte, diğer bir yandan çağın medyası olarak internet üzerinde yer alan bir nevi iletişim panosu işlevi görmektedir (Armadigital; Webstudio). Bu yönüyle de birçok alanda hizmet sunarak insanlar üzerindeki popülaritesini hızla artırmakta ve yeni alanlara yaygınlaştırılması sağlanmaktadır.

Web siteleri kısaca, internet üzerinden ziyaretçilerine ihtiyaca yönelik her türlü bilgiyi metin, görsel ve animasyon tarzında aktarmaktadır. Ayrıca yine, tüm bu ihtiyaçlar kapsamındaki gerekli olan hizmetleri sunarak karşılamaktadır. Sahip olduğu bu yapısı itibariyle de bir nevi internet üzerindeki tüm sayfaları kapsayan sanal bir doküman topluluğu olma özelliği taşımaktadır (Yağmurlu). Doğal olarak istihbarat açısından düşünüldüğünde, muazzam bir kaynak noktası olmaktadır.

4.1.1.2.3. Sosyal Medya Platformları

Sosyal medya, teknik anlamda Web 2.0[1] üzerinde üretilen her türlü içeriğin ve yapılanmanın kullanıcı merkezli bir şekilde üretilerek geliştirilmesine izin veren, aynı zamanda da tek yönlü bilgi paylaşımından çift taraflı ve eş zamanlı bilgi paylaşımına olanak sağlayan internet tabanlı uygulamaların bütününe verilen isimdir (Gül, 2020:41). Yapısı itibariyle kişi, kurum, kuruluş ve topluluklara internet üzerinden etkileşimli bir iletişim imkânı sağlayarak kişisel bilgi, resim, müzik, video, yazı vb. içerikleri paylaşılabildikleri ortamı yaratır (Oruç, 2019:40). Zaman, mekân ve erişilebilirlik açısından herhangi bir sınırlaması bulunmaz (Kartal, 2014:27). Kullanıcılarına ise bireysel ya da topluluk eşliğinde ilgilendikleri konulara ve alanlara yönelik sosyal ağ kurma, bazı konu ve kapsamlara katkı sağlama, gelişen olaylara hızlıca tepki verme fırsatı verir. Ayrıca büyük kitlelere hızlıca ulaşılarak kitlelerin davranışlarını etkileme ve de duygularını değiştirme kudreti sunar.

[1] Web 2.0, 2004 yılında ortaya çıkmış bir kavram olup, yazılım geliştiricilerin ve kullanıcılarının mevcut web teknolojilerinden yararlanışlarındaki değişimi yansıtır. Yani kısaca, ikinci nesil internet hizmetleri, toplumsal iletişim sistemleri ve iletişim araçları gibi internet kullanıcılarının ortaklaşa ve paylaşarak yarattığı sistemi tanımlamaktadır. Facebook, Twitter, Instagram, Youtube, Vikipedi, Blog, Ekşi Sözlük, Podcast, RSS, Wordpress vb. uygulamalar en bilindik örnekleridir.

Sosyal medya, sağlamış olduğu tüm bu kolaylıklar ve imkânların etkisiyle hızla yayılarak ekonomi, politika, sosyoloji, psikoloji, sanat, bilim, teknoloji gibi birçok alanda kullanılmaktadır. Etkinlik alanlarının genişlemesinin etkisiyle de günümüzde toplumun hemen her kesiminden bireylerin hayatına entegre olmayı başarmıştır (Tiryaki ve Özdal, 2020:18). Tablo 4'ün incelendiğinde, sosyal medyanın hızlı yayılımı ve günümüzdeki entegrasyonu daha iyi algılanabilecektir.

Tablo 4. Son On Yıla Ait Dünyadaki Sosyal Medya Kullanıcısı Verileri

Yılı	Dünya Nüfusu	Dünya Üzerindeki Sosyal Medya Kullanıcılarının	
		Sayısı	Dünya Nüfusuna Oranı
2021	7.83 Milyar	4.20 Milyar	%53
2020	7.75 Milyar	3.80 Milyar	%49
2019	7.67 Milyar	3.48 Milyar	%45
2018	7.59 Milyar	3.19 Milyar	%42
2017	7.47 Milyar	2.78 Milyar	%37
2016	7.39 Milyar	2.30 Milyar	%31
2015	7.21 Milyar	2.07 Milyar	%29
2014	7.09 Milyar	1.85 Milyar	%26
2013	7.01 Milyar	1.72 Milyar	%24
2012	6.80 Milyar	1.48 Milyar	%22

Kaynak: Hootsuite, 2012; 2013; 2014; 2015; 2016; 2017; 2018; 2019; 2020; 2021.

Tablo 4'de görüldüğü üzere; 2021 yılı dünyasında, yaklaşık olarak dünya nüfusunun %53'ünü oluşturan 4,20 milyar insan, sosyal medyayı o veya bu sebepten ötürü kullanmaktadır. Bu sayı, Tablo 3'de belirtilmiş olan 4,66 milyarlık internet kullanıcısı sayısına çok yakındır. Yani 2021 yılında interneti kullananların yaklaşık %90'ı aynı zamanda da sosyal medyayı kullanmayı tercih etmektedir. Dolayısıyla ilerleyen süreçte internet kullanımında yaşanacak artışlar sosyal medya kullanımını da artıracaktır.

Sosyal medyanın tüm bu yeri, önemi ve yapısı esnek, ucuz ve hızlı olması sebebiyle istihbarat açısından önemli bir veri kaynağıdır. Sosyal medya aracılığıyla kişisel verilerden yapılan etkinliklerin bilgisine, konum ve bulunulan yer bilgisinden etkileşime geçilen kişilerle olan sohbet ve paylaşım gibi bilgilere ulaşılabilir. Doğal olarak sosyal medyanın istihbarat toplayan kişi, grup veya servislere büyük fırsatlar yaratığı açıktır. Böylelikle sosyal medyadan istifade edilerek kişiler, gruplar, kurumlar, toplumlar ve hatta ülkeler hakkında bilgi toplayabilmek imkân dâhilindedir.

4.1.1.2.4. Bulut Ortamlar

Bulut ortamlar, siber uzayda yer alan ve İngilizce 'cloud computing' anlamına gelen 'bulut bilişim[2]' sistemlerinin tümünü ifade etmektedir. Bu sistemler internet tabanlı bilişim hizmeti sunarak temel kaynaklardaki yazılım ve bilgilerin internet üzerinden paylaşılmasına, veri depolama ve bilgi işlem gibi bilgisayar sistemlerine yönelik kaynakların aktif bir yönetim olmaksızın isteğe bağlı olarak doğrudan kullanılmasına imkân sağlamaktadır. Çalışma mantığı, mevcut bilişim hizmetlerinin kullanıcısı bakımından hiçbir donanıma gerek duyulmadan internet veya benzeri bir bilişim ağı üzerinden gerçekleştirilmesi biçimindedir. Bu yönüyle de bir ürün olmaktan daha çok fiziki olmayan hizmet vasfında sanal bir sunucudur. Kullanıcılarına her türlü dosya ve veriyi siber uzayda rahatlıkla saklama, yedekleme, kullanma ve paylaşma gibi fırsatlar sunmaktadır. Ayrıca kullanımları son derece kolay ve az maliyetlidir. İşletim giderleri düşük olmakla birlikte kurulumu ve değişimi de son derece hızlı ve de kolaydır. Her zaman ve her yerde erişim imkânı mümkün olup, enerji tüketimleri de düşüktür. Yedekleme işlemleri basitçe yapılarak ölçeklendirilebilmektedir. Güncellemeleri zamanında yapılarak yeni teknolojiler eklenmekte ve sorunlar çok çabuk çözülmektedir. Bu nedenle bulut teknolojisi kişi, grup, örgüt, kurum, kuruluş gibi kullanıcılarına cazip gelmekte ve hızla gelişmeye devam etmektedir.

Dünya artık bulut ortamlarında çalışmakta, üretmekte, yönetmekte, öğrenmekte, araştırmakta, geliştirmekte, hizmet vermekte, haberleşmekte ve paylaşımda bulunmaktadır (Sağıroğlu, 2019:53). Kişiler, gruplar, örgütler, kurum ve kuruluşlar ihtiyaçlarını bulut ortamlardan istifade ederek karşılayabilmektedir. Doğal olarak içerisinde barındırabileceği bilgileri göz önüne aldığımızda, istihbarat açısından önem verilmesi gereken kıymetli bir hedef noktası olduğu göz ardı edilemeyecektir.

[2] Bulut Bilişim, kullanıcılarına bilgisayar ve diğer cihazlara yönelik istenildiğinde kullanılabilecek, saklanabilecek ve de paylaşılabilecek kaynakları sunan, internet tabanlı bilişim hizmetlerine verilmiş olan genel bir isimdir (Yeniakit, 2020).

4.1.1.2.5. Mobil Teknolojiler

Mobil kelimesi, kolay hareket ettirilebilme becerisini tanımlayan bir sıfat manasındaki Latince "mobilis" kelimesinden türetilmiştir (Dictionary). Bu sıfata bağlı teknolojilerde, hücresel haberleşme teknolojisinin çeşitli türlerini tanımlamak üzere geliştirilmiştir (Çakmak ve Yalçın, 2013:2). Mobil teknolojilerin geliştirilmesiyle de genel ağa (internete), sosyal ağlara ve kablosuz ağlara bağlı, bilgisayar özelliklerine sahip akıllı cihazlar üretilerek insanlığın kablo bağımlılığı ortadan kaldırılmıştır.

Mobil teknolojiler, günümüzde çoğunlukla akıllı telefon, tablet, notebook, ultrabook, dizüstü bilgisayar, akıllı saat, akıllı gözlük, etkinlik izleyici gibi giyilebilir ya da el yordamıyla kolay taşınabilir cihazlar ile bu cihazlara ait olan her türlü donanım, yazılım, uygulama ve iletişim anlamındaki teknolojiyi tanımlamaktadır (Kayabaş, 2018:101). İşlemci, ekran, kamera, mikrofon, bağlantı kartları ve algılayıcı sistemlerin elektronik bileşenleri gibi mobil cihazları oluşturan her türlü somut parçalar, mobil donanımların en bilindik örneklerindendir. Mobil yazılımlar ise adından anlaşılacağı üzere (android, ios, windows 10, tizen vb.) mobil işletim sistemleri ile mobil uygulamaların makine komutları gibi, donanımların çalışmasını sağlayan ve de mobil uygulamaların tasarımının arka planında çalışan komut sistemlerinin bütünüdür. Mobil uygulamalarda, daha çok (siri, google now vb.) dijital yardımcılar, görüntü sabitleyici veya tanımlayıcıları, yüz, parmak izi, göz ve ses algılayıcıları gibi çok sayıdaki sistemler olup, tamamen kullanıcılarının güncel ihtiyaçlarına çözüm üretmek amacıyla ortaya çıkartılmaktadır. Bu teknolojilere mobil bankacılık uygulamalarından alışveriş uygulamalarına, mobil sosyal medya uygulamalarından oyun uygulamalarına kadar uzanan yüklenebilir tüm platformlarda dâhildir. Mobil iletişime ait teknolojinin bileşenleri ise telsiz, telefon, uydu sistemleri, (wi-fi, GPS, bluetooth vb.) hücresel bağlantı sistemleri, 1G'den 5G'ye hücresel ağlar gibi iletişime yönelik sistemlerdir. Bu sistemler mobil teknolojide yaşanan değişim ve dönüşüme bağlı olarak sürekli yenilenerek geliştirilmektedir. Böylelikle iletişimde kalite ve kapasite artışı sağlanmakta ve daha verimli bir model ortaya konmaktadır.

Mobil teknolojiler, tüm bu yapısından dolayı kullanıcılarına bulunulan yer ve zamandan bağımsız olarak anında işlem yapabilme yeteneği sunmaktadır (Kayabaş, 2018:101). Sunmuş olduğu tam zamanlı işlem ve iletişim yeteneği sayesinde, başta akıllı telefonlar ve tabletler olmak üzere hızla yayılarak hemen hemen her alanda kullanılmaktadır. Teknolojiye bağlı olarak yaşanan değişim ve dönüşüm süreci de yayılma hızına doğrudan etki etmektedir. Tablo 5'deki son yedi yıla ait dünyadaki benzersiz mobil kullanıcısı sayları incelendiğinde, mobil teknolojilere ait yayılım daha iyi anlaşılabilecektir.

Tablo 5. Son Yedi Yıla Ait Dünyadaki Benzersiz Mobil Kullanıcısı Verileri

Yılı	Dünya Nüfusu	Dünya Üzerindeki Benzersiz Mobil Kullanıcılarının	
		Sayısı	Dünya Nüfusuna Oranı
2021	7.83 Milyar	5.22 Milyar	%66
2020	7.75 Milyar	5.19 Milyar	%67
2019	7.67 Milyar	5.11 Milyar	%67
2018	7.59 Milyar	5.13 Milyar	%68
2017	7.47 Milyar	4.91 Milyar	%66
2016	7.39 Milyar	3.79 Milyar	%51
2015	7.21 Milyar	3.64 Milyar	%51

Kaynak: Hootsuite, 2015; 2016; 2017; 2018; 2019; 2020; 2021.

Tablo 5'den anlaşılacağı üzere, 2021 yılı itibariyle dünyadaki benzersiz mobil kullanıcı sayısı yaklaşık olarak 5,22 milyara ulaşmıştır. Bu sayı 2021 yılı itibariyle, dünya nüfusunun %66'sına denk gelmektedir. Çocuklar, yaşlılar ve hastalar gibi mobil kullanıcısı olmayacak insanları da düşündüğümüzde bu oranın %90'lara ulaşabileceğini değerlendirmek son derece mantıklıdır. Ayrıca yine tabloya baktığımızda, benzersiz mobil kullanıcısı ile birden fazla mobil kullanan kişilerin tek bir kullanıcı olarak sayıldığı anlaşılmaktadır. Dolayısıyla bir kişinin birden fazla mobil kullanıcısı olabileceğini göz ardı etmemek gerekir. Tüm bu sonuçlar da bizlere, mobil teknolojilerin yaşam düzeninde çok aktif bir rol oynayarak insanların hayatına adapte edildiğinin en büyük göstergesidir.

Mobil teknolojilerinin kısa zamanda ulaştığı bu yaygınlık ve gelişmişlik, ilerleyen yıllarda teknolojik gelişmelerinde etkisiyle toplumun hemen hemen her kesimince benimsenerek kullanılmasına neden olacaktır. Kullanılan teknolojinin içerisinde de bugün olduğu gibi, kişilerin yüz, ses, göz biyometrisi[3] ve parmak izi gibi kişisel özelliklerinden her

[3] Biyometri, kısaca yaşayan organizmalara ait ayırt edici ölçümlere verilen genel bir isimdir. Yüz biyometrisi, insanların kendilerine özgü yüz izlerini baz alınarak analog (yüz) bilgilerini dijital bilgiler (veri) kümesine dönüştürerek kimliklendirir. Ses biyometrisi, temel olarak bir ses imzası niteliğinde olup, insanların kimliğini eşsiz

türlü metin, resim, video, ses kayıtları ve konum bilgisinin bulunduğu, istihbari açıdan son derece değerli verileri barındıracaktır. İstihbari verileri barındırması ise istihbarat ihtiyacının karşılanabilmesi için mobil teknolojileri cazip kılacaktır. Nihayetinde de mobil teknolojiler, uzaktan erişildiği takdirde istihbarat servislerince son derece değerli bir bilgi deposu olacaktır.

4.1.2. Siber Savaşçılar

Siber savaşçılar, siber uzayda yer alan bilgileri elde etmeye çalışan hem zeki hem de yüksek donanıma sahip kişi veya gruplardan oluşmaktadır. Bilgi elde etmedeki maksatları farklılık göstermekle birlikte, kullandıkları metotlar hemen hemen aynıdır. Dolayısıyla siber savaşçıları, istihbarat açısından ele aldığımızda, siber uzayda gerek kişisel gerekse kurumsal ya da örgütsel anlamda yer alan önemli bilgileri, her ne sebeple olursa olsun ele geçirmek isteyen zeki ve yüksek donanıma sahip kişiler veya gruplar olarak değerlendirmek mümkündür (Keleştemur, 2015:209). Bu değerlendirmeye istinaden de siber savaşçılara mensup kişi veya grupların karakteristik özelliklerini belirtmek son derece faydalı olacaktır.

4.1.2.1. Hackers (Bilgisayar Korsanları)

Türkçede karşılığı ‘‘bilgisayar korsanı’’ anlamına gelen hacker kelimesi, kökeni itibariyle ‘‘koparmak, kırmak veya küçük parçalara ayırmak’’ gibi anlamlara gelen İngilizce ‘‘hack’’ kelimesinden türetilmiştir. Kelimenin ‘‘hacking’’ olarak genişletilmesi neticesinde de herhangi bir sistemde veya programda yer alan açıkların ortaya çıkartılarak ele geçirilmesi, değiştirilmesi ya da silinmesi kavramı ortaya çıkmıştır. Ortaya çıkan kavram çerçevesinde faaliyetlerde bulunan kişiler ise ‘‘hacker’’ olarak nitelendirilmiştir (Çokbildik, 2019:48). Ancak bu ifade hacker kavramını tam anlamıyla tanımlamakta yeterli değildir. Zira hackerlar, internet, bilgi teknolojileri ve ağ altyapılarına son derece hâkim kişiler olup, aynı zamanda programlama dillerinden en az bir tanesini çok ileri bir seviyede bilmektedirler. Sahip oldukları programlama yeteneğiyle, zararlı yazılımlar yazarak bilişim ağ ve sistemlerine kolaylıkla sızmaktadırlar. Sisteme sızdıkları andan itibaren ise arzu ettikleri her türlü verilere ve bilgilere fark edilmeden kolayca erişebilirler. Gerektiğinde sosyal mühendislik[4] gibi yöntemlere başvurarak hedef kitlelerini etkileyebilme kabiliyetleri de bulunabilmektedir. Dolayısıyla sahip oldukları tüm bu özellikleri sebebiyle, bilişim sistemlerine erişim yetkisi olmadığı halde herhangi bir yolunu bularak bu sistemlere fark edilmeden erişen, eriştiği sistemdeki bilgileri alan, değiştiren, silen

ses izleri ile tanımlar. Göz biyometrisi ise insanların kimliğini doğrulayabilmek için gözlerinin renkli çemberlerindeki benzersin desenleri ölçer.

[4] Bilginin güvenliği bağlamında değerlendirdiğimizde, ihtiyaç duyulan her türlü bilginin elde edilebilmesi amacıyla hedefte bulunan kişilerin psikolojik olarak manipüle edilmesi sosyal mühendislik olarak nitelendirilir. Sosyal mühendislik eylemleriyle insanların zafiyetlerinden faydalanılarak gizli bilgiler ifşa edilebilmektedir.

veya bozan son derece yetenekli ve bilgili kişiler olarak kısaca tanımlanabilirler (Akdeniz, 2013:9).

Hackerlar her türlü programı, siteyi veya bilgisayar sistemlerini güvenlik açıklarından yararlanarak kolayca kırabilmektedirler (Çiftçi'den [2013] aktaran Özçoban, 2014:55). Ancak yaptıkları saldırıların amaçları veya neticesi onları farklı bir kimliğe büründürmektedir. Çünkü hackerlar yaptıkları saldırının amaçları ve neticesi münasebetiyle siyah, beyaz ve gri şapkalı hackerlar olmak üzere üç ana gruba ayrılmaktadır. Sistemi kolayca kıran hackerlar, kötü bir amaçla bunu yaptıkları ya da sistemleri kullanılamaz hale getirip, bilgileri değiştirdikleri veya gizli bilgileri ele geçirdikleri takdirde siyah şapkalı grupta değerlendirilirler. İyi bir amaçla sistemi kırdıkları ya da kırdıkları sistemlerdeki açıkları sisteme zarar vermeden tespit ederek sistemin zarar görmemesi açısından ilgili sistem yöneticisine o açıkların kapatılmasını bildirdikleri takdirde de beyaz şapkalı olarak nitelendirilirler. Ancak yasallık sınırında bir saldırı yaparak iyi veya kötü olabildikleri takdirde, siyah ve beyaz arasından gri şapkalı grupta kendilerine yer bulurlar. Yani yöntemleri bakımından siyah şapkalılarla aynı çizgide olmakla birlikte amaçları bakımından beyaz şapkalılarla aynı düşüncede olup arada fakat beyaz gruba daha yakın bir duruş sergilediklerinde gri şapkalı hacker grubunda yer alırlar.

Hackerlar hangi grup ve düşünce yapısında olursa olsun son derece yetenekli kişilerdirler. Bir yandan büyük faydalar sağlayan önemli kişiler olabilecekleri gibi diğer bir yandan da son derece tehlikeli kişiler olabilme ihtimalleri yadsınamaz. Bu nedenle devletlerin hemen hemen her konuda olduğu gibi hackerlar konusuna da önem verilerek bu kişilerin insanlığın faydasına hizmet etmeye yönlendirilmesi gereklidir. Bu başarıldığı takdirde, yeni bir boyut olan siber uzayda gerek istihbari açıdan gerekse siber güvenlik açısından büyük kazanımlar elde edilebilecektir. Çünkü hackerlar, siber uzayda gerek istihbari açıdan gerekse güvenlik açısından son derece önemli kişilerdendirler. Siber uzayda büyük çaplı saldırılar gerçekleştirebilecekleri gibi aynı orandaki saldırıları savunma imkân ve kabiliyetleri de bulunmaktadır. Doğal olarak hackerların insanlığın yararına kazanılması, gerekli imkân ve fırsatların tanınarak faydalı işlerde kullanılması, her konuda önemli kazanımlar elde edilebilmesinde devletlere büyük katkı sunacaktır.

4.1.2.2. Siber Casuslar

Genel anlamda istihbarat toplamanın bir alt kümesi içerisinde yer alan casusluk kavramı, herhangi bir bilginin gizli ya da gizli olarak kabul edilen bilginin bir hükûmet veya şirketin hizmetinde olan ya da bağımsız olarak faaliyet gösteren bir kişi ya

da iş birliği yapan bir grup tarafından edinilmesi süreci olarak karşımıza çıkar (Güven, t.y.). Sürecin içerisinde bulunarak bilginin edinilmesini sağlayan kişi ya da iş birliği içerisinde olan grup üyeleri de casus veya ajan olarak adlandırılırlar. Ancak bir casusu tanımlayabilmek bu kadar basit değildir. Çünkü casuslar son derece yetenekli kişilerdir. Teknik, taktik ve teknolojik anlamdaki yeterlilik düzeyleri sayesinde, izlerini belli etmeden istedikleri bilgiye ulaşabilme ve de o bilgiyi bağlı olduğu birime servis edebilme konusunda uzmanlaşmışlardır. Dolayısıyla sahip oldukları özellikleri münasebetiyle gerek devletler gerekse gizli servislerce asla göz ardı edilmemişlerdir. Her daim üzerlerine düşülerek teknik, taktik ve teknolojik anlamdaki yetenekleri daha da geliştirilmiştir. Böylelikle istihbarat servisleri açısından son derece önemli kişiler haline gelmişlerdir.

Casuslara verilen bu önem, sahip oldukları tüm bu özellikleriyle birleşince, yaşanan yeni gelişmelere kısa sürede adapte olabilmelerini kolaylaştırmıştır. Özellikle siber uzayın yaratmış olduğu imkân, fırsat ve avantajlara adapte olarak faaliyetlerini bu alana kaydırmaları, siber casusluk[5] denilen yeni bir yöntemin ortaya çıkmasını sağlamıştır. Siber casusluk yöntemiyle casuslar, iletişim ağlarına veya bilgisayar ağlarına yasal olmayan yöntemlerle sızmayı başararak ihtiyaç duydukları her türlü bilgi ve belgeleri bağlı oldukları birime, fark edilmeden kolayca sızdırabilmişlerdir (Keleştemur, 2015:162). Sızdırdıkları bilgi ve belgeler sayesinde, bağlı oldukları yerin, karşı tarafa üstünlük sağlayabilecek güçte bir konuma gelebilme olasılığı kuvvetlenmiştir. Bu sonuç gerek devletlerin gerekse kurum veya kuruluşların siber casusluk faaliyetlerine olan ilgisini daha da artmıştır. Nihayetinde ise siber casusluk faaliyetini yürütebilecek casusların yetiştirilmesi ya da bulunarak devşirilmesi önemli bir gereksinim olmuştur.

Yetiştirilmesi ya da bulunarak devşirilmesi gereken bu kişileri, siber casus veya bir diğer adıyla siber ajan sıfatıyla anmak mümkündür. Çünkü siber casus olarak tanımlanan bu kişiler, bir yandan klasik casusluk yöntemlerini siber uzayda uygularken diğer bir yandan da siber casusluk faaliyetlerini yürütebilmektedirler. Bu sebepten klasik casusluk yöntemlerini siber uzayda uygulayan kişiler ile siber casusluk faaliyetlerini yürüten kişileri, birer siber casus olarak tanımlayabilmek doğru bir bakıştır. Ancak konunun derinliği açısından değerlendirdiğimizde, siber casus kavramını bu kadar basit tanımlamak yeterli olmayacaktır. Konuyu daha teknik boyutta düşündüğümüzde, siber casusların da aslında birer hacker türevleri

[5] Kısaca politik, askeri, siyasi vb. amaçlar için kurum, kuruluş ya da devletlerin bilgi sistemlerinden ihtiyaca yönelik her türlü bilgi veya belgelerin çalınması olarak tanımlanır (kotuamacliyazilim.com, 2016).

olduğu görülecektir. Siber casusların çoğu zaman hackerlar kadar teknik bilgiye sahip olmaları da bu düşünceyi desteklemektedir. Dolayısıyla hackerlar kadar teknik bilgisi bulunan siber casusları gerek yazılımsal gerekse donanımsal anlamda bilgiye sahip olmakla birlikte, sosyal mühendislik konularında son derece başarılı ve gelişmiş bir pratik zekâya sahip kişiler olarak nitelendirmek mantıklı bir yaklaşımdır.

Siber casuslara yönelik yapılan tüm bu açıklamaların yanında, yanlış anlaşılmaları ortadan kaldırmak adına, bir siber casusu hackerden ayıran önemli özelliklerin belirtilmesi gerekir. Siber casusları hackerlerden ayıran temel özellikler ise şöyledir. Siber casuslar bir devlete, kurum veya kuruluşa bağlı olarak onların hedefleri doğrultusunda faaliyetlerini yürütürken hackerlar daha çok kendi amacına hizmet etmektedir. Bu nedenle siber casusların sızdıkları sisteme herhangi bir zarar vermeden, arkalarında iz bırakmayıp elde ettikleri bilgiyi bir üst makama rapor etmeleri görevlerinin en önemli gerekliliğidir. Hackerların ise böyle bir görevi bulunmamakla birlikte, sızdıkları sisteme zarar verip vermemeleri tamamen kendi arzularında olan bir durumdur. Sonuç itibariyle siber casuslar herhangi bir devletin, kurum veya kuruluşun hizmetine yasal olmayan yollarla hizmet eden kişilerken hackerlar ise yine yasal olmayan yollarla kendi amaçlarına hizmet eden kişilerdir. Ancak kendi amacına hizmet eden hackerların ikna edildiği takdirde birer siber casusa devşirilebilme ihtimallerinin olabileceği göz ardı edilmemelidir.

4.1.2.3. Toplum Mühendisleri

Toplum mühendisleri, sosyal mühendislik konularında son derece uzmanlaşmış olmaları sebebiyle, genel anlamda sosyal mühendisler olarak bilinirler. Ancak onları tanımlayan en önemli özellikleri, ileri seviyede psikoloji ve sosyoloji bilmelerinin yanında bilişim teknolojilerine de son derece vakıf olmalarıdır. Hatta öyledir ki birçoğunun teknik anlamda kendisini, hackerlar kadar geliştirerek bilişim alanında uzmanlaşmış olduğu söylenmektedir (Keleştemur, 2015:212). Tam da bu noktada onları diğerlerinden ayıran kritik konu ise sahip oldukları bilgi ve birikimlerinin yanında üstün bir pratik zekâ ve hitabet yeteneklerinin de bulunmasıdır. Çünkü tüm bu özellikler, toplum mühendislerinin siber uzayda bireysel veya toplu verilere sahip olabilme kapasitelerini arttırarak internet üzerinden manipülatif eylemler gerçekleştirebilme yeteneklerini de geliştirmektedir. Bu sayede de ihtiyaç duyulan her türlü bilginin elde edilebilmesi amacıyla hedefte bulunan kişilerin psikolojik olarak manipüle edilmesi, toplum mühendisleri açısından kolaylıkla yürütülebilen bir faaliyet olmuştur.

Toplum mühendislerinin yapmış olduğu faaliyetlerinde, bir istihbaratçı veya bir ajan gibi farklı kişiliklere bürünebilmesi, hedefte olan kişilerin manipüle edilerek ihtiyaç duyulan bilgilere ulaşılabilmesi açısından önemli bir gereklilik oluşturabilecektir. Bu gereklilik başarılabildiği takdirde toplum mühendislerinin, hedeflerinde olan kişilere karşı güvenlerini kazanabilmesi daha kolay olabilecektir. Hedefin güveni kazanıldıktan sonra, açıklıkların tespit edilebilmesi ve istenilen her türlü bilgiye ulaşarak bilgilerin üst makamlara sızdırılabilmesi basitleşebilecektir. Bu nedenle toplum mühendislerinin harekete geçmeden önce hedef kişi hakkında önceden istihbarat elde etmeleri gerekmektedir. Çünkü elde ettikleri istihbarat sayesinde, kendilerine bir harekât planı belirleyerek hedefle irtibat kurmaları ve bu sayede hedef üzerinde güven ilişkisi tesis edebilmeleri mümkün olmaktadır. Böylelikle toplum mühendislerinin hedefledikleri kişileri faaliyetleriyle etkileyerek fikirlerini, amaçlarını ve eylem planlarını ortaya çıkarabilmeleri ve bu sayede bunları duruma göre gerek savuşturabilmeleri gerekse farklı bir hedefe yönlendirebilmeleri imkân dâhilinde olabilecektir.

Tüm bu sonuçları göz önüne aldığımızda, toplum mühendisliğinin istihbarat servislerince değer verilmesi gereken kritik bir alana dönüşmüş olduğunu söylemek doğal bir sonuçtur. Bu sonuçla toplum mühendislerinin toplum yararına gerek yetiştirilmesi gerekse yetiştirilmiş olanlarının geliştirilerek kullanılması önemli bir gereksinim haline gelmektedir. İnternet ve sosyal medya kullanım artışı oranları da göz önüne alındığında bu gereklilik daha da belirginleşmektedir. Dolayısıyla günümüzde toplum mühendisliği konusunda istihbarat servislerinin son derece aktif bir pozisyonda yer alarak toplumun yararına faaliyet yürütmesi elzemdir.

4.1.2.4. Kriptocular ve Kripto Analizciler

Kriptocular ve kripto analizciler, kriptografi[6] alanının önemli iki ögesini oluşturan ve aynı zamanda da kriptografi alanında son derece uzmanlaşmış kişilere denilmektedir. Ancak bu iki grubun her ne kadar ilgilendikleri alan aynı olsa da faaliyetleri farklılık göstermektedir. Çünkü kriptocular, verileri şifrelemekle sorumlu kişilerken kripto analizciler, tam tersi olarak şifreli verileri deşifre etmek ya da çözümlemekten sorumlu kişileri ifade etmektedir. Yani bir diğer ifadeyle, birbirlerinin rakipleri olup, birisi kriptografinin şifrelenme alanına yönelik çalışırken diğeri şifrelerin çözümlenerek deşifre edilmesi alanına yönelik çalışmalarını sürdürmektedir. Dolayısıyla bu iki kavramın birbirinden ayrı olarak kısaca incelenmesi gerekir.

[6] İletilmek ya da depolanmak istenen bir verinin, bir anahtar veya fonksiyon kullanılarak anlaşılamayacak hale getirilmesini (şifrelenmesini) ve yine aynı yöntemlerle istenildiği zamanda eski haline dönüştürülmesini (deşifrelemesini) sağlayan bilim dalıdır (Cenk, 2019:65).

Kriptografinin temelinde gizlilik, kimlik denetimi ve bütünlük gibi belli başlı bilgi güvenliğinin sağlanmasına yönelik matematiksel çalışma yöntemlerinin bulunduğu bilinmektedir (Keleştemur, 2015:218). Kriptoculardа, kriptografinin bu yöntemini kullanarak verilerin bir başkasının eline geçmesi ihtimaline karşı, gerekli şifreleme işlemlerini yaparak verinin okunulamaz ya da kullanılamaz bir hale getirilmesinden sorumludurlar. Şifreleme işlemini iyi yaptıkları takdirde, bilginin iletimi veya depolanması sırasında karşılaşılabilecek olası aktif ya da pasif saldırılara karşı bilgiyi koruyabilecekleri gibi, bilgiyle birlikte göndericiyi ve alıcıyı da korumayı başarabileceklerdir. Bu sonuçta kriptoculara, tıpkı istihbarata karşı koyma prensiplerinde olduğu gibi verinin yanında, veriyi oluşturan, alan ya da gönderen taraflarında korunarak deşifre edilmemesi gerektiği sorumluluğunu yüklemektedir. Ortaya çıkan sorumluğun en büyük gerekçesi ise bilgiye ulaşmak kadar eldeki bilgiyi korumanında önemli bir kazanım olduğu gerçeğidir. Bu gerçeklikte kriptocuların varlığını başta devletler olmak üzere kurum, kuruluş, güvenlik ve istihbarat servisleri açısından son derece gerekli kılmaktadır.

Kriptografinin içerisinde yer alan bir diğer önemli yöntem ise şifrelenmiş metinlere ait güvenlik algoritmalarının incelenmesi ve analiz edilerek çözümlenmesi sürecidir. Kriptoanaliz süreci olarak adlandırılan bu süreçte, kriptografik algoritmalarla şifrelenmiş verilerin çözümlenerek orijinal haline getirilmesi ya da çözümlenmesine yönelik gizli anahtarının ortaya çıkarılmasına çalışılmaktadır (Cenk, 2019:67). Kripto analizcilerde, kriptografinin burada belirtilen çalışmalarını yaparak kriptografik sistemleri ve algoritmaları analiz etmekle sorumludurlar. Ancak kriptografik algoritmalarla şifrelenmiş bir veriyi çözümlemek sanıldığı kadar kolay bir iş değildir. Çünkü kriptografik şifreleme yöntemleri, son derece geniş ve hayal gücünün sınırlarını zorlayan birçok metottan oluşabilmektedir. Bu zorluğu aşabilmek adına ilk olarak yeni ve gelişmiş kripto analiz metotlarının ortaya çıkarılması gerekmektedir. İkinci olarak ise ortaya çıkarılan bu metotları doğru yer ve zamanda kullanabilecek yetenekli kripto analizcilerin yetiştirilmesi gerekmektedir. Bu başarıldığı takdirde iyi yetiştirilmiş bir kripto analizcinin sahip olduğu yetenekle doğru metodu doğru yer ve zamanda uygulayarak sonuç alma olasılığı yükselecektir. Zira ele geçirilmiş olan veriler kriptografik algoritmalarla şifrelenmiş olduğundan çözümlenemediği takdirde bir anlam ifade etmeyeceği bilinmelidir. Dolayısıyla bu noktada kripto analizcilere, verilerin deşifre edilerek okunabilmesi ve bu sayede istihbarat niteliğindeki bir bilgiye dönüştürebilmesi açısından oldukça önemli işler düşecektir (Keleştemur, 2015:217).

4.1.2.5. Yazılımcılar

Siber istihbaratta başarılı sonuçların elde edilebilmesinde, bir diğer önemli etken de istihbarata yönelik yeni yazılım ve programların geliştirilmesidir. Çünkü doğru, etkin, başarılı ve içinde bulunulan dönemin ihtiyaçlarına cevap verebilecek şekilde yazılmış ya da güncellenmiş olan bir yazılım veya program, siber istihbaratın elde edilmesinde bir nevi silah olma rolü üslenmektedir. Ancak siber istihbaratta birer silah olma özelliği taşıyan tüm bu yazılımlar ve programların üretilmesi ya da geliştirilmesi sanıldığı kadar kolay değildir. İlk olarak ihtiyaç veya gereksinimlerin ortaya konulması gerekmektedir. İkinci olarak yeterli bilgi, birikim ve teknolojik altyapıya sahip bir yazılımcı bulunmalıdır. Sonrasında ise geriye sadece yazılımcının ihtiyaca yönelik siber silahı üretmesi aşaması kalacaktır. Hedefine uygun siber silahı ürettiği takdirde de başarıya ulaşılacaktır.

Siber istihbaratta yazılımcıların rolü bu kadarla sınırlı değildir. Aynı zamanda yazılımcılardan üretmiş ya da geliştirmiş oldukları yazılım ve programların yanında, tersi bir bakışla kendilerine karşı yazılmış ya da geliştirilmiş olan program ve yazılımlara karşı sistemi güvende tutmaları istenir. Sistemi güvende tutabilmek içinde, yazılımcıların çeşitli güvenlik ve saldırı önleyici yazılım ve programları yazmaları gerekir. Doğru zamanda doğru yazılımı veya programı geliştirebildikleri takdirde de sistem güvende tutulabilecektir. Bu sebepten gerek siber istihbaratın elde edilebilmesinde gerekse sistemi güvende tutmaya yönelik güvenlik ihlallerinin önlenebilmesinde ihtiyaç duyulan tüm yazılım ve programların üretilebilmesi için yetenekli yazılımcılara sahip olmak büyük bir gerekliliktir (Keleştemur, 2015:218).

Tüm bu gerekliliklerden ötürü, istihbarat teşkilatlarının birbirinden başarılı yazılımcıları istihdam etmeleri elzemdir. Çünkü ihtiyaca yönelik üretilen veya geliştirilen bir yazılım veya programın başarıya ulaşması için karmaşık problemleri çözebilen, analiz yapabilen, geçmişle bugün arasında bağ kurarak yarını değerlendirebilen yazılımcıların elinde şekillenmesi çok daha değerlidir. Dolayısıyla yazılımcıların istihbarat servislerince istihdam edilerek geliştirilmesi siber istihbarat açısından önemli bir gereksinimdir.

4.1.3. Siber Silahlar

Siber silahlar, siber uzayda gerek duyulan istihbaratın elde edilebilmesi için siber savaşçılarca kullanılmakta veya üretilmekte olan yazılım, program, uygulama ve donanım gibi soyut ve somut vasıtaları ifade etmektedir. Bu vasıtalar aracılığıyla siber savaşçıların siber uzayda fark edilmeden istihbarat faaliyetlerini yürütebilme olanakları artmaktadır. Dolayısıyla siber istihbaratın elde edilmesinde siber savaşçılara kolaylıklar sağlayacak siber silahların

bilinmesi önemlidir. Ancak siber silahlar, hedef sistemlere göre farklı üretilmiş olduklarından sağlamış oldukları faydalar kadar tehlike arz eden zararları da içermektedir. Siber silahları en tehlikeli kılan nokta ise, elektromanyetik ya da fiziksel bir etki olmaksızın siber uzaya entegre edilmiş sistemleri bozmak veya tahrip etmek gibi yıkıcı bir gücünün bulunmasıdır (Keleştemur, 2015:221). Bu sebepten siber silahların istihbarata sağladığı kolaylıkların yanında risk ve tehdit oluşturucu yönlerinin bulunduğu da göz ardı edilmemelidir. Risk ve tehditleri minimize etmek adına da devletlerce olasılık dâhilinde olan her bir kötü senaryolar göz önünde bulundurulmalı ve üretilmiş olan tüm siber silahlara karşı önleyici tedbirlerin alınması ihmal edilmemelidir.

4.1.3.1. Malware (Kötücül Yazılımlar)

Kötücül yazılımlar en basit haliyle, sistem üzerinde kullanıcı bilgisi dışında istenmeyen değişiklikleri yapan, son derece dinamik yapılı ve zaman zaman saldırı biçimi olarak da kullanılabilen yazılımlardır (Samet ve Aslan, 2018:225). Temel çalışma mantıkları, var olan sistemlerin ve programların açıklarından ve zafiyetlerinden yararlanma kurgusu üzerine kurulmuştur. Taşınabilir veri depolama ortamları, internet dosyaları, oyun, uygulama ve program uzantıları içerisine gömülebilme özellikleri sayesinde, hedef sistemlere hızlı ve kolayca yayılabilme potansiyeline erişmişlerdir. Genel olarak da sistemin içerisindeki zararsız gözüken dosyaların içerisine gizlendiklerinden sisteme yerleştikleri veya bulaştıkları andan itibaren fark edilmeleri oldukça zor olmaktadır. Bu yönleriyle de fark edilmeden bulaştığı sistemlere zarar veren veya sabotaj etme tehdidi oluşturan önemli birer silah olma özelliği taşımışlarıdır.

Siber uzayda önemli birer silah olma özelliği taşıyan kötücül yazılımların bir diğer önemli özelliği de sistemlere yerleştikleri veya bulaştıkları andan itibaren, dışarıdan erişim olanağı sağlamalarıdır. Bir sisteme dışarıdan erişim sağlandığı andan itibaren de kullanıcısının bilgisi dışında müdahale edilerek o sistemin işlevini bozmak veya içerisindeki kritik bilgileri toplamak mümkün olabilmektedir. Dolayısıyla tüm bu özellikler, sistemler üzerinden uzunca bir süre fark edilmeden istihbarat elde edilebilmesinde veya casusluk faaliyetlerinin eş zamanlı olarak yürütülebilmesinde kötücül yazılımları önemli birer araca dönüştürmektedir. Ancak kötücül yazılımların istihbarat ve casusluk acısından önemli bir araç olduğunu söylerken çok farklı türleri ve bu türlerin de kendine has yapısal özelliklerinin olduğu bilinmelidir. Çünkü her kötücül yazılım, istihbarat ve casusluk açısından kullanılabilecek bir yapıya sahip değildir. Hatta birçoğunun sadece sistemi yok etme veya sabotaj etme gibi işleve sahip olduğu görülmektedir. Ayrıca bilgisayar, mobil ve internet teknolojilerine bağlı olarak sürekli gelişmekte ve yeni türlerinin ortaya çıkarıldığı da bilinmektedir. Bu nedenle istihbarat elde etme

anlamında doğru yer, doğru zaman ve doğru sistem üzerinde en uygun kötücül yazılımın kullanılması, istenen sonucu alma açısından kritik bir seçimdir.

Tüm bu düşüncelerden hareketle, en uygun kötücül yazılımın istihbarat elde etme açısından seçilebilmesi büyük önem taşımaktadır. Seçiminin doğru yapılabilmesi açısından da günümüz kötücül yazılım türlerinin teknik anlamdaki özelliklerinin iyi bilinmesi gerekmektedir. Bu sebepten günümüzdeki en önemli kötücül yazılım türleri, teknik ve yapısal olarak kısaca açıklanmaya çalışılmıştır.

4.1.3.1.1. Viruses (Virüsler)

İçerisinde kötü amaçlı kod parçacığı barındıran, çoğalmaları için başka programlara ihtiyaç duyan ve adeta biyolojik virüs mantığıyla hareket eden programlardır (Samet ve Aslan, 2018:228). En önemli özelliklerini, bulaşmış oldukları sistemlerin içerisindeki programlara hızla enjekte olarak bu programları da birer virüs haline dönüştürmeleri oluşturur (Oruç, 2019:46). Sistemlere girdikleri andan itibaren, sistem dosyalarında değişiklikler yaparak ihtiyaca göre sistemlerin kullanılamaz bir hale getirilmesine, verilerin değiştirilmesine veya kopyalanarak ya da taşınarak çalınmasına imkân verirler (Keleştemur 2015:222). Üreticisine ya da kullanıcısına vermiş oldukları bu imkânlar sayesinde de istihbarat elde etme açısından kullanılabilirler (Topal, 2004:15). Siber istihbaratta sıklıkla kullanılan bir silah olma ihtimalleri de bu anlamda şaşırtıcı değildir.

4.1.3.1.2. Worms (Solucanlar/Kurtçullar)

Virüslerin aksine girmiş oldukları sistemlerde çoğalmak için başka programlara ihtiyaç duymayan, kendi kendilerine hızla yayılabilen ve sistem üzerindeki ağları kullanarak bir sistemden diğer bir sisteme kolayca bulaşabilen programlardır (Samet ve Aslan, 2018:229). Çalışma mantıkları, öncelikle bulaşmış oldukları sistemlerde kendi kopyalarını oluşturma, devamında ise iletişim kurulan tüm savunmasız sistemlere süratle yayılma üzerine kuruludur. Kendi kendilerine çoğalabildikleri ve saniyeler içerisinde milyonlarca sisteme ulaşabildikleri için de kurtçul veya solucan olarak adlandırılmışlardır (Güntay, 2014:5).

Solucanlar, genelde sistemlerde arka kapılar[7] ya da tüneller açarak bu sistemleri dışardan izinsiz girişlere karşı savunmasız bırakmaktadır (Oruç, 2019:47). Bir sisteme dışardan girilebildiği andan itibaren de o sistemdeki her türlü veriye ulaşılması, sisteme yüklü uygulama

[7] Sistemlerin normal güvenliğini es geçerek dışarıdan yetkisiz erişim sağlayabilmek ve yine sistemleri dışarıdan yetkisiz işlemlere açık hale getirebilmek için gizlice yerleştirilmiş yazılımlardır.

ve programların uzaktan çalıştırılması mümkün olmaktadır. Bu sonuçta solucanları siber istihbarat açısından son derece değerli kılmaktadır.

4.1.3.1.3. Trojan (Truva Atları)

Normal bir programmış gibi gözüken, gerçekte ise kötü amaçlı kodlar barındıran, çalıştırılır çalıştırılmaz sistemleri etkileyen programlardır (Samet ve Aslan, 2018:229-230). Her türlü yazılım, uygulama, oyun, video vb. dosya ve uzantı içeriklerine gizlenebildiklerinden sistemlere girmeleri kolay olmaktadır. Çalışma mantıkları, tarihte Yunanlılar tarafından Truva'ya, tahtadan inşa edilerek bırakılan ve zararsız gibi gözükerek şehrin düşmesine sebep olan Truva Atı'na benzemektedir (Keleştemur, 2015:223). Bu benzerlik münasebetiyle de truva atları ya da trojan olarak isimlendirilmişlerdir.

Truva atlarının en önemli özelliği, virüs veya solucanlar gibi kendini kopyalama ya da hızla yayılma özelliğine sahip olmadan, yararlı bir yazılımmış gibi veya önemli bir fonksiyonu varmış gibi gözükerek sistem içerisindeki gizli ve güvenlik mekanizmalarını aşabilecek bir potansiyele sahip olmalarıdır (Öğün ve Kaya, 2013:10). Bu nedenle ilk önce, sanki adeta bir oyun, animasyon gösterisi veya eğlenceli bir uygulamaymış gibi gösterilerek sistemlere kolayca yerleştirilmektedirler. Sisteme yerleştirildikleri andan itibaren de sistem üzerinde arka kapılar açarak yazılımcısına, sisteme uzaktan erişilebilme ya da sistemde depolanan kritik bilgileri transfer edebilme imkânı sağlarlar.

Truva atlarının yazılımcısına veya kullanıcısına sağladığı tüm bu imkânlar için yerleştirilmiş oldukları sistemlerde bir kez çalıştırılmaları yeterlidir. Bir kez çalıştırıldıkları andan itibaren sistem üzerinde yerini alarak sistemin çalıştırıldığı ya da ağa bağlı olduğu tüm süreler boyunca yazılımcısı veya kullanıcısıyla iletişim kurarak sistemin dışarıdan fark edilmeden kolayca kontrol edilmesine sebep olurlar. Bu sonuçlarda truva atlarını, tıpkı virüsler ve solucanlarda olduğu gibi siber istihbarat açısından önemli bir noktaya getirir.

4.1.3.1.4. Backdoors/Trapdors (Arka Kapılar/Tuzak Kapılar)

Sadece yazılımcısı veya kullanıcısı tarafından bilinen, hedef sistemlerde normal kimlik kontrol mekanizmalarını kullanmadan dışarıdan gizli bir yöntemle erişim sağlanabilmesi için kanallar veya giriş noktaları açan program ya da yazılımlara verilen isimdir (Güntay, 2018:5). Çalışma mantıkları, yazılımcısına veya kullanıcısına hedef sistemler üzerinde fark edilmeden dışardan giriş sağlayabilmeleri için tüneller açma üzerine kuruludur (Samet ve Aslan, 2018:230). Bu nedenle, yerleştirilmiş oldukları hedef sistemlerdeki geleneksel güvenlik

mekanizmalarını atlatarak sistemleri kullanıcılarının bilgileri dışında uzaktan erişime açık hale getirirler (Topal, 2004:17).

Sadece oluşturucusu tarafından bilinebilen arka kapılar, genel olarak truva atları, solucanlar ve virüsler aracılığıyla hedef sistemlere yerleştirilebilmektedir. Bunun yanında, sistemlerin içerisindeki her türlü yazılımlar, uygulamalar ve programların içerisinde de arka kapılar bulunabilmektedir. Dolayısıyla siber istihbaratın elde edilebilmesi açısından sistemlerde bulunan arka kapılardan yararlanılması veya sistemlere arka kapılar açılabilmesi çok kıymetli bir gerekliliktir. Bu gereklilik yerine getirildiği takdirde, hedef sistemden ihtiyaç duyulan her türlü istihbari bilgi ve belge eş zamanlı olarak elde edilebilecektir.

4.1.3.1.5. Rootkits (Korsan Amaçlı Kullanılan Yazılımlar)

Hedef sistemlere yönetici düzeyinde erişim hakkı vererek kendi dosya ve sistem bilgileri ile sistem üzerinde yapılan işlemleri, hedef işletim sisteminden gizlemek suretiyle varlığını gizlice sürdüren programlardır (Samet ve Aslan, 2018:230). Genel olarak işletim sistemlerinin çekirdek düzeyinde çalıştıklarından tespit edilmeleri ve sistemlerden kaldırılmaları oldukça zor olmaktadır. Çalışma mantıkları, bulunduğu sistemlerde varlığını gizleyerek kullanıcılarına sistemlerde yönetici düzeyinde işlem yapabilme, yönetim uygulamalarına ve sistem bilgilerine erişebilme yetisi verme üzerinedir (Keleştemur, 2015:226). Bu özellikleri sayesinde, hedef sistemlere yukarıda belirtilmiş olan virüs, solucan truva atları ve arka kapı yazılımları gibi diğer kötücül yazılımlar kolayca sızdırılabilmekte ya da sızdırılmış olan diğer zararlı yazılımların fark edilmeden rahatlıkla çalıştırılabilmesi sağlanmaktadır.

4.1.3.1.6. Bots (Robotlar)

Bir dizi robotlardan oluşup zafiyetli bilgisayar ve sistemlere veriler göndererek o sistemleri sonradan saldırı aracına dönüştüren programlardır (Samet ve Aslan, 2018:231). Bu programlar aracılığıyla, yazılan kodlar doğrultusunda otomatik işlemler yapılarak bir takım yönetimsel araçlar ele geçirilebilmektedir (Keleştemur, 2018:92). Özellikle zombi bilgisayarlar[8] ya da bir diğer adıyla köle bilgisayarlar, botların bu kullanım alanlarına en uygun örneklerdendir. Çünkü bu sitemler, botlar aracılığıyla kullanıcısının bilgisi ve iradesi dışında uzaktan kontrol edilerek birer saldırı makinesine dönüştürülebilmektedir. Bu nedenle de çalışma mantıklarının saldırgan, komuta ve kontrol mekanizması ile zombi bilgisayarlar üzerine kurulmuş olduğu söylenebilmektedir. Bu mantıkta saldırganlar, komuta ve kontrol

[8] Kullanıcısının haberi olmadan botlar aracılığıyla uzaktan kontrol edilerek saldırganın tüm amaçlarını yerine getirmek için kullanılan bilgisayarlardır. Bu bilgisayarlar gerçek kullanıcısının bilgisi ve rızası dışında komuta ve kontrol edilerek çok ciddi suçların işlenmesinde de kullanılabilmektedir.

mekanizması üzerinden savunmasız sistemleri bularak bu sistemleri birer zombi bilgisayara dönüştürmekte ve bu sayede de başka sistemlere saldırı gerçekleştirebilmektedir. Saldırının neticesinde deşifre edilmeden hedef sistemler çalışmaz hale getirilebilmekte ve köle olarak kullanılan sistemlerden istihbari açıdan önemli olabilecek bilgiler çalınabilmektedir.

4.1.3.2. Spyware (Casus Yazılımlar)

Bulunduğu sistemlerdeki bilgi ve faaliyetleri çeşitli amaçlarla izleyerek takip eden, gizli bilgileri toplayan ve nihayetinde tüm bunları yazılımcısına ya da kullanıcısına ileten yazılımlardır (Altınok ve Katman, 2009:73). Bu yazılımlar, bulundukları sistemlerde truva atları, rootkitler ve arka kapılar gibi gizlice çalışarak sistem üzerindeki her türlü veriyi dışarıda belirlenmiş başka sunuculara aktarmaktadırlar (Canbek ve Sağıroğlu, 2006:182-183). Ayrıca yazılımcıları ya da kullanıcıları tarafından kendilerine tanımlanmış olan her türlü görevleri de yerine getirebilmektedirler (Keleştemur, 2015:226). Genel anlamda da siber casusluk faaliyetlerinde kullanıldıklarından casus yazılımlar olarak isimlendirilmişlerdir (Keleştemur, 2018:94).

Casus yazılımlara örnek olarak tuş kaydediciler (keyloggers), ses kaydediciler, görüntü kaydediciler ve konum takip edici yazılımlar gibi istihbarat maksatlı birçok uygulamaları örnek olarak göstermek mümkündür. Çünkü bu yazılımlar aracılığıyla hedef sistemlerden kameraları ve mikrofonları vasıtasıyla sürekli olarak görüntü ve ses alınarak bu görüntüler başka tarafa aktarılabilmektedir. Yine konum uygulamaları vasıtasıyla bulunulan yerin anlık bilgisi, tuş kaydedicileri aracılığıyla da klavyede basılmış olan tüm harflerin bilgisine ulaşılabilmektedir. Bu sayede siber uzayda casusluk faaliyetlerini eş zamanlı olarak gerçekleştirebilmek mümkün olabilmektedir.

4.1.3.3. Yönlendirilmiş (Yoğunlaştırılmış) Enerji Silahları

İngilizce "directed energy weapons" olarak adlandırılan yönlendirilmiş enerji silahları, şekillendirilebilen ve yönlendirilebilen yoğunlaştırılmış elektro manyetik enerji dalgalarının veya atom parçacıklarının ışın yaymasıyla çalışarak hedefe zarar veren silahları tanımlamaktadır (savunma-sanayi.com, 2020). Şekillendirilebilen ve yönlendirilebilen yoğunlaştırılmış elektromanyetik enerji dalgalarının veya atom altı parçacıklarının ışın yayması prensibiyle çalışan bu silahlar, genel itibariyle de günümüzde lazer, mikrodalga, parçacık ışınlı, RF (radyo ve frekans) enerji ve yüksek güçlü sonik silahlar olmak üzere sınıflandırılmıştır (Thinktech, 2019:5-9). Bu sınıflandırmada lazer silahlar, uyarılmış ışımanın yayılımı ile ışığın güçlendirilerek yüksek enerji seviyesine ulaştırılmış olduğu silahları temsil etmektedir

(Thinktech, 2019:5). Bu silahlar, hedefi yoğun ısı oluşturarak yakma veya tahrip etme özellikleri sayesinde daha çok termal ve darbe niteliğindeki saldırılarda kullanılmaktadır. Sahip olduğu yoğun ısı enerjisiyle de uçak, füze, uydu gibi elektronik sistemler kolayca delinerek büyük hasarlar oluşturulabilmektedir. Mikrodalga silahlar ise radyo frekansı veya elektromanyetik spektrumun mikrodalga kısmını, bir hedefe enerji göndererek yıkıcı veya bozucu etki yaratmak için kullanılan silahları ifade etmektedir (Wang, 2018). Bu silahların lazer silahlarına göre dalga boyu 10 kat daha uzun olduğundan mesafe uzadıkça daha çok dağılma gösterdikleri görülmektedir (Defence Point, 2019). Ancak buna karşılık olarak da daha geniş bir alanda, çok sayıdaki hedeflere saldırı gerçekleştirmek için kullanılabilecekleri bilinmelidir (Thinktech, 2019:7). Parçacık ışınlı silahlar, elektrik yükü bulunmayan atom parçacıkları ve nötronları ışık hızında yönlendirerek yüksek güçte ışın oluşturan silahlara denilmektedir (savunma-sanayi.com, 2020). Çalışma prensiplerinde hedefin atomlarıyla buluşan ışınlar, bulunduğu yeri ısıtarak patlatmaktadır (Thinktech, 2019:8). Bu sayede de ışın, hedef platformun içine kadar sızarak elektronik sistemlere zarar verebilmektedir. Ayrıca parçacık ışınlı silahlar, lazer silahlar gibi parlak yüzeylerde yansıma yapmadıklarından hedef yüzeylerde sapma olasılıkları bulunmamakta ve atmosfer olaylarından çok fazla etkilenmemektedir (Mizokami, 2019). RF (radyo frekans) enerji silahları da yönlendirilmiş elektromanyetik alanların ışıması yöntemiyle enerjiyi hedefin hassas elektroniğine gönderen silahlar olarak karşımıza çıkmaktadır (Keleştemur, 2015:233). Bu silahlar, çok sayıdaki hedefi eş zamanlı olarak etkisi altına alabildikleri gibi belirli bir kayıpla da olsa toprak altı, duvarların arkası, katların arası, engellerin ardı vb. kapalı alanlara da nüfuz edebilmektedir (Karakuş, t.y.:11). Ayrıca elektromanyetik dalgalarının enerji hatları, anten, kablo gibi olası iletken yüzeyler ile dalga boyuna bağlı olarak etkileşime girdiklerinden, hedeflerde istem dışı açıklıklar, yarıklar, hasarlar vb. sonuçlar oluşturarak metal olmayan bağlantı yerlerinden cihazlara ve onları oluşturan birimlerine etki edebilmektedirler. Bu sayede RF enerji silahları aracılığıyla hedef bilgi sistemlerinde bulunan verileri silebilme, sistemlere hatalı bilgi yükleyebilme ve hatta sistemlere zararlı kodlar yerleştirerek istenilen amaçları gerçekleştirebilme fırsatı doğabilmektedir (Keleştemur, 2015:233). Yüksek güçlü sonik silahlar ise, hedeflerine yüksek enerjili ses yönlendiren silahları gruplandırmak için kullanılmaktadır (Thinktech, 2019:8). Bu silahlarda, yüksek enerjideki ses dalgaları ve frekanslar uzun mesafeler kat ederek çoğu binalardan ve vasıtalardan etkilenmeden geçebilmektedir (Altmann, 2001). Ancak bu silahların genel olarak canlıları hedef aldığı da bir başka gerçekliktir. Çünkü frekans ve gücüne bağlı olarak yüksek güçlü sonik silahların canlılar üzerinde korku, endişe ve depresyon gibi psikolojik ve bulantı, kusma, organ hasarı, yanık ve ölüm gibi biyolojik etkileri bulunduğu

gözlemlenmektedir (savunma-sanayi.com, 2020). Dolayısıyla konumuz açısından faydalı görünmemiş olsa da yönlendirilmiş enerji silahlarının bir türü olduğundan açıklanmasının gerekli olduğu düşünülmüştür.

Yapılan kısa açıklamalardan yönlendirilmiş enerji silahlarının diğer silahlara nazaran birçok üstün özelliğinin bulunduğu açıkça görülmektedir. Öyle ki hedefe ışık hızında ulaşma, duvardan dahi geçebilen uzun menzilli enerjiye sahip olma, enerji kaynağı kesilmediği sürece sınırsız ve sürekli atış yapma ve de çok sayıdaki hareketli hedeflere dahi nokta atışı yapma bu üstün özelliklerinin ilk akla gelenleridir. Tüm bu özellikler, yönlendirilmiş enerji silahlarının farklı alanda kullanılmasına neden olmaktadır. Günümüzde bu alanların roketler, insansız hava araçları, balistik füzeler ve diğer silah sistemlerinin hareket halinde imha edilmesi, elektronik taarruz faaliyetlerinin engellenmesi, düşman personelleri ile teröristlerin etkisiz hale getirilmesi ve devletlerin silah ve teçhizatlarının bulunduğu kara, deniz, hava, uzay ve siber uzaydaki üstlerinin korunması olduğu bilinmektedir (savunma-sanayi.com, 2020). Dolayısıyla, bu sonuçlardan yola çıkarak yönlendirilmiş enerji silahlarının teröristlerce uzaktan başlatılmış bir saldırının hedefine ulaşmadan önce, öğrenilmesi ve direk olarak hareket halindeyken imha edilmesi açısından kullanılabileceği söylenebilir. Ayrıca siber uzayda bulunan uydular, insansız hava araçları, iletişim ağları, bilgisayar sistemleri gibi donanımlara ait elektronik devrelere de hasar verme kapasitesine sahip olduğu göz ardı edilmemelidir (Keleştemur, 2015:232). Çünkü bu silahlar sayesinde düşmanın siber harekâtını kısıtlamak amaçlı, hassas elektronik ve elektro optik sistemlerine zarar verici saldırılar yapılabilecek, sistemlerine zararlı kodlar yerleştirilebilecek, hedef bilgi sistemlerde bulunan veriler yok edilebilecek veya silip değiştirilebilecektir. Bu sayede de devletler için hem istihbarata karşı koyma hem de zor dahi olsa istihbarat elde edebilme imkânı ortaya çıkacaktır.

4.2. Siber İstihbaratın Yöntemleri

Siber istihbaratın yöntemleri, siber savaşçıların imkân ve kabiliyetleri ile kullanım amaçlarına göre farklılık göstermekle birlikte, siber uzaya bağlı teknolojinin gelişmesiyle de ilerlemektedir. İlerleyen teknoloji, yeni siber istihbarat yöntemlerinin keşfedilmesine ve bu yöntemlere yönelik siber savunma tekniklerinin geliştirilmesine sebebiyet vermektedir (Bayraktar, 2010:13). Bu nedenle geleneksel istihbarat yöntemlerini sistematik bir şekilde sınıflandırabilirken; siber uzayın farklılığından ve gereksinimlerinden ötürü siber istihbarat yöntemlerini sınıflandırabilmek göreceli olabilmektedir. Ancak konumuz açısından, siber istihbarat yöntemlerinin teröristle mücadele noktasındaki olağan ve olası faaliyetleri ekseninde tasniflenmesinin daha uygun ve anlaşılabilir olacağı da göz ardı edilmemelidir. Bu kapsamda

siber istihbaratın yöntemleri; siber bal tuzağı, osint, socmint, siber saldırı, yönlendirilmiş (yoğunlaştırılmış) enerji silahları ve İHA (insansız hava araçları) kullanımı olmak üzere beş ana başlık altında incelenmek istenmiştir.

4.2.1. Siber Bal Tuzağı

İstihbarat literatüründe İngilizce "honey trap" anlamına gelen bal tuzağı, eskiden beri süregelen erkek veya kadın ajanların seksapelini kullanarak bilgi toplaması hadisesidir (Molatik, 2020). Hemen hemen bütün istihbarat örgütlerince kullanılan bu yöntem, cinselliğin kullanılarak casusluk faaliyetlerinde bulunulması, ihtiyaç duyulan bilgi ve belgelerin hedefteki kişiyi baştan çıkararak toplanması mantığı üzerine kurulmuştur. Kadınların erkekleri daha kolay etki altına alabilmesi münasebetiyle de çoğunlukla kadın kullanılarak istihbarat elde etmek maksatlı kullanılan bir yöntem olmuştur (Keleştemur, 2015:93). Bu nedenle de istihbarat dilinde, özellikle kadınların çekiciliğinin kullanılarak hedefin ava dönüştürüldüğü taktik olarak nitelendirilmiştir (Hürriyet, 2017).

Bu taktikte, öncelikli olarak hedef gözlenmekte ve hedefin karşı cins olarak hangi tarz fiziksel ve ruhsal özelliklere sahip kişilere ilgi duyduğu saptanmaktadır. Devamında ise hedefin ilgi duyduğu karşı cinse uygun bir ajan seçilerek hedefi etki altına alma çalışmalarına başlanmaktadır. Bu işlem, başarıyla sonuçlandığı andan itibaren de hedef gerek cinsel gerekse duygusal anlamda etki altına alınarak tuzağa düşürülmektedir. Böylelikle, adeta av ile avcı arasındaki kanca takma operasyonu başarıyla tamamlanarak istenilen bilgilere hedef üzerinden ulaşılmaktadır (Keleştemur, 215:94-96).

Klasik anlamdaki bal tuzağı operasyonları, temel olarak yukarıda belirtilen şekilde ilerlemektedir. Dolayısıyla hedefteki kişileri izlemek, karşı cinse olan zafiyetlerini ve hangi cinsel öğelere eğilim gösterdiği gibi pek çok hususu tespit etmek gerekmektedir. Ancak bu tespitlerin yapılabilmesi göründüğü kadar kolay olmamaktadır. Başarılı olabilmek için bir dizi istihbarat faaliyetlerinde bulunulması gerekmektedir. Oldukça zor ve geniş bir zaman gerektiren bu faaliyetler, derin istihbarat operasyonlarından oluşmaktadır. Bu durumda ortaya gerek maddi gerekse deşifre olma gibi riskleri de içerisinde barındıran uzun bir süreci çıkarmaktadır.

Tam da bu noktada, siber uzayın insan yaşamına entegrasyonunu göz önüne aldığımızda, zor ve uzun zaman gerektiren tüm bu istihbarat operasyonlarının tersi bir hal alacağı açıkça görülmektedir. Başta mobil teknolojiler, internet, sosyal medya platformları, bulut ortamlar ve veri tabanı sistemleri olmak üzere insanların siber uzaya olan bağımlılığı bu

durumun en büyük göstergesidir. Bu bağımlılık sayesinde insanların kişisel verilerinden günlük aktivitelerine, hobi ve etki alanlarından kişisel zevk ve tercihlerine kadar, kişiyi özel kılan birçok bilgisi o veya bu sebepten siber uzayda bulunmaktadır. Siber uzayda bulunan tüm bu verilere ise müteakip başlıklarda belirtili diğer siber istihbarat yöntemleriyle kısa bir süre içerisinde kolayca ulaşılabilmektedir. Bilgilere ulaşıldığı andan itibaren ise hedef hakkında gerekli analiz yapılarak doğru harekât planı belirlenebilmektedir. Böylelikle bal tuzağının uygulanması için gerekli olan tüm bilgi, kısa bir süre içerisinde kolayca elde edilerek tüm şartlar ve zemin hazırlanabilecektir.

Siber uzayın bal tuzağı için gerekli olan bilgileri elde etmedeki kolaylığının yanında, diğer bir önemli özelliği daha bulunmaktadır. Bu özellik, siber uzay üzerinden bal tuzağı yönteminin doğrudan uygulanabilmesi imkânı olarak kendisini birçok örnekle göstermektedir. Sıklıkla duyduğumuz internetten kadın sandığı kişiye çıplak fotoğraflarını göndererek şantaja uğrama, en basit örneklerdendir. Bu noktada, siber uzayın bal tuzağı için gerekli olan tüm bilginin elde edilmesiyle eş zamanlı olarak bal tuzağı yönteminin doğrudan uygulanmasına fırsat yarattığı açıktır. Dolayısıyla, siber uzay üzerinden doğrudan uygulanan bal tuzağı yöntemi, siber bal tuzağı olarak nitelendirilmeli ve ayrıca bir yöntem olarak vurgulamalıdır.

Siber bal tuzağı yönteminin daha iyi anlaşılabilmesi açısından, konuya yönelik birkaç olası örneğe değinmekte yarar vardır. İlk olarak terör örgütüyle doğrudan ilişkisi bulunmayan basit bir terör örgütü sempatizanı ele alındığında, görüştüğü kişilerin terör örgütüyle veya örgüt üyeleriyle doğrudan iletişim halinde olabileceği varsayımı açıkça tahmin edilebilmektedir. Bu varsayımdan hareketle, öncelikli olarak sempatizanın (sosyal medya, arkadaşlık ve form siteleri, internet, mobil uygulamalar, sanal oyunlar vb.) siber uzayda yapmış olduğu aktiviteleri, vermiş olduğu bilgileri, hobileri ve ilgi duyduğu içerikleri inceleyerek ruhsal, fiziksel ve cinsel eğilimlerini tespit etmek gerekmektedir. Devamında tüm bu eğilimlerine yönelik onu rahatlatabilecek, içinde bulunduğu ruhsal ve cinsel boşluğu doldurarak etkisi altına alabilecek karşı cinse ait profil saptanmalıdır. Profil saptandıktan sonra hedefin siber uzayda en çok ilgi duyduğu alan üzerinden yemlenme çalışmalarına başlanmalıdır. Bu alanlar sosyal medya sayfaları, arkadaşlık siteleri, form siteleri vb. gibi akla gelebilecek her türlü siber uzay içerisinde yer alan ortamlar olabileceği gibi online oynanan oyunlarda olabilmektedir. Dolayısıyla hedefe kanca takabilmek için doğru yer ve zamanda harekete geçilerek hedefin yemlenmesi önemlidir. Ayrıca hedef yemlenirken karşı tarafa kolay gözükmeyip, hedefin yaratılan profili tavladığı izlenimini vermekte ihmal edilmemelidir. Aksi takdirde hedefte, şüphe uyandırılabileceği gibi kolay elde edinilmiş izlenimiyle heyecanda uyandırılamamış olacaktır. Tüm bu hususlara

dikkat ederek hedef başarıyla yemlendiği andan itibaren, kanca takma operasyonu tamamlanacaktır. Son olarak da hedefle duygusal, cinsel vb. her türlü etkileşim halinde olunarak istenilen bilgilere ulaşmaya çalışılmalıdır. Bilgilere ulaşmaya çalışırken ısrarcı olmamak ve hedefi sıkmamak en doğru hareket tarzıdır. Çünkü hedeften sürekli bir şey istemek ve ısrarcı olmak ters etki yapabileceği gibi, şüphede çekerek başarısızlığa sebebiyet verebilecektir. Bu sebepten hedeften sürekli bir şey istemek ve ısrarcı olmak yerine onun her koşulda yanında olunduğunu hissettirerek iletişim kurmaya yönlendirmek başarının sürdürülebilir olması noktasında daha kıymetli adımlar olacaktır. En nihayetinde son derece başarıyla yönetilerek sürdürülen siber bal tuzağı yöntemi, hedefin görüşmekte olduğu kişilerden terör örgütüyle veya örgüt üyeleriyle doğrudan iletişim halinde olabilecek kişileri, tespit edebilme noktasında gerekli olan tüm istihbaratın elde edilmesiyle sonuçlanacaktır. Bu sonuçla da yeni hedefler belirlenerek onlar üzerinden istihbarat elde etme amaçlı uygun yöntemler seçilecek ve teröristle mücadele kapsamında daha derin istihbarat faaliyetleri yürütülebilecektir.

Siber bal tuzağı yöntemine bir başka olası örnek olması açısından düşük profilli bir terör örgütü üyesi ele alındığında, yine benzer yöntemleri izleyerek istihbarat elde edilebileceğini söylemek gerekmektedir. Ancak bu noktada konuya biraz daha teknik boyut katarak farklı vasıtalar üzerinden örnek vermek istenilmiştir. Çünkü siber bal tuzağı sayesinde terör örgütleri veya terör örgütü üyelerince kullanılan siber uzay teknolojilerine ait sistemlere erişmek dahi mümkün olabilmektedir. Bu erişimi sağlayabilmek içinde hedefe gönderilen mesaj, resim, video, ses kaydı vb. verilerin içerisine virüs, solucan, truva atı, casusu yazılım gibi siber silahların gizlenerek hedef sisteme yerleştirilmesi yeterlidir. Siber silahların hedef sisteme yerleştirildiği andan itibaren de sistemde bulunan her türlü veriye ulaşılarak arka planda eş zamanlı istihbarat faaliyetleri yürütmek mümkün olabilmektedir. Bu sonuçta teröristle mücadele noktasında doğru bilgiye ulaşılarak yeni hedeflerin seçilmesinde isabetli kararlar verilmesini sağlayabilecektir. Böylelikle az bir maliyetle devamlılık arz eden istihbaratın sürdürülebilme olasılığı artacaktır.

4.2.2. OSINT (Açık Kaynak İstihbaratı)

Açık kaynak bilgisi, kaynağı tarafından gizlenmeyen ya da gizlenmesi mümkün olmayan kamuya açık bilgileri ifade etmektedir (Tiryaki ve Özdal, 2020:10). Son derece geniş bir alan içerisinde yer alan bu bilgilerin çoğunluğu, günümüzde *(gazete, dergi, televizyon, radyo vb. kitle iletişim araçları gibi)* medya verileri, *(bütçeler, demografik istatistikler, projeler, anket çalışmaları, coğrafi yapı, gelenek ve göreneklerle ilgili)* kamuoyu verileri, *(sempozyum,*

konferans, kongre, panel vb.) toplantı verileri, *(web siteleri, bloglar, sosyal medya uygulamaları, oyun siteleri, araştırma siteleri, haber siteleri, wikiler, web yayınları vb.)* internet verileri, *(akademik bilgiler, tezler, makaleler, raporlar, araştırmalar vb.)* akademik ve mesleki veriler, *(ticari işletme bilgileri, patentler, çalışma belgeleri vb.)* ticari veriler, arşiv bilgileri, çalışma kağıtları, biyografiler ve gezi raporları içerisinde yer almaktadır (Best and Cumming, 2007:6). Bu nedenle de herkes tarafından kolayca ulaşmakta ve ulaşılması sırasında hissedilebilir bir karşı koyma söz konusu olmamaktadır (Tekek, 2016).

Herkese açık olan ve kolayca erişim sağlanabilen açık kaynak bilgilerinin birçok üstün yönü bulunmaktadır (Tiryaki ve Özdal, 2020:8). Bilgi anlamında oldukça zengin, ulaşılabilirlik açısından son derece hızlı ve maliyet olarak ucuz olma özellikleri, üstün yönlerini perçinlemektedir. Bu sebepten açık kaynak bilgisinin, başlı başına bir istihbarat kaynağı olabileceği gibi farklı yöntemlerle elde edilmiş istihbari bilgileri teyit noktasında kullanılabileceği söylenebilmektedir (Keleştemur, 2015:55). Ancak açık kaynak bilgilerinin istihbarat kaynağı olabileceğini belirtirken istihbarat haline getirilmeye muhtaç bilgiler olduğu da belirtilmelidir. Çünkü bir bilginin istihbarata dönüştürülebilmesi için bilgilerden elde edilen verilerin işlenip anlamlandırılması gerekmektedir. Bilgilerin işlenip anlamlandırılabilmesi içinde alanında uzman kişilerin açık kaynak verilerini ele alıp incelemesi ve analizini yapması önemlidir (Ateş, 2013:17). Böylelikle açık kaynaklardan elde edilen bilgilerin istihbarata dönüştürülmesi noktasında, arzu edilen başarıya ulaşılabilecektir.

Tüm bu anlatılanlardan açık kaynak istihbaratını; kamunun kullanımına açık olan her türlü bilgi, belge, haber ve verilerden belirli bir amacı gerçekleştirmek için istihbarattın toplandığı hadise olduğunu nitelendirmek mümkündür (Benes, 2013:22-37). Amaca yönelik istihbaratı toplarken de ihtiyaç duyulan araştırmaların tv, radyo, gazete, dergiler, periyodik yayınlar, broşürler, bildiriler, kataloglar, medya ve internet üzerinden yapılabileceği açıktır (Özdağ, 2020:296). Bu araştırmaların yapılması sırasında ise iyi bir stratejinin izlenerek araştırma için yeterli bilgiye haiz personellerin bulundurulması önemlidir. Böylelikle gerekli olan tüm bilgilerin toplanılarak verimli ve başarılı bir açık kaynak istihbaratının elde edilebilmesi olanaklı olmaktadır.

Açık kaynak istihbaratını tarihsel anlamda ele aldığımızda ise özellikle internetin yaygınlaşmaya başlamasına paralel olarak önemli bir konuma yükseldiği görülmektedir (Tirkayi ve Özdal, 2020:8). Hatta dahası, istihbaratın günümüzde internettin açık kaynakları üzerinden elde edildiği bir yönteme dönüştüğü dahi söylenebilmektedir (Özçoban, 2014:41).

Bunu söylerken de internetin açık kaynak bilgisi anlamındaki değerini vurgulamayı ihmal etmemek gerekmektedir. Zira internet, içerisine her gün yüklenen milyonlarca bilgiyle ve dahası diğer açık kaynaklarda bulunan verileri bir şekilde bünyesine katmasıyla, önemli bir bilgi yığınını haline gelmiştir. Ayrıca bilginin hızla yayımlanarak farklı kişilere anında ulaşma imkânı sağlamasıyla da istihbari değeri olan bilgiye ulaşılmasını kolaylaştırmıştır. En nihayetinde de doğruluk isabet ve devamlılık parametreleri ölçüsünde eş zamanlı olarak istihbaratın elde edilmeye çalışıldığı, önemli bir açık kaynak alanı olarak karşımıza çıkmıştır. Bu sonuçlar da internetin, açık kaynak istihbaratının elde edilmeye çalışıldığı ön önemli bilgi kaynağı olmasını sağlamıştır.

Konuyu örneklendirme noktasında birkaç tekniğe değinildiğinde, bugün internet ve sibernetiğe ilişkin uygulamaların etkin olarak kullanılmasıyla çok önemli bilgilere ulaşılabileceği görülmektedir. Örneği detaylandırmak açısından herhangi bir internet sitesinden terör örgütlerinin eğitim, tatbikat, eğlence, röportaj vb. görüntülerine ait resimler toplanabilmektedir. Toplanmış olan bu fotoğrafların, dikkatli ve titizlikle incelenerek görsellerde bulunan yapı, akarsu, kritik arazi arızaları vb. coğrafi şekilleri derlenip, önemli birer bulgu haline dönüştürülebilmektedir. Dahası terör örgütü mensuplarının kullandığı silah ve teçhizat türleri ile ruhsal ve bedensel güçleri anlamlandırılabilmektedir. Bu noktadan sonrada, gerekli analizler yapılarak Google Maps[9] gibi genel veya istihbarat servislerine ait özel uygulamalar üzerinden elde edilen bulgular eşleştirilerek teröristlere ait kamp, sığınak, barınak gibi yerler tespit edilebilmekte, orta ve uzun vadedeki hedefleri saptanabilmektedir. Yine bir başka örnek olması açısından internette yer alan teröristlere ait fotoğraf, ses kaydı, video vb. içeriklerin kimler tarafından izleniliyor olduğu tespit edilerek olumsuz yönde etkilenen kişilerin bilgisine ulaşabilmektedir. Böylece teröristle mücadelede, örgütlere insan kaynağı olabilecek potansiyel kişileri önceden durdurarak örgüt üyelerinin karamsarlığa kapılmasına neden olunabilecektir.

Sonuç olarak, günümüzde açık kaynak istihbaratı teröristle mücadele noktasında önemli bir konuma ulaşmıştır. Ayrıca teknik olarak belirsizlikleri azaltarak bilişsel zorlukların üstesinden gelme, alternatif yorumları inceleyerek istihbaratta doğruluk oranlarını artırma gibi birçok fayda sağlamıştır. Ancak bu noktada siber uzayda bulunan açık kaynak bilgilerinin sıkı çalışma ve iyi düşünülmüş esnek bir mekanizma ile toplanması, sıralanması ve değerlendirilmesi gerekmektedir. Aksi takdirde teröristle mücadele noktasında elde

[9] Google tarafından hizmete sunulmuş olan ücretsiz çevrimiçi haritalama servisidir.

edilebilecek her türlü fırsatlar kaçırılabilecek ya da daha kötüsü küresel tehdit boyutunda risk ve tehdit olgusuyla karşı karşıya kalınabilecektir.

4.2.3. SOCMINT (Sosyal Medya İstihbaratı)

SOCMINT kelimesi; Türkçede karşılığı ‘‘sosyal medya istihbaratı’’ anlamına gelen, İngilizce ‘‘social media intelligence’’ kelimelerinin kısaltılmasından türetilmiştir (BGA Security, 2019). Dolayısıyla kelime anlamından anlaşılacağı gibi istihbarat faaliyetlerinin sosyal medya platformları üzerinden gerçekleştirildiği bir yöntemi akıllara getirmiştir. Ancak sosyal medya istihbaratını, bu kadar basit tanımlamak konunun dahi iyi anlaşılması noktasında yeterli görülmemiştir. Bu nedenle de sosyal medya istihbaratının tüm boyutlarıyla değerlendirilerek teknik anlamdaki tanımlaması ortaya konmaya çalışılmıştır.

Önceki başlıklarda anlatılmaya çalışıldığı üzere sosyal medya, kullanıcı içeriğinin kişinin kendisi tarafından yayınlandığı veya paylaşıldığı her tür platformu tanımlamak için kullanılan genel bir isimdir (Doğan, 2016). Sosyal medya platformları ise, internet ve mobil servisler vasıtasıyla bireylerin ortak ilgi alanları, aktiviteleri, fikirleri gibi konularda birbiriyle bağlantı kurarak sosyalleşmelerini sağlamak maksadıyla oluşturdukları yazılımlardır (Doğan, 2016). Akla gelen en bilindik örnekleri Facebook, Instagram, Twitter, Tiktok ve Youtube olan bu yazılımlar kurumlar, topluluklar ve bireyler arasında etkileşimli bir iletişim imkânı sağlayarak kullanıcılarına kişisel ve kurumsal bazda bilgi, resim, müzik, video ve yazı paylaşabilme fırsatı sunmaktadır (Oruç, 2019:40). Ayrıca zaman ve mekân sınırlaması olmaksızın kişilere ilgi alanlarını, yaşam tarzlarını, kültürlerini, aktivitelerini, bilgilerini, fikir ve düşüncelerini paylaşabildikleri alanı da ortaya çıkarmaktadır (Tirkayi ve Özdal, 2020:13). Bu sonuçlarla da günümüzde iletişimde tek yönlü bilgi paylaşımından çift taraflı ve eş zamanlı bilgi paylaşımına ulaşılmasını sağlayan ve bu vesileyle iletişim yönünün çoğuldan çoğula doğru yürütülmesine aracılık eden yeni medya platformları olarak dünyadaki yerini almışlardır.

Yeni medya platformları olarak ortaya çıkan sosyal medya uygulamaları, istihbarat açısından incelendiğinde, birçok yenilik ve kolaylığı beraberinde getirdiği gözlemlenmektedir. Tüm bu yenilik ve kolaylıklar göz önüne getirildiğinde ise kişilerin doğum veya özel gün bilgilerinden eğitim, sağlık ve sosyal durum bilgilerinin neler olduğuna, kimlerle arkadaşlık ettiklerinden arkadaşları ile neler yaptıkları veya nasıl bir ilişki içerisinde bulunduklarına, neleri beğendiklerinden ilgi duydukları her türlü kişi, cisim, obje vb. şeylerin neler olduğuna, bulunmuş oldukları konumlardan kimlerle nerede ne yaptıklarına, kişisel duygu ve düşüncelerinden politik, dini veya ideolojik görüşlerine varıncaya kadar birçok önemli noktanın

zaman ve mekân sınırlamasına bağlı kalmaksızın tespit edilebilmesi örnek gösterilebilmektedir. Dolayısıyla sosyal medya platformları üzerinden kişilere, kurumlara ve topluluklara yönelik istihbarat odaklı yapılan çalışmaları, teknik anlamda ayrı bir boyutta değerlendirmek gerekmektedir. Yapılan değerlendirmelere binaen de sosyal medya istihbaratını; ‘‘açık veya kapalı her türlü sosyal medya hesapları veya bu hesapların paylaşımları üzerinden (gerek müdahaleci gerekse müdahaleci olmayan araçlar ve yöntemler kullanılarak) elde edilmiş olan verilerin, teknik araçlar kullanılarak istihbarata dönüştürüldüğü bir yöntem’’ olarak tanımlamak mümkün olabilmektedir (Privia Security, 2020).

Yapılan tanımlamayı örneklendirme noktasında birkaç olası örneğe değinildiğinde, sosyal medya verilerinin teröristle mücadele noktasında etkin bir yöntem olabileceği açıkça görülmektedir. İlk olarak bir teröriste ait sosyal medya hesabı ele alındığında, onun kimlerle neler yaptığını, kimlerle arkadaşlık kurarak nerelerde bulunduğunu, nelerden hoşlanıp nelerden hoşlanmadığını, nasıl bir ruh haline sahip olup psikolojik durumunun ne olduğunu, medeni veya ilişki durumunun ne olduğundan eğitim durumunun ne olduğuna varıncaya kadar birçok bilgiyi öğrenmek mümkün olabilmektedir. Öğrenilen bu bilgilerle de terör örgütü üyelerinin gerek siber bal tuzağı yöntemi gerekse sosyal mühendislik yöntemiyle aldatılması ve devamında doğrudan ya da siber silahlar aracılığıyla takibinin yapılarak izlenmesi, konuşma ve yazışmalarına ulaşılması, ses ve görüntülerinin kayda alınması, konum bilgilerinin öğrenilmesi olanaklı hale gelebilmektedir. İkinci bir örnekte ise sosyal medya platformlarının terör örgütlerince propaganda aracı olarak kullanılıyor oluşu bilindik bir durumdur. Propaganda aracı olabilecek tüm resim, yorum, video, şarkı, simge vb. bilgilerden yola çıkarak terör örgütü üyesi olan kişiler ile terör örgütü sempatizanlarını veya terör örgütlerince manipüle edilmeye hazır kişileri tespit edebilmek mümkündür. Doğru zamanda isabetli tespitlerin yapılmasıyla da terör örgütü üyesi olabilecek potansiyel kişilere yönelerek örgütlere katılımın engellenmesi noktasında tedbirler alınabilecektir. Böylece terör örgütlerinin olası insan kaynaklarını oluşturabilecek kişi sayısı minimize edilebilecektir. Üçüncü bir örnek olması açısından terör örgütlerine ait sosyal medyada propaganda aracı olabilecek veriler veya teröristlere ait hesaplar teknik anlamda ele alındığında, birçok bilgiye eş zamanlı ulaşabilmek mümkün olabilmektedir. Bu noktada, ilgili istihbarat servislerinin sosyal medya platformları ile iletişimi büyük önem arz etmektedir. Çünkü sosyal medya platformları ile yapılabilecek ikili bir anlaşmayla, yapılmakta olan tüm yazışma veya konuşmalara anahtar kelimeler üzerinden uyarı veren sistemler kurularak eş zamanlı erişilebilmesi mümkün olabilecek bir durumdur. Bu başarıldığı andan itibaren olası terör eylemleri gibi konulara yönelik bilgileri elde etmek ve daha gerçekleşmeden

engellemek imkân dâhilinde olabilecektir. En nihayetinde sosyal medya platformları üzerinde teröristle mücadelede işe yarar bilginin takibi doğruluk, isabet ve devamlılık ölçeğinde yapılarak yaşanabilecek tüm kötü senaryoları önleyebilmek mümkün olacaktır.

4.2.4. Siber Saldırı

Siber saldırı, tanım olarak siber uzaya entegre bir bilgi teknolojisi aracılığıyla, doğrudan ya da dolaylı olarak başka bir bilgi teknolojisi sistemini veya ağını zarara uğratma, engelleme veya istismar etme[10] amacıyla yapılan eylemlerin tümünü vurgulamak için kullanılmaktadır (Çahmutoğlu, 2020:6). Bu tanımlamadan yola çıkarak siber saldırıların iki temel eylem şeklinde gerçekleştirilebildiği söylenebilmektedir. İlk eylem şeklinde, bir siber saldırı; bilgi teknolojisi sistemleri ile ağlarını veya bu sistemlerde bulunan ya da bu sistemlerden geçiş yapan bilgi ve programları değiştirmek, bozmak veya yok etmek için kasıtlı eylemlerde bulunulması hadisesi olarak karşımıza çıkmaktadır. İkincisinde ise bir siber saldırı, siber uzaydaki bir takım teknik işlemlerin gerçekleştirilerek bilgi teknolojisi sistemlerinde ya da ağlarında bulunan bilgi veya verilerin istismar edilmesi şeklinde yürütülmektedir. Dolayısıyla bir siber saldırı, sadece hedefe zarar verilmesi amacıyla kuvvet uygulanması anlamına gelmemekle birlikte, ilave olarak bilgilerin veya verilerin ele geçirilmeye çalışıldığı casusluk faaliyetlerini de bünyesine alan kavram bütününü oluşturmuştur.

Siber saldırıya yönelik daha basit bir tanımlamaya gidildiğinde, siber savaşçılar tarafından siber uzayda belirli bir amacı gerçekleştirmek için hedeflenmiş sistemlere aktif veya pasif eylemlerde bulunulmasını, siber saldırı olarak kavramsallaştırmak mümkün olabilmektedir. Bu kavramsallaştırmayı yaparken de doğrudan hedefteki bilginin ele geçirilmesi, sisteme zarar verilmesi ya da sistemin devre dışı bırakılması gibi faaliyetleri aktif, sisteme bir şekilde sızılarak sistem üzerindeki bilgi akışının veya davranışların gözlemlenmesinin de pasif saldırı olarak vurgulandığı bilinmelidir (Keleştemur, 2015:287). Bu sonuçla da siber saldırıların teknik ve taktik anlamdaki farklılıklarını ortaya koyarak teröristle mücadeleye katkı sağlayabilecek en bilindik saldırı örneklerini, müteakip başlıklarda ayrıntılı olarak ele almak faydalı olabilecektir.

4.2.4.1. DDOS (Hizmet Dışı Bırakma)

DDOS, İngilizcede hizmet dışı bırakma anlamına gelen ‘‘Distributed Denial of Service’’ cümlesinin baş harflerinden oluşmaktadır (Yenal ve Akdemir, 2020:8). Adından da anlaşılacağı gibi bu saldırılarda, bir sisteme kullanıcılarının erişiminin engellenmesi veya

[10] Burada istismar etme tabiri ile hedeften veri elde etme veya veriyi manipüle etme gibi faaliyetler kastedilmiştir.

sistemin hizmet veremez hale getirilmesi sağlanmaktadır. Dolayısıyla da DDOS saldırılarının temel mantığında, sahte istekler göndermek suretiyle sistemlerin gerçek hizmet isteklerine cevap veremeyecek kadar meşgul edilmesi yatmaktadır (Öğün ve Kaya, 2013:15).

Teknik anlamdaki oluş şeklini incelediğimizde ise saldırıların, toplu trafik olarak bilinen, birbirine bağlı yüzbinlerce çevrimiçi cihazın daha önceden belirlenmiş hedef sisteme yönlendirilerek sistemin mevcut kapasitesini bunaltmak suretiyle gerçekleştirildiği görülmektedir (Yeniman, 2018:3). Burada sistemler gereksiz bilgilerle aşırı derecede yüklendiğinden yavaşlayarak işlev yapamaz veya kendisini savunamaz hale gelmektedir. Böylelikle savunamaz hale gelen sistemlerin güvenlik ağları devre dışı bırakılmakta ve de sistemlerin güvenlik duvarlarından[11] kolaylıkla geçilerek dışarıdan müdahale edilebilmektedir.

Önceden de bahsedildiği üzere, siber uzaya bağlı bir sistemin dışarıdan müdahale edilebilir olması, sistem üzerinden her türlü aktivitenin gerçekleştirilebileceği anlamına gelmektedir. Konumuz itibariyle de bu aktivitelerden birisinin istihbarat olabileceği söylenebilmektedir. Bu nedenle önceden belirlenmiş bir hedef sisteme DDOS saldırısının yapılması, hedefin savunmasız hale getirilerek içerisinde yer alan tüm bilginin kolaylıkla ele geçirilebilmesinde katkı sunabilecektir.

DDOS saldırılarının teröristle mücadelede sunabileceği katkıları olası örneklerle vurgulandığında iki konuda büyüt katkılar sağlayabileceği düşünülebilir. Bu örnekler terörist yapılarca haberleşme, propaganda, eğitim, eylem, saldırı, sabotaj vb. amaçlarla kullanılmakta olan siber uzaya entegre herhangi bir bilişim sistemi üzerinden vurgulandığında, çarpıcı sonuçları daha net görülebilir. Bu düşünceden hareketle ilk olarak, DDOS saldırılarıyla yavaşlayarak işlev yapamaz veya kendisini savunamaz hale getirilen bir sistemin, dış müdahaleyle öncelikli olarak içerisinde yer alan tüm istihbari bilgileri ele geçirmek mümkün olabilmektedir. Teröristle mücadele noktasında ele geçirilmiş olan istihbari bilgiler neticesinde de yeni hedeflere yönelebilmektedir. İkinci olarak ise dış müdahaleyle içerisinde yer alan tüm istihbari bilgilerin ele geçirilmesinin ardından hedef sistemi kalıcı olarak imha ederek büyük kazanımlar sağlanabilmektedir. Böylelikle teröristle mücadelede ihtiyaç duyulan istihbari bilgileri, bir yandan doğrudan kaynağından temin ederken, diğer bir yandan da kaynak sistemi tek bir tuşla eş zamanlı olarak kolaylıkla imha ederek önleyici tedbirler alınabilecektir.

[11] Güvenlik Duvarı, (İngilizce: Qrewall), bir kural kümesi temelinde ağa gelen giden paket trafiğini kontrol eden donanım tabanlı ağ güvenliği sistemidir. Çok sayıda farklı filtreleme özelliği ile bilgisayar ve ağın gelen ve giden paketler olmak üzere internet trafiğini kontrol altında tutar.

4.2.4.2. Kötücül Yazılım Kullanma

Kötücül yazılımlar, çalışmada siber istihbaratın üç ana unsurundan birisini oluşturan siber silahlar içerisinde ayrıntılı olarak vurgulanmıştır. Bu noktada, kötücül yazılım kategorisindeki en bilindik yazılımlardan olan virüsler, solucanlar, Truva atları, arka kapılar, casus ve korsan yazılımlar, robotlar ile tuş, ses vb. kaydediciler kısaca açıklanmıştır. Ancak çalışmanın bu bölümünde, bu silahların, siber istihbaratın elde edilmesinde bir yöntem olarak kullanılmasının genel olarak kısaca vurgulanmasının gerekli olduğu düşünülmüştür. Bu nedenle, siber istihbaratın elde edilmesinde bir siber saldırı türü olarak kötücül yazılımların oynayacağı rol, teröristle mücadele noktasında incelenmeye çalışılmıştır.

Kötücül yazılımlar, çok farklı türleri bulunan önemli siber silahlardandır. Genel kabul görmüş yapı ve özellikte somut bir sayısal türlerinin bulunduğunu söylemek oldukça güçtür. Çünkü kişilerin imkân ve kabiliyetleri ölçüsünde, hayal gücüne bağlı olarak üretildiklerinden hedef sistemlerde gerçekleştirecekleri işlemlerin bir sınırlaması bulunmamaktadır. Yani bir yandan hedef sistemdeki tüm verileri başka bir tarafa aktarırken, diğer bir yandan sistemi kullanılamaz hale getirebilmektedir. Ya da başka bir yöntemle, hedef sistemde hiçbir iz ve emare bırakmadan her türlü bilgiyi, başka bir tarafa aktarabildikleri gibi eş zamanlı olarak da sistemler üzerinden yazı, ses, görüntü, video vb. verileri canlı olarak kayda alarak kullanıcısına aktarabilmektedir. Örnek olması açısından James Wan'ın yönetmenliğini yaptığı 2015 yılında gösterime giren Hızlı ve Öfkeli 7 filminde, kurgusal olarak Ramsey adlı bir hacker tarafından üretilen Tanrının Gözü adlı canlı takip programı göz önüne getirildiğinde, kötücül yazılımların gücü daha iyi anlaşılabilmektedir (Beyazperde, 2015). Filmde kurgulanan bu programda, hedefteki kişinin ses, yüz, DNA veya parmak izi biyometrisinden siber ağa bağlı her sisteme anında erişim sağlanarak nerede olduğu kolayca bulunmaktadır. Sistemin hedefteki kişiyi bulması ve eş zamanlı olarak takibini yapması içinde, herhangi bir cep telefonu, bilgisayar, ATM kamerası, uydu, sinyal dağıtıcı vb. siber uzaya bağlı sistemlere ait mikrofon veya objektife ses, görüntü, kişisel veri gibi bilgilerinin yakalanması yetmektedir. Kısaca Tanrının Gözü adlı programın hedefteki kişiyi birkaç saniye içerisinde bulması için, hedefin herhangi bir siber uzaya bağlı kameranın görüş açısına girmesi veya konuşmasının mikrofonun çekim alanına yakalanması kâfi gelmektedir. Böylece Tanrının Gözüyle bulunan hedef kişi, canlı olarak takip edilerek kimlerle neler yaptığına ulaşılabilmekte ve gerek duyulduğunda uçak, helikopter, füze, roket vb. yardımıyla anında etkisiz hale getirilebilmektedir. Dolayısıyla bu ve benzeri programlar, teröristle mücadele anlamında hayata geçirilerek insanlık yararına kullanıldıkları takdirde, muazzam birer silah olabilmektedir.

Günümüzde böylesine ciddi bir yazılımın var olduğu düşünüldüğünde, kritik terör örgütü liderlerinin takibinin anında yapılabileceği bilinmelidir. Ya da canlı bomba, eylem, saldırı vb. anahtar kelimelerin takibi üzerinden yeni terör örgütü mensuplarının tespitinin yapılarak olası saldırıların gerçekleştirilmeden önlenmesi sağlanabilecektir. Örneğin 2001 yılında, 11 Eylül terör saldırıları göz önüne alındığında, günümüzde Tanrının Gözü benzeri yazılımların uygulamaya konmasıyla yeni 11 Eylül vakalarının yaşanması anında engellenebilecektir. Dolayısıyla da saldırının ardından on yıl sonra bulunabilen Usame bin Ladin gibi lider teröristlerin, bu sistemlerin kullanılmasıyla birkaç saat içinde konum bilgisini tespit ederek anında imha edilmesi sağlanabilecektir. Böylece az bir maliyetle, eş zamanlı olarak doğru ve isabetli bir istihbarat elde edilerek örgüt üyelerinin veya kullandıkları sığınak, mağara vb. yerlerin tespiti yapılabilecek, gerek görüldüğü takdirde de siber uzaya bağlı konvansiyonel veya yoğunlaştırılmış enerji silahlarıyla imhası sağlanabilecektir.

4.2.4.3. Phishing (Yemleme/Oltalama)

Türkçede yemleme veya oltalama anlamına gelen phishing, internette yer alan güvenli iletişim kaynaklarının taklit edilmesiyle veya yeni oluşturularak güvenli bir iletişim kanalı gibi gösterilmesiyle, hedef kullanıcıların irtibata geçmesinin sağlandığı ve bu sayede de hedef kullanıcılardan ihtiyaç duyulan tüm bilgilerin aldatma yoluyla elde edildiği eylem olarak karşımıza çıkmaktadır (Özcoban, 2014:63). Eylemin temel mantığında, ihtiyaç duyulan bilgilerin girilmesinin gerekli olduğu, bilindik bir kurum veya kuruluşun web sayfasının birebir kopyasının yapılması veya yeni ve güvenilir bir kuruluş imajıyla web sitesi oluşturularak sisteme giriş yapmak isteyen kullanıcıların bilgilerinin ele geçirilmesi amaçlanmaktadır (Yılmaz ve Salcan, 2008:59). Yani bir nevi yem takılarak denize atılan oltaya balığın yakalanması beklenmektedir. Bu sebepten de oltalama veya yemleme anlamına gelen phishing saldırısı olarak tanımlanmıştır.

Saldırıların yapılış şekli incelendiğinde, önceden açık kaynak istihbaratıyla elde edilmiş hedefe yönelik bilgilerden akılcı bir strateji izlenerek hedefin ilgisini çekecek bir web sitesi oluşturulup istenilen bilgilerin ele geçirildiği gözlemlenmektedir. Dahası ise yine önceden açık kaynaklardan elde edilmiş bilgilerden hedefin ilgi duyduğu web sitelerinin sahtesi tasarlanarak aynı şekilde istenilen bilgilerin alındığı görülmektedir. Bunları yaparken de hedefe üyesi olduğu bir web sitesi veya tanıdığı bir kişiymiş gibi mesaj, e-posta vb. yollarla ulaşılarak bilgilerini güncellemesi gerektiği, bir ödül kazandığı, ödülün kendisine teslimi için kimlik ve adres bilgisini vermesinin zorunlu olduğu gibi gerekçeler göndererek yönlendirildiği söylenebilmektedir. İlgili içeriklere tıklayarak bilgilerini güncellediğini zannetmekte olan

hedefin, adeta oltaya gelerek kendi bilgilerini, kendi eliyle karşı tarafa vermesiyle de saldırı nihayete ermektedir (Öğün ve Kaya, 2013:16).

Phishing saldırılarının bu noktada kötü amaçlı kişiler tarafından internet kullanıcılarına zararlar verebileceği görülmekle birlikte, istihbarat operasyonları açısından büyük katkılar sunacağı da açıkça değerlendirilebilmektedir (Keleştemur, 2018:105). Bu doğrultuda, olası bir terör örgütüne yönelik hedefe alınan kişinin gerekli takibi yapılarak ilgi duyduğu web sitelerine, sosyal medya hesaplarına erişim sağlayabilmek için saldırı düzenlenebilecektir. Saldırı sonucunda, erişim sağlanan profillerinden tüm yazışmaları ile irtibatlı olduğu kişilerin kimler olduğu bilgisi kolayca saptanarak olası yeni gizli hücreler tespit edilebilecektir.

4.2.4.4. Spam (İstem Dışı E-Posta) Gönderimi

İnternet üzerinden elde edilen elektronik adreslere, alıcının haberi olmaksızın ara sıra büyük hacimlerde gönderilen e-postalara istem dışı alınan e-postalar (spam) denilmektedir (Memiş, 2005:2-3). İstenmediği halde gönderilen bu e-postalarda, genellikle pazarlama, reklam, sosyal içerik vb. amaçlarla kitlelere ulaştırılmak istenen mesajların, kullanıcıların isteği dışında kendisine internet veya mobil teknolojiler yardımıyla gönderilmesi mantığı yatmaktadır (Aslay, 2017:3). Dolayısıyla elektronik ortamlarda çok sayıda farklı kişiye aynı anda veya özel olarak gönderilen gereksiz ve uygunsuz tüm iletiler birer spam olama özelliği taşımaktadır.

İstem dışı elektronik posta olarak gönderilen e-postalar aracılığıyla, tüm bu pazarlama, reklam, sosyal içerik vb. içeriklerin dışında ayrıca bilgisayarlara kötücül yazılımlar bulaştırılmak ve herhangi bir konuda propaganda yapmak amaçlı kullanım olabilmektedir (Öğün ve Kaya, 2013:12). Bu kullanımlarda yığın veya tek seferde gönderilen e-postalarda, öncelikle açıldığında sisteme gizlice kötücül yazılım yükleyen dosyalar, belgeler, uzantılar vb. veri yollarının bulunduğu görülmektedir. Bu veriler aracılığıyla, kötücül yazılımların sisteme kolayca yüklenebilmesi sağlanmaktadır. Bu noktada kötücül yazılımın sisteme fark edilmeden yüklenebilmesi için spam mesajın gönderildiği kişi tarafından açılması yeterli olmaktadır. Propaganda aracı olarak kullanımlarda ise bir anda yüzbinlerce kişiye anında ideolojik görüş, fikir, öneri gibi içerikler gönderilebilmektedir. Bu gönderiler siyasi kurum, kuruluş, parti, vakıf vb. olabileceği gibi terör örgütlerince de gönderilmiş olabilmektedir. Dolayısıyla herhangi bir terör örgütü tarafından propaganda amaçlı gelmiş olabilecek e-postalara tersine mühendislik[12] yöntemiyle ulaşmak mümkün olabilecektir. Bu sonuçla da gerek hedeflere içerisine kötücül

[12] Siber uzayda tersine mühendislik, belirli bir akış ile yapılmış olan herhangi bir işlemin en son noktasından başlangıç noktasına doğru gidilerek işlemi yapın kişiye ulaşılması anlamı taşımaktadır.

yazılımlar gömülü spam mesajlar göndererek istihbarat bilgisi elde edilebilecek, gerekse terör örgütlerince propaganda amaçlı gönderilmiş olan spam mesajların nereden ve kim tarafından gönderilmiş olduğu öğrenilebilecektir.

4.2.4.5. Şebeke Trafiğinin Dinlenmesi

Siber uzaya bağlı, bilgi sistem ağları arasındaki veri paketlerinin izinsiz ve yetkisiz bir şekilde dinlenmesi yöntemidir (Öğün ve Kaya, 2013:16). Bu yöntem, kendi içerisinde aktif ve pasif olmak üzere ikiye ayrılmaktadır. Aktif dinlemede daha çok izleme (monitoring) adı verilen hedefe alınmış ağ üzerindeki veri transferlerinin izlenerek dinlenmesi amaçlanırken, pasif dinlemede ise koklama (sniffing) adı verilen herhangi bir ağ üzerindeki veri transferlerinin yakalanarak dinlenmesi amaçlanmaktadır (Elfa, 2021 ve Demir, 2017). Bu sayede gerek şifreli gerekse şifreleri çözümlenebilen veriler ele geçirilerek üzerinden istihbarat elde edilebilmektedir.

Şebeke trafiğinin dinlenmesiyle elde edilebilecek istihbarat, teröristle mücadele noktasında da kıymetli bir yöntem olabilecektir. Çünkü pasif dinlemelerle terör örgütlerince kullanılan bilgisayarlar, haberleşme kanalları vb. bilgi sistemlerini tespit edebilmek imkân dâhilinde olabilecektir. Aktif dinlemelerle de tespit edilmiş bu hedefleri dinleyerek eylemleri, amaçları, çalışmaları, mevcut durumları gibi önemli bilgilerini toplamak mümkün olabilecektir. Elde edilen tüm bu kritik öneme sahip bilgilerden terör örgütlerinden her daim bir adım önde olunarak gerek önleyici gerekse imha edici müdahalelerde bulunulabilecektir.

4.2.4.6. Sosyal Mühendislik (Social Engineering)

Sosyal mühendislik yöntemi genel olarak gizlice hedef sistemlere erişim sağlamak, sistemlerde yönetici hakkı elde ederek kalıcı olmak veya sistemleri ele geçirerek kritik bilgileri toplamak amaçlı kullanılmaktadır (Özel, 2018). Bu amacı gerçekleştirirken de hedefe, güvenilir bir kişi gibi yaklaşmak, yardımsever bir tavır sergilemek, aynı ilgi alanlarına sahip olunduğunu hissettirmek, özellikle sosyal medyadan önce çevresi sonra kendisiyle takipleşilerek tanıdıkları üzerinden yakınlık kurmak veya başka bir kişiyi taklit ederek sanki bu kişiymiş gibi iletişime geçmek kullanılabilecek en sık metotlardandır (Keleştemur, 2015:307). Bu ve benzeri akla gelebilecek metotların kullanılmasıyla da hedeflerin kolayca kandırılarak istenilen amaç doğrultusunda yönlendirilmesi mümkün olabilmektedir. Hedefin doğru yönlendirilmesi neticesinde de kullandığı veya bağlı olduğu tüm sistemlere giriş yetkisi elde edilerek istenilen bilgilere kolayca erişim sağlanabilmektedir.

Sosyal mühendislik bir yöntem olarak incelendiğinde; kısaca ‘‘yalan söyleme veya karşı tarafı kandırarak ikna etme üzerine kurgulanmış bir bilgi toplama sanatı’’ olduğu görülmektedir (Mitnick ve Simon, 2006:303). Temel mantık olarak da hedef kişilerin güvenleri kazanılarak arzu edilen amaçlar doğrultusunda yönlendirilmeye çalışıldığı söylenebilmektedir. Bu yönlendirmelerin yapıldığı alanlar üzerinden gidildiğinde de siber uzaya bağlı tüm sistemlerin araç olarak kılınması konumuz açısından incelenebilmektedir. Böylelikle sosyal mühendisliğin siber uzay üzerinden gerçekleştirilmesini, siber istihbaratın elde edilmesinde kullanılan bir yöntem olarak görmek ve bu doğrultuda da örnekler üzerinden anlatmak mümkündür.

Sosyal mühendislik yöntemini konumuza yönelik olası bir örnekle açıklamak gerekirse, hedefe alınan bir terör örgütü üyesi veya sempatizanının kandırarak arzu edilen amaçlar doğrultusunda yönlendirilebileceği bilinmelidir. Bu yönlendirmeyi yaparken de form, oyun, alışveriş, arkadaşlık ve sosyal medya platformları üzerinden hedefi, sahte senaryolarla ikna etmek, güvenilir bir kaynaktan arıyormuş gibi yapmak veya para, eşantiyon, hediye vb. kazanmak vadiyle kandırarak üzerinde güven kazanmak gerekmektedir. Gerekli güven kazanıldıktan sonrada, hedefe gerek e-posta göndererek, gerekse sahte bir site, uygulama vb. bir sisteme giriş yapmasını sağlayarak hem ihtiyaç duyulan bilgileri elde etmek, hem de hedefin kullandığı sisteme kötücül yazılım yüklemek mümkün olabilmektedir. Böylelikle bir yandan elde edilen bilgilerle hedefin kullanmakta olduğu sistemlere girilebilmekte, diğer bir yandan da hedef tarafından kullanan sistemlere yüklenen kötücül yazılımlar vasıtasıyla hedefin eş zamanlı olarak takibi yapılabilmektedir. Sonuç itibariyle de hedeften teröristle mücadeleye yönelik her türlü istihbari bilgi, az bir maliyetle ve gerçek kimlik bilgisi deşifre edilmeden eş zamanlı olarak temin edilebilecektir. Dahası ise görüştüğü kişiler ve hareketleri takip edilerek bağlı olduğu terör örgütünün yeni üyeleri, eylemleri ve hedefleri saptanabilecektir. Bu sayede gerek önleyici gerekse imha edici müdahalelerde bulunarak teröristle mücadele noktasında önemli kazanımlar elde edilebilecektir.

4.2.4.7. Eavesdropping (Kulak Yöntemi)

Türkçede amiyane tabirle “kulak misafiri olmak” anlamına gelen eavesdropping yöntemi, günümüz dijital dünyasında cihazlar arasında iletilen verilerin üçüncü kişiler tarafından takibi, ele geçirilmesi ve izinsiz olarak kullanılmasını ifade eden bir yöntem olarak karşımıza çıkmaktadır (Bergnet, 2021). İletilen verinin ele geçirilmesi, takibi ve izinsiz olarak kullanılması içinde gerek siber uzaya bağlı ağ kablolarına saplama yapılmakta gerekse siber uzaya bağlı ağ kablolarının elektromanyetik yayılımları yakalanmaktadır (Donanım Haber Forum, 2011). Bu sayede siber uzaya entegre bilgi sistemlerinden, ağlardan, mikro dalga

devrelerden ve uydu sinyallerinden çıkan yayılımları yakalayarak ihtiyaç duyulan konuşma, ileti, gönderi vb. tüm veriler elde edilebilmektedir.

Günümüzde tüm bu veriler kişilerin birbiriyle iletişiminde akıllı telefonlar, bilgisayarlar, tabletler vb. aracılığıyla internet veya mobil teknolojiler üzerinden kolayca aktarılmaktadır. İnternet veya mobil teknolojiler üzerinden aktarılan verilerde, doğal olarak kendisini istihbaratın elde edilmesinde önemli birer hedefe dönüştürmektedir. Dolayısıyla da buradan anahtar kelimeler, sözcükler ve sesler üzerinden yakalama yapılarak ihtiyaç duyulan istihbarata yönelik önemli bilgilere ulaşılabilmesi mümkün olabilmektedir. Örneğin; teröre müzahir bir bölgede siber uzaya bağlı ağ kablolarına saplama yapıldığı veya elektromanyetik yayılımlarının yakalandığı varsayımı göz önüne getirildiğinde, o bölgedeki tüm iletişimin veya veri akışının takip edilebileceği açıkça görülebilecektir. Bu noktada eylem, saldırı, propaganda, bomba, c4, silah, bilinen terör örgütü üyeleri isimleri vb. anahtar kelimeler üzerinden yakalama yapılarak binlerce veri akışından teröristle mücadeleye yönelik ihtiyaç duyulan istihbarat kolayca sağlanabilecektir. İhtiyaç duyulan bilginin sağlanmasıyla da teröristle mücadelede etkin ve üstün bir konumda olunabilecektir.

4.2.4.8. Casus Araç Kullanımı

Casus araç kullanımı, gizli birtakım aktivitelerle spyware (casus yazılımlar) olarak adlandırdığımız yazılımların kullanılarak bilginin elde edilmesi yöntemidir. Dolayısıyla Casus araç kullanımı yöntemiyle, siber uzaya bağlı herhangi bir bilgi sistemine veya bilgi ağı bölgesine gizlice sızılarak casusluk faaliyetlerinde bulunulabilmektedir. Böylece, casus araçlar kullanılarak hedef sistemlerdeki bilgiler ve faaliyetlerin kullanıcılarının fark etmesine ihtimal bırakılmadan toplanması veya izlenerek takip edilmesi sağlanabilmektedir. Bu sonuçlarda casus araç kullanımını, siber istihbaratın elde edilmesinde bir yöntem olarak karşımıza çıkarmaktadır.

Bilgi sistem veya ağ bölgesinde yapılan casusluğa, terörist kullanıcıların terminal veya çalışma istasyonlarında, çalıştıkları anda ekranlarına gelen görüntü, ses, dosya, metin ya da klavyeden girilen bilgilerin gözetlenebilmesini veya takip edilebilmesini örnek gösterebilmek mümkündür. Bu noktada da teröristlerin birbiri arasındaki iletişim, görüşme, veri transferi vb. bilgilerinin fark edilmeden gözlemlendiği düşünüldüğünde, elde edilebilecek istihbaratın olası sonuçları daha iyi anlamlandırılabilmektedir. Sonuç itibariyle de teröristle mücadele noktasında ihtiyaç duyulan doğru bilginin casus yazılımlar vasıtasıyla, kaynağından eş zamanlı olarak toplanabileceği açıkça görülebilmektedir.

4.2.4.9. Masquerading (Yerine Geçme)

Yetkisiz bir kişinin herhangi bir sistemin tüm imkânlarından istifade edebilmek amacıyla, sisteme yetkisi bulanan bir kişiymiş gibi gözükerek giriş sağlandığı yöntemi ifade etmektedir (Keleştemur, 2015:309-310). Temel mantığında, sistemlerde yapılacak hileler ile erişim imkânı kısıtlı ya da yetkisi hiç olmayan kullanıcıların, erişime yetkisi olan başka kullanıcıların bilgi ve yetkilerini kullanarak yani bir nevi onların yerine geçerek sisteme erişim sağlaması yatmaktadır (Aslay, 2017:3). Bu erişimi sağlayabilmek içinde, yerine geçilecek kişilerin kullanıcı adları, şifreleri, e-posta ve kimlik bilgileri gibi çeşitli verilerini diğer siber istihbarat yöntemleriyle ele geçirmek gerekmektedir. Giriş yapılmak istenilen sisteme ait verilerin ele geçirilmesiyle de bilgileri ele geçirilen kişinin yerine geçilerek sistem üzerinde yetkili olunan tüm işlemleri yapmak mümkün olabilmektedir. Böylelikle gerek istihbaratın elde edilebilmesi gerekse sistemlerin yavaşlatılması, kullanılamaz hale getirilmesi veya yok edilebilmesi gibi sonuçlar, sisteme giriş yapan kişinin parmak uçlarında olabilecektir.

Yerine geçme yöntemi teröristle mücadele noktasında incelendiğinde, yine daha önceden verilen benzer örneklere yakın sonuçların alınabileceği söylenebilir. Çünkü hedefe konan bir örgüt üyesinin siber uzaya bağlı sitemlere ait bilgilerinin sosyal mühendislik, bal tuzağı, kötücül yazılım, açık kaynak, sniffing veya monitoring gibi çeşitli siber istihbarat yöntemleriyle kolayca elde edilmesi imkân dâhilindedir. Bu nedenle kullanmış oldukları sistemlere ait bilgiler ele geçirilebildiğinde, zaman ve mekân kısıtlaması bulunmaksızın bu sistemlere, rahatlıkla giriş yapılabilmektedir. Sistemlere giriş yapıldığı andan itibaren de gerek her türlü yazışma, konuşma, aktivite vb. veriler ele geçirilebilecek gerekse iletişim halinde olduğu kişilerle, yerine geçilen kişiymiş gibi görüşülerek yeni bilgiler edinilebilecektir. Dahası, sistem ve iletişim halinde olduğu diğer sistemlere kötücül yazılımlar göndererek istihbarat ağı genişletilebilecek ve de gerek duyulduğunda bu ağa bağlı tüm sistemler imha edilebilecektir. Nihai olarak da yine teröristle mücadele noktasında önemli istihbarat faaliyetlerinde bulunularak etkinlik ve üstünlük sağlanabilecektir.

4.2.4.10. Network Scanning (Ağ Tarama)

Siber saldırı öncesinde ya da siber saldırı hazırlığı aşamasında hedef sistemlerle ilgili, sistemlerin zafiyetlerine yönelik açıklıkların tespit edilmesi amacıyla yapılan gözlemleme yöntemidir (Keleştemur, 2018:98). Temel mantığı, siber uzay ağları üzerindeki sistemleri tespit etmek, tespit edilen sistemlerdeki açıklıkları saptamak ve sistemler üzerinde çalışmakta olan

bileşenleri analiz etmek üzerinedir (Şen, 2018). Dolayısıyla da aktif hostları[13], ip adreslerini[14], aktif hostların açık portlarını[15], işletim sistemlerini[16], sistem mimarisini[17], sistem topolojisini[18], hostlarda çalışan servisleri ve aktif hostların zafiyetlerini keşfetmek için kullanılabilmektedir. Bu sayede hedef sistemler hakkında detaylı bilgilere ulaşılarak sistem üzerinden gerçekleştirilmek istenecek faaliyetlere yönelik en doğru harekât tarzı belirlenebilmektedir.

Ağ taraması yaparken gerek internet üzerinde yer alan gerekse bu iş için yazılmış uygulamalardan yararlanılmaktadır. Ancak bu uygulamalar kendi içerisinde farklı taramalar yapan, çok sayıda farklı işlevlere sahip olabilmektedir. TCP Syn Scan[19], TCP Connect Scan[20],

[13] Host, Türkçede ağ anlamına gelmekte olup, daha çok bir bilgisayar ağına bağlı bulunan bilgisayar veya başka cihazları ifade eder. Aktif hostlarda, ana bir bilgisayar görevi görerek ağdaki kullanıcılara veya diğer ana bilgisayarlara bilgi kaynakları, hizmetler ve uygulamalar sunan sunuculardır. Dolayısıyla bir web sitesine internette yer ve erişim sağlayıcı hizmet veren firmalara hosting firması denilir.

[14] IP adresi, İngilizce internet protocol address kelimelerinin kısaltmasıdır. İnterneti ya da TCP/IP (Transmission Control Protocol/İletim Kontrol Protokolü) protokolünü kullanan diğer paket anahtarlamalı ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişini yapmak için kullandıkları adresleri ifade eder.

[15] Port, bir bilgisayarla dış aygıtlar ve programlar arasındaki iletişimi sağlayan veri kanalıdır. Bu veri kanalları üzerinden kişiler sistemlere erişim sağlayarak veri transferi, iletişim, alışveriş, oyun vb. aktivitelerini gerçekleştirmektedir.

[16] İletim sistemi; bilgisayarda çalışan donanım kaynaklarını yöneten ve çeşitli uygulama yazılımları için yaygın servisleri sağlayan bir yazılımlar bütünüdür. Uygulama programları ve bilgisayar donanımı arasındaki iletişimi sağlamaktadır. Microsoft Windows, IOS, Android, Mac OS, BeOs ve GNU/Linux en bilindik örneklerindendir.

[17] Mimari tanımı; sistemin yapıları ve davranışları hakkında mantıksallığı destekleyecek şekilde organize edilen ilişkiselliğin standart bir açıklaması veya temsilidir. Dolayısıyla bir sistem mimarisi de sistemin uygulanması için birlikte çalışan sistem bileşenlerini, geliştirilmiş ve genelleştirilmiş sistemleri içermektedir. Çoklu sistemlerin mimarisi olarak da adlandırılan bu yapı; sistemin yapısını, davranışını ve biçimselliğini tanımlayan kavramsal bir modeldir.

[18] Ağ bilgisayar sistemlerinin nasıl konumlandırılacağını, nasıl bağlanacağını ve veri iletişiminin nasıl olacağını belirleyen genel yapıdır. Fiziksel ve mantıksal olarak ikiye ayrılmaktadır. Fiziksel topoloji; ağın fiziksel olarak nasıl görüneceğini belirleyen katmandır. Mantıksal topoloji ise; bir ağdaki veri akışının nasıl olacağını belirleyen veri iletim katmanıdır.

[19] Kaynak makinanın hedef makinaya TCP SYN bayraklı segment göndererek başlattığı bir tarama türüdür. Portların kapalı olduğu durumlarda hedef makina cevap olarak RST + ACK bayraklı segmenti döndürür. Portların açık olduğu durumlarda ise hedef makina SYN + ACK bayraklı segment döndürür. Daha sonra kaynak makina RST bayraklı segment göndererek bağlantıyı koparır ve böylelikle TCP üçlü el sıkışma (TCP three-way handshaking) tamamlanmaz. Bu tarama türünde TCP üçlü el sıkışma gerçekleşmediği için bu tarama türü hedef sistemlerinde herhangi bir şekilde iz bırakmaz.

[20] Kaynak makinanın gerçekleştireceği TCP Connect Scan, kapalı portlara yapıldığı zaman RST + ACK bayraklı segment dönecektir. Ancak açık portlara yapıldığı durumlarda hedef makinanın göndereceği SYN + ACK bayraklı segmenti, kaynak makina ACK bayraklı segment göndererek cevaplar ve üçlü el sıkışmayı tamamlar.

FIN Scan[21], Xmaps (Christmas) Scan[22], Null Scan[23], Ping Scan[24], UDP Scan[25], IP Protocol Scan[26], ACK Scan[27], Window Scan[28] vb. taramaları, bu farklılığın işlevsellik anlamındaki en bilindik örneklerindendir (Çıtak, 2016:91-94). Dolayısıyla tek tek ele almak yerine genel anlamda değerlendirildiğinde, yapılan taramalarla hedef sisteme yönelik ihtiyaç duyulan her türlü bilginin öğrenilebileceği açıkça gözlemlenebilmektedir. Hedefe yönelik ihtiyaç duyulan bilgilerin elde edilmesiyle birlikte, gerek hedefe kötücül veya casus yazılımlar yüklenerek, gerekse tespit edilen arka kapıları üzerinden istenildiği anda sisteme giriş yapılarak istihbarat, saldırı, veri hırsızlığı, casusluk gibi faaliyetler icra edilebilmektedir. Sonuç olarak da teröristle mücadeleye yönelik çalışmalarda, hedef sistemlere sızarak hedefi izlemek, verilerini ele geçirmek, irtibatlı olduğu sistemlere erişebilmek ya da gerekli görüldüğünde saldırıda bulunarak imha etmek amacıyla kullanılabileceklerdir.

[21] Hedef makinaya TCP bağlantı isteği olmadan gönderilen segmentle tarama yapılır. Kaynak makinanın göndereceği FIN bayraklı segment, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı segment döndürecektir. Eğer açık portuna gelirse hedef makinadan herhangi bir tepki dönmeyecektir.

[22] Bu tarama türünde kaynak bilgisayarın TCP segmentine URG, PSH ve FIN bayraklarını set edeceği ("1" yapılacağı) segment hedef makinaya gönderilir. Eğer Kaynak makinanın göndereceği URG, PSH ve FIN bayraklı segment, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı segment döndürecektir. Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir. Bu tarama türünde TCP başlığı içerisinde yer alan toplam altı adet bayraktan üç tanesi set edildiği ("1" yapıldığı) için, gönderilen segment yılbaşı ağacının yanan lambalarına benzetilmiştir. Bundan dolayı da bu tarama türüne Xmas (Christmas) Scan denmiştir.

[23] Hiçbir bayrağın bulunmayacağı bu tarama türü, gerçek hayatta karşımıza çıkmayan bir durumdur. Kaynak makinanın göndereceği bayraksız segmentler karşısında hedef makinanın vereceği tepkiler FIN Scan ile aynıdır. Kaynak makinanın göndereceği bayraksız segment, hedef makinanın kapalı bir portuna gelirse hedef makina RST + ACK bayraklı segment döndürecektir. Eğer port açık olursa hedef makinadan herhangi bir tepki dönmeyecektir.

[24] Bu tarama türünde kaynak makina hedef makinaya tek bir ICMP Echo istek paketi gönderir. IP adresi erişilebilir ve ICMP filtreleme bulunmadığı sürece, hedef makina ICMP Echo cevabı döndürecektir. Eğer hedef makina erişilebilir değilse veya paket filtreleyici ICMP paketlerini filtreliyorsa, hedef makinadan herhangi bir cevap dönmeyecektir.

[25] Kaynak makinanın hedef makinaya göndereceği UDP datagramına, ICMP Port Unreachable cevabı döndürülüyorsa hedef makina kapalı kabul edilecektir. Herhangi bir tepki döndürmeyen hedef makina open filtered kabul edilecektir. UDP datagramıyla cevap döndüren hedef makinaya ait port ise açık kabul edilecektir.

[26] Bu tarama türü standart NMAP tarama türlerinden biraz farklıdır. Bu tarama türünde hedef makinaların üzerlerinde çalışan IP tabanlı protokoller tespit edilmektedir. Bu yüzden bu tarama türüne tam anlamıyla bir port taraması demek mümkün değildir. Hedef makina üzerinde, taramasını yaptığımız IP protokolü aktif haldeyse hedef makinadan bu taramaya herhangi bir cevap gelmeyecektir. Hedef makina üzerinde, taramasını yaptığımız IP protokolü aktif halde değilse hedef makinadan bu taramaya, tarama yapılan protokolün türüne göre değişebilen RST bayraklı (RST bayrağı "1" yapılmış) bir segment cevap olarak gelecektir.

[27] Bu tarama türünde kaynak makina hedef makinaya TCP ACK bayraklı segment gönderir. Eğer hedef makina ICMP Destination Unreachable mesajını dönerse ya da hedef makinada bu taramaya karşılık herhangi bir tepki oluşmazsa port “filtered” olarak kabul edilir. Eğer hedef makina RST bayraklı segment döndürürse port “unfiltered” kabul edilir.

[28] Window Scan, ACK Scan türüne benzer ancak bir önemli farkı vardır. Window Scan portların açık olma durumlarını yani “open” durumlarını gösterebilir. Bu taramanın ismi TCP Windowing işleminden gelmektedir. Bazı TCP yığınları, RST bayraklı segmentlere cevap döndüreceği zaman, kendilerine özel window boyutları sağlarlar. Hedef makinaya ait kapalı bir porttan dönen RST segmentine ait window boyutu sıfırdır. Hedef makinaya ait açık bir porttan dönen RST segmentine ait window boyutu sıfırdan farklı olur.

4.2.4.11. Açık Mikrofon Dinleme

Klasik anlamdaki açık mikrofon dinlemesi, geçmişten günümüze istihbaratın elde edilmesinde gerek mobil teknolojiler gerekse böcek mikrofon adı verilen cihazlar vasıtasıyla ortam dinlemesinin yapıldığı bir yöntemi akıllara getirmektedir. Ancak ortam dinlemesinin yapıldığı bu yöntem, günümüzde mobil teknolojiler ve böcek mikrofonlarla sınırlı kalmamıştır. Teknolojik anlamdaki yaşanan gelişmelere paralel olarak yeni teknik ve taktikleri ortaya çıkarmıştır. Ortaya çıkan bu yeni teknik ve taktiklerde, cep telefonu gibi üzerinde mikrofon bulunan bilgisayar, televizyon, buzdolabı, çamaşır makinesi, süpürge, akıllı saat vb. cihazlar üzerinden ortam dinlemesinin yapılabilmesine imkân tanımıştır (Keleştemur, 2018:97).

İçerisinde mikrofon bulunan tüm bu cihazlar üzerinden dinlemenin yapılabilmesi için cihazların öncelikle internete bağlı bulunması gerekmektedir. Çünkü internete bağlı bulunan cihazlara kötücül yazılımlar, arka kapılar veya diğer siber saldırı yöntemleriyle erişim sağlanarak mikrofonları aktive etmek mümkün olabilmektedir. Örnek olması açısından siber savaşçılarca bir web sitesine, uygulamaya veya oyuna her giriş yapan cihaz ile bu cihazların iletişime geçtiği diğer cihazların mikrofon ikonlarını aktive edebilecek gizli bir kod yazıldığı düşünüldüğünde, olası sonuçları daha net anlaşılabilmektedir. Bu noktada herhangi birinin içerisinde gizli kod barındıran web sitesine, uygulamaya veya oyuna giriş yapması gerek kendisinin gerekse iletişime geçtiği diğer cihazların mikrofonlarının fark edilmeden aktive edilmesiyle neticelenecektir. Sonuç itibariyle de aktive edilen mikrofonlar üzerinden, canlı olarak ortam dinlemesinin yapılabilmesi sağlanabilecektir.

Verilen örnekte, gizli kod veya casus yazılım barındıran web sitesi, uygulama veya oyuna terörle iltisaklı kişilerin girdikleri varsayımında bulunulduğunda, açık mikrofon dinlemenin teröristle mücadeledeki önemi daha net kavranabilecektir. Burada, canlı olarak dinlenmekte olan kişi sayılarının yüzbinleri bulabileceğinden, anahtar sözcüklerin yakalanarak hedefe dikkat çekilmesinin mantıklı bir yol olacağı açıktır. Anahtar sözcüklerin yakalanarak yapılan konuşmaların dinlenmesi sayesinde de terörle iltisaklı kişiler tespit edilebilecektir. Sonuç olarak gerek yeni terör hedeflerini gerekse teröristlerin son planlarını açığa çıkararak önleyici ve imha edici önlemler alınabilecektir.

4.2.4.12. IP Spoofing (IP Aldatmacası)

İnternete bağlanan cihazlar arasındaki bağlantı TCP/IP[29] olarak bilinen birtakım protokoller üzerinden sağlanmaktadır. Bu protokoller aracılığıyla, başka bir sisteme bağlanıldığında bağlantı yapan cihazın IP adresi[30] karşı tarafa tanıtılmaktadır. Ancak IP adreslerindeki kaynak IP adresini değiştirerek ya da vekil sunucular vasıtasıyla diğer sitelerde işlem yaparak gerçek IP adreslerini gizlemek mümkün olabilmektedir. Bu durumda ortaya Ip spoofing (IP aldatmacası) denilen, bir sisteme yanlış veya taklit bir IP adresinin gösterilerek gerçek IP adresinin gizlenmesini sağlayan yöntemi çıkarmaktadır (Öğün ve Kaya, 2013:15). Ortaya çıkan yöntemle de hedef sistemler güvenilir bir sistemle iletişim kurduğuna ikna edilerek sızılmaya açık hale gelmektedir.

Ip spoofing yöntemi genel hatlarıyla değerlendirildiğinde, siber savaşçıların kimliğini gizlemek, başka bir bilgisayar sistemini taklit etmek veya her ikisini birden değiştirmek için, olduğundan farklı bir kaynak adresi ile IP paketlerini oluşturmak amaçlı kullanılabileceği görülmektedir (Yenal ve Akdemir, 2020:10). Dolayısıyla da teröristlere ait olduğu tespit edilen sistemlere yönelik kullanıldığı düşünüldüğünde, deşifre olunmadan sistemlere sızılabileceği dikkate alınmalıdır. Sızılan sistem üzerinden de gerek istihbarat gerekse saldırı gibi arzu edilen her türlü işlemleri, saniyeler içerisinde gerçekleştirebilmek mümkün olmaktadır.

Sonuç olarak siber istihbaratın siber saldırı yöntemiyle elde edilmesi, son derece dinamik bir yapıda yürütülmektedir. Yaşanan yeni gelişmelerde, farklı türlerde yeni saldırı tekniklerinin geliştirilmesini sağlamaktadır. Bu teknikler, trapdoor (tuzak kapı), DNS[31] aldatmacası, internet servis saldırıları, kriptografik saldırılar, zamanlama saldırıları, bilgi ve veri aldatmacası gibi daha da çok çoğaltılabilmektedir. Ancak yukarıda anlatılan tekniklerin, bu alanda günümüzdeki en bilindikleri olması sebebiyle daha fazla örnek yöntemleri vurgulamanın gereksiz bir uzatma olabileceği değerlendirilmiştir. Bu nedenle de konu hayal

[29] Açılımı Transmission Control Protocol/Internet Protokol (İletim Kontrol Protokolü/İnternet Protokolü) olan TCP/IP internetin temel protokollerini içeren bir pakettir. Birçok protokolün bir araya gelmesi ile oluşmuştur. TCP kısmı veri transferinde önemli noktaları belirtirken IP kısmı taşıma yolunu bulmayı belirtir. Bu sayede de iki ya da daha fazla bilgisayarın birbirleriyle iletişim kurabilmesine imkân tanır.

[30] Açılımı ***I****nternet* ***P****rotocol Address (İnternet Protokol Adresi) olan Ip adresi, interneti* ya da TCP/IP protokolünü kullanan diğer paket anahtarlamalı ağlara bağlı cihazların, ağ üzerinden birbirleri ile veri alışverişi yapmak için kullandıkları adrestir. İnternete bağlanan her cihaza, internet servis sağlayıcısı tarafından atanarak internetteki diğer cihazların bu cihazlara verilen IP adresleri ile ulaşması sağlanır.

[31] Açılımı Domain Name System (Alan Adı Sistemi) olan DNS, internet uzayını bölümlemeye, bölümleri adlandırmaya ve bölümler arası iletişimi organize etmeye yarayan, bilgisayar, servis, internet veya özel bir ağa bağlı herhangi bir kaynak için hiyerarşik dağıtılmış bir adlandırma sistemidir.

gücünü zorlayan yeni saldırı yöntemlerinin de her an üretilebileceği düşüncesinden hareketle özenle seçilmiş yöntemler üzerinden anlatılmıştır.

Tüm bu anlatılan yöntemlerden siber saldırıların, teröristle mücadelede gerek ihtiyaç duyulan istihbaratın gerekse hedef sistemlerin etkisiz hale getirilmesi amaçlı kullanılabileceği net olarak anlaşılmaktadır. Çünkü siber saldırılar sayesinde doğru hedeften, devamlı olarak isabetli istihbaratın elde edilmesi ve yine doğru hedefin, eş zamanlı olarak ucuz bir maliyetle etkisiz hale getirilmesi büyük olasılıkla mümkün olabilecektir. Bu sonuçla da teröristle mücadelede sert müdahaleleri gerçekleştirmek için ihtiyaç duyulan istihbarat, az bir maliyetle sağlanabilecektir.

4.2.5. Yönlendirilmiş (Yoğunlaştırılmış) Enerji Silahları ve İHA (İnsansız Hava Araçları) Kullanımı

Yönlendirilmiş enerji silahları, çalışmada siber istihbaratın üç ana unsurundan birisini oluşturan siber silahlar içerisinde genel olarak vurgulanmıştır. Bu noktada, yönlendirilmiş enerji silahları kategorisindeki en bilindik silahlardan lazer, mikrodalga, parçacık ışınlı, RF enerji ve yüksek güçlü sonik silahlar kısaca açıklanmıştır. Ancak çalışmanın bu bölümünde, yönlendirilmiş enerji silahlarının teröristle mücadele noktasında, ihtiyaç duyulan siber istihbaratın elde edilmesinde bir yöntem olarak kullanılmasının vurgulanması gerektiği düşünülmüştür. Bu doğrultuda en çok İHA (İnsansız Hava Araçları) aracılığıyla kullanılıyor olmalarından yola çıkarak teröristle mücadelede olası katkıları incelenmeye çalışılmıştır.

Yönlendirilmiş enerji silahları, çeşitli yapılara sahip önemli siber silahlardandır. Her birisinin hedefe yönelirken kullanmış oldukları saldırı biçimleri farklılık göstermektedir. Ancak genellemek gerekirse, hedef üzerindeki olası etkileri benzerlik göstermektedir. Bu etkiler de kendisini daha çok hedef sistemleri tahrip ve imha etme üzerine kuruludur. Dolayısıyla da İHA teknolojisiyle bütünleştirilerek kullanılmaya başlanmaları, gerek hedeflerin teşhis, tespit ve analizi gerekse tahrip ve imhasının kolaylığı bakımından olumlu sonuçlar ortaya çıkarmaktadır.

İHA teknolojisi ise içerisinde insan bulunmayıp genel olarak siber uzaya bağlı sistemler üzerinden, bir uzaktan kumanda aracılığıyla uçurulan veya önceden programlanmış bir plan dâhilinde otomatik hareket ederek uçan araçları tanımlamak için kullanılmaktadır (Ostim Teknik Üniversitesi, 2021). Dolayısıyla silahlı veya silahsız herhangi bir drone, dron savar, uçak, füze, uydu vb. tüm teknolojiler, birer İHA teknolojisi kategorisine girmektedir. Bu teknolojiler amaca uygun olan gerek konvansiyonel ve yönlendirilmiş enerji silahları gerekse video kamera, fotoğraf makinesi, mikrofon, sinyal yakalayıcı, termal ve optik gece görüş

sistemleri, lazer tarama cihazı gibi çeşitli teknolojik ekipmanlarla rahatlıkla donatılabilmektedir. Böylelikle siber uzay sistemleri vasıtasıyla uzaktan uçurularak önemli istihbari bilgilerin elde edilebilmesine ve sıfır zayiatla operasyonların tamamlanmasına imkân sağlamaktadır (Bulut, 2019:37)

Gerek istihbaratın elde edilmesinde işe yarar teknolojiler gerekse konvansiyonel ve yönlendirilmiş enerji silahlarıyla donatılmış İHA'lar, teröristle mücadele noktasında örneklendirildiğinde, olası katkıları daha net anlaşılabilir olabilecektir. Bu doğrultuda uzaktan kontrol edilerek veya programlanarak olası terörist noktalarına yönlendirilen İHA'lar, bölgede istihbari bilgilerin eş zamanlı olarak çok daha kolay elde edilebilmesini sağlayabilecektir. Eş zamanlı elde edilebilen istihbaratın anlık bir değerlendirmeye tabi tutulmasıyla, terör hedeflerinin teşhis ve tespiti yapılabilecektir. Teşhis ve tespit edilen terör hedefleri de eş zamanlı olarak operasyona dönüştürülerek İHA sistemleri üzerinde yer alan gerek konvansiyonel gerekse yönlendirilmiş enerji silahlarıyla anında vurulabilecektir. Bu sonuçla da bir yandan teröristle mücadelede ihtiyaç duyulan doğru ve isabetli bilgi elde edilebilirken bir yandan da tespit edilen terör hedeflerinin eş zamanlı imhası mümkün olabilecektir.

BEŞİNCİ BÖLÜM

VAKA İNCELEMESİ: DAEŞ'E YÖNELİK SİBER İSTİHARAT GAYRETLERİ

Siber istihbarat, terörle mücadele noktasında ihtiyaç duyulan doğru ve isabetli bilgiyi eşzamanlı ve devamlılık ekseninde elde edebilme fırsat ve gayretleriyle terörist yapıların marjinalleştirmesinde önemli bir rol oynamaya çalışmaktadır. Bu doğrultuda teröristle mücadeleyi maliyet etkin bir yapıda, sert mücadeleye katkı sağlayacak bir duruma dönüştürerek ulaşılması gereken nihai duruma bir adım daha yaklaştırmaktadır. Dolayısıyla bu sonuçları ortaya koyabilmek anlamında, farklı devletlerin ortak bir tehdit unsuru olarak gördükleri DAEŞ'e yönelik siber istihbarat gayretlerinin incelenmesinin faydalı olacağı düşünülmektedir. Bu çerçevede de açık kaynaklardan elde edilen DAEŞ'e yönelik siber istihbarat çabaları, olağan ve olası sonuçları üzerinden aktarılmaya çalışılacaktır. Ancak DAEŞ'e yönelik siber istihbarat çabalarının olağan ve olası sonuçlarının iyi değerlendirilebilmesi için öncelikli olarak DAEŞ'in kısaca incelenmesi, amaç ve hedefleri ile tehdit boyutunun anlaşılabilmesi gerekmektedir. Bu doğrultuda da ilk olarak DAEŞ'in örgütsel anlamdaki geçmişi, amaç ve hedefleri ile ortaya koyduğu tehdit durumu kısaca vurgulanmalıdır. Devamında DAEŞ'le mücadeleye yönelik olası ve olağan siber istihbarat örneklerine değinilerek tespit edilen parametreler üzerinden vakanın analizi yapılmaya çalışılacaktır.

5.1. DAEŞ'in Örgütsel Anlamdaki Geçmişi

DAEŞ'in örgütsel alamdaki geçmişi, El-Kaide temellerine dayanan bir süreç olarak karşımıza çıkmaktadır. Bu bağlamda ilk olarak, ABD'nin Irak'ı işgal etme olasılığı üzerine, El-Kaide üyesi olan Ürdünlü Ebu Asım El-Makdisi'nin öğrencisi Ebu Mus'ab ez-Zerkavi, Irak'a gelmiş ve burada ''Tevhit ve Cihat'' isimli bir oluşumu kurmuştur (Ünsal ve Olçar, 2015:14). Ekim 2004 yılına geldiğinde bu oluşum, El-Kaide'ye biat etmiş ve ''İki Nehir Arasındaki El-Kaide'' (Tanzimul Kaide Fi Biladi'r-Rafideyn) olarak anılmaya başlanmıştır (Şen, 2015:83). Adeta El-Kaide'nin Irak'taki uzantısı haline dönüşen örgüt, 2006 yılında grup lideri Zerkavi'nin ABD tarafından yapılan hava saldırısında öldürülmesiyle yeni bir sürece girmiştir (Karakaya, 2019:12). Bu süreçte Zerkavi'nin ölümüyle grup liderliğini Ebu Ömer El-Bağdadi sürdürmüş ve Mücahitler Şura Konseyi (Meclis Şura El-Mücahidin fi al-Irak), Fatihler Ordusu (Ceyş El-Fatihin) ve Sahabelerin Askerleri (Cund El-Sahaba) gibi El-Kaide çizgisine yakın olan birçok Iraklı grubu kendi bünyesinde birleştirmiştir (Ulutaş ve Hoca, 2014:20). Birleşen bu gruplar, Ekim 2016 tarihine gelindiğinde, kendilerini Irak İslam Devleti (IİD) olarak

adlandırmışlardır. Yayınlanan bir deklarasyon sonucunda Irak'ı işgal eden ABD ve beraberindeki Koalisyon güçlerine yönelik silahlı mücadeleyi başlattıklarını duyurmuşlardır. ABD ise 2007 yılında ''Yeni Bush Doktrini'' kapsamında Irak'ta bulunan askeri gücünü artırmış ve IİD'ye karşı olan tüm grupları destekleyerek karşı mücadele başlatmıştır. Bu kapsamda, Nisan 2010 tarihinde Ebu Ömer El-Bağdadi'yi yapmış oldukları bir baskın sonucunda öldürmeyi başarmışlardır (Polat, 2016:214). Ancak örgüt tamamen ortadan kaldırılamadığı için kısa bir süre sonra Ebu Bekir El-Bağdadi örgütün yeni lideri seçilmiştir.

Aralık 2011'e gelindiğinde, ABD'nin Irak'ta bulunan askeri kuvvetlerini geri çekmesi, bölgede büyük bir güç boşluğuna neden olmuştur. Ortaya çıkan boşluk, aşırılık yanlısı gruplara hareket alanı sağlamıştır. Irak hükümeti ise bu durumu kontrol altında tutmak için Sünnilere yönelik baskısını artırmıştır. Ancak artan bu baskılar, bölgede bulunan birçok radikal Sünni grubu IİD'ye daha da yakınlaştırmıştır (Gürler ve Özdemir, 2014:7). Bu yakınlaşmayla bölgede büyük bir sempati kazanan IİD, Suriye krizinin de patlak vermesiyle müthiş bir ivme yakalayarak büyümüştür. Zamanla da hem militan sayısını hem de eylemlerini artırmıştır. Nisan 2013'e gelindiğinde de Suriye'yi de içerisine alacak şekilde büyümüş ve yayınlamış olduğu bir bildiriyle kendisini Irak ve Şam İslam Devleti (IŞİD) olarak adlandırmıştır (Ulutaş ve Hoca, 2014:21).

Zevahiri liderliğindeki El-Kaide terör örgütü ise kendisine bağlı bir yapılanma içerisinde olan IİD örgütünün, bu faaliyetlerinden son derece rahatsızlık duymuştur. Bu çerçevede IŞİD'in ilanının iptalini isteyen Zevahiri, Bağdadi'nin bu adımından vazgeçmemesi üzerine ''El-Kaide'nin IŞİD'le olan tüm bağını kopardığını ve hiçbir suretle herhangi bir bağlantısının bulunmayacağını'' açıklamıştır (Miş ve Özdemir, 2014:212). Ancak IŞİD bunu dikkate almayarak genişleme stratejisini uygulamaya devam etmiştir. Son derece etkin bir 'Selefi İslam Devleti' kurabilmek için de başta Şia ve Hristiyanlığa karşı olmak üzere, kendisine biat etmeyen tüm otoritelerden laik ve demokratik topluluklara kadar savaşma anlayışı içerisinde hareket etmiştir. Böylelikle farklı milletlerden çok sayıda militanı bünyesine katarak küresel anlamda adından söz ettiren, aynı zamanda tüm dünyayı tehdit eden radikal Sünni bir yapıya dönüşmüştür.

Yaptığı eylem ve saldırılarla bölgede ilk olarak Suriyeli Muhalifleri baskı altına almaya çalışmıştır. Esad rejiminin Suriye'nin kuzey bölgelerinden çekilmesiyle de ortaya çıkan boşluğu doldurmuş ve rejimden kalan silahları ele geçirmiştir. 10 Haziran 2014'e gelindiğinde, Irak güçlerini yenerek Musul kentini tamamen ele geçirmiştir. 11 Haziran'da da Türkiye'nin

Musul Konsolosluğuna saldırarak 49 görevliyi rehin almıştır. Alınan rehineler ise 20 Eylül'de Türkiye tarafından düzenlenen operasyon sonucunda kurtarılmıştır. Ancak yine de IŞİD'in ilerlemesi durdurulamamıştır. Kısa süre içinde Irak Kürdistan Bölgesel Yönetimi ve başkenti Erbil düşme noktasına gelmiştir. Bağdat'ın da tehlikeye girmesiyle mevcut durum çok daha tehlikeli boyutlara ulaşmıştır. Bu noktada, ABD ve Batılı Ülkeler bir araya gelerek IŞİD'e karşı mücadeleye girişmiştir. Zamanla da kayda değer başarılı sonuçlar elde edilerek IŞİD'in ilerlemesi durdurulmuş ve ele geçirmiş olduğu birçok bölge kurtarılmıştır.

Bu ilerlemesiyle 2014 yılının sonlarına doğru 89,000 kilometrekarelik bir bölgeyi kontrolü altına almış olan IŞİD, 2015 yılının Nisan ayına kadar kontrol alanını 138,000 kilometrekareye çıkarmayı başarmıştır (Sönmez, 2018:4). Ortaya çıkan bu yüz ölçümüyle, bugünkü Avusturya, Hırvatistan, Belçika, Danimarka ve İsrail'de dâhil olmak üzere birçok ülkenin yüzölçümünden daha fazla alanı hâkimiyeti altına almıştır. Süreç içerisinde elde etmiş olduğu veya elde edebilme fırsatının bulunduğu konvansiyonel, kimyasal ve nükleer gibi kitle imha silahlarını kullanma ya da kullanabilme potansiyeliyle de küresel bir tehdit saçmıştır. Ancak yavaş yavaş toprak kaybetmeye başlamasıyla birlikte Musul ve Rakka'nın elinden çıkması, sahadaki alan kontrolünü zayıflatmıştır. Bu nedenle de gücünün doruğundayken kullanmış olduğu terör, direniş, ayaklanma, gerilla ve hibrit savaş gibi teknik ve taktiklerini, küresel olarak ulaşabildiği her bölgede uygulamaya çalışmıştır.

Yapmış olduğu kanlı eylemlerin giderek artmasıyla uluslararası arenada İslam'la terörün ayırt edilmesi tartışmaları ortaya çıkmıştır. Bu çerçevede ilk olarak, Eylül 2014 tarihlerinde Fransa Dışişleri Bakanı Laurent Fabius ve Türkiye Cumhurbaşkanı Recep Tayyip Erdoğan'ın, İslam ve terörün ayrımına yönelik ifadeleri dikkate alınmıştır. Bu açıklamalar sonrasında da uluslararası arenada IŞİD yerine DEAŞ veya DAEŞ (Devletü'l-Irak ve'ş-Şam (Irak ve Şam Devleti)) terimi kullanılmaya özen gösterilmiştir (Hürriyet Haber, 10 Kasım 2014).

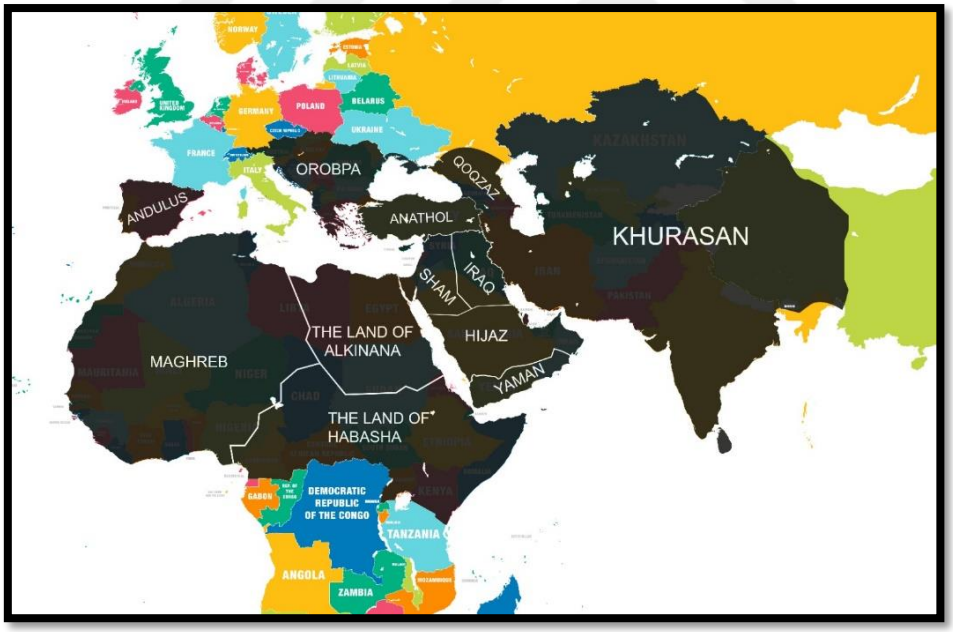
5.2. DAEŞ'in Amaç ve Hedefleri ile Ortaya Koyduğu Tehdit Boyutu

DAEŞ terör örgütünün örgütsel anlamdaki geçmişini incelerken üç temel ideoloji etrafında bütünleştiği görülmektedir. Bu ideolojilerin ilkinde, İslam Halifeliğinin yeniden kurulmasını sağlama ve bunun için gerekli olan tüm çalışmaları yapma fikri yatmaktadır. İkincisinde ise tekfircilik[1] ve Şiilerle mücadele etme anlayışı hâkimdir. Üçüncü olarak ise cihat etme ve bunu düşman olarak gördükleri tüm toplumlara karşı uygulamaya koyma düşüncesi

[1] İslam hukukuna göre bir Müslümanın başka bir Müslümanı kâfir ilan etmesidir.

bulunmaktadır. Bu üç ideolojisine istinaden de Sünni İslam Halifeliğini yeniden tesis ederek hâkimiyet alanlarında şeriat ile hüküm sürmeyi amaçlamışlardır. Bu amaç doğrultusunda şiddeti araçsallaştırarak mevcut rejimlerin yıkılmasını ve yerine bir hilafet devleti kurulmasını kendilerine ilham kaynağı olarak almışlardır.

Tüm bu anlatılanlardan DAEŞ Terör örgütünün, en temel ilham kaynağının 'Küresel Sünni İslam Halifeliğini' yeniden tesis etmek ve bunu kalıcı hale getirerek genişlemek için birçok eylem gerçekleştirmek olduğu anlaşılmaktadır. Bu eylemleriyle de kısa vadede Irak ve Suriye'deki kazanımlarını savunarak kalıcı olmayı, orta vadede Irak ve Suriye'deki durumunu sağlamlaştırarak genişleme hedefini sürdürmeyi, uzun vadede ise Sünni ülkelere doğru genişleyerek tüm dünyaya cihat anlayışıyla saldırmayı amaçladıkları bilinmektedir (Karakaya, 2019:23). Bu sonuçla da DAEŞ'in yayınlarından olan Dabiq dergisinde ''The Return of Khalifah'' (Hilafetin dönüşümü) başlığıyla yayınlanan Şekil 2'de belirtilmiş sözde halifelik haritasındaki sınırlara ulaşma arzusuyla hareket ettikleri gözlemlenmektedir.



Şekil 2. DAEŞ'in Sözde Halifelik Haritası

Kaynak: Yeşiltaş, 2015:66.

Şekil 2'de belirtilen bu harita, DAEŞ'in amaç ve hedeflerinin dikkate alınmasıyla birlikte incelendiğinde, DAEŞ Terör örgütünün küresel ölçekte, ne denli büyük bir tehdit unsuru oluşturduğunu ortaya koymaktadır. Bu tehdidin boyutuna, DAEŞ'in sahip olduğu üstün silah

gücü ile farklı milletlerden oluşan insan çeşitliliğinin eklenmesiyle de küresel ölçekli riskler daha da artmaktadır. Özellikle Irak ve Suriye'de askeri tesis ve üstlerden ele geçirdiği konvansiyonel ve kimyasal silah kapasitesi, başta bölge coğrafyası olmak üzere tüm Batı toplumlarında korku ve endişe yaratmaktadır. Ortaya çıkan bu korku ve endişelerin iyi anlaşılabilmesi içinde DAEŞ'in önceden gerçekleştirmiş olduğu küresel ölçekli eylemlerin akıllara getirilmesinde fayda vardır.

DAEŞ Terör örgütü küresel ölçekte Türkiye'de 10'u canlı bomba, 1'i bombalı saldırı ve 3'ü silahlı saldırı olmak üzere toplam 14 kanlı terör saldırısı gerçekleştirmiştir. Gerçekleştirilen saldırılarda ise 10'u polis ve 1'i asker olmak üzere toplam 304 kişi hayatını kaybetmiş, 62'si polis ve 7'si asker olmak üzere toplam 1338 kişide yaralanmıştır (Uludağ, 2017). Fransa'nın Paris kentinin birinci, onuncu ve on birinci bölgeleriyle Fransa Stadyumunda ise eş zamanlı olarak yapılan silahlı ve bombalı saldırılarda en az 153 kişi hayatını kaybetmiş ve çok sayıda kişi ise yaralanmıştır (Hürriyet, 2021). Yine yakın dönemlerde Fransa'da 20, ABD'de 16, Almanya'da 12, Avustralya'da 10, İngiltere'de 8 ve Ürdün'de 8 olmak üzere toplam 74 terör saldırısının gerçekleştirilmiş olduğu, yaklaşık olarak 2100 kişinin hayatını kaybettiği kayıtlara geçmiştir (Orton, 2017:6). Bu saldırılarında DAEŞ merkezi ile bağlantısı bulunan gizli hücreler aracılığıyla yapıldığı anlaşılmıştır (Karakaya, 2019:39).

Tüm bu saldırılar detaylı olarak incelendiğinde, insanların toplu halde bulundukları konser, tiyatro, düğün, eğlence, spor müsabakaları, havalimanları, sahil kenarları, turizm alanları vb. yerlerin seçildiği gözlenmektedir. Bu minvalde de DAEŞ'in bazı özellikleri, nedenleri ve sonuçları ile alakalı detaylar ve saptamalar öne çıkarılabilmektedir. Bunlardan; ilki, DAEŞ'in Suriye, Irak ve Ortadoğu ülkeleri dışındaki diğer Batı ülkelerine mensup kişileri de eylemlerinde militan olarak kullandığı; ikincisi, dünyanın hemen hemen her bölgesine uyuyan hücre yerleştirerek olası bir eyleme hazır oldukları; üçüncüsü, DAEŞ'in gerek Ortadoğu gerekse Batı ülkelerindeki eylem tiplerinin silahlı saldırı, intihar saldırısı, canlı bomba vb. şeklinde yoğunlaştığı; dördüncüsü, DAEŞ'in ideolojisine uygun olarak sivil, asker, kadın, çocuk, masum demeden herkese karşı vahşi saldırılarda bulunduğu; son olarak da DAEŞ'in yapmış olduğu saldırıların özellikle batı coğrafyasında İslam karşıtı ideolojiyi tetikleyerek ırkçılığı körüklediğidir (Alkan, 2016:193-194). Bu sonuçlar, küresel ölçekte değerlendirildiğinde ayrışmaları tetikleyerek insanları kutuplaştırmakta ve de belirsizlik yaratarak korku, panik, endişe ve kaos ortamını yaygınlaştırmaktadır. Devamında terör örgütlerinin en sevdiği ortamı yaratarak toplumları kargaşaya sürüklemekte ve toplumsal birlik, beraberlik, bütünlük gibi değerlere zarar vermektedir.

Bir toplumda toplumsal birlik, beraberlik ve bütünlüğün bozulması, terör örgütleri için en çok tercih edilen durumlardan birisidir. Çünkü birlik, beraberlik ve bütünlüğü bozulan toplumlar militan kazanma, toplumun yanlış yönlendirilmesi, yeni hücrelerin konumlandırılması gibi durumlarda terör örgütlerine kayda değer fırsatlar yaratmaktadır. Bu fırsatları vermemek içinde terörle mücadeleye yönelik tüm imkânların seferber edilerek küresel ölçekli bir mücadele yönteminin belirlenmesi gerekmektedir. Bu mücadele başarıldığı takdirde de terörle mücadelede kayda değer sonuçlar alınarak terörist yapıların marjinalleştirmesinde arzulanan noktalara ulaşılacaktır.

5.3. DAEŞ'le Mücadeleye yönelik Olası ve Olağan Siber İstihbarat Örnekleri

DAEŞ'le mücadelede, kayda değer sonuçların alınmasına yönelik yapılan siber istihbarat faaliyetleri incelendiğinde, örgütün marjinalleştirmesine yönelik olası katkılarını daha net görmek mümkün olabilmektedir. Bu vesileyle de siber istihbarat gayretlerinin teröristle mücadelede doğru, isabetli ve devamlılık parametreleri ölçüsünde, maliyet etkin bir yapıda, sert mücadele yöntemlerini mümkün kılacak istihbaratı elde etmedeki katkısı incelenebilecektir. Ancak çoğu siber istihbarat faaliyetlerinin gizli yapılıyor oluşu, olağan siber istihbarat faaliyetlerinden çok, olası siber istihbarat faaliyetlerine değinilmesini zorunlu kılmaktadır. Bu nedenle de çalışmada, ulaşılmak istenen sonuçlara yönelik DAEŞ terör örgütünün geçerlilik testi, açık kaynaklar üzerinden elde edilen örneklerle tartışılmaya çalışılacaktır.

5.3.1. DAEŞ Mensuplarına Yönelik Siber Bal Tuzağı

Devletlerin ya da istihbarat servislerinin hedefi haline gelen kişiler için çok sayıda harekât tarzları gözden geçirilmektedir. Bu harekât tarzlarının da işleyiş mantığına göre en zararsızı, sıcak savaşa tutuşmadan ve herhangi bir saldırıya maruz kalmadan hedef kişinin ikna edilmesidir. Ancak hedef kişiyi ikna edebilmek sanıldığı kadar kolay bir durumda değildir. Çünkü insanlar bulundukları ülkelerde, kendilerini güvende hissederek gerek ailevi gerekse çevresel faktörler sebebiyle rutinlerinin dışına kolay kolay çıkmamaktadır. Çevresel ve ailevi faktörler sebebiyle insanların rutininin dışına çıkamaması, etraflarında otomatik bir kontrol mekanizmasını oluşturarak daha temkinli olmalarını sağlamaktadır. Dolayısıyla da hedef kişilerin ikna edilebilmesi için çevrelerinden uzaklaştırılması veya yalnızlaştırılmaları büyük önem taşımaktadır (Şahin, 2021).

Çevresinden ve ailesinden uzaklaşan insanlar, yüksek stres altına girerek yalnız oldukları hissiyatına kapılmaktadır. Bu nedenle de er ya da geç güvenebilecekleri bir karşı

cinsin dostluğuna ve cinselliğine ihtiyaç duyacaklardır. Bu noktada da ihtiyaç duyulan boşluk, siber bal tuzağı yöntemiyle kolayca doldurularak minimum risk, tehlike ve maliyetle hedef üzerinden amaca yönelik istihbaratı toplamak imkân dâhilinde olacaktır.

Örnek olması açısından Mia Ash adlı bir hacker grubu incelendiğinde, sahte bir sanal kadın karakteri yaratarak oluşturdukları profille, birçok firmanın bilgisayar sistemlerine sızmayı başardıkları görülmektedir. Başarının arkasındaki faktörler incelendiğinde ise öncelikli olarak oluşturulan karakterin gerek görsel gerekse karakteristik anlamda güçlü bir yapıya sahip olduğu tespit edilmektedir. Çünkü oluşturulan bu sanal profilde Mia Ash, 30 yaşında olup 2 sanat okulu bitirmiş, başarılı bir fotoğrafçı ve oldukça güzel bir kadındır. Dahası ise birçok Amerikan güvenlik firmasına göre, şimdiye kadar oluşturulmuş en iyi sosyal medya profilidir. Bu sayede de başta ABD olmak üzere İsrail, Irak, Suudi Arabistan ve İran gibi teknoloji şirketleri çalışanlarını hedef alarak etki altına aldıkları bilinmektedir. Çalışanların etki altına alınarak yönlendirilmesiyle, güvenlik sistemlerine sızdıkları ve sistemlerde bulunan tüm verileri ele geçirdikleri açıktır (NTV, 2017).

Siber savaşçıların sıklıkla başvurduğu bu yönteme dair açık kaynaklardan binlerce örneğe rastlanmaktadır. Ancak DAEŞ'le mücadelede ihtiyaç duyulan istihbaratın elde edilmesi faaliyetleri, gizli yürütüldüğünden konumuza yönelik bir örneğe rastlamak oldukça güçtür. Olası sonuçları anlamlandırmak adına verilen örneğin, herhangi bir DAEŞ örgütü üyesine karşı yapıldığını göz önüne aldığımızda, sağlayacağı katkıyı anlamak mümkündür. Bu nedenle siber bal tuzağına yönelik gerek yukarıda verilen örneği gerekse dördüncü bölümde vurgulanan yöntemi DAEŞ'le mücadeleye yönelik istihbaratın elde edilmesi ekseninde değerlendirmek akılcı olacaktır.

Sonuç olarak teröristler, geneli itibariyle büyüdükleri çevre ve ailelerinden uzaklaşmış, yüksek stres altında ve yalnız olan insanlardır. Doğal olarak da her daim güvenebilecekleri bir karşı cinsin dostluğuna ve cinselliğine eğilim göstermektedirler. Bu eğilimde onları siber bal tuzağı yönteminde potansiyel birer hedefe dönüştürmektedir. İsabetli bir hedefe gidilerek hedefin avuç içine alınması başarıldığında, az bir maliyetle sert mücadeleyi etkin kılabilecek doğru istihbari bilgiye, kaynağından erişilebilecektir. Dahası ise hedefe ait sistemlere gizlice kötücül ve casus yazılımlar yerleştirilmesiyle, ihtiyaç duyulan istihbaratın devamlılık ekseninde sürdürülebilirliği, fark edilmediği süreç içerisinde yapılabilecektir. Böylece DAEŞ'e yönelik yeni hedefler tespit edilerek mücadeleye yönelik uygun taktik ve stratejiler belirlenebilecektir.

5.3.2. DAEŞ Hedeflerine Yönelik OSINT (Açık Kaynak İstihbaratı)

OSINT kelimesi; Türkçede karşılığı ‘‘açık kaynak istihbaratı’’ anlamına gelen, İngilizce ‘open source intelligence’ kelimesinin kısaltılmasından türetilmiştir (Prisma, 2021). Dolayısıyla kelime anlamından anlaşılacağı gibi istihbarat faaliyetlerinin açık kaynaklardan gerçekleştirildiği bir yöntemi akıllara getirmektedir. Peki, bu açık kaynaklar günümüzde nelerdir diye düşünüldüğünde ise kitap, dergi, makale, rapor, resim, müzik, video, ses kaydı, sanat eseri, afiş, radyo, televizyon ve internet sitesi gibi herkesçe ulaşılan kaynakların akla geldiği bilinmektedir. Ancak gelişen teknolojiyle birlikte tüm bu kaynakların o veya bu sebepten siber uzayla bütünleşmesi ve internet aracılığıyla tüm bu kaynaklara kolayca ulaşılması, açık kaynak algısında interneti ilk sıraya yerleştirmiştir. Çünkü internet, akla gelebilecek her türlü açık kaynak bilgisini zaman içerinde bünyesine dâhil etmiş ve bu sayede de açık kaynak tabirinin ana öznesi haline gelmiştir. En nihayetinde de açık kaynak istihbaratı, internet ortamında yayımlanan verilerden ya da bilgilerden ihtiyaç duyulan istihbaratın toplanmaya çalışıldığı bir yönteme dönüşmüştür.

Örneğin, DAEŞ terör örgütünü övücü nitelikte yayınlar yapan bir internet sitesi ele alındığında, bu sitenin öncelikli olarak internet üzerinden (yani Goole, Bing, Yandex, DuckDuckGo vb. arama motorlarından) çeşitli kelimeler aracılığıyla aramalar yapılarak tespit edilmesi mümkün olabilmektedir. İkinci olarak, tespit edilen sitenin DNS kayıtları ve IP adresleri, yine internet üzerinde yer alan siteler aracılığıyla sorgulanarak alan adlarına ait kayıt defterleri ve hizmet aldıkları hosting[2] bilgileri öğrenilebilmektedir. Üçüncü olarak ise öğrenilen bu bilgiler üzerinden gerekli yasal prosedürler izlenerek hosting hizmeti sunan şirketle irtibata geçilip, sitenin internette barınması hizmetini alan kişinin iletişim, ödeme ve veri yükleme anına ilişkin bilgileri alınabilmektedir. Dahası ise bu bilgilerin yanında siteye erişim sağlayan yani girerek içerisinde yer alan bilgileri okuyan, indiren, iletişim kuran vb. tüm profil listesinin dahi bilgilerini almak mümkün olabilmektedir. Dördüncü olarak da elde edilen tüm bu bilgilerden gerçek kişi listesinin tespit edilerek gerek DAEŞ terör örgütü propagandası yapan kişilerin gerekse etkilenerek sempatizan kategorisinde bulunabilen kişilerin tespiti yapılabilmektedir. Bu sayede de bir yandan hem örgütün hamiliğini yapan kişilerin hem de örgüt sempatizanlarının yakalanarak yargılanması, diğer bir yandan da olası yeni örgüt üyesi olabilecek kişilerin tespit edilerek önceden önlenmesi sağlanabilecektir.

[2] Türkçede barındırma anlamına gelmekte olup, her hangi bir internet sitesinin yayınlamak istediği verilerinin internet kullanıcıları tarafından erişilebilir olması için bir büyük çaplı bilgisayarlarda tutulmasını sağlayan hizmetlerdir. Bir nevi internette yer sağlama hizmeti olarak da anlaşılabilir.

Tam da bu noktada olağan örneklere bakıldığında, internetin açık kaynaklarından yapılan araştırmalarla, 25 Temmuz 2015 ile 13 Ağustos 2015 tarihleri arasında 100'ü aşkın terör örgütlerini övücü nitelikte yayın yapan internet sitesinin tespit edilerek yasaklandığı bilgisi görülmektedir (Boyacıoğlu, 2015). Yine Eskişehir İl Jandarma Komutanlığınca 01 Temmuz 2021 ile 10 Ağustos 2021 tarihleri arasında internetin açık kaynaklarında yapılan araştırmalarda, yurt dışından terör örgütlerini övücü nitelikte yayın yapan 2 internet sitesinin tespit edilerek erişime engellendiği, site sahiplerinin tespitine yönelik yapılan çalışmalarda, yurt dışında ikamet eden 2 yönetici şahsın tespit edilerek haklarında yasal işlem başlatıldığı bilgisi görülmektedir (Eskişehir İl Jandarma Komutanlığı, 2021). Konuya ilişkin internette benzeri aramalar yapıldığında da benzeri birçok haberin bulunduğu görülebilecektir. Dolayısıyla örgüt üyelerince gerek propaganda gerekse eleman temini ve iletişim anlamında kullanılan internetin, yapılan açık kaynak istihbaratıyla örgüt üyelerinin ve sempatizanlarının tespit edilebilmesinde büyük katkılar sunabileceği söylenebilmektedir.

Bir başka örnek olması açısından DAEŞ terör örgütü üyelerine yönelik internettin açık kaynakları içerisinde yer alan resim, video, ses kaydı, metin gibi veriler incelendiğinde, elde edilebilecek istihbari bilgilere yönelik olası sonuçları vurgulamak mantıklı olabilmektedir. Bu doğrultuda ilk olarak örgüt üyelerine ait eğitim, eylem vb. resim ve videoların incelenerek gerek göz gerekse yüz biyometrilerinden kimlik bilgilerinin tespiti, kritik arazi arızalarından muhtemel sığınak, barınak, mağara, hücre evi gibi saklanma alanlarının bulunabileceği yerlerin analizi yapılabilecektir. İkinci olarak ise ses kayıtlarından yine ses biyometrisi analiziyle örgüt üyelerine yönelik kimlik tespiti çalışmaları yürütülebilecektir. Üçüncü olarak da metin, yazışma, haber vb. veriler üzerinde ayrıntılı incelemelerde bulunularak olası şifreli konuşmalar açığa çıkarılabilecektir. Dahası ise sonuca yönelik akla gelebilecek hemen hemen her türlü akılcı çalışmalarda bulunularak DAEŞ hedeflerinin tespit ve teşhisi sağlanabilecektir. Bu sayede de DAEŞ'le mücadeleye yönelik akla gelebilecek her türlü araştırma, inceleme ve analiz çalışmalarında bulunularak ihtiyaç duyulan istihbarata kolayca ulaşılabilecektir.

Sonuç olarak, teröristler gerek iletişim gerekse propaganda anlamında internette görünür olmayı tercih etmekte ve internetin sağladığı tüm imkânlardan da faydalanmaya çalışmaktadır. Bu noktada yapılması gerekenler sırasıyla, DAEŞ'e yönelik hemen hemen her türlü veriyi tespit etmek, tespit edilen veriler üzerinde gerekli inceleme ve analizler yaparak çıkarımlarda bulunmak, bu çıkarımlardan da akla gelebilecek her türlü akılcı yöntemle DAEŞ hedeflerinin tespit ve teşhis edilmesini sağlamaktır. Süreç başarıyla yürütüldüğü takdirde, tespit

ve teşhis edilen hedeflerin gerek duyulan ölçüde müdahalelerle, mücadele anlamında nihai maksada matuf sonuçlara katkıda bulunacağı gözlemlenebilecektir.

5.3.3. DAEŞ Mensuplarına Yönelik SOCMINT (Sosyal Medya İstihbaratı)

Günümüzde sosyal medya katılım, açıklık, sohbet, toplum ve bağlantılılık gibi özellikleri bünyesinde barındıran yeni bir çevrimiçi medya aracı olarak karşımıza çıkmaktadır (Taşdemir, 2017:8). Bu özellikleri sebebiyle, geleneksel medya araçlarından farklı olarak kullanıcılarını merkeze koyan, hızlı ve kolay tepki vermeyi sağlayan, organize olmanın kolay olduğu bir alanı oluşturmuşlardır. Bu sayede de birçok içeriğin tek bir platform üzerinden büyük kitlelere anında iletilmesini sağlayan ve kitlelerin duygu, düşünce, davranış biçimi gibi tepkilerini etkileyebilen önemli bir araç olmuşlardır.

Sosyal medya platformlarının sahip olduğu tüm bu özellikler, terör örgütleri tarafından ilgiyle karşılanmıştır. Öyle ki hemen hemen tüm terörist gruplar, sosyal medyayı faaliyetlerinde ideal bir mekân yapmışlardır. Kolay erişim, gizlilik, hızlı bilgi akışı, eğitim, multimedya ortamı, ucuz ve basit oluşu, düzenleme, sansür veya denetimin olmayışı, dünya geneline yayılmış büyük kitlesel yapısı gibi nedenlerde, örgüt üyelerine en önemli gerekçeler olmuştur (Weimann, 2017:3). Bu vesileyle de terör örgütleri, sosyal medyadan tanıtım, propaganda, psikolojik savaş, veri madenciliği, bağış, istihdam, seferberlik, bilgi paylaşımı, planlama ve koordinasyon gibi faaliyetlerini çevrimiçi gerçekleştirebilme imkânına kavuşmuşlardır (Taşdemir, 2017:9).

DAEŞ'in sosyal medya kullanımı incelendiğinde ise hem resmi hem de gayri resmi birçok profil ve grup sayfaları kullandıkları görülmektedir. Sosyal medya sayfaları üzerinden analiz yapıldığında, özellikle 'cihat' kelimesini ön plana çıkararak adeta 'cihat sosyal medyası' imajını yaratmaya çalıştıkları anlaşılmaktadır. Bu imaj üzerinden de kendisini pazarlayarak artan dünya nüfusunda savaşçı sayılarını artırmaya ve tüm dünyada taraftar kitlesi oluşturmaya çalıştıkları açıktır. Bu sonuçla da sosyal medya üzerinden topladıkları taraftar kitlesiyle dirsek temasında olarak hücresel yapılanmalara gidebileceklerini, gerekli eğitimleri vererek zamanı geldiğinde, bu hücreleri harekete geçirip eylem yapabileceklerini söylemek mümkündür.

Örnek olması açısından 14 kişinin öldüğü, 21 kişinin yaralandığı San Bernardino saldırısını incelendiğinde, sosyal medyanın dünyadaki aşırılık yanlısı grupları eğitmek ve üye almak açısından muazzam bir ortam sunduğu açıkça gözlemlenebilmektedir. Bu doğrultuda yapılan saldırının detaylarına bakıldığında sosyal medyanın aşırılık yanlısı gruplara sağladığı fonksiyonlar daha net anlaşılabilmektedir. 2 Aralık 2015'de Kaliforniya'daki San Bernardino, Inland Bölge Merkezi'nde bir partide gerçekleştirilen saldırıda: Pakistan uyruklu Seyyid

Rıdwan Faruk ve Taşfin Malik isimli evli çift, ellerine aldıkları silahlarla masum insanları hedef alarak katletmişler; devamında yapılan operasyon sonucunda, vurularak ölü ele geçirilmişlerdir. Saldırganlar hakkında yapılan araştırmalarda, partinin yapıldığı Inland Bölge Merkezi'nde beş yıldır çalıştıkları, çevrede dikkat çekici ve şüphe uyandırıcı bir hal ve hareketlerinin bulunmadığı bilgisi edinilmiştir. Ancak sosyal medya hesaplarında yapılan incelemelerde ise saldırıdan yaklaşık iki gün önce DAEŞ lideri Ebu Bekir El-Bağdadi'ye Facebook'ta bağlılık sözü verdikleri bir mesajı gönderdikleri tespit edilmiştir (Martin, 2017:191). Böylelikle saldırganların sosyal medya üzerinde örgüt üyeleriyle iletişim kurarak saldırıyı gerçekleştirdikleri anlaşılmıştır.

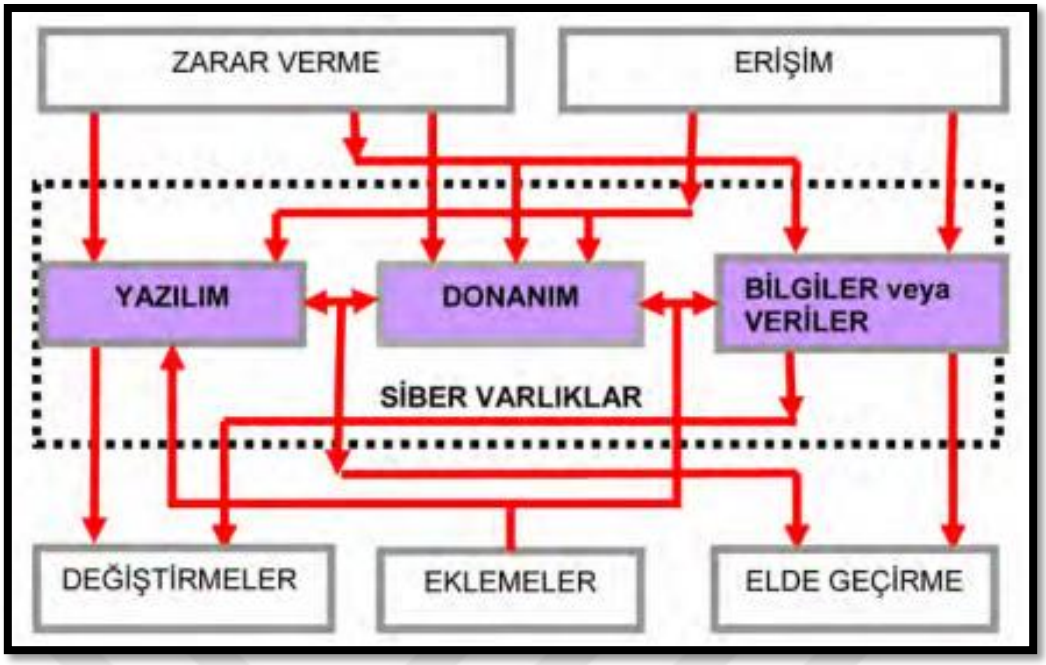
Verilen örnekten de anlaşılacağı üzere, Facebook, Instagram, Twitter, Whatsapp, Youtube vb. sosyal medya platformları, terör örgütlerine gizlenme, eğitim, propaganda, eylem planı, saldırı hazırlığı, eleman temini, uyuyan hücre oluşumu gibi konularda büyük fırsatlar sunmaktadır. Bu fırsatlar sayesinde ise terör örgütlerince, örgüt içi iletişim sağlanarak militan devşirilebilmektedir. Öyle ki Amerikan Brookings Enstitüsünün 2014 yılının son üç ayına yönelik hazırladığı rapor incelendiğinde, terör örgütlerinin sosyal medyadaki etkinlik durumu daha net gözler önüne serilebilmektedir. Raporda 2014 yılının son üç ayında yapılan sayımlarda DAEŞ terör örgütüyle ilişkili 90 bine yakın Twitter hesabının bulunduğu gözlemlenmiştir (T.C. İçişleri Bakanlığı, 2017:24). Bu sayıya, gözden kaçabilecek hesaplar ile 2014'ten günümüze yeni oluşturulabilecek hesapları ve diğer sosyal medya platformlarında bulunabilecek hesapları dâhil ettiğimizde, ortaya büyük bir rakamın çıkacağı aşikârdır. Dolayısıyla, buradan elde edilebilecek her türlü bilginin, teröristle mücadeleye yönelik istihbaratın elde edilmesinde aynı oranda istihbarat servislerine büyük fırsatlar sunacağı göz ardı edilmemelidir.

Konuya ilişkin internetin açık kaynaklarında yapılan araştırmalarda, teröristle mücadele kapsamındaki sosyal medya istihbaratı faaliyetlerinin sonuçlarına yönelik birtakım örneklerle karşılaşılmıştır. Bu kapsamda da Türkiye İçişleri Bakanlığının kamuoyuna yaptığı açıklamalar resmi veriler olduğundan dikkate alınmıştır. İlk olarak 09 Şubat 2021 tarihinde yapılan açıklamaya bakıldığında; 1 ve 7 Şubat 2021 tarihinde, yani bir hafta içerisinde sosyal medya platformlarından terör örgütü propagandası yapan 1264 hesap hakkında inceleme yapıldığı, bu hesaplardan 575'inin DAEŞ terör örgütü güdümünde bulunduğu, yapılan incelemeler sonucunda da terör örgütleriyle ilintili 39 şahsın yakalandığı bilgisi görülmüştür (T.C. İçişleri Bakanlığı, 2021). İkinci olarak 23 Mart 2020 tarihinde yapılan açıklamaya bakıldığında; son bir hafta içerisinde terör örgütü propagandası yaparak halkı kin, nefret, korku ve paniğe sürükleyen 1748 sosyal medya hesabının tespit edildiği, tespit edilen hesaplardan da 316

şüpheli şahsa ulaşıldığı bilgisi görülmüştür (T.C. İçişleri Bakanlığı, 2020). Üçüncü olarak 11 Aralık 2018 tarihinde 5. Uluslararası Siber Suçlar Çalıştayı sonucuna yönelik yapılan açıklamaya bakıldığında; İçişleri Bakanı Süleyman SOYLU'nun internet üzerinden 7/24 esasına göre çalışan sanal devriyeler oluşturdukları, bu sonuçla da 2018 yılı içerisinde "terör örgütü yanlısı siber faaliyet içinde bulundukları tespit edilen 110 bin civarında sosyal medya hesabının takip edilerek 45 bin hesabın kullanıcısının deşifre edildiğini, bunlardan da 7 bin kişinin yakalanarak adli makamlara teslim edildiğini" belirtiği açıklamalarının bulunduğu bilgisi görülmüştür (T.C. içişleri Bakanlığı, 2018). Dördüncü olarak da 31 Aralık 2018 tarihinde, 2018 yılı genelinde yürütülen operasyonel faaliyetlere yönelik yapılan açıklamaya bakıldığında; 1 Ocak – 31 Aralık 2018 tarihleri arasında kırsalda 96.745, şehirde 33.895 olmak üzere 130.640 operasyon yapıldığı, yapılan operasyonlar sonucunda terör örgütlerine yardım ve yataklık eden ve de terör örgütleri ile irtibatlı olduğu değerlendirilen 72.239 şahsın yakalandığı, 107 sözde üst düzey olmak üzere toplam 1746 teröristin etkisiz hale getirildiği, ayrıca çok sayıda silah, mühimmat, gıda vb. muhtelif malzemelerin ele geçirildiği bilgisi görülmüştür (T.C. İçişleri Bakanlığı, 2018). Yapılan açıklamalardan da sosyal medya istihbaratının teröristle mücadelede, büyük kazanımlara sahne olduğu çıkarımında bulunulmuştur.

5.3.4. DAEŞ Hedeflerine Yönelik Siber Saldırı

Siber saldırı yöntemleriyle, siber uzaya bağlı tüm sistemlerin sahip olduğu yazılım, donanım, veri veya bilgi varlıklarına uzaktan erişim sağlanarak; zarar verme, sisteme yeni eklemeler yapma, verileri veya bilgileri kopyalama, silme, değiştirme, çalma, yok etme ve ele geçirme gibi işlemler zaman ve mekândan bağımsız olarak şekil 3'de belirtildiği üzere gerçekleştirilebilmektedir. Dolayısıyla gerçekleştirilebilme ihtimali bulunan bu saldırılar üzerinden teröristle mücadele noktasında da önemli kazanımlar elde edilebileceği değerlendirilmelidir. Bu doğrultuda da ilk olarak, mücadeleye yönelik doğru ve isabetli istihbari bilgiye fark edilmeden eş zamanlı olarak ulaşılabileceği kuvvetle muhtemeldir. İkinci olarak, uzaktan fark edilmeden erişim sağlanarak ele geçirilen istihbari bilgilerin veya bilgilerin bulunduğu sistem ve donanımlara ait yazılımların değiştirilerek gerek İKK gerekse hedeflerin kandırılması ölçüsünde kullanılabileceği açıktır. Son olarak da tüm bu sistemlere ihtiyaç duyulduğunda imha etmek veya çalışmaz hale getirmek maksadıyla zarar verilmesi mümkündür.

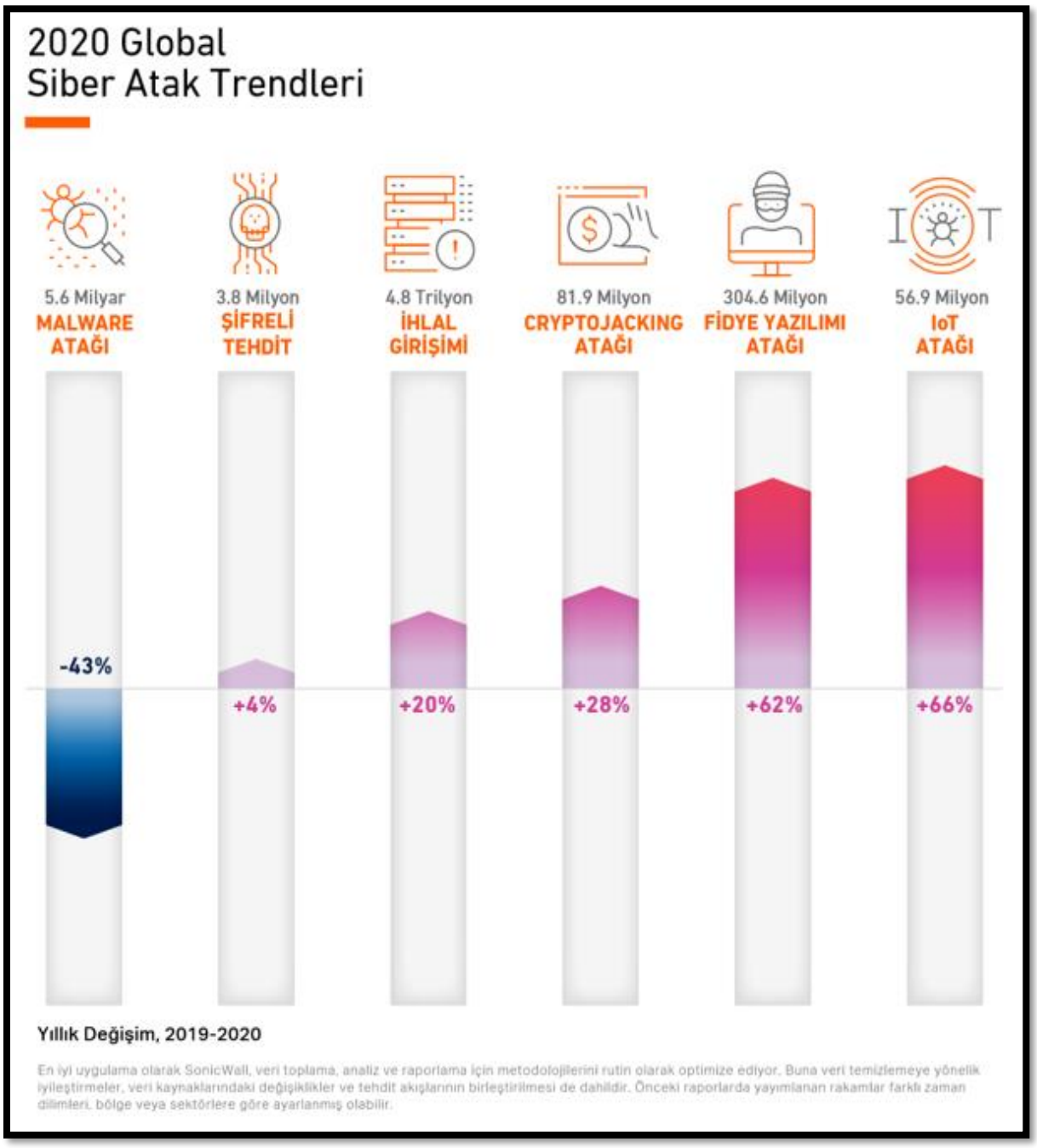


Şekil 3. Siber Uzaya Bağlı Sistemlere Yapılabilecek Saldırılar ve Türleri

Kaynak: Sağıroğlu, 2018:35.

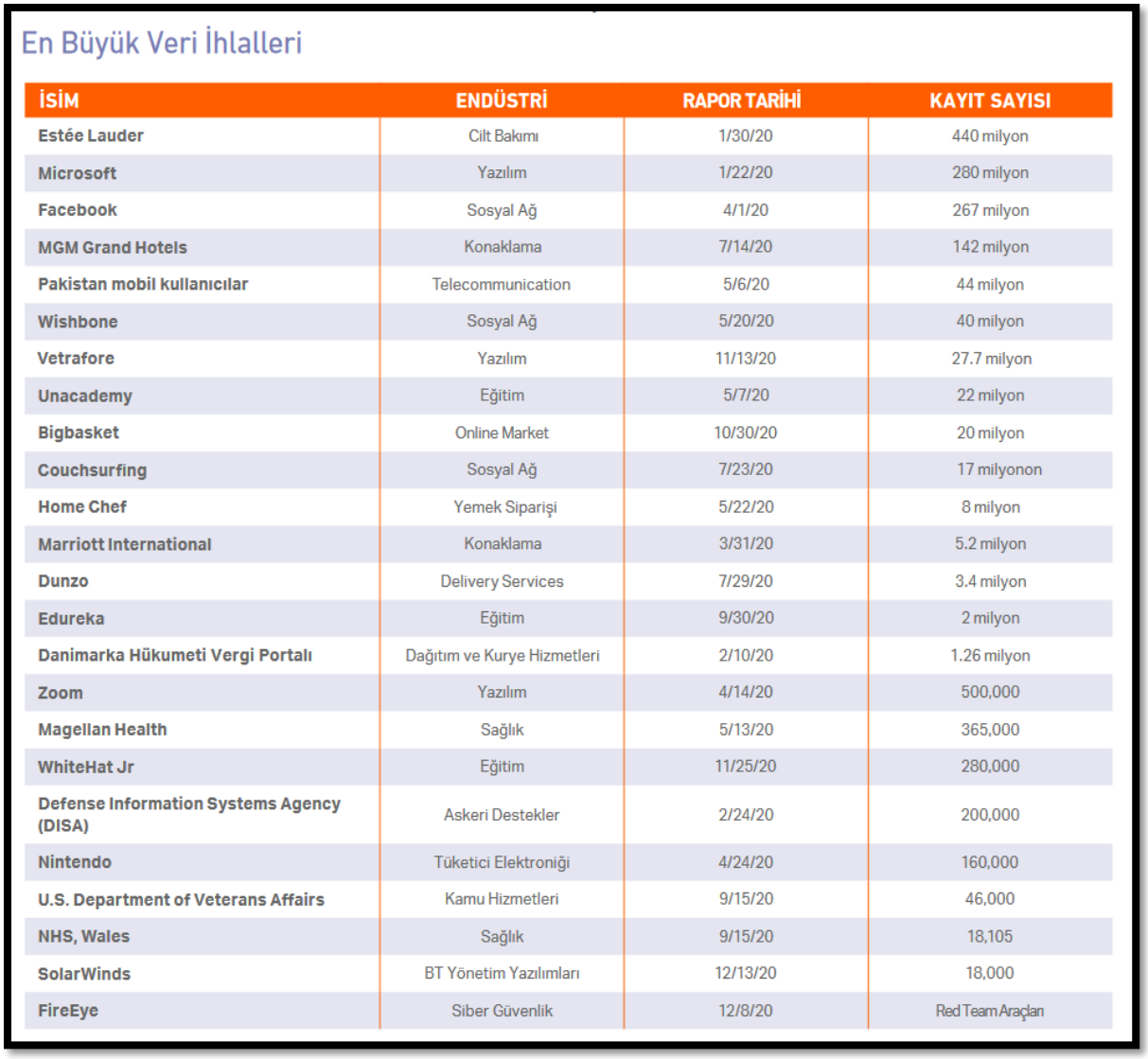
Örnek olması açısından siber saldırılara yönelik yapılan bir takım istatistiki değerlendirilmelere bakıldığında; dünya çapında her gün 30 bin web sitesinin saldırıya uğradığı, her 30 saniyede bir internettin yeni bir yerinde saldırı gerçekleştiği, dünya çapındaki şirketlerin %64'ünün en az bir tür siber saldırı yaşadığı, her gün 300 bin yeni kötü amaçlı yazılım parçası oluşturulduğu, fidye yazılımlarının 2020'de %150 artığı, mobil uygulama mağazalarında günlük ortalama 24 bin kötü amaçlı uygulamanın engellendiği, 24 saatte bir 23 bin DDOS saldırısının yapıldığı gibi çeşitli verilerin olduğu görülmektedir (Affde, 2020). Bu verilerin tespit edilen saldırılar olduğunu dikkate aldığımızda ise olası siber saldırı sayısının tahmin edilemeyecek kadar fazla olduğunu ifade etmek gerekmektedir. Yapılan saldırı yöntemlerine yönelik bilgilere bakıldığında da 2021 yılı içerisinde en çok DDOS, fishing, fidye ve kötü amaçlı yazılım saldırılarının gerçekleştirilmiş olduğu anlaşılmaktadır (Can, 2021). Aynı doğrultuda Sonicwall şirketince 2021 yılında yayımlanan siber tehdit raporuna bakıldığında ise 2020 yılında Şekil 4'de belirtili 5 trilyona yakın siber saldırının kayıtlara geçtiği, bu saldırılar neticesinde de Şekil 5'de belirtili 1,4 milyara yakın verinin güvenliğinin ihlal edildiği bilgisi görülmektedir (Sonicwall, 2021:5-6). Yapılan matematiksel oranlamada bu saldırıların 2019

yılına oranla toplam %137 artığı hesaplanmaktadır. Tüm bu istatistiklerde, siber saldırıların bilgileri ele geçirmede ne denli büyük bir yöntem olduğu gerçeğini göz önüne sermektedir.



Şekil 4. 2020 Yılında Kayıtlara Geçen En Çok Siber Saldırı Türleri ve 2019 Kıyaslaması

Kaynak: (Sonicwall, 2021:5).



En Büyük Veri İhlalleri

İSİM	ENDÜSTRİ	RAPOR TARİHİ	KAYIT SAYISI
Estée Lauder	Cilt Bakımı	1/30/20	440 milyon
Microsoft	Yazılım	1/22/20	280 milyon
Facebook	Sosyal Ağ	4/1/20	267 milyon
MGM Grand Hotels	Konaklama	7/14/20	142 milyon
Pakistan mobil kullanıcılar	Telecommunication	5/6/20	44 milyon
Wishbone	Sosyal Ağ	5/20/20	40 milyon
Vetrafore	Yazılım	11/13/20	27.7 milyon
Unacademy	Eğitim	5/7/20	22 milyon
Bigbasket	Online Market	10/30/20	20 milyon
Couchsurfing	Sosyal Ağ	7/23/20	17 milyonon
Home Chef	Yemek Siparişi	5/22/20	8 milyon
Marriott International	Konaklama	3/31/20	5.2 milyon
Dunzo	Delivery Services	7/29/20	3.4 milyon
Edureka	Eğitim	9/30/20	2 milyon
Danimarka Hükumeti Vergi Portalı	Dağıtım ve Kurye Hizmetleri	2/10/20	1.26 milyon
Zoom	Yazılım	4/14/20	500,000
Magellan Health	Sağlık	5/13/20	365,000
WhiteHat Jr	Eğitim	11/25/20	280,000
Defense Information Systems Agency (DISA)	Askeri Destekler	2/24/20	200,000
Nintendo	Tüketici Elektroniği	4/24/20	160,000
U.S. Department of Veterans Affairs	Kamu Hizmetleri	9/15/20	46,000
NHS, Wales	Sağlık	9/15/20	18,105
SolarWinds	BT Yönetim Yazılımları	12/13/20	18,000
FireEye	Siber Güvenlik	12/8/20	Red Team Araçları

Şekil 5. 2020 Yılında Kayıtlara Geçen Saldırılar Sonucunda En Çok Yaşanan Veri İhlalleri

Kaynak: (Sonicwall, 2021:6).

Tüm bu anlatılanlardan siber saldırıların, teröristle mücadelede ihtiyaç duyulan istihbaratın elde edilmesinde büyük katkılar sunabileceği açık bir gerçekliktir. Ancak teröristle mücadelede, ihtiyaç duyulan istihbaratın elde edilebilmesi için başvurulabilecek siber saldırı yöntem ve örnekleri gizli bilgiler olduğundan kamuoyuyla paylaşılmadığı gözlemlenmektedir. Bu sebepten konunun anlaşılması açısından, siber uzayın dördüncü bölümde belirtilen çok katmanlı yapısıyla, gerek duyulan istihbaratın toplanmasında sanal ortamı oluşturmasını dikkate alıp, siber saldırılarla elde edilmek istenen istihbarata yönelik olası örneklerin zihinlerimizde canlandırmamızın mantıklı olacağı düşünülmüştür. Bu düşünceden hareketle de

konunun anlaşılması açısından internetin açık kaynakları üzerinde yer alan siber saldırılara yönelik bilgilerden örnekler verilerek, DAEŞ'le mücadeleye yönelik olası çıkarımlarda bulunulmaya çalışmıştır.

İnternetin açık kaynakları incelendiğinde, yine Sonicwall'ın 2021 yılı siber tehdit raporunda; 2020 yılında meydana gelen en büyük siber saldırı olaylarını aylara göre sıraladığı görülmüştür. Bu sıralamada: Ocak ayında; ABD ordusu, Çin'in TikTok platformundan kullanıcılarının bilgilerine erişebildiğini iddiasında bulunmuştur. Ayrıca, WordPress[3] programının eklentisinde kimlik doğrulama hatalarının bulunduğu, bu hatalar üzerinden de admin kullanıcı yetkisine sahip kişilerin sitenin arka planından siteye ait tüm bilgilere erişebildiği anlaşılmıştır. Şubat ayında; WhatsApp uygulamasından kötü amaçlı, fidye ve kimlik avı yazılımların kullanıcılara tamamen normal bir yazılımmış gibi görünmesini sağlayan güvenlik açığının bulunduğu tespit edilmiştir. Mart ayında; siber saldırıların Dünya Sağlık Örgütüne karşı gerçekleştirilen sofistike hacking atağı da dâhil olmak üzere ikiye katlandığı belirtilmiştir. Nisan ayında; Apple Iphone ve diğer İOS/macOS cihazlarda Sindhi dilinde mesajlar veya gönderiler yüklenirken cihazın kilitlenmesine neden olan güvenlik açığının keşfedildiği söylenmiştir. Mayıs ayında; Alman Şansölyesi Angela Merkel, Rusya devletini kendisine ve Alman Milletvekillerine bir dizi hackleme girişimlerinde bulunmakla suçlamıştır. Aynı ayda, 15 yaşında olan Ellis Pinsky ve arkadaşlarının bulunduğu bir hacker grubunun, Transform Group adlı firmadan 24 milyon dolar değerindeki kripto parayı çaldığı açıklanmıştır. Haziran ayında; pandemi nedeniyle insanların uzaktan çalışmaya başlaması mobil kimlik avı saldırılarında %37'lik artış yaratmıştır. Netgear router (ağ yönlendiricisi) bir yazılımda, 79 cihaz modelinin tümüyle ele geçirilebilmesine imkân tanıyan güvenlik açığı keşfedilmiştir. Ayrıca ismini açıklamayan bir Avrupa bankasının saniyede 809 milyon paket gönderilen bir DDOS saldırısına maruz kaldığı, bu saldırının da bugüne kadar bir ağa yapılmış en büyük saldırı olduğu açıklanmıştır. Temmuz ayında; 62 ülkede farklı sektörlerden iş liderliği yapan milyonlarca Microsoft Office 365 kullanıcısı insana, büyük bir kimlik avı saldırısı yapılmıştır. Dahası, Çin hükümetinin kendisiyle bağlantılı olan hackerlerle Covid-19 aşı çalışmalarına yönelik paha biçilemez verilerini çalmak amaçlı, ABD merkezli biyoteknoloji şirketi Moderna'yı hedefe alarak siber saldırılarda bulunduğu iddiası ortaya atılmıştır. Ayrıca ABD Başkanlarından Joe Biden ve Barack Obama'nın ve de iş adamlarından Bill Gates ve Elon Musk'ın Twitter hesaplarının hacklenerek takipçilerinin kandırılmaya çalışıldığı açıklanmıştır.

[3] Genel kamu lisanslı bir kişisel yayın sistemidir. Bu niteliği ile her türlü içeriğin düzenlenerek yayımlanabileceği bir platform olmaktadır.

Ağustos ayında; TikTok'un android işletim sistemine sahip milyonlarca kullanıcısını rızası bulunmaksızın izlediği tespit edilmiştir. Ayrıca, sistemlerde arka kapılar ve kripto madenciler oluşturan benzersiz ve gelişmiş bir P2P botner[4]'i olan FritzForg[5] adlı, milyonlarca SHH sunucusunu hedef alan saldırının gerçekleştirildiği belirtilmiştir. Eylül ayında; Almanya'nın Duesseldorf Üniversitesi Kliniğine yapılan bir fidye yazılım saldırısı sonucunda, bir kadının uzaktan başka bir tesise yönlendirilerek zaman kaybetmesi neticesinde ölümüne yol açıldığı anlaşılmıştır. Ekim ayında; İran hükümeti tarafından desteklenen bir hacker grubunun hedef sistemlerdeki domain kontrollerini ele geçirerek üzerinde tam denetim kurmalarını sağlayan Zerologon[6] güvenlik açığını buldukları iddiasında bulunulmuştur. Kasım ayında; UVM[7] Sağlık Ağlarına yapılan bir siber saldırı neticesinde, kemoterapi, mamografi ve tarama randevularını durdurarak 300 personelin ücretsiz izne ayrılmasına veya yeniden atama yapılmasına neden olunmuştur. Son olarak Aralık ayında; SolarWinds isimli teknoloji şirketinin Orion[8] yazılımına ait güvenliği ihlal edilmiş bir güncellemeyle, devlet destekli bir siber saldırgan gruba hükümet sistemlerine ve diğer sistemlere erişmesine olanak tanındığı iddiasında bulunulmuştur. (Sonicwall, 2021:6).16-18).

Tüm bu örneklerden de anlaşılacağı üzere, siber saldırılarla hedeflenen amaçlara yönelik hedef sistemler ve içerisinde bulunan her türlü veriyi elde etmek, değiştirmek veya bu sistemleri yine belirlenmiş amaçlar doğrultusunda kullanmak, hatta istenildiği anda imha etmek mümkündür. Bu durum pek tabi tehlikeli ellerde son derece risk ve tehdit dolu bir ortam yaratmaktadır. Ancak iyi yönetilerek insanlığın yararına kullanıldıklarında da bir o kadar yararlı ve faydalı olmaktadır. Dolayısıyla DAEŞ'le mücadelede, ihtiyaç duyulan istihbaratın elde edilmesinde kullanıldığını düşünüldüğünde, devletlere muazzam bir üstünlük yaratacağı açıktır. Bu üstünlük sayesinde de DAEŞ hedeflerinin gerek tespiti ve takibi gerekse imhası, konumdan bağımsız olarak eş zamanlı bir şekilde yürütülebilecektir. Böylelikle DAEŞ'in olası iletişim ağı, saklanma alınları, hücre yapılanmaları, eylem hazırlıklarına yönelik plan ve hedefleri önceden tespit edilerek zamanında müdahale edilmesi sağlanabilecektir. Sonuç

[4] Sahiplerinin bilgisi olmadan bir saldırganın amacı için birlikte çalışan, merkezi olmayan, kötü amaçlı yazılımdan ödün vermeyen makineler grubudur.
[5] Kontrolü tüm düğümleri üzerinde dağıtmak için P2P protokollerini kullanan, böylece tek bir denetleyiciye veya tek bir arıza noktasına sahip olmaktan kaçınan merkezi olmayan bir botnettir.
[6] Microsoft Windows ve Samba'nın *(işletim sistemleri arasındaki iletişimi sağlayan bir ağ sunucusu uygulamasıdır)* bazı sürümlerinde uygulanan Microsoft kimlik doğrulama protokolü Netlogon'daki kritik bir güvenlik açığıdır.
[7] Evrensel doğrulama metodolojisi anlamına gelir. Entegre devre tasarımını doğrulamak için standartlaştırılmış bir metodolojidir.
[8] Ağ performans izleyicisi olarak tasarlanmıştır. Ağ performansı sorunlarını ve kesinti süresini bulmanıza, sorun gidermenize ve düzeltmenize yardımcı olmak için kullanılmaktadır.

itibariyle de hem risk ve tehditleri önleyebilmek hem de hedefleri ve gizli yapılanmalarını deşifre ederek DAEŞ'in harekât alanını kısıtlamak siber saldırılar sayesinde gerçekleştirilebilecektir.

5.3.5. DAEŞ Hedeflerine Yönelik İHA (İnsansız Hava Araçları) Kullanımı

İHA'lar yapısal olarak kendi güç sistemleri bulunan, üzerinde silah, bomba, füze vb. ölümcül silah sistemleri ile kamera, radar, termal, optik, gece görüş vb. izleme ve takibe yarar sistemler taşıyan, içinde insan bulunmadan siber uzay teknolojileri aracılığıyla otomatik olarak veya uzaktan komuta edilen hava araçlarını ifade etmektedir (Akyürek, 2012:1). Sahip oldukları tüm bu yapısal özellikleri sayesinde ise insan kaybı olmadan herhangi bir hedefi tespit, teşhis, takip ve görüntüleyerek veri toplama, ölçüm yapma, işaretleme ve imha etme maksatlı kullanılmaktadırlar (Terkan, 2015:56). Bu sayede de bir yandan radar sistemleri, istihbarat, keşif ve gözetleme görevleri icra ederken diğer bir yandan da tespit ve teşhis edilen hedeflerin imha edilmesinde temel bir araç teşkil etmektedirler.

İHA'ların bir araç olarak kullanıldığı alanlara bakıldığında, dünyanın birçok bölgesinde devletler tarafından teröristle mücadelede etkin olarak kullanıldığı görülmektedir. Ancak birçok terör faaliyetlerine karşı İHA'lar etkin olarak kullanılmış olsa da DAEŞ ile mücadeleye yönelik örnekler verilmesi, bir yandan İHA'ların rolünün anlaşılması diğer bir yandan da DAEŞ'in faaliyetleri üzerinde ne gibi etkiler yaratarak olası sonuçlarının kavranmasında faydalı olacaktır. Bu kapsamda; ABD'nin 2015 yılında ilk kez İncirlik Hava Üstü'nden kalkan İHA uçaklarıyla DAEŞ'e ait hedefleri vurmasına yönelik yapılan açıklamayı incelediğimizde, Predatör adlı silahlı İHA'nın 11.100 km uzaklıktaki ABD'nin Nevada eyaletinden uzaktan komuta edilerek, DAEŞ'in o tarihte merkezi konumunu oluşturan Rakka'da kritik hedefleri vurduğu görülmektedir (Haberler.com, 2015). Yapılan operasyonu dikkatle düşündüğümüzde ise adeta bilgisayar oyununa benzediği söylenebilmektedir. Çünkü operasyonda; Pradatör adı verilen silahlı İHA, uzaktan bir komuta kontrol sistemiyle kontrol edilerek kıtalar arası operasyonda kullanılabilmiştir. Böylelikle ABD askerleri, hiçbir risk ve tehdit altında kalmadan binlerce km uzaklıktan terör hedeflerine yönelik istihbaratı elde etmiş ve de eş zamanlı olarak bu hedefleri imha edebilmiştir. Yine bir benzer yöntemle İngiltere aynı dönemlerde DAEŞ'in Irak'ta silah yüklü kamyonlarını vurduğunu açıklamış, yapılan açıklamada da keşif amaçlı bölgede uçan İHA'larının DAEŞ'e yönelik silah sevkiyatını tespit ettikleri ve devamında da harekete geçerek silah yüklü iki kamyonu vurdukları görülmüştür (Hürriyet, 2021). Son derece başarıyla gerçekleştirilen bu operasyonlar birbiri arkasına devam etmiş ve zamanla Fransa da

dâhil olmak üzere DAEŞ'in imhasına yönelik oluşturulan koalisyon güçleri de bu operasyonları gerçekleştirmiştir.

DAEŞ'e yönelik yapılan gerek İHA gerekse diğer operasyonlar değerlendirildiğinde ise en etkin mücadeleyi, Türkiye Cumhuriyeti Devletinin ortaya koyduğu görülmektedir. Bu kapsamda, yapılan açıklamalara bakıldığında; 12.01.2018 tarihli bir haberde, Fırat Kalkanı Harekâtıyla 3.060 DAEŞ üyesinin imha edildiği, 12.03.2018 tarihli bir haberde ise Zeytin Dalı Harekâtıyla 3300 teröristi imha ederek 16 köyün terörden arındırdığı bilgileri görülmektedir (Anadolu ajansı, 2018). Ayrıca 2016 yılında yapılan 10. Balkan Ülkeleri Genel Kurmay Başkanlığı Konferansı'nda, Türkiye Cumhuriyeti Cumhurbaşkanı Recep Tayyip ERDOĞAN tarafından Türkiye'nin bugüne kadar 3 bin DAEŞ üyesini öldürdüğü açıklanmıştır (Yazıcıoğlu, 2016). Yine benzeri bir açıklamayla; 29.12.2020 tarihinde Türkiye Cumhuriyeti Devleti Milli Savunma Bakanı Hulusi AKAR, yılsonu değerlendirmesine yönelik Genelkurmay Başkanı, Kuvvet Komutanları ile Bakan Yardımcılarının da katılımıyla gerçekleştirdiği bir toplantıda Türkiye'nin 24 Temmuz 2015'ten bu yana toplam 30 bin 416 teröristi etkisiz hale getirdiğini açıklamıştır (Özer, 2020). Tüm bu açıklamalardan da Türkiye Cumhuriyeti Devletinin DAEŞ terör örgütüne yönelik etkin mücadelesi anlaşılabilmektedir. Açıklanan bu sayıları Anadolu Ajansı tarafından hazırlanan Şekil 6'da belirtili İHA etkinlik durumuna yönelik görsel üzerinden incelediğimizde ise İHA'ların teröristle mücadeledeki performanslarını gözümüzde canlandırabilmek mümkün olabilmektedir.

Şekil 6. Anadolu Ajansı Tarafından Hazırlanan Teröristle Mücadeleye Yönelik İHA Etkinlik Durumu

Kaynak: (Gemici, 2020).

Anadolu Ajansı Tarafından Hazırlanan Teröristle Mücadeleye Yönelik İHA Etkinlik Durumu incelendiğinde; 2020'den geriye son beş yılda 63 bin 409 saat uçuşun gerçekleştirilmiş olduğu, bu uçuşlarla da doğrudan 1165 terörist ve 416 sığınağın imha edilmiş olduğu görülmüştür. Görülen bu sayılardan istatistiksel olarak ortalama her 40 saatte bir terör hedefinin imha edildiği hesaplanmaktadır. Hesaplanan bu sayılara ise İHA ile elde edilen istihbarat sayesinde sonradan operasyona dönüştürülerek hava, kara vb. harekâtlarla etkisiz hale getirilen hedeflerin sayısının dâhil edilmediği açıktır. Dolayısıyla gerek İHA'lar aracılığıyla doğrudan gerekse dolaylı olarak etkisiz hale getirilen terör hedefleri göz önüne alındığında, İHA teknolojisinin teröristle mücadelede geldiği nokta son derce aşikârdır. Bu sebepten, İHA teknolojilerinin daha da geliştirilerek etkinlik alanlarının genişletilmesi gerekmektedir. Böylece terörist yapıların mekândan ve konumdan bağımsız bir şekilde, binlerce kilometre uzaklıktan eş zamanlı olarak tespiti, teşhisi, takibi ve izlenmesi yapılıp, gerek görüldüğü anda da imha edilerek etkisizleştirilmesi sağlanabilecektir.

ALTINCI BÖLÜM

SONUÇ VE ÖNERİLER

Doğası gereği terörizm, yaşanan gelişmeler doğrultusunda değişim ve dönüşüm geçirerek geçmişten günümüze tekrar etmiş tarihsel bir fenomen olarak karşımıza çıkmaktadır. Çünkü geçmişten günümüze terör olgusu, insanların veya toplumların belirlenmiş bir hedefi gerçekleştirme uğruna korkutulması, caydırılması, yıldırılması, sindirilmesi, boyun eğdirilmesi ya da ortadan kaldırılması maksatlı her türlü tehdittin, saldırının ve eylemin gerçekleştirilmesinde, başvurulan acımasız bir aracı veya silahı vurgulayan şiddet biçimi olmuştur. Terörizm olgusu ise, terörün yani herhangi bir hedefi gerçekleştirmeye yönelik bir araç veya silah olarak uygulanan acımasız şiddet biçiminin, bir ideoloji güdümünde eylemle propagandayı öne çıkararak siyasi ya da sosyal amaçlar doğrultusunda sistemli olarak kullanılması olagelmiştir. Bu nedenle tarihsel süreç bağlamında, terör ve terörizm olgusunun kavramı değişmemekle birlikte şekil, tür, uygulama yöntemi ve doğurduğu sonuç itibariyle farklı boyutlarının ortaya çıktığı görülmüştür. Ortaya çıkan bu boyutlarında ilk terör hareketlerinden sırasıyla modern terörizm, nükleer terörizm, biyoterörizm, yeni terörizm ve siber terörizm gibi farklı tür ve şekillerde dönüşüm geçirerek geniş bir alana uzandığı anlaşılmıştır. Bu sonuçta terörizmi gerek teknolojik gerekse sosyopolitik anlamda yaşanan tüm yeniliklere ve değişikliklere paralel olarak etkileşimsel bir değişim ve dönüşüm sürecine uğratmış ve de son derece geniş bir alana yaymıştır.

Terörizme yönelik yaşanan tüm bu değişim ve dönüşüm süreci incelendiğinde ise siber terörizmin günümüzdeki en dikkat çekici boyut olduğu görülmektedir. Özellikle siber uzay teknolojisinin gelişimi ve yayılımıyla ortaya çıkan bu boyutun, sahip olduğu yapısıyla terör örgütlerine muazzam bir harekât alanı yarattığı itiraf edilmelidir. Bu alanları irdelediğimizde ise üç ana nokta karşımıza çıkmaktadır. İlk noktada, terör örgütlerinin siber uzay içerisinde yer alan internete dair web siteleri, oyun siteleri, sosyal medya hesapları ve online uygulamalar gibi platformlar üzerinden amaç, hedef ve ideolojileri doğrultusunda yazı, resim, müzik, video, ses vb. paylaşımlarla propaganda faaliyetlerinde bulunarak taraftarlarına moral ve motivasyon sağladığı ya da yeni taraftarlar toplamaya çalıştığı görülmektedir. İkinci noktada ise yine aynı yöntemlerle gerek aktif gerekse pasif olarak gizlenmiş uyuyan hücre yapılanmalarındaki örgüt üyeleriyle teknik, taktik ve ideolojik olarak hem canlı hem de kayda alınan verilerle eğitim verme, iletişim kurarak saldırı, sabotaj ve eylem planı sunma anlamında kullanıldığı

görülmektedir. Üçüncü ve en ölümcül senaryo olarak da siber uzaya bağlı tüm askeri, güvenlik, savaş teknolojisi ile enerji, uzay, nükleer, biyolojik, kimyasal, radyolojik, robotik ve yapay zekâ teknolojisi gibi kritik alt yapı sistemlerinin siber saldırılarla terör örgütlerinin eline geçme olasılığı ifade edilmelidir. Son derece tehlikeli olan bu olasılık, gerekli tüm tedbirlerin alınmadığı ve gerçekleşme ihtimali dahi olan tüm senaryoların önceden öngörülerek engellenmediği takdirde, tüm dünyayı geri döndürülemez bir gerçeğe uyandıracaktır. Bu gerçeklik ihtimalide siber terörizmi, tüm dünyanın her an her saniye terör tehditliyle karşı karşıya kaldığı büyük bir risk ve tehdit altında bırakacaktır.

Terörizmin, gerek geçmişten günümüze yayıldığı alanlara yönelik yaşanan insanlık dışı örnekleri, gerekse bugünden yarına yayılabileceği alanlara yönelik yaşanabilecek dehşet senaryoları dikkate alındığında, küresel ölçekte ne denli büyük bir tehdit oluşturduğu tüm devletler tarafından tahmin edilmektedir. Ancak ortada böyle bir tehdit varken günümüzde dahi hala devletlerin terörizme yönelik hemfikir olduğu ortak bir algılamasının bulunmaması, son derece dramatik bir durum ortaya koymaktadır. Daha kötüsü ise devletler tarafından çıkar odaklı sergilenen yaklaşımların kiminin teröristinin kiminin özgürlük savaşçısı olduğu algısına dönüşmesi, devlet destekli terörizm olgusunu yarattığı gibi, terörizmin daha da yaygınlaşarak bir kurtuluş aracı gibi görülmesine neden olmaktadır. Bu durumunda dünya sahnesine terör örgütlerinin savaştırılarak üzerlerinden çıkar sağlanmaya çalışıldığı vekâlet savaşlarını sunduğu görülmektedir. Ancak sahnelenen bu senaryo her geçen gün daha da tehlikeli bir boyuta dönüşebileceği göz ardı edilmemelidir. Çünkü o veya bu sebepten desteklenmekte olan terör örgütleri, zaman geçtikçe teknik, taktik ve teknolojik imkân ve kabiliyetlerini geliştirmekte, bu doğrultuda da ideolojik yapılarını daha da derinleştirerek aynı ölçüde eylem ve saldırılarını artırmaktadır. Artan eylem ve saldırılarda, daha çok insanın zarar gördüğü toplu katliamlara dönüşen kitlesel yıkımları beraberinde getirmektedir. Dolayısıyla her ne sebep olursa olsun terörizmin bir insanlık suçu olduğu, yer, zaman ve mekân sınırlaması bulunmaksızın hızla yaygınlaşarak bumerang etkisi yapabileceği unutulmalıdır. Bu gerçeklikten hareketle de devletlerce bir an önce terörizme yönelik küresel ölçekli bir iş birliği sağlanarak terörizmin her türlüsüne karşı etkin bir mücadele konsepti ortaya konmalıdır.

Terörizmle mücadeleye yönelik devletler tarafından etkin bir mücadele ortaya koyarken dört temel yaklaşım benimsenmelidir. Bu yaklaşımlardan ilkinin altında yatan nedenlerin tespit edilerek ortadan kaldırılması olduğu açıktır. İkinci yaklaşımda etkili ve sonuç odaklı bir askeri mücadelenin aralıksız bir şekilde sürdürülmesi elzemdir. Üçüncü yaklaşım olarak da her daim hukukun üstünlüğü prensibinin uygulanabilmesi gereklidir. Dördüncü ve son yaklaşımda ise

üst paragrafta da belirtildiği gibi terörizme yönelik en büyük sorunsal olan küresel yani uluslararası ölçekte bir iş birliğine gidilmesi şarttır. Aksi takdirde terörizmle mücadeleye yönelik yaklaşımlar devlet tekelinde veya bölgesel bir kısır döngüde sürdürülmeye devam edecektir.

Terörizme yönelik bu dört yaklaşımı belirtirken etkin bir istihbaratın varlığının da olmazsa olmaz bir ihtiyaç olduğunu belirtmek gerekmektedir. Çünkü ilk üç yaklaşımda sürdürülebilir bir başarı elde edilmek isteniyorsa doğru, isabetli ve devamlılık arz eden bir istihbaratın varlığına ihtiyaç duyulmaktadır. Dördüncü ve son yaklaşımda ise yapılması gerekli olan küresel ölçekli iş birliğinde yine aynı parametrelerde uluslararası bir istihbarat paylaşımına gidilmesi gerekmektedir. Tüm bunlar sağlanabildiği takdirde de terörle mücadelede topyekûn bir mücadeleye girişilerek önemli kazanımlar elde edilebilecektir.

Terörle mücadelede istihbaratın yeri ve önemini inceldiğimizde ise sahip olduğu kapasiteyle orantılı olarak terörle mücadelenin merkezinde yer aldığı söylenebilmektedir. İstihbaratın terörle mücadeleye yönelik sağladığı kazanımlarda bu düşünceyi desteklemektedir. Bu noktada belirtilmesi gereken en önemli kazanımında, etkin bir istihbaratın varlığıyla terör eyleminin gerçekleştirilmeden önlenmesi veya ön alınarak ortadan kaldırılabilmesinin mümkün oluşudur. Dolayısıyla istihbaratın gerek terörü ortaya çıkaran neden ve koşulların anlaşılmasında gerekse terörist organizasyonlarının deşifre edilerek yerlerinin, irtibatlarının, planlarının ve hedeflerinin açığa çıkarılmasında en akılcı disiplin olduğu gerçeği bir kez daha gün yüzüne çıkmaktadır. Bu gerçeklikten hareketle her daim terörle mücadelenin merkezinde yer alarak hem olası terör saldırılarını önleyici hem de olası terör hedeflerinin yok edilmesinde temel bilgi kaynağını oluşturacağı açıktır.

Terörle mücadelede konvansiyonel anlamda icra edilen istihbarat faaliyetleri incelendiğinde, teksif edilen gayretlere olumlu katkı sağlarken zaman, konum, terkip ve faaliyet bağlamında teyit ve tekzip sürecine katkı sağlamada yetersiz kaldığı göze çarpmaktadır. İstenilen katkının alınamaması da niteliği bakımından gelenekselleştirilmiş istihbarat yapı ve algılamalarının sorgulanmasına neden olmaktadır. Sorgulanan istihbarat yapı ve algılamaları ise ihtiyaç duyulan bilgilerin elde edilmesinde istihbaratı, yeni arayışlara yönlendirmektedir. Ayrıca bu noktada terörizmde yaşanmış değişim ve dönüşüm sürecinin etkisini de göz ardı etmemek gerekmektedir. Çünkü terörizm ve istihbaratın birbiriyle etkileşimsel bir dönüşüm içerisinde bulunduğu, tarihsel süreç içerisinde açıkça gözlenmektedir. Tam da bu noktada siber uzayla değişen dünya, anlatılmak istenen etkileşimsel dönüşümü net bir şekilde

örneklendirmektedir. Çünkü siber uzay bir yandan terörizme büyük bir hareket alanı sağlarken diğer bir yandan da istihbaratı doğru, isabetli ve devamlılık parametreleri ölçüsünde eş zamanlı sürdürülebilen bir yapıya kavuşturabilmektedir. Bu sayede de siber terörizmle ortaya çıkan tehdit boyutu, yine siber tabanlı istihbarat gayretleriyle önlenmeye çalışılarak terörizmle mücadeleyi daha kapsamlı bir yapıya dönüştürebilmektedir.

Siber uzay yapısı itibariyle, sanalla gerçeği iç içe geçirerek soyut ve düşünce düzeyindeki olguları, somutlaştırabilme imkânına kavuşturabilmektedir. Bu sayede de hayatın içerisinde var olan sağlık, ekonomi, iletişim, eğitim, finans, askeri, güvenlik, sosyal, coğrafi, ulaşım, savunma vb. alanlara hızla yayıldığı görülmektedir. Yayıldığı alanlar özelinde de her türlü işlemin anlık ve kolayca gerçekleştirilmesine imkân tanıyan cihaz, program, uygulama vb. özel sistemlerin geliştirilmesiyle, kendisini bu alanlara entegre ederek değişim ve dönüşüme neden olmaktadır. Bu dönüşümle birlikte de insanların günlük yaşantısına etki eden en karmaşık ve uzun zaman gerektiren işlemler kolaylaştırılarak anında çözümlenmektedir.

Siber uzayın insanların günlük yaşamını kolaylaştıran yapısı, her geçen saniye içerisine milyonlarca verinin dâhil edilmesine neden olmaktadır. Öyle ki eş zamanlı olarak kıtalar arası iletişimden uzaktan komuta kontrol sistemlerine, veri alışverişinden online eğitim sistemlerine, ihtiyaca yönelik kişisel sistemlerden devlet bazlı sistemlere varıncaya kadar gelişen siber uzay teknolojileri, bu durumun açık bir göstergesidir. Dolayısıyla tüm bu imkân, kolaylık ve fırsatların istihbarat özelinde de muazzam bir etki yaratarak istihbarat konseptlerinde devrimsel bir gelişime yön verdiği gözlemlenmektedir. Bu etkiyle de istihbaratın yeni imkânlar ve kabiliyetler kazanarak daha gizli, hızlı ve ekonomik bir kisveye bürünerek siber istihbarat olarak adlandırılan ve diğer tüm teknik ve taktikleri bünyesinde barındıran bir yapıya dönüştüğü açıkça görülmektedir.

Siber istihbaratın yeni bir alan olarak incelendiğinde, siber uzay üzerinden ihtiyaç duyulan her türlü istihbarat bilgisinin, siber uzayın sağlamış olduğu imkân ve kabiliyetler ölçüsünde, tespit edilen hedeften uygun bir yöntem kullanılarak elde edilmesi şeklinde kavramsallaştırılması mümkündür. Bu kavramsallaştırmadan harekenle de ilk olarak siber istihbarat, siber uzay üzerinden istihbaratın oluşturulmaya çalışılması şeklinde nitelendirilebilmektedir. İkinci olarak da yine herhangi bir hedefe ait siber uzay üzerindeki iletişim ağlarına, web sitelerine, bilgisayarlarına, mobil teknolojilerine vb. sistemlerine kişisel, kurumsal, ekonomik, politik veya askeri kazanımlar sağlamak amaçlı gizli bir şekilde sızılarak istenilen bilginin elde edilmesi ölçüsünde değerlendirilebilmektedir. Nihai olarak da siber

istihbaratın, diğer tüm istihbarat alan ve yöntemlerine yönelik teknik ve taktikleri bünyesinde barındıran kapsamlı bir yapıya dönüşmüş olduğu ifade edilebilmektedir.

Tüm bu ifadeleri desteklemek adına, siber istihbaratın siber uzaydaki önemli hedef alanları değerlendirildiğinde, veri tabanlarından bulut ortamlara, web sitelerinden sosyal medya platformlarına, mobil teknolojilerden internete bağlı tüm uygulamalara kadar uzanan geniş bir alanı kapsadığı görülmektedir. Bu alanlarında günümüzde insanlar için öncelikli ihtiyaçlar grubunda olduğu düşünüldüğünde, içerisinde yer alabilecek bilgilerin istihbarat açısından ne denli büyük bir hazineyi barındırmış olabileceği söylenebilmektedir. Dolayısıyla istihbarat bilgisine yönelik ortada duran bu hazineye ulaşılması içinde, belli başlı siber istihbarat yöntemlerinin devreye sokularak önemli bilgilerin elde edilebileceği bilinmelidir.

Siber istihbaratın elde edilmesinde ne gibi yöntemlerin uygulanabileceği araştırıldığında ise genel manada siber bal tuzağı, açık kaynak istihbaratı, sosyal medya istihbaratı, siber saldırı, yönlendirilmiş enerji silahları ve insansız hava araçları kullanımı gibi yöntemlerin son derece etkili olduğu gözlemlenebilmektedir. Bu yöntemler özelinde de doğru isabetli ve devamlılık arz eden istihbarata eş zamanlı olarak ulaşılabilmektedir. Gerek duyulduğu takdirde de yine eş zamanlı olarak dağıtımının yapılarak her daim hedeften bir adım önde olunabilmektedir.

Siber istihbaratın siber uzaydaki önemli hedef alanları ile yöntemlerini belirtirken, siber istihbarata yönelik üç sorunsalının da ifade edilmesi gerekmektedir. İlk olarak siber uzayın sürekli genişleyen ve gelişen yapısının siber istihbaratın siber uzaydaki hedef alanlarına yenileri ekleyeceği ve de günümüzdeki alanlar ile yeni ekleyeceği alanlara yönelik kendisini güncelleyeceği açıkça tahmin edilebilmektedir. İkinci olarak genişleyen, gelişen ve dönüşen siber uzay sistemlerinin günümüze kadar olduğu gibi yine aynı doğrultuda yeni siber istihbarat yöntemlerini ortaya çıkaracağı bilinmelidir. Son olarak da ortaya çıkan yeni siber uzay sistemleri ve siber istihbarat yöntemlerinin karşı istihbarat faaliyetlerine katkı sağlayarak İKK anlamında risk ve tehdit barındırabileceği göz ardı edilmemelidir. Bu minvalde de devletler tarafından üç sorunsal her daim göz önünde bulundurularak gelişen, değişen ve dönüşen siber uzay teknolojileriyle senkronize bir istihbarat yapılanmasına sahip olunabildiği takdirde, olası risk ve tehditler minimize edilebilecektir.

Verilen örneklerden ve DAEŞ vakası incelemesinden de anlaşılacağı üzere, siber istihbaratın teröristle mücadeleye yönelik bir araç olarak ele alındığında, devletlere teknik, taktik ve operasyonel anlamda büyük kazanımlar sağlayacağı açıkça görülebilmektedir. Bu kazanımlar incelendiğinde ise öncelikli olarak teröristle mücadelede ihtiyaç duyulan doğru,

isabetli ve devamlılık arz eden istihbaratın sağlanmasında, birçok yönden başarılı sonuçlar alınabileceği malumdur. Devamında yine doğru, isabetli ve devamlılık arz eden istihbaratın varlığıyla eş zamanlı olarak tespit ve teşhis eden terör hedeflerinin imha edilebileceği açıktır. Bu sonuçlar özelinde de etkin bir siber istihbaratın varlığıyla, teröristle mücadelede maliyet etkin 'sert' mücadele yöntemlerini mümkün kılabilecek istihbarata ulaşılarak nihai maksada matuf sonuçlara ulaşılabileceğini söylemek mümkündür.

Teröristle mücadelede nihai maksada matuf hedefler, öncelikli olarak terörist örgütlerin marjinalleştirilerek görünürlük ve propaganda kabiliyetlerinin düşük profile indirgenebilmesi, akabinde de terörist örgütlerin etkisiz hale getirilmesi temelinde şekillendirilmektedir. Dolayısıyla da siber istihbaratın nihai maksada matuf sonuçları, DAEŞ örneği özelinde incelendiğinde anlatılmak istenen duruma ölçüt gösterilebilmiştir. Vakanın incelenmesi neticesinde ise siber istihbaratın bir yandan ihtiyaç duyulan istihbaratı sağlarken diğer bir yandan da eş zamanlı olarak terörist hedeflerinin imha edilmesinde önemli bir rol oynayan araç olduğu görülebilmiştir. Bu sonuç özelinde de terörist örgütlerin tamamen etkisiz hale getirilemese dâhi marjinalleştirilerek görünürlük ve propaganda kabiliyetlerinin düşük bir profile indirgenebileceği ve bu sayede de tüm alanlardaki harekât kabiliyetlerinin kısıtlanabileceği anlaşılmıştır.

Yapılan araştırma, siber istihbaratı DAEŞ örneği üzerinden terörist yapıların etkisizleştirilebilmesinde, sert mücadele yöntemlerini çarpan etkisi yaratarak maliyet etkin kılabilecek doğru, isabetli ve devamlılık parametreleri ölçüsünde ihtiyaç duyulan istihbaratı sağlamada önemli bir araç olarak ortaya koymaktadır. Ancak siber istihbaratın aynı oranda karşı tarafa da imkân, fırsat ve harekât alanı yaratması, İKK bakımından da risk ve tehditleri artırmaktadır. Ayrıca gerek devletlerin gerekse uluslararası ve ulusüstü örgütlerin siber istihbaratın sağlanmasına yönelik birçok yöntemi hukuki açıdan suç olarak nitelendirmesi, siber istihbaratın terörist yapılarla mücadelede uygulanmasında sınırlılıklar yaratmaktadır. Bu sınırlılıkları önlemek adına da ulusal, uluslararası ve ulusüstü kurum ve kuruluşlar ile tüm devletlerin bir araya gelerek terörle mücadeleye yönelik bir istihbarat konsorsiyumu oluşturması, bu sayede de açık, şeffaf ve güven ilişkisi özelinde gerekli hukuki düzenlemeleri yaparak terörist yapılarla etkin bir mücadeleyi başlatması, sınırlılıkların ortadan kaldırılmasında çözüm yolu olacaktır.

KAYNAKÇA

Affde. (2020). *2021'de Günde Kaç Siber Saldırı Gerçekleşiyor?* https://www.affde.com/tr/how-many-cyber-attacks-per-day.html (24.12.2021).

Akmaral, K. (2013). *Anti Teröristin El Kitabı* (3.Baskı). İstanbul: Anatolia Yayınları.

Akyazı, U. (2013). Uluslararası Siber Güvenlik Stratejisi ve Doktrinler Arasında Alınabilecek Tedbirler. *6. Uluslararası Siber Güvenlik ve Kriptoloji Konferansı (2016-220).* https://www.iscturkey.org/assets/files/2016/03/2013-paper105.pdf (26.06.2021).

Akyürek, S. (2012). *İnsansız Hava Araçları Muhabere Alanında ve Terörle Mücadelede Devrimsel Dönüşüm* (Rapor No:53). Ankara: BİLGESAM.

Altmann, J. (2001). *Acoustic Weapons – A Prospective Assessment. Science & Global Security.* https://thinktech.stm.com.tr/uploads/docs/1608994680_stm-yonlendirilmis-enerji-silahlari.pdf (01.10.2021).

Alexander,Y. (1979). *International Terrorism: National, Regional and Global Perspectives.* New York: Praeger Publisher.

Alkan, N. (2016). *El Kaide'den IŞİD'e Din, Şiddet ve Terörizm* (1.Baskı). Ankara: Karınca Yayınları.

Altınok, T. ve Katman, F. (2019). *Suç, Terör ve Savaş Üçgeninde Siber Dünya* (1.Baskı). Ankara: Barış Platin Kitapevi.

Altuğ, Y. (1995). *Terörün Anatomisi* (1.Baskı). İstanbul: Altın Kitaplar Yayınevi.

Anadolu Ajansı. (2018). *TSK 2017'de Etkisiz Hale Getirilen Terörist Sayısını Açıkladı.* https://www.aa.com.tr/tr/gunun-basliklari/tsk-2017de-etkisiz-hale-getirilen-terorist-sayisini-acikladi/1029254 (25.12.2021).

Anadolu Ajansı. (2018). *Zeytin Dalı Harekatı'nda 3300 Terörist Etkisiz Hale Getirildi.* https://www.aa.com.tr/tr/dunya/zeytin-dali-harekatinda-3300-terorist-etkisiz-hale-getirildi/1085426 (25.12.2021).

Aslay, F. (2017). Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi. *IJMSIT (International Journal of Multidisciplinary Studies and Innovative Technologies), 1* (1), 24-28.

Atasever, S., Özçelik, İ. ve Sağıroğlu, Ş. (2019). Siber Terör ve DDoS. *Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Dergisi, 23* (1), 238-244.

Ateş, H. (2013). *Türk İstihbarat Sisteminin Sorunsalları* (1.Baskı). Ankara: Detay Yayınları.

Avşar, Z. (2017). İnternet Çağında Medya, Terör ve Güvenlik. *TRT Akademi,* 2 (3), 116-132.

Ay, Z. (2013). Siyaset ve teoloji: Orta çağ İsmaili Teolojisinin Oluşmasında Siyasi Gelişmelerin Rolü. *İSTEM Dergisi,* (21), 149-162.

Aydın, N. (2016). *Küresel Terör ve Türkiye* (2. Baskı). İstanbul: Remzi Kitapevi.

Baharçiçek, A. (2000). Etnik Terör ve Etnik Terörle Mücadele Sorunu. *Fırat Üniversitesi Sosyal Bilimler Dergisi, 10* (1), 11-27.

Bal, İ. (2006). *Terörizm; Terörizm ve Küresel Terörle Mücadelede Ulusal ve Bölgesel Deneyimler* (1.Baskı). Ankara: Uluslararası Stratejik Araştırmalar Kurumu.

Bal, M. A. (2003). *Savaş Stratejisinde Terör* (2.Baskı). İstanbul: IQ Kültür Sanat Yayıncılık.

Bankoff, G. (2004). Risk bölgeleri: Batının Terör Üzerine Görüşleri ve İslam'ın Yeri. *Dini Araştırmalar, 7* (20),377-386.

Bayraktar, G. (2010). Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat. *Güvenlik Stratejileri Dergisi, 10* (20), 119-147.

Benes, L. (2013). OSINT, New Technologies, Education: Expanding Opportunities and Threats. A New Paradigm. *Journal of Strategic Security, 6* (5), 21-37. https://www.jstor.org/stable/26485053?seq=17#metadata_info_tab_contents (21.11.2021).

Bergnet. (2021). *Eavesdropping Nedir? Orta Kulak Saldırıları.* https://berqnet.com/blog/eavesdropping (11.12.2021).

Best, R. A. & Cumming, A. (2007). *Open Source Intelligence (OSINT): Issues for Congress.* https://sgp.fas.org/crs/intel/RL34270.pdf (20.11.2021).

Beyazperde. (2015). *Hızlı ve Öfkeli 7.* https://www.beyazperde.com/filmler/film-198750/ (05.12.2021).

BGA Security. (2019). *Sosyal Medya İstihbaratı SOCMINT Nedir?* https://www.bgasecurity.com/2019/09/sosyal-medya-istihbarati-socmint-nedir/ (29.11.2021).

Bilir, H. (2009). *Terör Medya ve Devlet* (1.Baskı). İstanbul: IQ Kültür Sanat Yayıncılık.

Boyacıoğlu, H. (13.08.2015). 100'den Fazla Site Kapatıldı. *Hürriyet.com.* https://www.hurriyet.com.tr/gundem/100-den-fazla-site-kapatildi-29797980 (22.12.2021).

Bulut, A. (2019). *Terörizm ve İstihbarat: Etkileşimsel Dönüşüm*. Yayımlanmış Yüksek Lisans Tezi. Hasan Kalyoncu Üniversitesi, Gaziantep.

Can, M. (30.01.2021). Türkiye'ye 110 Bin Siber Saldırı Yapıldı! Peki ne Kadarı Başarılı Oldu? *Sabah.* https://www.sabah.com.tr/ekonomi/2021/01/30/turkiyeye-110-bin-siber-saldiri-yapildi-peki-ne-kadari-basari-oldu (24.12.2021).

Canbek, G. ve Sağıroğlu, Ş. (2006). *Bilgi ve Bilgisayar Güvenliği: Casus Yazılımlar ve Korunma Yöntemleri* (1.Baskı). Ankara: Grafiker Yayıncılık.

Carl, L.D. (1990). *International Dictionary of Intelligence* (1.Baskı). VA: Maven Books.

Cemalioğlu, K. (08.05.2020). İnternet Nedir? İnternetin Tarihçesi. *Millenicom.* https://www.milleni.com.tr/blog/internet/internet-nedir (29.06.2021).

Cenk, M. (2019). Siber Güvenlikte Kriptografi. Ş. Sağıroğlu ve M. Alkan. (Ed.), *Siber Güvenlik ve Savunma Problemler ve Çözümler* (61-83). Ankara: Grafiker Yayınları.

Chaliand, G. ve Blin, A. (2016). *Terörizmin Tarihi Antikçağdan IŞİD'e.* (B. Tanatar, Çev.). İstanbul: Nora Kitap.

Chertoff, M. (2006). *Secretary of Homeland Security Michael Chertoff 2006 Bureau of Justice Assistance, U.S. Department of Justice and SEARCH Symposium on Justice and Public Safety Information Sharing.* https://www.hsdl.org/?view&did=474507 (24.04.2021).

Cin, H. (1987). Anarşi ve Teröre Karşı Atatürkçülükte Bütünleşme. (Ed.), Milli Eğitim Gençlik ve Spor Bakanlığı Gençlik Hizmetleri Genel Müdürlüğü. (Ed.), *Uluslararası Terörizm ve Gençlik* (54-64). Ankara: MEB Yayınları.

Clemente, D. (2015). Fundamentals of Cyber Security. L.Macfaul. (Ed.), *Verıfıcatıon & Implementatıon A Biennial Collection of Analysis on International Agreements For*

Security and Development (163-179). London: Vertic. http://www.vertic.org/media/assets/Publications/Verification%20and%20Implementation%202015.pdf (25.05.2021).

CNNTürk. (2019). *World Wide Web Ne Demek?* https://www.cnnturk.com/turkiye/world-wide-web-nedir-google-wwwnun-tarihini-unutmadi (4.07.2021).

Conway, M. (2002). Reality Bytes: Cyberterrorism and Terror ‘‘Use’’ of the Internet. *First Monday, 7* (11), https://firstmonday.org/ojs/index.php/fm/article/download/1001/922 (13.05.2021).

Çağıltay, K. (1997). İnternet: Kullanıcı Servisleri. *Midole East Technical University.* https://ocw.metu.edu.tr/mod/resource/view.php?id=748 (3.07.1990).

Çahmutoğlu, E. (2020). Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi. *Analytical Politics, 1* (1), 1-17.

Çakmak, H. (2008). *Terörizm* (1.Baskı). Ankara: Platin Yayınları.

Çakmak, T. ve Yalçın, H. (2013). Üniversite Öğrencilerinin Mobil Teknoloji Kullanımı: Hacettepe Üniversitesi Bilgi ve Belge Yönetimi Bölümü Örneği. *Hacettepe Üniversitesi Türkiyat Araştırmaları Dergisi, 2013 Bahar* (18), 47-61.

Çelik, S. (2018). Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım. *Academic Review Of Hummanities and Social Sciences, 2* (1), 110-119.

Çiftçi, H. (2017). *Her Yönüyle Siber Savaş* (2.Baskı). Ankara: TÜBİTAK Popüler Bilim Kitapları.

Çınar, B. (1997). *Devletin Güvenliği, İstihbarat ve Terör* (1.Baskı). Ankara: Sam Yayınları.

Çıtak, Ö. (2016). *Ethical Hacking Offensive & Defensive* (1.Baskı). Kocaeli: Level Kitap.

Çokbildik, A. C. (2019). *Siber Terörizm: Radikal/Dini Örgütler.* Yayımlanmış Yüksek Lisans Tezi. Selçuk Üniversitesi. Konya.

Çomak, H., Sancaktar, C. ve Demir, S. (2016). *Uluslararası Güvenlik.* İstanbul: Beta Yayınları.

Davies, P. H. J. (2002). Ideas of Intelligence: Divergent National Concepts and Institutions. *Harvard International Review, 24* (3), 62-66.

Defence Point. (2019). *Directed Energy Weapons Market Report 2019-2029.* https://defence-point.com/2019/02/20/directed-energy-weapons-dew-market-report-2019-2029/ (01.10.2021).

Demir, C. (11.06.2017). Monitoring Nedir? *Pazarlamailetisimi.com.* https://pazarlamailetisimi.com/monitoring-nedir/ (11.12.2021).

Demirci, S. (2012). Nükleer Terörizm ve Tehdit Boyutlarına Yönelik Çıkarımlar. *Ege Stratejik Araştırmalar Dergisi, 3* (1), 59-84.

Dictionary. Origin Of Mobile. (12.07.2021). https://www.dictionary.com/browse/mobile?s=t

Doğan, U. (05.03.2016). Sosyal Medya Platformu. *Uysaldogan.com.* http://uysaldogan.com.tr/blogdetay/sosyal-medya-platformu.aspx (28.11.2021).

Donanım Haber Forum. (2011). *Sistemlere Yönelik Tehditler.* https://forum.donanimhaber.com/bilgisayar-saldirilari-ve-onlemleri-nelerdir--50032476 (11.12.2021).

Elfa. (2021). *Sniffing ve Spoofing Nedir?* https://elfanet.com.tr/tr/main/article/sniffing-ve-spoofing-nedir/43 (11.12.2021).

Eskişehir İl Jandarma Komutanlığı, (2021). *İnternet Üzerinden PKK/YPG/KCK, Terör Örgütlerinin Propagandasını Yaptıkları Tespit Edilen 3 Şüpheli Yakalandı, 2 İnternet Sitesi Kapatıldı.* https://eskisehir.jandarma.gov.tr/internet-uzerinden-pkkypgkck-teror-orgutlerinin-propagandasini-yaptiklari-tespit-edilen-3-supheli-yakalandi-2-internet-sitesi-kapatildi (22.12.2021).

Ferris, J. R. (2005). *Intelligence and Strategy: Selected Essays* (1.Baskı). New York: Routledge.

Gaxotte, P. (1961). *Fransız İhtilali Tarihi* (Tiryakioğlu, S. Çev.). İstanbul: Varlık Yayınları.

Gemici, O.O. (07.03.2020). İHA ve SİHA'lar Teröristlerin Korkulu Rüyası Oluyor. *Anadolu Ajansı.* https://www.aa.com.tr/tr/turkiye/iha-ve-sihalar-teroristlerin-korkulu-ruyasi-oluyor/1757756 (25.12.2021).

Gibbs, J.P. (1989). Conceptualization of Terrorism. *American Sociological Review. 54* (3), 329-340.

Gill, P. (2009). *Theories of Intelligence: Where are We, Where Should We Go and How Might We Proceed* (1.Baskı). New York: Routledge Press.

Gül, K.M. (2016). *Yüz İcat ve Olayda Dünya Tarihi* (1.Baskı). Kafe Kültür Yayıncılık. https://books.google.com.tr/books?id=DqvmDwAAQBAJ&pg=PA41&lpg=PA41&dq#v=onepage&q&f=false (4.07.2021).

Güntay, V. (2018). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler. *Güvenlik Stratejileri Dergisi, 14* (27), 79-111.

Gürler, R.T. ve Özdemir, Ö.B. (2014). El Kaide'den Post-Kaide'ye Dönüşüm: IŞİD. *Türkiye Ortadoğu Çalışmaları Dergisi, 1* (1), 113-155.

Güven, M. (25.08.2021). *Casusluk.* https://hukukdershanesi.com/casusluk/

Haberler.com. (2015). *ABD, 11 bin 10 Km'den IŞİD'i Vurdu.* https://www.haberler.com/abd-11-bin-100-km-den-isid-i-vurdu-7577266-haberi/ (25.12.2021).

Herbst, P. (2003). *Talking Terrorism a Dictionary of The Loaded of Political Violence.* London: Greenwood Press.

Herman, M. (2001). *Intelligence Services in The Information Age: Theory and Pratice* (1.Baskı). London: Frank Cass.

Hootsuite. (2012; 2013; 2014; 2015; 2016; 2017; 2018; 2019; 2020; 2021). *Digital Global Overview Report.* https://wearesocial.com/uk/special-reports ; https://www.slideshare.net/search/slideshow?searchfrom=header&q=global+digital+overview (3.07.2021).

Hoffman, B. (1998). *Inside Terrorism* (1.Baskı). New York: Columbia University Press.

Hürriyet. (1993). *Temel Britannica Genel Kültür Ansiklopedisi,* 17, İstanbul: Hürriyet Ana Yayıncılık.

Hürriyet. (2017). *Bal Tuzağı Nedir.* https://www.hurriyet.com.tr/gundem/bal-tuzagi-nedir-40682137 (21.10.2021).

Hürriyet. (2020). *World Wide Web Nedir?* https://www.hurriyet.com.tr/egitim/world-wide-web-nedir-www-ne-demek-kim-tarafindan-ne-zaman-kuruldu-ve-tarihi-41623064 (4.07.2021).

Hürriyet. (2021). *CNN: Paris'teki Terör Saldırılarında En Az 153 Kişi Öldürüldü.* https://www.hurriyet.com.tr/dunya/pariste-silahli-saldiri-40013825 (21.12.2021).

Hürriyet. (2021). *İngiltere İlk Kez IŞİD'i Vurdu.* https://www.hurriyet.com.tr/dunya/malezyada-agir-bilanco-46-olu-5-yarali-41968391 (25.12.2021).

Hürriyet Haber. (2014). *Neden 'İslam Devleti' Demiyoruz?* https://www.hurriyet.com.tr/neden-islam-devleti-demiyoruz-27334634 (16.04.2021).

İzol, R. ve Zenginoğlu, S. (2014). 11 Eylül ve Sonrası: Terörizm, Petrol ve Nükleer Tehdit Ekseninde Ortadoğu. *Hitit Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 7* (2), 423-439.

INSA. (2015). *Cyber Intelligence: Preparing Today's Talent for Tomorrow's Threats.* Virginia: Intelligence and National Security Alliance, September 2015.

Johnson, P. (1980). *The Seven Deadly Sins of Terrorism. Jeusalem: The Jonathan Institue.* (1.Baskı). New York: Routledge.

Johnson, R. and Zenko, M. (2002). All Dressed Up and No Place To Go: Why NATO Should Be On The Front Lines İn The War On Terror. *US Army War College Parameters, 32* (4), 47-63.

Kahn, D. (2002). İstihbaratın Tarihsel Teorisi. *Avrasya Dosyası, 8* (2), 5-20.

Kanat, S., Kodaman, T. ve İren, A.A. (2016). İnsani Güvenlik ve Terörizmle Mücadele. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Dergisi. 21* (2), 567-588.

Karaağaç, Y. (2019). Terörizmle Mücadele Yöntemleri: İngiltere ve Kolombiya Örneği. *Avrasya Sosyal ve Ekonomi Araştırmaları Dergisi. 6* (1), 231-242.

Karakaya, İ. (2019). Küresel Terörizmin dönüşümü: Irak ve Şam İslam Devleti (IŞİD) Örneği. *B.U.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi, 38* (1), 149-198.

Karakuş, C. (02.10.2021). *Yönlendirilmiş Enerji Kaynakları.* https://ckk.com.tr/em/Y%C3%B6nenerji.pdf

Kartal, A.B. (2014). Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye'de DAEŞ ve YPG Örneği. *Güvenlik Stratejileri Dergisi.* (27), 39-77.

Kayabaş, İ. (2018). Yeni İletişim Teknolojileri. T. V. Yüzer ve M. E. Mutlu (Ed.), *Mobil Teknolojiler* (100-135). Eskişehir: Anadolu Üniversitesi.

Kazan, H. (2012). Terör – Medya İlişkisi ve Medyada Terör Haberciliği. *Güvenlik Stratejileri Dergisi.* (24), 109-147.

Keleştemur, S. A. (2018). *Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi.* Yayımlanmamış Yüksek Lisans Tezi, İstanbul.

Kent, S. (2003). *Stratejik İstihbarat.* (Özbek, B.Y ve Arıca, N.Ş. Çev.). Ankara: ASAM Yayınları.

Kotuamacliyazilim.com. (2016). *Siber Savaşlar: Başlangıç.* https://www.kotuamacliyazilim.com/siber-savaslar-baslangic/ (28.08.2021).

Köknar, A. M. (2001). Sanal Ortamda Terörizm. *T.C. İçişleri Bakanlığı Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Semineri'ne Sunulan Bildiri.* Bursa: 24 Mart 2001.

Köseli, M. (2009). Terörle Mücadelede İstihbaratın Rolü. *Polis Bilimleri Dergisi, 11* (2), 51-72.

Köşüş, B. (2019). *Kırılgan Devlet – Terörizm İlişkisi ve Terörizmle Mücadelede Yönetilemeyen Alan Sorunu: Sahra Altı Afrika Örneği.* Yayımlanmış Yüksek Lisans Tezi, Süleyman Demirel Üniversitesi, Isparta.

Kuçuradi, İ. (2002). İnsan Haklarından Devlet Kavramına. C. Güzel. (Ed.). *Silinen Yüzler Karşısında Terör* (332-344). Ankara: Ayraç Yayınları.

Laqueur, W. (1977). *The Age of Terrorism.* Boston: Little Brown and Company.

Laqueur, W. (2002). Bomba Felsefesi. C. Güzel. (Ed.), *Silinen Yüzler Karşısında Terör* (21-94). Ankara: Ayraç Yayınları.

Lenin, V. İ. (2009). *Devlet ve devrim* (Aydar, F. B. Çev.). (1.Baskı). İstanbul: Agora Kitaplığı.

Martin, G. (2017). *Terörizm Kavramlar ve Kuramlar.* (İ. Çapcıoğlu ve B. Metin, Çev.). Ankara: Adres Yayınları.

Memiş, T. (2001). Hukuki Açıdan Kitlelere E-posta Gönderilmesi. *Atatürk Üniversitesi Erzincan Hukuk Fakültesi Dergisi 5* (1-4), 431-444.

Migaux, P. (2016). El Kaide. G. Chaliand. ve A.Blin. (Ed.), *Terörizmin Tarihi: Antikçağdan Işid'e* (390-436). (B. Tanatar, Çev.). İstanbul: Nora Kitap.

Millî İstihbarat Teşkilâtı. *İstihbarat Oluşumu.* https://www.mit.gov.tr/isth-olusum.html (13.03.2021).

Miş, N. ve Özdemir, Ö.B. (2014). Suriye 2013. K. İnat ve M. Ataman. (Ed.), *Ortadoğu Yıllığı* (195-220). İstanbul: Açılım Kitap.

MİT. *İstihbarat Oluşumu.* https://www.mit.gov.tr/isth-olusum.html (21.04.2021).

Mitnick, K.D. ve Simon, W.L. *Aldatma Sanatı.* (Tezcan, N.E. Çev.). Ankara: ODTÜ Yayıncılık.

Mizokami, K. (18.03.2019). The Pentagon Wants to Test a Spance-Based 'Particle Beam' by 2023. *Popular Mechanics.* https://www.popularmechanics.com/military/weapons/a26858944/pentagon-particle-beam-space-2023/ (01.10.2021).

Molatik. (2020). *Bal Tuzağı Nedir.* https://www.milliyet.com.tr/bal-tuzagi-nedir--molatik-16983/ (21.10.2021).

Nasrat, Q. (2015). *Siber Terörizmle Mücadele ve Uluslararası Hukuk.* Yayımlanmış Yüksek Lisans Tezi. Atatürk Üniversitesi, Erzurum.

NTV. (2017). *Hacker'ların yeni "Bal Tuzağı".* https://www.ntv.com.tr/galeri/teknoloji/hackerlarinyeni-bal-tuzagi,pA7WK_ZQ5E2EaTruZ6pT1Q/P7FYldSwq0KVSGyKRurSmA (22.12.2021).

Olgunsoy, F. (2019). *Terörle Mücadelede İstihbarat Faaliyetlerinin Özgürlükler Rejimine Etkisi: Türkiye, Birleşik Krallık, Amerika Birleşik Devletleri.* Yayımlanmış Doktora Tezi. İstanbul Üniversitesi, İstanbul.

Orton, K. (2017). *Foreign Terrorist Attacks By The Islamic State, 2002-2016.* Center fort he Responseto Radicalisation and Terrorism Report, Henry Jackson Society.

Oruç, M. A. (2019). *İstihbaratın Geleceği: Siber Uzayda İstihbarat ve Karşı İstihbarat Faaliyetlerinde Yapay Zekâ ve Veri Bilimi Kullanımı.* Yayımlanmış Yüksek Lisans Tezi. İstanbul Aydın Üniversitesi, İstanbul.

Ostim Teknik Üniversitesi. (2021). *İnsansız Hava Aracı Teknolojisi ve Operatörlüğü Programı.* https://www.ostimteknik.edu.tr/insansiz-hava-araci-teknolojisi-ve-operatorlugu-programi-758 (19.12.2021).

Özçoban, C. (2014). *21. Yüzyılda Ulusal Güvenliğin Sağlanmasında Siber İstihbaratın Rolü.* Yayımlanmış Yüksek Lisans Tezi. Harp Akademisi. İstanbul.

Öğün, M.N. ve Kaya, A. (2013). Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. *Güvenlik Stratejileri Dergisi, 9* (18), 145-181.

Özdağ, Ü. (2002). Stratejik İstihbarat. *Avrasya Dosyası: Üç Aylık Uluslararası İlişkiler ve Stratejik Araştırmalar Dergisi, İstihbarat Özel, 8* (2), 109-149.

Özdağ, Ü. (2020). *İstihbarat Teorisi* (14.Baskı). Ankara: Kripto Basım Yayım.

Özel, H. (16.07.2018). Sosyal Mühendislik Nedir? *halilozel.com.* https://halilozel1903.medium.com/sosyal-m%C3%BChendislik-nedir-754984e5b0aa (11.12.2021).

Özer, S. (30.12.2020). Milli Savunma Bakanı Akar: 2015'ten Bugüne Kadar Etkisiz Hale Getirilen Toplam Terörist Sayısı 30 Bin 416 Oldu. *Anadolu Ajansı.* https://www.aa.com.tr/tr/turkiye/milli-savunma-bakani-akar-2015ten-bugune-kadar-etkisiz-hale-getirilen-toplam-terorist-sayisi-30-bin-416-oldu/2093006 (25.12.2021).

Özkan, S. (11.07.2021). *Veri Tabanı Yönetim Sistemleri.* https://personel.klu.edu.tr/dosyalar/kullanicilar/selcuk.ozkan/dosyalar/dosya_ve_belgeler/dersler/Ders1.pdf

Özkan, T. (2006). *Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi.* Yayımlanmış Yüksek Lisans Tezi. Eskişehir Anadolu Üniversitesi. Eskişehir.

Özman, R. ve Açıl, O. (2019). Sicarii örgütü ve faaliyetleri. *Ankara Üniversitesi Dergisi, 38* (65), 21-42.

Pfiffner, J. (2006). Les décisions de guerre de George W. Bush: l'Afghanistan et l'Irak. *Politique Américaine, 5* (2), 35-52.

Polat, D.Ş. (2016). Irak Şam İslam Devleti. H. Çomak., C. Sancaktar. ve Z.Yıldırım.(Ed.), *Uluslararası Politikada Suriye Krizi* (211-226). İstanbul: BETA Basım.

Privia Security. (2020). *SOCMINT Sosyal Medya İstihbaratı Nedir?* https://www.priviasecurity.com/socmint-sosyal-medya-istihbarati-nedir/ (29.11.2021).

Richelson, J.T. (2012). *The US Intelligence Community* (4.Baskı). Philadelphia: Westviews Press.

Robertson, K. G. (1987). Intelligence, Terrorism and Civil Liberties. *Journal of Conflict Studies, 7* (2), 43-62.

Ruhle, M. (2003). NATO After Prague: Learning The Lessons Of 9/11. *The US Army War College Quarterly: Parameters, 33* (2), 88-97.

Sağıroğlu, Ş. (2018). Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler. Ş. Sağıroğlu ve M. Alkan. (Ed.), *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* (18-45). Ankara: Grafiker Yayınları.

Sağıroğlu, Ş. (2019). Siber Güvenlik ve Ötesi. Ş. Sağıroğlu ve M. Alkan. (Ed.), *Siber Güvenlik ve Savunma Problemler ve Çözümler* (25-58). Ankara: Grafiker Yayınları.

Shughart, W. F. (2006). An Analytical History of Terrorism, 1945-2000. *Public Choice, 128* (1), 7-39.

Sander, O. (2000). *Siyasi Tarih 1918-1994* (10. Baskı). Ankara: İmge Kitabevi.

Sandıklı, A. ve Yivciger, G. (2004). *Siber Terörizm.* İstanbul: TASAM Yayınları, (47).

Saraçlı, M. (2007). Uluslararası Hukukta Terörizm. *Gazi Üniversitesi Hukuk Fakültesi Dergisi. XI* (1-2), 1049-1078.

Savunma-sanayi.com. (29.09.2021). *Yönlendirilmiş Enerji Silahları.* https://savunma-sanayi.com/yonlendirilmis-enerji-silahlari/

Scheuer, M. (2012). *Osama Bin Laden* (2.Baskı). New York: Oxford University Press.

Semercioğlu, H. (2016). Uluslararası Terörizmde Küresel İşbirliği: Bir Ütopya. *Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 34* (2), 97-114.

Seren, M. (2017). *Stratejik İstihbarat & Ulusal Güvenlik* (1.Baskı). Ankara: Orion Kitapevi.

Sonicwaal, (2021). *2021 Sonicwall Siber Tehdit Raporu.* https://www.e-data.com.tr/wp-content/uploads/2021/05/2021-SonicWall-Cyber-Threat-Report_lowres-%20tr.pdf (24.12.2021).

Sönmez, İ. (2013). *Terörizmle Mücadelede İstihbaratın Yeri ve Önemi.* Yayımlanmış Yüksek Lisans Tezi. Haliç Üniversitesi, İstanbul.

Sönmez, G. (2018). IŞİD'in Dönüşümü ve Önümüzdeki Yeni Meseleler. *ORSAM, Haziran 2018* (217).

Sözcü. (2019). *World Wide Web Nedir?* https://www.sozcu.com.tr/2019/teknoloji/world-wide-web-nedir-world-wide-web-doodle-oldu-iste-tarihi-ve-onemi-3874366/ (4.07.2021).

Şahin, B. (10.07.2021). Abdullah Öcalan'a Bal Tuzağı. *Pusula Güvenlik Araştırmaları Topluluğu.* https://www.pugat.org/istihbarat/2021/07/10/abdullah-ocalana-bal-tuzagi/ (22.12.2021).

Şen, A. (2015). Suriye Askeri Muhalefeti. *ORSAM Raporu,* (202).

Şen, H. (2019). *PKK Terör Örgütünün İdeolojik ve Yapısal Dönüşümü.* Yayımlanmış Yüksek Lisans Tezi. Polis Akademisi, Ankara.

Şen, İ. (14.03.2018). Ağ Tarama / Analiz Saldırıları. *ismailsen.com.* http://ismailsen.com.tr/ag-tarama-analiz-saldirilari/ (12.12.2021).

Taşdemir, E. (2017). Sosyal Medyada Terör Propagandası: DEAŞ Örneği. *Gümüşhane Üniversitesi İletişim Fakültesi Dergisi 5* (2), 726-752.

Taylor, S.A. (2007). The Role of Intelligence in National Security. A. Colins. (Ed.), *Contemporary Security Studies.* New York: Oxfort University Press.

TBB. (2006). *Türkiye ve Terörizm.* Ankara: Şen Matbaa.

T.C. İçişleri Bakanlığı. (2017). *Türkiye'nin DEAŞ ile Mücadelesi.* https://www.icisleri.gov.tr/kurumlar/mia.gov.tr/Genel/deas%CC%A7%207%20temmuz.pdf (23.12.2021).

T.C. İçişleri Bakanlığı, (2018). *1 Ocak – 31 Aralık 2018 Yılı İçerisinde Yürütülen Operasyonlar.* https://www.icisleri.gov.tr/1-ocak-31-aralik-2018-yili-icerisinde-yurutulen-operasyonlar (23.12.2021).

T.C. İçişleri Bakanlığı, (2018). *5.Uluslararası Siber Suçlar Çalıştayı.* https://www.icisleri.gov.tr/5-uluslararasi-siber-suclar-calistayi (23.12.2021).

T.C. İçişleri Bakanlığı. (2020). *Dünyadan Örneklerle Siber Güvenlik Stratejileri ve Siber Uzay.* İç güvenlik Stratejileri Dairesi Başkanlığı.

T.C. İçişleri Bakanlığı, (2020). *Sosyal Medyada Asılsız Koronavirüs Paylaşımları ve Terör Propagandası Yapan 1748 Hesap Tespit Edildi.* https://www.icisleri.gov.tr/sosyal-medyada-asilsiz-koronavirus-paylasimlari-ve-teror-propagandasi-yapan-1748-hesap-tespit-edildi (23.12.2021).

T.C. İçişleri Bakanlığı, (2021). *Sosyal Medyadan Terör Propagandasına 39 Gözaltı.* https://www.icisleri.gov.tr/sosyal-medyadan-teror-propagandasina-39-gozalti (23.12.2021).

TDK. *Güncel Türkçe Sözlük.* https://sozluk.gov.tr/ (21.04.2021).

Tekek, M. (11.03.2016). Açık Kaynak İstihbaratı (Open Source Intelligence) ve Düşünce Kuruluşları. *Hidropolitik Akademi.* https://hidropolitikakademi.org/tr/article/11752/acik-kaynak-istihbarati-open-source-intelligence-ve-dusunce-kuruluslari (17.11.2021).

Tekeli, E. (2015). *Veri tabanı Ders Notları.* https://abs.cu.edu.tr/Dokumanlar/2015/BL%20213/549956129_veritabani-not1.pdf (11.07.2021).

Terkan, A. (2015). *Terörizmle Mücadele Kapsamında İnsansız Hava Araçlarının Rolü: Federal Yönetimli Aşiret Bölgesi Örneği.* Yayımlanmış Yüksek Lisans Tezi. Kara Harp Okulu. Ankara.

The Amarican Heritage Dictionary of The English Language. https://www.ahdictionary.com/word/search.html?q=Intelligence (23.04.2021).

Timisi, N. (2003). *Yeni İletişim Teknolojileri ve Demokrasi* (1.Baskı). Ankara: Dost Kitapevi.

Thinktech STM Teknolojik Düşünce Merkezi. (2019). *Yönlendirilmiş Enerji Silahları: Teknolojiler, Uygulamalar ve Beklentiler. Trent Analizi 2019.* https://thinktech.stm.com.tr/uploads/docs/1608994680_stm-yonlendirilmis-enerji-silahlari.pdf (24.12.2021).

Tiryaki, E. ve Özdal, B. (2020). Açık Kaynak İstihbaratında Sosyal Medyanın Rolünün Analizi. *Academic Review Of Humanities and social Sciences, 3* (2), 267-296.

Tokgöz, O. (1994). *Temel Gazetecilik* (4.Baskı). Ankara: İmge Kitapevi.

Topal, H. (2004). *Siber Terör.* Yayımlanmış Yüksek Lisans Tezi. İstanbul Üniversitesi, İstanbul.

Türk Dil Kurumu. *Yabancı Sözlere Karşılıklar Kılavuzu.* https://sozluk.gov.tr (13.03.2021)

TürkNet. Sözlük. (3.07.2021). *İnternet Nedir?* https://turk.net/destek/sozluk/internet/internet-nedir.html

Ulaştırma ve Altyapı Bakanlığı. *Ulusal Siber Güvenlik Stratejileri ve Eylem Planları.* https://hgm.uab.gov.tr/siber-guvenlik (14.03.2021).

Uludağ, A. (10.07.2017). İçişleri'nden 76 Sayfalık Rapor: IŞİD'liler Yalnız Kurt Eylemi Yapabilir. *Cumhuriyet.* https://www.cumhuriyet.com.tr/haber/icislerinden-76-sayfalik-rapor-isidliler-yalniz-kurt-eylemi-yapabilir-778416 (21.12.2021).

Ulutaş, G. (2018). Siber Güvenlik. Ş. Sağıroğlu ve M. Alkan. (Ed.), *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık* (85-102). Ankara: Grafiker Yayınları.

Ulutaş, U. Ve Hoca, H. (2014). Suriye Devrim Mi, Bölünme Mi? *SETA, Mayıs 2014* (95).

Ünsal, Z.E. ve Olçar, K. (2015). Avrupa'da Radikalleşme ve DAEŞ: DAEŞ'in Evirilmesi ve Avrupa'da Güvenliğine Yönelik Tehditler. *Güvenlik Stratejileri Dergisi,* (29), 115-150.

Viotti, P.R. ve Kauppi, M.V. (2014). *Uluslararası İlişkiler ve Dünya Siyaseti.* (Erozan, A.Ö. Çev.). Ankara: Nobel Akademik Yayıncılık.

Wang, B. (5.09.2018). Navy Seeking High Power Microware Weapons Against Speedboats. *NextBigFuture.com.* https://www.nextbigfuture.com/2018/09/navy-seeking-high-power-microwave-weapons-against-speedboats.html (01.10.2021).

Weimann, G. (2004). *Cyberterrorism: How Real Is the Threat?* United States Institute of Peace Special Report No:119, https://www.usip.org/sites/default/files/sr119.pdf (13.05.2021).

Weimann, G. (2017). *How Modern Terrorism User the Internet.* Whashington DC: United States Institute of Peace, Special Report 116. https://www.usip.org/sites/default/files/sr116.pdf (22.12.2021).

Wilkinson, P. (1975). *Political Terrorism* (5.Baskı). New York: Macmillan.

Wilkinson, P. (2002). Terör ve Terörizm. C. Güzel. (Ed.). *Silinen Yüzler Karşısında Terör* (142-162). Ankara: Ayraç Yayınları.

Yağmurlu, A. (4.07.2021). *Kamu Diplomasisi ve İnternet Kullanımı.* https://acikders.ankara.edu.tr/mod/resource/view.php?id=90551

Yaman, D. (2006). NATO'nun Yeni Görevi: 'Terörizmle Mücadele' ve Bu Eksende Atılan Adımlar. *Uluslararası Hukuk ve Politika, 2* (7), 41-53.

Yayla, A. (1990). Terörizm: Kavramsal Bir Çerçeve. *Ankara Üniversitesi SBF Dergisi, 4* (1), 9-14.

Yazıcıoğlu, Y. (11.05.2016). Erdoğan: 'Türkiye 3 Bin IŞİD'liyi Öldürdü'. *Amerikaninsesi.com.* https://www.amerikaninsesi.com/a/erdogan-turkiye-3-bin-isid-liyi-oldurdu/3324862.html (25.12.2021).

Yenal, S. (2013). *İsrail'in Penceresinden Irak Savaşı* (1.Baskı). Ankara: Barış Kitap.

Yenal, S. ve Akdemir, N. (2020). Uluslararası İlişkilerde Yeni Bir Kuvvet Çarpanı: Siber Savaşlar Üzerine Bir Vaka Analizi. *ÇAKÜ Sosyal Bilimler Enstitüsü Dergisi, 11* (1), 414-450.

Yenal, S. ve Begenirbaş, M. (2019). Değişen Terörizm Konseptinde Latin Amerika ülkelerinde Terörizmin Değerlendirilmesi. *Kara Harp Okulu Bilim Dergisi. 29* (2), 203-227.

Yeniakit. (2020). *Bulut Teknolojisi.* https://www.yeniakit.com.tr/haber/bulut-teknolojisi-1426378.html (10.07.2021).

Yeniman, E. (2018). Bilişim Sistemlerine Yönelik Siber Saldırılar ve Siber Güvenliğin Sağlanması. *Mesleki Bilimler Dergisi, 7* (2), 24-33.

Yeşiltaş, M. (2015). *Apokaliptik, Jeopolitik, Radikal, Antagonizma ve IŞİD.* ORSAM, 7(71), 64-66.

Yılmaz, B.A. (2020). Siber Terörizm ve Değişen İstihbarat Anlayışı. *Anadolu Stratejisi Dergisi, 1* (1), 65-81.

Yılmaz, S. ve Salcan, O. (2008). *Siber Uzay'da Güvenlik ve Türkiye* (1.Baskı). İstanbul: Milenyum Yayınları.

Yönem, A. (2013). Ortadoğu'nun Geleceği Açısından Şii-Sünni İlişkileri Sempozyumu. *Çanakkale On sekiz Mart Üniversitesi İlahiyat Fakültesi Dergisi,* (3), 121-129.

Zafer, H. (1996). *Sosyolojik Boyutlarıyla Terörizm* (1. Baskı). İstanbul: Beta Yayınevi.

3713 Sayılı Terörle Mücadele Kanunu. (1991). *T.C. Resmî Gazete, 20843*, 12 Nisan 1991.