ANASAM
ANADOLU
STRATEJİ DERGİSİ
Journal of Anadolu Strategy

# Siber Terörizm ve Değişen İstihbarat Anlayışı

## Cyber Terrorism and Changing Intelligence

***Birkan Anıl Yılmaz****

**Başvuru Tarihi:** 15.01.2020
**Kabul Tarihi:** 28.02.2020

**Özet**
Günümüzde devletlerin güvenlikleri açısından siber uzaya bağımlı hale geldiği düşünüldüğünde bu bağımlılığın ciddi bir risk ortamını da beraberinde getirdiği görülmektedir. Buradaki risk, simetrik ve tek boyutlu değil, asimetrik ve çok boyutludur. Dolayısıyla gerek düşman tanımlarında gerekse de dünyadaki tehdit algılamalarında önemli değişimler yaşanmıştır. Bu değişimlerle birlikte teröristler saldırmak için bombalara, uçaklara, silahlı ordulara ihtiyaç duymamaktadır. Teröristlerin siber taarruzlar neticesinde klasik bir terör saldırısı gibi toplumda korku ve dehşet ortamı oluşturacakları öngörülmektedir. Siber teröristlerin bilişim sistemlerini kullanarak birçok ülkenin enerji sistemlerinin kullanımını engelleyebilecekleri, baraj kapaklarını açabilecekleri, hava trafik kontrol sistemlerini ele geçirerek uçak kazalarına neden olabilecekleri ya da gıda fabrikalarının karışım oranlarını ele geçirerek karışım oranlarını değiştirebilecekleri ve böylece kitlesel ölümlere yol açabilecekleri iddia edilmektedir. Dolayısıyla istihbarat da ülke güvenliğinden, ekonomi, uzay, siber-uzay ve diplomasinin örtülü faaliyetlerle desteklenmesine kadar geniş bir alanda değişmektedir. Çalışma, yaşanan teknolojik gelişmelerin istihbarat anlayışını nasıl değiştirdiğini ortaya koymaktadır. Bu bağlamda çalışma yöntemi olarak literatür taraması yapılmış ve incelenen örnek olaylarla siber terörizmin istihbarat anlayışına yeni bir boyut kazandırdığı sonucuna ulaşılmıştır. Bu bakımdan siber uzayın getirdiği imkanlar ve dünyadaki tehdit unsurlarının değişiminin, istihbarat faaliyetlerine de etki ettiği savunulmuş ve istihbaratın tüm imkanlarının da bu gelişmelerle birlikte evrim geçirdiği sonucuna varılmıştır.

**Anahtar Kelimeler:** Siber Uzay, Siber Terörizm, İstihbarat

**Abstract**
Nowadays; considering that states have become dependent on cyberspace for their security, this dependence seems to bring with it a serious risk environment. The risk is asymmetrical and multidimensional, not symmetrical and one-dimensional. Therefore, there have been significant changes both in the definitions of enemies and in the perceptions of threats in the world. With these changes, terrorists do not need bombs, planes, armed armies to attack. As a result of cyber attacks, terrorists are expected to create an atmosphere of fear and terror

* Anadolu Üniversitesi Siyaset Bilimi ve Uluslararası İlişkiler Doktora Programı Öğrencisi, **birkananilyilmaz@gmail.com**, ORCID: 0000-0002-5808-3369

in society like a classic terrorist attack. It is claimed that cyber terrorists can block the use of many countries ' energy systems by using information systems, open dam closures, hijack air traffic control systems, cause plane crashes or change mix rates by hijacking food factories and thus lead to mass deaths. Therefore, intelligence varies widely, from country security to economy, space, cyberspace and diplomacy backed by veiled activities. The study reveals how technological developments have changed the understanding of intelligence. In this context, a literature review was conducted as a working method and it was concluded that cyber terrorism has brought a new dimension to the intelligence understanding with the case studies examined. In this respect, it has been argued that the possibilities of cyber space and the change of threatening elements in the world also affect intelligence activities, and it has been concluded that all possibilities of intelligence have evolved with these developments.

**Keywords:** Cyber Space, Cyber Terrorism, Intelligence

## Giriş

Ülkeler teknolojik gelişmeler doğrultusunda uygulamalarını siber uzaya[1] transfer etmek durumunda kalmaktadırlar. Dolayısıyla bu ülkelerin sahip olduğu tüm değerli bilgiler ve veriler siber uzayın bir parçası haline gelmektedir. Bu eksende ülkelerin güvenlikleriyle ilgili risk faktörü olabilecek belge ve veriler de siber uzayda yerini almaktadır (Oğuz, Ceyhan, & Sağıroğlu, 2016: 2). Bu sebeple toplumları terörize eden bir takım saldırılar her geçen gün artış göstermekte, saldırmanın savunmaktan çok daha basit ve maliyetsiz olduğu yeni bir güvenlik alanı ortaya çıkmaktadır.

Soğuk Savaş dönemi sonrasında, gerek düşman tanımlarında gerekse de dünyadaki güvenlik ve tehdit algılamalarında önemli değişimler yaşanmıştır. Bu değişimlerle birlikte "artık hiçbir şey eskisi gibi olmayacak" sözünü doğrularcasına her alanda çok hızlı ve önüne geçilemez bir süreç başlamıştır. Bu süreçte öncelikle askeri olduğu kadar ekonomik, sosyal, dini ya da kültürel, ideolojik, çevresel, toplumsal ve sağlıkla ilgili birçok tehdit unsuru ortaya çıkmıştır. Siber terör de bu dönemde etkili bir araç olarak yerini almıştır. Siber uzayın her ne kadar Soğuk Savaş döneminde var olduğu bilinse de özellikle bu dönemden sonra terörün sıklıkla kullandığı etkili araçlardan biri haline gelmiştir. Bu sebeple yaşanan siber terör örnekleri Soğuk Savaş sonrasında artış göstermiştir. Siber terörün kendi içerisindeki boyutsal nitelik ile uzayda yapılan çalışmalar, insanların sosyal hayatta yaşadıkları her alanı içerisine dahil etmiştir.

Bilişim sistemlerinin ve siber alemin toplumun tüm kesiminde kullanılıyor olmasına paralel bir şekilde, kamu kurumlarında da bu teknolojiler yaygınlaştırılmıştır. Bu bağlamda istihbarat birimlerinin de bilişim teknolojilerinden yoğun olarak faydalandıkları şüphesizdir. Bilişim teknolojilerine ulaşmak maksadıyla yarış içinde olan devletler ve/veya değişik örgütlenmeler de istihbaratlarında ciddi değişimlere gitmektedirler. Bu değişimlerde günümüz ordularının operasyonel üstünlükleri dikkate alınırken harp silah araçları ve komuta-kontrol sistemlerinin yanı sıra elektronik harp kabiliyetleri ile görüntü alma, uzaktan algılama gibi İstihbarat Gözetleme Keşif unsurlarının ve uzayın daha etkin kullanımının çok önemli olduğu görülmektedir (Bayraktar, 2015: 121).

ABD ve Çin arasında geçen ticaret savaşlarının arka planında ciddi bir istihbarat dönüşümünün varlığı göze çarpmaktadır. Şöyle ki; Soğuk Savaş dönemindeki istihbarat anlayışında düşmanı bulmak kolay, yok etmek

1 Elektronik cihazların birbirine bağlı sistemler ve alt yapı aracılığıyla bilgiyi kullandığı operasyonel alan.

zordu. Fakat günümüzdeki terör algısıyla birlikte bu durumun düşmanı bulmak zor, yok etmek kolay olarak evrildiği görülmektedir. Dolayısıyla Çin ve ABD rekabetinde istihbaratın çok boyutlu olarak değişimi dikkate değerdir.

Çalışma, yaşanan teknolojik gelişmelerin istihbarat anlayışını nasıl değiştirdiğini ortaya koymaktadır. Ayrıca literatürde terör ve terörizm üzerine birçok çalışma yapılmasına karşın siber terörizm üzerine yeterli çalışma yapılmaması araştırmanın çıkış noktasını oluşturmaktadır. Bu bağlamda çalışma yöntemi olarak literatür taraması yapılmış ve incelenen örnek olaylarla siber terörizmin istihbarat anlayışına yeni bir boyut kazandırdığı sonucuna ulaşılmıştır. Bu bakımdan siber uzayın getirdiği imkanlar ve dünyadaki tehdit unsurlarının değişiminin, istihbarat faaliyetlerine de etki ettiği savunulmuş ve istihbaratın tüm imkanlarının da bu gelişmelerle birlikte evrim geçirdiği sonucuna varılmıştır.

## Siber Uzay

1990'lı yıllarda insanlığın geldiği nokta akıl almaz bir hızla ilerlemekte, ürün pazara sunuluncaya kadar güncelliğini kaybetmektedir. Bu ilerlemedeki en temel etken ise doğru bilgiye zamanında erişim ve bu bilginin etkin kullanımıdır (Keleştemur, 2015: 128). Kuehl, elektronik cihazların birbirine bağlı sistemler ve alt yapı aracılığıyla bilgiyi kullandığı operasyonel alanı, siber uzay olarak tanımlamaktadır. Siber kavramı ise bilgi-teknoloji alt yapısının birbirine bağlı ağı anlamına karşılık gelmektedir. Siber uzay veya siber ortam, elektronik ve elektromanyetik spektrumun oluşturduğu çeşitli verileri depolamak için tasarlanan küresel bir etki alanıdır. Siber, bilgi iletişim teknolojilerini kullanarak birbirine bağlantılı ağlar aracılığıyla bilgiyi değiştirebilmekte ve kullanabilmektedir (Kuehl, 2009 :3). Yani telefon, radyo, televizyon gibi elektronik olarak kumanda edilebilen her türlü cihaz, kayıt edilebilen ses ve görüntüler, grafikler, projeler, banka işlemleri, e-ticaret, e-devlet üzerinden yapılan tüm işlemler de siber uzay tanımlamasının içinde yer almaktadır (Yılmaz, 2017: 28).

Siber uzay, uluslararası alanda güncel meselelerin yer aldığı dört fiziksel boyuta (kara-deniz-hava-uzay) insanlar tarafından üretilmiş ve eklenmiş beşinci bir boyuttur denilebilir. Nitekim 2016 Varşova Zirvesi'nde NATO tarafından operasyonel bir alan olarak resmen tanınmış bulunmaktadır. ABD siber komutanlığı, siber uzayı yeni bir savaş alanı olarak tanımlamıştır. FBI ise üç önceliğini terörizm, casusluk ve siber saldırılar olarak belirlemiştir (Çelik, 2018: 115).

Siber uzay, devletlerin güvenlikleri açısından her geçen gün daha büyük bir risk haline gelmektedir. Buradaki risk, simetrik ve tek boyutlu değil, asimetrik ve çok boyutludur. Diğer bir deyişle, sınırları belli olan ve uluslararası hukuk normları tarafından büyük ölçüde kontrol altına alınmış sistemde, konvansiyonel güvenliğin yerine sınırları belli olmayan, anonimliğin hüküm sürdüğü, saldırmanın savunmaktan çok daha basit ve maliyetsiz olduğu yeni bir güvenlik alanı ortaya çıkmaktadır (Ermiş, 2018: 6). Kara ve denizde baskın güce sahip olan devletler benzer şekilde siber uzayda yeterli kapasiteye sahip olamamaktadır. Aksine daha küçük veya devlet dışı aktörler siber uzayı asimetrik bir boyutla çok daha etkin bir şekilde kullanabilmektedir (Çelik, 2018: 116). Dolayısıyla birçok devlet siber uzaya yönelik güvenlik politikalarına yer vermek durumunda kalmışlardır. Bu anlamda devletler özellikle bu politikaları hayata geçirmek adına, kalifiye ordular oluşturmak ve alt yapı hizmetleri sağlamak gibi büyük yatırımlar yapmaktadırlar (Yılmaz, 2017 :31).

Siber uzay alanında sistemleşen devletlerin, rakiplerine karşı kolaylıklar kazandığı söylenebilir. Fakat Kshetri'ye göre siber; devletlere, rakipleri karşısında kolaylıklar sağlarken aynı zamanda alt yapı sistemini siber alana entegre eden devletleri savunmasız bırakmaktadır. Bu özelliğiyle de "iki ucu keskin bir kılıç" olarak ifade edilmektedir (Kshetri,2014:5).

Gelişen bilişim sistemleriyle birlikte hem devletler hem de devlet dışı aktörler için yeni tehditler ortaya çıkmaktadır. Fakat buradaki tehditlerin soyut bir alandan geliyor olması ve tespit edilebilme özelliğinin az olması, tehditlerin sonuçları açısından bir öngörülmezlik durumu oluşturmaktadır. Diğer yandan bu tehditlerin merkezi bir yapıya sahip olmaması da belirsizliği artırmaktadır. Bu bağlamda tehdidin kaynağı tek bir birey, birey toplulukları, terör örgütleri veya devletler de olabilmektedir. Dolayısıyla siber uzay devletlerin hem birbirleriyle yarışacağı hem de birbirlerinden, terör örgütlerinden ve hatta bireylerden gelebilecek tehditleri bertaraf etmeleri gereken yeni bir durum yaratmaktadır (Yılmaz, 2017: 24-29).

Değişen dünya sistemiyle birlikte "artık hiçbir şey eskisi gibi olmayacak" sözünü doğrularcasına her alanda çok hızlı ve önüne geçilemez bir süreç başlamıştır. Bu süreçte öncelikle askeri olduğu kadar ekonomik, sosyal, dini ya da kültürel, ideolojik, çevresel, toplumsal ve sağlıkla ilgili birçok tehdit unsuru ortaya çıkmıştır. Siber terör de bu dönemde etkili bir araç olarak yerini almıştır. Siber terörün kendi içerisindeki boyutsal nitelik ile uzayda yapılan çalışmalar, insanların sosyal hayatta yaşadıkları her alanı içerisine dahil etmiştir (Güntay, 2017: 17).

**Siber Terörizm**

Günümüzde çok sık kullanılmasına rağmen hangi tür eylemlerin "siber terörizm" kavramına dahil olacağı konusunda bir uzlaşı mevcut değildir. Siber uzay ve terörizm terimlerinin birleştirilmesiyle yeni bir kavram olarak ortaya çıkan siber terörizm, ilk olarak 1980 yılında Güvenlik ve İstihbarat Enstitüsü(Institute for Security and Intelligence) araştırmacılarından Barry Collin tarafından kullanılmıştır. Collin'e göre siber terörizm korkusunun oluşmasının altında yatan neden; dönemin iki önemli korkusu olan bilgisayar teknolojilerine olan güvensizlik ve teknolojik araçlardan mahrumiyet endişesidir (Collin, 1996).

Siber terörizm kavramını anlayabilmek için öncelikle terör ve terörizm kavramını açıklamak faydalı olacaktır. Terör ve terörle ilgili kavramları tanımlarken tek ve genel kabul görmüş bir tanımlamadan bahsetmek oldukça güçtür. Dolayısıyla farklı unsurları içeren tanımlamalarla karşılaşmak olasıdır. Terör ve terörizm kavramları toplumdan topluma, hükümetten hükümete, bazen de yazardan yazara farklı biçimlerde tanımlanmaktadır. Lakin terör; herkese, her şarta ya da bölgelere göre değişim gösteren bir olgu anlamına gelmemektedir. Burada belirtilmek istenen; terör kavramının sınırlarının çizilmesinin zor olması ve evrensel olarak kabul edilen bir tanımlamaya henüz ulaşılamamış olmasıdır (Çınar, 1997: 197).

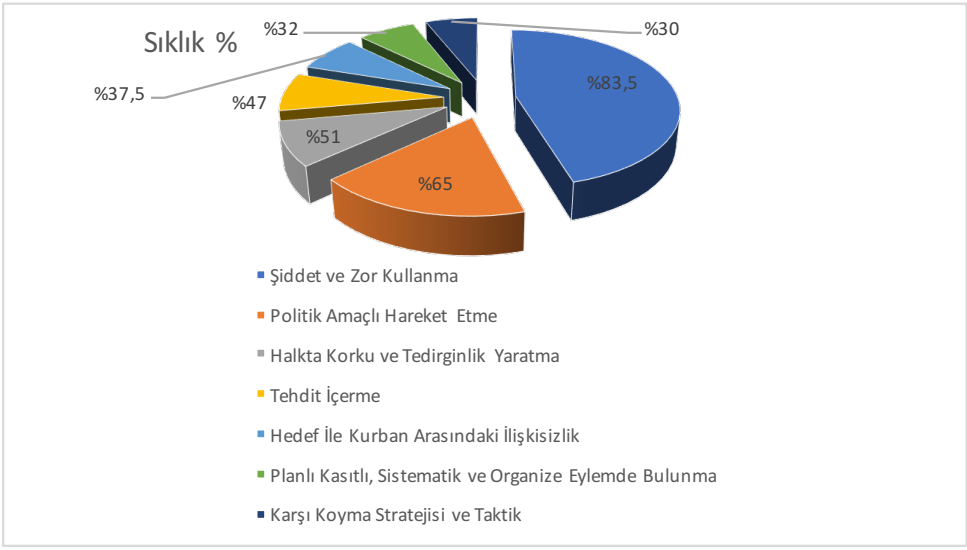
12 Nisan 1991 tarihinde 3713 sayılı Terörle Mücadele Kanunu'nda Terör: "*Cebir ve şiddet kullanarak; baskı, korkutma, yıldırma, sindirme veya tehdit yöntemlerinden biriyle, Anayasa'da belirtilen Cumhuriyet'in niteliklerini, siyasî, hukukî, sosyal, laik, ekonomik düzeni değiştirmek, Devletin ülkesi ve milletiyle bölünmez bütünlüğünü bozmak, Türk Devleti'nin ve Cumhuriyet'in varlığını tehlikeye düşürmek, Devlet otoritesini zaafa uğratmak veya yıkmak veya ele geçirmek, temel hak ve hürriyetleri yok etmek, Devletin iç ve dış güvenliğini, kamu düzenini veya genel sağlığı bozmak amacıyla bir örgüte mensup kişi veya kişiler tarafından girişilecek her türlü suç teşkil eden eylemlerdir.*" şeklinde tanımlanmıştır (Terörle Mücadele Kanunu, 1991). ABD Savunma Bakanlığı terörü, toplumları ve hükümeti korkutmak ya da zorlamak amacıyla kanunsuzca şiddet kullanmak veya şiddetle tehdit etmek olarak tanımlamıştır (U.S. Depertment of State, 2009). Fransa Terörle Mücadele Kanunu ise terörü baskı veya tehdit yoluyla, mevcut kamu düzeninin ciddi olarak bozulması amacıyla bireysel veya toplu olarak herhangi bir faaliyette bulunulmasıdır şeklinde tanımlamıştır (France Law on The Fight Against Terrorism, 1986).

Tanımlamalardan da yola çıkılarak hem batı dillerinde hem de Türkçede terörün korku içerdiğini söylemek mümkündür. Buradaki korku sıradan bir korku değil bir korku durumunu ifade etmektedir. Bu durumu açık-

layabilmek için Türkçede daha yoğun kavramlar da kullanılmıştır. Dehşet kavramı burada örnek olarak verilebilir. Fakat terör kavramının çağrıştıracağı rahatsızlıkları en aza indirebilmek için birçok kişi şiddet kavramını kullanmayı seçmiştir. Yani daha yumuşak bir şekilde ifade etmek için şiddet kavramının kullanılması terörün alternatifi gibi düşünülse de aynı anlamı taşımadığı açıktır. O halde terörün şiddet içerdiği ancak bundan çok öte bir şey olduğu söylenebilir (Cirhinlioğlu, 2004 :23-24).

Terörizm kavramı ise terör yöntemlerinin siyasi bir amaçla örgütlü, sistemli ve sürekli bir şekilde kullanılmasını benimseyen bir strateji olarak, terör kavramından ayrılmaktadır. Her ne kadar terör ve terörizm kavramları aynı kökten türetilmişse de anlam bakımından farklılık göstermektedirler. Nitekim terör terimi, korku ve şiddeti çağrıştırırken, terörizm bu kavrama süreklilik ve siyasal içerik katmaktadır. Bu bağlamda terörizm topluma karşı siyasal amaçlı şiddet kullanımını ifade eder (Gül, 2012: 9). Genellikle "–izm" ile biten ifadeler ideolojileri çağrıştırsa da burada terörizmden kast edilen bir ideolojiden çok bir olgusal durumdur. Bir başka deyişle terör kavramı özeli/olayı, terörizm kavramı ise geneli/olguyu dile getirmektedir denilebilir (Cirhinlioğlu, 2004 :25).

Schmid ve Jongman'ın "Politik Terörizm" adlı eserlerinde, terör alanında uzman akademisyenlerin araştırmalarında 109 farklı terörizm tanımı yapıldığına dikkat çekilmiştir (Schmid ve Jongman, 2005: 6). Bu tanımlarda ortak olarak belirlenen unsurlar aşağıdaki grafikte gösterilmiştir.




Kaynak: Schmid, A. P., & Jongman, A. (2005). *Political Terrorism.* Transaction Books, s,5.

***Grafik 1. 109 Farklı Terörizm Tanımında Yer Alan Unsurlar***

21. yüzyılda artan internet kullanımıyla, bilgi ve iletişime dayalı oluşumlara karşı ortaya çıkan tehdit; siber terörizmdir. Bir başka deyişle bilgi tabanlı ekonomi, bilgi toplumu, e-devlet, FTP tarzı örgütlenmeler, uluslararası sivil toplum kuruluşları düzeni temsil ederken siber terörizm bu düzene karşı bir tehdidi temsil etmektedir (Terzi, 2018: 89). Amerikan kaynaklı küresel medyada siber terörizm kavramının çoğunlukla yanlış olarak kullanıldığı söylenebilir. Siber terörizmin tehdit potansiyelini anlayabilmemiz için öncelikle terimi doğru bir şe-

kilde tanımlamak gerekmektedir. Siber terörizm, siyasi ve sosyal mercilere, kişi ve kurumlara göz dağı vermek, baskı oluşturmak amacıyla resmi kuruluşların bilgisayarlarına, network sistemlerine, bilgi ve veri tabanlarına yapılan yasadışı tehdit ve zarar verici saldırılardır. Üzerinde durulması gereken önemli noktalardan biri de bir saldırının siber terörizm olarak tanımlanması için bireye ya da mala karşı şiddet içermesi ve/veya en azından korku yaratacak kadar hasara yol açması gerekmektedir. Ülkelerin kritik alt yapı sistemlerine yapılan saldırılar da, yarattığı etkiye göre, siber terörizm olarak tanımlanabilir (Sandıklı ve Yivciger, 2004: 5).

Siber terörizmin amacı, bilgisayar ağlarını kullanılamaz hale getirmeye yönelik istemli olarak yapılan, geniş kapsamlı eylemleri de içerisinde barındırmak üzere, terör eylemlerinde internete bağlı kişisel bilgisayarları kullanmak ve internet tabanlı saldırılar yapmaktadır. Fakat burada belirli bir birikime sahip olmak gerektiği belirtilmiş olsa da sosyal ağlar üzerinden yapılan, terörü destekleyen faaliyetler de siber terörizmin kapsamı içine girmektedir. Şöyle ki gerçek hayatta teröre destek vermek, teröristlere yardım ve yataklık etmek nasıl bir terörizm faaliyetiyse, sosyal medyada terörizm adına propaganda yapmak da siber terörizm faaliyeti olarak kabul edilmektedir (Keleştemur, 2015: 161).

Siber saldırı yönteminin terör grupları tarafından kullanılmasının en önemli nedenlerinden biri saldırıyı düzenleyen kişilerin takip edilmesinin oldukça zor olmasıdır. Siber saldırı yöntemi, gerçek dünyada meydana gelen saldırı yöntemlerine göre daha anonim bir kimlikle yapıldığı için saldırıyı düzenlemekte olan gruplar bir gümrük noktası veya havaalanı kontrolünden geçmeden hedef ülkeye ulaşabilmektedirler. Diğer bir yandan saldırı düzenleyecek hedef sayısı oldukça fazladır. Dolasıyla terör grupları fiziki eğitim veya ölüm riski bulunan konvansiyonel saldırılar yerine siber saldırıları benimsemektedirler. Bu sayede saldırıları düzenleyecek adamları kiralama ya da yetiştirme konusunda da sıkıntı çekmemektedirler (Gürkaynak ve İren, 2011: 267). Örneğin internet üzerinde bulunan tartışma gruplarında önemsiz görülen bazı mesaj veya resimlerin teröristler arasındaki bir iletişim biçimi olarak kullanıldığı görülmektedir. Bu durum bilginin bilgi içinde gizlendiği steganografi gibi teknikler kullanılarak gerçekleştirilmektedir (Çetinkaya, 2011). Teröristlerin adam bulma ve iletişime geçme konusunda bu gibi kolay yöntemleri kullandıkları söylenebilir.

Siber terörizmin radikal faaliyetlerle teknoloji arasında bir kesişme noktası olarak kaldığı söylenebilir. Şöyle ki geçmişte düşman tanımlanabiliyor ve/veya coğrafi olarak yeri tespit ediliyor, hapsediliyor ve yok edilebiliyordu. Fakat günümüzün teknolojisiyle terör faaliyeti yapan düşmanı ayırt edebilecek keskin sınırlar bulunmamaktadır. Bu haliyle terörizmin daha tehlikeli olduğu, teröristlerin saldırmak için bombalara, uçaklara, silahlı ordulara ihtiyaç duymadıkları söylenebilir. Dolayısıyla bir ülkenin belki de bir kıtanın politik ve askeri kaynaklarını barındıran ve hayati önem taşıyan sistemlere, güç kaynaklarına ve hava trafiklerine saldırı imkanı doğmaktadır (Yonah & Swetman, 2000: 4). Teröristlerin siber taarruzlar neticesinde klasik bir terör saldırısı gibi toplumda korku ve dehşet ortamı oluşturacakları öngörülmektedir. Siber teröristlerin bilişim sistemlerini kullanarak birçok ülkenin enerji sistemlerinin kullanımını engelleyebilecekleri, baraj kapaklarını açabilecekleri, hava trafik kontrol sistemlerini ele geçirerek uçak kazalarına neden olabilecekleri ya da gıda fabrikalarının karışım oranlarını ele geçirerek karışım oranlarını değiştirebilecekleri ve böylece kitlesel ölümlere yol açabilecekleri iddia edilmektedir (Bayraktar, 2015: 142). Eski istihbarat direktörü Mike McConnell, ABD'nin finansal ve elektrik sistemlerinin savunmalarını kırmak isteyen herhangi bir grup için siber uzayın büyük imkanlar sunduğunu söylemektedir. Böylelikle de bu tür grupların ulus-devletlerden daha büyük bir tehdit haline geleceğine inanmaktadır (Nye, 2010: 12).

### Siber Terör Olarak Kabul Edilen Örnek Olaylar

Günümüzde hala tartışma konusu olarak devamlılığını sürdüren durum hangi tür saldırıların siber terörizm olarak değerlendirileceğidir. Hukukçular, emniyet güçleri, bilişim uzmanları ve teknoloji şirketleri farklı görüş-

leri savunabilmektedir. Literatürde siber suç ve siber terörizm olaylarının birlikte kullanıldığı görülmektedir. Bu bağlamda araştırılan örneklemler de siber suç ve/veya siber saldırılardan ziyade siber terör olaylarına yer vermektedir. Siber terörizm olarak genel kabul gören bazı olaylar şu şekilde sıralanabilir (Sağıroğlu ve Alkan, 2018: 265).

1996 yılında web sitesi kırılması olayında CIA'in gizli dosyalarına girilememiş olsa da sitenin içindeki tüm bilgiler değiştirilmiş ve oldukça büyük bir hasar verilmiştir. Bu olaydan yaklaşık bir ay önce de ABD Adalet Bakanlığı'nın sitelerine erişilmiş ve siteye Adolf Hitler'in fotoğrafı yerleştirilmiştir(Çetinkaya, 2011).

"Tubac Amaru" adlı terör örgütü, 1996 yılında Peru'nun Lima şehrinde Japonya Büyük Elçiliği'ne saldırarak siyasi ve askeri personeli rehin almıştır. Terör örgütünün ABD ve Kanada'da bulunan sempatizanları örgütün faaliyetlerini destekleyen birçok site kurmuşlardır. Bu sitelerde terör lehine propaganda yapılmış ve eyleme destek verilmiştir. Japon büyükelçilik binasına saldırı planları da bu sitelerde yayınlanmıştır(Terzi, 2018: 90).

24 Mart 1999'da NATO genel sekreteri Javier Solona'nın emri doğrultusunda Sırp hedeflerin bombalanmaya başlamasıyla birlikte NATO'ya yönelik siber saldırılar başlamıştır. Kısa süre içerisinde NATO karargahına ve üye ülkelerin askeri haberleşme sistemlerine saldırılar gerçekleştirilmiştir. NATO sunucularının yanında ABD Savunma Bakanlığı'nın alt yapısına yönelik saldırılar da düzenlenmiştir. Bu şekilde NATO sunucu işlemcileri talep veremez hale getirilmiş, ABD savunma ordusu da sistemlerini virüslerden temizleyebilmek için dünyadaki tüm sunucularını bir hafta süreyle kapatmıştır. Saldırıların izleri araştırıldığında Sırpların yanı sıra Rus ve Çinli hackerların da bu saldırılara destek verdiği iddia edilmiştir. Böyle bir durum fiziki dünyadaki ittifakların siber ortamda da devam ettiği şeklinde değerlendirilebilir (Bıçakcı, 2012: 211).

Sovyet ordusunun II. Dünya Savaşı sırasında Alman işgaline karşı verilen mücadelenin anısına dikilen "Tallinn'in Bronz Askeri" adlı Kızıl Ordu Anıtı'nın, Estonya hükümeti tarafından yerinin değiştirilmesi üzerine yaşanan tartışmalar, dünyada ilk kez bir ülkeye yönelik sistematik ve çok taraflı siber saldırılar gerçekleştirilmesine neden olmuştur. Bu saldırılar öncelikle finans merkezleri ve bankalar olmak üzere, parlamentosunu, bakanlıklarını, medya organlarını, güvenlik ve ulaşım alt yapısını hedef almıştır. 27 Nisan-18 Mayıs 2007 tarihleri arasında gerçekleştirilen saldırıların ilk aşamasında siyasi kurumların, güvenlik ve medya organlarının internet siteleri geçici olarak kullanım dışı kalmıştır. Estonya hükümeti saldırılara karşı önlem almaya çalışsa da ikinci aşamada banka ve finans işlemleri de sekteye uğratılmıştır. Dolayısıyla Avrupa'nın en gelişmiş bilgi sistemlerine sahip olan, internet erişiminin temel insan hakkı olduğunu ilan eden ve bilgi sistemlerinin yoğun kullanımından dolayı kendini "E-stonia" olarak tanımlayan bu Doğu Avrupa ülkesinde devlet otoritesi oldukça sarsılmıştır (Bayraktar, 2015: 156).

Siber saldırıların nereden geldiğinin tespit edilmesi bir hayli zor olduğundan bu saldırıların Rusya tarafından yapılıp yapılmadığı da belirlenememiştir. Fakat Rusya'da ki internet sitelerinde Estonya internet sitelerinin nasıl çökertileceğine ilişkin bilgilerin yer alması dikkat çekicidir (Bayraktar, 2015: 157).

2014 yılında Ukrayna'da internetin kesintiye uğraması ile Rusya taraftarlarının Kırım'ın kontrolünü ele almasını destekleyen ve Rusya kaynaklı olduğu iddia edilen bir saldırı olmuştur. Akabinde Ukrayna Cumhurbaşkanlığı seçimi öncesi, seçim komisyonu sistemi hedef alınmış ve işlevsiz hale getirilmesi için birçok saldırı düzenlendiği iddia edilmiştir. Yine 2014 yılında 500 milyon "Yahoo" kullanıcısının şifreleri çalınmıştır. Yahoo sadece şifrelerin değil kişisel bilgiler ve gizli soru cevaplarının da çalındığını kabul etmiştir. Bu olaydan çok kısa bir süre öncede MySpace'in 359 milyon, LinkedIn'in 159 milyon ve Adobe'un 152 milyon kullanıcı bilgisi çalınmıştır (Sağıroğlu ve Alkan, 2018: 266-267).

2016 yılında Siber saldırganlar, Ukrayna'daki üç bölgesel elektrik şirketine saldırılar düzenlemiştir. Toplamda 225 bin kullanıcının elektrikleri kesintiye uğramıştır. Saldırı aynı zamanda telefon hatlarını da kullanılamaz hale getirmiştir (Sağıroğlu ve Alkan, 2018: 267).

2017 yılında dünya genelinde devlet daireleri ve hastaneler WannaCry isimli fidye yazılımından dolayı oldukça hasar almıştır. Virüsün çalışma şekli ele geçirdiği dosyaların fidye karşılığında iadesini sağlamaktır. Virüsün 99 ülkede 75 bin civarında saldırısı rapor edilmiştir (Sağıroğlu ve Alkan, 2018: 267).

TSK'nın 20 Ocak 2018'de gerçekleştirdiği Zeytin Dalı Harekatı sonrasında terör bağlantılı veya motivasyonlu saldırgan gruplar tarafından #OpTurkey etiketi ile Türkiye Cumhuriyeti'nin kamu kurum ve kuruluşlarına siber saldırılar düzenlenmeye başladığı belirlenmiştir. Saldırıların en temel amacının harekat süresince zemin kaybeden terör örgütlerinin, TSK'nın sahip olduğu üstünlüğü sabote etme, kitleleri tahrik etme ve algı yanılması oluşturmaya çalıştıkları değerlendirilmektedir. #OpTurkey olarak başlatılan saldırılarda yoğunluklu olarak sahte haber üretme, propaganda yapma ve kamu kurum ve kuruluşlarına siber saldırı gerçekleştirme faaliyetleri yürütülmektedir. Saldırı sonuçlarına göre mesaj ve propaganda cümlelerinin birebir terör örgütlerinin mesaj ve paylaşımları ile örtüştüğünü bu durum da saldırıların tamamının Zeytin Dalı Harekatı'na tepki olarak yapıldığını kuvvetlendirmektedir. Süreç bazında saldırıyı gerçekleştiren gruplar dışında sosyal medyada da propaganda mesajlarının paylaşıldığı tespit edilmiştir. Dolayısıyla söz konusu unsurların sosyal medyayı haber ve ifşa ortamı olarak kullandıkları söylenebilir (STM, 2018: 6).

Siber saldırı özelinde verilen siber terörizm örneklerinin uluslararası düzeyde kapsamlı bir tanıma ihtiyacı olduğu görülmektedir. Zira Estonya örneğinde görülen banka ve finans sistemlerine yapılan saldırının, Rusya'nın saldırısı olarak mı yoksa yasa dışı bir örgüt saldırısı olarak mı değerlendirileceği netlik kazanmamaktadır (Terzi, 2018: 92).

WannaCry örneğinde saldırganların para temin etme isteği siber suç olarak değerlendirilebilmekle birlikte, internet ve bilgisayar kullanıcıları üzerinde yarattığı korku ve sistemlerin çalışmamasını sağlaması gibi sebepler de siber terörizm olarak değerlendirilebilmektedir. Bu durum da siber uzayın getirmiş olduğu siber terörizm olgusunu daha sofistike hale getirmekte ve zorlaştırmaktadır. Her siber suç, siber terörizm olarak görülmese de her siber terörizm faaliyetinin siber suç olarak değerlendirilebileceği söylenebilir (Sağıroğlu ve Alkan, 2018: 268). Diğer bir yandan bu saldırıların artışı ve bıraktığı hasarların maliyetleri de çok ciddi boyutlardadır. New York Times 2007'de iç güvenlik bakanlığına tahmini, 37 bin girişim özel ve devlet bilgisayar sistemi ihlali ve Pentagon sistemlerine 80 binden fazla saldırı kaydettiğini ileri sürmektedir (Bruno, 2008). ABD merkezli Cyber Security Ventures'in araştırmasına göre bu saldırıların maliyeti; 2007 yılında 100 milyar dolar, 2008 yılında 140 milyar dolar, 2015 yılında 3 trilyon dolardır. 2021 yılında ise dünya ekonomisine toplam maliyetinin 6 trilyon dolara çıkması öngörülmektedir (Cyber Security Ventures, 2017).

Siber uzayın tartışıldığı ve konumlandığı alanda, artık siber müdahale araçları olarak siber saldırı yöntemleri geliştirilmiştir. Siber saldırıların yapılmasına ilişkin verilerin toplanması ve bunların politik boyuta taşınmasıyla beraber, siber istihbarat dediğimiz bir çalışma alanı ortaya çıkmış ve bu alanda nitelikli personele ihtiyaç duyulmaya başlanmıştır. Siber saldırıların hazırlık ve savunma aşamalarına ilişkin konularda ise devletler bazen iş birliği içerisinde hareket ederken, bazen de kendi kabiliyetleri ve öz imkanları doğrultusunda bu alanda etkili olmaya çalışmaktadır (Güntay, 2018: 82).

**İstihbarat Tanımları**

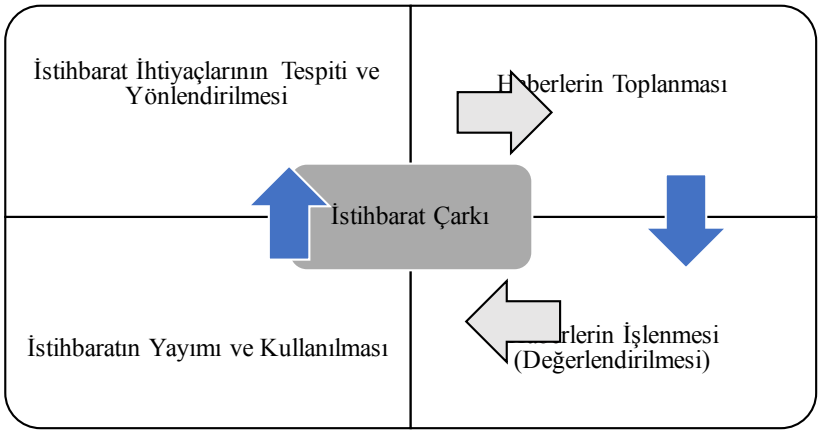
Warner istihbaratı en genel manada; önceden bilinmesi gereken tüm konular üzerine bilgi toplanması ve kullanıma hazır hale getirilerek uygulama kapasitesi kazandırılması şeklinde tanımlamıştır (Warner, 2002: 15). Shulsky ise istihbaratın iki görüşünü öne sürmektedir. Öncelikle, Sun Tzu'nun M.Ö. 6.yy'dan kalma yazılarından yola çıkarak istihbaratın savunuculuğunu öne çıkartan "geleneksel görüşe" önem vermektedir. Bu bağlamda askeri ya da ulusal güvenlik olarak milletler arasındaki "sessiz savaşın" rakiplerin sırlarını toplamaya ve analiz etmeye bağlı kalmasını ve açık kaynak bilgilerine erişilebilir durumlarla ilgilenilmemesi gerektiğini belirtmektedir (Shulsky, 2001). Minix ve Hawley de istihbaratta toplanan bilgilerin doğru ve güncel olmasına değinmektedir. Çünkü karar vericilerin eline geç düşen istihbarat, istihbarat değildir. İstihbarat hem kalite hem de zamanlamayı gerektirir (Minix ve Hawley, 1998: 326).

İstihbarat tanımının dönemlere ve tanımlayanların bakış açılarına göre şekillendiği söylenebilir. Tanımlanan istihbarat kavramlarında bilginin ön plana çıktığı görülmektedir. Bu bağlamda daha geniş çaplı bir tanımlama yapan Bimfort'a göre istihbarat; bir ülkenin dış politika ve milli güvenlik stratejileri doğrultusunda ülkeler hakkında bilgi toplamak ve işlemek, politika uygulayıcılarına yardımcı olmak hususunda devrede tutulan ve bu bağlamda girdi–çıktıların, kişilerin–organizasyonların ifşa olmaması sürecine yönelik yapılan çalışmalar şeklinde ifade edilmiştir (Bimfort, 1958: 75-78).

İstihbarat kavramı üzerine yazılan hemen hemen her kitap ve/veya makalede istihbaratın ne anlama geldiği sorunu ya da en azından bu kavramla ilgili farklı tartışmaların yaşandığı göze çarpmaktadır. Dolayısıyla istihbarat tanımının neden bir sorun haline geldiğine değinmek faydalı olacaktır. Öncelikle birçok araştırmacı için istihbaratın "bilgi" olarak algılandığı gözlemlenmektedir. Fakat bilgi ve istihbarat arasındaki ayrım büyük önem taşımaktadır. Şöyle ki bilgi, nasıl keşfedildiğine bakılmaksızın, bilinen bir şeydir. İstihbarat ise politika yapıcılarının istekleri doğrultusundaki ihtiyaçlarını karşılayan ve bu ihtiyaçları karşılamak için toplanmış, işlenmiş ve daraltılmış bilgileri ifade etmektedir (Lowenthal, 2006). Bu ayrımı Yom Kippur Savaşı'ndaki istihbarat-bilgi ve noktaları birleştirme problemiyle desteklemek yerinde olacaktır.

"1973 sonbaharında Mısır Ordusu Süveyş Kanalı boyunca uçaksavar ve topçu pozisyonlarını hazırladılar. Bölgeye binlerce yedek asker çağıran ve büyük bir askeri müdahale niteliğinde Doğudan saldıran ordular Golan Tepesi'ndeki İsrail'in tüm savunma kuvvetlerini bombaladılar. İsrail askeri istihbarat başkanı ve üst düzey yetkililer tüm bilgileri toplamalarına rağmen sürpriz bir şekilde bu durumla karşılaştıklarını bildirdiler." Dolayısıyla tüm bilgilerin toplanmasına rağmen Yom Kippur Savaşı'nın neden önlenemediğini İsrail istihbarat başkanı şu şekilde dile getirmiştir. 1971 yılında Mısır Cumhurbaşkanı savaş saatinin yaklaştığını açıkça belirtmiştir. Tüm hazırlıklarının gerçekleştirilmesine ve saldırı pozisyonlarına rağmen hiçbir şey olmamıştır.1972 yılında aynı şekilde Mısırlılar harekete geçmiş, tanklar ve köprüleme ekipmanları kurulmuştur. Fakat yine hiçbir şey olmamıştır.1973 yılına kadar neredeyse her gün Mısır ordusunun hazırlanmasına yönelik bilgi akışları istihbarat servislerince toplanmıştır. İstihbarat bu durumun Orta Doğu ülkeleri için rutin bir hale geldiğini ve ciddi bir savaş halinin gerçekleşmeyeceğini öngörmüştür.1973 sonbaharında gelen bilgilerin de dikkate değer olmadığı üst düzey yetkililerce düşünülmüş fakat savaş sürpriz bir şekilde gerçekleşmiştir. Dolayısıyla bilgi ve istihbarat ayrımı son derece önem taşımaktadır (Gladwell, 2003: 83). Bu noktada Milli İstihbarat Teşkilatı'nın tanımıyla olmuş ya da olacak bir olay hakkında toplanılmış bilginin tasnif, kıymetlendirme, yorum ve yayım aşamalarından geçirilerek değerlendirilip işlenmesi hali önem arz etmektedir.

Tüm istihbarat faaliyetleri kesintisiz süren çalışmalardır ve bu manada tüm istihbarat kuruluşları tarafından bir çarka benzetilmektedir.




Kaynak: MİT, 2019; http://www.mit.gov.tr/isth-olusum.html# (E.T. 03.12.2019)

***Şekil 1. İstihbarat Döngüsü***

İstihbarat döngüsüne göre elde edilen haber bilgi ve belgenin belli bir sistematik içerisinde değerlendirilmesi gerekmektedir (MİT, 2019). Önemli bir haber doğru bir şekilde işlenemezse Yom Kippur Savaşı'nın sonuçlarına benzer sonuçlarla karşılaşmak mümkündür. Nitekim noktaları birleştirilmemiş bilginin ya da hatalı birleştirilmiş noktaların, yanıltıcı sonuçlara götürdüğü söylenebilir.

**İstihbaratın Değişimi**

İstihbarat, kökleri çok eski dönemlere uzanmakla birlikte Sun Tzu'nun *Savaş Sanatı,* Thucydides'in *Peloponnesian Savaşının Tarihi*, Machiavelli'nin *Prensi*, Clauswitzn'in *Savaş Üzerine* gibi birçok tarihi yapıtı literatüründe barındırmaktadır. Dolayısıyla istihbarat literatürünün de istihbarat servislerinin dönüşümü gibi tarihselliği kapsadığı söylenebilir (Webb, 2009: 35). İstihbaratın köklü tarihi itibarıyla birçok değişim geçirdiği ve bu bağlamda da çok boyutlu bir çalışma alanına sahip olduğu kabul edilmektedir. Zira istihbarat alanı her yer olabilmektedir. Klasik istihbarat zamanlarında ki yakın tehditler ve/veya komşu ülkelerdeki istihbarat anlayışı yerine, gelişen teknolojiyle birlikte dünyanın her köşesi istihbarat faaliyetlerinin mekanı olmaktadır.

Terörizmin yıkıcı etkiler bırakacak saldırılarının yanında para, silah, bilgi ve doküman transferleriyle ilgilenerek verilere yönelmiş olması istihbaratın karakteristik niteliğini değişime uğratmıştır (Güntay, 2018: 88). Bununla birlikte gelişen teknolojinin, ulusların güvenliğini ve özgürlüğünü doğrudan etkilediği, dünyada gücü belirleyen en önemli unsur haline geldiği çağımızda, teknolojik ve ekonomik istihbarat oldukça ehemmiyetli bir duruma gelmiştir. Eski zamanlarda istihbarat faaliyetleri sadece askeri ve siyasi alanlara yönelirken, günümüzde telekomünikasyondan bilgisayar teknolojisine, taşımacılıktan tekstil endüstrisine, nano teknoloji ile optik alandaki araştırmalara kadar dünyanın her yerini istihbarat faaliyet merkezi haline getirmeye devam etmektedir (Oğuz, Ceyhan, & Sağıroğlu, 2016: 2).

İstihbarat faaliyetlerinin mekanları arttıkça istihbarata konu olan alanların sayısı da paralel olarak artış göstermektedir. Genel olarak istihbaratta; askeri, siyasal, sosyal, ekonomik, bilim ve teknolojik gelişmeler esas alınmaktadır. Konularının fazla olmasıyla birlikte, temel olarak iki tür istihbarat faaliyet şeklinden söz edilmekte-

dir. Birincisi; stratejik istihbarat, ikincisi ise bilgi istihbaratı(taktik istihbarat)'dır. Stratejik istihbaratı, muharebe istihbaratının içinde ele alan araştırmacılar da vardır. Her ne kadar bu konuda farklı görüşlere rastlanılsa da muharebe istihbaratının hem stratejik istihbarat hem de taktik istihbarat içinde yer aldığını görmek mümkündür. Stratejik istihbarat; hedef olarak seçilen birimin güçleri, zafiyetleri, amaçları, politika ve stratejilerinin tespiti ve bu tespite dayanarak yapılan bilgi üretimi, analizi ve bilgi yayma eylemlerinden oluşur (Çınar, 1997: 115-118). Dolayısıyla terör örgütlerinin organizasyonel yapıları, amaçları, hareket tarzları, kaynakları silah ve patlayıcıları ve dışarıdaki bağlantılarıyla ilgili bilgilerin ele geçirilmesi olarak ifade edilebilir (Köseli, 2009: 59). CIA tarafından stratejik istihbaratın kurucusu sayılan Prof. S. Kent, "stratejik istihbarat" adlı kitabında stratejik istihbarat kavramını; karar alıcıların politikaları uygularken kendi çıkarlarına zarar vermeden diğer devletlerle ilgili sahip olmaları gereken bilgi olarak tanımlamaktadır (Kent, 2003). Özdağ da stratejik istihbaratın iki önemli unsuruna dikkat çekmektedir (Özdağ, 2002: 115):

- ✓ Stratejik istihbarat: Uzun vadeli politikaları, çevre koşullarını rakip ve müttefiklerin tüm unsurların politikalarını dikkate alır.
- ✓ Operasyonel olarak gelecekte ne olacağı ile ilgili bilgi vererek taktik istihbaratın gideceği yönü belirler.

Taktik istihbarat ise düşmanın farkında olmak ve düşman tarafından koordine edilen saldırıların, zamanının ve yerinin öğrenilebileceği istihbarat olarak tanımlanmaktadır (Köseli, 2009: 60). Taktik istihbaratın hemen kullanılması gerekir, kısa vadelidir. Stratejik istihbarat gibi uzun vadeli değildir (Özdağ, 2002: 115).Dönemin şartları istihbaratın dönüşümünü mecbur kılmaktadır. Soğuk Savaş zamanında klasik ve askeri istihbarat anlayışının, hedefin kapasitesinin ve saldırı düzeninin ortaya çıkarılarak "bul, odaklan ve imha et" stratejisiyle hareket ettiği söylenebilir. Çünkü bu dönemde düşmanı bulmak kolay, yok etmek zor bir süreçtir. Fakat zaman içerisinde terörizm algısıyla, düşmanı bulmak zor, yok etmek kolay bir hale gelmiştir (Özer, 2015: 60). Soğuk Savaş sonrası dünya dengelerinde yaşanan büyük değişimler istihbarat faaliyetlerine de etki etmiştir. Bilgi teknolojilerindeki yeni gelişmelerle birlikte küresel haber alma imkanları da artmıştır. Diğer yandan kitle imha silahlarının artması; küresel terörizm ve uluslararası örgütlü suçlarda istihbaratın, uzayın kullanımı ve gözetleme-keşif sistemlerindeki yeniliklere yönelmesini sağlamıştır. Dolayısıyla istihbarat tarihi boyunca stratejik boyutta önemli bir yer tutan görüntü istihbaratı, yeni sistemler sayesinde stratejik bir değer olmaktan ziyade taktik seviyede hizmet eder bir niteliğe kavuşmuştur (Bayraktar, 2014: 127). Taktik istihbarat aynı zamanda önleyici istihbarat olarak da ifade edilmektedir (Köseli, 2009: 60). 11 Eylül saldırılarından sonra ABD'nin uygulamaya geçirdiği Protected War (Önleyici Savaş) doktrini bu konuda önemli bir örneği teşkil etmektedir (Bayraktar, 2014: 128).

Teknolojinin gelişmesi ve küreselleşmenin de etkisiyle ulusal ve uluslararası seviyelerdeki kurumlar da şekil değiştirmektedir. Bu değişim ve dönüşüm içerisinde istihbarat servisleri de eskiye nazaran oldukça farklılık göstermektedir. Örneğin; Deaş Lideri Ebubekir el Bagdadi'nin yerinin tespit edilmesinde ABD istihbarat topluluğunun uzay ve uydu teknolojileri, iletişim teknikleri ve istihbarat sağlamak için yaptığı tüm buluş ve yatırımların etkisinden söz edilmektedir. Ayrıca operasyonun daha önceki bir zaman içerisinde planlandığı, fakat gelen istihbaratın el Bagdadi'nin bulunduğu konumu değiştirmiş olmasından dolayı iptal edildiği belirtilmektedir (Walcott, 2019). Dolayısıyla değişen dünya düzeninde istihbaratın geleneksel sistem dışına çıktığı, teknolojinin gelişmesi ve bilgisayarların devreye girmesiyle de siber istihbarata ve uzay istihbaratına yönelimin arttığı söylenebilir. Bu bağlamda dünya üzerindeki her türlü kitle iletişimini kontrol eden "Echelon Ağı"[2] uzaydan tüm

2 ABD'nin Echelon sistemi ağı aracılıyla, Avrupa uçak şirketi Airbus ile Suudi Arabistan arasındaki ihale sürecini dinlemiş ve antlaşmanın arka planındaki Avrupalı yetkililerin Suudi yetkililere rüşvet vermesi olayını bilinçli ortaya çıkararak ilgili ihaleyi iptal ettirmiştir. Ek olarak, ABD Echelon sistemini kullanarak, Amerikan şirketi Raytheon'un Brezilya'da milyarca dolarlık iş akdini Fransız elektronik ve savunma sanayi şirketi Fransız Thomson-CSF elinden almıştır (Dixon , 2016:133).

görüntüleri kaydeden gelişmiş uydu sistemleri, klasik istihbaratın tüm fonksiyonlarını devre dışı bırakmıştır denilebilir. Dolayısıyla tüm bilgi toplama imkanları da yeni teknolojik gelişmeler ile evrim geçirmiştir. Elektronik istihbarat, siber casusluk ya da teknolojik istihbarat günümüz istihbaratının en önemli unsurları haline gelmiştir. Şüphesiz yüzyılın en önemli olaylarından biri Julian Assange isimli bilgisayar korsanının Wikileaks adı altında gizli Amerikan görüşmelerini açığa çıkarmasıdır. Nitekim halkların sınır tanımadan birbiri ile iletişim kurduğu, iş yaptığı, sonsuz bilgiye anında ulaşabilme imkanı sağlayan siber alan, istihbarat alanında da en kolay bilgi erişim alanı olmuştur. Bu bağlamda Derin İnternet adı verilen ağdan bahsetmek faydalı olacaktır. NSA; 2012 Haziran tarihli Tor Stinks adlı sunumda 10 yıl önce internetin içinde derin internet adı verilen gizli bir ağ kurulduğu ve bu ağın istihbaratçılar ve orduya hizmet ettiği bir alan haline geldiğini belirtmiştir. Projenin temeli 1996 yılında Hiding Routing İnformation (Gizli Yönlendirme Bilgileri) adlı bir başka projeye dayanmaktadır. Temel amaç olarak da kullanıcıların kimliklerini belli etmeden internetteki faaliyetlerini gerçekleştirebilmeyi kapsamaktadır. Dolayısıyla da istihbaratçıların iletişim ve işlem yapma yerleri olarak hizmet eden siber alanlardan biri olmuştur (Sökmen, 2017: 280-281).

Yeni istihbarat ülke güvenliğinden, ekonomi, uzay, siber-uzay ve diplomasinin örtülü faaliyetlerle desteklenmesine kadar geniş bir alanda değişmektedir. İstihbarat alanında yapılan toplayıcı ve analizci değişimler kadar, bilgi ile istihbarat arasındaki farkı ortaya koyacak bir sistemle de çalışmaktadır. Echelon gibi küresel istihbarat gayretlerine bilgi teknolojileri ve internet kontrol çabalarının da eklenmesiyle, siber güvenlik alanında ülkeler birer birer teşkilatlanmaya başlamışlardır. Bu bağlamda iş dünyası istihbaratı ve özel güvenlik şirketlerinin istihbarat fonksiyonları baş döndürücü bir şekilde gelişmektedir. Ticaret görünümlü istihbarat faaliyetleri de hız kesmeden devam etmektedir (Yılmaz, 2014: 2).

2004-2010 yılları arasında siber suçlardan sorumlu olan saldırganları sınıflandırmak ve mücadele yöntemleri geliştirebilmek için bir araştırma projesi yapılmıştır. Proje detayında saldırganların yetenekleri, hedefleri, tehlike seviyeleri belirlenmeye çalışılmıştır. Projenin ikinci aşamasında ise siber terörizm faaliyetlerinin ortaya çıkmadan önlenebilmesi için ne gibi yöntemler geliştirilebileceği üzerinde durulmuş ve potansiyel siber teröristlerin önceden belirlenebilmesi için çalışmalar yapılmıştır. ABD Savunma Bakanlığı içerisinde proje geliştiren DARPA tarafından 2010 yılında Siber Genom Projesi başlatılmıştır. Proje kapsamında siber atakların genetik yapısı analiz edilmeye ve hangi grup/saldırgan tarafından gerçekleştirileceği, saldırının şekline göre savunma/karşı atak stratejileri belirlenmeye çalışılmaktadır (Sağıroğlu ve Alkan, 2018: 272). Bu projelerin de istihbaratın dönüşümü açısından güzel birer örnek teşkil edeceği söylenebilir.

İstihbaratın siber ortamlardaki imkanlarından biri de virüs gönderme yöntemidir. Şöyle ki bilişim teknolojilerini kullanan ülkelerin kritik alt yapı tesislerinin gönderilen bir virüs ile devre dışı kalması, gönderen ülke açısından önemli bir amacın gerçekleşmesine hizmet etmektedir. Örneğin; İran'ın uranyum zenginleştirme tesislerini bir süreliğine felç eden "Stuxnet" adlı bilgisayar solucanını ABD ile İsrail'in ortaklaşa ürettiği ortaya çıkmıştır. Bir diğer ölümcül virüs olan Flame'i keşfeden Rus Vitaly Kamlyuk virüsü İran'ın hem nükleer sırlarını hem de petrol üretimini hedef alan ilk süper siber silah olarak nitelendirmiştir (Sökmen, 2017: 282). Siber istihbaratın sağladığı avantajların yanında karşı bir saldırı gerçekleştirilmesine yönelik engellerin önemli ölçüde düşük olduğu söylenebilir. Zira İnsansız Uçak Sistemi ABD'ye yaklaşık 45 milyon dolara ve bu sistemin verilerinin depolandığı uzay uydu şebekesi milyonlarca dolara mal olmuştur. Fakat bu sistemleri etkisiz hale getirmek için "skygrabber" olarak bilinen bir program ise sadece 25,95 dolardır (Güntay, 2018: 91). Bu durum Kshetri'nin siber uzayı iki ucu keskin kılıç olarak tanımlamasıyla birebir örtüşmektedir.

ABD ve Çin arasında geçen ticaret savaşlarının arka planında ciddi bir istihbarat dönüşümünün varlığından söz etmek mümkündür. Şöyle ki Çin ABD'nin gelişmiş teknolojilerine erişebilmek için kesintisiz siber saldırılar gerçekleştirmektedir. ABD basınına yansıyan iddialarda 25 bin Çinli istihbarat ajanının ABD'deki farklı kurumlarda çalıştığı ileri sürülmektedir. Çin'in ABD üzerindeki istihbarat faaliyetlerinin hem askeri hem de ticari alanlarda olduğu dolayısıyla da ABD'nin yaptırımlarıyla[3] karşılaştığı söylenmektedir. Çin'in son dönem politikalarına bakıldığında karşı istihbarat bilinci adı altında yoğun programlar yürüttüğü söylenebilir. Çin ülke içinde kurduğu yüz tanıma destekli kamera ağı, çevrim içi ödeme metodları, sıkı internet denetimleri ve bu alandaki kişisel verilerin toplanmasıyla 2020'ye kadar tüm ülkede gelişmiş bir sistem kurmayı planlamaktadır. Çin dijital ordusu bünyesinde kaç kişinin çalıştığı bilinmemekle birlikte ülkenin Siber Çin Seddi olarak tanımlanmaktadır. Ayrıca bu ordunun elde ettiği veriler otel ve rezidans görünümlü dev veri depolarında muhafaza edilmektedir (Durul, 2018).

Çin'in çalışmalarına karşılık ABD'nin de farklı teknolojilere yöneldiği gözlemlenmektedir. Siber alanın faaliyet imkanlarıyla Nörobilimin uç noktası birleştirilince DARPA(Savunma İleri Araştırma Projeleri Ajansı)'nın geliştirmiş olduğu Beyin Arayüz Projesi ile Amerikan askerlerinin sinaptik bağlantılarını artırmayı ve bellek eklemek yoluyla yeni yetenekler kazandırmak amaçlanmıştır. Ayrıca sessiz konuşma projesi de beyin içindeki preverbal elektrik sinyallerinin şifresinin çözülerek askerlerin herhangi bir iletişim aracı olmadan iletişim kurabilmesini sağlayabilecek etkin telapati üzerinde çalıştığı ileri sürülmektedir.[4] Siber alanda kullanılan ve görsel hafızayı etkileyen 25 kare tekniği bilinç altına bilgi girme ve bireyi yönlendirme çalışmasına hizmet etmektedir. Subliminal mesajları dinledikçe veya internet ortamında seyrettikçe farkında olmadan bireyin düşünceleri etkilenmektedir. Rusya bu yönteme karşı bir teknik geliştirerek TV kanallarının kontrolünü yapmaktadır. Fakat internet gibi sınırsız bilgiye ulaşılan bir ortamda, yöntemin ne kadar etkili olduğu tartışma konusudur. İstihbarat servisleri tarafından geliştirilen bilgisayar oyunları da kişinin beynine mesajlar göndererek şiddet ve nefret duygularının oluşumuna hizmet etmektedir. Örneğin 11 Eylül 2001 terör saldırısı sonrası oluşturulan bilgisayar oyunlarının İslam düşmanlığını körükleyen savaş oyunları olması dikkat çekicidir (Sökmen, 2017: 284-285). Son olarak günümüzde makine öğrenimi ve yapay zeka sayesinde geliştirilen "Deepfake"[5] adı verilen yöntemin geniş çapta karmaşa yaratabileceği öngörülmektedir. ABD senatosu istihbarat komitesinde Marco Rubio Deepfake yönteminin Amerika'ya ve Batı demokrasilerine karşı bir saldırı aracı olarak kullanılacağı konusunda uyarılar yapmıştır (Parkin, 2019).

Günümüz istihbaratının yönelimi, toplanıp analiz edilecek bilgi miktarında ciddi artışlar oluşturmuştur. Uluslararası iletişim, teknoloji ve internet kullanımı sayesinde yüzde 800 artmış, ABD'nin istihbarat servislerinin istihbaratlarının yüzde 80'inden fazlasının bu kaynaklardan elde edildiği gözlemlenmiştir (Biçer, 2017: 441). Böylesi bir durumun tehlikeli sonuçlara yol açabileceği aşikardır. Nitekim küresel terörle mücadele ile ilgili kurulan teknolojik istihbarat sistemleri, ülkeler tarafından suistimal edilir olmuştur. Eski NSA görevlisi Edward Snowden'ın açığa çıkardığı dinleme skandalı Fransa'da sadece 10 Aralık 2012-8 Ocak 2013 tarihleri arasında 70 milyon telefon görüşmesinin dinlenildiği ve verilerine ulaşıldığını ortaya koymuştur. Bu durumun ülkeler arası gerginlik ortamının başlangıcı ve diplomatik ilişkilerin sonlandırılması olarak algılandığı görülmektedir. Ayrıca verilerin bu denli hızlı ve çok sayıda toplanabilmesi ülkeler arası ilişkileri sekteye uğratmış olsa da

3 Huawei yasağı; ABD, Huawei'nin Çin hükümeti ile ilişkileri ve yeni nesil mobil teknoloji olan 5G piyasasına küresel ölçekte egemen olması nedeniyle Batılı ülke vatandaşları, kurumları ve devletleri hakkında bilgi toplayabileceğini savunuyor. Washington, Huawei'yi bir "ulusal güvenlik tehdidi" olarak görüyor ve federal hükümet tarafından açılan ihalelere katılmasını yasaklıyor. Bu bağlamda Çin'in istihbarat faaliyetlerini kısıtladığı söylenebilir ( Wei, C. Y. 2019).

4 İstihbarat yarışında Çin'in 5G sine karşılık böyle bir projenin hayata geçirildiği söylenebilir.

5 Deepfake(Derin Sahtelik);Kişilerin ses ve mimikleri de dahil olmak üzere görüntülerinin taklit edilebilmesidir. Yöntemin Gabon'daki siyasi bir krizde rol oynadığı iddia edilmektedir (Parkin, 2019).

birbirlerine karşı yeni avantajlar sağlamaktadır (Saran, 2017: 338-339). Fakat, açık kaynaklardan elde edilen verilerin artmasıyla birlikte gereksiz bilgilerin, değerli bilgilerden ayrılması sorunu istihbarat servisleri için kritik noktalardan biri haline gelmiştir. Dolayısıyla kapalı ve gizli kaynak döneminde bile ayrıntıların gözden kaçırıldığı düşünüldüğünde, artan veriler ile birlikte istihbarat servislerinin değerli bilgilere ulaşmasının zahmetli bir süreç olacağı elzemdir (Biçer, 2017: 442).

Geride bıraktığımız 20.yüzyılın sonlarına doğru kendini gösteren uluslararası terörizm hareketleri, yeni istihbarat anlayışında dünyadaki birçok istihbarat servisinin artan bir iş birliği ve bilgi paylaşımına gitmelerini gerekli kılmıştır. Fakat buradaki bilgi paylaşımının ancak karşılıklı çıkar ortamında gerçekleştirildiğinin altı çizilmelidir. Çünkü hiçbir istihbarat servisi elde ettiği bilgiyi ülkesinin çıkarları söz konusu olmadıkça paylaşmaz. Aynı istihbarat servisi içindeki birimlerin bile kendi arasında bilgi sakladığı düşünüldüğünde, bir ülkenin başka bir ülkenin çıkarı için bilgi paylaşması fazlasıyla hayalcilik olacaktır. Bu bağlamda istihbarat servislerinin ülke çıkarları doğrultusunda yapılmayan bilgi paylaşımlarının, ince elenip sık dokunması gerekmektedir (Acar, 2017: 51). Zira terörizmle mücadelede her türlü elde edilen bilginin gizli, örtülü ve acımasızsa bir süreçten geçtiği hatırlatıldığında dost ve müttefik olmanın hiçbir önemi kalmayacaktır.

## Sonuç

Devletlerin, kurumların, özel işletmelerin ve/veya bireysel işlemlere ait süreçlerin gün geçtikçe daha çok siber uzaya aktarıldığı düşünüldüğünde şüphesiz ki uzaydaki güvenliğin sağlanması kaçınılmaz olacaktır. Siber saldırıların özelinde siber terörizmin bırakmış olduğu hasarlar gerek devlet gerekse de kurumsal düzeyde maddi ve manevi kayıplara yol açmaktadır (Sağıroğlu ve Alkan, 2018: 99). Bu bakımdan tüm dünya genelindeki politikaların siber alan üzerine yoğunlaştığı ve devletlerin kendi siber uzaylarını savunabilecek siber ordular kurmaya çalıştığı görülmektedir.

21. yüzyılla birlikte teknolojinin getirdiği imkanlar ve dünyadaki tehdit unsurlarının değişimi, istihbarat faaliyetlerine etki etmiştir. Kitle imha silahlarının artması, küresel terörizm ve uluslararası örgütlü suçlar da istihbaratın, uzayın kullanımı ve gözetleme-keşif sistemlerindeki yeniliklere yönelmesini sağlamıştır. Dolayısıyla istihbaratın tüm imkanları da bu gelişmelerle birlikte evrim geçirmiştir. Elektronik istihbarat, siber casusluk ya da teknolojik istihbarat günümüz istihbaratının en önemli unsurları haline gelmiştir. Fakat bu noktada ülkelerin tüm alt yapı hizmetlerini siber alana entegre etmesi, onlara ayrıcalıklar kazandırırken aynı zamanda ülkeleri siber saldırılara karşı savunmasız bırakmaktadır.

İstihbarat anlayışındaki değişimlerin teknolojik gelişimlerle birlikte evrildiği ve teknolojiyle birlikte gelişen siber terörizmin de istihbarata ve istihbarat faaliyetlerine yeni bir boyut kazandırdığı görülmektedir. Bu bağlamda yeni istihbarat ülke güvenliğinden, ekonomi, uzay, siber-uzay ve diplomasinin örtülü faaliyetlerle desteklenmesine kadar geniş bir alanda değişmektedir. İstihbarat alanında yapılan toplayıcı ve analizci değişimler kadar, bilgi ile istihbarat arasındaki farkı ortaya koyacak bir sistemle de çalışmaktadır. Echelon gibi küresel istihbarat gayretlerine bilgi teknolojileri ve internet kontrol çabalarının da eklenmesiyle, siber güvenlik alanında ülkeler birer birer teşkilatlanmaya başlamışlardır. Bu bağlamda iş dünyası istihbaratı ve özel güvenlik şirketlerinin istihbarat fonksiyonları baş döndürücü bir şekilde gelişmektedir. Ticaret görünümlü istihbarat faaliyetleri de hız kesmeden devam etmektedir.

**Kaynakça**

Acar, Ü. (2017). Türk İstihbaratında Yapısal Sorunlar. S. Yılmaz içinde, *İstihbarat Dünyası* (s. 37-55). Ankara: Kripto.

Bayraktar, G. (2014). Harbin Beşinci Boyutunun Yeni Gereksinimi:Siber İstihbarat. *Güvenlik Stratejileri*, 119-147.

Bayraktar, G. (2015). *Siber Savaş ve Ulusal Güvenlik Stratejisi.* İstanbul: Yeniyüzyıl Yayınları.

Bıçakcı, S. (2012). Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu. *Uluslararası İlişkiler, 9*(34), 205-226.

Biçer, S. (2017). Ulusal Güvenlik ve İstihbarat Sisteminde Geleneksel Anlayıştan Modern ve Değişen İhtiyaçlar Dönemine Geçiş. *KSBD Dergipark, 9*(2), 435-464.

Bimfort, M. T. (1958). *A Definition of İntelligence ,*. Studies in İntelligence 2(4).

Bruno, G. (2008). *Backgrounder: The Evolution of Cyber Warfare.* 12 24, 2019 tarihinde https://archive.nytimes.com/www.nytimes.com/cfr/world/slot1_20080227.html?_r=0 adresinden alındı

Cirhinlioğlu, Z. (2004). *Terör ve Toplum.* İstanbul: Gündoğan Yayınları.

Collin, B. C. (1996). *The Future of CyberTerrorism:Where the Physical and Virtual Worlds Converge.* 11th Annual International Symposium on Ccriminal Justice Issues.

Cyber Security Ventures. (2017). *Cybercrime Damages $6 Trillion By 2021.* 12 10, 2019 tarihinde https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/ adresinden alındı

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

Çetinkaya, Ş. (2011). *Siber Terör ve Siber İstihbarat.* 12 24, 2019 tarihinde 21. Yüzyıl Türkiye Enstitüsü: https://21yyte.org/tr/merkezler/islevsel-arastirma-merkezleri/terorizm-ve-terorizmle-mucadele/siber-teror-ve-siber-istihbarat adresinden alındı

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

Durul, T. (2018). *Çin'in Dijital İstihbarat Savaşı.* 12 14, 2019 tarihinde https://www.aa.com.tr/tr/dunya/cinin-dijital-istihbarat-savasi/1287647 adresinden alındı

Ermiş, U. (2018). Bir Güvenlik Sorunu Olarak Siber Uzay. *Tasam*.

Gill, P., Marrin, S., & Phytian, M. (2009). *Intelligence Theory: Key Questions and Debates.* (J. Webb, Dü.) New York: Routledge Press.

Gladwell, M. (2003). Connecting The Dots, The Paradoxes of İntelligence Reform. *Newyorker*, 83.

Gül, T. (2012). *Terör & Terörizm.* İstanbul: Özgü Yayıncılık ve Tanıtım Hizmetleri San. Tic. Ltd. Şti.

Güntay, V. (2018). Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler. *Güvenlik Stratejileri, 14*(27), 80-111.

Gürkaynak, M., & İren, A. (2011). Reel Dünyada Sanal Açmaz:Siber Alanda Uluslararası İlişkiler. *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Dergisi, 16*(2), 263-279.

Keleştemur, A. (2015). *Siber İstihbarat.* Level Yayınları.

Kent, S. (2003). *Stratejik İstihbarat.* (B. Y. Özbek, & N. Şüküroğlu-Arıca, Çev.) Ankara: Asam.

Kshetri, N. (2014). *Cybersecurity and International Relations: The U.S. Engagement with China and Russia.* Prepared for FLACSO-ISA , University of Buenos Aires, School of Economics, Buenos Aires.

Kuehl, D. (2009). *From Cyberspace to Cyberpower: Defining the Problem.* (L. Wentz, S. Star, & F. Kramer, Dü) In Cyberpower and National Security: Wahington DC. National Defense University Press.

Law on The Fight Against Terrorism. (1986). 12 14, 2019 tarihinde https://www.legislationline.org/download/id/7905/file/France_law_fight_terrorism_1986_as_of_2018_fr.pdf adresinden alındı

Lowenthal, M. M. (2006). *Intelligence From Secrets To Policiy.* Washington Dc :CQ Press.

Minix, D. A., & Hawley, S. (1998). *Global Politics.* Belmont CA:West /Wadsworth.

MİT. (2019). *MİT*. 12 10, 2019 tarihinde http://www.mit.gov.tr/isth-olusum.html# adresinden alındı

Mombelli, F. P. (2014). The ECHELON Affair. *European Parliamentary Research Service*.

Nye, J. S. (2010). *Cyber Power.* Cambridge: Harvard Kennedy School / Belfer Center for Science and International Affairs.

Oğuz, S., Ceyhan, E., & Sağıroğlu, Ş. (2016). *Teknolojinin Casuslukta Kullanılması ve Karşı Önlemler.* https://www.iscturkey.org/assets/files/2016/03/paper.pdf.

Özdağ, Ü. (2002). *Avrasya Dosyası: Üç Aylık Uluslararası İlişkiler ve Stratejik Araştırma Dergisi : İstihbarat Özel.* Ankara: Asam.

Özer, Y. (2015). Terörizmle Mücadelede İstihbaratın Rolü:Kültürel İstihbarat Konsepti. *İGÜSBD, 2*(1), 52-80.

Parkin, S. (2019). *The Rise of the Deepfake and the Threat to Democracy.* 12 19, 2019 tarihinde https://www.theguardian.com/technology/ng-interactive/2019/jun/22/the-rise-of-the-deepfake-and-the-threat-to-democracy adresinden alındı

Sağıroğlu, Ş., Alkan, M., & vd. (2018). *Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık.* Ankara: Grafiker Yayınları.

Sandıklı, A., & Yivciger, G. (2004). *Siber Terörizm.* İstanbul: Tasam.

Saran, H. (2017). Değişen Diplomasi Sistemi ve İstihbarat. S. Yılmaz içinde, *İstihbarat Dünyası* (s. 327-349). Ankara: Kripto.

Schmid, A. P., & Jongman, A. (2005). *Political Terrorism.* Transaction Books.

Shulsky, A. N. (2001). *Silent Warfare:Understanding the World of İntelligence.* New York : Brassey's.

Sökmen, A. İ. (2017). İstihbarat Politikaları Kapsamında Dünyada Uygulanan Örtülü Operasyonların Teori ve Pratiği. S. Yılmaz içinde, *İstihbarat Dünyası* (s. 263-287). Ankara: Kripto.

STM. (2018). *2018 Ocak-Mart Dönemi Sİber Tehdit Durum Raporu.* STM Mühendislik Teknoloji Danışmanlık.

Terörle Mücadele Kanunu. (2019). 12 10, 1991 tarihinde https://www.mevzuat.gov.tr/MevzuatMetin/1.5.3713.pdf adresinden alındı

Terzi, M. (2018). Bilgi İletişim Teknolojilerine Dayalı Oluşumlar ile Bu Oluşumların Uluslararası İlişkilere Güvenlik Bağlamındaki Etkisi:Siber Terörizm. *Kara Harp Okulu Bilim Dergisi*, 73-108.

U.S Depertment of State. (2009). 12 14, 2019 tarihinde https://2009-2017.state.gov//index.htm adresinden alındı

Walcott, J. (2019). *Here's How U.S. Forces Finally Tracked Down and Killed al-Baghdadi*. 12 08, 2019 tarihinde https://time.com/5711905/al-baghdadi-capture-isis-intelligence/ adresinden alındı

Warner, M. (2002). Wanted:A Definition of İntelligence. *Studies in İntelligence 46*, 15-22.

Wei, C. Y. (2019). *Huawei: Batılı ülkeler neden Çinli teknoloji devinden korkuyor?* 12 06, 2019 tarihinde https://www.bbc.com/turkce/haberler-dunya-47606805 adresinden alındı

Yılmaz, O. (2017). Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik. *Siber Politikalar Dergisi, 4*(2), 22-44.

Yonah, A., & Swetman, S. (2000). *Cyber Terrorism and Information Warfare: Threats and Responses.* Transnational Publisher.