SİBER TERÖRİZM:

POTANSİYELİN GERÇEKÇİ TEHDİDİ

Emre Çıtak[1]

Özet

Günümüzde siber alan; siyasi, ekonomik, sosyal ve kültürel olanlar başta olmak üzere pek çok düzeyde yaşanan etkileşimi barındırmaktadır. Birey etkinliği siber uzay içinde daha belirgin şekilde var olmakta ve de insanlık varlığını giderek bu alanla özdeşleştirmektedir. Siber alan da böylece bilgisayar ve ağ sistemleri üzerine kurulu devasa bir mecrayı oluşturmaktadır. Olumlu ve faydalı pek çok yönü olduğu gibi bu mecra, çeşitli riskler ve tehditler de barındırmaktadır. Bu durum da gündeme, alanın güvenliğiyle ilgili soruları ve siber güvenlik kavramını getirmektedir. Siber güvenlik; siber tehdit, siber saldırı, siber savunma, siber savaş, siber istihbarat, siber casusluk, siber suç ve siber terörizm gibi alt başlıkları içermektedir. Bu çalışmada ise internet ve bilgisayar sistemleri üzerinden tanımlanan siber alanın toplumun kullanımını açılmasından beri ciddi bir endişe kaynağı olan siber terörizm ele alınmaktadır. Çalışma boyunca terör örgütlerinin sözde amaçlarına ulaşmak için uyguladıkları stratejilerinde siber alanı kullanımı incelenmektedir. Terör örgütlerinin, örgütsel fayda sağlama ve saldırı gerçekleştirme amacıyla yoğun ilgi gösterdikleri siber alanın nasıl güvende olacağı konusu çalışmada tartışılan temel noktayı oluşturmaktadır. Çalışmada siber terörizmle mücadele ve siber caydırı konularına da değinilerek alana mütevazı bir katkı yapılmaya çalışılmıştır.

Anahtar Kelimeler: Siber Terörizm, Siber Caydırıcılık, Terörizm, Siber Güvenlik

Jel Kodu: F52, H56, D74

CYBER TERRORISM:

THE REALISTIC THREAT OF THE POTENTIAL

Abstract

Today, the cyber space contains interactions at many levels, especially political, economic, social and cultural ones. Individual activity exists more clearly in cyberspace, and humanity increasingly identifies its existence with this space. Cyber space thus constitutes a gigantic medium built on computer and network systems. As it has many positive and beneficial aspects, the space also contains various risks and threats. This situation brings to the agenda questions about the security of the field and the concept of cyber security. Cyber security includes subheadings such as cyber threat, cyber attack, cyber defense, cyber war, cyber intelligence, cyber espionage, cyber crime and cyber terrorism. In this study, cyber terrorism, which has been a serious concern since the society's use of cyber space, which is defined through the internet and computer systems, is discussed. Throughout the study, the use of cyber space

[1] Doç. Dr., Hitit Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Uluslararası İlişkiler Bölümü, emrecitak@hitit.edu.tr ORCID: 0000-0002-8704-6495

in the strategies that terrorist organizations implement to achieve their so-called goals is examined. The main point discussed in the study is how the cyber space, which terrorist organizations show great interest in order to gain organizational benefits and carry out attacks, will be safe. In the study, it has been tried to make a modest contribution to the field by addressing the issues of combating cyber terrorism and cyber deterrence.

Keywords: Cyber Terrorism, Cyber Deterrence, Terrorism, Cyber Security

Jel Code: F52, H56, D74

GİRİŞ

Mekana sınır çizmek mümkün müdür? Bu soruya geleneksel bir bakış açısıyla olumlu yanıt vermek olasıdır; fakat tecrübe edilen dönemde siber alanın varlığı "mümkün değil" cevabını beraberinde getirmektedir. Zaman zaman sanal dünya tanımlamasıyla da kullanılan siber alan, muğlaklığın ve belirsizliğin yoğun olduğu bir yapıdadır. Sınırları olmayan bu alanda gerçekleşen olayların, ilişkilerin ve davranış tutumlarının da çok yönlü ve çok boyutlu bir halde olduğunu ifade etmek gerekmektedir. İnsanlığın giderek siber alan içinde daha çok yer alması, alanın sınırlarının genişlemesine yol açarken ortaya her türlü niyet için bir çekim sahası çıkmaktadır.

Günümüzde siber alan; siyasi, ekonomik, sosyal ve kültürel olanlar başta olmak üzere pek çok düzeyde yaşanan etkileşimi barındırmaktadır. Teknoloji ve bilgi alanlarında gözlemlenen radikal gelişmeler, siber alanın hacmini daha da artırmaktadır. Birey etkinliği siber uzay içinde daha belirgin şekilde var olmakta ve de insanlık varlığını giderek bu alanla özdeşleştirmektedir. Siber alan da böylece bilgisayar ve ağ sistemleri üzerine kurulu devasa bir mecrayı oluşturmaktadır. Olumlu ve faydalı pek çok yönü olduğu gibi bu mecra, çeşitli riskler ve tehditler de barındırmaktadır. Bu durum da gündeme alanın güvenliğiyle ilgili soruları ve siber güvenlik kavramını getirmektedir. Siber güvenlik; siber alanda var olan veri, donanım, yazılımlara, ağ ve kullanıcılara yönelik tehditlerle, müdahaleyle ve yasa dışı eylemlerle ilgili bir konu alanını oluşturmaktadır. Bilgisayar ağ ve sistemlerinin oluşturduğu yapay gerçekliğin önemi, onu korunması gereken bir öğe olarak güvenlik tartışmalarının temeline oturtmaktadır.

Siber terörizm ise siber güvenlik endişeleri içinde daha çok yer bulan ve gündem oluşturan bir konu niteliğindedir. Terör örgütlerinin, saldırılarını veya en azından saldırı tehditlerini siber alana aktarmaları şüphesiz ki ciddi bir korku yaratmaktadır. Doğaları gereği uyguladıkları vahşi stratejinin yeni yöntemlerini ve teknikleri teknolojiden aldıkları destekle daha girift bir hale getiren terör örgütlerinin, siber alandaki faaliyetleri insanlık için ciddi bir meydan okumayı ifade etmektedir. Hedef devleti veya toplumu korkutma ve yıldırmaya yönelik anlayışları terörist grupların sözde nihai amaçlarını gerçekleştirmek için önemli bir

noktayı oluşturmaktadır. Siber alanın doğasında var olan muğlaklık ve bilinmezlik, saldırıların kaynağını belirlemeyi güçleştirse de terör örgütlerinin siber saldırı gerçekleştirmeye yoğunlaştıklarını ileri sürmek yanlış olmayacaktır. Siber alan terör örgütü üyelerine kimliklerini de saklayarak ve iz bırakmayarak hareket etme, sempatizan ve üye kazanma, propaganda yapma, iletişim kurma, finansal gelir elde etme, saldırı gerçekleştirme, eğitim alma gibi pek çok olanak sunmakta ve böylece örgütler bu alanda daha yoğun şekilde ilgi sahibi olmaktadırlar.

Bu çalışma; günümüzde giderek artan siber güvenlik endişesini temel alarak alandaki terörist tehdidi incelemek için ele alınmıştır. Öncelikle terörizm ve siber terörizm üzerine kavramsal bir çerçeve çizilmiş, sonrasında ise siber terörizmin potansiyel tehdidine ve bu tehditle mücadele stratejilerine yer verilmiştir. Özellikle terör örgütlerinin siber alandaki faaliyetleri ve saldırı potansiyelleri hakkında, benzer kalıpları ve güncel eğilimleri konusunda alandaki araştırmalara mütevazı bir katkı sunulmak istenmektedir. Pek tabii siber uzayın anonimliği çalışmadaki en önemli zorluğu oluşturmaktadır ve kayıtlara geçen siber terörist saldırılar konusunda belirsiz hakimdir; fakat siber güvenlik üzerine oluşan geniş literatür ve konuyla ilgili tartışmalar oldukça yardımcı olmuştur. Hayat seyrinin her boyutunun daha çok siber alana aktarıldığı günümüzde, güvenlik de en önemli eğilim noktasını oluşturmaktadır ve bu bağlamda terörizm temelinde yapılacak bir değerlendirme ciddi bir gereksinimi karşılayacaktır. Bugüne kadar çeşitli siber saldırılarının hatalı şekilde terör saldırısı olarak sınıflandırıldığı bilindiğinden, bu çalışmadaki genel yaklaşım siber terörizmi halihazırdaki terör örgütlerinin siber alanda uyguladığı yaşa dışı fiiller ve saldırılar üzerinden tanımlama çerçevesinde olacaktır. Terör grupları dışındaki bireysel veya yasa dışı gruplardan yapılan saldırılar, siber terör olarak değerlendirilmemiştir.

1. Siber Güvenlik ve Siber Terörizm

Kimi zaman dijital terörizm ismiyle de kullanılan siber terörizm kavramı, terörizm stratejisi kapsamındaki saldırıların veya saldırı tehdidinin siber uzayda gerçekleşmesini ifade etmektedir. Terör gruplarının uyguladığı terörizmin mekânsal olarak sanal boyuta yansıması ve siber güvenlik kapsamında korunması gereken değerler olan yazılım, donanım, ağ ve kullanıcılara yönelik saldırıların olması temel çerçeveyi çizmektedir. Siber terörizmi, suç gruplarının işlediği bilişim suçları veya hackerlerin faaliyetleri ile karıştırmamak gerekmektedir; zira terörizmin siyasi bir amacı bulunmaktadır ve örgütsel bir davranış olarak ortaya çıkmaktadır.

Siber terörizm tanımından önce siber güvenliğe değinmek faydalı olacaktır. Siber güvenlik, siber uzayın oluşmasıyla birlikte gündeme gelen güvenlik endişelerini, tehditlerini, risklerini ve koruma süreçlerini içeren geniş bir konuyu oluşturmaktadır. Siber alan halen bilinmeyenleri olan, multidisipliner ve çok boyutlu bir mecradır. Martin Libicki (2009: 10-12)

siber alanın geleneksel mekan algısıyla hem benzer hem de farklı yönlerinin olduğunu ifade etmektedir. Siber uzay bir taraftan kara, hava, deniz, uzay gibi bilinen mecralara benzerlikler oluştururken, diğer yönüyle tamamen insan yapımı bir alan olması nedeniyle kendine has özellikleri olduğunu belirtmektedir. Bu alanın fiziksel, semantik ve sentetik olmak üzere üç katmandan meydana geldiğini ileri sürmektedir. Pek tabii henüz yeni sayılabilecek ve genişleyeceği sınırı belli olmayan bu alanda, güvenliğin nasıl ele alınması gerektiği ve güvenlik tehditlerinin neler olduğu üzerine yapılan çalışmaların da eksikler barındıracağı ön kabulünü belirtmek gerekmektedir. Nezir Akyeşilmen'e (2018: 53) göre bu mecra, büyüklüğü ve derinliği nedeniyle bir uzay, insanlığa sağladığı fayda ile önemli bir teknolojik buluş ve burada oluşan tehditler nedeniyle ciddi bir güvenlik sorunudur. Bu alanda devletler, devletlerin kurum ve kuruluşları, şirketler, bireyler, suç grupları, terör örgütleri veya bağımsız gruplar aktif halde bulunmaktadır (Andress ve Winterfeld, 2011: 193). Siber alan genel bir yanılgı olarak sadece internet ağları üzerinden tanımlansa da içerisinde donanım, yazılım, bilgi sistemleri ve ilgili ağların da olduğu daha geniş çerçevede bir boyutu düşünmek gerekmektedir. Siber uzay olarak düşünülen bu alanda birbiriyle iç içe geçmiş ağlar üzerinde çok boyutlu bir yapı bulunmaktadır (Kasapoğlu, 2017: 2-3). Bu yapı içerisinde askeri, siyasi, ekonomik, ticari, kültürel, bilimsel, teknolojik, sportif, sosyal olmak üzere pek çok türden paylaşım mümkün hale gelmiştir. Buradaki aktörler arasındaki bağlar ve ağlar karşılıklı bağlantılılık ilişkileri üzerinden bir ekosistem sistem oluşturmakta ve buradaki bir devletin, şirketin veya bireyin davranışları diğerleri üzerinde de etkiler yaratmaktadır (Schaake ve Vermeulen, 2016: 77).

Siber güvenlik denildiğinde akla gelen en önemli konu siber saldırı veya tehdit olarak öne çıkmaktadır. Siber alandaki sistemlere, ağlara ve kullanıcılara yöneltilen doğrudan veya dolaylı kötü amaçlı etkenlere siber tehdit, çeşitli araçlar kullanılarak tehditlerin hedefe yöneltilmesine ise siber saldırı denilmektedir. Bayraktar (2015: 82-92) siber saldırı yöntemlerini; kötü amaçlı yazılımlar, mikroçipler, spam postalar, DoS ve DDoS saldırıları, eşzamansız saldırılar, süper darbe, kaynak kod istismarı, veri aldatmacası, yemleme, web sayfası yönlendirmesi, gizlice dinleme ve hackleme olarak başlıklandırmaktadır. Tüm bu yöntemler devletler, gruplar veya bireyler tarafından uygulanabilmektedir. Kimi zaman kendini yetiştiren ve tek bir bilgisayara sahip olan bireyler, kimi zaman da devlet destekli bir organizasyon siber saldırı gerçekleştirebilmektedir.

Siber güvenlik konunun genel boyutunu oluştururken, uluslararası alanda giderek etkisi artan bir siber mücadelenin olduğunu ifade etmek gerekmektedir. Siber mücadele devletler arası savaşlara ve diğer çatışmalara yansımış, böylece siber saldırılar da hem geleneksel askeri karşılaşmalara hem de bağımsız mücadelelere yeni bir saha oluşturmuştur (Schmitt, 2012: 250-259). Siber alandaki özgü şiddet ve saldırılar bağlamında alandaki güvenlik sorunları kendini geliştirmiş hacker olarak tanımlanan bireylerden, çeşitli gruplardan

veya devletlerden gelebilmektedir. Temelde olan bireysel suçlar ve devletler arası siber saldırırlarken, özellikle devlet dışı aktörlerin düzenledikleri saldırılar giderek daha göz önüne gelmektedir (Yenal ve Akdemir, 2020: 417-424). Dünya genelinde her geçen gün daha fazla özel ve tüzel varlığın siber alanda faaliyet alanlarını genişletmeleri sonucunda bireyler, gruplar, devlet dışı aktörler, devletler ve çeşitli şirketler siber saldırılara başvurabilmekte veya saldırıların hedefi olabilmektedirler. Bu noktada siyasi amaçlarla hareket eden devlet dışı bir aktör olarak terör örgütlerinin siber alandaki müdahaleleri ve saldırıları siber terörizmin çerçevesini oluşturmaktadır.

Riskler, açıklar, saldırılar ve suç girişimleri siber alandaki aktörler için doğrudan ve dolaylı etkiler yaratabilmektedir. Bu olumsuz durumlara karşı güvenlik ihtiyacı güçlü şekilde hâsıl olmaktadır. Siber alandaki risk, tehdit ve tehlikelerin önlenmesi ve bertaraf edilmesi güvenliğin sağlanmasının yolu olarak görülmektedir (Akyeşilmen, 2018: 86). Siber güvenlik, bu alandaki kullanıcıların veya kurum ve kuruluşların varlık özelliklerine yönelik risklere karşı çözüm üretme işi olarak da görülebilmektedir (Keleştemur, 2015: 162). Siber uzayın bir referans nesne olarak düşünülerek her türlü risk ve tehditten arındırılmasına yönelik önlem ve faaliyetler de siber güvenlik tanımı olarak ortaya çıkmaktadır.

Ananonimliği, reddedilebilirliği ve maliyetinin düşüklüğü siber saldırıları çekici bir tercih sebebi yapmaktadır (Şeker, 2017: 33). Keleştemur (2015: 267); siber saldırı kaynaklarının bilgisayar korsanları, siber teröristler, organize suç örgütleri, endüstri casusları, istihbarat çalışanları, kurum içi casuslar ve diğer devletlerin birimleri olarak sıralamaktadır. Siber alana yönelik farkındalık ve kullanım alanı arttıkça olumlu gelişmelerin yanı sıra risk, tehdit, suç gibi güvenlik sorunlarında da yükseliş gözlemlenmektedir. Bu durum da güvenlik çalışmaları içerisinde önemli bir yeri olan siber güvenlik konusunu gündeme getirmektedir. Siber güvenlik; giderek ulusal güvenlik politikalarının önemli bir yönünü oluşturmakta ve bu yeni alan hem tecrübeler hem diğer devletlerin uygulamalarıyla güvenli hale getirilmeye çalışılmaktadır (Hekim ve Başıbüyük, 2013: 152-155). Siber saldırılarda saldıran taraf; bu alandaki fiziksel ve sanal yapıyı, donanım, yazılım ve altyapı olmak üzere ilgili sistemleri, bilgileri ve doğrudan kullanıcıları hedef alabilmektedir (Şenol, 2017: 2).

Siber güvenlik tartışmaları kapsamında devletlerin birbirilerine karşı yürüttükleri mücadelelerin tezahürü olan siber savaşlara ve terör gruplarının yürüttükleri kampanyalara da değinmek gerekmektedir. Günümüzde geleneksel savaşların karakteristiği değişmiş ve siber savaşlar saha ve araç bağlamında yeni bir boyut sunmuştur. Bu bağlamda devletler arasında, birbirilerine zarar vermek veya güçlerini test etmek için yoğun olarak gerçekleşen siber saldırıların önemli mücadele boyutu haline geldiğini ifade etmek, terör örgütlerinin de bu alandaki artan faaliyetlerine dikkat çekmek gerekmektedir.

Günümüzün güvenlik tartışmalarındaki tehdit tanımlaması önceliğinde olan konulardan birini hiç şüphesiz terörizm oluşturmaktadır. Devletlerin güvenlik politikalarının temel başlıklarından ve ulusal güvenlik endişelerinin en önemli baskı unsurlarından birini oluşturan terörist faaliyetler ve eylemler giderek mücadelesi daha da zorlaşan bir sorundur. Gary Ackerman ve Michael Burnham (2019: 12) terörizmi; devlet dışı bir aktörün geniş bir kitleyi yönlendirmek, davranışlarını değiştirmek veya yıldırı oluşturmak gibi amaçlarla sembolik veya temsili olarak seçilen bir gruba karşı ideolojik yaklaşımla şiddet kullanması veya şiddet tehdidinde bulunması olarak ifade etmektedirler. Drake (1998) terörizmi, hedef aldıkları toplumun istedikleri doğrultuda inanmasını sağlamak isteyen grupların başvurdukları politik güdülü ve gizli organize edilmiş şiddet kullanma durumu olarak tanımlamaktadır.

Bir şiddet türü olarak terör eyleminin ortaya çıkmasında kimi nedenlerin veya örgütler tarafından suiistimal edilen koşulların bulunduğunu ifade etmek gerekmektedir. Örneğin; toplumsal eşitsizlik, yoksulluk, siyasi düzensizlik, devlet otoritesi eksikliği, dışlanma ve ötekileştirme, insan hakları ihlalleri, ideolojik ve kültürel baskı gibi nedenler bu bağlamda değerlendirilebilmektedir (Newman, 2006: 750-751). Terör örgütleri devlet egemenliğinin sorgu altında olduğu, toplumsal dayanışmanın güçlü olmadığı, vatandaşların temel hak ve yaşam standartlarına erişemediği koşulları lehlerine kullanmayı stratejilerinin bir parçası haline getirebilmektedirler. Bu bağlamda terörizm genel bir tanımla siyasi bir amaca ulaşmak isteyen örgütsel bir yapının yasa dışı şiddet kullanarak uyguladığı bir strateji olarak ifade edilebilmektedir. Bu stratejiyle kimi ideoloji ve olumsuz koşulları suiistimal edilerek hedef toplum ve devlet üzerinde korku, kargaşa ve kaos oluşturularak taviz elde edilmek istenmektedir.

Terörizm kamuoyunda doğrudan bir tepki ve rahatsızlık oluşturan, sürekli önlemlerin alınmasını gerektiren, kısa ve uzun vadeli ekonomik, siyasi, toplumsal, kültürel etkiler doğuran ve mücadele yöntemlerini çoğunlukla boşa çıkaran bir strateji olarak öne çıkmaktadır (Smelser, 2007: 131-154). Terörizm yine, meşru olmayan şiddet ve yöntemlerin sistematik şekilde hem devlet unsurlarına hem de sivil halka yöneltilmesi olarak tanımlanabilmektedir. Terörizm stratejisi uygulayan gruplar, karşı toplum üzerindeki siyasi hedeflerini gerçekleştirmek için organize bir şiddet eylemi ve propaganda faaliyeti yürütmektedirler. Uygulanan şiddetin oluşturduğu güvensizlik durumu terör örgütlerinin sözde ideolojilerini yaymaları için uygun ortam yaratabilmekte ve karar alıcıları zor durumda bırakabilmektedir. Terör saldırıları ve bilinmezlikle sıkıştırılan toplum teröre olduğu kadar, terör karşısında başarısız olan devlet kurumlarına da tepki vermektedir. Böylece terör örgütlerinin yöntem ve teknikleri etkili hale gelmeye başlamaktadır.

Terörle mücadele gücü bir devletin askeri imkanları başta olmak üzere ulusal kapasitesini, emniyet birimlerinin faaliyetlerini ve hukuk uygulamalarını esas almaktadır. Bu bağlamda istihbarat çalışmaları, anti terörizm faaliyetleri, terörizmle doğrudan karşılık ve sonuçların analizi gibi taktiksel yaklaşımlar terörle mücadele uygulamaları olarak öne çıkmaktadır (Bolz, Dudonis ve Schulz, 2002: 12-15). Bir grup tarafından ortaya konulan tehditle mücadele etmede, hem işlevsel yapının hem de ideolojik çerçevenin dağıtılması gerekmektedir. Terör örgütlerinin şiddet eylemlerinin engellenmesinin yanı sıra terörizmin tehlikeli bir ideolojik aşırılık olduğu düşünüldüğünde devlet ve toplum nezdinde bir karşı ideolojik duruşun da oluşması terörizmle mücadele kapsamında elzemdir (Gunaratna, 2007: 21). Ulusal, bölgesel ve uluslararası düzeyde ciddi bir tehdit oluşturan terörizm, çok boyutlu bir mücadele ile bertaraf edilen bir sorun olarak gündemin üst noktasında yer bulmaktadır.

Terörist gruplar siber alanı iki temel bağlamda kullanmaktadırlar. Bu alandaki iletişim ve kaynak elde etme gibi faydacı faaliyetler ve hedeflerine saldırı gerçekleştirme gibi terör hareketleri bu iki kapsamı oluşturmaktadır. Bireyler, aktivist gruplar, şirketler, sivil toplum örgütleri, yasa dışı gruplar, kurum ve kuruluşlar giderek daha çok siber alan içinde faaliyet gösterirken terör örgütlerinin de paralel bir seyir izlemediklerini düşünmek doğru olmayacaktır. Siber alanın sunduğu avantajlar terör grupları için de arkalarını dönemedikleri fırsatlar sunmakta ve böylece de karşı oldukları toplumlar için de daha büyük bir risk oluşturmaktadır. Örgütler bir yandan siber alanın sunduğu "nimetlerden" yararlanırken, diğer taraftan eylemlerini gerçekleştirmek için zayıf yönler aramaktadırlar.

Siber terörizmi, terörizmden ayıran nokta saldırıların doğrudan fiziksel bir şiddet içermemesi ve saldırılar için siber alanı oluşturan altyapının kullanılmasıdır. Terör örgütleri tarafından mevcut sistemler üzerinden veya özel olarak için üretilen yazılım, donanım, programlarla saldırılar gerçekleştirilmektedir (Shiryaev, 2012: 146-147). Siber dünyada işlenen hırsızlık, sabotaj, özel alana sızma, sahtecilik, casusluk, hizmet engelleme saldırısı, dolandırıcılık, kötü amaçlı yazılım yayma, zorbalık gibi tüm suçları terör örgütleri de gerçekleştirebilmekte ve bu mecra üzerinden bir korku iklimi oluşmaktadır (Singh ve Siddiqui, 2011). Alandaki ilk tanımlardan biri olarak Pollitt (1998: 9) siber terörizmi devlet altı gruplar veya gizli örgütler tarafından savaşmayan unsurlar üzerinde şiddetle sonuçlanan bilgi sistemleri, bilgisayar sistemleri, bilgisayar programlarına ve data depolarına yönelik tasarlanmış ve politik güdülü saldırılar olarak ele almıştır. Her ne kadar geleneksel terörizm gibi doğrudan fiziksel zararlar oluşturmasa da siber terör saldırılarının gündelik hayatın akışını etkileyecek, ulusal güvenlik sorunlarına neden olabilecek ve maddi kayıplar yaratacak sonuçlar oluşturması oldukça ciddi bir endişe doğurmaktadır (Hua ve Bapna, 2012: 104). Genel bir ele alış ile siber terörizmi; siyasi amaçlarla bir devleti veya toplumu yıldırmak veya

baskılamak için bilgisayar temelli sistemlere, ağlara veya bilgi altyapısına yönelik yapılan yasa dışı müdahaleler veya saldırılar olarak tanımlamak mümkündür.

Ali Burak Darıcılı (2020: 96) oldukça geniş bir tanımla siber terörizmi; bir terör örgütünün üyeleri ve ilişkili kişiler tarafından siyasi bir amaca ulaşmak için ağ sistemleri üzerinden gerçekleştirilen şiddet içere suç eylemi ve faaliyetler ile propaganda ve lojistik ihtiyaçların karşılanması olarak ifade etmektedir. Diğer bir tanımda ise siber terörün karşı tarafın can ve mal güvenliğine zarar vermek veya risk oluşturmak için etkileşim sahasını oluşturan sayısal teknolojiler ve platformlara gerçekleştirilen saldırılar olduğu ifade edilmektedir (Atasever, Özçelik ve Sağıroğlu, 2019: 239). Hasan Çifçi ise (2013: 5-6) değerlendirmesinde siber terörizmi genel bir çerçevede bilgisayar ağ ve sistemlerine yönelik çeşitli amaçlarla gerçekleştirilen ve çeşitli noktalarda zarar oluşturan saldırılar olarak nitelemektedir. Saldırıların bu alanda oluşturduğu korku ve hasar durumunu öne çıkarmıştır. Siber alan terör grupları için basitçe bir internet sayfasından ele geçirilmesinden nükleer silahların kod sistemlerine sızılmasına kadar geniş bir suiistimal ve saldırı potansiyeli sunmaktadır. Terör örgütlerinin bu alanda ne kadar etkili olabilecekleri kendi güçlerine bağlı olmanın yanı sıra devletlerce ortaya konulan savunma ve caydırıcılık durumuna göre şekillenmektedir (Foltz, 2004: 155-157).

Siber terörizm, yeni terörizm tartışması içinde de yer bulmaktadır. Terörizmin örgütsel, ekonomik-finansal, yöntem, imkan-kabiliyet, teknolojik yönlerden farklı bir boyuta ulaştığı ve bu bağlamda da terör örgütlerinin özellikle teknolojik gelişmelerine uyumlarıyla birlikte temel stratejileri olan karşı toplum üzerinde korku ve panik yaratmak için güçlü bir yeniliğe kavuşmuş oldukları ifade edilebilir (Morgan, 2004: 36-40). Terör grupları siber alanı oldukça geniş bir yelpaze çerçevesinde kullanmaktadırlar. Propaganda, iletişim, eğitim, araştırma, istihbarat, gelir elde etme, sosyal medya üzerinden hedef kitlelere ulaşma gibi konularda söz konusu gruplar ağ sistemlerini kullanmaktadırlar (Darıcılı, 2020: 95). Nasıl ki bireyler, toplumlar, özel ve tüze kuruluşlar bilgisayar ağ ve sistemleri sayesinde her türlü ihtiyaç ve işlemlerinde daha kolay şekilde erişme, düzenleme ve gerçekleştirme olanağına kavuştularsa, terör örgütleri ve üyeleri de böylesi bir fırsatlar dünyasına adım atmışlardır. Terör örgütleri çatışma halinde eş zamanlı olarak veya çatışmasızlık durumunda siber alanda faaliyetlerini yürütmektedirler. Günümüzde kimi terör örgütleri silahlı eylemleriyle paralel olarak karşı toplumun siber altyapısına zarar verme ve faaliyetlerini daha organize gerçekleştirme eğiliminde olurlarken, aktif eylemlerine ara verip internet temelli aktivitelerine yön veren gruplar da bulunmaktadır (Shiryaev, 2012: 173-190). Vahit Güntay (2017a: 89-90) özellikle siber terör saldırılarının organize bir grubun eylem biçimi olmasına vurgu yaparak sonuçların daha ciddi olması ve farklı hedefleri etkileyebilmesi durumunun altını çizmektedir. Özellikle kritik altyapı olarak tanımlanan iletişim-haberleşme, ulaşım, enerji, finansal servisler gibi

alanlardaki ağ ve sistemlere yönelik saldırılar can kayıplarına, ciddi ölçekte maddi kayıplara, ulusal güvenlik açıklarına ve hayat akışının bozulmasına neden olabilmektedir. Gordon ve Ford (2002: 638-643) ise bilinen terörizm tanımlamasındaki unsurlar olan fail, yer, eylem, araçlar, hedef, grup üyeliği ve motivasyon çerçevesinde siber terörizmi tartışarak yeni terörizm yaklaşımı içinde bilgisayarların birer silah gibi işlev görerek devletler ve siviller üzerinde baskı kurmaya çalışan grupların siyasi eylemlerine hizmet edebileceğine dikkat çekmektedirler.

Terör örgütlerinin siber saldırılarla üzerinden amaçları belirlenen hedeflere zarar verme, karşı tarafta güvensizlik ve korku oluşturma, panik havası yaratma, hedef ülkeyi güçsüz ve itibarsız gösterme, sempatizanlara ve üçüncü taraflara mesaj verme, propaganda ve güç gösterisi yapma şeklinde özetlenebilmektedir. Siber terörizmin potansiyel hedefleri; enerji altyapısı, telekomünikasyon, askeri sektörler, bilgi güvenliği, sağlık kayıtları, şehirlerin sinyalizasyon sistemleri, hava ve tren yollarındaki sistemler, eğitim kurumları, finansal altyapı ve bankalar, sosyal medya, kişisel sayfalar ve hesaplar gibi geniş bir çerçevede olabilmektedir. Nihayetinde terörizmin dayandığı korku, panik, güvensizlik ve korku oluşturma stratejisi siber alanda da kendini göstermekte, zayıf olan hedefler daha çok tercih edilmekte ve kimsenin güvende olmadığına yönelik bir algı oluşturma arayışında olmaktadır. Devam eden sayfalarda da bahsedileceği gibi terör örgütlerinin üst düzey zarar verebildikleri bir siber saldırı henüz kayıtlara geçmemiştir; fakat hem devlet savunmasına takılan çeşitli girişimleri hem de bu alandaki etkinlikleri her an kaos yaratabilecek bir potansiyeli hesaba katmayı zorunlu kılmaktadır. Çeşitli devletlerce açıklanan ve teyidi tam yapılamayan birkaç olay dışında siber alanın tümünü etkileyen bir terör saldırısı olmamış olsa da potansiyel tehdit, tüm tarafları endişeye sevk etmekte ve bir baskı unsuru olarak görünür olmasa da zararlar verebilmektedir. Siber terörizmin aynı zamanda karşı toplumda psikolojik bir baskı unsuru olduğunu ifade etmek gerekmektedir. Bireylerin ve kamunun günlük hayatı ve önemli bilgileri bilgisayar ağ ve sistemleri üzerinde yoğunlaştıkça güvenlik sorunu ayrıca mental ve duygusal bir ağırlığı da beraberinde getirmektedir. Bu nedenle terör örgütlerinin bu mecrada faal olduğunun bilinmesi ve saldırı korkusu ciddi bir baskı oluşturmaktadır (Gross, Canetti ve Vashdi, 2016: 2-3).

2. Siber Terörizme Karşı Mücadele ve Siber Caydırıcılık

Siber alan iç ve dış tehditlere oldukça açık bir alandır. Saldırıların farklı kaynakları, yöntemleri ve hedefleri olabilmektedir. Dış tehditler sisteme yönelik sızmalar ve doğrudan riskler üzerinden şekillenirken, iç tehditler ise hem sistemin oluşturduğu hem de sistemi koruması gereken kişilerin neden olduğu sorunlar üzerinde tanımlanmaktadır (Libicki, 2009: 22-23). Siber uzay genel olarak herhangi bir amaçla yapılacak saldırılar için uygun bir ortam sunmaktadır. Bir bireyin diğerinin sosyal medya hesaplarını çalmak için işe koştuğu casus yazılımdan, bir devletin diğerinin kritik bilgi depolarını işlemez hale getirebildiği sistem saldırısına kadar geniş bir yelpazedeki güvenlik tartışması işin özünü oluşturmaktadır. Terör

örgütleri de stratejilerini tecrübe edilen döneme uyarlama bağlamında internet ve bilgisayar sistemleri üzerinden edindikleri etkinliklerini karşı taraf üzerinde kullanma eğilimindedirler. Söz konusu alandaki açıklar, gizlilik, takipteki zorluk ve saldırı çeşitlerinin çokluğu terör gruplarını mecraya çekmektedir (Chu, Deng, Chao ve Huang, 2009: 2397-2398).

Bilgisayar ve internet temelli siber alanın özellikle toplum kullanımına açılmasından beri bu alanda yaşanabilecek terör saldırıları temel endişelerden biri olmuş ve analizlerde terör örgütlerinin siber potansiyelleri üzerinde durulmuştur. Güncel değerlendirmelerin yanı sıra gelecekte olabilecek saldırılar temel endişeyi oluşturmuştur. Zira bir yandan terör örgütlerinin zamanla imkan ve kaynak yönlerinden gelişecekleri diğer yandan ise insanlığın siber alana daha çok tutunmaya devam edeceği yönünde analizler yapılmıştır (Cohen, 2014; Weiman, 2004; O'Brian, 2003). Yerel veya küresel nitelikteki bir terör saldırısının neden olabilecekleri, bilim kurgu filmlerin ötesinde gerçek bir tehdit olarak algılanmıştır. Günümüze gelen süreç içinde terör örgütlerin toplumların gizli bilgilerini tamamen ele geçireceklerine, kişisel bilgisayarları kullanılmaz hale getireceklerine, kamusal iş ve işlemleri sekteye uğratacaklarına, kritik altyapıya zarar vereceklerine ve hatta askeri kod veya sistemleri ele geçirerek saldırılar düzenleyeceklerine yönelik tahminler ve güvenlik kaygıları dile getirilmiştir. Fakat bugüne kadar bu denli ciddi bir terör saldırısı kayıtlara geçmemiştir. Hiç şüphesiz ki terör örgütleri siber alanda saldırılar gerçekleştirmekte ve etkin şekilde bu mecrayı avantajlarına olabilecek şekilde kullanmaya çalışmaktadır. Hackleme, casus yazılım, Dos ve DDoS saldırıları, serverlara sızma gibi bireylerin ve yasa dışı grupların başvurdukları siber saldırılar, terör örgütleri için oldukça özendirici olmuştur. Yine de bir ülkeyi veya uluslararası alanı felce uğratacak düzeyde bir terör saldırısının var olduğu bilinmemektedir. Bunun için; terör örgütlerinin henüz kompleks saldırılar yapabilecek yeterli kapasiteye erişememeleri, devletlerin savunma önlemlerin oldukça ileri seviyede olması ve başarıya ulaşan siber saldırıların devletler tarafından kamuoyuna duyurulmaması gibi nedenler sayabilmek mümkündür.

Terör örgütleri için siber alanın tercih edilmesinin çeşitli nedenleri vardır. Terör örgütleri açısından siber saldırılar geleneksel saldırılara göre daha az maliyetli, anonimliği yüksek, hedef yelpazesi geniş, uzaktan idare edilebilir ve etki düzeyi ve medya yansıması daha fazla durumdadır (TASAM, 2004: 5-6). Terör örgütleri çok elemana, kaynağa, yere ihtiyaç duymadan ve daha az risk alarak bu alanda varlıklarını hissettirme imkanı bulabilmektedirler. Bu nedenle günümüzde devlet önlemlerini aşacak seviyeye gelmemiş olsalar da siber terör saldırıları, oldukça endişe verici bir potansiyel olarak insanlığın karşısında durmaktadır.

Siber güvenlik genel bağlamda savunma merkezli bir anlayışını ifade etmektedir. Siber güvenlik denildiğinde söz konusu alandaki tehdit ve risklere karşı önlemlerin alınması ve karşı konulması üzerinden bir çerçeve çizilmektedir. Siber alandaki savaş, mücadelece, saldırı ve

suçlar henüz tam anlamıyla tanımlaması yapılmamış ve hukuksal çerçevesi çizilmemiş durumlar olduğu için mücadele için politikaların ve stratejilerin ortaya konulması oldukça zordur (Güntay, 2017b:19-20). Terörizmin ulusal, bölgesel ve uluslararası bir tehdit olması mücadelenin de bu bağlamda yapılması gerekliliğini oluşturmaktadır. Siber terörizmin özgü bir şekilde sınırötesi, daha doğru bir ifadeyle sınır tanımayan yapısı uluslararası ve ortak bir mücadeleyi gerektirmektedir. Zira siber saldırı uygulayan terör grupları doğrudan bir hedef gözetseler de uluslararası toplumun geri kalanı için potansiyel bir tehdit oluşturmaktadır. Bu bağlamda siber terörizmle mücadelede birey, devlet ve uluslararası seviyelerde iradenin ortaya konulması özellikle önem arz etmektedir.

Terörizm, sert ve yumuşak güçlerin bir arada kullanılmasıyla bertaraf edilebilecek bir tehdittir. Amaçlarına ulaşabilmek için terör örgütlerinin ortaya koydukları tüm eylemlere, stratejilerine, sözde ideolojilerine ve örgüt yapılarına karşı bütüncül bir mücadelenin yürütülmesi gerekmektedir (Rineheart, 2010: 37-38). Normal olarak siber terörizmle mücadelede doğrudan gözler ülkenin teknolojik kapasitesine dönse de bilinçlenme, farkındalık, eğitim, özel ve kamu kuruluşları arasındaki birliktelik ve ulusal ve uluslararası kurumların eşgüdümlü çalışmaları oldukça önemlidir (Cox, 2015). Siber terörizme karşı koymak için çok yönlü bir mücadele örneğinin gösterilmesi ve terör örgütlerinin avantaj elde edebilecek herhangi bir zaafın bırakılmaması gerekmektedir. Siber terörizme karşı konulmasında temelde iki ciddi strateji belirmektedir: karşı koyma ve caydırıcılık. Bunlardan birincisi saldırı geldiğinde karşı koyma becerisini, ikincisi ise tehdit kaynağını saldırıdan vazgeçirme gücünü ifade etmektedir. Böylece hem savunma duvarlarının yükseltilmesi hem de potansiyelin kuvvetin ortaya konulması terörle mücadelede anahtar iki yönü oluşturmaktadır. Özele inilecek olursa geleneksel terörizmle mücadelede ortaya konulan siyasi, askeri, ekonomik, toplumsal ve hukuksal tüm araçların işe koşulması siber terörizmi önlemede de elzemdir.

Jian Hua ve Sanjay Bapna (2012) yaptıkları değerlendirmede siber terörizmle mücadelede teknolojik, hukuksal ve siyasi olmak üzere üç ayaklı bir çerçeve üzerinde durmaktadır. Teknolojik altyapının terörist saldırı caydırması ve önlemesi, siber suçlara karışanlara yönelik hukuksal düzenlemelerin daha net hale getirilmesi ve siyasi erkin ekonomi başta olmak üzere çeşitli alanlardaki uygulamalarla kişilerin siber terörizme bulaşmasını veya süreçten mağdur olmalarını engellemesi genel çizgisinde iddialarını temellendirmektedirler.

Terör gruplarının siber alanda sadece doğrudan saldırılar ile değil propaganda, psikolojik savaş ve algı yönetimi çerçevesinde de faaliyet sürdürmeleri karşı mücadelenin bu yönünü gündeme getirmektedir. Her ne kadar doğrudan saldırı veya şiddet eylemi olarak görülmese de bu faaliyetler terör örgütlerinin etkin ve etkili olmasında oldukça önemlidir. Siber alandaki bu girişimlerin önlenmesi bütüncül bir mücadelenin gereksinimlerindendir

(Darıcılı, 2020: 102-103). Toplumu ilgilendiren çeşitli olaylarda veya kararlarda örgütlerin müdahalesi ve manipülasyonları özellikle dikkat edilmesi gereken bir konuyu oluşturmaktadır. Doğrudan saldırıların yanı sıra özellikle sosyal medya üzerinden oluşturulmaya çalışılan kargaşa, panik ve güvensizlik ortamına yönelik ciddi incelemelerin yapılması gerekmektedir.

Siber terörizmle mücadelede savunma kadar değer verilmesi gereken nokta siber caydırıcılıktır. Siber caydırıcılık, alınan önlemler ve ortaya konulan savunma gücü sayesinde tehdit ortaya koyacak unsurun vazgeçmesi veya emellerini ertelemesi anlamına gelmektedir. Siber saldırıların ve tehdit kaynaklarının belirlenmesinin zor olması siber caydırıcılığı tartışmalı bir konu haline getirse de siber güç ve siber savunma artırımı karşı tarafın saldırılarını önledikçe caydırıcılık durumu da daha belirgin olmaktadır (Güntay, 2017a: 91-92). Genel güvenlik tartışmalarında en iyi savunmanın düşmanın kaçınmasına ve vazgeçmesine neden olan önlemler olduğu ifade edilmektedir. Bu noktada devletler hem kurumları hem de bireyleri korumak için alacağı önlemlerin ve uygulayabilecekleri karşı saldırıların terör örgütleri tarafından algılanması gerekmektedir. Önceki bölümde de bahsedildiği üzere terörizm fiziksel olduğu kadar psikolojik-zihinsel bir harekâttır. Hedef toplumdaki güven, inanç ve dayanışma bağlarını yok ederek avantaj elde etmeye çabalayan terör örgütlerine karşı savunmada etkili olabilecek unsur toplumsal irade ve birlikteliktir (Çıtak, 2020: 197). Ülkenin siber caydırı gücü topluma anlatılabildiği sürece, teröre karşı söz konusu birlikteliği sağlayan bir kolaylaştırıcı olabilecek ve güvende olduklarını hisseden halk yasal kurumlara bağlılıklarını pekiştireceklerdir. Ayrıca terörizme karşı mücadelenin topyekun bir faaliyet olması gerektiği anlayışıyla, toplum da devletin uygulamaya koyduğu siber savunmayı güçlendirmek için bireysel önlemler alma eğiliminde olabilecektir.

Siber dünyanın bilinmezlik ve muğlaklıkla dolu olması ve teknoloji alandaki dinamik yapı her türlü savunmayı bir gecede zamanın gerisinde bırakmaktadır. Fakat terörizmle mücadele mantalitesi de halihazırda bu şekilde işlemektedir. Zira alınan tüm önlemlere rağmen terör örgütleri toplumdaki açıkları kollayarak bir şekilde eylem girişiminde bulunabilmektedirler. Konu siber dünya olduğunda ise devletlerin henüz sınırlarını çizemediği ve hukuksal düzenlemeleri oluşturmadığı bir mecrada görünmeyen bir tehdide karşı ne kadar etkili olabilecekleri oldukça tartışmalıdır. Yine de terör örgütlerine bugüne kadar geçit verilmemesi, bu alandaki ulusal ve uluslararası önlemlerin etkililiğin kanıtını oluşturmaktadır.

Sonuç ve Değerlendirme

Terörizm çağımızın "belası" olarak tanımlanmaktadır. Dünya genelinde hiçbir toplum terörizm saldırısından muaf değildir ve bu da genele bir korku ortamı oluşturmaktadır. Halihazırda geleneksel terörizm devletler için oldukça ciddi bir meydan okumayı oluştururken, yeni terörizmin önemli bir boyutunu oluşturan siber terörizm ise üzerinde en çok tartışılan endişe kaynaklarından biridir. Bilgisayar ağ ve sistemlerini hem örgütsel ihtiyaçlarını

karşılamak hem de hedeflerine saldırılar düzenlemek için kullanabilen terör örgütleri oldukça kıymetli bir fırsata ulaşmışlardır.

Günümüzde siber alan tehlike ve tehditlerle dolu olan bir mecra olarak görülmektedir. Siber savaşlar, siber casusluk, siber saldırı, siber suçlar, siber terörizm gibi konular bu alanın kullanıcılarının risk endişesini artırmaktadır. Siber terörizm ise özelinde sadece isminde "terör" sözcüğü geçmesi nedeniyle korku ve panik halini artırmaya yetmektedir. Siber alanda hemen hemen her devlet, toplum, şirket veya birey bir şekilde siber saldırının bir türüne maruz kalmaktadır. Çeşitli gruplar oldukça uzmanlık gerektiren saldırılar düzenleyerek devletleri ve büyük şirketleri zora sokabilmektedirler. Buna rağmen terör örgütleri temelinde yıllardır beklenilen büyük saldırıların henüz gerçekleştiğine dair herhangi bir kayıt bulunmamaktadır. Pek tabii terör örgütleri casusluk yapma, çeşitli internet sayfalarını ele geçirme veya işlevsiz hale getirme, sosyal medyayı yönlendirme, bireysel hesaplara saldırma gibi faaliyetler gerçekleştirmektedirler; fakat günlük yaşamı veya ulusal güvenliği felce uğratacak düzeyde saldırılar düzenleyen terör örgütleri olmamıştır. Yine de geleceğin her türlü gelişmeye açık olduğunu ve siber terörizmi önleme için gerekli mücadelenin her an veriliyor olması elzemdir.

Terör örgütlerinin devlet denetimin kısmen muaf oldukları, daha az maliyetle ve insan kaynağıyla zarar oluşturabilecekleri siber saldırı fırsatını değerlendirmeye çalışmayacaklarını düşünmek oldukça güçtür. Kendini bir şekilde teknoloji alanında yetiştirmiş bir terör örgütü üyesinin dünyanın herhangi bir yerinden hedefinde olan özel ve tüzel kişiliklere saldırı yapabilmesi zor bir durum değildir. Fakat her ne kadar gizliliğin perdesi arkasına saklansalar da devletlerin karşı önlemleri saldırıyı ileri boyuta varmadan bertaraf edebilmekte ve bırakılan izlerin takip edilmesini olası kılmaktadır. Yine de geleceğimizde terör örgütlerinin siber saldırı kapasitelerini daha da artıracaklarını, zaaf yaşayan devletlere ciddi zararlar verebileceklerini ve hatta sadece siber alanda faaliyet gösteren terör gruplarının ortaya çıkabileceklerini ileri sürmek güç değildir.

Kaynakça

Ackerman, G. ve Burnham, M. (2019). Towards A Definition of Terrorist Ideology, *Terrorism and Political Violance*, 1-30.

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik*, Ankara: Orion.

Andress, J. ve Winterfeld, S. (2011), *Cyber Warfare: Techniques, Tactics, Tools for Security Practitioners*, Amsterdam: Syngress.

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

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

Bolz, F., Dudonis, K. J. ve Schulz, D. P. (2002). *The Counterterrorism Handbook: Tactics, Procedures, and Techiques*, CRC Press, Boca Raton.

Chu, H., Deng, D., Chao H. ve Huang, Y. (2009). Next Generation of Terrorism: Ubiquitous Cyber Terrorism with the Accumulation of All Intangible Fears, *Journal of Universal Computer Science*, 15(12), 2373-2386.

Cohen, D. (2014). Cyber Terrorism: Case Studies, Akhgar, B., Staniforth, A. ve Bosco, F. (Ed.), içinde *Cvber Crime and Cyber Terrorism Investigator's Handbook*, Syngress, 165-174.

Cox, C. (2015). Cyber Capabilities and Intent of Terrorist Forces, *Information Security Journal: A Global Perspective*, 24(1-3), 31-38.

Çıtak, E. (2020). Küresel Terörizm: Uluslararası Toplumun İmtihanı, Emre Çıtak ve Sami Kiraz (Ed.), içinde *Uluslararası Güvenlik: Gelenekselden Güncele Bir Gündem Analizi*, Ankara: Orion, 189-232.

Çifçi, H. (2013). *Her Yönüyle Siber Savaş*, Ankara: TÜBİTAK Bilim Kitapları.

Darıcılı, A. B. (2020). "Küresel Terörün Teknolojik Yönü: Siber Terörizm", Hasan Acar Ed., içinde *Küresel Terör ve Güvenlik Politikaları*, Ankara: Nobel, 93-106.

Drake, C. J. M. (1998). *Terrorist's Target Selection*, New York: St. Martin's Press.

Foltz, C. B. (2004). Cybercrime, Computer Crime, and Reality, *Information Management&Computer Security*, 12(2), 154-166.

Geers, K. (2009). The Cyber Threat to National Critical Infrastructures: Beyond Theory, *Information Security Journal: A Global Perspective*, 18(1), 1-7.

Gordon, S. ve Ford, R. (2002). Cyberterrorism?, *Computer&Security*, 21(7), 636-647.

Gross, M. L., Canetti, D. ve Vashdi, D. R. (2016). The Physchological Effects of Cyber Terrorism, *Bulletin of the Atomic Scientists*, 1-8.

Gunaratna, R. (2007). Ideology in Terrorism and Counter Terrorism: Lessons From Al Qaeda, Ed: A. Aldis ve G. P. Herd, içinde *The Ideological War on Terror: Worldwide Strategies on Counter-terrorism*, Londra: Routledge 21-34.

Güntay, V. (2017a). Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu: Siber Savaş Örneği, *Güvenlik Bilimleri Dergisi*, 6(2), 81-108.

Güntay, V. (2017b). Siber Uzay ve Güvenlik Politikası Üzerine Teorik Bir Yaklaşım, *Cyberpolitik Journal*, 2(4), 9-21.

Hekim, H. ve Başıbüyük, O. (2013). Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, *Uluslararası Güvenlik ve Terörizm Dergisi*, 4(2), 135-158.

Hua, J ve Bapna, S. (2012), How Can We Deter Cyber Terrorism, *Information Security Journal: A Global Perspective*, 21(2), 102-114.

Kasapoğlu, C. (2017). *Siber Güvenlik: 5. Boyutu Anlamak*, EDAM: Center For Economics And Foreign Policy Studies.

Keleştemur, A. (2015). *Siber İstihbarat*, Kocaeli: Level Kitap

Libicki, M. C. (2009). *Cyberdeterrence and Cyberwar*, Santa Monica: RAND Corporation.

Morgan, M. J. (2004). The Origins of New Terrorism, *Parameters*, 34, 9-42.

Newman, E. (2006). Exploring the 'Roots Causes' of Terrorism, *Studies in Conflict and Terrorism*, 29(8), 749-772

O'Brian, K. (2003). Information Age, Terrorism and Warfare, *Small Wars& Insurgencies*, 14(1), 183-206.

Pollitt, M. M. (1998). Cyberterrorism- Fact or Fancy?, *Computer Freud&Security*, 8-10.

Rineheart, J. (2010). Counterterrorism and Counterinsurgency, *Perspectives on Terrorism*, 4(5), 31-47

Schaake, M. ve Vermeulen, M. (2016). Towards A Values-Based European Foreign Policy To Cybersecurity, *Journal of Cyber Policy*, 1(1), 75-84.

Schmitt, M. (2012). Classification of Cyber Conflict, *Journal of Conflict&Security Law*, 17(2), 245-260.

Shiryaev, Y. (2012). Cyberterrorism in the Context of Contemporary International Law, *San Diego International Law Journal*, 14: 139, 139-192.

Singh, A. ve Siddiqui, A. T. (2011). New Face of Terror: Cyber Threats, Emails Containing Viruses, *Asian Journal of Technology&Management Research*, 1(1)

Smelser, N. J. (2007). *The Faces of Terrorism: Social and Psychological Dimensions*, Princeton: Princeton University Press.

Şeker, E. (2017). Siber Savunma Tatbikatları: Planlama, Uygulama Ve Değerlendirme, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 3(2), 33-41.

Şenol, M. (2016). Siber Güçle Caydırıcılık Ama Nasıl?, *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, 2 (2), 10-17.

Türkiye Stratejik Araştırmalar Merkezi (TASAM) (2004). Siber Terörizm Raporu, TASAM, İstanbul.

Weiman, G. (2004). Cyberterrorism: How Real Is The Threat?, *United States Institute of Peace*, Special Report 119.

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.