International
SOCIAL SCIENCES STUDIES Journal
Open Access Refereed E-Journal & Indexed & Publishing
e-ISSN: 2587-1587

Research Article

Subject Area
International Relations

Year: 2022
Vol: 8 Issue: 102
PP: 3100-3112

Arrival
14 July 2022
Published
30 September 2022
Article ID Number
64610
Article Serial Number
26

Doi Number
http://dx.doi.org/10.29228/sssj.64610

How to Cite This Article
Güven, F., Kanat, S. & Aktel, M. (2022). "Terörizm ve Siber Uzay" International Social Sciences Studies Journal, (e-ISSN:2587-1587) Vol:8, Issue:102; pp:3100-3112

Terörizm ve Siber Uzay[1]

Terrorism and Cyber Space

Ferit Güven [1] Selim Kanat [2] Mehmet Aktel [3]

[1] Dr., Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Kamu Yönetimi Bölümü, Isparta, Türkiye
[2] Dr. Öğr. Üyesi., Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü, Isparta, Türkiye
[3] Prof. Dr., Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Kamu Yönetimi Bölümü, Isparta, Türkiye

ÖZET

Bu çalışma terörizmin siber uzayda ne amaçla ne oranda ve nasıl faaliyet gösterdiğini ortaya koymayı amaçlamaktadır. Bu amaçla yapılan araştırmadaki motivasyon, terörizm ile internet ve siber uzay arasındaki ilişkinin güncel mevcut durumunun tespitiyle hem kavramsal hem de politik çalışmalara bir alt yapı oluşturma hedefimizdir. Çalışmanın hipotezi, terörizmin her geçen zaman siber uzayda varlığını ve etkinliğini artırdığıdır. Hipotez testinde kullanılan yöntem olarak literatür taraması ve örnek olayların analizi yoluyla bilimsel verilerden faydalanılmıştır. Bu konuda alanda kaleme alınmış yerli literatürün ötesinde yabancı literatür de incelenmiştir. Zira bu konudaki güncel literatür ağırlıklı olarak İngilizcedir. Hipotez testinde aynı zamanda sayısal ve oransal veriler de kullanılarak veri çeşitliliğinin ve objektifliğinin ortaya konulmasına çalışılmıştır. Araştırma neticesinde terörizmin siber uzayı her geçen gün daha fazla oranda ve yoğunlukta kullanıldığı anlaşılmıştır. Terörizmin günümüzde siber uzayı, haklı gördükleri davalarının propagandasını yapmak, örgüt içi iletişim kurmak, örgüte yeni üye kazanmak, eylemler gerçekleştirmek için bilgi ve istihbarat toplamak ve paylaşmak, örgüt içi eğitim vermek hem eylemsel hem de örgütsel planlama yapmak ve örgüt içi koordinasyonu sağlamak, eylemlerin ve örgütün finansmanını sağlamak amaçları ile kullandığı sonuçlarına ulaşılmıştır.

Anahtar Kelimeler: Siber Uzay, Terörizm, İnternet ve Terörizm, Yeni Terörizm, Siber Terörizm

ABSTRACT

This study aims to reveal how and for what purpose terrorism operates in cyberspace. The motivation in the research conducted for this purpose is to establish an infrastructure for both conceptual and political studies by determining the current state of the relationship between terrorism and internet and cyberspace. The hypothesis of the study is that terrorism increases its presence and effectiveness in cyberspace with each passing day. As the method used in hypothesis testing, scientific data was used through literature review and analysis of case studies. In addition to the domestic literature on this subject, foreign literature has also been examined. Because the current literature on this subject is mainly in English. In the hypothesis test, numerical and proportional data were also used to reveal the diversity and objectivity of the data. As a result of the research, it has been understood that terrorism uses cyberspace more and more every day. Today, cyberspace of terrorism is used to propagate the cases they deem justified, to communicate within the organization, to recruit new members to the organization, to gather and share information and intelligence to carry out actions, to provide in-organization training, to make both operational and organizational planning and to ensure intra-organizational coordination. It has been reached the results that the organization uses it for the purpose of financing.

Keywords: Cyberspace, Terrorism, Internet and Terrorism, New Terrorism, Cyber Terrorism

1. GİRİŞ

Terörizm ve siber uzay veya internet konusu üzerinde oldukça fazla bilimsel, akademik çalışma yapılmış bir alan olarak kabul edilebilir. Bunun en önde gelen nedeni olarak internetin terörizm üzerinde oldukça fark edilebilir, hatta devrim niteliğinde etkiler yapmış olması kabul edilebilir. Hatta internet ile terörizm eskisine nazaran çok daha küresel ciddi bir tehdit haline gelmiştir denilebilir. Terörizm bakış açısıyla internet ve terörizmin ilişkisini "gaz ile alevin buluşması" şeklinde tarif eden değerlendirmeler de yapılmıştır (Mantel, 2010: 130). Hatta bazı yorumlara göre internet, terörizme "terrorism 2.0" dönemini getirmiştir (Virkar, 2016: 1, 14). İnternet, terör örgütlerinin tehdit çeşitlerini, eylemlerini, etkilerini ve faaliyetlerini birçok alanda değiştirmiştir (Freiburger ve Crane, 2011: 127).

Siber uzay terimi ise interneti ve sunduğu imkanları kullanan insanların oluşturdukları varsayılan sanal bir aleme işaret etmektedir. Araştırmada bu terimin tercih edilmesinin nedeni internetin günümüzde gelmiş olduğu noktada siber alem ile gerçek yaşantı arasında etkileşim ve bağın bir yandan güçlenirken bir diğer yandan da somut gerçeklik karşısında giderek yaygınlaşan bir sanal gerçekliğin ortaya çıkmasıdır. Bu durum pek çok beşeri, toplumsal olguyu etkilediği gibi terörizmi de etkilemektedir ve ilerleyen zamanlarda da muhtemelen daha çok etkileyecektir. Artık teröristlerin siber uzaydaki eylemleri ile gerçek hayattaki teröristlerin fiziksel saldırıları arasındaki sınır giderek silikleşmektedir (Prince, 2016: 39-41).

[1] Bu çalışma Süleyman Demirel Üniversitesi Kamu Yönetimi Bölümü Doktora Programında yazılan "Siber Saldırılar ve Türk Kamu Yönetiminin Çözümleri" isimli tezden türetilmiştir.

Artık siber uzayda gerçekleştirilen terörist eylemler, teröristlerin silahlı saldırılarıyla benzer bir etki yaratmaktır (Yannakogeorgos, 2014: 43). Terör örgütleri, kendi ideolojileri, saldırıları ve eylemlerine yönelik propaganda, iletişim, para bulma, üye temini (Jarmon ve Yannakogeorgos, 2018: 156), eğitim, bilgi toplama ve silahlı ya da bombalı saldırıları planlama gibi faaliyetlerini çok büyük bir oranla siber uzayda gerçekleştirmektedirler. Örneğin yeni nesil teröristler artık siber uzayda yetişmektedir (Silke, 2010: 27-28). İnsanlık nasıl ki gerçek dünyada terör ile iç içe yaşamak durumundaysa bir bakıma internet üzerindeki insan topluluğu olarak niteleyebileceğimiz siber uzaya da terör ile birlikte yaşamak durumunda kalacaktır. (PoKempner, 2017: 42). Dolayısıyla en az gerçek hayatta terörizme karşı alınan önlemler kadar ciddi ve yaygın önlemlerin de siber uzayda da alınması gereklidir. Diğer türlü terörizmle mücadelenin önemli bir kanadı ihmal edilmiş olmaktadır.

Araştırmacıların değerlendirmelerinin de ötesinde siber uzay ve terörizm arasında her geçen gün yaygınlaşan derinleşen bir ilişki vardır. Gerçekleşen eylemlerin niteliği ve sayısal veriler incelendiğinde bu ilişki görülebilir. Bu çalışma da bu ilişkinin hangi başlıklar üzerinde yoğunlaştığını tespit ederek tem teorik hem de pratik çalışmalara katkı sağlamayı amaçlamaktadır. Bu faydanın ötesinde siber uzayda terörle nasıl mücadele edilmesi gerektiği konusunda bilgi ve veriye ihtiyacı olan uygulayıcılara da katkı sağlaması hedeflenmiştir.

Bu motivasyon ile yapılan bu çalışmanın cevap aradığı soru "terörizm siber uzaydan nasıl yararlanmaktadır?" sorusudur. Bu araştırma sorusuna dair hipotezimiz ise terörizmin siber uzaydan propaganda, iletişim, yeni üye kazanmak, bilgi toplamak ve paylaşmak, eğitim, eylem planlama ve gerçekleştirme, finans sağlamak hususlarında faydalandığıdır. Bu araştırma sorusu beraberinde "terörizm siber uzayda ne oranda varlık göstermektedir?", "terörizmin dijitalleşme eğilimi nedir?", "terörizmin başarısı siber uzayda gösterdiği faaliyetlere ne oranda bağlıdır?" gibi alt araştırma sorularını da çalışmada cevaplanmaya çalışılmıştır. Bu alt sorulara ilişkin araştırma hipotezlerimiz ise terörizmin her geçen gün giderek artan oranda siber uzayda ekinliğini artırdığı, Soğuk Savaşın bitişinden bu yana ve bilhassa son on yıldır hızlıca dijitalleştiği, siber uzaydan faydalanmanın terör örgütlerine ve eylemlerin başarısına katkı sağladığı, siber uzayın terörizmin cenneti haline geldiğidir.

Bu hipotezlerin testinde kullanılan temel yöntem ise literatür taraması yoluyla monografik tekniklerin kullanılmasıdır. Bu kapsamda yabancı literatür başta olmak üzere kapsamlı bir belgesel kaynak incelemesi yapılmış elde edilen veriler süreç değişim monografisi yöntemleriyle günümüze nasıl geldiği ortaya konuşmaya çalışılmıştır. Bunun yanında hipotezlerin testinde sayısal verilerden de faydalanılmış iddialar görüşler değerlendirmeler ve somut sayılar ve oranlar ile test edilmiş, desteklenmiştir.

Bu kapsamda yapılan bu araştırma raporunda önce terörizm ile siber uzay arasındaki güncel ilişki ilk başlıkta ortaya konuşmaya çalışılmıştır. Akabinde terörizmin siber uzayı nasıl hem bir propaganda ortamı ve aracı olarak kullandığına değinilmiştir. Sonrasında terörizmin siber uzayı iletişim için nasıl kullandığı ele alınmıştır. Bunlardan sonra terörizmin siber uzaydan yeni üye kazanmak, bilgi toplamak ve eğitim için nasıl faydalandığı açıklanmıştır. Ayrıca terörizmin siber uzaydan eylemlerin planlanması ve gerçekleştirilmesinde nasıl faydalandığı ortaya konuşmaya çalışılmıştır. Son olarak ise terörizmin siber uzaydan finansman elde etmek için nasıl faydalandığı değerlendirilmiştir.

2. TERÖRÜN SİBER UZAYI KULLANMA AMAÇLARI

İnternetin yaygınlaşmasıyla terör örgütleri giderek artan oranda doğrudan terör eylemleri gerçekleştirmenin yanında dolaylı yollardan internetten faydalanmaktadırlar. Siber uzayda, 1998 yılına kadar ABD'nin belirlediği 30 terör örgütünün ancak 12 tanesinin web sitesi vardı, oysa 2000 yılına gelindiğinde ise İsrail'in belirlediği 18 terör örgütünün 29 web sitesi tespit edilmiştir (Denning, 2010: 196). 2001 yılında internetteki 1.600 web sitesi, terör örgütleri ile ilişkiliydi. Terör örgütlerinin 2005 yılında 4.650 web sitesi varken, 2009 yılında bu rakam 6.800 adete çıkmıştır. Günümüzde küçük ya da büyük terör örgütlerinin hepsinin neredeyse tamamının web sitesi/siteleri bulunmaktadır (Weimann ve Kaplan, 2011: 95-96). Ocak 2008 tarihinde internet ortamında sadece El-Kaide'ye ait 5.600 web sitesi olduğu tahmin edilmekte ve her yıl bu sayıya 900'den fazla web sitesi eklenmektedir (Denning, 2010: 196).

Terör örgütleri internet ortamında, kendi ideolojilerinin yayılması ve örgütlerinin devamlılığının sağlanmasına yönelik çeşitli siber terör faaliyetlerini gerçekleştirirler (Baldi ve Gelbstein, 2003: 34). ABD Dışişleri Bakanlığı verilerine göre; 1997-2017 yılları arasında kurulmuş 70 farklı terör örgütü bulunmaktadır (USDSBCCVE, 2019). Bu terör örgütleri siber uzayı, ideolojilerini yayma, yeni üye kazanma, maddi kazanç elde etme, propaganda, iletişim, bilgi toplama ve paylaşımı, terör eğitimi, eylem planlama ve koordinasyon, örgüt yönetimi ve kontrolü maksatları doğrultusunda kullanmaktadırlar. Bu amaçlara yönelik terör örgütlerine ait web siteleri, sosyal medya hesapları, oyun siteleri, medya siteleri, videolar, e-mail hesapları, sohbet odaları (chat rooms), e-grups, forum sayfaları sayısı gün geçtikçe artmaktadır (Weimann, 2006: 27-30).

Artık terör örgütleri varlıklarını bir başka şekilde siber uzaya taşımışlardır (Radziwill, 2015: 88, 241). El-Kaide, 11 Eylül'den itibaren küresel düzeyde "siber cihad (cyber jihad)" başlatmış (Denning, 2016), özellikle 2003 ABD'nin Irak işgalinden sonra "cihadi (jihadi)" web sitelerinin sayısı artmıştır. El-Kaide, interneti planlama, yeni üye bulma ve para bulma açısından "güvenli cennet- safe haven" olarak tanımlamıştır (Ramsay, 2013: 1). 2002 yılında Arapça, İspanyolca ve İngilizce olmak üzere 1.000 ayrı web sitesi aktif halde terörist amaçlarla oluşturulduğu tahmin edilirken, 2010 yılına gelindiğinde ise 15 farklı dilde 100.000 web sitesi, forum, blog, sosyal medya hesabı teröristler tarafından kullanılır hale geldiği tahmin edilmektedir (Chen, 2012: 3).

Siber uzayı üye bulma, finans sağlama, propaganda yapma, taktik operasyon organizasyonu ve planlama maksatları ile kullanan ve siber uzayı iyi kullanan örgütlerden biri de IŞİD'dir. Dönemin IŞİD lideri Abu Bakar al-Baghdadi'nin 20 dakikalık ses kaydı ile kendisini "İslam Devleti (Islamic State- IS) Halifesi (Caliphate)" ilan ettiği 4 Temmuz 2014 tarihindeki Irak, Musul Ulu Cami'deki konuşması tüm sosyal medya ve aşırı radikal internet sitelerinde yayınlamış ve yayılmıştır (Kello, 2017: 128). IŞİD terör örgütü de, tıpkı EL-Kaide gibi siber uzayı etkin kullanmış ve uluslararası topluma "siber cihad" ilan etmiştir. Cyber Caliphate Army (CCA), Sons of Caliphate Army (SCA), Kalachnikov.TN(KTN) ve The United Cyber Caliphate (UCC) IŞİD'e ait hacking grupları içlerindeki en etkin olanlarıdır (Al-Bayati, 2017: 201). Cyber Caliphate, siber cihad (cyber jihad) ilan ederek ilk önce 12 Ocak 2015 tarihinde ABD'nin Merkez Kuvvetler Komutanlığı (U.S. Central Command)'na ait resmi Twitter ve YouTube sayfalarını tam da Başkan Obama'nın konuşması esnasında hacklemişlerdir (Anderson, 2020: 28). Nisan 2014'te ise IŞİD hackerları, Fransız TV5 kanalını kontrolünü ele geçirmişlerdir. IŞİD, TV5 kanalı üzerinden "Fransız askerleri IŞİD'den uzak durun, ailelerinizi kurtarma şansınız var. Bu fırsatı kaçırmayın. Cyber Caliphate İslam Devletinin düşmanlarına karşı siber cihada devam edecektir" şeklinde yayın yapmıştır (Goodman, 2015: 579-580). Şubat 2015'te Charlie Hebdo saldırısına ait görüntülerin yayınlanması üzerine Fransız İçişleri Bakanı Bernard Cazeneuve, ülkenin IŞİD'e ait 87 ayrı hacker grup tarafından 25.000 siber saldırıya maruz kaldığını açıklamıştır. Fransa Siber Savunma Şefi Amiral Arnaud Coustilliere basın açıklamasında; "ülkenin ilk kez bu kadar büyük çapta bir siber saldırı dalgasına maruz kaldığını" duyurmuştur (Atwan, 2015: 18, 27-28).

Weimann, teröristlerin interneti; psikolojik savaş, propaganda, veri sızıntısı, maddi gelir elde etme, üye temini, iletişim, eylemleri planlama, yönetme ve koordinasyon gibi konularda kullandıklarını belirtmiştir (2004: 1, 3, 5-10). 2012'de Fedotov tarafından BM için hazırlanan rapora göre de; terör örgütleri interneti, özellikle propaganda, üye toplama, iletişim, eylemlere yönelik üyelerini tahrik ve ikna çalışması, para bulma, eylem hazırlığı, saldırılarda kullandıkları malzemelerin temini, patlayıcı madde yapmak için kullanılan malzeme ve teknik bilgilere ulaşma gibi konularda etkin bir şekilde kullanmaktadır (2019).

2.1. Propaganda Yapmak

Terörizmde eylemler her zaman sembolik yani bir mesaj verme amacı taşıdığından propaganda, terörizmin adeta temelidir denilebilir. Propagandanın amacı; terör örgütlerinin ve eylemlerinin ideolojik mesajını aktarmaktır. İnternetin yaygınlaşmasından önceki dönemde propaganda yazılı-basılı materyaller, yüz yüze görüşmeler-toplantılar, radyo televizyon gibi geleneksel medya araçları ile yapılmaya çalışılırdı. Devletin istediğinde kontrol edebildiği, kısıtlı sayıca az kişilerin erişebildiği yazılı ve görsel medya, kitaplar, dergiler ve broşürlerin aksine düzensiz, devletin çok da kolay kontrol edemediği ve neredeyse herkesin erişebildiği internet, teröristler için bulunmaz bir propaganda aracı ve ortamı haline gelmiştir (Charvat, 2009: 79-80; Conway, 2004: 79). Bu açıdan siber uzay adeta, "terörizmin oksijeni" konumundadır (Carruthers, 1996: 102).

Terörizm, siber uzayı her şeyden önce davalarının sözde haklı gerekçelerinin propagandasını yapmak için kullanmaktadırlar. Örgütler, ikinci olarak da siber uzayda propagandayı, kendi üyelerine yönelik ikna ve motivasyon aracı olarak kullanmaktadırlar. Üçüncü olarak ise teröristler siber uzayda propagandayı hedef ülkedeki toplumda korku, endişe, panik ve kriz duygusu oluşturmak, kamu kurumlarına ve idarecilerine olan güveni sarsmak için kullanmaktadırlar (Barrett, 2012: 3).

Siber uzay terörizme, her çeşit propaganda için web sitelerinden, siber sosyal topluluklara kadar geniş bir yelpazede birçok olanaklar sunmaktadır (Bowman-Grieve, 2011: 76). Terör örgütlerinin propaganda maksadı ile internette halen en çok tercih ettiği yöntemlerden birisi, kendi ideolojilerini yaydıkları, liderlerini yücelttikleri ve eylemlerini duyurdukları web siteleridir. Terör örgütlerinin web siteleri, kendileri ile ilgili bilgileri aktardıkları, saldırılar sonrası olayı üstlendikleri, örgütün diğer üyelerine güç gösterisi yaptığı, örgüte bağlılık ve devamlılık ikna ve motivasyonu sağladığı, aynı zamanda da diğer örgütlerede ideolojik mesaj aktardıkları bir propaganda platformudur (Lachow, 2019).

Örneği Túpac Amaru terör örgütü 1996'da gerçekleştirdiği eylem ile Peru Japon elçiliğini işgal etmiştir. Rehin aldıkları kişiler karşılığında Peru hapishanelerindeki 400 mahkumunun serbest bırakılmasıdır. 5 aydan fazla süren işgal esnasında Peru Hükümeti ile pazarlık sürdürülmüştür. Görüşmeler sona erdiğinde, Peru Özel Kuvvetleri 22

Nisan 1997 tarihinde elçilik binasına girmişler, rehineleri kurtarmışlar, teröristlerin hepsini öldürmüşlerdir. Ancak operasyon esnasında rehinelerden biri ile 2 asker hayatını kaybetmiştir (Atkins, 2004: 321-323). Bu eylemin önemi ise teröristlerin bir uydu telefonu ve bir dizüstü bilgisayar ile Almanya merkezli bir web sitesi kurmuş olmalarıdır. Başta New York Times olmak üzere dünya medyası terör örgütünün kurduğu bu web sitesinden elde ettiği bilgilerle haber yayınları gerçekleştirmiştir. Terör örgütü bu web sitesi üzerinden asıl amaçlarına ulaşmış, dünya kamuoyuna eylemlerine ve ideolojilerine yönelik propagandalarını yapmışlardır. Dünya bu terör eylemi ile ilgili bilgileri Peru Devleti'nin resmi makamlarından değil, bu web sitesinden almıştır ve örgütün propaganda yapmasına dolaylı şekilde hizmet etmiştir (Denning, 2010: 195).

Web siteleri haricinde terör örgütleri, sosyal medya (dijital medya)'yı da giderek artan oranda bir propaganda platformu olarak kullanmaktadırlar. Hatta günümüzde teröristlerin temel propaganda aracı sosyal medya olmuştur (Cottee, 2019: 4). Günümüzde sosyal medya devletler ile terör örgütleri arasındaki geçmişten günümüze kadar uzanan mücadelenin yeni sahası olarak düşünülmektedir (Weimann, 2014: 15). Çünkü terör örgütleri, gerçekleştirdikleri saldırılarla, medyada ve sosyal medyada görünür ve duyulur olmak istemektedir (Anderson, 2004: 156). Artık terör örgütlerinin propaganda faaliyetlerinin %90'ı sosyal medya platformlarının kullanılması ile gerçekleştirdiği tahmin edilmektedir (Weimann, 2010: 19).

Siber uzayı ve bilhassa dijital medyayı propaganda maksadıyla ileri seviyede kullanan örgütlerin ilki El-Kaide'dir denilebilir. Sonrasında ise IŞİD sosyal medyayı bu amaç için en etkin kullanan örgüt olarak söylenebilir. Ladin'in ve Baghdadi'nin "siber cihad" ilan etmesi ile El-Kaide ve IŞİD, siber uzayın sunduğu tüm imkanları propaganda aracına dönüştürmüştür (Boletsi, 2013: 40). Her iki terör örgütü de özellikle "düşman" diye tanımladıkları devletlerin vatandaşlarının teröristlerce kafalarının acımasızca kesilerek öldürüldüğü videoları sosyal medyada yayınlayarak propaganda yapmışlardır (Darling, 2016: 147). Bilhassa IŞİD, soysal medyayı özel iletişim yöntemleri ve propaganda maksatlı kullanan bugüne kadarki en etkin terör örgütüdür (Edwards, 2019: 13). IŞİD ilk İngilizce propaganda videosunu 2014'te "cihaddan başka bir hayat yok - there is no life without Jihad" adı ile yayınlamıştır (Cottee, 2019: 11). Örgüt kendine ait propaganda maksatlı yüzlerce video, ses kaydı, film gibi yayınlar yapan aylık internet dergisi "Dabiq"i yayınlamıştır. IŞİD, aynı zamanda şifreli video ve sesli mesajlaşmayı sağlayan "Zello" adlı akıllı telefon uygulaması ve cep telefonlarını volki-tolkiye çeviren "Ansar al-Dawla al-Islamiya" adlı özel bir uygulamayı da hayata geçirmiştir (Weiss ve Hassan, 2016: 173, 176).

Benzer şekilde Eş-Şebab terör örgütü, 21 Eylül 2013'de Kenya'da gerçekleştirdiği Westgate Mall alışveriş merkezindeki saldırısını canlı olarak Twitter'dan yayınlamış ve anlık propaganda yapmıştır. 21-24 Eylül 2013 tarihleri arasında 4 gün süren eylem boyunca Eş-Şebab 556 tweet atmıştır (Mair, 2016: 65-67). Twitter, terör örgütünün hesabını kapatmış, Eş-Şebab sürekli yeni hesap açmayı denemiş ancak her seferinde Twitter kapatmıştır (Royce, 2015: 2). Saldırı sırasında adeta güvenlik güçleri ile teröristler arasında silahlı çatışma sürerken, siber uzayda da Twitter ile Eş-Şebab terör örgütü arasında adeta ayrı bir siber çatışma yaşanmıştır. Örneklerden hareketle denilebilir ki giderek yaygınlaşan dijital medya, terör örgütlerinin ideolojik amaçları doğrultusunda etkin rol oynamaya devam etmesi kuvvetle muhtemeldir (Hoffman, 2006: 225, 232; Weimann, 2004: 6)

Örgütlerin haricinde bir örgüte bağlı olmaksızın terör eylemi gerçekleştirenler için de siber uzay, neredeyse tek reklam ve propaganda mecrası haline gelmiştir. Örneğin 2011 de Norveç'in başkenti Oslo da bireysel terör eylemleri gerçekleştiren Breivik, "Eurabia" ve çok kültürlülük diye tanımladığı Avrupa'daki artan Arap nüfusu öldürmeyi hedefleyen ideolojisini yaymak ve destek kazanmak için kendi propagandasını internet vasıtasıyla yapmıştır (Miller ve Stivachtis, 2020: 445). Breivik, bireysel ve lidersiz bir aktör olarak internette çevrim içi (online) terör propagandası yapanların öncülerinden olmuştur (Wiederer, 2013: 50). Breivik, Şubat 2007 ile Kasım 2009 tarihleri arasında yazdığı ve ideolojisini yansıttığı 1.517 sayfalık manifestosunu saldırısından önce internette yayınlamıştır Spaaij, 2012: 1-2). Bu radikal ideolojisini yaymak maksadıyla da söz konusu manifestoyu 8.000 kişiye de e-maille göndermiştir. Breivik, bu adresleri Facebook'tan Ekim 2009 ile Mart 2010 tarihleri arasında topladığını eyleminden sonra polise verdiği ifadesinde belirtmiştir. Breivik sorgusunda, manifestosunun siber uzay yoluyla kendisi gibi 350.000 aşırı milliyetçiye ulaştığını iddia etmiştir (Gill, 2015: 78-83).

Benzer bir şekilde 2019'da Yeni Zelanda'da "Al Noor" camisi ve "Linwood Islamic Center" terör saldırılarında, saldırgan Brenton Tarrant saldırısını Facebook'ta 16 dakika boyunca canlı yayınlamıştır. Kullandığı 5 adet silahı da internet üzerinden online sipariş vererek satın aldığı anlaşılan Tarrant'ın Facebook'ta yayınlanan ilk videosu kaldırılmadan 4.000 kez izlenmiştir. Videonun yayılmasıyla ilk 24 saatte 1.5 milyon kişi bu katliam videosunu seyretmiştir (Macklin, 2019).

2.2. İletişim Kurmak

Terörizmin kalbi iletişimdir (Smith, 2015: 62). Yaklaşık 38 yıl önce Schmid ve Graaf; "İletişim olmadan terörizm de olmayabilirdi" diyerek iletişimin terör örgütleri için önemine dikkat çekmişlerdir (1982: 15). Çünkü terörizm

şiddetin planlı, uzun vadeli bir şekilde siyasi bir amacı hayata geçirmek üzere tercih edilen bir taktiktir. Siber uzay ise artık günümüzce web sitelerinden sanal iletişim platformlarına kadar geniş bir yelpazede teröristlere iletişim ve mesaj aktarma imkanı sunmaktadır (Bowman-Grieve, 2011: 76). Dünya iletişim anlamında 30-40 yıl öncesi ile kıyaslanamayacak bir seviyedir ve terörizm siber uzayı masrafsız, kolay bir iletişim aracı olarak da kullanmaktadır.

Örneğin 11 Eylül saldırılarını gerçekleştiren teröristler e-posta ile haberleşmişleridir. E-posta göndermeden saldırıyı şifreli olarak ortak e-posta hesaplarına notlar bırakarak iletişim kurarak gerçekleştirmişlerdir (Rustad ve Daftary, 2002: 828). Saldırının yöneticilerinden Abu Zubaydah'ın ele geçirilen bilgisayarında Mayıs 2001 tarihinden 2 Eylül 2001 tarihine kadar şifre ile korunmuş bir web sitesinde saldırı ile ilgili binlerce kriptolu mesaj tespit edilmiştir (Combs, 2006: 143). Siber uzay teröristlere bu imkanı ve hızı sunmaktadır (Singer ve Friedman, 2014: 101). Başka bir örnek olarak Taliban ise ABD merkezli bir web sunucusundan alan kiralamış ve iletişiminin bir kısmını burası üzerinden yapmıştır (Singer ve Friedman, 2014: 101)

Bu şekilde siber uzay sunduğu sosyal medya gibi çoklu iletişim imkanları ile terör örgütlerine aynı anda birden fazla eylem planlama ve gerçekleştirme ile bu eylemleri şifreli iletişimle alt liderlerle birlikte çoklu yönetme olanağı da sunmaktadır. Bu durum teröristlerin gizlenmesini kolaylaştırmakta, güvenlik ve istihbarat birimlerince izlenmelerini, takip edilmelerini ve ele geçirilmelerini zorlaştırmaktadır (Conway, 2006: 285-292). Terör örgütlerinin siber uzaydaki iletişimlerinin ve bilgi paylaşımlarının %90'ı çoğunlukla sosyal medya uygulamaları üzerinden gerçekleşmektedir (Stacey, 2017: 53). Facebook, Twitter, MySpace gibi sosyal medya platformları terör örgütlerince yoğun olarak kullanılmaktadır (Hesterman, 2013: 243). Teröristler, internet üzerinden siber uzayda özellikle sosyal medya uygulamalarının da artmasıyla stratejik iletişim tercihlerini internete taşımaya, interneti güvenli, sürdürülebilir, asimetrik bir ortam olarak (Bockstette, 2008: 20) hem diğer insanlar gibi açık hem de gizli iletişim maksatlı kullanmaya devam edeceklerdir (Reilly, 2006: 106).

2.3. Yeni Üye Kazanmak

Terör örgütleri her zaman yeni üyeler kazanmak için potansiyel aday havuzlarını geniş tutmak isterler. Artık günümüzde yeni üye kazanmanın en pratik ve etkili yöntemi internet üzerinden hareket etmektir. Özel çevrim içi yöntemler, videolar ve sosyal medya üzerinden kurulan temaslarla yeni üyeler tespit edilip, izole edilip, etkileme süresince terör örgütüne uygunluğu test edilip yeni üyeler terör örgütlerine kazandırılmaktadır (Don, 2007: 12-13). Bunun için yeni üyenin görüşüne uygun sohbet odaları kurmaktadırlar (Weimann, 2004: 8-9). Web sitesileri, oyun platformları ve sosyal medya üzerinden özellikle bilhassa gençlere yönelik videolar ve paylaşımlarla onları etkilemeye, güvenlerini kazanmaya çalışmaktadırlar (Weimann, 2006: 9-10, 15).

Terör örgütleri siber uzayda gençleri ırkçı ve dini sömürülerle birlikte (Gendron, 2016: 30-31), yaşadıkları ülkedeki politik ve yaşamsal ötekileştirme neticesinde gördükleri ayrımcılık ve baskıları da kullanarak kendi saflarına çekmeye çalışırlar (Sageman, 2004: 180). İnternette "brain drain" denilen beyin yıkama yöntemleri ile ABD, Avrupa ve dünyanın çeşitli ülkelerinden birçok genç Afganistan, Irak, Suriye ve Yemen'deki kriz bölgelerine El-Kaide ve IŞİD gibi terör örgütlerine savaşçı, canlı bomba, hacker, teknik üye olarak katılmışlardır (Cruickshank, 2014: 257-258).

Terör örgütlerinin potansiyel yeni üyeler için kurmuş olduğu birçok web sitesi ile (Kramer ve Wentz, 2008: 109) Irak'ın işgalinin başladığı 2002 yılından beri en az 200 canlı bomba intihar saldırısıcısı internet üzerinden örgütlere dahil edilmiştir. 1998 yılında sadece 12 adet terör örgütü web sitesinin bulunduğu bir siber uzay ortamının 2005 yılında 4.400 terör örgütü web sitesine çıkmasının bir nedeni de bu tür videolarla yeni üye kazanmak içindir (Johnson, 2008: 71).

Tarihte interneti yeni üye kazanımında etkin kullanan ilk terör örgütlerinden biri Zapatistalar'dır. Zapatistalar, 1994 yılında, dijital medyanın olmadığı internet imkanları ile sempatizanlarına ulaşmış ve binlerce insanı ideolojileri etrafında dünya çapında toplamışlardır (Hardcastle, 2011: 395). Zapatistalar, Temmuz 1994'ten itibaren ateş kes ilan edip "sivil seferberlik barışı" ile interneti etkin kullanmaya, destekçilerine ulaşmaya ve örgüte yeni üye bulmaya internet üzerinden başlamıştır (Nail, 2012: 104-105). Zapatistalar, Meksika'da bir anda 200-300 bin kişiyi Zocalo meydanında toplayabilirken, 40 farklı ülkede 100 farklı şehirde de internet üzerinden eriştiği benzer kalabalıkları aynı şekilde toplayabilir hale gelmiştir (Ronfeldt, 1998: 32). Zapatistalar, internet üzerinden iletişim sayesinde Meksika'daki Chiapas ormanlarından uluslararası arenada tüm dünyaca tanınan bir harekete dönüşmüştür (Belausteguigoitia, 2016: 97). Zapatistalar, halkın çoğunluğunun elektriği ve telefon hattı olmadığı bir ortamda 1994 yılında Zapatista Ulusal Kurtuluş Ordusu (Ejercito Zapatista de Liberacion Nacional - EZLN) adı verilen bir iletişim topluluğu kurmuşlardır. Zapatistalar, bu topluluğa ait olan websitesi "www.ezln.org" ile ulusal ve uluslararası düzeyde birçok destekçi ve yeni üye edinmiştir (Krovel, 2016: 351). Web siteleri ve e-maillerle devlet karşıtı olan 12.000 kişilik bir network olan "social netwar" ağını kurmuşlar ve örgütü genişletmişlerdir (Pitman, 2013: 96).

Örgüte yeni üye kazandırmada siber uzayın kullanılması günümüzde artık en yaygın yöntemdir. Uluslararası Radikalleşme Araştırma Merkezi (International Centre for the Study of Radicalisation - ICSR) çalışmasına göre; Nisan 2013 ile Haziran 2018 tarihleri arasında 80 farklı ülkeden 41.490 kişi IŞİD'e'a katılmak için Suriye ve Irak'a akmıştır. Bunların 7.366'sı geri dönmüştür. Son beş yılda katılımın en çok olduğu bölgeler; %92'lik bir oranla Orta Doğu ve Kuzey Afrika (Middle East and North Africa – MENA) Bölgesi, Rusya ve Eurasia Bölgesi ve Avrupa'dır. IŞİD'e 48 ülkeden en az 100 kişi katılırken (toplamda en az 4.800), 33 ülkeden de en az bir kişi katılım sağlamıştır (START, 2020).

IŞİD, özellikle Batı dünyasında doğmuş gençleri ve kadınları, online iletişim ve sosyal medya ağları üzerinden, Batı toplumunun onları nasıl ötekileştirdiği üzerine kurulu propaganda ile saflarına katmak noktasında başarılı olmuştur. Europol, 2017 yılında Avrupa'ya yönelik bu maksatla propaganda yapan 150 sosyal medya platformu tespit etmiştir (Smith ve Alarid, 2020: 186-187, 240). Tıpkı Londra'dan Shamima Begum (15), Kadiza Sultana (16) ve yaşı 15 olan adı bilinmeyen bir kızın da dahil olduğu 3 genç kızın Türk Havayolları ile İstanbul'a gelip buradan da sınırı geçerek Suriye'ye gidip IŞİD'e katılması düşündürücü bir şekilde bu tarz bir çabanın sonucudur. Batı devletlerinden özellikle internette yapılan propaganda ile 550'den fazla kadın IŞİD'in saflarına katılmıştır (Hill ve Marion, 2016: 158). West Point's Combating Terrorism Centre raporuna göre; yeni üye kazanımı maksadıyla IŞİD'e ait Ağustos 2015'de 700 web sitesi, 2017 yılında ise 200 web sitesi bulunmaktaydı. IŞİD'in yabancı savaşçı bulma ortalaması da 2015 yılında 2.000 iken, 2017 yılında ise örgütün etkinliğinin azalması ile 200'e düşmüştür (Gunaratna, 2017: 9). Ancak bu düşüş terör örgütlerinin yeni üye kazanmada en etkin ve örgüt için en verimli yöntemin siber uzay yoluyla üye kazanmak olduğu gerçeğini değiştirmemektedir.

2.4. Bilgi Toplamak ve Paylaşmak

Siber uzay, her bir birey ve organizasyon için olduğu kadar terör örgütleri için de bir bilgi toplama ve paylaşma kaynağıdır. Siber uzayın dünya toplumuna ışık hızında sunduğu en önemli hizmetlerinden biri de bilgidir (Amidror, 2008: 5). Bilgi herkes ve her organizasyon için başarı ile başarısızlık, doğru ile yanlış, yaşam ile ölüm arasında fark yaratan en hayati kaynaktır. Dolayısıyla terör örgütleri için de her türden bilgi en önemli kaynaktır (Forest, 2009: 273, 277).

Bu açıdan bakıldığında siber uzay terör örgütlerince açık kaynak istihbaratı gibi kullanılmaktadır. Limitsiz bir bilgi kaynağı, internette herkesin kullanımına açıktır. Böylelikle siber uzay aynı zamanda teröristlerce çok büyük bir bilgi aktarma ve paylaşım amaçlı kullanılan bir araçtır (Bockstette, 2008: 18-19). Terör örgütleri, silahlı ya da bombalı eylem gerçekleştirecekleri ülkelerdeki hedeflere yönelik istedikleri birçok bilgiye çok hızlı bir şekilde internet üzerinden ulaşabilmektedirler. Siber terörist hackerler kullanarak hedef sistemlere siber saldırı yöntemleri ile sızıp, erişim gerçekleştirip önemli ve gizli verilere ulaşabilmektedirler. Ayrıca terör örgütleri interneti bir kütüphane ve okul gibi kullanarak istedikleri her türlü silah kullanma ve patlayıcı hazırlama bilgisine erişebilmektedirler. Aynı zamanda bu edindikleri bilgileri ve verileri de yine internet üzerinden örgüt üyeleri ile paylaşmaktadırlar (Conway, 2006: 285-292).

2.5. Eğitim Vermek

Birçok terör uzmanı interneti, "terörist üniversitesi" olarak değerlendirmektedir. Teröristler saldırıları için gerekli olan birçok tekniği ve bilgiyi internetten öğrenebilmektedirler. El Kaide, ideolojik ve taktik eğitimlerini yazılı ve görsel olarak siber uzaya taşıyan ve etkin olarak kullanan terör örgütlerinin öncüsü konumundadır. Onu sosyal medyanın da yaygınlaşması ile diğerleri de takip etmiştir (Weimann, 2006). Nisan 2013'de ABD'deki Boston Maratonu bombalı saldırısında yakalanan Dzhokhar Tsarnaev ve kardeşi, El-Kaide'ye ait olan online dergi "Inspire"daki bir makaleden, adım adım nasıl "basınç ve parça tesirli bomba" yapılacağını öğrendiklerini sorgularında itiraf etmişlerdir. Eylemi de öğrendikleri gibi bu tarz bir bomba hazırlayarak gerçekleştirmişlerdir (Goodman, 2015: 50). Yani bir bomba yapmak için gerekli olanlar ya da çeşitli silah kullanma kılavuzları terör örgütlerince internet vasıtasıyla örgüt üyelerine öğretilmektedir (Barrett, 2012: 8-9). 2004 yılında İspanya'daki Madrid tren istasyonuna bombalı saldırıyı gerçekleştiren teröristlerden ele geçirilen bilgisayarda yapılan inceleme neticesinde, saldırı için ihtiyaç duydukları tüm bilgileri ve yöntemleri web sitelerinden öğrendikleri tespit edilmiştir (Mantel, 2009: 130).

Bunun haricinde teröristler siber uzay sayesinde yeni teknolojik silahlar hakkında teknik bilgiye ve saldırı taktiklerine ulaştıkları gibi onları nasıl elde edeceklerini de öğrenmektedirler (Dyson, 2015: 8). Tamil Kaplanları terör örgütü, intihar saldırılarında kullandıkları sürat botları için basit radar gizleme teknolojilerini, Kolombiya eylemler düzenleyen FARC örgütü ise uzaktan komutalı otomobillerle canlı bomba saldırıları için kullandıkları teknolojik bilgiyi ve hazırlama yöntemlerini internet üzerinden öğrenmişlerdir (Bennett, 2007: 3).

Yıllar içinde internetin yaygınlaşması ile canlı bomba saldırıları arasında bir ilişki olduğuna dair iddialar da vardır. Örneğin Afganistan'da 2001 ve 2002 yıllarında birer tane canlı bomba saldırısı olmuşken, 2003 yılında 2 adet, 2004 yılında 6 adet, 2005 yılında 21 adet, 2006 yılında 139 adet, 2007 yılında 140 adet, 2008 yılında 150 adet, 2011 yılında 461 adet, 2012 yılında ise 328 adet canlı bomba saldırısı olmuştur. Bomba yapımı ile ilgili bilgilerin siber uzay üzerinden aktarılarak öğretilmesi Afganistan'daki canlı bomba saldırılarının sayısının yıllara göre artmasında bir etken olarak değerlendirilmektedir (Jones, 2014: 390-391). Geleneksel terör eylemlerine dair eğitimlerin verilmesinin yanında siber uzayda, siber terörizme dair eğitimler de verilmektedir. İnternette sızma, uzaktan erişim sağlama, şifre çalma, güvenlik gibi hacking metotları eğitimleri verilmekte bu metotları öğreten yayınlar bile bulunabilmektedir (Denning, 2010: 199-200).

2.6. Planlama Yapmak ve Koordinasyon Sağlamak

Terör örgütleri ve bireysel eylemler gerçekleştirenler, siber uzayı eylemlerinin planlama ve koordinasyon aracı olarak da kullanmaktadırlar (Al-Bayati, 2017: 90-94). Yani teröristler interneti sadece nasıl bomba yapılacağını öğrenmek için değil aynı zamanda özellikli saldırıların planlaması ve koordinasyonu için de kullanırlar. 11 Eylül saldırılarının planlayıcılarından ve Mart 2002'de Pakistan'da tutuklanan El-Kaide'nin operasyon şefi Abu Zubaydah'ın (Fawdah, Fouda, Fielding, 2003: 102) bilgisayarında, Mayıs 2001 ile Eylül 2001 tarihleri arasında saldırının planlanmasına yönelik uçakları kaçıran teröristlerle binlerce şifreli mesajı bulunmuştur (Weimann, 2004: 10).

El-Kaide, 7 Ağustos 1998'de ABD'nin Kenya ve Tanzanya'daki elçiliklerinin yakınlarına bomba yüklü kamyonlarla eş zamanlı intihar saldırıları gerçekleştirmiştir. Teröristlerce intihar saldırılarının planlama ve koordinasyonu yerel internet ağları ile (Mogire, 2011: 133) SMS üzerinden gerçekleştirilmiştir. El-Kaide eş zamanlı saldırıların yönetimini de icraatını da (Moghadam, 2008: 86-87) internet üzerinden gizli ve şifreli iletişim sayesinde bir orkestra yönetir gibi planlamış ve koordine etmiştir (Atwan, 2015: 16).

El-Kaide ve IŞİD gibi (Almagor, 2017: 62) Eş-Şebab örgütü de interneti, 2007 yılından itibaren uluslararası küresel seviyede görünürlüğünü artıracak (Hansen, 2013: 59-60) seviyede, web siteleri, sohbet odaları ve sosyal medya imkanları ile saldırılarını planlama ve koordinasyon için kullanmıştır (Ploch, 2010: 9-10). Örgüt, Eylül 2013'te, Kenya Nairobi'de Westgate Mall adlı alışveriş merkezine yönelik 72 kişinin öldüğü silahlı ve bombalı bir saldırı gerçekleştirmiştir. Eylemi planlayan ve yöneten Al-Shabaab üyesi teröristler, saldırıyı Tweeter üzerinden koordine ederek anlık olarak emir komuta etmiştir. Bu terör saldırısı siber uzayda bir sosyal medya uygulaması üzerinden gerçek zamanlı yönetilen tarihteki ilk terör saldırısı olarak kayda geçmiştir (Weimann, 2014: 8). Terör saldırısını planlayan ve komuta eden 8 terörist, 21-24 Eylül 2013 tarihleri arasında saldırının koordinesi ve icraatına yönelik 556 tweet atmıştır. Saldırı esnasında 175 kişi de yaralanmıştır (Mair, 2016: 65-67). Günümüzde siber uzay teröristlerin lider kadrosunun saldırıları planladığı ve yönettiği, gizli bir karargâh gibi toplandıkları bir alan, mağara ya da hücre evi olmuştur.

2.7. Finans Sağlamak

Günümüzde teröristler için paranın olduğu yer artık bankalar, finans kurumları vb yerlerden ziyade, internettir (Smith, 2014: 9). Ekim 2002'de Endonezya Denpasar'daki ABD diplomatik temsilciliğine düzenlenen saldırıların planlayıcılarından Imam Samudra hapishanede kaleme aldığı otobiyografisinde; "iyi bir hackleme ile birkaç saat içinde bir polisin 6 aylık gelirini internette kazanabilirsin" diyerek internetin teröristler için kolay para bulma merkezi olduğunu belirtmiştir (Mantel, 2009: 144; Goodman, 2015: 51).

Eylemleri gerçekleştirmek için paraya ihtiyacı olan teröristler bu parayı artık daha çok internet ortamında bulmakta, toplamakta, saklamakta, transfer etmekte ve amaçları doğrultusunda kullanmaktadırlar (OECD, 2019: 23-24 ; Statista, 2019). İnternet bu terör örgütlerine ve teröristlere birçok farklı para bulma yöntemi sunmaktadır (Bocij, 2006: 16). Terör örgütleri internet sayesinde birkaç tuşa basarak bireysel kredi kartlarından para çekerek büyük bir operasyonun mali kaynağını da sağlayabilmektedirler (Lewis, 2002: 8). Terör örgütleri yüksek maliyetli saldırılarının parasal kaynağını genellikle internet üzerinden elde etmiş ve teröristlerine saldırılarını finanse etmek için aktarmışlardır (Freeman, 2016: 9-11; Williams, 2007: 78 ; Ryder, 2015: 20-24). Bu anlamda teröristler siber uzaydan bağışlar, çalma, hacking, siber dolandırıcılık gibi yöntemlerle para toplarlar (Barrett, 2012: 8-9 ; Goodman, 2015: 50). Para toplamanın yanında teröristler kanun dışı şekilllerde elde ettikleri kara paraları aklamak için de siber uzayı kullanmaktadır (United Nations Office on Drugs and Crime, 2019 ; Wilson, 2008: 16). İzi sürülemeyen kripto paraların da terörizm açısından bir kolaylık sağladığı da bu konuda söylenebilir.

3. SONUÇ VE ÖNERİLER

Siyasal bir şiddet türü olarak terörizm neredeyse insanlık tarihi ile eş geçmişiyle binyıllardır varlığı sürdürmektedir. Toplumsal hayatın devam ettiği sürece de sürdürmeye devam edecektir. Çünkü toplumsal yaşam devleti, devlet

siyaseti, siyaset de farklı siyasi amaçları doğurmaktadır. Birbiri ile çıkar çatışması olan siyasi amaçları savunanlardan nispeten güçsüz olanın tercih edeceği gayri insani siyasi şiddet türü olarak terörizm var olacaktır. Ancak gayri insani şiddetin eylemlerini gerçekleştirmek, toplumda korku yaratmak araçları zaman içerisinde değişmektedir. Örneğin ilk çağlarda korku yaratmak için kılıçlar kullanılırken sonraki zamanlarda silahlar kullanılmıştır. Günümüzde ise internet ve internet vasıtasıyla oluşan siber uzay, terörizmin hızla hem faaliyet yeni alanı hem de yeni aracı haline gelmektedir.

Denilebilir ki terörizm siber uzayda her geçen gün, üstelik büyük bir hızla varlığını artırmaktadır. 2000'li yılların başında sayıları onlarla ölçülen ve terörizm propagandası yapan internet sitelerinin sayısı günümüzde artık on binlerle ifade edilir hale gelmiştir. İnternet ağı büyüdükçe terörizmin de bu büyümeyle paralel bir şekilde ve olağanüstü bir hızla bu alanda faaliyetlerini artırdığını söylemek mümkündür. Bunu hayatın akışına toplumun değişimine terörizmin ayak uydurması olarak görmek mümkündür. Terörizmin en önemli unsurlarından birisinin propaganda yaparak hem taraftar toplamak hem de toplumun geneline korku salmak olduğu düşünülecek olursa, toplum en çok hangi haber kaynaklarını takip ediyorsa terörizmin de o mecrada varlığını artırması amacına ulaşması için yapması gereken şeydir.

Diğer bir değişle toplumun yaşamı dijitalleştikçe terörizm de dijitalleşmektedir. Bilişim teknolojilerinin yaygınlaşması ile insanların bu imkanlara ulaşmalarının kolaylaşmasına paralel bir şekilde kamu hizmetlerinin de, finans işlemlerinin de, iletişimin de, sosyal hayatın da kısaca hayatın dijitalleşmesi terörizmin de dijitalleşmesini beraberinde getirmektedir. Artık terörizmde iletişim, bilgi toplama ve istihbarat faaliyetlerinin neredeyse tamamı internet üzerinden gerçekleştirilmektedir. Özellikle dijital medyanın sunduğu anonim, isimsiz ve zamana mekana bağlı olmaksızın hareket edebilme imkanı, ucuzluğu, hızı, yaygınlığı dijitalleşmeyen terörist yapılarının varlıklarını daha fazla sürdürememeleri neticesini doğurmaktadır. Dijitalleşme dünyayı, sosyal yapıyı dönüştürürken bu yapının içinde olan terörizm de dönüşmektedir.

Bu durum aslında dijitalleşmeyen, siber uzayda varlık gösteremeyen ve kendisine bir yer edinemeyen terörizmin de etkinliğini kaybedeceği anlamına gelmektedir. Gerçek hayatta başarılı eylemler gerçekleştirmek için kriter adeta finans toplamak, örgüt üyelerini eğitmek, eylemleri planlamak ve koordinasyonu sağlamak için ne kadar siber uzaydan ne kadar yararlandığı haline gelmiştir. Diğer bir değişle siber uzaydan çağın gerektirdiği kadar yararlanamayan örgütlerin kendileri için başarılı sayılacak eylemler gerçekleştirmeleri çok güçtür. Artık çoğu terör uzmanının internet ortamını ve siber uzayı bir terörist üniversitesine benzetmelerinin altında bu gerçek yatmaktadır.

Dolayısıyla terörizmin dijitalleşmesi, siber uzaydan yararlanması ve siber uzayda eylemler gerçekleştirmesi terörizmin etkinliği için bir gerekliliktir. Terörizm hem gerçek hayattaki hem de siber uzayda gerçekleştireceği eylemlerin etkinliği için internetten mümkün olabildiğince faydalanmaktadır. Terörizmin siber uzaydaki faaliyetlerine bakacak olursak, bu faaliyetleri yedi başlık altında toplamak mümkündür. Bu tabi ki terörizm siber uzayda sadece bu başlıklar altında faaliyet gösterir anlamına gelmemektedir. Bu başlıklar siber uzayda terörizmin en yoğun faaliyet gösterdiği konular olarak tespit edilmiştir.

Her şeyden önce terörizm interneti propaganda yapmak için kullanmaktadır. Terörizmin özü propagandadır ve teröristlerin herhangi bir kısıtlamaya maruz kalmadan en geniş kitlelere en kolay ve maliyetsiz şekilde ulaşmasının yolu siber uzaydır. Bir diğer konu ise iletişimdir. Terörizm bilhassa örgüt içinde iletişim kurmak için internetten faydalanmaktadır. Zira iletişimin en ucuz, en kolay, en etkili ve güvenlik güçlerince takip edilmesi en zor aracı dijital medya yoluyla yapılan çeşididir. İletişim konusundaki bu durum terörizmin yeni üye kazanma faaliyetlerini neredeyse tamamen siber uzaya taşıması neticesini doğurmuştur. Terörizm ayrıca her türlü bilgi ve istihbarat toplamak ve paylaşmak için de doğal olarak siber uzayı kullanmaktadır. İnternet ve siber uzay çağımızın en büyük bilgi kaynağıdır. Bir tıklama ile dünyanın her yerinden her türlü bilgi cihazımızın ekranında karşımıza gelmektedir. Terörizmin siber uzayda faaliyet gösterdiği alanlardan birisi de eğitim faaliyetleridir. Bu aslında siber uzayın dünyanın bilgi kaynağı olmasının da etkisiyle ortaya çıkmaktadır. Elde edilen bilginin zaman ve mekandan bağımsız bir şekilde insanlara aktarılmasının en pratik yolu siber uzay olmaktadır. Dünyanın en büyük bilgi kaynağı olarak siber uzay başarılı eylemler gerçekleştirmek için etkin planlar yapmak, bu eylemleri etkin bir koordinasyon içinde gerçekleştirmek için de en etkin ve elverişli ortamı sunmaktadır. Tüm bunların yapılabilmesi için ise finansal kaynak gereklidir. Finans sektörü ise neredeyse tamamen siber uzaya taşınmıştır. Bankaların internet şubelerinin yanında, pek çok menkul kıymete internet üzerinden erişim mümkündür. Finansın siber uzaya taşınmasının belki de en son halkası tamamen dijital kripto paralar söylenebilir. Böylesi bir ortamda terörizmin de finansal faaliyetleri büyük oranda siber uzayda cereyan etmektedir.

İlerleyen zamanlarda ise terörizmin bu yedi alanda siber uzaydaki faaliyetlerini yoğunlaştırması ve hatta eylemlerini daha çok siber uzayda gerçekleştirmeyi tercih etmesi muhtemeldir. Bu dünyanın topyekûn

dijitalleşmesinin getirdiği bir sonuç olarak düşünülebilir. Toplumlar, insanlar dijitalleştikçe dijital varlıklar yaygınlaştıkça bunlara karşı gerçekleştirilen eylemler terörizmin de tipolojisini dijitalleştirecektir.

KAYNAKÇA

1. Al-Bayati, T. H., (2017), A New Counterterrorism Strategy: A New Counterterrorism Strategy: Why the World Failed to Stop Al Qaeda and ISIS/ISIL, and How to Defeat Terrorists, CA, USA, ABC-CLIO.
2. Amidror, Y., (2008), The Internet and Terrorism, Gal, C. S. - Kantor, P. B. - Shapira, B., (eds.), Security Informatics and Terrorism: Patrolling the Web, Amsterdam, The Netherlands, IOS Press.
3. Anderson, A., (2004), Risk, Terrorism, and the Internet, Clarke, D., (ed.), Technology and Terrorism, USA, Transaction Publishers.
4. Anderson, R. A., (2020), Online Utilization for Terrorist Self-Radcalization Purposes, Vacca, J. R., (ed.), Online Terrorist Propaganda, Recruitment, and Radicalization, NY, USA, CRC Press.
5. Atkins, S. E., (2004), Encyclopedia of Modern Worldwide Extremists and Extremist Groups, Westport, USA, Greenwood Publishing.
6. Atwan, A. B., (2015), Islamic State: The Digital Caliphate, CA, USA, Univercity of California Press.
7. Baldi, S. - Gelbstein, E. - Kurbalija, J., (2003), Hacktivism, Cyber-terrorism and Cyberwar: The Activities of the Uncivil Society in Cyberspace, Switzerland, Diplo Foundation.
8. Barrett, R., (2012), The Use of the Internet for Terrorist Purposes, NY, USA, United Nations Office on Drugs and Crime in Collaboration with the United Nations Counter-Terrorism Implementation Task Force Publishing and Library Section.
9. Belausteguigoitia, M., (2016), On Line, Off Line and In Line: The Zapatista Rebellion and the Uses of Technology by Indian Women, Landzelius, K., (ed.), Native on the Net: Indigenous and Diasporic Peoples in the Virtual Age, London, UK, Routledge.
10. Bennett, B. T., (2007), Understanding, Assessing, and Responding to Terrorism: Protecting Critical Infrastructure and Personnel, New Jersey, USA, John Wiley & Sons.
11. Bocij, P., (2006), The Dark Side of the Internet, Westport, CT, USA, Praeger Publishers.
12. Bockstette, C., (2008), Jihadist Terrorist Use of Strategic Communication Management Techniques, Germany, DIANE Publishing.
13. Boletsi, M., (2013), Barbarism and Its Discontents, CA, USA, Stanford University Press.
14. Bowman-Grieve, L., (2011), The Internet and Terrorism: Pathways towards Terrorism and Counter-Terrorism, Silke, A., (ed.), The Psychology of Counter-Terrorism, London, UK, Routledge.
15. Carruthers, S. L., (1996), Reporting Terrorism: The British State and the Media, 1919-94, Stewart, I. - Carruthers, S. L., (eds.), War, Culture, and the Media: Representations of the Military in 20th Century Britian, England, Fairleigh Dickinson University Press.
16. Charvat, J.P.I.A.G., Cyber Terrorism: A New Dimension in Battlespace, Czosseck, C. - Geers, K., (eds.), The Virtual Battlefield: Perspectives on Cyber Warfare, Amsterdam, The Netherlands, IOS Press.
17. Chen, H., (2012), Dark Web: Exploring and Data Mining the Dark Side of the Web, NY, USA, Springer Science & Business Media.
18. Cohen-Almagor, R., (2017), Jihad Online: How do Terrorists Use the Internet?, Freire, F. C., et al., (eds.), Media and Metamedia Management, Switzerland, Springer.
19. Combs, C. C., (2006), The Media as a Showcase for Terrorism, Forest, J. J. F., (ed.), Teaching Terror: Strategic and Tactical Learning in the Terrorist World, NY, USA, Rowman & Littlefield Publishers.
20. Conway, M., (2004), Cyberterrorism: Media Myth or Clear and Present Danger?, Irwin, J., (ed.), War and Virtual War: The Challenges to Communities, Amsterdam, The Netherlands, Rodopi.
21. Conway, M., (2006), "Terrorism and the Internet: New Media—New Threat?", Parliamentary Affairs, Volume 59, Issue 2, April 2006, ss. 283–298.
22. Cottee, S., (2019), ISIS and the Pornography of Violence, London, UK, Anthem Press.

23. Cruickshank, P., (2014), The 2006 Airline Plot, Hoffman, B. - Reinares, F., (eds.), The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden's Death, NY, USA, Columbia University Press.
24. Darling, D., (2016), Perspectives on the Insurgency, Steed, B. L., (ed.), Voices of the Iraq War: Contemporary Accounts of Daily Life: Contemporary Accounts od Daily Life, CA, USA, ABC-CLIO.
25. Denning, D. E., (2010), Terror's Web: How the Internet is Transforming Terrorism, Jewkes, Y. - Yar, M., (eds.), Handbook of Internet Crime, NY, USA, Routledge.
26. Denning, D. E., "Whither Cyber Terror?", http://essays.ssrc.org/10yearsafter911/whither-cyber-terror/, (24.01.2016).
27. Don, B. W., et al., (2007), Network Technologies for Networked Terrorists, CA, USA, Rand Corporation.
28. Dyson, W. E., (2015), Terrorism: An Investigator's Handbook, Fourth Edition, London, UK, Routledge.
29. Edwards, J. A., (2019), The Myth of the Caliph: Suffering and Redemption in the Rhetoric os ISIS, Krona, M. - Pennington, R., (eds.), The Media World of ISIS, Indiana, USA, Indiana University Press.
30. Fawdah, Y. - Fouda, Y. - Fielding, N., (2003), Masterminds of Terror: The Truth Behind the Most Devastating Terrorist Attack The World has ever Seen, NY, USA, Arcade Publishing.
31. Fedotov, Y., "The Use of the Internet for Terrorist Purposes", United Nations, September 2012, https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, (28.01.2019).
32. Forest, J. J. F., (2009), Knowledge Transfer and Shared Learning among Armed Groups, Norwitz, J. H., (ed.), Pirates, Terrorists, and Warlords: The History, Influence, and Future ofArmed Groups Around the World, NY, USA, Skyhorse Publishing Inc.
33. Freeman, M., (2016), Sources of Terrorist Financing: Theory and Typology, Freeman, M., (ed.), Financing Terrorism: Case Studies, NY, USA, Routledge.
34. Freiburger, T. - Crane, J. S., (2011), The Internet as a Terrorist's Tool: A Social Learning Perspective, Jaishankar, K., (ed.), Cyber Criminology: Exploring Internet Crimes and Criminal Behavior, NY, USA, CRC Press.
35. Gendron, A., (2016), The Call to Jihad:Charismatic Preachers adn the Internet, Aly, A., et al., (eds.), Violent Extremism Online: New Perspectives on Terrorism and the Internet, London, UK, Routledge.
36. Gill, P., (2015), Lone-Actor Terrorists: A Behavioural Analysis, London, UK, Routledge.
37. Goodman, M., (2015), Future Crimes, London, Great Britain, Penguin Random House.
38. Gunaratna, R. (2017), "Global Threat Forecast", Counter Terrorist Trends and Analyses, January 2017, Volume 9, Issue 1, ss. 1-79.
39. Hansen, S. J., (2013), Al-Shabaab in Somalia: The History and Ideology of a Militant Islamist Group, 2005-2012, NY, USA, Oxford University Press.
40. Hardcastle, D. A., (2011), Community Practice: Theories and Skills for Social Workers, Third Editon, Oxford, UK, Oxford University Press.
41. Hesterman, J. L., (2013), The Terrorist-Criminal Nexus: An Alliance of International Drug Cartels Organized Crime, and Terror Groups, USA, CRC Press.
42. Hill, J. B. - Marion, N. E., (2016), Introduction to Cybercrime: Computer Crimes, Laws, and Policing in the 21st Century, CA, USA, ABC-CLIO.
43. Hoffman, B., (2006), "The Use of the Interent by Islamic Extremists", ss. 1-23, http://www.rand.org/content/dam/rand/pubs/testimonies/2006/RAND_CT262-1.pdf, (23.07.2019).
44. Hoffman, B., (2006), Inside Terrorism, NY, USA, Columbia University Press.
45. Jarmon, J. A. - Yannakogeorgos, P., (2018), The Cyber Threat and Globalization: The Impact on U.S. National and International Security, Maryland, USA, Rowman & Littlefield.
46. Johnson, T. A., (2008), The War on Terrorism: A Collision of Values, Strategies, and Societies, NY, USA, CRC Press.

47. Jones, S. G., (2014), Al-Qaeda Terrorism in Afghanistan, Bruce Hoffman - Fernando Reinares, (eds.), The Evolution of the Global Terrorist Threat: From 9/11 to Osama bin Laden's Death, NY, USA, Columbia University Press.
48. Kello, L., (2017), The Virtual Weapon and International Order, USA, Yale University Press.
49. Kramer, F. D. - Wentz, L. K., (2008), Cyber Influence and International Security, Washington D.C., USA, DIANE Publishing.
50. Krovel, R., (2016), Insurgency in the Age of the Internet: The Case of the Zapatistas, Fahlenbrach, K. - Sivertsen, E. - Werenskjold, R., (eds.), Media and Revolt: Strategies and Performances from the 1960s to the Present, Oxford, UK, Berghahn Books.
51. Lachow, I., "Cyber Terrorism: Menace or Myth?", http://ctnsp.dodlive.mil/files/2014/03/Cyberpower-I-Chap-19.pdf, (26.02.2019).
52. Lewis, J. A., (2002), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", Center for Strategic and International Studies, December 2002, pp. 1-12.
53. Macklin, G., "The Christchurch Attacks: Livestream Terror in the Viral Video Age", July 2019, https://ctc.usma.edu/christchurch-attacks-livestream-terror-viral-video-age/, (14.10.2019).
54. Mair, D., (2016), #Westgate: A Case Study – How al- Shabaab used Twitter During an ongoing Attack, Aly, A., et al., (eds.), Violent Extremism Online: New Perspectives on Terrorism and the Internet, NY, USA, Routledge.
55. Mantel, B. (2010), Terrorism and the Internet: Should Web Sites That Promote Terrorism Be Shut Down?, Jost, K., et al., (eds.), Issues in Terrorism and Homeland Security: Selections From CQ Researcher, Second Edition, California, USA, SAGE.
56. Mantel, B., (2009), "Terrorism and the Internet", CQ Resarcher, November 2009, Volume 3, Issue 11, ss. 129-153.
57. Miller, A. - Stivachtis, Y. A., (2020), Public-Private Partnerships and the Private Sector's Role in Countering the Use of the Internet for Terrorist Purposes, Vacca, J. R., (ed.), Online Terrorist Propaganda, Recruitment, and Radicalization, USA, CRC Press.
58. Moghadam, A., (2008), The Globalization of Martyrdom: Al Qaeda, Salafi Jihad, and the Diffusion of Suicide Attacks, Baltimore, USA, Johns Hopkins University Press.
59. Mogire, E., (2011), Victims as Security Threats: Refugee Impact on Host State Security in Africa, Farnham, UK, Ashgate Publishing.
60. Nail, T., (2012), Returning to Revolution, Edinburg, UK, Edinburg University Press.
61. OECD, "Money Laundering and Terrorist Financing Awareness Handbook for Tax Examiners and Tax Auditors", https://www.oecd.org/tax/crime/money-laundering-and-terroristfinancing-awareness-handbook-for-tax-examiners-and-tax-auditors.pdf, (18.12.2019).
62. Pitman, T., (2013), Latin American Cyberprotest: Before and After the Zapatistas, Taylor, C. - Pitman, T., (eds.), Latin American Cyberculture and Cyberliterature, Liverpol, UK, Liverpool University Press.
63. Ploch, L., (2010), Countering Terrorism in East Africa: The U. S. Response, Wshington, D.C., USA, DIANE Publishing.
64. PoKempner, D., (2017), The Internet is Not the Enemy, Human Rights Watch, World Report 2017: Events of 2016, USA, Seven Stories Press.
65. Prince, J., (2016), Psychological Aspects of Cyber Hate and Cyber Terrorism, Awan, I. - Blakemore, B., (eds.), Policing Cyber Hate, Cyber Threats and Cyber Terrorism, NY, USA, Routledge.
66. Ramsay, G., (2013), Jihadi Culture on the World Wide Web, USA, Bloomsbury Publishing.
67. Reilly, P., (2006), Civil Society, the Internet and Terrorism, Oates, S. - Owen, D. - Gibson, R. K., (eds.), The Internet and Politics: Citizens, Voters and Activists, NY, USA, Routledge.
68. Ronfeldt, D., et al., (1998), The Zapatista 'Social Netwar' in Mexico, CA, USA, RAND.

69. Royce, E. R., (2015), The Evolution of Terrorist Propaganda: The Paris Attack and Social Media, Washington, USA, U.S. Government Publishing Office.
70. Rustad, M. - Daftary, C., (2002), E-business Legal Handbook, USA, Aspen Law & Business.
71. Ryder, N., (2015), The Financial War on Terrorism: A Review of Counter-Terrorist Financing Strategies since 2001, NY, USA, Routledge.
72. Sageman, M., (2004), Understanding Terror Networks, USA, University of Pennsylvania Press.
73. Schmid, A. P. - Graaf, J., (1982), Violance as Communication: Insurgent Terrorism and the Western News Media, Beverly Hills, CA, USA, SAGE.
74. Silke, A., (2010), The Internet&Terrorist Radicalisation: The Psychological Dimension, Dienel, H. L., (ed.), Terrorism and the Internet: Threats, Target Groups, Deradicalisation Strategies, Amsterdam, Netherlands, IOS Press.
75. Singer, P. W. - Friedman, A., (2014), Cybersecurity: What Everyone Needs to Know, NY, USA, Oxford University Press.
76. Smith, J. M. - Alarid, M., (2020), Terrorism Recruitment and Radicalization into 21st Century, Vacca, J. R., (ed.), Online Terrorist Propaganda, Recruitment, and Radicalization, NY, USA, CRC Press.
77. Smith, P. J., (2015), The Terrorism Ahead: Confronting Transnational Violence in the Twenty-First, NY, USA, Routledge.
78. Smith, R., (2014), CyberCrime - A Clear and Present Danger The CEO's Guide to Cyber Security, USA, Lulu.
79. Spaaij, R., (2012), Understanding Lone Wolf Terrorism: Global Patterns, Motivations and Prevention, London, UK, Springer Science & Business Media.
80. Stacey, E., (2017), Combating Internet-Enabled Terrorism: Emerging Research and Opportunities, PA, USA, IGI Global.
81. Statista, "Richest terrorist organizations worldwide in 2017 (in million U.S. dollars)", https://www.statista.com/statistics/950492/richest-terrorist-organizations-worldwide/, (28. 06 .2019).
82. The National Consortium for the Study of Terrorism and Responses to Terrorism (START), "Global Terrorism Index 2018: Measuring the Impact of Terrorism", http://visionofhumanity.org/app/uploads/2018/12/Global-Terrorism-Index-2018-1.pdf, (03.11.2019).
83. United Nations Office on Drugs and Crime, "The Use Of The Internet For Terrorıst Purposes", https://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf, (17.02.2019).
84. Virkar, S., (2016), The Miror Has Two Faces: The terroist use of the Internet and Challenges of Governing Cyberspace, Silva, E., (ed.), National Security and Counterintelligence in the Era of Cyber Espionage, USA, IGI Global.
85. Weimann, G., (2004), Www.terror.net: How Modern Terrorism Uses the Internet, Washington, USA, DIANE Publishing.
86. Weimann, G., (2006), Terror on the Internet: The New Arena, the New Challenges, Washington, D.C., USA, US Institute of Peace Press.
87. Weimann, G., (2010), Terrorist Facebook: Terrorists and Online Social Networking, Last, M. - Kandel, A., (eds.), Web Intelligence and Security, Amsterdam, Netherlands, IOS Press.
88. Weimann, G., (2014), "New Terrorism and New Media", Commons Lab of the Woodrow Wilson International Center for Scholars, 2014, Volume 2, ss. 1-20.
89. Weimann, G., "Terror on the Internet – The New Arena, the New Challenges", The Washington Times, May 22, 2006, http://www.washingtontimes.com/news/2006/may/22/20060522-101437-1668r/, (08.02.2019).
90. Weiss, M. - Hassan, H., (2016), ISIS: Inside the Army of Terror, Updated Edition, NY, USA, Regan Arts.
91. Wiederer, R., (2013), Maping the Right-Wing Extremist Movement on the Internet – Strustual Patterns 2006-2011, Deland, M. - Minkenberg, M. - Mays, C., (eds.), In the Tracks of Breivik: Far Right Networks in Northern and Eastern Europe, Berlin, Germany, LIT Verlag Münster.

92. Williams, H. J. - Chandler, N. - Robinson, E., (2018), Trends in the Draw of Americans to Foreign Terrorist Organizations from 9/11 to Today, CA, USA, Rand Corporation.

93. Williams, P., (2007), Warning Indicators and Terrorist Finances, Giraldo, J. K. - Trinkunas, H. A., (eds.), Terrorism Financing and State Responses: A Comparative Perspective, CA, USA, Stanford University Press.

94. Wilson, C., (2008), "Botnets, Cybercrime, and Cyberterrorism: Vulnerabilities and Policy Issues for Congress", Congressional Research Service (CRS) Report for Congress, January 29, 2008, ss. 1-43.

95. Yannakogeorgos, P .A., (2014), Rethinking the Threat of Cyberterrorism, Chen, T. M. - Jarvis, L. - Macdonald, S., (eds.), Cyberterrorism: Understanding, Assessment, and Response, NY, USA, Springer.