Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Kasım 2022,Cilt:11, Sayı:2, 441-470
doi:10.28956/gbd.1092120

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, November 2022,Volume:11, Issue:2, 441-470
doi:10.28956/gbd.1092120

Makale Türü ve Başlığı / Article Type and Title
Araştırma/ Research Article
Siber Alanda Radikalleşme ve İnternetin Panoptik Gözetimi
Radicalization in Cyberspace and Panoptic Surveillance of the Internet

Yazar(lar) / Writer(s)
1- Mehmet KURUM, Dr., Jandarma ve Sahil Güvenlik Akademisi Terörizm Araştırmaları Merkezi Müdürlüğü, Ankara, mkurum@yahoo.com, ORCID ID https://orcid.org/0000-0002-5387-4188
2- Alper BİLGİÇ, Dr., Jandarma ve Sahil Güvenlik Akademisi Terörizm Araştırmaları Merkezi Müdürlüğü, Ankara, alperbilgic@yahoo.com, ORCID ID https://orcid.org/0000-0002-1918-2233
3- Begüm ÇARDAK, Dr., Jandarma ve Sahil Güvenlik Akademisi Terörizm Araştırmaları Merkezi Müdürlüğü, Ankara, begumcrdk@gmail.com, ORCID ID https://orcid.org/0000-0002-1847-3477

Bilgilendirme / Acknowledgement:
-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.-

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received :23.03.2022
Makale Kabul Tarihi / Accepted :08.09.2022

Atıf Bilgisi / Citation:
Kurum M. Bilgiç A. ve Çardak B. (2022). Siber alanda radikalleşme ve internetin panoptik gözetimi, *Güvenlik Bilimleri Dergisi, 11(2), ss 441-470. doi:10.28956/gbd.1092120*

SİBER ALANDA RADİKALLEŞME VE İNTERNETİN PANOPTİK GÖZETİMİ

Öz

Siber alanın kullanımının bireyleri geniş bir kitleye hızlı bir şekilde kolayca bağlaması ve etkileşim ağı oluşturması, benzer düşünen insanlardan oluşan bir hareket ve sinerji yaratmaktadır. Bu durum terörizm kavramlaştırması bakımından protesto, propaganda, finansman, eleman temini, eğitim ve eylem planlaması üzerinde radikalleşme bağlamında dönüştürücü etki yaratmaktadır. Böylesi bir ortamda anonimlik sağlayan uygulamaların da varlığıyla çeşitli gruplar hareket serbestisi kazanmaktadır. Bu çok etkileşimli ortamda kontrol ve gözetim, devlet aktörleri bakımından da sorunlu bir alan yaratmaktadır. 1785 yılında, Jeremy Bentham`ın fikriyatını temel alarak Samuel Bentham tarafından mimari tasarımı yapılan panoptikon kavramı, bütünü gözetlemek anlamı taşımaktadır. Gözetim kavramı, fiziksel alan başta olmak üzere pek çok alanda kitlelerin kontrol edilebilirliği düşüncesini etkilemektedir. Bu çalışma; siber alanda çeşitli unsurlar aracılığıyla bireylerin aşırılıkçılığa yönelenebilmesi risk durumuna karşı, siber alanın suç grupları ve özellikle terör örgütleri tarafından istismar edilebilir olmasının neden ve nasıl olduğunu ortaya koymakta aynı zamanda da bu tehdidin önüne geçmek için siber alanda alınabilecek tedbirler hakkında farkındalık yaratmayı amaçlamaktadır.

Anahtar Kelimeler: *Algokrasi, Panoptikon, Radikalleşme, Siber, Şeffaf Toplum*

RADICALIZATION IN CYBERSPACE AND PANOPTIC SURVEILLANCE OF THE INTERNET

Abstract

The fact that the use of cyberspace, easily connects individuals to a wider audience in a rapid sense and creates an interaction network, develops a movement and synergy within like-minded people. In terms of terrorism conceptualization, this creates a transformative effect on protest, propaganda, financing, recruitment, education and action planning in the context of radicalization. In such environment, various groups gain freedom of movement through the existence of applications that provide anonymity. Control and surveillance in this highly interactive environment also creates an area of concern for state actors. The concept of the panopticon, which was designed by Samuel Bentham in 1785, based on the idea of Jeremy Bentham. This concept means monitoring the whole. The notion of surveillance affects the idea of controllability of the masses in many areas, especially in the physical ones. This study aims to raise awareness in the context of the use of mass surveillance in cyberspace since individuals can be radicalized there. In this study, the descriptive method will be used and the state actors use of mass surveillance of the Internet will be discussed in the context of radicalization in cyberspace.

Keywords: *Algocracy, Panopticon, Radicalization, Cyber, Transparency Society.*

GİRİŞ

Siber alan, siber uzay, siber dünya, siber ortam vb. adlar altında tanımlanan ağlar üzerinden birbirine bağlı sistemlerin ve hizmetlerin elektronik cihazlar ve bilgisayarlar vasıtasıyla kullanıcılarının İnternet üzerinde küresel anlamda etkileşimleri; söz konusu kullanıcıların giderek artan sayısına koşut olarak artış göstermektedir (Bilgiç, 2021, s. 33). Yirminci yüzyılın son yarısından itibaren giderek artan İnternet üzerinden etkileşimin, bu ortamda bilgisayar sistemlerinin ve kullanıcılarının istismarının yaygınlaşmasına da vesile olduğu değerlendirilmektedir.

Diğer birçok faktörün yanı sıra, "Soğuk Savaş" olarak adlandırılan dönemin sona ermesi, güvenlik algısı ve ortamının da dönüşümüne neden olmuştur. Bu durum, siber alanı; diğer suç türlerinin yanında, özellikle yeni terörizm tanımlaması altında çeşitli gruplar için sömürünün de ilgi odağı hâline getirmiştir. Dünya üzerinde artan çatışma alanlarına çok sayıda "yabancı terörist savaşçı" olarak tabir edilebilecek kişiler dâhil olmuştur. Bu çatışmaların, fiziksel ortamda olduğu kadar siber alanda da var olmasıyla, mesafenin görece önemsizleştiği ve sınırların bulanıklaştığı, tehdidin giderek arttığı bir ortam oluşmaktadır (Çardak, 2021, s. 320).

Yirminci yüzyılın son yarısında İnternet kullanımının yaygınlaşmaya başladığı dönemde, ilk sosyal bağlantı araçlarından birisi olarak e-postalar öne çıkmaktaydı. Tek tuşun uzakları yakın ettiği bu iletişim devrimi, günümüzde bir anlamda dünyanın nispeten küçülmesine neden olmuştur. Stanley Milgram'ın çok bilindik "Küçük Dünya Deneyi"nde vurgulanan ayrılığın altı derecesinde[1] küçülen dünya; İnternetteki artan kullanıcı etkileşimleri ve kullanıcıların çeşitli mecralarda takipleşmeleri nedeniyle bir bakıma daha da küçülmektedir. Bu küçülme; terör örgütlerinin hedef kitlelerine erişimini kolaylaştırarak örgütlerin kaynak ve hedefini bir başka ifade ile terör örgütünün hem müzahir hem de düşman olarak tanımladığı unsurları olağanüstü bir ölçüde yakınlaştırmıştır. Bu ortam radikalleşmeye de yeni bir pencere açmıştır.

Her ne kadar radikalleşme yeni ortaya çıkan bir olgu olmasa da, İnternet ve İnternet araçlarının kullanımı; özellikle terörizm kavramlaştırması bakımından protesto, propaganda, finansman, eleman temini, eğitim ve eylem planlaması üzerinde radikalleşme bağlamında dönüştürücü etki yaratmaktadır. İnternet kullanımının bireyleri geniş bir kitleye hızlı bir şekilde kolayca bağlaması ve

[1] Dünya üzerinde farklı yerlerdeki iki birey arasında altı adımda ilişki kurulabileceğine dayalı bir sosyal teoridir.

etkileşim ağı oluşturması, benzer düşünen insanlardan oluşan bir hareket ve sinerji yaratmaktadır. Bu bağlamda, İnternet aracılığıyla grupların radikalleştirilmesi ve bunlar arasındaki fikir alışverişi ve birlikte hareket etme durumu güçlü bir grup dinamiği meydana getirmektedir (Thompson, 2011, s. 175). Kitlesel hareketlerin başarısını haberleşme araçlarının genişlemesine bağlayan Cronin'in ifadesiyle; dergiler, gazeteler, broşürler ve el ilanları gibi o dönemin kitle iletişim araçları vasıtasıyla ulaşılan halk kitlesi Fransız ihtilaline katılma yönünde radikalleştirilmiş, eğitilmiş ve örgütlenmiştir. Telefon ve e-posta gibi kişiler arasındaki iletişim araçları ile televizyon ve gazete gibi kitle iletişim araçlarındaki teknolojik gelişmeler, terör örgütlerinin hem örgütsel hem de işlevsel kapasitelerinin artmasına katkıda bulunmuştur (Cronin'den (2010) aktaran Kurum, 2017, s. 97, 98). Günümüzde söz konusu kitlesel iletişimin ve kitlesel iletişim araçlarının tür, teknik ve yöntem bakımından artmasının, radikalleştirmenin muhatabı olacak muhtemel hedefleri ve o hedeflere ulaşmayı kolaylaştıracağını söylemek yanlış olmayacaktır.

Zaman ve mekân bağlamında farklılaşan bir çatışma zemini de barındıran çok etkileşimli siber ortamda kontrol ve gözetim, devlet aktörleri bakımından da sorunlu bir alan yaratmaktadır. Sorun, yalnızca söz konusu aşırı etkileşim ortamında güvenliğin sağlanması değil bazı aktörlerin diğerlerinin ve bireysel özgürlüklerin hilafına aşırı gözetim uygulaması olarak da ortaya çıkabilmektedir. Küresel kamuoyu; Amerika Birleşik Devletleri (ABD)'nde, Edward Snowden ve Harold Martin vakaları neticesinde patlak veren ABD Ulusal Güvenlik Ajansı (NSA) skandalları sonucunda bu yönde bir iddiayla aşina olmuştur (Paçacı, 2018, s. 105; Anadolu Ajansı, 2016). Bu durum karşısında bazı ülkeler, örneğin Almanya, ulusal İnternet yapılarını oluşturma niyetini açık ettiğinden esasında genele yaygın eşitlikçi olarak tasvir edilen İnternetin; "İnternetin balkanizasyonu" olarak tanımlanan, çeşitli faktörlerden dolayı parçalı ve bölünmüş bir karaktere dönüşümünü betimleyen bir sürece evrilebileceği endişeleri de dillendirilmektedir (Kuner, Cate, Millard, Svantesson, & Lynskey, 2015, s. 2). Ancak hâlihazırda İnternet ortamı küresel anlamda bir ortak çatışma zemini olarak bütünleşik yapısını sürdürmektedir. Böylesi bir ortamda anonimlik sağlayan uygulamaların da varlığıyla çeşitli gruplar hareket serbestikazanmaktadır. Bu bağlamda, "netizen" (net citizen) (ağdaş) (Hauben, 2019, s. 3) anlayışı çerçevesinde egemenlik ve millî kimlik tanımlamalarının yeniden yorumunun karşısında, ötekileşen grupların varlığının da oluşması beklendik bir durumdur.

1785 yılında, Jeremy Bentham`ın fikriyatını temel alarak Samuel Bentham tarafından mimari tasarımı yapılan ve genel anlamda halk hareketlerinde ataletin veya isyanın kurulan sisteme olumsuz etki etmesini önlemek için bireylerin gözetim altında tutulması düşüncesine dayanan bir yapı olarak panoptikon kavramı, Fransız düşünür Michel Foucault'un çalışmalarında da yer almaktadır (Elektrik Mühendisleri Odası İstanbul Şubesi, 2016, s. 3; Lang, 2004, s. 52). Bu kavram "bütünü gözetlemek" (Özdel, 2012, s. 23) anlamı taşımakta ve önemli bir güç unsuru olarak nitelendirilen gözetim kavramı fiziksel alan başta olmak üzere pek çok alanda kitlelerin kontrol edilebilirliği düşüncesini etkilemektedir. Bu bağlamda, İnternet'in gelişimiyle beraber sanal alanda da gözetim önemli bir tema olarak işlenmektedir. Bu ortamdaki gözetim süreçlerinde de yeni teknolojilerin ön plana çıkmaya başlaması; ağdaşların hareketlerinin gözetimine yönelik yeni yaklaşımların geliştirilmesini teşvik etmektedir (Kaygısız, 2017, s. 2075). Devletin kendi vatandaşlarının veri trafiğini izlemesi bağlamında, ABD, Avustralya, Birleşik Krallık ve Yeni Zelanda'da deneyimlenen bir Anglo-Sakson olgusunun yansıması olarak ABD'nin Echelon ve Avrupa Birliği'nin Enfopol (Law Enforcement Police Matters) sistemlerinin kapsamlı veri gözetimi için kullanıldığı ileri sürülmektedir (Bannister, 2005, s. 67).

Bu çalışmanın amacı, diğer pek çok alanda olduğu gibi siber alanda da terör örgütlerince bireylerin radikalleştirilebilmesi nedeniyle bu alanda kitlesel gözetimin radikalleşme ile mücadelede kullanımı bağlamında farkındalık yaratmaktır. Bu araştırmada; "Siber alanda terör örgütlerinin yaşam döngüsünde radikalleşme boyutuyla İnternet'in yeri ve bir ulus devletin bu olguyla mücadelede kitlesel gözetimi araçsallaştırmasının etkisi nedir?" sorusuna cevap aranmaktadır. Çalışmada;panoptikon kavramsallaştırması çerçevesinde yukarıda belirtilen amaca uygun olacak biçimde İnternet'in kitlesel gözetiminin radikalleşmeyle mücadelede kullanımı üzerine bir tartışma yapılacaktır. Bu çalışma; siber alanda çeşitli unsurlar aracılığıyla bireylerin aşırılıkçılığa yönelmesi risk durumuna karşı, siber alanın suç grupları ve özellikle terör örgütleri tarafından istismar edilebilir olmasının nedenleri ve nasıl olduğunu ortaya koymakta aynı zamanda da bu tehdidin önüne geçmek için siber alanda alınabilecek tedbirler hakkında farkındalık yaratmayı amaçlamaktadır. Ancak siber alan kavramı içerisinde terör örgütlerinin ağ temelli iletişim yapılarından genel kullanıma açık İnternet üzerinde gerçekleştirdiği faaliyetlerle mücadele konusuna odaklanılacaktır. Bu bağlamda, siber alan kavramsallaştırması dar anlamda İnternet etkileşimi özelinde ele alınacağından metaverse (sanal evren), web 3.0 (merkeziyetsiz İnternet) gibi sosyal medya

platformları üzerinden bir tartışma kapsam dışında tutulacaktır, dolayısıyla söz konusu araçların radikalleşme ve gözetime etkisinin detayı bu çalışma kapsamında ele alınmayacaktır.

Bu çalışmada, nitel araştırma metotlarından literatür taraması yoluyla, betimleme yöntemi kullanılacak olup siber alanda terör örgütlerinin faaliyetleri bağlamında radikalleşme ile mücadelede panoptikon kavramı temelinde İnternetin kitlesel gözetimi yönünde devlet aktörlerinin eylemselliği ele alınacaktır. Çalışmada, karşılaşılan en önemli sınırlılık, devlet aktörlerinin uyguladığı kitlesel gözetim araçları hakkındaki bilimsel nitelikli çalışmaların görece azlığıdır.

Üç bölüm hâlinde aktarılan bu çalışmada: "Çevrim içi Radikalleşme ve Büyük Göz" başlıklı ilk bölümde öncelikle siber alan, radikalleşme ve panoptikon kavramları açıklanarak bir çerçeve çizilmiş; "Siber Vatan ve Risk Toplumu: Çevrim içi Radikalleşmeyle Mücadele" başlıklı ikinci bölümde siber alanda artan etkileşim ve radikalleşmeye etkisi ile bu alanda radikalleşme ile mücadelenin önemi irdelenmiştir. Müteakiben son bölümde; çalışmada büyük göz olarak kavramsallaştırılan kitlesel gözetim araçlarının kullanımı hususunda, siber alanda radikalleşmeyle mücadelede devlet aktörlerince alınan önleyici tedbirlerin nasıl ve ne şekilde araçsallaştırıldığına yönelik varılan sonuç hakkında genel bir değerlendirmeye yer verilmiştir.

1. ÇEVRİM İÇİ RADİKALLEŞME VE BÜYÜK GÖZ

1.1. Siber alan ve Radikalleşme

Uluslararası alanda çeşitli şekillerde ifade edilen siber alan kavramını tanımlamaya yönelik çabalar bulunmaktadır. ABD Savunma Bakanlığına göre siber alan; bilgisayar sistemleri, telekomünikasyon ağları ve İnterneti kapsayan ve birbirine ilintili bilgi teknolojileri altyapılarının olduğu dünya çapında bir alan olarak tanımlanmaktadır (Gürkaynak & İren, 2011, s. 265). Bu tanımdan hareketle, günümüzde teknoloji kullanımının ve kapasitesinin geldiği nokta göz önünde bulundurulduğunda siber alan, bireylerin gerçek dünyada gerçek etkileşim ve iletişim alanlarında yapabileceği her çeşit aktiviteyi ve paylaşımı, teknoloji ve ağ destekli sistemler üzerinden gerçekleştirebildiği bir ortama işaret etmektedir (Erken, 2021, s. 466). Terörizm bağlamında radikalleşme de bu ortamda zemin ve olanak bulmaktadır.

Radikalleşme, terörizm literatüründe önemli kavramlardan bir tanesidir. Tıpkı terörizmin tanımlanması meselesinde olduğu gibi radikalleşme kavramı da

alanyazında değişik boyutlarıyla tartışılan, çeşitli tanımlar üzerinden açıklanmaya çalışılan ancak üzerinde herkesin uzlaştığı bir tanımı olmayan kavramdır (Çakır, vd., 2017, s. 10) Literatürde radikalleşme kavramının ortak bir tanımı oluşmadığından pek çok terim onunla birlikte hatta kimi zaman da onun yerine kullanılmakta; köktencilik, aşırıcılık, fundamentalizm gibi çeşitli kavramlar aracılığıyla konu açıklanmaya çalışılmaktadır (Avcı, 2021, s. 3). Alanyazında radikalleşme kavramının özellikle terörizm ile daha sık yer alması 11 Eylül saldırıları ile birlikte olmuştur. Sonraki dönemde de özellikle Avrupa'da önemli metropollerde gerçekleşen terör saldırılarını müteakip kavram alanyazında daha çok yer bulmaya başlamıştır (Kurum & Avcı, 2018, s. 39).

Genel olarak ifade edilmek istenirse radikalleşme; toplumsal yaşamın her boyutunda mevcut düzene yönelik köklü değişimlerin olması gerektiğini savunan bir harekettir. McCauley ve Moskalenko'ya (2008) göre radikalleşme, bireyin içinde bulunduğu grubu savunma isteği ve grubun isteğini gerçekleştirme açısından artan grup şiddetini meşrulaştıran duygu, davranış ve inançlarda meydana gelen değişimdir (Derin & Öztürk, 2019, s. 1127). Radikalleşmede sosyal ve siyasal düzeyde cezrî bir değişimin yolu, etkin şiddet kullanımının meşrulaştırılması ve araçsallaştırılmasından geçmektedir (Ünsal & Olçar, 2015, s. 122; Yaşa, 2019, s. 31).

Radikalleşme; bireysel yönelimin ya da grup dinamiğinin siyasal düzende değişimini hedefleyen terör eylemlerine katılma taahhüdünün artmasıdır (Schmid, 2013, s. 1; Sönmez, 2017, s. 3). Özellikle 11 Eylül saldırıları sonrasında radikalleşme ve terörizm kavramları birlikte ele alınır olmuş, belirli durumlarda da iç içe geçmiştir (Muro, 2016; Ünsal & Olçar, 2015, s. 122).

Radikalleşme, esas itibarıyla şiddeti meşrulaştıran aşırı uçlardaki inanç ve düşüncelerin bir araya gelmesidir (Borum, 2011, s. 38). Bu doğrultuda, radikalleşme; mevcut siyasal güce karşı duyulan rahatsızlık bahanesiyle veya diğer politik, sosyo-ekonomik ve sosyo-kültürel gerekçelerle kendi gruplarından olmayan ve hedef olarak tanımlanan her şeye karşı şiddet eylemleri yöneltme sürecidir (Gunn & Demirden, 2019, s. 33). Bu bağlamda radikalleşme, toplumun genelinde hâkim olan politik, sosyal, kültürel, ekonomik araçlara ve bu araçları kullananlara tepki olarak önemli bir değişimi öngören şiddetli bir mücadele olarak tanımlanmaktadır (Beck & Schoon, 2018, s. 700). Bir süreç olarak radikalleşmeyi etkileyebilecek pek çok faktör bulunmaktadır. Bireylerin içinde bulundukları topluma ve onun sunduğu kimliklere ve değerlere yabancılaşması ve sonrasında devletin politikalarına ve söylemlerine nefret duymaktan doğan reddetme hâli

radikalleşme süreçlerini etkileyebilecek faktörler arasında sayılabilir. Bu minvalde, radikalleşmenin tek bir şeklinden bahsedebilmek mümkün değildir çünkü radikalleşme özü itibarıyla kişiden kişiye değişebilen bir süreçtir (Kurum & Avcı, 2018, s. 40, 41).

Radikalleşme; bireylerin veya grupların, kendilerine ait olanların dışındaki diğer tüm değerleri kötü, bozuk, saptırılmış vb. olduğu inancının aşılandığı ve en nihayetinde tüm karşıtlıklara "öteki" etiketini yapıştırıp mücadele edilmesi gerektiğine inanılan bir söylem ve eylem alanıdır (Sönmez, 2017, s. 3). Radikalleşme, değişimi isteyen ve bu değişim çerçevesinde şiddet kullanımını normalleştiren grupların bir araya gelmesi sonucunda gelişmektedir (Kurum & Avcı, 2018, s. 56). Bireyin yaşadığı sorunlar, sıkıntılar, yakınmalar ve ortak paydada var olma isteğinin sonucu olarak o bireyin içinde yer aldığı grubu köklü değişim gerçekleştirebilme noktasında savunmasına ve grup şiddetini meşru görmesine zemin hazırlamaktadır (Gunn & Demirden, 2019, s. 15). Çeşitli boyutlarda gerçekleşebilen bireysel ve grupsal radikalleşme süreçlerinde önemli bir yer tutan propaganda; sorun alanları üzerinden dinamikler arası çatışma alanı ve yeni bir grup kimliği yaratarak siyasal katılımın doğasını şekillendirmektedir (Ünsal & Olçar, 2015, s. 127).

Günümüzde teknolojik gelişmelerin hızlı dönüşümü paralelinde sosyal medya platformlarına erişim kolaylığı, ortamın anonimliği ve dijital alanda sınırların kaybolması, bireylerin/grupların sanal ortamda yoğun propagandaya maruz kalmalarına ve böylelikle radikalleşmelerine ortam hazırlamaktadır (Ünsal & Olçar, 2015, s. 128; Yüksel, 2020, s. 1091). Bireyler veya gruplar bilgi teknolojilerindeki hızlı gelişmeler vasıtasıyla radikalleşme eğilimi içerisinde olan ve benzer radikal fikirlere sahip, kendisi gibi düşünen insanlara dünyanın herhangi bir yerinde kolayca ulaşım sağlamakta ve bu çerçevede hızlıca kurulan ağbağlar vasıtasıyla örgütlenme kolayca olmaktadır (Kurum & Avcı, 2018, s. 59). Toplumlarda değişimi hedefleyen hareketler, sonuca ulaşmak için kaynak kullanımına gereksinim duyduğundan bilgi teknolojilerinin kullanımı önemli bir kaynak olarak değerlendirilmektedir. Siber alanda kurulan ağ tipi ilişkiler örüntüsünde özellikle sosyal medya vasıtasıyla söylemlerin ve savunulan değerlerin inşası; kitleleri etkileyebilmekte ve yaratılan algılar, gerçeklerin önüne geçebilmektedir (Çakır, vd., 2017, s. 30).

Alanyazında İnternet'i de kapsayan siber alanın, radikalleşme eğilimindeki bireyler için geleneksel engelleri yıkmakta etkili, bireyler ve gruplar arası etkileşimi güçlendirici veya hızlandırıcı bir ajan olduğu ifade edilmektedir (Behr,

Reding, Edwards, & Gribbon, 2013, s. 17). Anonimleştirme yoluyla aralarındaki farkların azaltılması, kurduğu iletişim kanallarıyla benzer düşüncelere sahip kişilerin bağlanmasına yardımcı olması gibi kolaylaştırıcı faktörleri sayesinde İnternet; cinsiyetleri, geçmişleri veya ülkeleri ne olursa olsun, dünyanın dört bir yanından bireyler için iletişim ve koordine kurmanın, itibar kazanmanın en kısa yolu olarak değerlendirilmektedir (Behr, Reding, Edwards, & Gribbon, 2013, s. 18). Siber alan; bireylerin radikalleşmelerine sebep olacak bir odak noktası sağlamakta ve bireylerin birbiriyle benzer düşünen bir topluluğa doğrudan erişimini sağlamaktadır.

Bu bağlamda, "Zapatista hareketi" ile ilgili bilgileri hatırlamak faydalı olabilir. "Zapatistalar" (Zapatista Ulusal Kurtuluş Ordusu / Ejército Zapatista de Liberación Nacional) üzerinden Meksika'da gerçekleştirilen Chiapas vakası "sürü ağları"nın ortaya çıkmasına bağlı olan ağ çatışmasında, sürüleşmenin dağıtık grupların en iyi "kolektif çeşitlilik" ve "koordineli anarşi" biçiminde İnternet'e bağlanmak suretiyle iş birliği yaptığı yerlerde gerçekleştiğini göstermektedir (Ronfeldt & Arquilla, 2001, s. 193). Cleaver'a (1995 ve 1998) göre "Zapatista etkisi" olarak tanımlanan ve bilgi çağı sosyal ağ çatışmasında sosyal hareketlenmeyle inşa edilen yeni "elektronik mücadele dokusu" küresel anlamda eylemci hareketleri birbirine bağlamaya ve eylemci hareketlere ilham vererek onların radikalleşmesine yardımcı olmaktadır (Ronfeldt & Arquilla, 2001, s. 192). Zapatista sempatizanları ve hareket hakkında bilgi arayan kişilerle İnternet'te yaratılan çatışma alanı; sonrasında ordu tarafından kuşatılan Zapatistalar'ın harekete dış destek sağlamak ve ayrıca çatışma bölgesi içindeki olaylarla ilgili iletişim ve uyarılar yayımlamak için İnterneti araç olarak kullanmasıyla evrilmiştir (Franchi & Vichi, 2019, s. 131). Böylelikle çatışmanın karakteri kısa sürede dönüşüm geçirmiştir (Ronfeldt & Arquilla, 2001, s. 187).

Terör örgütleri özellikle eleman temininde anlatılar ve görsel sunular üzerinden hareket ederek bireylerin radikalleşebilmesini sağlamaktadır. Bu yolla bireylere sunulan değerler ve fikirler, hedef kitlenin kişisel ve sosyal gerçeklikleriyle örtüşüyorsa radikalleşme gerçekleşebilmektedir. Örneğin, DEAŞ anlatılarının Avrupa'da özellikle Müslüman gençler arasında karşılık bulması ve onların özellikle yabancı terörist savaşçı olarak örgüte katılımları, Avrupa'da anlatılara muhatap olanlar bakımından kişisel ve sosyal faktörlerin örtüşmesinden kaynaklanmaktadır (Çakır, vd., 2017, s. 13). Günümüzde özellikle gençlerin, yaşadıkları ülkelerde artan yabancı ötekileştirmesi ve bunun yansıması olarak deneyimledikleri yabancılaşma, siber alanda çeşitli terör örgütlerinin yarattıkları ve

sundukları yalancı kimlikler üzerinden radikalleşmelerine fırsat sağlayabilmektedir. Bu sayede ötekileştirildiğini düşünen bireyler yeni bir grup kimliği üzerinden farklı bir dönüşüm yaşayabilmektedir. Bu bağlamda bireyler sanal ortamda bir gruba ait olma ihtiyacını gidermenin yanı sıra radikalleşerek hayatlarını dönüştürmektedirler (Çakır, vd., 2017, s. 13).

1.2. Panoptikon ve Gözetim

Her bir bireyin gözetlenmesi, toplumun bütününde cereyan eden olayların izlenmesine yönelmek olarak değerlendirilebilir. Bu bağlamda, panoptikon kavramının tanımı faydalı olacaktır. "Bütün" anlamını ifade eden "pan" ve "gözlemlemek" anlamını veren "optikon" sözcüklerinin birleşiminden türetilen "panoptikon" kavramı "bütünü gözetlemek" (Özdel, 2012, s. 23) anlamı taşımakta ve kitlelerin kontrol edilebilirliği düşüncesine tesir etmektedir. 1785 yılında, Jeremy Bentham`ın düşüncesini esas alarak Samuel Bentham tarafından mimari tasarımı yapılan bu yapıda; mahkûmları, onlara görülmeden, gören ve her hareketlerinin görüldüğü algısını yerleştiren bir kontrol unsuru bulunmaktadır (Lang, 2004, s. 52; Elektrik Mühendisleri Odası İstanbul Şubesi, 2016, s. 3). Panoptikon kavramı idareyi elinde bulunduran yetkililerin, tele-ekranlar ile toplumun bütününü gözetim altında tuttuğu bir ortamda, herkesin her an izlendiği izlenimi yaratan "Big Brother" kavramı ile benzeştirilebilir (Şimşek, 2021a, s. 394). Bu kavramın da; George Orwell'in "Ninety Eighty Four" (1984) başlıklı kitabında "Oceania" ülkesinde neredeyse her yerde duvarlara iliştirilmiş posterlerle "Büyük Kardeş Seni İzliyor" (Big Brother Is Watching You) notuyla verilen mesajın ve her yerde kurulu tele-ekranlarla oluşturulan, çok alçak bir fısıltı seviyesinin üzerinde çıkarılan herhangi bir sesin duyulabilir ayrıca emredilen görüş alanı içinde kalındığı sürece hareketlerin görülebilir olduğu ancak herhangi bir anda izlenip izlenilmediğini kişinin bilmesinin bir yolu olmayan bir gözetim sistemini anlatan kurgusal bir ortamı tasvir ettiği hatırlanacaktır (Orwell, 1949, s. 2).

Foucault, "norm etrafında örgütlenen şeyleri algılamanın bir biçimi" olarak tanımladığı "tıbbi düşünce"nin; normal olanını ve olmayanını ayırıp, "tam anlamıyla cezalandırma araçları yerine kişiyi dönüştürme araçları olan hizaya getirme araçlarının geliştirmenin ve buna bağlı olarak insan varlığının davranışıyla ilgili tüm bir teknolojiye" erişmenin çabasında olduğunu ileri sürmektedir (Foucault, 1994, s. 156). Foucault; bu düşünce doğrultusunda meydana gelen "tıbbileştirmenin" neticesinde, kapitalizmin gelişimine bağlı olarak feodal tipteki toplum düzeni dönemindekinden farklılaşan iktidarın bireyi ele alış biçiminde

"işbölümünde kimilerinin şu işi, kimilerinin bu işi yapmasına ihtiyaç olduğunda, halkın direniş hareketlerinin, ataletin ya da isyanın, doğmakta olan tüm bu kapitalist düzeni altüst etmesinden korkulduğunda, o zaman, her bireyin somut ve kesin gözetlenmesi(nin) gerekli oldu(ğunu)" savlamaktadır (Foucault, 1994, s. 157). Foucault'un anlayışına göre, belirli bir deneyime veya kimliğe ilişkin negatif bir sınıflandırma, diğer bir deyişle, o deneyimi veya kimliği toplumsal çerçevede sakıncalı ve buna bağlı olarak arzu edilmez gösteren bir sınıflandırma, bu deneyimi veya kimliği yalıtmak, düzeltmek ve ortadan kaldırmak için yapılan uygulamalara ve bu uygulamaları gerçekleştiren kurumların varlığına meşruiyet kazandırabilmektedir (Foucault, 1994, s. 14). Bu durum içselleştirmeyle ilişkilendirildiğinde, gözetleyenin gizliliğinin esas olduğu panoptikonda gözetlenenler merkezi bir gözetimin varlığını ve gözetlendiğini bilmekte ve bir deneyim olarak öznelleştirmektedir (Şimşek, 2021a, s. 393).

Küreselleşme ve ulus-devlet arasındaki etkileşim süre gelmektedir (Kömürcü, 2009, s. 84). Bauman, küreselleşen dünyada toplumlar arasında artan etkileşimin birbirlerine yabancılaştırılmış bireylerden oluşan bir toplum düzenine yol açabileceğine işaret ederek, endüstri toplumuna özgü bulduğu "Panopticon"dan ziyade, dışlanma temelinde "Pelican Bay"ın küreselleşmenin özüne uygun olduğunu ifade etmektedir (Tanrıverdi, 2008, s. 122). Bauman ve Lyon'a (2013 ve 2016) göre; gelişen teknoloji sayesinde "akışkan" hâle gelen modern toplumlar dinamizm içindedir ancak bu durum onların gözetlenmesine mani olmadığı gibi, "akışkan gözetim" olarak tanımlanan gözetim biçimiyle de gözetim pratikleri günlük yaşamın birçok alanına nüfuz etmiş ve gözetleyene ulaşmak ise imkânsız hâle gelmiştir (Şimşek, 2021a, s. 394).

Yerel denetimin uç bir simgesi olarak panoptikon kavramının evrimleşme sürecinde, toplumsal yaşamın ve teknolojik imkân ve kabiliyetlerin artışına koşut olarak terime ilişkin birçok farklı tanım ve yaklaşımlar da gelişmiştir. Bu çerçevede, Mark Poster'ın (1990) gözetlenenin gözetim için gerekli bilgileri kendisinin sağladığı "süperpanoptikon", Thomas Mathiesen'in (1997) çoğunluğu temsil eden gözetlenenin televizyon örneğinde olduğu gibi talepleri yönlendiren azınlık bir grup olan gözetleyeni izledikleri çift taraflı gözetime dayalı "sinoptikon" ve Jeffrey Rosen'ın (2004) çoğunluğun çoğunluğu diğer bir deyişle takipleşerek herkesin birbirini karşılıklı ve etkileşimli gözetimine dayalı "omnioptikon" tanımlamalarının olduğu bilinmektedir (Şimşek, 2021a, s. 395, 396). Ayrıca, "post-panoptikon" (Şimşek, 2021b, s. 208) kavramının da tartışıldığı görülmekle birlikte, "post" ön ekinin; bir nevi sonlanmayı ifade etse de, Alain Touraine'nin (1994)

"Modernliğin Eleştirisi" başlıklı eserindeki "post-modernlik" tartışmalarından da anımsanacağı gibi, eklendiği kavramın sonu değil sadece eleştirisi veya yeniden yorumlanması olarak da algılanabileceği ileri sürülebilir. Sonuç olarak gözetim modellemesinde ve kavramlaştırmasında yaşanan bu dönüşüm bir nevi herkesin birbirini gözetlediği, gözetleyen ve gözetlenenin bulanıklaştığı bir güvenlik ortamının tasviridir. Ancak bu durum fertlerin kendi bireysel takipleşmelerinin ötesinde, tüm ortamı ve tüm bireyleri gözetleme isteği taşıyan yapıların da işaretçisidir.

Bulanıklaşan güvenlik ortamında kamuoyunun yaratılmasında etkili bir yöntem, iletişim aygıtlarının kontrolüdür (Akkol, 2019, s. 171). Gözetimin sayısallaştığı siber alanda bu durum dijital panoptikon olarak adlandırılabilir (Şimşek, 2021a, s. 395). Han'a (2012) göre sosyal medya giderek dijital panoptik bir yapıya benzemektedir. Dijital panoptikonda özgür olduğunu düşünen bireyler aktif olarak iş birliği kurdukları canlı bir iletişimle kendi özgür iradeleriyle kendilerini açığa vurmaktadırlar ve hâl böyleyken "şeffaflık toplumu"nda ideolojileştirilen şeffaflık bütünleştirildiğinde radikalleşme ve akabinde terör yaratma potansiyelini barındırmaktadır (Han, 2012, s. viii). Byung-Chul Han'a (2017) göre tasvir edilen bu ortamda;

"Tüketiciler ihtiyaçlarını yönlendiren ve tatmin eden panoptik gözetime gönüllü olarak teslim ederler kendilerini. Bu noktada artık sosyal medya ile panoptik makineler arasında fark yoktur. İletişim ve ticaret, özgürlük ve kontrol aynı şey hâline gelir. (...) Kendilerini özgürlük alanları olarak sunan Google ve sosyal ağlar panoptik biçimlere bürünüyorlar. Bugün gözetleme, genelde sanıldığı şekliyle özgürlüğe saldırı şeklinde gerçekleşmiyor. İnsanlar daha ziyade kendilerini gönüllü olarak teslim ediyorlar panoptik bakışa. Kendilerini soyarak ve teşhir ederek dijital panoptikonun oluşuna bilerek katkıda bulunuyorlar." (Ünlü, 2018, s. 288, 289)

Söz konusu dijital teşhir ortamında insanlar gözetime kendi kendilerine gönüllü olarak katılmaktadır. Örneğin, herkese açık Facebook profili oluşturmak, İnternette kamuya açık kişisel paylaşımlar yapmak gibi eylemlerle insanlar; dijital teşhir yoluyla kendi özel hayatlarına ilişkin kişisel verilerini başka bir ortamda ve şekilde, kendilerinden istense vermekten imtina edeceği verileri genel toplumun gözetimine açmaktadır. Bu durumun bireyleri radikalleştirmeye iten odaklar için de bulunmaz fırsatlara yataklık edeceği gözden kaçırılmamalıdır. Nihayetinde, Byung-Chul Han (2017)'ın da belirttiği gibi söz konusu topyekûn gözetlemenin, "şeffaf toplumu"

dönüştürdüğü "kontrol toplumu"nda, herkes herkesi kontrol ettiği görülmektedir (Ünlü, 2018, s. 288, 289).

Joseph S. Nye'a (2014) göre, karmaşık bir karakterde tasvir edilebilecek siber alanda hükümetler ve devlet dışı aktörler güç için iş birliği yapmakta ve birbirleriyle rekabet etmektedir (Nye, 2014, s. 5). Devletler de siber alanı kontrol etme çabalarında siber alanda etkin olma gücünü ve siber yönetişimi bir araç olarak kullanmaktadırlar (Şimşek, 2021c, s. 512). Siber alanda elde edilen güç; ağ temelli iletişime dayanan bu alanda tercih edilen sonuçları elde etmek için kullanılabileceği gibi, bu sanal ortam dışında da sonuç üretmek için siber araçları kullanabilir (Nye, 2014, s. 5).

Görünürlüğe dayalı panoptik kavramı dışında yönetim işlevini tanımlayan programlanabilirliğe dayalı "algokrasi" kavramlaştırması da dikkat çekicidir. Bir yönetim modellemesi olarak "algokrat" bir çerçevede, örgütsel yapı içerisinde bireyin çalışırken izlemesi gereken yol alternatifi olmayacak tarzda tasarlanmış ya da önceden verilmiş ve programlanmıştır bu nedenleotoriteyi gayri meşru kılmak için kullanılabilecek kıyaslanabilir bir yol bulunmamaktadır (Aneesh, 2002, s. 9). Esasında, örgütsel yapı içerisinde çalışan bireyin örgütsel gözetimden kaçamadığı "panoptik" yapıda gözetimin yerine alternatif yol bırakmayan "algokrat" yapıdan daha fazla özgürlüklere müdahale ortamı yarattığından bahsetmek ayrı bir tartışmanın konusudur (Aneesh, 2002, s. 7). Ancak en nihayetinde algoritmaya dayalı yazılımlar yoluyla gerçekleştirilen etkileşimlerin de arka planda görülmeden kullanıcı hareketlerini görmeyi mümkün kıldığını göz ardı etmemek gerekir.

Teknolojinin mevcut kuralları uygulamak için kullanıldığı bir düzenleme şeklini ifade eden Lawrence Lessig'in (1999) "kod yasadır" söylemi, kayıt zinciri (blockchain) ve makine öğrenmesi kavramlarının ortaya çıkmasıyla birlikte, teknolojinin giderek bu kuralların önüne geçtiği yeni bir eğilim yaratmaktadır (Hassan & deFilippi, 2017, s. 88). Anayasalar, kanunlar, tüzükler ve benzeri yasal kodlarla normlar hiyerarşisi içerisinde toplumsal hayatın akışının devam ettiği gerçek alan düzenlenirken, bilgi toplumunun yaşam ortamı olarak donanımlar ve yazılımlarla hayat bulan siber alan da bir nevi bu ortamın yasası olan yazılımlarla kodlanarak düzenlenmektedir (Reidenberg, 1998, s. 1). Teknoloji ve iletişim ağlarının bilgi akışları için zorunlu kıldığı kurallar dizisi; politika yapıcıların idrak ve teşvik etmesi gereken yazılım mimarisi standartları ve yetki alanı ağbağlar olan bir "Bilgi Hukuku" ("Lex Informatica") oluşturduğu ileri sürülmektedir (Reidenberg, 1998, s. 555).

İktidar, ilk çağlarda kabile reisi ile tasvir edilirken günümüzde görünmeyen ancak eskiye nazaran daha büyük bir güç olarak dünyadaki gelişmelerden bilgi sahibi olan, dahası anılan gelişmelerin yaratıcısı ve gözetleyicisi rolündedir (Özdel, 2012, s. 23). Frank Bannister'a (2005) göre, bir devlet; kendi vatandaşları hakkında "casusluk" yapmasının kendi hukuk düzenine göre yasa dışı olduğu durumlarda, anlaşmaya vardığı müttefik devletlerle her birinin diğerinin vatandaşlarını gözetlediği ve ardından bilgi alışverişinde bulunduğu bir anlaşma düzlemi yaratabilir (Bannister, 2005, s. 67). ABD'nin Echelon ve Avrupa Birliği'nin Enfopol (Law Enforcement Police Matters) sistemi kapsamlı veri gözetimi konusunda adı geçen konseptlerdendir (Bannister, 2005, s. 67). Echelon sisteminin ABD'ye giren ve çıkan her bir e-posta trafiğini okuduğu iddia edilmektedir (Bannister, 2005, s. 68). Aynı şekilde, Birleşik Krallık istihbarat kuruluşunun 2001 yılında Birleşik Krallık'tan alınan ve gönderilen tüm e-posta ve İnternet mesajlarını izleyebilecek e-posta gözetim sistemi kuruluşuna ilişkin duyurusunun bulunduğu ve "FreeServe" ile "AOL" gibi İnternet servis sağlayıcılarının Devlet Teknik Yardım Merkezine ("Government Technical Assistance Centre" - GTAC) kablo bağlantısı kurmalarını şart koşmakta olduğu ileri sürülmektedir (Todd & Bloch, 2003, s. 63). Bu durum, dijital panoptikon çağında, devlet gözetiminin otoriter toplumlarla sınırlı olmadığını göstermektedir.

İçinde bulunduğumuz yüzyılda, küreselleşme çerçevesinde; merkez ve çevre ilişkisinde, küresel anlamda uluslar ve diğer ekonomik güçler arasındaki farklılık hızla artmakta, bu unsurların arasındaki bağımlılık zinciri ve eşitsiz gelişme aşırı noktalara gelmektedir (BBCNews, 2019). Dijital teknolojilerin yaşam alanımızı hem kavramsal hem de pratik olarak genişletmesinin yarattığı tehlikeler, panoptikonun "özgürlük teknolojileri" ile bütünleştirilmesi talebini de beraberinde getirmektedir (Boyle, 1997, s. 204). Diğer bir deyişle, devletlerin siber alanda vatandaşlarının etkileşimleri üzerinde de gözetim sağlama güdüsü panoptik yaklaşımın siber alana yansımasını da beraberinde getirmektedir. Radikalleşme ve terörizmle mücadele, yeni hukuki düzenlemelere anlam kazandırarak İnternet'in denetimine de olanak sağlamaktadır (Paye, 2003).

2.SİBER VATAN VE RİSK TOPLUMU: ÇEVRİM İÇİ RADİKALLEŞME

2.1. Potansiyel Risk Kaynağı: Siber Alanda Etkileşimin Artışı

Siber alanda cereyan eden etkileşimin boyutlarını ve bunun yerel izdüşümünü gözümüzde canlandırabilmek için küresel ve yerel bağlamda İnternet'e erişimi ve İnternet'in kullanım durumunu ortaya koymak faydalı olacaktır. 2021 yılının ilk

çeyreğini içeren döneme ilişkin tahminlere göre dünya nüfusunun %65,6'sı İnternet kullanmakta ve bu oran 2000-2021 arası dönem için İnternet Kullanımında %1.331,9 'lık bir artışa tekabül etmektedir (Tablo 1).

Tablo 1 İnternet Kullanımı ve Dünya Nüfusu İstatistikleri 2021 Yılı İlk Çeyrek Tahminleri[2]

İnternet Kullanımı ve Dünya Nüfusu İstatistikleri 2021 Yılı İlk Çeyrek Tahminleri						
Dünya Bölgeleri	**Nüfus (2021 Tah.)**	**Dünya Nüfusu İçinde %**	**Internet Kullanıcıları 31.03.2021**	**Penetrasyon Oranı (% Nüfus)**	**Büyüme 2000-2021**	**Dünya İnternet Kullanıcıları içinde %**
Asya	4.327.333.821	% 54,9	2.762.187.516	% 63,8	% 2.316,5	% 53,4
Avrupa	835.817.920	% 10,6	736.995.638	% 88,2	% 601,30	% 14,3
Afrika	1.373.486.514	% 17,4	594.008.009	% 43,2	% 13.058	% 11,5
Latin Amerika / Karayipler	659.743.522	% 8,4	498.437.116	% 75,6	% 2.658,5	% 9,6
Kuzey Amerika	370.322.393	% 4,7	347.916.627	% 93,9	% 221,9	% 6,7
Orta Doğu	265.587.661	% 3,4	198.850.130	% 74,9	% 5.953,6	% 3,9
Okyanusya / Avusturalya	43.473.756	% 0,6	30.385.571	% 69,9	% 298,7	% 0,6
TOPLAM	7.875.765.587	% 100,0	5.168.780.607	% 65,6	% 1.331,9	% 100,0

2021 yıl ortası istatistiklerine göre Türkiye'de İnternet kullanıcılarının nüfusa oranı %83,3'tür. Bu sayı Avrupa'daki kullanıcıların %9,5'ini oluşturmaktadır (Tablo 2).

Tablo 2 Avrupa'da İnternet İstatistikleri ve Facebook Kullanımı 2021 Yıl Ortası İstatistikler[3]i

Avrupa'da İnternet İstatistikleri ve Facebook Kullanımı 2021 Yıl Ortası İstatistikleri					
Ülke	**Nüfus (2021 Tah.)**	**Internet Kullanıcıları 31.12.2020**	**Penetrasyon Oranı (% Nüfus)**	**Avrupa'daki Kullanıcılar İçinde %**	**Facebook 31.12.2020**
Türkiye	82,961,805	**69.107.183**	% 83,3	% 9,5	44.000.000

Türkiye İstatistik Kurumunun (TÜİK), gerçekleştirdiği "Hane Halkı Bilişim Teknolojileri (BT) Kullanım Araştırması" çerçevesinde yayımladığı verilere göre, 2011-2021 yıllarını kapsayan 11 yıllık bir dönemde İnternet kullanım oranında 16-74 yaş grubundaki bireylerde %45'ten zaman içerisinde %82,6'ya yükselen bir artış gözlemlenmektedir (Tablo 3). Cinsiyete göre incelendiğinde bu oranın; bu

[2] **Kaynak:** © Telif Hakkı 2021, Miniwatts Marketing Group. www.internetworldstats.com internet sitesinden tercüme edilerek aynen alınmıştır. İnternet Kullanımı ve Dünya Nüfusu İstatistikleri, 31 Mart 2021 için tahmini değerlerdir. Demografik sayılar (nüfus), Birleşmiş Milletler Nüfus Birimi verilerine dayalı olarak hesaplanmıştır.

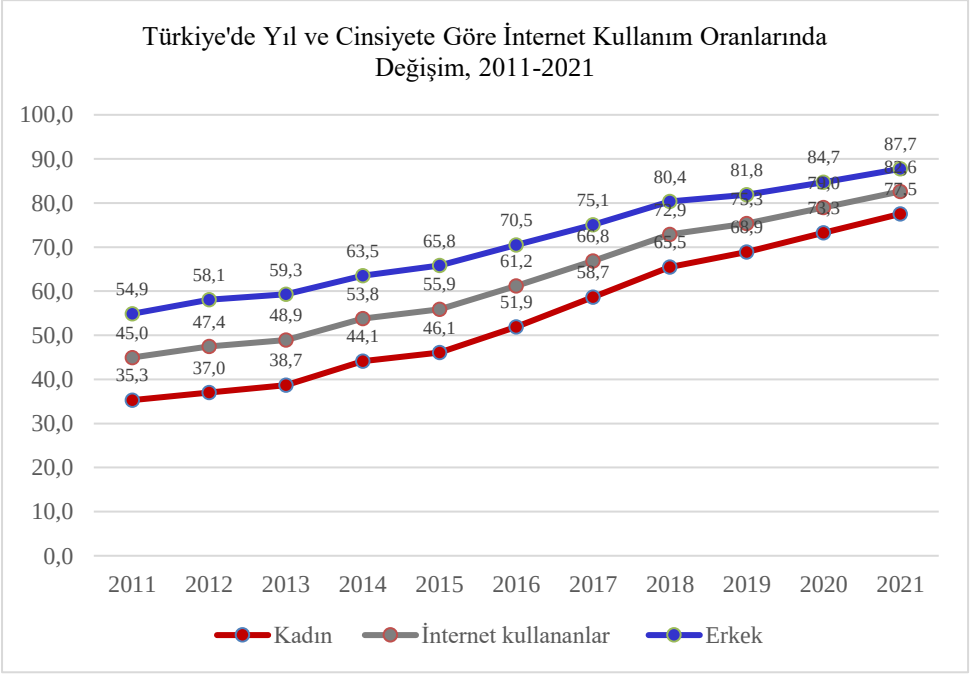
[3] **Kaynak:** © Telif Hakkı 2021, Miniwatts Marketing Group. www.internetworldstats.com İnternet sitesinden tercüme edilerek aynen alınmıştır. Avrupa İnternet İstatistikleri, 30 Haziran 2020; Facebook abone verileri ise 31 Aralık 2020 için tahmini değerlerdir. Nüfus, esas olarak Birleşmiş Milletler Nüfus Birimi verilerine dayalı olarak 2020 yılı ortası için hesaplanmıştır.

süre zarfında erkeklerde %54,9'dan %87,7'ye, kadınlarda ise %35,3'ten %77,5'ye yükseldiği görülmektedir (Tablo 3 ve Şekil 1)[4]

Tablo 3 Türkiye'de İnternet Kullanımı Oranları, 2011-2021[5]

Türkiye'de İnternet Kullanım Oranları, 2011-2021

	(%)											(%)											(%)										
	İnternet																																
	Toplam											Erkek											Kadın										
En son kullanım zamanı	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
İnternet kullananlar	45,0	47,4	48,9	53,8	55,9	61,2	66,8	72,9	75,3	79,0	82,6	54,9	58,1	59,3	63,5	65,8	70,5	75,1	80,4	81,8	84,7	87,7	35,3	37,0	38,7	44,1	46,1	51,9	58,7	65,5	68,9	73,3	77,5
Son üç ay içinde	40,5	42,7	43,2	48,5	51,6	58,3	64,7	71,0	74,0	77,7	81,4	49,8	53,0	53,1	58,2	61,2	67,6	72,8	78,2	80,4	83,3	86,5	31,3	32,6	33,4	38,8	42,1	49,2	56,6	63,9	67,6	72,1	76,4
Üç ay ile bir yıl arasında	2,6	2,4	3,1	2,6	2,1	1,1	1,1	0,9	0,6	0,6	0,5	3,1	2,8	3,5	2,6	2,4	1,2	1,1	1,0	0,5	0,6	0,5	2,1	2,0	2,6	2,5	1,9	1,0	1,1	0,8	0,6	0,5	0,6
Bir yıldan önce	1,9	2,3	2,7	2,7	2,2	1,7	1,1	0,9	0,8	0,7	0,7	2,0	2,3	2,7	2,7	2,3	1,7	1,2	1,1	0,9	0,8	0,8	1,8	2,4	2,6	2,8	2,1	1,7	1,0	0,8	0,6	0,7	0,6
Hiç kullanmadı	55,0	52,6	51,1	46,2	44,1	38,8	33,2	27,1	24,7	21,0	17,4	45,1	41,9	40,7	36,5	34,2	29,5	24,9	19,6	18,2	15,3	12,3	64,7	63,0	61,3	55,9	53,9	48,1	41,3	34,5	31,1	26,7	22,5



Şekil 1 Türkiye'de Yıl ve Cinsiyete Göre İnternet Kullanım Oranlarında Değişim, 2011-2021

[4] Veriler, https://data.tuik.gov.tr/Kategori/GetKategori?p=Bilim,-Teknoloji-ve-Bilgi-Toplumu-102 internet sitesinden alınmıştır.

[5] TÜİK Hane Halkı Bilişim Teknolojileri (BT) Kullanım Araştırması'nın 2011-2021 yıllarına ait verilerinden derlenmiştir. Tablodaki rakamlar yuvarlamadan dolayı toplamı vermeyebilir.

TÜİK'in söz konusu araştırma çerçevesinde yayımladığı verilere göre, 2011-2021 yıllarını kapsayan 11 yıllık bir dönemde "İstatistiki Bölge Birimleri Sınıflaması"nın (İBBS) 1. düzeyine göre hanelerde İnternet erişim oranlarında ülke genelinde bir artış yaşandığı ve bu artışın 2021 yılında da [Bir önceki yıla kıyasla TRA - Kuzeydoğu Anadolu (Erzurum, Erzincan, Bayburt, Ağrı, Kars, Iğdır, Ardahan) ve TR3 - Ege (İzmir, Aydın, Denizli, Muğla, Manisa, Afyonkarahisar, Kütahya, Uşak) bölgelerinde hafif düşme haricinde] devam ettiği gözlemlenmektedir (Tablo 4). Özellikle, TRC - Güneydoğu Anadolu (Gaziantep, Adıyaman, Kilis, Şanlıurfa, Diyarbakır, Mardin, Batman, Şırnak, Siirt) bölgesinde hanelerde nternet erişim oranı 2011 yılında ülke ortalamasının neredeyse yarısı iken 2021 yılında ülke ortalamasının üzerine çıktığı görülmektedir (Tablo 4 ve Şekil 2) [6]

Tablo 4 İstatistiki Bölge Birimleri Sınıflaması 1.Düzey'e göre Hanelerde İnternet Erişimi, 2011-2021[7]

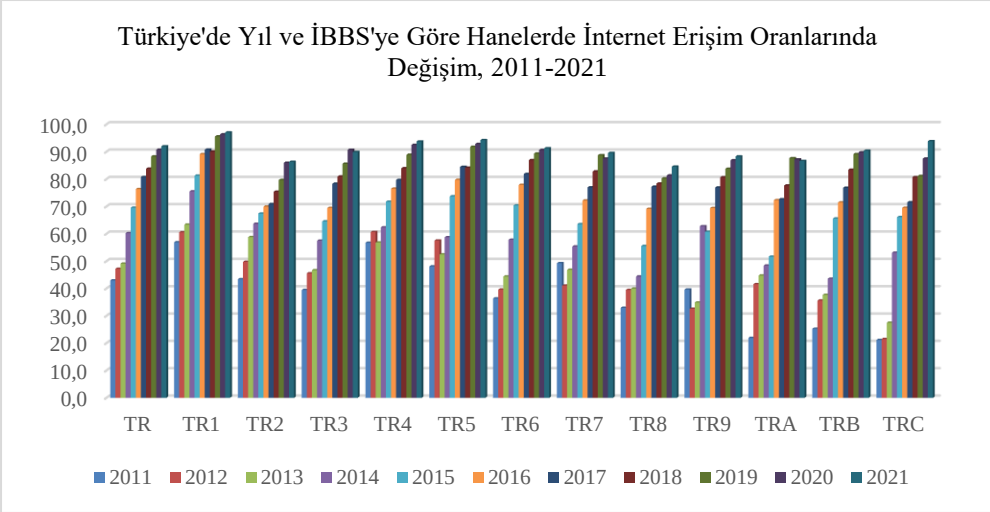
İstatistiki Bölge Birimleri Sınıflaması 1.Düzey'e Göre Hanelerde İnternet Erişimi, 2011-2021

(%)

İstatistiki Bölge Birimleri Sınıflaması (İBBS) 1. Düzey		2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
TR	Türkiye	42,9	47,2	49,1	60,2	69,5	76,3	80,7	83,8	88,3	90,7	92,0
TR1	İstanbul	56,9	60,5	63,3	75,5	81,3	89,1	90,8	90,1	95,6	96,4	97,1
TR2	Batı Marmara (Tekirdağ, Edirne, Kırklareli, Balıkesir, Çanakkale)	43,4	49,7	58,8	63,6	67,4	69,9	70,8	75,4	79,7	86,0	86,3
TR3	Ege (İzmir, Aydın, Denizli, Muğla, Manisa, Afyonkarahisar, Kütahya, Uşak)	39,4	45,5	46,7	57,4	64,5	69,4	78,3	80,9	85,6	90,7	89,9
TR4	Doğu Marmara (Bursa, Eskişehir, Bilecik, Kocaeli, Sakarya, Düzce, Bolu, Yalova)	56,7	60,6	56,8	62,3	71,7	76,5	79,7	84,0	88,9	92,5	93,7
TR5	Batı Anadolu (Ankara, Konya, Karaman)	48,0	57,5	52,4	58,7	73,7	79,7	84,4	84,1	91,8	92,8	94,2
TR6	Akdeniz (Antalya, Isparta, Burdur, Adana, Mersin, Hatay, Kahramanmaraş, Osmaniye)	36,4	39,6	44,4	57,8	70,4	77,9	81,8	86,9	89,3	90,7	91,3
TR7	Orta Anadolu (Kırıkkale, Aksaray, Niğde, Nevşehir, Kırşehir, Kayseri, Sivas, Yozgat)	49,2	41,0	46,8	55,3	63,5	72,1	77,0	82,8	88,7	87,5	89,6
TR8	Batı Karadeniz (Zonguldak, Karabük, Bartın, Kastamonu, Çankırı, Sinop, Samsun, Tokat, Çorum, Amasya)	32,9	39,5	39,9	44,4	55,5	69,1	77,2	78,4	80,2	81,3	84,5
TR9	Doğu Karadeniz (Trabzon, Ordu, Giresun, Rize, Artvin, Gümüşhane)	39,6	32,6	34,8	62,7	60,7	69,4	76,9	80,7	83,8	86,9	88,3
TRA	Kuzeydoğu Anadolu (Erzurum, Erzincan, Bayburt, Ağrı, Kars, Iğdır, Ardahan)	21,9	41,5	44,7	48,4	51,6	72,3	72,6	77,6	87,6	87,2	86,6
TRB	Ortadoğu Anadolu (Malatya, Elazığ, Bingöl, Tunceli, Van, Muş, Bitlis, Hakkari)	25,3	35,6	37,7	43,6	65,6	71,5	76,8	83,4	89,1	89,8	90,4
TRC	Güneydoğu Anadolu (Gaziantep, Adıyaman, Kilis, Şanlıurfa, Diyarbakır, Mardin, Batman, Şırnak, Siirt)	21,2	21,5	27,5	53,0	66,1	69,5	71,5	80,7	81,1	87,5	93,8

[6] Veriler, https://data.tuik.gov.tr/Kategori/GetKategori?p=Bilim,-Teknoloji-ve-Bilgi-Toplumu-102 internet sitesinden alınmıştır.

[7] TÜİK Hane Halkı Bilişim Teknolojileri (BT) Kullanım Araştırması'nın 2011-2021 yıllarına ait verilerinden derlenmiştir.



Şekil 2 Türkiye'de Yıl ve İBBS'ye Göre Hanelerde İnternet Erişim Oranlarında Değişim, 2011-2021

Siber suçlar ve diğer kötücül kullanımlar bakımından siber kaynakların istismar potansiyeli de göz önünde bulundurulduğunda, İnternet'e erişimin artması aynı zamanda, İnternet ortamını kullanan toplumun büyük kesiminin risk altında olması anlamına da gelmektedir.

2.2. Siber Alanda Radikalleşmeyle Mücadelenin Önemi

Siber alanda devlet egemenliğinin sağlanmasında, "siber vatan"ın[8] "netizen"leri (ağdaşları) bakımından, toplum sözleşmesi teorisine dayalı anlatımlar temelinde bir devletin egemenliğinin ve bunun kaynağı olan meşruiyetin yönetilenlerin rızasına bağlı olduğu varsayımının da esasen bir algıya dayalı olduğu ileri sürülebilir. Devletlerin, siber alandaki iletişim teknolojileri ve yöntemleri üzerindeki kontrolünün, yönetilenlerin algısının bu yönde oluşturulmasında ve yönlendirilmesinde etkili olması bu anlamda beklendik bir durumdur. Türkiye'de İnternet'e erişimin ve İnternet kullanımının son yıllarda gösterdiği artış ve bu artışa bağlı olarak yoğun etkileşimin ortaya çıkardığı yeni risk ortamlarında devletler başta olmak üzere geniş kitleleri negatif yönde etkileyebilecek tehditlerin çoğaldığı da artık aşikârdır (Akdemir ve Tuncer, 2021, s.ıv). Tüm tehditleri içeren kapsayıcı bir güvenlik anlayışıyla, devlet yapısının önemli unsurlarından biri olan insan

[8] Batı Karadeniz Kalkınma Ajansı (BAKKA) tarafından üst düzey siber güvenlik uzmanlarının yetiştirilmesi için hazırlanan "BAKKA Siber Güvenlik Uzmanı Yetiştirme Projesi (Siber Vatan)"nde kullanılan bir kavram olarak ortaya çıkmıştır.

topluluğunun fertlerinin siber alanda hem kendi içinde hem de küresel anlamda yoğun bir etkileşim içinde olduğu da göz önünde bulundurulmalıdır. Bu etkileşimin gerçekleştiği siber alan, nispeten mesafenin önemsizleştiği ve sınırların bulanıklaştığı artan bir tehdit ortamına da yataklık etmektedir (Bilgiç, 2021, s. 33). Bu çerçevede, sayısallaşan (dijitalleşen) devlet hizmetlerinin beraberinde, anonimlik sağlayan ve asimetrik olan siber alan (Gökçer & Gözen Ercan, 2020, s. 186) içinde devletin hak ve menfaatlerinin gözetilmesi gereken kavramsal bir alan olarak "siber vatan" kavramı da güvenlik bağlamında önem kazanmaktadır (Bilgiç, 2021, s. 34).

Son yıllarda, teröristler; giderek artan şekilde yeni teknik ve gelişmiş taktikleri alınan iç güvenlik tedbirlerini aşmak ve bireylerin güvenliğini, emniyetini ve refahını tehdit etmek üzere kullanmaktadır (ABD Anayurt Güvenliği Bakanlığı, 2019, s. 8). Bu bağlamda, güvenlik tedbirleri; devletin toprak unsurunun sınırları içinden ve dışından devletin egemenlik haklarını kullanmasına ve o devletin insan unsurunun yaşam tarzı ve düzenine yönelebilecek tehlikelerden korunmuş olma durumunu yaratmaya yönelik olmalıdır. Kamu güvenliği, özelde kişileri ve genelde toplumu tehdit eden her türlü tehlikenin önlenmesiyle sağlanır (Bilgiç, 2019a, s. 20). Bir ülkenin karşılaşabileceği tehditler ve bunun sonucunda beliren tehlikeler terörizm dâhil, salgın hastalıklardan afetlere kadar uzanan geniş bir yelpazede yer almaktadır. Fiziksel alanda çok aktörlü, karmaşık terör saldırılarını tespit etme ve önleme çabasına rağmen, terörist unsurlar saldırılarını gerçekleştirebilmek adına mümkün olan her türlü güvenlik açığını aramaya devam etmektedir. Bu tehdit ortamında, merkezî olmayan terörist grupların; ülkedeki bireyleri şiddete yönelik radikalleşmeye teşvik ve eleman olarak temin eden terör propagandasını ve eğitim materyallerini yaymak için İnternet'i ve sosyal medyayı kullandığı değerlendirilmektedir (ABD Anayurt Güvenliği Bakanlığı, 2019, s. 11). Bununla mücadele bir gayret birliği gerektirdiğinden, mücadelenin gerektirdiği tasarımı da içermelidir. Bu tasarım; özetle, mevcut veya gelecek güvenlik ihtiyaçlarını karşılamak üzere uzun vadeli ve stratejik çözümlere odaklanan hizmetleri tasarlamada kullanılan genel bir çerçeveyi betimleyen güvenlik mimarlığı kavramını işaret etmekte ve bu yönde strateji geliştirilmesi hususunu vurgulamaktadır (Yayla, 2020). Bu tasarımda kamu gücünün, hukuk düzeni içerisinde kanunların açıkça verdiği bir yetkiye dayanılarak kullanılması esastır. Zira içinde bulunulan durum gerektirdiğinde bu yetki; mevzuata uygun olarak zor kullanabilmeye imkân tanır. Kolluk faaliyetlerinde gerçekleştirilen eylem ve işlemlerin meşruiyeti, kamu düzeni için gereken haklı bir durumda bu yetkinin

hukukilik ve ölçülülük temelinde kullanılmasına dayalıdır (Bilgiç, 2019a, s. 326). Bu husus, kamu özgürlükleri ile güvenlik arasındaki dengenin hangi temelde kurulması gerektiğinin göstergesidir.

"Risk toplumu"nda, [9] (Beck U., 1992, s. 34) özellikle bireylerin teknoloji kullanım seviyesinin artışı ve beraberinde yaşanacak toplumsal değişimlere koşut olarak gelecekte güvenlik tehditlerinin de artacağı ve çeşitleneceği beklendik bir durumdur. Teknolojideki gelişmeler ve siber alandaki yoğun etkileşim suçlu düşünen beyinler için artırılmış suç işleme imkân ve kabiliyeti ile fırsatları yaratmakta olduğundan terörizm de bir suç türü olarak bundan nasibini alacaktır. Siber güvenlik olaylarının tespiti ve bunlara yönelik olarak gerçekleştirilecek müdahalelerde bu mecranın gözetiminde hem önleyici hem de adli bakımdan kapasite inşası önemli ihtiyaçtır (Bilgiç, 2021, s. 38). 2020-2023 dönemi için hazırlanan "Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" çerçevesinde stratejik amaçlar arasında da yer alan "siber güvenliğin milli güvenliğe entegrasyonu" önemlidir (Bilgiç, 2021, s. 38).

Teknolojinin gelişimi ve İnternet'in artan kullanımı ile beraber günümüzde siber alan özellikle terör örgütleri ve radikalleşen gruplar için pek çok amaç doğrultusunda kullanılmakta ve stratejik önemi haiz faktörlerden biridir. Bireyleri ve grupları radikalleştirme, propaganda yapma, finansal destek, terör eylemlerine teşvik, terör örgütlerine eleman temini, terör eylemlerine teşvik ve terörist amaçlarla bilginin toplanması ve yayılması gibi hususlarda siber alan aktif olarak kullanılmaktadır (UNODC, 2012, s. 1).

Bilgi teknolojilerinin gelişimi işletmeler, tüketiciler ve hükümetler gibi çeşitli resmî ve gayri resmî grupların birbirleriyle iletişim kurmaları ve "küresel köy"ün yer aldığı bir forumun oluşturulması için eşsiz fırsatlar sunmakla beraber, ağın büyüklüğü ve kullanımındaki muazzam büyüme, İnternet'in sunmuş olduğu ütopik vizyonlar, pornografik ve şiddet içerikli unsurlar ve İnternet'in aşırılık yanlısı kişiler tarafından kullanılması gibi faktörler; çok farklı siyasi hedefleri olan grupları bir araya getirmektedir. Radikalleşen gruplar; propaganda yapmak, destekçileriyle iletişim kurmak, kamuoyunu yönlendirmek ve davalarına sempati duyulmasını sağlamak ve eylemlerini planlayıp koordine etmek için siber alanı bir katalizöre dönüştürmüştür (Weimann, 2004, s. 3). 1990'lı yıllardan itibaren bireyler ve gruplar, çevrim içi kimlik harcıyla İnternet'te yeni sosyal gruplar, mekânlar ve

[9] Ulrich Beck (1992), "Risk Society: Towards a New Modernity" isimli kitabında insanlığın gelecekte karşılaşacağı belirsizlik bağlamında geleceğin toplumunu bu şekilde tanımlamıştır.

ağlar kararak dijitalleşme deneyimleri kapsamını genişletmektedirler. Bu nedenle iletişimin siber alana kayması özellikle terörizm ve radikalleşme üzerine yapılan kavramsallaştırmalar, klasik radikalleşme teorilerinin ötesine geçmiştir (Topal, 2018, s. 210). Bireylere her türlü kimliğe bürünme fırsatı veren siber alandaki anonimlik; yüz yüze etkileşimin baskısı olmadan çevrimiçi iletişim kurmanın görece kolaylığıyla da özellikle yalnız, marjinalleşmiş, iddialı olmayan ve asosyal bireylerin çok hızlı bir şekilde radikalleşmesine zemin hazırlamaktadır. Siber alanda bireyler anonimlik perdesi gerisinde daha düşük sosyal kaygı, daha fazla sosyal arzu edilebilirlik ve yüksek benlik saygısı yaşayarak kendilerininkine benzer düşüncelerle kolayca tanışmakta ve sonrasında şiddet ve aşırılık yanlısı faaliyetlerde bulunma eğilimi göstermektedirler (Topal, 2018, s. 215).

Siber alanda radikalleşme süreci, bünyesinde propaganda kullanımını içermektedir. Bu ortamda radikalleşme ve teröre teşvik; bireysel koşullara ve ilişkilere bağlı olarak değişkenlik göstermekle birlikte, öncelikle bireylerin aşırılık yanlısı ideolojilere dayalı şiddetle hareket etmeyi içselleştirmesine etki eden telkin sürecini ifade etmektedir (UNODC, 2012, s. 6). Radikalleşmeyi yaratan koşullar bağlamında, radikalleşen grup aslında buz dağı metaforunda yalnızca görünen kısmın bir ifadesidir. Bu bağlamda radikalleşmeyle mücadelede kapsamlı bir stratejinin birey, örgüt ve toplum düzeyinde dikkate alması gerekmektedir (Muro, 2016).

Adına devlet denen aygıtın, sosyal sözleşme teorisi anlatımıyla, en bilinen anlamda, kendisini oluşturan insanların güvende olma isteğiyle gücüne rıza gösterdiği ve kendisinden kamu düzenini sağlaması beklenen bir yapı olduğunu söylemek yanlış olmayacaktır (Bilgiç, 2021, s. 34). Kamu düzenini sağlamak maksadıyla, bu yapı; halkın bütününe ve onu meydana getiren bireylere yönelen her türlü tehlikelerden onları korumak için, hukuk düzenini içerisinde kendisine açıkça tanınan yetkilere dayanarak, teşkilatlar kurup etkinlikler yürüterek tedbirler almakta, kendisine özgülenmiş güçle kamu özgürlüklerine sınırlamalar koymakta, belli kamu makam ve görevlilerini bununla yetkilendirmekte ve tüm bunları denetlemektedir. Burada bahsedilenler, devletin kamu düzenini sağlamaya yönelen bir kamu hizmeti olarak kolluk görevini tanımlamaktadır (Bilgiç, 2019b, s. 19). Kamu düzeninin unsurlarından biri olarak kamu güvenliği, "tehlikelerin önlenmesi ile bu yapıyı meydana getiren unsurların devletle ve birbirleri ile ilişkilerinin ve varlıklarının tehlikelerden korunması durumu ve bu duruma ilişkin toplumda bir inanç oluşmasıyla, toplumsal yaşayışta güvenliğin sağlanmış olması hâlidir" (Bilgiç, 2019a, s. 20). Bu hâl, iç ve dış güvenlik kavramlarıyla da ilişkilidir.

Devletin kendi toprak alanının sınırları içinde devletin en üstün otorite olmasını ifade eden iç egemenliğin ve uluslararası hukuk açısından bağımsız ve diğer devletlerle kurduğu ilişkilerde eşit olmasını ifade eden dış egemenliğin gereği ve sonucu olan iç ve dış güvenlik sınırları günümüzdeki siber ortamda artık bulanıklaşmıştır (Bilgiç, 2021, s. 34). Güvenlik kavramı klasik anlamda devletin toprak unsurunun sınırlarıyla ilişkilendirilerek tanımlanabilmektedir. Ancak sınırları aşan küresel bir fenomen olarak İnternet ortamında gerçekleşen etkileşimin ve bu etkileşimin hızının yoğunluğu sayesinde, bu ortamda radikalleşen bireyler ve davranışları da fiziksel sınırlardan bağımsız hâle gelmiştir (Marion & Twede, 2020, s. xiv, xv). Bu minvalde, terörizmin niteliğinin ve yöntemlerinin de bu gelişmelerden etkilenmesi doğaldır.

Geleneksel medya ve bugün bütün sınırları değiştirip kendine yeni ve kontrollü zor kapılar açan sosyal medya; bireylerin ve toplumların hayata dönük algılarını, düşüncelerini şekillendirme gücü yüksek bir potansiyele sahiptir. Özellikle bilgi teknolojilerindeki gelişime bağlı olarak gelişen İnternet etkileşimi vasıtasıyla iletişim okuma-yazma boyutundan, sadece okumaya ve bugün gelinen noktada okuma ve dönüşmeye sebep olan bir işleve dönüşmüştür. Siber alanda iletişimde sınırların ortadan kalkması sebebiyle denetim ve kontrol boşlukları ortaya çıkmakta ve bu boşluktan da özellikle terör örgütleri faydalanmakta, terör örgütleri aktif bir şekilde destekçi ve sempatizan devşirme imkânına kavuşmaktadır (Çakır, vd., 2017, s. 31, 32).

SONUÇ

İletişim bakımından siber alan, gelişen teknolojiler vasıtasıyla küresel erişimi kolaylaştıran ve dünya çapında sürekli büyüyen bir kitleye ulaşmaya imkân tanıyan, sınırsız seyirci ile bilgi ve fikir paylaşımına uygun eşsiz bir ağ örmüştür (UNODC, 2012, s. 3). Bu örüntü, günümüzde insanların çevreleriyle iletişim kurarken edindikleri algıları ağırlıklı olarak teknolojik araçlar vasıtasıyla şekillenmektedir (Al, 2022, s. 15). Günümüzde siber alanda "çevrim içi radikalleşme"nin (Topal, 2018, s. 19) öznesi olan gruplar, sosyal medyanın da kullanımıyla, belirli bir süre içerisinde terör örgütlerine destek sağlayan bir noktaya evrilmektedir. Bu bağlamda siber alanda terör örgütlerinin yaşam döngüsünde habitat ve besin sağlayan araçları kontrol altına almak özellikle kamu güvenliğini koruma noktasında elzem olarak değerlendirilmektedir (Çakır, vd., 2017, s. 33).

Klasik iletişim araçlarının ötesinde her geçen gün popülerliğini arttıran yeni medya, özellikle Telegram, Instagram, Facebook, Twitter gibi sosyal medya

platformları, kullanıcılarının etkileşimleriyle, bilginin oluşumuna, yayımına ve zamanla tekrar ortaya çıkışına hız kazandırmıştır (Albayrak, Topal, & Altıntaş, 2017, s. 1991). Bu hızlı akıştan ve teknolojik gelişmelerden sadece yerleşik devlet düzenine ve onun kurallarına uyan vatandaşlar değil, örülmeye çalışılan toplumsal dokunun temellerini sarsan oluşumlar da faydalanmaktadır.

İnternetteki bilgilere erişimin engellenmesi ve içeriğin yayılmasına ilişkin yasal kısıtlamalar konmasına bir alternatif yaratmak üzere teknolojik bir çözüm olarak İnternet İçeriği Seçimi Platformu (The Platform for Internet Content Selection - PICS), ifade ve haberleşme özgürlüğü değerlerinden ödün vermeden İnternette yayımlanan içeriklere yönelik politika sorununu çözmek için tasarlanmıştır (Reidenberg, 1998, s. 558, 559). Anayasa'ya göre Türkiye Cumhuriyeti Devleti'nde herkes haberleşme, düşünceyi açıklama ve yayma ile haber alma hürriyetine sahiptir. Ancak temel hak ve özgürlükler kapsamında kişilere tanınan Anayasal güvenceler; millî güvenliği, devletin iç ve dış güvenliğini, devletin ülkesi ve milletiyle bölünmez bütünlüğünü, kamu düzenini ve güvenliğini tehdit etmeye, suç işlemeye, ayaklanmaya ya da isyana teşvik eder nitelikte yorumlanarak kullanılamayacak olmakla birlikte (örneğin; md.22, md.26 ve md.28); bu haklar özlerine dokunulmaksızın yalnızca belirtilen sebeplere bağlı olarak ve ancak kanunla sınırlanabilecektir (md.13) (Türkiye Cumhuriyeti Anayasası, 1982). Bu doğrultuda, müstehcenlik ile ilgili sınırlamaların ve yaptırımların varlığı da hatırlandığında, yasa yapıcının nazarında da İnternet'in, başta terör olmak üzere, suç işlemek için kullanılmasının kişisel özgürlük olarak görülmediği ortadadır. İnternet içeriklerinin otomatik filtrelenmesini sağlayacak, olası tehdit ve risk durumlarını ortaya çıkaracak bir standart kanunen yaratılabilir. Böyle bir düzenleme yapma ihtiyacı hâsıl olsa bile, temel hak ve özgürlüklerin de aynı hassasiyetle korunması demokratik toplum gerekliliklerindendir ancak bunun nasıl yapılacağı ayrıca incelenmesi gereken bir konu başlığı olarak değerlendirilmektedir.

KAYNAKÇA

ABD Anayurt Güvenliği Bakanlığı (2019). The DHS Strategic Plan: Fiscal Years 2020-2024. Erişim tarihi: 22.02.2022, https://www.dhs.gov/sites/default/files/publications/19_0702_plcy_dhs-strategic-plan-fy20-24.pdf

Akdemir, N & C. O. Tuncer. (2021). Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım, Ankara: Pegem Akademi.

Akkol, M. L. (2019). Jürgen Habermas'ın İletişimsel Eylem Kuramı ve Kamusal Alan Kavramının Analizi. Pamukkale Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, 37, 171-180. doi:DOI:10.30794/pausbed.541364.

Al, E. (2022). Covid Döneminde Radikalleşen Zaman ve Mekân: İletişim Araçları Örneği. Erciyes İletişim Dergisi, 9(1), 145-164. Erişim tarihi: 25.02.2022, https://dergipark.org.tr/tr/download/article-file/1998046

Albayrak, M., Topal, K., & Altıntaş, V. (2017). , Sosyal Medya Üzerinde Veri Analizi: Twitter. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 22(Special Issue on Kayfor15), 1991-1998.

Anadolu Ajansı (2016). NSA çalışanı "çok gizli belgeleri çalmak" suçundan tutuklandı. Erişim tarihi: 18.02.2022, https://www.aa.com.tr/tr/dunya/nsa-calisani-cok-gizli-belgeleri-calmak-sucundan-tutuklandi/659258

Aneesh, A. (2002). Technologically Coded Authority: The Post-Industrial Decline in Bureaucratic Hierarchies. International Summer Academy on Technology Studies. Deutschlandsberg, Austria. Erişim tarihi: 15.02.2022, https://www.researchgate.net/publication/254843955_Technologically_Coded_Authority_The_Post-Industrial_Decline_in_Bureaucratic_Hierarchies

Avcı, E. (2021). Terörist Rehabilitasyonu ve Radikalleşmeden Dönüş: Bir Model Önerisi. Ege Stratejik Araştırmalar Dergisi, 12(1), 1-19.

Bannister, F. (2005). The Panoptic State: Privacy, Surveillance and the Balance of Risk. Information Polity, 10, 65-78. doi:DOI:10.3233/ip-2005-0068.

BBCNews (2019). Immanuel Wallerstein: Dünya Sistemleri Teorisi'ni Geliştiren Ünlü Sosyolog Kimdir?. Erişim tarihi: 20.02.2022, https://www.bbc.com/turkce/haberler-dunya-49558423

Beck, C. J., & Schoon, E. W. (2018). Terrorism and Social Movements. D. A. Snow, S. A. Soule, H. Kriesi, & H. J. McCammon içinde, The Wiley Blackwell Companion to Social Movements (s. 698-713). doi:DOI:10.1002/9781119168577.ch40.

Beck, U. (1992). Risk Society: Towards a New Modernity. (M. Ritter, Çev.) London: SAGE Publications Ltd.

Behr, I. v., Reding, A., Edwards, C., & Gribbon, L. (2013). Radicalisation in the Digital Era: The Use of the Internet in 15 Cases of Terrorism and Extremism. California: The RAND Corporation. Erişim tarihi; 17.02.2022, https://www.rand.org/pubs/research_reports/RR453.html

Bilgiç, A. (2019a). Düzenli Karmaşa: İç Güvenlik Yapılanmasında Çoklu Kolluk Sistemi. Ankara: Gazi Kitabevi.

Bilgiç, A. (2019b). Tarihsel Süreçte Türk İç Güvenlik Yapılanması ve Yönetimi. T. Avaner, & O. Zengin içinde, Türkiye'de İç Güvenlik Yönetimi (s. 18-39). Ankara: Gazi Kitabevi.

Bilgiç, A. (2021). Siber Vatan ve Siber Güvenlik: Siber Tehditlerle Mücadele Örgütlenmesinde Türkiye Örneği. İdarecinin Sesi, 32-39.

Borum, R. (2011). Radicalization into Violent Extremism II: A Review of Conceptual Models and Empirical Research. Journal of Strategic Security, 4(4), 37-62.

Boyle, J. (1997). Foucault in Cyberspace: Surveillance, Sovereignty, and Hardwired Censors. University of Cincinnati Law Review, 66, 177-205.

Çakır, M., Aslan, Ö., Söylemez, H., Öztürk, M., Şahin, Y., & Demirbaş, M. (2017). Radikalleşme, Şiddet İçeren Aşırılık ve Terörizm. Ankara: Polis Akademisi Yayınları.

Çardak, B. (2021). Değişen Güvenlik Ortamlarında Radikalleşme ve Sosyal Medyanın Radikalleşme Üzerine Etkisi. 1. Uluslararası Hitit Güvenlik Çalışmaları Kongresi Bildiri Kitabı (s. 320-325). Çorum: Hitit Üniversitesi.

Derin, G., & Öztürk, E. (2019). Terör ve terörizmin psikolojik dinamikleri ve radikalleşme, , . V. Uluslararası TURKCESS Eğitim ve Sosyal Bilimler Kongresi, (s. 1125-1132).

Elektrik Mühendisleri Odası İstanbul Şubesi (2016). Önsöz. B. Çoban, & B. Ataman içinde, Gözetim Toplumu: Panoptikon (s. 3-4). İstanbul: Ege Basım. Erişim tarihi: 18.02.2022, https://www.emo.org.tr/ekler/dbf17031f5a9c1f_ek.pdf

Erken, E. (2021). Siber Ortam (Cyberspace). N. Akdemir, & C. O. Tuncer içinde, Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım (s. 465-467). Ankara: Pegem Akademi.

Foucault, M. (1994). İktidarın Gözü: Seçme Yazılar 4 (3 b.). (I. Ergüden, Çev.) İstanbul: Ayrıntı Yayınları.

Franchi, T., & Vichi, L. P. (2019). The Beginning of Warfare on the Internet: Zapatista Strategic Communications. Defence Strategic Communications, 6. doi:DOI 10.30966/2018.RIGA.6.4.

Gökçer, O., & Gözen Ercan, P. (2020). Siber Savaşlarda Jus ad Bellum ve Jus in Bello. Alternatif Politika, 12(1), 172-203. Erişim tarihi: 15.02.2022, https://alternatifpolitika.com/site/cilt/12/sayi/1/7-Gokcer%26Gozen-Ercan-Siber-Savas-Jus-Ad-Bellum-Jus-In-Bello.pdf

Gunn, A., & Demirden, A. (2019). Radikalleşmenin Önlenmesi & Terörizm Olgusu. Polis Akademisi Yayınları.

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

Han, B. C. (2012). The Transparency Society. (E. Butler, Çev.) Berlin: MSB Matthes & Seitz Berlin.

Hassan, S., & deFilippi, P. (2017). The Expansion of Algorithmic Governance: From Code is Law to Law is Code. Field Actions Science Reports: The Journal of Field Actions(Special Issue 17). Erişim tarihi: 15.02.2022, http://journals.openedition.org/factsreports/4518

Hauben, M. (2019). Researching the "Net": A Talk on The Evolution of Usenet News and The Significance of the Global Computer Network. The Amateur Computerist, 32(2), 3-11. Erişim tarihi: 18.02.2022, http://www.ais.org/~jrh/acn/ACn32-2_one_column.pdf#page=3

Kaygısız, Ü. (2017). Panoptikon: Demokrasi Ekseninde Realiteden Kurgusala Doğru Bir Bakış. Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 22(Kayfor15 Özel Sayısı), .2073-2094. Erişim tarihi: 17.02.2022, https://iibfdergi.sdu.edu.tr/assets/uploads/sites/352/files/yil-2017-cilt-22-sayi-kayfor15-yazi36-30122017.pdf

Kömürcü, R. R. (2009). Avrupa Birliği'nin Bölgeselleşmesi ve Ulus Devlet: Fransa Örneği. Ankara: Ankara Üniversitesi Sosyal Bilimler Enstitüsü. Erişim tarihi: 15.02.2022, https://dspace.ankara.edu.tr/xmlui/bitstream/handle/20.500.12575/37526/250137.pdf?sequence=1

Kuner, C., Cate, F. H., Millard, C., Svantesson, D. J., & Lynskey, O. (2015). Internet Balkanization Gather Pace: Is Prıvacy The Real Driver? International Data Privacy Law, 5(1), 1-2. doi:DOI:10.1093/idpl/ipu032.

Kurum, M. (2017). Terörist Örgütlerin Güvenli Ortamları ve PKK. Ankara: Nobel Yayınevi.

Kurum, M., & Avcı, E. (2018). Radikalizm ve Aşırıcılıktan Terörizme: Siyasal Şiddetin Araçsallaştırılması. Güvenlik Stratejileri Dergisi, 14(28), 37-90.

Lang, S. B. (2004). The Impact of Video Systems on Architecture. Zurich: Swiss Federal Institute of Technology Zurich. Erişim tarihi: 14.02.2022, https://cgl.ethz.ch/Downloads/Publications/Dissertations/Lan04.pdf

Marion, N. E., & Twede, J. (2020). Cybercrime: An Encyclopedia of Digital Crime. Santa Barbara: ABC-CLIO, LLC.

Muro, D. (2016). What Does Radiaclization Look Like? Four Visualisations of Socialisation into Violent Extremism. Erişim tarihi: 15.02.2022, https://www.cidob.org/publicaciones/serie_de_publicacion/notes_internacionals_cidob/n1_163/what_does_radicalisation_look_like_four_visualisations_of_socialisation_into_violent_extremism

Nye, J. S. (2014). The Regime Complex For Managing Global Cyber Activities. Global Commission on Internet Governance Paper Series: No. 1.

Orwell, G. (1949). Nineteen Eighty Four. 2003, New York: Plume.

Özdel, G. (2012). Foucault Bağlamında İktidarın Görünmezliği Ve ‘’Panoptikon’’ İle ‘’İktidarın Gözü’’ Göstergeleri. The Turkish Online Journal of Design, Art and Communication, 2(1), 22-29. Erişim tarihi: 12.02.2022, https://dergipark.org.tr/tr/download/article-file/138301

Paçacı, İ. (2018). Akademik Sosyal Araştırmalar Dergisi, 6(85), 104-125. Erişim tarihi: 11.02.2022, https://www.researchgate.net/publication/334573451_KURESEL_GOZETIM_DUZENI_VE_ILETISIM_ALTYAPISI_KURESEL_ILETISIM_DUZENININ_ARKA_PLANI

Paye, J. C. (2003). Terörle Mücadele ve Özel Hayatın Denetimi. (Ç. E. Sinirlioğlu, Dü.) Conatus Çeviri Dergisi, 1. Erişim tarihi: 12.02.2022, http://www.antimai.org/bs/elifconatus.htm

Reidenberg, J. R. (1998). Lex Informatica: The Formulation of Information Policy Rules through Technology. Texas Law Review, ,, 76(3), 553-593. Erişim tarihi: 11.02.2022, https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1041&context=faculty_scholarship

Ronfeldt, D., & Arquilla, J. (2001). Emergence And Influence Of The Zapatista Social Netwar. D. Ronfeldt, & J. Arquilla içinde, Networks and Netwars: The Future of Terror, Crime, and Militancy. Santa Monica, CA: RAND Corporation.

Schmid, A. (2013). Radicalisation, De-Radicalisation, Counter-Radicalisation: A Conceptual Discussion and Literature Review. ICCT Research Paper.

Sönmez, G. (2017). Çoklu Radikalleşmenin Odağında Türkiye ve Mücadelesi. Journal of Security Studies, 1-19.

Şimşek, S. S. (2021a). Siber Gözetim. N. Akdemir, & C. O. Tuncer içinde, Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım (s. 392-397). Ankara: Pegem Akademi.

Şimşek, S. S. (2021b). Post-Panoptikon Çağda Gözetim, Ulusal Kimlik ve Egemenlik İnşası: Türkiye’nin Ulusal Araştırma Motoru “Yaani” Örneği. II. Uluslararası Güvenlik Kongresi Bildiri Özet Kitabı. Ankara: Jandarma ve Sahil Güvenlik Akademisi. Erişim tarihi: 11.02.2022, http://www.jsga.edu.tr/kurumlar/jsga.edu.tr/Haberler/2021/Eylul/UluslararasiGKProgram/II-Uluslararasi-Guvenlik-Kongresi_-Bildiri-Ozet-Kitabi.pdf

Şimşek, S. S. (2021c). Siber Yönetişim (Cyber Governance). N. Akdemir, & C. O. Tuncer içinde, Siber Ansiklopedi: Siber Ortama Çok Disiplinli Bir Yaklaşım (s. 508-513). Ankara: Pegem Akademi.

Tanrıverdi, E. G. (2008). Sosyolojik Açıdan Küreselleşme ve Ulus-Devlet: Giddens, Bauman ve Habermas Örneği. Sakarya: Sakarya Üniversitesi Sosyal Bilimler Enstitütüsü. Erişim tarihi: 13.02.2022, https://acikerisim.sakarya.edu.tr/bitstream/handle/20.500.12619/77593/T03808.pdf?sequence=1&isAllowed=y

Thompson, R. (2011). Radicalization and the Use of Social Media. Journal of Strategic Security, 4(4), 167-190.

Todd, P., & Bloch, J. (2003). Global Intelligence: the World's Secret Services Today. London: Zed Books.

Topal, R. (2018). A Cyber-Psychological and Behavioral Approach to Online Radicalization. J. McAlaney, L. A. Frumkin, & V. Benson içinde, Psychological and Behavioral Examinations in Cyber Security (s. 210-221).

Türkiye Cumhuriyeti Anayasası (Cilt (17863; Mükerrer)). (1982). T.C. Resmî Gazete. Erişim tarihi: 14.02.2022 https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=2709&MevzuatTur=1&MevzuatTertip=5

UNODC (2012). The Use of the Internet for Terrorist Purposes. United Nations.

Ünlü, D. G. (2018). Şeffaflık Toplumu: Şeffaf Toplumun Eleştirisi Üzerine Bir Okuma. Galatasaray Üniversitesi İletişim Dergisi, 28, 281-290. doi:DOI:10.16878/gsuilet.436058.

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

Weimann, G. (2004). www.terror.net: How Modern Terrorism Uses the Internet. United States Institute of Peace. Erişim tarihi: 16.02.2022 https://www.usip.org/sites/default/files/sr116.pdf

Yaşa, G. A. (2019). Dini Referanslı Radikalleşme Örüntüleri: Suriye Örneği. Ankara: Ankara Yıldırım Beyazıt Üniversitesi.

Yayla, U. (2020). Bilgi Güvenliği Bakış Açısı ile Kurumsal Güvenlik Mimarisi. Erişim tarihi: 15.02.2022, https://www.siberportal.org/white-team/governance/bilgi-guvenligi-bakis-acisi-ile-kurumsal-guvenlik-mimarisi/

Yüksel, C. (2020). Uluslararası Hukukta İnternet ve Sosyal Medyanın Terörist Amaçlarla Kullanılmasına Karşı Mücadele ve Çözüm Önerileri. Public and Private International Law Bulletin, 40(2), 1089–1112.