TESAM Akademi Dergisi
Journal of TESAM Academy
ISSN 2148-2462 / E-ISSN 2458-9217

Çevrimiçi Radikalleşmeye Karşı Çevrimiçi Mücadele: İnternetin Radikalleşmeyle Mücadelede Kullanılması

Online Fight Against Online Radicalization: Using the Internet for Counter Radicalization

Emre ÇITAK

Doç. Dr.,
Hitit Üniversitesi, İİBF, Uluslararasi İlişkiler Bölümü .
emrecitak@hitit.edu.tr
ORCID : 0000-0002-8704-6495

Cilt / Issue: 11(2) 485-514
Geliş Tarihi: 25.12.2023
Kabul Tarihi: 11.06.2024

Atıf: Çıtak, E. (2024). Çevrimiçi radikalleşmeye karşı çevrimiçi mücadele: İnternetin radikalleşmeyle mücadelede kullanılması. *Tesam Akademi Dergisi*, *11*(2), 485-514. http://dx.doi.org/10.30626/tesamakademi.1409425.

Öz

Bu çalışmada çevrimiçi radikalleşmeyle mücadelede çevrimiçi ortamdan ve araçlardan nasıl yaralanabileceği üzerine bir çerçeve çizilmesi planlanmaktadır. Günümüzde radikalleşmeyle mücadele ve radikalleşmenin tersine döndürülmesi güvenlik güçlerinin önemli bir sorumluluğuyken, her ne kadar yeni bir olgu olmasa da oldukça dinamik ve karmaşık bir nitelikte olması nedeniyle çevrimiçi radikalleşme özel bir meydan okuma muhteva etmektedir. Çevrimiçi ortamın her türlü arayışı ve paylaşımı kolaylaştırıcı etkisi, radikalleşmenin gerçekleşmesinde oldukça belirleyicidir. Bu nedenle günümüzde geleneksel yüz yüze ve grup içi radikalleşmeden daha yoğun ve etkili şekilde çevrimiçi ortamların kullanılması kapsamlı bir inceleme yapılmasını gerekli kılmaktadır. Bunun yanında radikalleşmenin önlenmesi ve ilgili mücadele için uygulanan pek çok strateji bulunurken, çevrimiçi boyutun temele alındığı bir analizin yapılması bu çalışmanın temel eğilim noktasıdır. Çevrimiçi radikalleşmenin geleneksel radikalleşmeden oldukça farklı özellikler göstermesi, ilgili önleme ve mücadele faaliyetlerinin de kendine has özelliklerinin olmasını gerektirmektedir. Özellikle çevrimiçi platformların ve araçların çevrimiçi radikalleşmeyle mücadele kullanılmasına yönelik öneriler bu çalışmanın özel yönünü yansıtacaktır. Çalışma öncelikle çevrimiçi radikalleşme üzerine bilgilendirici bir bölümle başlayacak, izleyen bölümde radikalleşme ve çevrimiçi radikalleşmeyle mücadelede çevrimiçi stratejiler üzerine bir tartışma ortaya konulacaktır. Sonuç bölümünde ise internet ve teknolojideki gelişimin radikal gruplar tarafından ne şekilde kullanılmaya devam edeceğine yönelik bir risk değerlendirmesi yapılacaktır. Böylece çevrimiçi radikalleşme ve deradikalizasyon özelinde, radikalleşme literatürüne katkı sağlanması amaçlanmaktadır.

Anahtar Kelimeler: Radikalleşme, Çevrimiçi Radikalleşme, Deradikalizasyon, Terörizm, Radikalleşmeyle Mücadele

Abstract

This study is planned to draw a framework on how to benefit from online space and tools in the fight against online radicalization. While combating and reversing radicalization is a significant responsibility of security forces today, online radicalization poses a special challenge since it is quite dynamic and complex, although it is not a new phenomenon. The facilitating effect of the online environment in all kinds of searches and sharing is very decisive in the realization of radicalization. For this reason, today's use of online environments more intensely and effectively than traditional face-to-face and in-group radicalization requires a comprehensive examination. In addition, while there are many strategies implemented to prevent and combat radicalization, the main trend of this study is to conduct an analysis based on the online dimension. The fact that online radicalization has very different characteristics from traditional radicalization requires that relevant prevention and combat activities have their characteristics. In particular, suggestions for using online platforms and tools to combat online radicalization will reflect the special aspect of this study. The study will first begin with an informative section on online radicalization, and the following section will present a discussion on online strategies to combat radicalization and online radicalization. In the conclusion section, a risk assessment will be made regarding how the developments in the internet and technology will continue to be used by radical groups. Thus, it is aimed to contribute to the radicalization literature, specifically on online radicalization and deradicalization.

Keywords: Radicalization, Online Radicalization, Deradicalization, Terrorism, Counter-Radicalization

Extended Abstract

Radicalization is one of the most frequently cited concepts in current security discussions. The essence of the definition of radicalization is that people experience a process that leads to extremism based on an ideology or intellectual approach. In this process, the perception of life and others is shaped in its psychological and sociological dimensions, the individual can engage in a wide range of orientations, from social isolation to legitimizing the use of violence against others. The basis of this process, which is also referred to as change or transformation, is the person's encounter with a new way of thinking or different interpretations of his/her existing views. Afterwards, depending on the course of the process, radicalization can be experienced at various levels and directions. For example, radicalization can be observed at the cognitive-mental level or to the extent that it shapes behavior.

Social media, web pages and the dark net create a virtual environment with unclear boundaries. While the unique features of this medium

enable individuals to reach their searches more easily, it also provides advantages for radical groups to meet many of their needs. Here, materials containing excessive or harmful content are produced, circulated and shared without being subjected to serious obstruction, discussions on the most contrary views are held in forums and chat rooms with the participation of many users, pioneers of various ideologies can address their followers through audio and video broadcasts, illegal groups are able to reach large audiences with secret and open messages and preliminary meetings/communication are provided for relationships that will be reflected in real life. Thus, favorable conditions emerge for radicalization relationships and processes. In this regard, online radicalization stands out as an important topic that needs to be discussed in security, terrorism and radicalization research.

Online radicalization is under the spotlight today, especially as it has become a part of the intense activities of terrorist organizations and some populist groups on the internet. It is noteworthy that individuals have moved to a radical level in their cognition and behavior levels with the conversations they have on the internet, the information they acquire and the relationships they enter into. In addition to the numerous advantages that online platforms provide for general users, the fact that they have become an area of intense activity for radical groups also brings to the fore the necessity and importance of the struggle in this area.

This study is planned to draw a framework on how to benefit from online space and tools in the fight against online radicalization. While combating and reversing radicalization is a significant responsibility of security forces today, online radicalization poses a special challenge since it is quite dynamic and complex, although it is not a new phenomenon. The facilitating effect of the online environment in all kinds of searches and sharing is very decisive in the realization of radicalization. For this reason, today's use of online environments more intensely and effectively than traditional face-to-face and in-group radicalization requires a comprehensive examination. In addition, while there are many strategies implemented to prevent and combat radicalization, the main trend of this study is to conduct an analysis based on the online dimension. The fact that online radicalization has very different characteristics from traditional radicalization requires that relevant prevention and combat activities have their characteristics. In particular, suggestions for using online platforms and tools to combat online radicalization will reflect the special aspect of this study. The study will first begin with an informative section on online radicalization, and the following section will present

a discussion on online strategies to combat radicalization and online radicalization. In the conclusion section, a risk assessment will be made regarding how the developments in the internet and technology will continue to be used by radical groups. Thus, it is aimed to contribute to the radicalization literature, specifically on online radicalization and deradicalization.

Giriş

Radikalleşme, güncel güvenlik tartışmalarının içinde en çok atıf yapılan kavramlardan biridir. Kişilerin bir ideoloji veya fikrî yaklaşım üzerinden aşırılaşmaya giden bir süreci tecrübe etmeleri radikalleşme tanımının özünü oluşturmaktadır. Psikolojik ve sosyolojik boyutlarıyla hayata ve diğerlerine yönelik algının şekillendiği bu süreçte kişi, toplumsal izole eğiliminden diğerlerine yönelik şiddet kullanmayı meşrulaştırmaya kadar geniş bir yelpazede yönelim içine girebilmektedir. Kökten değişim veya dönüşüm olarak da ifade edilen bu süreçte temeli, kişinin yeni bir düşünce tarzıyla veya mevcut görüşlerinin farklı yorumlarıyla karşılaşması oluşturmaktadır. Sonrasında ise sürecin seyrine göre, radikalleşme çeşitli düzeylerde ve yönlerde tecrübe edilebilmektedir. Örneğin; bilişsel-zihinsel düzeyde veya davranışları şekillendiren ölçüde radikalleşme gözlemlenebilmektedir.

Geleneksel çerçevede radikalleşme bireyin içine dâhil olduğu sosyal bir grup ve grup içindeki etkileşimle gerçekleşmektedir. Birey sahip olduğu, merak ettiği veya etkisinde kaldığı düşüncelerin farklı boyutlarıyla grup dinamizmi etkisiyle tanışmakta ve görüşlerinde zamanla ciddi bir değişim gerçekleşmektedir. Benzer fikirlerin yüksek perdeden ve kısıtlanmadan tartışıldığı çevrelerde, grup üyelerinin birbirlerinden etkilenme ihtimalleri daha yüksek olurken ortak görüşe olan bağlılıkları da doğal olarak artmaktadır. Zaman içinde kendi görüşlerinin giderek kemikleşmesi ve diğer görüşlerin reddedilmesi durumu belirgin şekilde ortaya çıkmaktadır. Böylece birey radikal dönüşüm olarak adlandırılan sürecin aşamalarını yaşamaktadır. Günümüzde çevrimiçi alan radikalleşme süreci için oldukça uygun bir ortam oluşturmaktadır. İnsanlar çevrimiçi ortamda daha rahat şekilde bir araya gelebilmekte, var olan gruplarını genişletebilmekte veya ilgi alanlarına göre yeni ilişkiler kurabilmektedirler. Yoğun iletişim ve etkileşim olanakları, radikal grupların çevrimiçi faaliyetlerinin giderek artması sonucunu doğurmaktadır.

Sosyal medya, ağ sayfaları ve karanlık net sınırları belirsiz sanal bir mecra oluşturmaktadır. Bu mecranın kendine has özellikleri bireylerin arayışlarına daha kolay ulaşmalarını sağlarken, radikal grupların da pek çok ihtiyacını karşılamaları için avantajlar sağlamaktadır. Burada aşırı veya zararlı içerik muhteva eden materyaller ciddi bir engellemeye maruz kalmadan üretilmekte, dolaşıma sokulmakta ve paylaşılmakta, forum ve sohbet odalarında en aykırı görüşler üzerine pek çok kullanıcının katıldığı tartışmalar gerçekleştirilmekte, sesli ve videolu yayınlarla çeşitli

ideolojinin öncüleri takipçilerine seslenebilmekte, yasa dışı gruplar gizli veya açık mesajlarla geniş kitlelere ulaşabilmekte ve gerçek hayata yansıtılacak ilişkiler için ön görüşme/ haberleşme sağlanmaktadır. Böylece radikalleşme ilişkileri ve süreci için uygun koşullar ortaya çıkmaktadır. Bu doğrultuda çevrimiçi radikalleşme; güvenlik, terörizm ve radikalleşme araştırmalarında üzerinde tartışılması gereken önemli bir başlık olarak öne çıkmaktadır.

Çevrimiçi radikalleşme, özellikle terör örgütlerinin ve kimi popülist grupların internetteki yoğun faaliyetlerinin bir parçası haline gelmesi nedeniyle günümüzde mercek altındadır. Bireylerin internet üzerindeki görüşmeleri, edindiği bilgiler ve girdikleri ilişkilerle birlikte biliş ve davranış düzeylerinde radikal bir seviyeye geçmeleri dikkat çeken noktadır. Çevrimiçi platformların genel kullanıcıların için sağladığı sayısız avantajın yanı sıra radikal grupların yoğun faaliyet alanı haline gelmesi bu alandaki mücadelenin gerekliliğini ve önemini de gündeme getirmektedir.

Bu çalışmada çevrimiçi radikalleşmeyle mücadelede çevrimiçi alandan ve araçlardan nasıl yaralanabileceği üzerine bir çerçeve çizilmesi planlanmaktadır. Günümüzde radikalleşmeyle mücadele ve radikalleşmenin tersine döndürülmesi güvenlik güçlerinin önemli bir sorumluluğuyken, her ne kadar yeni bir olgu olmasa da oldukça dinamik ve karmaşık bir nitelikte olması nedeniyle çevrimiçi radikalleşme özel bir meydan okuma muhteva etmektedir. Çevrimiçi ortamın her türlü arayışı ve paylaşımı kolaylaştırıcı etkisi, radikalleşmenin gerçekleşmesinde oldukça belirleyicidir. Bu nedenle günümüzde geleneksel yüz yüze ve grup içi radikalleşmeden daha yoğun ve etkili şekilde çevrimiçi ortamların kullanılması kapsamlı bir inceleme yapılmasını gerekli kılmaktadır. Bunun yanında radikalleşmenin önlenmesi ve ilgili mücadele için uygulanan pek çok strateji bulunurken, çevrimiçi boyutun temele alındığı bir analizin yapılması bu çalışmanın temel eğilim noktasıdır. Çevrimiçi radikalleşmenin geleneksel radikalleşmeden oldukça farklı özellikler göstermesi, ilgili önleme ve mücadele faaliyetlerinin de kendine has özelliklerinin olmasını gerektirmektedir. Özellikle çevrimiçi platform ve araçların çevrimiçi radikalleşmeyle mücadele kullanılabilmesine yönelik öneriler bu çalışmanın özel yönünü yansıtacaktır. Çalışma öncelikle çevrimiçi radikalleşme üzerine bilgilendirici bir bölümle başlayacak, izleyen bölümde radikalleşme ve çevrimiçi radikalleşmeyle mücadelede çevrimiçi stratejiler üzerine bir tartışma ortaya konulacaktır. Sonuç bölümünde ise internet ve teknolojideki gelişimin radikal gruplar tarafından ne şekilde kullanılmaya devam edeceğine yönelik

bir risk değerlendirmesi yapılacaktır. Böylece çevrimiçi radikalleşme ve deradikalizasyon özelinde, radikalleşme literatürüne katkı sağlanması amaçlanmaktadır.

Dijital Kodları Okumak: Radikalleşme ve Çevrimiçi Radikalleşme

Radikalleşme bireylerin herhangi bir görüşün veya ideolojinin aşırı taraflarını benimseme yolculuğunu ifade etmektedir. Herkesin hayatın gidişatı, devlet yönetimi veya varlık nedenleriyle ilgili siyasi, felsefi veya dini düşünceleri bulunmaktadır. Hangi nitelikte ve boyutta olursa olsun bu tür düşünceler genel olarak toplum kültürüyle uyumluluk, zararsızlık ve diğer görüşlere saygılılık temelinde var olmaktadır. Fakat kimi kişiler görüşlerine ve inançlarına zamanla ve çeşitli nedenlerle öylesi bağlı (ileri seviyede bağnaz) hale gelmektedirler ki aşırı yönleri benimsemekte, yaşamlarını bu çerçevede kurmakta ve diğerlerini ötekileştirmektedirler. Radikal hale gelme süreci, zihin ve davranış temelinde ortaya çıkmaya başlamaktadır. Özellikle terörizm tartışmalarının içinde radikalleşmeye yapılan atfın giderek artması, ilgili konuda yapılan çalışmaların sayısını artırmaktadır. İdeolojilerin aşırıcı uçlarını benimseyen kişilerin zamanla geçirdikleri dönüşüm; diğerlerine karşı tahammülsüz olmaları, görüşlerini baskıyla kabul ettirmeye çalışmaları ve şiddet uygulamalarını meşrulaştırmaları ile sonuçlanmaktadır. Böylece aşırı görüşleri savunan kişiler zamanla radikal bir hayat seyrine uyum sağlamakta ve radikal gruplara yönelmektedirler. Radikalleşmenin ve şiddetin sistematik uygulanışının örgütlenmesi olan terör grupları başta olmak üzere yasa dışı gruplar, bu sürecin değerlendiricileri olmaktadırlar. Hem mevcut üyelerini hem de dışarıda hazır şekilde bulunan kişileri şiddet süreçlerinin içine dahil edecek bir ortam bulabilmektedirler (Muro, 2016; Koomen ve van der Plight, 2016, ss. 174-239).

Radikalleşme kişinin kendi kendine veya etkileşim halinde tecrübe ettiği bir süreçtir. Bu süreç bilişsel veya bilişsel-davranışsal şekilde gerçekleşebilmektedir (Macdonald ve Whittaker, 2020, ss. 35-36). Birleşmiş Milletler'e göre radikalleşme, yeni katılanların aşırı ideolojilere dayalı şiddete başvurmaya istekli bireylere dönüşmesine sıklıkla eşlik eden beyin yıkama sürecini yansıtmaktadır (2012, ss. 6-7). Radikalleşme sadece bilişsel/düşünce düzeyde kalabilmekte veya kişinin hayat seyrini değiştirebilecek şekilde etki değeri yüksek olabilmektedir. Radikal görüşler ve davranışlar kimi zaman bireysel/içe dönük bir süreç olarak yaşanırken, kimi zaman diğer görüşlere ve diğerlerine karşı şiddet hali olarak tezahür edebilmektedir (Neumann, 2013a, ss. 875-877). John Horgan çalışmasında temel bir tanımla radikalleşmeyi, aşırılaşmış bir

siyasi veya dini ideolojiye aşama aşama bağlanılan sosyal ve psikolojik bir süreç olarak tartışmaktadır (2009, s. 152). Jamie Barlett ve Carl Miller makalelerinde radikalleşmenin şiddete evrilmesinde duygusal çekim oranı, heyecan ve havalı görünme, belirli bir grup içinde statü veya saygınlık elde etme ve akran baskısı/etkisi gibi faktörleri saymışlardır (2012, ss. 13-16)

Mark Sedgwick (2010) radikalleşmenin kelime anlamı olarak tanımlaması kolay olsa da farklı yerlerde kullanılmasının belirli bir karmaşayı beraberinde getirdiğini ifade etmektedir. Güvenlik, dış politika ve entegrasyon bağlamında radikalizmin farklı anlamlar ihtiva ettiğini belirtmektedir. Güvenlik tartışmaları içinde de radikalleşmenin aşırılaşma ile çerçevesinin çizildiğini ve ılımlı olmanın zıttı bir süreç olarak gerçekleştiğini belirtmektedir. Alex Schmid ise süreç yaklaşımı ile radikalleşmenin; (1) aşırıcılığa doğru siyasi bir sosyalleşme, (2) bir rakiple karşı karşıya gelindiğinde yasadışı siyasi eylem yöntemlerinin kullanımının artması açısından çatışmanın tırmanması veya (3) manipülatif siyasi veya dini girişimciler tarafından yönetilen bir harekete geçirme ve eleman elde etme faaliyeti üzerinden tanımlanabileceğini ileri sürmektedir. Söz konusu dönüşüm sürecinde kişi birey merkezli kişisel kimlikten, gerçek inancı yaşayan üstün insanlardan oluştuğunu düşündüğü aşırıcı bir grubun taleplerine boyun eğen ve aynı zamanda onu daha özgür hale getiren yeni ve kolektif bir kimlik sahipliğine yönelebilmektedir (2016, s. 27).

Kurt Braddock radikalleşmenin; (1) kişinin kendi düşünceleri ile aşırı bir gurubunun ideolojisi arasındaki bir kimlik pazarlığı olarak, (2) bir örgütün ideolojisinin veya motivasyonel bilgisinin özümsenmesi olarak, (3) güvene dayanan normal ilişkilerden kaynaklı sosyal ağ mensubiyeti bir işlevi olarak veya (4) bir grubun düşüncelerine bağlı olarak kişinin tırmanan bir sosyal ve psikolojik değişim olarak dört farklı kategorik tanımlama içinde yer alabileceğini ifade etmektedir (2020, ss.17-33). Diğer taraftan Clark McCauley ve Sophia Moskalenko radikalleşmenin gruplar arası şiddeti ve grup içi fedakârlığı meşrulaştıran inanç, duygu ve davranış değişikliği olarak tanımlamaktadırlar. Ayrıca radikalleşme sürecinin bir siyasi görüş ve o görüşün temsilcisi grup için giderek daha fazla zaman, para ve emek vermenin ve risk almanın zemini oluşturan bir değişim olduğunu belirtmektedirler (2008, s. 416).

Radikalleşmenin temelinde etkileşim ve paylaşımın olması, bu sürecin "nerede" ve "nasıl" gerçekleştiğini daha önemli hale getirmektedir. İçinde bulunulan ortam ve bu ortamdaki çevre radikalleşme süreci üzerinde doğrudan etkilidir. Günümüzde geleneksel radikal grupların içinde ve

yüz yüze etkileşimle gerçekleşen süreçler devam ederken, internetin giderek daha çok toplumsal ilişkilerin yoğunlaştığı bir mecra haline gelmesi radikalleşmenin çevrimiçi boyutunu ön plana çıkarmaktadır. Özellikle gerçek kimlik paylaşmayı gerekli kılmayan sosyal medya platformlarında bireyler daha rahat davranabilmekte, daha açık sözlü olabilmekte ve gerçek hayatta yüksek sesle seslendiremedikleri düşünceleri aktarabilmektedirler. Söz konusu platformlarda aynı ve karşı düşüncelerin buluşmasıyla birlikte daha agresif ve toplum normlarına meydan okuyan tartışmalar ortaya çıkabilmektedir. Böylece her alandan aşırı düşünceler bireylerin önüne serilmektedir.

Jytte Klausen iletişimin örgütlenme ve örgüt stratejisi için hayati derecede önemli olduğunu ve internetin de bu ihtiyaca cevap veren önemli bir gelişme olduğunu ifade etmektedir. Merkezi olmayan, yoğun etkileşimli ve sıkı bağlantılı bu mecrada aşırıcı gruplar da eylemlerini, ideolojilerini ve etkinliklerini sahneye koyma imkânı bulmaktadırlar (2015, ss. 2-3). Çevrimiçi ortam bireylere radikalleşme öncesi araştırmalar, kendini keşfetme, daha fazla ideolojik bilgiye erişim ve hatta operasyonel eğitim gibi olanaklar sunmaktadır (Smith ve Alarid, 2020, s.186). Özellikle teknoloji çağının içine doğmuş bireyler sanal ortamda kendi içeriklerini üretme ve özel iletişim kanalları kurma şansına erişebilmektedirler. Çevrimiçi alanda daha fazla gencin bir araya gelmesi farklı fikirlerin ve ifadelerin aktarılmasını ve tartışılmasını sağlamaktadır. Bu tür yoğun etkileşim, düşünce alışverişi sağlarken çeşitli motivasyonlarla birlikte ideolojilerin daha rahat yayılmasını sağlamaktadır. Özellikle radikal düşüncelerin ve ilgili materyallerin dolaşımının rahatlığı ve sürekliliği bu noktada ayırt edici bir özellik taşımaktadır.

Bireyler internet dolaşımlarıyla sohbet odaları, sosyal medya veya web sayfaları aracılığıyla bireysel radikalleşme eğilimi gösterebilmekte veya etkileşime girdikleri kişiler aracılığıyla bir örgütlenmeye dâhil olabilmektedirler (Anderson, 2020, ss. 14-15). İnternet kullanıcıları herhangi bir grupla iletişime geçmeden bulabildikleri içeriklerle aşırılaşabildikleri gibi, buradaki etkileşim ve etkinlikler üzerinden de sürece maruz kalabilmektedir. Süreç içinde bir ideolojiye, harekete veya bir gruba aidiyet hissedebilmektedirler. Destekleyici paylaşımlar yapma, beğenilerini gösterme, finansal katkı sunma, toplantılara katılma ve diğer insanları etkileme gibi düşük düzeyde davranışlar sergileyebilmektedirler. Zamanla bu kişiler şiddeti meşru gören adımları kendileri atabilmekte veya bir grup tarafından motive edilebilmektedirler (Dauber ve İlter, 2020, ss. 48-50). Guri Molmen ve Jacob Ravndal çevrimiçi radikalleşmenin; (1) telafi etme, (2) izolasyon, (3) kolaylaştırma,

(4) hızlandırma, (5) yankı ve (6) eylemi tetikleme olmak üzere altı mekanizmasından bahsetmektedirler. Birinci süreçte bireyler gerçek hayattaki hassas noktalarını bir çevrimiçi topluluk bağlılığı oluşturarak telafi etmektedir. Böylece kendine alternatif bir dünya yaratmaktadır. İkinci süreçte toplumsal soyutlanmayla birlikte çevrimiçi hareketlilik daha da artabilmektedir. Sosyal çevresinde görüşlerinin karşılığını bulamayan kişiler çevrimiçi ortamlarda kendilerini daha rahat ifade ettiklerini düşünebilmektedirler. Kolaylaştırma, bireylerin çevrimiçi ortamda aşırıcı materyallere veya gruplara daha rahat şekilde ulaşmalarını ifade etmektedir. Normal hayat akışında bu tür buluşmalar daha yoğun bir arayış gerektirebilmektedir. Dördüncü mekanizma ise internetin radikalleştirmede bir hızlandırıcı etkisi yaratması durumudur. Geleneksel süreçten çok daha yoğun bir sürece maruz kalan bireylerin radikalleşme seviyeleri daha hızlı gelişebilmektedir. Beşinci durum aynı veya benzer görüşü paylaşan insanların girdikleri etkileşim, düşüncelerini karşılıklı olarak daha uç noktaya taşıyacakları üzerinedir. Çeşitli topluluklarda bir araya gelen insanlar ortak görüşlerini meşru hale getirme, anlamlandırma ve aşırılaştırma ile yankı odaları oluşturabilmektedirler. Son olarak ise internet üzerinden radikal bireylere iletilen mesajlar ve videolar onları siyasi şiddet içerecek şekilde harekete geçmeye yönlendirebilmektedir (2023, ss. 464-470).

Farklı hayat hikâyelerinden pek çok kullanıcıyı bir araya getiren sohbet odaları fikir alış verişi temelinde oluşturulmuş sanal toplantı alanları olarak düşünülebilmektedir. Çoğu sohbet odası ve forum sitesi profil tabanlıdır. Gerçek kimlikleriyle uyumlu profiller kullananlar olduğu kadar, tamamen sahte/yaratılmış kimliklerle var olan kişiler de mevcuttur. Kullanıcılar dini, siyasi veya başka bir konuda bilgi alabileceği veya düşüncelerini paylaşacağı kişiler aramaktadırlar. Bu noktada iletişim kuran diğer kullanıcıların gerçek profillerinin bilinmemesi, verdikleri bilgilerin ne amaçla verildiğini ve doğruluğunu tartışma altına sokmaktadır. Benzer şekilde forumlarda da kullanıcıların oluşturdukları profillerde verilen izlenim ve konularla ilgili anlattıkları elde edilebilecek tek verilerdir. Bu nedenle onların yazdıklarının doğruluğu veya uzmanlık alanıyla ilgili yazılıp yazılmadığı incelemeye açık değildir. Özellikle tartışmalı konularda kötü niyetli kişilerin oluşturdukları çoklu profiller, konunun bir yönünü öne çıkmasına neden olarak diğer kullanıcıları etkileme, onların dikkatini çekme ve yoğun iletişim kanalları kurma amacı taşımaktadır. Böylece en sert görüşlerin rahatlıkla ve farklı profiller tarafından savulduğunu gören gerçek kullanıcılar radikalleşme sürecine maruz kalmaya başlamaktadırlar (Charvat, 2010, pp. 82-83). Çeşitli sosyal paylaşım platformlarında kurulan sohbet odalarında örgütler,

üyeleri için özel ve süreli bağlantılar oluşturmaktadır. Örgüt üyeleri bu linkleri tıklayarak odaya dahil olabilmekte, süre bitiminde linkler inaktif olmaktadır. Böylece kontrollü şekilde güvenli ortamda görüşme olanaklarına sahip olabilmektedirler. Bu tür odaların kimi zaman üye listeleri bulunurken, kimi zaman da yeni kişilerin katılımına yönelik oluşturulmaktadırlar (Bloom, vd., 2019, ss. 1242-1243).

İnternetin oluşturduğu imkanlar kaçınılmaz şekilde sıradan kullanıcılar kadar yasadışı grupların da ilgisini çekmektedir ve terör örgütleri başta olmak üzere bu tür gruplar etkin bir çevrimiçi strateji izlemektedirler. Esasında zararlı amaçlar taşıyan gruplar tarafından yoğun şekilde kullanılacağı internetin daha ilk yaygınlaştığı zamanlarda ifade edilmiştir. Örneğin; Wayne Rash 1997 yılında yayımladığı kitabında politik grupların interneti örgütlenme, iletişim, kaynak toplama, eleman temini, medya faaliyetleri, uluslararası bağlantılar kurma ve çekicilik oluşturma gibi amaçlarla kullanacaklarını ifade etmiştir. Pek tabii bu genel çerçeve ilerleyen yıllarda terör gruplarının çevrimiçi faaliyetlerini açıklamada da faydalı olmuştur (ss. 176-178). Terörizm stratejisi bir siyasi amaca ulaşılma adına sistematik bir şiddet ile karşı tarafta kargaşa ve korku oluşturma üzerine kuruludur. Bu çerçevede faaliyet gösterebilecek kişilerin örgüt yapısı içinde yer almaları için siyasi amaca güçlü bir ideolojik bağ gerekmektedir. Bu bağın radikalleşen düşüncelerle oluştuğunu ifade etmek doğru olacaktır (Neumann ve Smith, 2007). Steve Furnell ve Matthew Warren ise 21. yüzyıla yaklaşılırken terör örgütü üyelerinin internet üzerinden oluşturabileceği hack saldırılarına ve propaganda, finans temini, bilgi dağıtımı ve şifrelenmiş haberleşme gibi etkinliklerine dikkat çekmişlerdir (1999, ss. 30-32). Terör örgütleri için internet; kolay erişilebilirlik, kuralların ve sansürün minimum düzeyde olması, hedef kitlenin genişliği, bilgi akışının hızlılığı, maliyetinin düşüklüğü, multimedya imkânı sunması ve geleneksel medyanın interneti temel kaynakları arasına alması gibi noktalarda oldukça yararlı bir mecra sunmaktadır (Haig ve Kovacs, 2007, ss. 660-661).

Günümüze gelen süreçte terör örgütleri yeniliklere kendilerini adapte ederek çevrimiçi ortamdaki tüm avantajlardan yararlanmaya çalışmışlardır. Daniel Koehler görüşmeler üzerinden oluşturduğu çalışmasında internetin; (1) iletişim kurmak, ağ kurmak ve toplantılar düzenlemek veya başka düzenlemeler yapmak için ucuz ve verimli bir yol ve bunun da her üyenin harekete daha iyi entegrasyon, (2) göreceli olarak kısıtlamasız bir alan ve anonimlikle birlikte bireyleri normalde çevrimdışı ortamlarda yapacaklarından daha radikal konuşmaları veya davranmaları için motivasyon, (3) yasaklanmış edebiyat, müzik, giysi

ve kitap gibi yaşam tarzıyla bağlantılı bilgileri paylaşmak için alan, (4) tartışmalara katılan potansiyel olarak sınırsız sayıda birey aracılığıyla ideolojik gelişme ve ilerleme için bir temel ve ideolojik olarak yetersiz bireylerin hızlı bir şekilde tespit edilmesi için fırsat, (5) bireylerde daha fazla dahil olma veya daha radikal davranma eğilimi oluşturabilecek güçlü bir kitle ile hareket algısı, (6) propagandanın etkileri üzerinde doğrudan düşünme ve hedef grubun talebine uyum sağlama imkanı ve (7) çeşitli yöntemlerle maddi kazanç sağlamaktadır (2014/2015, ss. 118-122). Terör örgütleri için eylemlerinde diğerlerini izleyici durumuna getirmek temel motivasyonlardan biridir. Bu şekilden propagandalarını gerçekleştirirlerken bir yandan karşı toplum üzerinde baskı ve korku yayarlarken diğer yandan sempatizan ve sempatizan potansiyeli olan kişilere mesaj vermeleri mümkün hale gelmektedir. Bunu sağlamak için medyanın gücü oldukça önemlidir. Günümüzde yeni medya ve sosyal medya bu rolün yoğunluğunu üstlenmektedir (Smelser, 2007, ss. 106-107). Yeni terörizm tartışmalarında, terör örgütlerinin çevrimiçi ortamlardaki radikalleştirme ve eleman temini, ağ kurma ve propaganda başta olmak üzere faaliyetlerinin etkisinin göz ardı edilmemesi gerekmektedir (Macdonald ve Mair, 2015).

Dijital dünya, teröristlere ucuz ve rahat iletişim, ücretsiz ve anonim web sayfaları, e-postalar ve kripto hizmetleri, sahte bloglar, sosyal ağ profilleri ve hatta zararlı oyun avatarları sağlamaktadır. Propaganda faaliyetlerinin ve toplum mühendisliğinin de bu ortamda yoğun olarak gerçekleştirildiğini ifade etmek gerekmektedir. Gençler üzerinde ciddi etki oluşturabilecek radikal fikirlerin, hedeflerin ve eylemlerin teşviki giderek yoğunlaşmakta ve teröristlerin aktif takipçileri ve sempatizanları üretilmektedir (Rusumanov, 2016, s.148). Radikalleşmenin nedenlerinin aynı zamanda terörizmin de nedenleri olması, çevrimiçi ortamdaki ilişkinin incelenmesi gerektirmektedir. Alex Schmid bu bağlamda mikro düzeyde, yani bireysel temelde kimlik sorunları, başarısız entegrasyon, yabancılaşma, marjinalleşme, ayrımcılık, göreli yoksunluk, aşağılanma, damgalanma ve reddedilme gibi durumların; orta düzeyde yani destekleyici ve suç ortağı olan geniş radikal grubun uğranılan hukuksuz durumları ileri sürerek genç kesimleri radikalleştirme ve hatta terör örgütlerinin oluşmasının önünü açmasının; makro düzeyde yani devletin ve toplumun yurtiçinde ve yurtdışındaki rolü, kamuoyunun ve parti siyasetinin radikalleşmesi, özellikle yabancı diasporalar söz konusu olduğunda gergin çoğunluk-azınlık ilişkileri ve sosyo-ekonomik fırsatlardan yoksun olmanın etkisi bazıları terörizm biçimini alabilen hoşnutsuzların harekete geçmesine yol açmasının olasılığına dikkat çekmektedir (2013).

Eklenmesi gereken diğer bir konu da terör örgütlerinin internet üzerinden oluşturdukları yazılı, işitsel ve görsellerden oluşan içeriklerin fotokopi ile çoğaltılarak, ekran görüntüleri veya metinleri paylaşılarak, harici belleklere kaydedilerek veya ağızdan ağıza söylenerek çevrimiçi ortamdan çevrimdışı ortamlara da aktarılması gerçeğidir. Böylece siber ortamdaki yayınlar veya tartışmalar, gerçek hayatın şekillendirilmesine hizmet etmekte ve radikalleşme sürecine katkı sağlamaktadır (Conway, 2012, ss. 7-8). Ayrıca terör örgütleri tarafından paylaşılan video veya ses kaydı gibi materyaller otoriteler tarafından ne kadar yasaklansa ve engellense de başka bir platformdan veya başka bir hesaptan tekrar paylaşılabilmektedir. Herhangi bir devlet sınırları içine tarafından yasaklanan materyal farklı bir yerde dolaşıma sokulabilmektedir. Bu durum da terör örgütlerinin lehine olacak bir kalıcılık oluşturmaktadır (Klausen vd., 2012).

Gabriel Weimann geleneksel iletişim araçlarının genele yayın yaptığını (broadcasting); fakat teröristlerin sosyal medya üzerinde belirli bir kitleye yayın yapabilme (narrowcasting) olanağına dikkat çekmektedir. Böylece hedef gruplara örneğin gençlere veya belirli bir ortak bağı olanlara yönelik propaganda yürütebilmektelerdir (2015, s. 182). İçinde bulunduğumuz dönemde terör örgütleri kendi kaynaklarıyla içerik üretebildikleri için interneti bir propaganda mecrası ve aracı olarak kullanmaktadırlar. Küresel düzeyde, anlık ve neredeyse maliyetsiz paylaşım yapılabilmesi bu noktada terör gruplarının ihtiyaç duydukları iletişim ve açılım kanalını oluşturmaktadır. Terör grupları hem karşı oldukları toplum üzerinde etki yaratmak hem de sempatizanlara ulaşmak için ürettikleri veya eriştikleri tüm materyalleri kullanıma açmaktadırlar (Dauber ve Robinson, 2020, ss.85-92). Terör örgütleri propagandaları ile gerçeklerden öte, hedef kitlenin algılarında ve belleğinde yer tutacak ideolojik motifleri anlatma arayışındadırlar. Böylece interneti bir iletişim kanalı olmanın yanı sıra, ikna amacıyla ortaya konulan tek yönlü bir hitap şekli olarak da düşünmek mümkündür (Payne, 2009, ss. 110-111).

Çevrimiçi ortamlar aynı zamanda terör örgütleri için materyal paylaşımı ve depolama alanı da oluşturmaktadır. Örneğin DEAŞ'ın kitleleri etkilemek için yayınladığı Dabık (Arapça), Rumiyah (İngilizce) ve Konstantiniye (Türkçe) dergileri dosya paylaşımı yapılan pek çok servis sağlayıcıya yüklenmiştir. Böylece denetime veya askıya alınmaya maruz kalsalar da örgüt üyeleri dergilerini sempatizanlara ulaştırabilmişlerdir (Macdonald vd., 2019). Diğer yönden Telegram uygulaması üzerinden söz konusu örgüt Amaq, Nashir ve Dabiq haber ajanslarıyla ilişkili olarak kurduğu kanallarda son dakika haberleri, durum raporları, analizler ve kontrol

altındaki tuttukları yerlerde yaşayanların günlük hayatlarıyla ilgili materyaller paylaşmışlardır (Bloom, vd., 2019, s.1244). Örneğin J. M. Berger ve Jonathan Morgan yaptıkları araştırmada DEAŞ'ın en güçlü olduğu dönemler arasında olan Eylül-Aralık 2014 tarihlerinde en az 46.000 (üst sayı olarak 90.000) destekleyen Twitter hesabı olduğunu ve bu hesapların ortalaması alındığında günlük 7.3 tweet atıldığını ifade etmektedirler (2015, s.9). Twitter şirketinden yapılan resmi bir açıklama, 2015 ortasından Ağustos 2016'ya kadar terörizmle ile alakalı yaklaşık 360.000 hesabın askıya alındığını duyurmuştur (Twitter Blog, 2016). Bu dönem DEAŞ'ın aynı zamanda sosyal medyada en aktif olduğu zamanlar olarak görülmektedir. Örgütün güç kaybetmesi, kaçınılmaz şekilde örgütün sosyal medya varlığını da etkilemiştir. Örneğin yine Twitter 2021 yılın ilk çeyreğinde "promotion of terrorism and violent organizations" kapsamında 44,974 hesabı askıya aldığını ve bunların %93'ünü tamamen kaldırıldığını belirtmiştir (Transparency Report, 2022).

Sosyal medya çevrimiçi radikalleşmede oldukça önemli bir ayağı oluşturmaktadır. Sosyal medyanın temel özellikleri merkesizleşmemiş ve sıkı kalıplara bağlı olmayan kişiler arası bir ağ oluşturması ve burada doğrudan sorumlu merciinin veya resmi düzenlemenin olmamasıdır. Bu durum da pek tabii terör grupları için sınırları olmayan bir paylaşım fırsatı sunmaktadır. Kişiler benzer düşünceye sahip kişilerle buluşmakta, benimsedikleri ideolojiye yakın olanlarla küresel ölçekte iletişim kurabilmekte ve aşırılaşan düşünce ve davranışlarına göre birliktelik yapabilecekleri diğerlerine ulaşabilmektedirler (Dauber ve İlter, 2020, ss. 53-54). Terör örgütü elemanlarının sosyal medya platformlarına girişi bir anda olmamıştır. İletişimlerini ve planlamalarını gerçekleştirmek için çevrimiçi ortamları kullanan gruplara karşı özellikle 11 Eylül sonrasında istihbarat ve emniyet güçlerinin gerçekleştirdikleri yoğun izleme ve önleme faaliyetleri onları giderek sayısı artan sosyal medya kullanıcıları arasına daha hızlı şekilde girmelerine neden olmuştur (Weimann, 2015, s.181). Ayrıca sahadaki etkinliklerini ve fiziksel alanlarını kaybeden örgütlerin daha yoğun şekilde internet alanlarını oluşturabilecekleri göz ardı edilmemelidir. Silahlı mücadelede kontrol etmeye çalıştığı topraklardan çekilmek zorunda kalan, finansal faaliyetlerine operasyon gerçekleştirilen ve üyelerinin aktiviteleri yoğun bir takipte olan örgütler, çevirimiçi ortamda manevra alanı elde etmeye çalışmaktadırlar. Bu eğilimi sadece DEAŞ üzerinden okumamak gerekmekte ve pragmatist örgütlerin genel bir yaklaşımı olarak ele almak doğru olacaktır (Conway vd., 2019, ss. 156-157). Telegram, Whatsapp ve Signal gibi şifrelenmiş iletişim kanallarında kurulan ve üye sayıları binleri bulan gruplarda paylaşılan materyaller, videolar ve analizler önemli bir noktayı oluşturmaktadır.

Bu tür şifreli koruma sağlanan iletişim kanallarında var olan topluluklar ve gruplar yoğun şekilde bilgi ve materyal paylaşımına, çoklu katılım içeren tartışmalara ve tek taraflı yayınlara sahne olmaktadır. Özellikle çeşitli kriz zamanlarında topluluk ve grup yöneticileri kendi yargıları çerçevesinde takipçileri bilgilendirecek, onları tartışmanın belirli bir noktasına yönlendirecek ve dışarıda kalan ilgililerin dikkatini çekecek paylaşımlar yapmaktadırlar. Böylece bir yandan takipçilerin daha fazla tepki göstermeleri, tartışmaya girmeleri ve nihayetinde yönlendirilen görüşe bağlılık göstermeleri hedeflenirken, diğer yandan benzer-yakın görüşe sahip kişiler için çekim merkezi oluşturulmaya çalışılmaktadır.

Çevrimiçi ortamların kendi kendine radikalleşmenin üzerindeki etkisi oldukça açıktır. Bireylerin kendileri gibi düşünenlerle aynı platformlarda bir arada olabilmeleri, inançlarını destekleyecek materyallere ulaşabilmeleri ve sanal olan gerçek bir toplulukla beraber hareket etmeleri bu durumun sağlayıcısıdır. Böylece giderek artan şekilde yalnız kurt eylemleri artmaktadır (Briggs, 2014, ss. 5-6). Yalnız kurtlar bir örgüte doğrudan üyelik bağı olmadan ve ideolojik bir motivasyonla bireysel terör eylemi gerçekleştiren kişilerdir. Yalnız kurtların radikalleşmesinin bireysel temelde bir dönüşüm olması farklı bir süreci tecrübe etmeleri anlamına gelmektedir. Grup içi dinamiklerden ve yüz yüze görüşmelerden ziyade, sanal sürecin sonucu olması çevrimiçi radikalleşmenin etkisinin doğrudan görünmesi açısından oldukça önemlidir. Weimann bu doğrultuda yalnız kurtların bir gruba dâhil olmamalarına rağmen, internet üzerinden yardım alabildiklerini, eğitilebildiklerini, yönlendirilebildiklerini ve radikalleştirilebildiklerini ifade etmektedir (2012, ss. 78-79).

Yalnız kurt olarak tanımlanan kişileri belirlemek veya faaliyetlerini izlemek oldukça zor bir iştir. Özellikle teknoloji ve internet imkânlarıyla ideoloji tartışmalarından bomba yapımına kadar tek başına radikalleşenlerin aktif olup olmayacakları, aktif olacaklarsa ne zaman, nerede ve ne şekilde bir eyleme kalkışacakları ciddi bir muammadır (Jurczak, Lachaz ve Nitsch, 2020). Paul Gill vd. yalnız kurtların grup etkileşiminden ve örgütlenmenin merkezinden uzak kalmaları nedeniyle daha çok çevrimiçi ortamlara ihtiyaç duyduklarını ifade etmektedirler. Bu doğrultuda iletişim ve öğrenme süreçlerinin çevrimiçi çerçevede olması yalnız kurtların radikalleşme süreçleri için oldukça önemli bir yön ifade etmektedir (2017, ss. 15-16). Yalnız kurtların tüm ihtiyaçlarına çevrimiçi ortamlarda ulaşabilmeleri ve görüşmelerini gizli şekilde gerçekleştirmeleri denetimden ve izlemeden büyük oradan kaçabilmelerini sağlamaktadır. Yalnız kurtlar özellikle DEAŞ'ın eylemlerinde uyguladıkları strateji olmuştur. Normal hayat süreçleri içinde radikal görüşlerle tanışan kişilerin, tek başlarına

gerçekleştirdikleri eylemler bu doğrultuda pek çok toplumda ciddi bir tehdit haline gelmiştir. Özellikle yaptığı paylaşımlarda DEAŞ'ın ulaşabildiği insanları kendi bulundukları ülkelerde faaliyete geçmeye yönlendirmesi ve örgüt ile doğrudan bağlantısı olmasa da sosyal medya içeriklerinden etkilenen radikal bireylerin şiddet uygulamayı hak görmeleri bu noktada dikkat edilmesi gereken yönlerdir.

Bölümü sonlandırırken Ali Dizboni ve Christian Leuprecht'in çalışmalarının girişinde internet ile radikalleşme arasındaki ilişkiye yönelik temel üç uzman yaklaşımı olduğunu belirttiklerini eklemek gerekmektedir. Gerçek hayattaki faktörlerin sanal olanlardan daha etkili olması sebebiyle ilişkiyi zayıf bulanlar, her ne kadar çok ayrıntılı veriler olmasa da aradaki bağlantının oldukça güçlü olduğunu düşüneneler, radikalleşmenin ancak siber ve fiziksel dünyaların bir etkileşimi ile kişilerin geçirdiği bir süreç olduğunu ileri sürenler bu grupları oluşturmaktadır (2020, ss. 373-374). Her ne kadar çevrimiçi alanın radikalleşmenin son derece önemli bir boyutu olduğu genel kabul görse de internet etkileşiminin radikalleşme üzerinde doğrudan etkisinin olmadığı veya sınırlı oranda etkisinin olduğu alanda tartışılmaktadır. Bu noktada belirtmek gerekir ki bilgisayarları başında aşırı düşüncelere destek veren kişilerin bunu geçici bir heves olarak görebildikleri, gerçek hayattaki şiddet eylemlerine doğrudan bulaşma olasılıklarını hesaplamanın oldukça zor olduğu, aşırı düşüncelerin tartışılmasının kişilerin öfkelerinin azalmasına hizmet edebileceği, radikal içeriklerin erişimine açık olmasına rağmen tüm internet kullanıcılarının radikal eylemlere başvurma noktasında güdülenmesi sonucunun ortaya çıkmadığı gibi öneriler mevcuttur (Archetti, 2015; Conway, 2017; von Behr vd., 2013).

Çevrimiçi Radikalleşme Karşısında Çevrimiçi Mücadele

Irkçılık, ideolojik fanatizm ve dini bağnazlık gibi artan radikal düşünceler ve radikalleşme-terörizm ilişkisi günümüz güvenlik tartışmalarında ön sıralarda yer almaktadır. Özellikle El-Kaide ve DEAŞ gibi terör örgütlerinin belirli dönemlerde bölgesel ve uluslararası toplum için ciddi bir tehdit haline gelmesi, Avrupa'da yükselen göçmen ve yabancı karşıtlığına yönelik akımlar ve aşırıcı motivasyonlarla hareket eden grupların toplumsal suç olaylarına daha çok karışmaları radikalleşmenin önlenmesine ve ilgili mücadeleye yönelik gerekliliği de artırmıştır.

Radikalleşme ile mücadele geniş bir perspektifle incelenmesi gereken bir uğraştır. Bu doğrultuda uygulanan politikaların, tasarlanan stratejilerin ve iyileştirme programlarının; radikalleşmenin boyutu/derecesi, türü, radikal grubun/bireyin süreci ve özellikleri gibi unsurlar bağlamında

oluşturulması gerekmektedir. Mücadele kapsamında önleme, koruma, cezalandırma ve rehabilitasyon gibi uygulamalar mevcuttur. Ortaya konulan mücadele radikal grupların dağıtılması, şiddet eylemlerinin önüne geçilmesi, radikal düşüncelerin yayılmasının önlenmesi ve radikalleşme sürecinde olan/radikalleşen bireylerin aşırıcı görüşlerinden vazgeçmelerinin sağlanması üzerine kuruludur.

Çevrimiçi radikalleşmeyle mücadele, genel radikalleşme mücadelesi içinde giderek daha önemli bir alanı oluşturmaktadır. İnternetin sunduğu olanaklarının ve kullanıcı sayısının şaşırtıcı şekilde artması, radikal grupların ve düşüncelerin çevrimiçi ortamlardaki etkilerinin de bu doğrultuda yoğunlaşmasını beraberinde getirmiştir. Terörizmle ve radikalleşmeyle mücadelede çevrimiçi alanda ortaya konulan çabanın gerekliliği aşikârdır. Bu noktada tartışılması gereken, çevrimiçi radikalleşme ile mücadelede çevrimiçi bir anlayışın geliştirilmesi gerektiğidir. Çevrimiçi radikalleşmeyle mücadele etmek ve bu mecrada radikalleşme eğilimi gösteren kişilerin süreçlerini tersine döndürmek için internet platformlarının, kullanıcı eğilimlerinin, paylaşılan içeriklerin ve genel avantaj-dezavantajların bilinmesi gerekmektedir.

Gerçek ya da sanal olsun sosyal çevre radikal görüşleri ve şiddet içeren aşırıcılığı tetikleyebildiği gibi tam tersine radikalleşmenin döndürülmesinde ve şiddet yerine farklı çözümlere gidilmesini de sağlayabilmektedir. Benzer konuları (siyasi, dini, hukuki vb.) kendilerine sorun edinen ve paylaşım içinde bulunan sosyal grup (fiziki veya çevrimiçi ortam) giderek radikal bir eğilim sergileyebilirken, uygun yönlendirme ile toplumla uyumlu bir aktivizm haline gelebilmektedir (Pilkington, 2023, ss. 2-3). Bu nedenle gerçek veya sanal dünyada dolaşımda olan ideolojilerden öte herhangi bir motivasyonla şiddet içeren veya içermeyen aşırıcı boyutlara odaklanmak faydalı olacaktır. Zira tarih boyunca her toplumda genel dışında düşüncelere sahip olan ve radikal olarak nitelenen bireyler ve gruplar var olmuştur; başarılı olan yaklaşım şiddet eşiğine erişmeden radikal olanları normale çekebilmek ve diğerlerinin radikal sürece kapılmalarını önlemeye çalışmaktadır.

Çevrimiçinin radikalleşmeyle mücadelede kullanılması için söz konusu ortamdaki hareketliliğin yakından takip edilmesi gerekmektedir. Sosyal medya paylaşımları, videolar, metin yayınları gibi içeriklerin sürekli olarak takip ve analiz edilmesi gerekmektedir. Bu durum da devletler için çok ciddi bir yükü beraberinde getirmekte ve istihbarat kurumları ve kolluk güçleri diğer kurumlar ve özel şirketlerle çalışmak zorunda kalmaktadır (Holt vd., 2015, ss. 115-117). Anlaşılmayan herhangi bir duruma karşı

mücadele etmenin imkânsız olması, sınırları ve imkânları sürekli genişlese de çevrimiçi alanın özelliklerinin anlaşılmasını zorunlu kılmaktadır. Devletler günümüzde siber savaşlara, siber suçlara ve siber terörizme karşı her türlü önlemi almaya çalıştıkları gibi çevrimiçi radikalleşmeye yönelik kapsamlı bir program geliştirmekle yükümlüdürler.

Bu noktada resmi kurumlar ile özel sektörün işbirliği içinde çalışmasında özel bir dikkat çekmek gerekmektedir. Teknoloji geliştirme, bilgi paylaşımı ve araştırma faaliyetleri için bu birliktelik oldukça önemlidir (Miller ve Stivachtis, 2020, ss. 451-453). Devletlerden gelen talepler bağlamında sosyal medya şirketlerinin nefret söylemi, aşırı düşüncelerin propagandası ve terör örgütü üyelerinin paylaşımları gibi konularda kendi ilkelerini belirlemişler ve bu doğrultuda çeşitli politikalar izlemeye başlamışlardır. Amaç, zararlı içeriklerin ve bununla ilgili hesapların kaldırılması olmuştur. Fakat internet sayfalarından ve sosyal medya platformlarından aşırı paylaşımların tamamen kaldırılması ciddi bir meydanı okumayı oluşturmaktadır. Bu nedenle çeşitli yapay zekâ uygulamaları ve özel yetişmiş personel ile filtreleme ve tespit işlemleri gerçekleştirilmektedir (Gonzales, 2022, ss.168-170). Özellikle sosyal medya istihbaratı pek çok alandaki faydasının yanı sıra, terör örgütlerinin sanal sosyal faaliyetlerinin, radikalleşme süreçlerinin ve etkileşim ortamlarının araştırılması ve anlaşılması için katkı sağlamaktadır (Oman vd., 2012, s.805). Buradaki adımlardan biri de kişisel bilgilerin toplanmasıyla birlikte çevrimiçi platformlarda varlık gösteren aşırıcı kişi ve grupların takip edilmesidir. Resmi kurumların yaptığı bu tür araştırmalar terör örgütü üyelerinin yaptıkları çevrimiçi faaliyetlerin engellenmesi için paylaşımlarının engellenmesi, hesaplarının kapatılması, IP adresleri üzerinden tespit edilmeleri ve e-posta da dâhil olmak üzere özel yazışmaların tespiti gibi noktalarda oldukça önemlidir (Balboni ve Macenaite, 2020).

Çevrimiçi ortamlarda radikal grupların hareketi ve bu bağlamdaki materyallerini yaymalarıyla ilgili Rachel Briggs; (1) sıfır toleransa ve yasal yaptırımlara dayalı sert strateji, (2) internet kullanıcıların kendilerinin mücadele ettiği ve yetkili mercilere aşırılık içeren hesapları-materyalleri rapor ettikleri yumuşak strateji ve (3) hedefi bulma, soruşturma, işleyişi durdurma ve tutuklamayı sağlayan izleme sistemine dayanan istihbarat stratejisinin olduğu ifade etmektedir. Her üç stratejinin olumlu ve olumsuz yönlerinin olduğunu belirterek devletlerin bütünleşik bir tercihte bulunduklarını ileri sürmektedir (2014, s.14). Peter Neumann çevrimiçi radikalleşmenin önlenmesi ve ilgili mücadeleyle ilgili; (1) kaynakların azaltılması, (2) talebin azaltılması ve (3) çevrimiçi içeriğin ve etkileşimin incelenmesi olmak üzere üç yöntemi tartışmaktadır. Öncelikle çevrimiçi

ortamda bulunan ve kitleleri etkileyen her türlü materyalin ortadan kaldırılmasına yönelik kısıtlamanın önemine, ikinci olarak toplumdaki bilinçlendirme ve yardım faaliyetleriyle bu tür kaynaklara erişmek isteyen insanların caydırılması ve son olarak da söz konusu içeriğin analiziyle birlikte istihbarat faaliyetlerin için önemli verilerin elde edilmesi olarak mücadelenin ana hatları ifade edilmektedir (2013b, ss. 437-453).

Karen Greenberg çalışmasında internetin şiddet içeren aşırıcılık ve radikalleşmeyle mücadele kapsamında (1) bozma (disruption), (2) yönünü değiştirme (diversion) ve (3) karşı mesaj (countermessaging) olmak üzere üç boyutta etkili şekilde kullanılabileceğini ifade etmektedir. Bozma aşamasında terör örgütlerinin faaliyetlerine yönelik doğrudan müdahale veya izleme söz konusudur. İkinci durum ise özellikle internette arayış içinde olan kişileri çeşitli olumlu içerikli sayfalara çekilmesi, alternatif bir mesaj iletilmesi ve risk altındaki kişilere yönelik sosyal faaliyetlerin ortaya konulmasını ifade etmektedir. Üçüncü olarak terörizmin ortaya koyduğu mesaj ve iddialara yönelik karşı anlatım ve karşı mesaj oluşturulması gerekmektedir. Terörizm mesajını toplumlara ilettiği ve eylemlerini insanların nezdinde meşru zemine taşıdığı sürece başarılı bir strateji olabilmektedir. Bu nedenle çevrimiçi ortamlarda resmi ve resmi olmayan kanallardan iletilen karşı mesajlar bir mücadele şekli olarak görülebilmektedir (2016, ss. 167-174). Tim Aistrope çalışmasının sonuç bölümünde çevrimiçi radikalleşmeyle mücadele çalışmalarının etkililiğinin, güvenirlilik ve bağlantılar kurma ile sağlanabileceğini ifade etmektedir. Devlet tarafından gerçekleştirilen faaliyetlerde güven sağlanamadığı takdirde, hedef kitle farklı bir algılamayla maruz kalınan durumun propaganda olduğunu hissedebilecektir. Bu nedenle topluluklarla, sivil toplum örgütleriyle ve özel teşebbüslerle işbirliği yapılmasının faydalı olacağını ileri sürmektedir (2015, s. 15).

Çevrimiçi radikalleşme ile mücadele siber güvenlik ve siber istihbarat çerçevesinde ele alınabilmektedir. Tehlikeli içeriğin ve risklerin tanımlanması, içeriklerin oluşturulmasının önlenmesi, talebin engellenmesi ve var olanların kaldırılması, radikalleşme araçları barındıran ve şiddet içeren olayları, eğilimleri ve sistemlerin takip edilmesi gibi adımlar siber mücadelenin temelini oluşturmaktadır (Blanco, Cohen ve Nitsch, 2020, s.61). Terör örgütleri başta olmak üzere yasadışı grupların çevrimiçi alandaki faaliyetlerinin temel amaçlarından biri olan eleman ve sempatizan kazanma girişimleri, tamamen yürüttükleri propaganda, materyal paylaşımı ve mesaj iletme üzerinden gerçekleşmektedir. Bu nedenle siber güvenliğine yönelik her türlü önlem, aynı zamanda radikalleşmeyle mücadelede ve radikalleşmenin tersine döndürülmesinde etkili olacaktır.

Radikalleşme sürecinde olan kişiler toplumdan izole halde yaşayabilmektedir; fakat süreçlerinde çevrimiçi faktörler olanlar mesajlarını veya tehditlerini e-postalar, forumlar veya sosyal medya gönderileriyle paylaşabilmektedirler (Dauber ve İlter, 2020, s. 50). Böylece çevrimiçi ortam radikal kişileri daha aktif olma fırsatı vermektedir. Çevrimiçi izleme ve takip olanakları şiddet eğilimi gösterebilecek radikal kişilerin belirlenmesi için oldukça önemlidir. İnternet kullanıcıların yaptıkları paylaşımlar, girdikleri tartışmalar, özel mesajlaşmaları ve takipleri-beğenileri bazen açık şekilde bazen de uzman incelemesiyle radikal eğilimler gösterip göstermediklerinin belirlenmesinde yeterli veri sağlayabilmektedir. Çevrimiçi çalışmalar radikalleşme sürecinin başındaki veya şiddet eşiğini aşmış kişilerin yetkili kurumlarca tespit edilmelerini, müdahaleyi veya farkında olmadan deradikalizasyon sürecine yönlendirilmelerini sağlamaktadır.

Terör örgütleri çevrimiçi ortamlarda ikinci bir mücadele ve etki alanı bulmuşlardır. Sahada kaybeden terör örgütleri bile siber alanı farklı bir çerçevede ele alarak faaliyetlerini kesintisiz şekilde yürütmektedirler. Farklı dillerde ve farklı platformlarda yapılan paylaşımlarla örgütler, çevrimiçi üye ve sempatizan toplayabilmektedirler. Bu nedenle terörizmle mücadele, çevrimiçi alanda da eylemlerinin etkisiz hale getirilmesine dayanmaktadır (Blanco, Cohen ve Nitsch, 2020, s. 56). Pek tabii ki internet terör örgütlerinin faaliyet gösterdikleri tek yer değildir; fakat getirdiği avantajlar her türde faaliyetlerinin gelişmesini sağlamıştır. Özellikle bilgi paylaşımı, yoğun iletişim, içerik aktarımı sempatizanlara oldukça etkili multimedya kanalları aracılığıyla gerçekleştirilmekte ve bu durum da bireyleri dinamik tutmaktadır (Conway, 2006, ss. 16-25). Laura Huey internetin ve özellikle sosyal medyanın terör grupları tarafından ideolojilerini ve eylemlerini gençlerin gözünde "havalı" göstermek için kullanıldığını belirtmektedir. Mizah ya da çeşitli ilgi çekici görseller kullanılarak yapılan paylaşımlar hedef sempatizan grubun ilgisini çekmekte ve sürecin içinde olmalarını kolaylaştırmaktadır. Bu durumla mücadele için Huey, söz konusu paylaşımların engellenmesinden öte karşı paylaşımların yapılmasını, propagandanın etkisinin azaltılmasına yönelik içerik üretilmesini ve internet izleyicisinin dikkatinin doğru yöne çekilmesini önererek bu havalı durumu tersine çevirmenin gerekliliğine vurgu yapmaktadır (2015, s. 14).

Deradikalizasyonu, radikal olarak ifade edilen değerlerle ve düşüncelerle ilişiğini kesme ile birlikte zihinsel bir değişim olarak tanımlamak mümkündür (Schmid, 2013, ss. 29-20). Elaine Pressman, deradikalizasyonun radikalleşme sürecinin tam karşıtı olduğunu ifade etmektedir. Kişilerin süreç içinde görüşlerini sorgulama, radikal düşüncelerden kopma

ve normalleşme aşamalarından geçtiği ifade edilmektedir. Kişiler ve gruplar radikal davranışların ve eylemlerin ideolojileriyle veya hayat görüşleriyle ilişkisinin kalmadığını gördüklerinde bir kopma süreci yaşanabilmektedir. Bu kopma doğrudan deradikalizasyon sürecini başlatmasa da yeniden sosyalleşme ve normalleşmeyle birlikte önemli bir adım haline gelmektedir (2009, s.21). Bu süreçte hem davranışsal hem de bilişsel olarak bir farklılaşmanın altı çizilmelidir. Kişinin davranışlarında gözlemlenen değişim ve bilişsel yenilenme radikalleşme sürecinin tersine dönmesinin anahtarlarıdır. Ayrıca bu süreç bireysel veya kolektif şekilde tecrübe edilebilmektedir (Bjorgo ve Horgan, 2009, ss. 1-6).

Omar Ashour radikalleşmenin tersine döndürülmesinde çevrimiçi stratejilerin karşı-anlatı üzerine kurulu olabileceğini ileri sürmektedir. Karşı-anlatı stratejisi mesaj, mesajcılar ve medya olmak üzere üç temel üzerine inşa edilebilmektedir. Birincisi mesajın kapsamlılığı, derinliği ve çok katmanlılığıdır. İkincisi, mesajcıların arka planı ve inanılırlığıdır. Üçüncüsü çevrimiçi medyanın kullanıldığı tanıtım ve yaymadır (2010, ss.16-18). Motivasyon, ideoloji ve toplumsal süreç etmenleri bireyin radikalleşmesinde kendi düşüncesinin anlamını artırma ve diğer görüşlere karşıtlık yaratma sonucunu doğurmaktadır. Bu noktada benzer bir şekilde sürecin tersine döndürülmesi yani deradikalizasyon gerçekleştirilebilmektedir (Kruglanski vd., 2014, ss. 74-78). Bireylerin radikalleşmesinde belirleyici olan çevrimiçi süreçlerden, etmenlerden ve etkileşimden deradikalizasyonda kullanılması olasıdır. Örneğin; çevrimiçi topluluklarda sahip olduğu/merak ettiği düşüncenin aşırı uçlarıyla tanışan birey, radikal olmayan gruplar içinde normal sürecine dönebilmektedir. Bu noktada çevrimiçi alanda faaliyet gösteren yasal ve uyumlu grupların rehabilitasyon faydasının olduğu açıktır. Bu nedenle bu tür grupların desteklenmesi, korunması ve çevrimiçi imkânlarının artırılması doğru olacaktır.

Daniel Gonzales sosyal medya platformlarındaki yasadışı içeriklerle mücadeleyle ilgili hükümetlerin uygulayabileceği politikaları üç kategoride incelemektedir. Bunlar; (1) sosyal medyanın tamamıyla tüm vatandaşlara kapatılması, (2) yetkinin ve sorumluluğun şirketlere yüklenilmesi ve (3) tüm denetim işleminin devletin geliştirdiği stratejilerle gerçekleştirilmesi olarak tanımlanmaktadır. Pek tabii tüm bu tercihlerin de güvenlik-kişisel özgürlükler bağlamında dezavantajları mevcut olacaktır (2022, ss. 170-171). İnternet çağı olarak adlandırdığımız günümüzde devletin koruma ve önleme amacıyla uygulamaya koydukları, vatandaşlar tarafından kişisel özgürlüklere ve özel hayatın gizliliğine tehdit olarak algılandığında toplumsal destekten yoksun kalmaktadır. Ayrıca sansür

ve müdahale algısı karşısında bireyler devlete karşı öfke biriktirerek daha radikal düşünceleri savunma, yasaklanan içeriklere daha çok yönelme ve bilinçsiz şekilde radikal grupların propagandasını yapma eğilimleri gösterebilmektedirler.

Radikalleşmiş bireylerin normalleşme sürecinde hapiste veya toplum içinde kontrol altında tutulmaları gerekmektedir. Bu kontrolün yasa dışı ve kişilerin rahatsız olacakları ölçüde yapılması ciddi sonuçlar oluşturacaktır. Hâlihazırda radikalleşme eğiliminde olan veya radikal düşüncelerle çeşitli şiddet olaylarına karışmış kişilerin kişisel özgürlüklerine yönelik gizli ve hukuk dışı bir denetim altında olduklarını hissetmeleri normalleşme sürecini sekteye uğratabilecek ve hatta radikalleşmenin boyutunu artırabilecektir (Bianchi, Ladu ve Bianchi, 2020). Çevrimiçi alanda bireyleri hedef almadan, mecburi bırakmadan ve özel hayatlarına müdahale etmeden sağlanabilecek deradikalizasyon programları bu nedenle oldukça önemlidir.

Radikalleşmeyle mücadelede hukuksal düzenlemelerin gerekliği, çevrimiçi radikalleşmede de değinilmesi gereken noktalardan biridir. Siber-uzayın merkezi otorite ve hukuksal çerçeve noksanlığı, bu alandaki radikal grupların faaliyetlerinin yoğun olarak gerçekleştirilmesi sorununu doğurmaktadır. Çevrimiçi ortamlardaki paylaşımların, iletişimin ve aktivitenin büyük oranda denetimden muaf olması, radikalleşme için daha fazla fırsat oluşturmaktadır. Bu nedenle ulusal ve uluslararası kapsamda çevrimiçi radikalleşmeyle mücadelede hukuksal önlem ve yaptırımların uygulanması tartışmaların esaslarından biridir. Kötü niyetli kişilerin ele geçirilmesi ve yargılanması, sıkı bir izleme ile anlık ortaya çıkan sayfa ve hesapların erişime kapatılması, radikal materyaller yayanların sosyal medya ortamından men edilmesi için ilkeler konulması ve terör örgütlerine hizmet eden çevrimiçi topluluklara caydırıcı cezalar verilmesi gibi başlıklar bu çerçevede değerlendirilebilecektir. Şüphesiz ki çevrimiçi alanda bu tür bir izleme ve denetim yapılırken, sıradan kullanıcıların kişisel hak ve özgürlüklerine müdahale edilmeyecek şekilde hassas bir yaklaşım sergilenmesi gerekliliği de göz ardı edilmemelidir.

Sonuç olarak çevrimiçi ortam, çevrimiçi radikalleşmeye karşı aşağıdaki listelendiği şekilde kullanabilmektedir:

- Radikal gruplardan ayrılmak isteyen fakat imkân ve cesaret bulamayan kişiler için resmi kanallara ulaşabilecekleri bir yol sunmaktadır.
- Radikal hale gelmiş veya süreçte olan kişilere yönelik çevrimiçi rehabilitasyon faaliyetlerinin yürütülebilmektedir.

- Herhangi bir hedef mecra veya grup olmadan genele yönelik bilgilendirme ve yönlendirme materyalleri paylaşılabilmektedir.
- Terör örgütlerinin yürüttükleri çevrimiçi propaganda ve psikolojik savaş faaliyetlerine karşı üretilen materyaller paylaşılabilmektedir.
- Herhangi bir başvuru yapmadan ve resmi süreç içine girmeden kişilerin kendi kendilerine tersine radikalleşme gerçekleştirmelerine olanak sunulabilmektedir.
- Özellikle sosyal medya platformlarında dolaşan materyallerin engellenmesi, filtrelenmesi veya zararlarının ifade edilmesiyle "genç radikalleşmesiyle" mücadele edilebilmektedir.
- Ulusal ve uluslararası alanda popülerliği/güvenirliliği/etkileyiciliği olan kişilerin sosyal medya paylaşımlarıyla radikal düşüncelerin tersine açık veya kapalı mesajlar verebilmelerinin önü açılabilmektedir.
- Yoğun çevrimiçi faaliyetleri nedeniyle yalnız kurtlar daha kolay şekilde belirlenebilmekte ve izlenebilmektedir.
- Yükselen radikal-popülist akımların kullandığı jargon ve mesajlar takip edilebilmekte ve karşı mesajlar üretilebilmektedir.

Sonuç

Terörizm mesaj iletme üzerine kurulu bir stratejidir. Terör örgütleri mesajlarını iletmek için her türlü ortamı kullanmakta ve devamlı olarak yeni yollar bulmaktadırlar. Günümüzde çevrimiçi alan terör örgütlerine her türden faaliyetleri için bir nevi güvenli alan oluştururken teknolojideki her gelişmeye de hızlıca adapte olabilmeleri konunun önemli bir noktasını oluşturmaktadır. Çalışmada boyunca bahsedildiği gibi çevrimiçi ortamlardaki etkileşim ve paylaşım imkanları bireyleri her türden fikrin tartışıldığı ve bu fikirlerin temsilciğini yapan kişilere rahatlıkla ulaşılabildiği bir çerçeve oluşturmaktadır. Diğer taraftan terör örgütleri de üyelerine, sempatizanlarına veya hedef olarak belirledikleri kitlelere doğrudan ve dolaylı yollarla ulaşma fırsatları yakalayabilmektedirler. Böylece ideolojik tartışmaların, geleneksel ortamlarda dillendirilemeyen düşüncelerin, propaganda içeren işitsel ve görsel materyallerin genele açık ve özel platformlarda dolaşımıyla birlikte radikalleşme süreci de etkilenmiş olmaktadır. Radikalleşmenin zihinsel süreci ve grupla hareket etme dinamiği çevrimiçi ortamlarda bu tür etkileşimle birlikte oluşmaya başlamaktadır.

Teknoloji alanındaki gelişmeler ve siber alanın her boyuttaki sınırlarının genişlemesi şüphesiz ki gelecekte de devam edecek bir süreçtir. Terör örgütleri, toplumların içine yerleşen radikal gruplar ve suç örgütleri amaçları çerçevesinde avantaj elde etmeye ve normal kullanıcıların süreçlerini suiistimal etmeye çalışacaklardır. Özellikle İnternet 3.0 çerçevesinde var olan ve beklenen gelişmeler ve yeni platformlar çevrimiçi imkânların farklı bir boyut alacağını göstermektedir. Metaverse, blockchain, yapay zeka, kripto ekonomi, artırılmış gerçeklik ve big data gibi getirileri sanal dünyanın geleceğimizi ciddi şekilde etkileyecek sonuçları ortaya koyacaktır. Bu çerçevede radikalleşme derecelerini, radikal grupları ve radikalleşme süreçlerini tekrar düşünmemiz gereken bir çağa adım atıldığını belirtmek gerekmektedir. Yeni dönem tecrübe edilecek dönüşüm nedeniyle siber tehditlerin, zararlı grupların çevrimiçi faaliyetlerinin ve sanal varoluşun ciddi bir yaklaşımla mercek tutulması gereken yönleri ortaya çıkacaktır.

Çevrimiçi alanın daha çok adem-i merkeziyetçi hale gelmesi, etkileşim boyutlarının ve platformlarının çeşitlenmesi, kullanıcıların kendilerini ifade edebileceği araçların çoğalması ve kurulan ilişkilerin düzeylerinin farklılaşması; radikal düşüncelerin dolaşımının ve etki güçlerinin, radikal grupların toplanma ve mesaj iletme imkanlarının, kimlik arayışında olan bireylerin aşırıcı görüşlerle tanışma ihtimallerinin ve terör örgütlerinin stratejilerini uygulayabilmek için ihtiyaç duydukları araçlara ulaşma fırsatlarının artması anlamına gelecektir. Bu çerçevede aşırılık içeren daha fazla içerik, ağ sayfası, sosyal medya hesabı, topluluk, toplantı ve tartışma görülmesi işten değildir. Böylece giderek artan sayıda kullanıcı pek çok yönden radikal akımlar tarafından kuşatılacaktır. Sanal ve gerçek dünya arasındaki sınırların giderek kalkması/muğlaklaşması çevrimiçi radikalleşme ve çevrimiçi radikalleşmeyle mücadele süreçlerini ve stratejilerini daha esnek, kapsamlı ve yenilikçi düşünmeyi zorunlu kılmaktadır.

Ek Beyan / Declaration

Makalenin tüm süreçlerinde TESAM'ın araştırma ve yayın etiği ilkelerine uygun olarak hareket edilmiştir.

Bu çalışmada herhangi bir potansiyel çıkar çatışması bulunmamaktadır.

Yazar bu çalışma için finansal destek almadığını beyan etmiştir.

In all processes of the article, TESAM's research and publication ethics

principles were followed.

There is no potential conflict of interest in this study.

The author declared that this study has received no financial support.

Kaynakça

Aistrope, T. (2015). Social media and counterterrorism strateg,. *Australian Journal of International Affairs, 70*(2) 1-17.

Anderson, R. A. (2020). Online utilization for terrorist self-radicalization purposes. İçinde J. R. Vacca (Ed.), Online terrorist propaganda, recruitment, and radicalization (ss. 3–33). CRC Press.

Archetti, C. (2015). Terrorism, communication and new media: Explaining radicalization in the digital age. *Perspectives on Terrorism*, *9*(1), 49-59.

Ashour, O. (2010). Online de-radicalization? Countering violent extremist narratives: Message, messenger and media. *Perspectives on Terrorism*, *4*(6), 15-19.

Balboni, P. ve Macenaite, M. (2020). The relationship between personal data protection and use of information to fight online terrorist propaganda, recruitment, and radicalization. İçinde J. R. Vacca (Ed.), Online terrorist propaganda, recruitment, and radicalization (ss. 239-266). CRC Press.

Barlett, J. ve Miller, C. (2012). The edge of violance: Towards telling the difference between violent and non-violent radicalization. *Terrorism and Political Violence*, 24, 1-21.

Berger, J. M. ve Morgan, J. (2015). The ISIS Twitter census: Defining and describing the population of the ISIS supporters on Twitter. *Analysis Paper, No: 20*, Center for Middle East Policy at Brookings.

Bianchi, S., Ladu, M. ve Bianchi, S. (2020). Radicalisation: No prevention without 'juridicalisation', B. Akhgar vd. (Ed.), Investigating Radicalization Trends: Cases Studies in Europe and Asia (ss. 123-178), Springer International Publisher.

Bjorgo, T. ve Horgan, J. (2009). Introduction. İçinde T. Bjorge ve J. Horgan (Ed.), Leaving terrorism behind: Individual and collective disengagement.

Routledge.

Blanco, J. M., Cohen, J. ve Nitsch, H. (2020). Cyber intelligence against radicalization and violent extremism. B. Akhgar vd. (Ed.), *Investigating Radicalization Trends: Cases Studies in Europe and Asia* (ss. 55-81), Springer International Publisher.

Bloom, M. vd. (2019). Navigating ISIS's preferred platform: Telegram. *Terrorism and Political Violence*, *31*(6), 1242-1254.

Braddock, K. (2020). Weaponized words: The strategic role of persuasion in violent radicalization and counter-radicalization. Cambridge University Press.

Briggs, R. (2014). Radicalisation: The role of the internet. Policy Brief, Institute for Strategic Dialogue.

Charvat, J. (2010). Radicalization on the internet. Defence Against Terrorism Review- *DATR, 3*(2), 75-86.

Conway, M. (2006). Terrorists 'use' of the internet and fighting back. *Information and Security*, *19*, 9-30.

Conway, M. (2012). From al-Zarqawi to al-Awlaki: The emregence and development of an online radical milieu. *Combating Terrorism Exchange*, *2*(4), 1-10.

Conway, M. (2017). Determining the role of the internet in violent extremisim and terrorism: Six suggestions for progressing research. *Studies in Conflict and Terrorism*, *40*(1), 77-98.

Conway, M. vd. (2019). Distrupting DAESH: Measuring takedown of online terrorist material and its impacts. *Studies in Coflict&Terrorism*, *42*(1-2), 141-160.

Dauber, C. E. ve Ilter, K. (2020). The relationship between social media and radicalization. İçinde J. R. Vacca (Ed.), Online terrorist propaganda, recruitment, and radicalization (ss. 46-63). CRC Press.

Dauber, C. E. ve Robinson, M. D. (2020). How homegrown violent extremism will likely continue to evolve as a significant threat. İçinde J. R. Vacca (Ed.), Online terrorist propaganda, recruitment, and radicalization (ss. 81-102). CRC Press.

Dizboni, A. ve Leuprecht, C. (2020). Instruments and arrangements

against online terrorism relating to international cooperation. İçinde J.R. Vacca (Ed.), Online terrorist propaganda, recruitment, and radicalization (ss. 373-387). CRC Press.

Furnell, S. M. ve Warren, M. J. (1999). Computer hacking and cyber terrorism: the real threats in the new millennium? *Computers&Security*, *18* (1), 28-34.

Gill, P. vd. (2017). Terrorist use of the internet by the numbers: Quantifying behaviors, patterns, and processes. *Criminology&Public Policy*, *16*(1), 99-117.

Gonzales, D. (2022). Its getting harder to do: Countering terrosit use of the internet. İçinde K. Larers ve T. Hos (Ed.), Terrorism and Transatlantic Relations: Threats and Challanges (ss.165-190), Palgrave Macmillian.

Greenberg, K. J. (2016). Counter-radicalization via internet. *The Annals of the American Academy of Political and Social Science*, *668*, 165-179.

Mølmen, G. N. ve Ravndal, J. A. (2021). Mechanisms of online radicalisation: How the internet affects the radicalisation of extreme-right lone actor terrorists. *Behavioral Sciences of Terrorism and Political Aggression,* 1-25.

Haig, Z. ve Kovacs, L. (2007). New way of terrorism: Internet and cyber terrorism. *AARMS, 6*(4), 659-671.

Holt, T. vd. (2015). Political radicalization on the internet: Extremist content, government control, and the power of victim and jihad videos. *Dynamics of Asymmetric Conflict*, *8*(2), 107-120.

Horgan, J. (2009). Walking away from terrorism: Accounts of disengagement from radical and extremist movements. Routledge.

Huey, L. (2015). This is not your mother's terrorism: Social media, online radicalization and the practice of political jamming. *Journal of Terrorism Research*, *6*(2), 1-16.

Jurczak, J., Lachacz, T. ve Nitsch, H. (2020). The so-called "lone-wolf" phenomenon. İçinde B. Akhgar vd. (Ed.), Investigating Radicalization Trends: Cases Studies in Europe and Asia (ss. 39-53), Springer International Publisher.

Klausen, J. (2015). Tweeting the jihad: Social media networks of western foreign fighters in Syria and Iraq. *Studies in Conflict&Terrorism*, *38*(1), 1-22.

Klausen, J. vd. (2012). The youtube jihadists: A social network analysis

of Al-Muhajiroun's propoganda campaign. *Perspectives on Terrorism*, *6*(1), 36-53.

Koehler, D. (2014/2015). The radical online: Individual radicalization processes and role of the internet. *Journal for Deredacalization*, *1*, 116-134.

Koomen, W. ve van der Plight, J. (2016). The psychology of radicalization and terrorism. Routledge.

Kruglanski, A. W. vd. (2014). The psychology of radicalization and deradicalization: How significance quest impacts violent extremism. *Advances in Political Psychology*, *35*(1), 69-93.

Macdonald, S. vd. (2019). Deash, Twitter and the social media ecosystem: A study of outlinks contained in tweets mentioning Rumiyan. *The RUSI Journal*, *164*(4), 60-72.

Macdonald, S. ve Mair, D. (2015). Terrorism online: A new strategic environment. İçinde L. Jarvis, S. Macdonald ve T. M. Chen (Ed.), Terrorism online: Politics, law and technology. Routledge.

Macdonald, S. ve Whittake, J. (2020). Online radicalization: Contested words and conceptual clarity, İçinde J. R. Vacca (Ed.), Online terrorist propaganda, recruitment, and radicalization (ss. 33-46). CRC Press.

Mccauley, C ve Moskalenko, S. (2008). Mechanism of political radicalization: Pathways towards terrorism. *Terrorism and Political Violance*, *20*(3), 415-433.

Miller, A. ve Stivachtis, Y. A. (2020**).** Public–private partnerships and the private sector's role in countering the use of the internet for terrorist purposes. İçinde J. R. Vacca (Ed.), Online terrorist propaganda, recruitment, and radicalization (ss. 443-456). CRC Press.

Molmen, G. N. ve Ravndal, J. A. (2021). Mechanism of online radicalisation: How the internet affects the radicalization of extreme-right lone actor terrorists. *Behavioral Sciences of Terrorism and Political Aggression*, *15*(4), 463-487.

Muro, D. (2016). What does radicalization look like: Four visualisations of socialisation into violent extremisim. *Notes Internacionals CIDOB*, *163*, 1-5.

Neumann, P. R. (2013a). The trouble with radicalization. *International Affairs*, *89*(4), 873-893.

Neumann, P. R. (2013b). Options and strategies for countering online

radicalization in the United States. *Studies in Conflict&Terrorism*, *36*(6), 431-459.

Neumann, P. R. ve Smith, M.L.R. (2007). The strategy of terrorism: How it works, and why it fails. Routledge.

Oman, S. D. (2012). Introducing social media intelligence (SOCMINT). *Intelligence and National Security*, *27*(6), 801-823.

Payne, K. (2009). Winning the battle of ideas: Propaganda, ideology, and terror. *Studies in Conflict and Terrorism*, *32*(2), 109-128.

Pilkington, H. (2023). Radicalization as and in process: Tracing journeys through an "extreme-right" milieu. Studies in Conflict&Terrorism.

Pressman, D. E. (2009). Risk assessment decisions for violent political extremism. Public Safety, Canada.

Rash, W. (1997). Politics on the net: wiring the political process. W. H. Freeman.

Rusumanov, V. (2016). The use of internet by terrorist organization. *Information and Security: An International Journal*, *34*(2), 137-150.

Schmid, A. P. (2013). Radicalisation, de-radicalisation, counter-radicalisation: A conceptual discussion and literature review. ICCT Research Paper, The Hague.

Schmid, A. P. (2016). Research on Radicalisation: Topics and themes. *Perspectives on Terrorism. 10*(3), 26-32.

Sedgwick, M. (2010). The concept of radicalization as a source of confusion. *Terrorism and Political Violance*, *22*(4), 479-494.

Smelser, N. J. (2007). The faces of terrorism: Social and psychological dimensions. Princeton University Press.

Smith, J. M. ve Alarid, M. (2020). Terrorism recruitment and radicalization into 21st century. İçinde J. R. Vacca (Ed.), Online terrorist propaganda, recruitment, and radicalization (ss. 179-195). CRC Press.

Twitter, (18 August 2016). An update on our efforts to combat violent extremisim, Twitter Blog, Access date: 20.12.2022 , https://blog.twitter.com/en_us/a/2016/an-update-on-our-efforts-to-combat-violent-extremism.

Twitter, (25 January 2022), An update to the Twitter transparancy

center, Access date: 20.12.2022, https://blog.twitter.com/en_us/topics/company/2021/transparency-19.

United Nations (2012). The use of the internet for terrorist purposes. United Nations Office on Drugs and Crime, United Nations Office at Vienna.

Von Behr, I. vd. (2013). Radicalization in digital era: The use of internet in 15 case of terrorism and extremism. RAND Europe.

Weimann, G. (2012), Lone wolfs in cyberspace. *Journal of Terrorism Research*, *3*(2), 75-90.

Weimann, G. (2015). Terrorist migration to social media. *Georgetown Journal of International Affairs*, *16*(1), 180-187.