Güvenlik Çalışmaları Dergisi

ISSN: 2148-6166
Yıl: 22, Cilt: 22, Sayı: 1, Haziran 2020, s. 66-88, Makale Türü: Araştırma
Makalenin Geliş Tarihi: 01/03/2020 Makalenin Kabul Tarihi: 19/05/2020

Anonimlik ile İllegalite Arasında: Deep Web, Dark Web ve Devlet Dışı Silahlı Aktörlerin Uluslararası Siber Faaliyetleri

Göktuğ Sönmez[*]
Emine Çelik[**]

Öz: İletişim devrimiyle birlikte günlük hayatın bir parçası haline dönüşen internet, sağladığı pek çok avantajla birlikte güvenlik eksenli önemli endişelere de yol açmaktadır. Bu anlamda yüzey internetinin ötesinde Deep Web ve onun bir parçası olan Dark Web platformları ve bunlara erişim sağlayan Tor, I2P ve FreeNet gibi yapılar, üzerinde dikkatle çalışılması gereken unsurlar olarak öne çıkmaktadır. Zira 1990'lardan itibaren devlet dışı silahlı aktörlerin ve bir alt sınıflandırılması olarak terör yapılanmalarının bu platformlar üzerinden savaşçı/militan devşirme, operasyon planlama, kaynak sağlama, haberleşme ve 'uzaktan eğitim' gibi fonksiyonları icra etmektedir. Bu çalışmada temel olarak ikincil kaynaklar ve ağırlıklı olarak vak'a analizleri üzerinde odaklanılmıştır. Elde edilen veriler ışığında bahsi geçen kavramlara ışık tutulacak, devlet-dışı silahlı aktörlerin bunları kullanımına dair örnekler ve temel araçlardan bahsedilecek, nihayeten de bu çerçeveye binaen bazı mevcut mücadele araçlarına ve atılması gereken adımlara değinilecektir.

Anahtar Kelimeler: Deep Web, Dark Web, Yüzey İnternet, Tor, Siber Güvenlik

[*] Dr. Öğr. Üyesi, Necmettin Erbakan Üniversitesi, Uluslararası İlişkiler Bölümü, goktugsonmez@gmail.com, ORCID: 0000-0001-5067-4693

[**] Doktora Adayı, Necmettin Erbakan Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, eminegvenilir@gmail.com, ORCID: 0000-0001-9793-2143

Journal of Security Studies

ISSN: 2148-6166
Year: 22, Volume: 22, Issue: 1, June 2020, p. 66-88, Article Type: Research
Received Date: 01/03/2020 Accepted Date: 19/05/2020

Between Anonimity and Illegality:Depp Web, Dark Web and International Cyber Activities of Non-State Actors

Göktuğ Sönmez
Emine Çelik

Abstract: As a result of the information and communication revolution, the Internet has become a part of daily life. Alongside the many advantages it provide, it also raises important concerns with respect to security. In this sence, Deep Web and Dark Web platforms, beneath the surface of the Internet and Tor, I2P and FreeNet, which provide access to these layers of cyber world, are some key components that should be studied. Since the 1990's, non-state armed actors (NSAAs) and terrorist organizations as a subclass of NSAAs, utilize the cyber arena for many purposes such as rucruitment, operation planning, fundraising, intra-group communication and "distance education". This study mainly focuses on secondary sources and case studies. In the light of the data obtained, it is aimed to shed light on the key concepts mentioned above and touch upon the examples and basic tools of non-state armed actors. Finally, some of the existing means of the fight against illegal use of the information and communication technologies (ICT) and further steps need to be taken will be discussed.

Keywords: Deep Web, Dark Web, Surface Web, Tor, Cyber Security

Giriş

İnternet kavramı Amerika Birleşik Devletleri (ABD) ordusunun geliştirme kolu olan "İleri Araştırma Projeleri Ajansı" tarafından 1960'ların sonlarında yürütülen ve desteklenen küçük bir bilim projesi olarak hayatımıza girmiş (Bartlett, 2016, s.15) ve günümüz dünyasında yaşamımızın her anında kullandığımız vazgeçilmez bir nesne olmuştur. Dünyada 4 milyardan fazla internet kullanıcısı, yüzey internetinde tarayıcılardaki spider[1](örümcek) yazılımlarının indekslemesi[2] sonucunda bulunan 2 milyara yakın web sitesi, günlük 206 milyara yakın e-posta gönderimi, atılan 600 milyon Tweet, 5,5 milyara yakın YouTube videosu, aktif olarak 2,5 milyar Facebook ve 343 milyon Twitter kullanıcısı bulunmaktadır (http://www.internetlivestats.com, 2020). Bu bağlamda da internetin 21. yüzyıldaki öğrenme, örgütlenme ve sosyalleşme alanlarında çığır açan bir buluş olduğu ifade edilebilir. İnternetin dünyada giderek artan bir nüfus tarafından kullanıldığı bilinmektedir. Bu kapsamda internet, bireyler, şirketler, devletler ve devlet dışı aktörler için de hayati önem arz eden bir yapı teşkil etmektedir. Buna mukabil, askeri olarak siber alan kara, deniz, hava ve uzayın arkasından 5. mücadele alanı ya da cephe olarak nitelenmektedir. Bu gelişen tehdit algısı neticesinde, örneğin ABD Savunma Bakanlığı, 2013 yılı itibariyle mevcut Siber Komutanlığı'nı yaklaşık 5 kat büyüterek 5000 personel ve sivilden müteşekkil hale getirmiştir (Nakashima, 2013).

Son 20 yılda yapılan araştırmalar ise internetin iki ayrı yüzeyinin olduğunu göstermektedir. Yüzey interneti ya da üst katman olarak isimlendirilen kısımda Yahoo, Internet Explorer, Chrome gibi sıradan browserlar(tarayıcılar) ile aramalar yapıp web tarayıcısı ile bilinen bir internet sitesine -Facebook, Twitter, YouTube vb. siteler- erişim sağlanabilmektedir. İnternetin ikinci kısmı olarak isimlendirilen Deep Web (Derin İnternet) ve onun karanlık yüzü olarak betimlenen Dark Web'e (Karanlık İnternet) ise sıradan browserlar ile – Yahoo Search, Internet Explorer, Crome vb...-erişim sağlanamazken Deep Web ve Dark Web'de barındırılan internet siteleri, yüzey internetinde kullanılan Google, Yahoo Search, Baidu, Bing gibi arama motorları tarafından indekslenmemektedirler.

[1] *Spider*; Arama motorları (*Google, Yahoo, etc*.) için web sitelerini dolaşıp, indeksleyen bu yüzdende örümcek adı verilen bir yazılım programıdır. Bu yazılımlar sürekli web içerisinde gezinerek yeni eklenen web sitelerini ve web sitesi içerisinde yer alan verileri indekslerler. Örneğin bir web sitesi içerisinde 30'un üzerinde farklı bağlantı söz konusu olabilir *Spider* yazılımları bu bağlantılarının her birine giden yolu işaretleyerek ilgili verileri hafızasına, daha sonrasında ise arama motorlarına aktarır. Böylelikle web siteleri üzerine işlenen verilerin yolları arama motorlarına da işlenmiş olur. Web sitelerinde bağlantıların sinir ağlarındaki yapılar gibi iç içe geçmiş olması örümcekler tarafından hafızaya alınır ve ilk olarak dizini alınan sayfaya dönülmesini sağlar. Sonuç olarak da gelen sayfanın indekslenen linkleri ne kadar fazla ise arama motorlarındaki sonuçlar da o kadar yüksek sıralarda yer almaktadır. *Spider* yazılımları web sitelerini belirli aralıklarla tarayarak arama motorlarındaki dizinlerin güncel kalmasını sağlamaktadır.

[2] İndeksleme: *Spider* yazılımlar vasıtasıyla arama motorlarının (*Google, Yahoo, Bing etc*.) veri tabanlarına kayıt olunmasıdır.

Deep Web ve Dark Web'e erişim için özel olarak tasarlanmış yazılımsal araçlar kullanılmaktadır. Tor (The Onion Router), I2P (Invisible Internet Project/Görünmez İnternet Projesi) ve FreeNet en yaygın kullanılan araçlardır. Birçok ülkede kullanım alanları ve şekilleri farklılık gösterse de yüzey internetinin daha karmaşık yapısına erişim için bahsedilen araçlar hayati önem taşımaktadır. İnternete erişimin kısıtlandığı dönemlerde başta muhalifler, gazeteciler, akademisyenler ve öğrenciler gibi gruplar tarafından kullanılan bu araçlar, kimi devlet, devlet dışı aktör ve şirketler tarafından desteklenirken, yasal olmayan sanal pazarlara (Black Markets) erişimde ya da terörist gruplar tarafından anonim iletişim sağlamak adına kullanıldığındaysa yasa dışı olarak değerlendirilmektedir. Bu bağlamda da birçok ülkede Tor başta olmak üzere FreeNet ve I2P yasaklı konumda olmakla birlikte, bu araçları bilgisayarlarına indiren kişiler güvenlik birimleri tarafından takip edilmektedir.[3] Özellikle Tor tarayıcısı yasaklılarda liste başı durumundadır. Bu durumda Tor tarayıcısının Deep Web ve Dark Web'e erişimde en çok tercih edilen ve anonimliği en üst seviyede sağlayan yazılımsal araç olarak tercih edilmesinin payı yüksektir. Sürveyans[4] teriminin bir karşıtı olarak hayata geçirilen anonimlik ise kısaca kimin kim olduğunun bilinmemesi durumu manasına gelmektedir. İnternet üzerinde anonimlik; kişilerin potansiyel olarak ne yaptıklarını görme ve kimliklerine gizleme prensibi üzerine inşa edilmiştir.

Kavramsal Çerçeve; İnternet: Yüzey İnternet, Deep Web ve Dark Web

Bilişim çağının en önemli keşiflerinden olan internet, kuşkusuz insanlık tarihinde bir dönüm noktasını oluşturmuştur. İnternet içerisinde var olan bilgilere erişim, bilgilerin dağıtılması, paylaşımı gibi parametrelerin ise giderek önemi artmaktadır. İnternete erişim sağlayabilen birçok kişi Google, Yahoo Search ya da Bing gibi arama motorları sayesinde internette bulunan birçok bilgiye erişim sağladığını düşünmektedir. Oysa bilinen arama motorlarıyla erişilebilen ve "yüzey internet" ya da "üst katman" olarak isimlendirilen internet sitelerindeki bilgilerin çok daha fazlası derin internet (Deep Web) ve onun karanlık yanı olarak betimlenen karanlık internet (Dark Web) içerisinde karşımıza çıkmaktadır (Çelik, 2017, s.151).

İnternetin kendi içerisinde üç katmana ayrıldığını söylemek mümkündür; yüzey internet, derin internet (Deep Web) ve karanlık internet (Dark Web). Birçok kullanıcının erişim sağladığı yüzey internet, tüm internet içerisindeki bilgilerin yalnızca %5'lik kısmının biraz daha azını oluşturmaktadır. Kalan kısım ise Deep Web ve Dark Web içeriklerinden oluşmakta ve yüzey internetinde kullanılan arama motorları ile erişim sağlanamayan devlet ve akademik kaynaklar, yasal olan/

[3] Detaylı bilgi için bknz: Bruce Schneier, "Attacking Tor: How the NSA TargetsUsers Online Anonymity", The Guardian ,4 Ekim 2013, https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity, (Erişim Tarihi: 12.12.2019)

[4] Bir kişiyi, nesneyi veya veri grubunu sürekli ve sistematik olarak gözlemleme akabinde de kişi, nesne veya veri grubunu analiz etme üzerine dayanan sistem, *surveillance*.

olmayan belgeler, yasadışı pazarlar, tıbbi kayıtlar gibi bilgileri barındırmaktadır (Santos, 2017).

İçerisinde barındırdığı bilgiler, sıradan browserlar ile erişimin sağlanamaması, yüzey internetinde kullanılan arama motorlarıyla indekslenememesi ve sıradan insanların kullanmadığı Deep Web ve Dark Web kavramları son dönemlerde Bitcoin başta olmak üzere dijital paranın da aktif şekilde fiziksel dünyada kendine yer bulmasıyla giderek daha popüler hale gelmiştir. Son dönemlerde Microsoft, Dell, Steam gibi büyük firmalar Bitcoin ile çevrimiçi alışverişe onay vermektedirler (https://financialanalystinsider.com/use-cryptocurrency-real-world, 2018). Bu şirketlerin yanı sıra uluslararası sistemde birden fazla borsada işlem gören dijital paralar daha fazla insana ulaşmıştır (Peaster, 2019).

Bir diğer taraftan ise Deep Web ve Dark Web'teki iletişim trafiği yasal olmayan birçok metanın alım satımının gerçekleştiği bir alana doğru da evirilmiştir. Özellikle terör örgütlerinin de anonimliği kullanarak bu alışverişe dahil olması, uluslararası platformda devletler, devlet dışı aktörler ve akademik camia tarafından da terörizmin ve terör örgütlerinin bu bağlamda yeniden tartışılmasına zemin hazırlamıştır.

En yalın haliyle tanımlaması yapıldığında, Deep Web, Invisible Web (Görünmeyen Web) gibi isimlendirmeleri olan kavram, "www" uzantısı içerisindeki standart arama motorları ile indekslenmemiş içeriklerin bulunduğu alanı ifade etmektedir (Weimann, 2016, s.40). 1990 yılında ABD'li akademisyen Michael K. Bergman "Deep Web" ifadesini kavramsallaştırmıştır. Bergman 2000 yılında internetin derinliğini ölçmek adına yapmış olduğu ölçek araştırmasının akabinde çalışanlarına Deep Web'in yüzey internetinden 2-3 kat daha büyük olduğunu belirtmiştir (Beckett, 2009). Bergman'ın ilk dönem çalışmalarından elde ettiği verilerden yola çıkarak ifade edilen bu oransal değerin ilerleyen dönemlerde çok daha fazla olduğunun anlaşıldığı da belirtilmelidir.

Bergman, 2001 yılında yayınlanan Derin Ağ: Gizli Değeri Ortaya Çıkarmak (The Deep Web: Surfacing Hidden Value) isimli makalesinde: "*Bilgi çağında en çok rağbet gören meta gerçekten bilgi ise o zaman Deep Web'in içeriğinin değeri ölçülemez. Bugün internette araştırma yapmak okyanusun yüzeyinde bir ağ sürüklemek olarak düşünülmektedir. Ağda birçok şey yakalanabilir ancak derinlerde büyük bir bilgi hazinesi var*" (Bergman, 2001, s.2) ifadelerini kullanarak Deep Web'in sürekli genişleyen yapısı hakkında bir fikir vermiştir. Nitekim Bright Planet firması ile 2000'li yılların sonlarına doğru ortaklaşa yapmış oldukları çalışma sonucunda:

- Deep Web'de (Tor ile giriş yapılarak) ulaşılabilen verilerin büyüklüğü yüzey internetinin tahmini olarak 400 ile 550 katı daha büyüklüktedir.[5]

[5] Yüzey internetin bilgilerin yalnızca %5'ini oluşturduğu ifadesi günümüzdeki güncel oran olmakla birlikte buradaki rakamsal değer Bergman ve Bright Planet firmasının 2000'li yıllarda yürütmüş oldukları ortak araştırmanın sonucu olarak ortaya çıkmıştır. Nitekim veri girişinin aktif olarak her saniye devam ettiği internet içerisinde yüzey internetinin ve *Deep Web*'in her

- Deep Web, sayısı her gün giderek artmakla birlikte "araştırma esnasında" erişilebilen 200.000'den fazla siteye sahiptir.
- Deep Web internet üzerinde bilinen en hızlı büyüyen bilgi kaynağıdır.
- Deep Web'in toplam kaliteli içeriği yani içerisinde barındırdığı geniş bilgi havuzu yüzey ağına kıyasla 1.000 ile 2.000 kat daha geniştir.
- Deep Web içerisinde içeriğin yarısından fazlası konuya özel veri tabanlarında[6] bulunur

şeklinde sonuçlara ulaşılmıştır (Bergman, 2001, s.1).

Anonimliği ve bilgi genişliği göz önüne alındığında akademisyenler, güvenlik görevlileri, gazeteciler, öğrenciler, aktivistler Deep Web'e erişmek için Tor, I2P ya da FreeNet'i kullanmaktadırlar (Lee, 2017). Tor Projesi Genel Müdürü Andrew Lewman günlük olarak 2.5 milyon insanın Tor ağını kullandığını ifade etmiştir (Kelion, 2014). Özellikle Arap Baharı sürecinde otoriter rejimlerin internet erişimini kısıtladığı ya da tamamen engellediği birçok ülkede Tor kullanımı yaygınlaşmıştır. Tunus'ta 2010 yılında 3.6 milyon kişinin internet kullandığı bilinmekle beraber Kasım 2010 yılı içerisinde Tor kullanıcısı 20-30 kişi iken iletişim gizliliğini arttırmak isteyerek Tor kullanan kişi sayısı 2011 Ocak ayının ortalarına doğru 700'e ulaşmıştır (Eriksson, 2013, s.21). Günlük Tor ağına giriş yapan kişi sayısı göz önüne alındığında rakamsal olarak bölgede Tor'un ne denli aktif kullanıldığı açıktır.

Genel olarak anonimliği sağlayan ve kullanıcıların yasa dışı faaliyetlerden uzak durarak bilgi, veri erişimi ve iletişim boyutunda kullandığı Deep Web, güvenlik açısından nispeten daha az riskli bir boyuttadır. Esas sorun teşkil eden alan ise Deep Web içerisinde yasa dışı faaliyetlerin yürütüldüğü alan olarak tasvir edilen Dark Web ile ortaya çıkmıştır. Nitekim Dark Web de tıpkı Deep Web gibi kriptografik olarak gizlenmiş siteleri destekleyen farklı bir ağdır.

Dark Web'in dünya kamuoyuyla tanışması da yasa dışı bir sanal market olan Silk Road'a (İpek Yolu) FBI'ın 2013 yılında düzenlediği operasyon neticesinde olmuştur. Dark Web'deki yasa dışı bir sanal pazar olarak belirtilen Silk Road e-Bay mantığı ile çalışmaktadır (Ball, 2013). Silk Road'un içerisinde çeşitli uyuşturucuların, yasa dışı malların ve silahların satıldığı bir alan olması ise Dark Web'in tamamen yasa dışı bir yer olduğuna dair kanıların giderek artmasına neden olmuştur. Silk Road'un operasyon öncesindeki 2 yıllık süreçte yalnızca

geçen gün giderek büyüdüğü bilinmektedir. Çalışmada ifade edilen rakamsal veriler yalnızca internetin ve *Deep Web*'in gelişimini izah etmek adına kullanılmaktadır.

[6] Veritabanı; bilgilerin ve açığa çıkan verilerin depolandığı yazılım aracıdır. Fiziksel ve sanal dünyada çalışmaları kolaylaştırmak adına her sektör içerisindeki kurum, kuruluş ve şahıslar kendi ihtiyacı doğrultusunda *SQL, Microsoft Access, MySQL, Oracle* gibi araçlarla kendi veri tabanlarını oluşturabilmektedirler. Örneğin akademide, kütüphanelerde, hastanelerde çeşitli şekillerde kullanılan veritabanları mevcuttur. Tıpkı fiziksel dünyada olduğu gibi DeepWeb'de de kişilerin aradıkları bilgi ve verilere göre veritabanları bulunmaktadır.

Bitcoin bazında 1.2 milyar dolarlık işlem hacmi oluşturduğu ve 10'dan fazla ülkede yer alan satıcıların sayısının 100 binden fazla olduğu belirlenmiştir. FBI'ın düzenlediği operasyon neticesinde Silk Road kurucusu Ross William Ulbricht tutuklanmış ve Dark Web tüm dünyanın mücadele etmek zorunda kalacağı yeni bir suç alanı olarak lanse edilmeye başlanmıştır (U.S. Department of Justice Office of Public Affairs, 2015).

Dark Web, bireylerin uyuşturucu ve ateşli silahların yanı sıra genel manada uluslararası hukukun yasakladığı birçok nesneye ulaşabileceği ve son dönemlerde de terörizm faaliyetlerine yönelik iletişim kurulması ve beşeri ve maddi kaynağa erişime imkan verebilen, Deep Web içerisinde yer alan karanlık ağ yapısını ifade etmektedir (Yang, 2019, s.2). Bununla birlikte Deep Web'in ne kadarının Dark Web içeriği barındırdığı, dolayısıyla da Deep Web'in ne kadarının yasal veya yasa dışı faaliyetler için kullanıldığı tam olarak bilinmemektedir (Finklea, 2017, s.3).

Tablo 1: *İnternetin 3 Katmanı*

	Erişim	**Erişim**	**Yasallık Durumu**
Yüzey İnternet	Yahoo!-Google-Reddit-Bing- Facebook-Twitter	Erişim Kısıtlaması Yok	Yasal
Deep Web	TOR- I2P –FreeNet	Erişim yalnızca Tor, I2P ve FreeNet üzerinden	Birçok ülkede yasal (ABD, İngiltere, Hollanda)
Dark Web	TOR- I2P –FreeNet	Erişim yalnızca Tor, I2P ve FreeNet üzerinden	Yasal Değil

Deep Web ve Dark Web'in tanımlamalarından da anlaşılacağı üzere her iki kavram arasında temelde farklılık olmadığı ifade edilebilmektedir. Deep Web ve Dark Web'in ayrımı ve işlevsel farklılıkları ise bu alanların kullanım şekillerinden kaynaklanmaktadır. Yukarıdaki tablodan da anlaşılacağı üzere kısa bir ifadeyle Deep Web "göreceli" olarak yasal bir alan, Dark Web ise yasadışı faaliyetlerin ortaya çıktığı alan olarak tasvir edilmektedir (Charlton, 2014). Ayrıca Dark Web içerisindeki yasa dışı alanlara ve sanal pazarlara tesadüfen erişimin imkansız olması da, bu ağa giriş yapan kişilerin potansiyel suçlu olduğu değerlendirmesini beraberinde getirmektedir.

Son olarak ise Deep Web ve Dark Web arasında yasal olan/olmayan ayrımının yapılamamasının, internetin küresel sistemde her ülkeye göre farklı alanlarının yasa dışı veya yasal olarak değerlendirilmesinin bir sonucu olduğunu da söylemek mümkündür. Bu bağlamda da Deep Web ve Dark Web'deki hangi sitelerin, yasal yada yasa dışı sınıflandırmasının içerisine dahil edileceği konusunda ortak bir mutabakat sağlanamadığından söz etmek mümkündür. Ayrıca Deep Web ve Dark Web'de bulunan sitelerin yüzey internetindeki gibi uzantılara sahip olma-

ması, bu nedenle de birçoğuna erişilememesinden dolayı sınıflandırma yapılmasının çok zor olduğu ifade edilmektedir (Owen ve Savage, 2015, s.4).

Anonimlik ve Şifreleme: Tor, I2P, FreeNet

Tor, ABD ordusu tarafından anonim haberleşmeyi sağlaması ve çıkan I2P ve FreeNet ise bireysel kullanımlardaki veri paylaşımlarına getirilen kısıtlamaların önüne geçmek maksadıyla tasarlanmıştır. Ancak günümüzde terör örgütlerinin teknolojik gelişmelere hızla adapte olması, bu platformların amaçları dışında kullanılmasına neden olmuştur. Anonimlik ile Dark Web'e erişim sağlayan bu platformlar terör örgütlerinin iletişim, veri paylaşımı ve yasa dışı alış-verişlerini takip edilemeden gerçekleştirmesine zemin hazırlamıştır. Tor, I2P ve FreeNet'in oluşturulma amacına bakıldığında anonimliğin ön planda olduğu anlaşılmaktadır. Anonimlik ile ilgili tüm platformların oluşturulma sürecinde gizlilik ve veri güvenliği ana çıkış noktalarını oluşturmaktadır.

Tor, I2P ve FreeNet: Erişilememezlik

Deep Web ve onun karanlık yüzü olarak isimlendirilen Dark Web'e giriş için standart tarayıcıların (Yahoo, Internet Explorer, Crome vb...) haricinde kullanılan bazı yazılımsal platformlara ihtiyaç duyulmaktadır. Yaygınlığı ve bilinirliği bağlamında ise ilk olarak karşımıza Tor, FreeNet ve I2P çıkmaktadır. İçerilerindeki ağ mimarileri bağlamında büyüklükleri ve sınırları tahmin edilemese dahi Tor'un I2P'den veri çekme, veri yükleme ve sunuculara bağlanma esnasında 1-2 saniyelik fark ile önde olduğu bilinmektedir (Moore ve Rid, 2016, s.15).

Tor

Tor başlangıçta ABD Deniz Kuvvetleri Araştırma Laboratuarı (U.S. Naval Research Laboratory) ve Free Haven Projesi ile ortaklaşa yürütülen bir çalışmada anonimliğin ön planda tutulduğu, isimsiz olarak çevrimiçi iletişim kurmanın bir aracı olarak oluşturulmuştur. 2002 yılında ise Roger Dingledine ve Nick Mathewson tarafından bağımsız (askeri olmayan) bir projeye dönüştürülmüş ve 2004 yılında da yazılım geliştiriciler için açık kaynak haline getirilmiştir (Sigalos, 2018). Tor Projesi şu anda kâr amacı gütmeyen, Tor'un sürdürülmesi ve geliştirilmesini hedefleyen bir organizasyondur. ABD hükümeti tarafından finanse edilen Tor'un İsveç hükümeti, farklı STK'lar ve bireysel sponsorlar tarafından da yardım aldığı bilinmektedir (Tiwarii, 2017). Tor'un ilk hedefi; kullanıcıların web trafiğini başka bilgisayarlar üzerinden yönlendirerek asıl kullanıcının internet ortamındaki hareketlerinin izlenememesidir (Macrina ve Phetteplace, 2015, s.18). Kısaca Tor; anonim ve şifreli bir ağ oluşturmak için tasarlanmış, (Chaabaneet vd., 2010, s.167) çevrimiçi geliştirilebilir bağımsız bir projeye dönüştürülmesinin akabindeyse anonimliği daha da arttırılarak izlenmesi imkânsızlaştırılmıştır. Dolayısıyla

Tor, internetin anonim olarak kullanılmasına izin veren bir proxy'dir[7] (ara sunucu). Böylelikle de Tor kullanan kişilerin temel konum bilgisinin, IP adresinin ve browser üzerindeki arama geçmişinin gizli kalması sağlanmaktadır. Bununla birlikte, Tor, anonimlik ağı üzerinden iletişimi yönlendirmek için e-posta, anında mesajlaşma uygulamaları (Telegram, Whatsapp, Tango vb...), cep telefonları ve daha fazlası ile birlikte kullanılabilmektedir (Macrina ve Phetteplace, 2015, s.18).

Tor'un en basit tanımı, Tor projesini ortaya çıkaranlar tarafından yapılmış, Tor, "insanların ve grupların yüzey interneti haricinde internetteki gizlilikleri ve güvenliklerini geliştirmelerine olanak sağlayan sanal tüneller ağı" şeklinde ifade edilmiştir (Tor: Overview, 2019). Geliştiricileri Dingledine ve Mathewson'da dediği gibi Tor; yönlendirmeler sayesinde internette güvenli gezinme ve mesajlaşma gibi TCP tabanlı uygulamaları anonimleştirmek için tasarlanmış bir paylaşım ağıdır (Dingledine ve Mathewson, 2014, s.1). Tor'un birden fazla isimlendirmesi olmakla birlikte en yaygın kullanım şekli; "Tor Tarayıcı", "Tor Tarayıcı Paketi" ya da kısaca "Tor" şeklindedir.

Tor, kullanıcının bir web sitesinde tanımlanmadan ve izlenmeden güvenli bir şekilde erişebilmesi adına kullanıcıyı bir dizi ara sunucuya –proxy mantığı ile aynı şekilde çalışan sunucular- yönlendirmektedir. Tor'un kendi terminolojisi içerisinde ise bu ara sunucular arasındaki gezinmeye "devreler" ismi verilmektedir (Dingledine, 2014, s.1). Tor ağı üzerinden aktarılacak olan her bilgi paketinin, görselin vb. her biri sadece sıradaki devre tarafından sonraki node/düğüm noktasında kaldırılabilecek olan birden fazla şifreleme katmanının içerisine yerleştirilir. Tor bağlantısı ile giriş yapılan Deep Web ve Dark Web'de aranılan bilgileri, sanal pazarları, siteleri bulmak ise düşünüldüğü kadar zor gözükmemektedir. Bunun temel nedeniyse; Tor ile giriş yapılan Deep Web ve Dark Web'de internetin yüzey kısmı olarak isimlendirilen kısmındaki sitelerle Deep Web ve Dark Web'deki sitelerin benzerlik göstermesidir (Çelik, 2017, s.154). Tor üzerinden giriş yapılan Deep Web ve Dark Web'te siteler arası bağlantı söz konusu değildir. Her site kendi içerisinde bağımsız ve tamamen anonimlik üzerine gizli adresler üzerinden yayınlanmaktadır.

Tor, sıkı ve katı internet sansürüne sahip toplumlarda internete serbest erişimi teşvik etmek için ücretsiz bir hizmet olarak kabul edilmiş ve baskıcı devletler tarafından yasadışı olarak kabul edilen ezberin dışına çıkılmıştır. Anonimlikten dolayı;

- Rose Topluluklar ve Çevre Vakfı (Rose Foundation for Communities and the Environment) (2017-2019)
- Mozilla (2016-2018)
- Açık Teknoloji Fonu (Open Technology Fund) (2012-2019)

[7] Proxy; tıpkı web tarayıcıları gibi gerçek sunucu ile iletişimi sağlayan sunucudur. Kişi ulaşmak istediği web sitesi için ilk olarak proxy ara sunucusuna sonrasında ise proxy sunucusu üzerinden gerçek sunucuya ulaşarak web sitesine erişim sağlar.

- SIDA- İsveç Uluslararası Kalkınma İşbirliği Ajansı (Swedish International Development CooperationAgency) (2010-2013, 2017-2020)
- The Handshake Foundation (2018)
- Princeton Üniversitesi / Ulusal Bilim Vakfı (National Science Foundation joint with Princeton University) (2012-2018)
- Minnesota Üniversitesi/ Ulusal Bilim Vakfı (National Science Foundation via University of Minnesota) (2013- 2018),
- Georgetown Üniversitesi/ Ulusal Bilim Vakfı (National Science Foundation joint with Georgetown) (2015-2019),
- Rochester Teknoloji Enstitüsü / Ulusal Bilim Vakfı (National Science Foundation joint with Rochester Institute of Technology) (2016-2019),
- Illınois Üniversitesi/ Ulusal Bilim Vakfı National Science Foundation joint with University of Illinois at Chicago (2016-2018),
- ABD Dışişleri Bakanlığı Demokrasi, İnsan Hakları ve Çalışma Bürosu (US Department of State Bureau of Democracy, Human Rights and Labor) (2013-2019)
- Harvard ABD Dışişleri Bakanlığı Demokrasi, İnsan Hakları ve Çalışma Bürosu (US Department of State Bureau of Democracy, Human Rights and Laborvia Harvard) (2017-2019)
- Pennsylvania Üniversitesi Aracılığıyla DARPA (DARPA via University of Pennsylvania) (2018- 2019)
- New York Üniversitesi Aracılığıyla Müze ve Kütüphane Hizmetleri Enstitüsü (Institute of Museumand Library Services via New York University) (2017-2020)

gibi üniversiteler, kurumlar, kuruluşlar Tor tarayıcısını savunmakta, baskıcı hükümetlere karşı muhalifler tarafından kullanımını desteklemekte ve Tor ağının gelişimi için, kodlama, ağın gelişimi, aracı proje ve finansal yardımda bulunmaktadırlar (Tor, 2019).

Tor ile giriş yapılan Deep Web, kullanıcı kimliğini koruduğu ve kişisel bilgilerini maskelediği için bireylerin (muhalifler, insan hakları aktivistleri ve gazeteciler dahil) güvenli bir şekilde bilgi aktarımı sağlaması nedeniyle tercih edilmektedir (Watson, 2012, ss.718-723). Bu kullanımın en iyi örneklerinden biri 2011 yılında Mısır'da ortaya çıkmıştır. Hüsnü Mübarek rejimin göstericileri engellemek adına internete sansür getirmesi sonucu Mısır'da birçok muhalifin, aktivistin ve gazetecinin SecureDrop[8] (açık kaynaklı yazılım) sayesinde haber merkezlerine Tor üzerinden protestolardaki bilgileri ilettiği ve yaydığı bilinmektedir (Watson, 2012,

[8] Açık kaynaklı SecureDrop'un da bir parçası olan Tor aynı zamanda AssociatedPress, Washington Post, New York Times, CBC gibi haber kuruluşları tarafından da kullanılmaktadır. Detaylı bilgi için bknz; TOR, "Normal People Use Tor", https://www.torproject.org/about/torpeople.html.en, (Erişim Tarihi: 31.12.2019).

ss.719-720). Dikkat çeken bir başka örnek ise, Suriye'de rejim karşıtı kişilerin rejimin gerçekleştirdiği işkenceler ve orantısız güç kullanımı gibi insan hakları ihlallerini Tor üzerinden Deep Web'e göndermeleri ve bunları dijital kayıt olarak uluslararası sisteme sunmalarıdır (Sec Dev Foundation, 2018).

Ayrıca Tor ağı herhangi biri tarafından trafik analizinin yapılması durumunda gizliliği arttırmak adına yaklaşık olarak her 10 dakika da bir yeni yollar oluşturabilmektedir (Core, 2018). Bir veri Tor üzerinden çıkıldığında ya da Tor ağı içerisinde internet erişimi sağlanmak istendiğinde anonimlik esaslı olarak kişiler node'lar üzerinden rastgele üç sunucuya atanmakta ve örnek olarak; Güney Afrika, New York ve sonrasında da Türkiye üzerinden çıkış sağlayabilmektedir. Böylelikle de gönderilen bilgi, veri vb. her metanın izlenen yol boyunca yakalanması ve kodunun çözülmesi (imkansız olmasa da) önemli ölçüde zor olacaktır (More ve Rid, 2016, s.16-17). Kabaca Tor ağı ile Deep Web'e ya da Dark Web'e erişilmek istenildiğinde, Tor browser, internete çıkışı birden fazla node ve ara sunucular arasında gezinerek yapmaktadır. Tor ağı sayesinde internete çıkışta ana sunucuya ulaşıldığında ise, ana sunucuda yalnızca son node verinin kaynağı olarak görülmektedir. Dolayısıyla da kullanıcının IP adresi vb ya da ana sunucuya ulaşan sunucunun kimliğini ortaya çıkarmak çok zordur.

Rakamsal olarak ifade edilecek olur ise son araştırmalarda Tor ağı 7000'den fazla aracı sunucuyla birlikte çalışmakta ve gönderilen her bir veri pakedi rastgele bu sunucuların birinden internete çıkmaktadır. Bu ifadeyi destekleyen bir açıklama olarak, Tor yöneticilerinden olan Andrew Lewman, 2014 yılında BBC'e vermiş olduğu röportajında Tor ağı'nın 6000 node'dan oluştuğunu ve 89 ülkeye yayılan bir sunucu ağı kullandığını ifade etmiştir (Kelion, 2014).

Günümüzde dünyadaki insanların birçoğunun yalnızca yüzey interneti olarak kullandığı, sonu "com", "org", "en, "tr" vs. olan adreslerin yerine Tor ile giriş yapılan Deep Web ve Dark Web'de karşılaşılan adres uzantıları "rtgfvmcadeoopp.42r5.onion" şeklindedir. URL farklılığının yanı sıra bu adresler Tor ağı içerisindeki "Gizli Servisler" tarafından belirsiz, düzensiz aralıklarla sürekli değiştirilmektedir. Ancak Deep Web ve Dark Web'deki kullanıcıların ulaşmak istedikleri sitelerin adreslerini bulabilmeleri adına, aktif olarak çalışan sitelerin indekslendiği bazı özel siteler yer almaktadır. Bilinirliği açısından en popüler olanı ise "Hidden Wiki"dir. Wikipedia mantığı ile inşa edilen site, Deep Web ve Dark Web'deki adresleri sürekli değişen siteleri indekslemektedir (Bartlett, 2016, s. 15). Hidden Wiki'nin bilinirliğinin ortaya çıkması örneğinde olduğu gibi Deep Web ve Dark Web içerisinde açığa çıkan bu tarz sitelerin konuyla ilgili çalışmalar yürüten güvenlik birimleri tarafından takip edildiği bir gerçektir. Nitekim Tor ağı tasarlanışı itibariyle yasal bir browser mantığıyla çalışmaktadır. Ancak Dark Web'e girişi mümkün kılması ve Dark Web'in içeriğindeki yasa dışı alanlarda gerçekleştirilen faaliyetler nedeniyle de son dönemlerde bazı ülkeler tarafından yasa dışı ilan edilmiştir.

I2P/ Invisible Internet Project

I2P ile ilgili çalışmalara bakıldığında da tıpkı Tor mimarisinde olduğu gibi ilk olarak karşılaşılan soru şudur: "I2P ağı ne için kullanılır?". Bu sorunun da Tor'un işlevselliğinden yola çıkarak aslında tek kısa ve net bir cevabı vardır: Anonimlik. I2P de Tor ağı mantığı ile çalışmaktadır. I2P,anonimleştirici karma bir ağ hizmet servisi olarak tanımlanmaktadır. I2P veri içeriğini gizlemek ve veri yükü teslimatını sağlamak için geniş bir şifreleme standardı kümesi kullanarak gönderenin ve alıcının kimliğini gizlemek üzere tasarlanmıştır. Tıpkı Tor gibi veri node'ları arasından verileri yönlendirerek birden fazla node içerisinden geçirme yeteneğine sahiptir (Zantout ve Haraty, 2011, s.401). Tor ile I2P mukayesesi yapıldığında, Tor'un anonimliği, yaygınlığı ve hızı neticesinde daha çok terörist gruplar, hacker'lar ve genel itibariyle sınıflandırıldığında kriminal faaliyetler yürüten kişi ve/ya gruplar tarafından tercih edildiği söylenebilmektedir.

FreeNet

Anonimlik maksadıyla kullanılan bit diğer yapı ise FreeNet'tir (Clarke, 1999). FreeNet bir proxy olmamakla birlikte dağıtılmış bir veri deposudur.[9] Google veya Facebook gibi hizmetlere doğrudan bağlanması mümkün değildir. FreeNet, yalnızca isimsiz ve içerisinde barındırılan web sitelerine, anonim kullanıcılar tarafından paylaşılmış dosyalara, forum odalarına ve e-mail yoluyla iletişim kanallarına sahiptir. Bahsi geçen veriler FreeNet'te paylaşım için dolaşıma girdiğinde FreeNet içerisinde sonsuza dek kalabilmektedir. Tüm bu özelliklerinin yanı sıra FreeNet'in "arkadaş moduna" sahip bir yapıyı içerisinde barındırması sayesinde içerisindeki node'lar ile arkadaştan arkadaşa sistem mantığıyla yalnızca tanımlanan kişiler arasında veri trafiğine node'lar üzerinden izin verir ve böylelikle de ulusal güvenlik ağında FreeNet'in engellenmesi son derece zor bir hale gelmektedir (https://www.quora.com/Is-Freenet-more-secure-and-anonymous-than-Tor, 2018). 2001 yılından itibaren sürekli geliştirilen FreeNet, Tor'un aksine internet üzerinden isimsiz bir kanal vasıtasıyla hizmet vermemekle birlikte, yalnızca kişilerin birbirilerine izin verdikleri ölçüde önceden yayınlanmış içeriklerin paylaşılmasına olanak tanımaktadır (Levine, Liberatore, Lynn ve Wright, 2017, s.1). FreeNet'in kurucuları bu durumu; "İletişim özgürlüğü demokratik toplumlarda temel bir değerdir. FreeNet azınlık dini gruplar, muhalif gruplar ya da verilerini anonimlik düzeyinde kullanmak isteyen sıradan vatandaşlar için tasarlanmıştır. Ancak günümüzde FreeNet bir terörist saldırı planlamak için kullanılabilmekte ya da teröristlerin iletişim alanı olabilmektedir" şeklinde ifade etmişlerdir (Clarke vd, 2002, s.41).

Tor mantığından erişim şekli olarak farklı olsa bile anonimliği ön planda tutan FreeNet'te de tıpkı Tor'daki gibi com, org, gov, vb. gibi standart uzantılar

[9] Tek bir sistem içerisinde sınırlı olmayan veritabanı olarak ifade edilen dağıtılmış veri deposu, birden fazla sunucuya veya farkı birden fazla yerdeki sunucuyu ifade etmektedir. Fiziksel olarak donanımları farklı yerlerde olsa bile tek bir veritabanıymış gibi çalışmaktadır.

kullanılmamaktadır. Bunun yerine yalnızca kişilerin birbirlerine iletebilecekleri, düzensiz, rastgele oluşturulmuş rakamlar ve harf dizilimlerinden oluşan adresler yoluyla iletişim sağlanabilmektedir (Çelik, 2017, s. 154).

Kurucuları tarafından FreeNet'in iki temel amaç doğrultusunda tasarlandığı öne sürülmektedir. İlk olarak demokratik olmayan hükümetlerin internet sağlayıcıları tarafından getirilen içerik kısıtlamalarını ortadan kaldırmaktır. İkinci olarak ise muhalif grupların anonim şekilde düşünce özgürlüğü çerçevesinde içerik üretmelerine uygun bir platform oluşturmaktır (Clarke vd, 2002, s.41).

İllegal Yapılar, Devlet Dışı Silahlı Aktörler ve Terör Örgütlerinin Kullanımı

Tarihteki en eski saldırı biçimlerinden olan terör eylemleri 21. yüzyılda güvenlik ve çatışma alanında yaşanan birçok parametreyle doğru orantılı olarak evrimleşmiştir. Teknolojinin ve buna entegre şekilde internetin gelişimi de terör örgütlerinin bu alanlara yoğunlaşmasına neden olmuştur. Bu bağlamda da terör örgütlerinin internet kullanımının ve siber dünyadaki etkinliklerinin giderek arttığını söylemek mümkündür.

Tarihsel olarak bakıldığında, 1990'lı yılların sonundan itibaren çevrimiçi platformlar (Weimann, 2010) terörist grupların propagandalarını geniş çevrelere yaymaları için cazip yerler olmuşlardır. Bununla birlikte yüzey ağındaki web sitelerine erişimin ve son dönemlerde sosyal medya kullanımın tüm dünyada artması ise terörist gruplar için propaganda yapmak, militan kazanmak, finansal kaynak sağlamak adına geniş iş sahalarına dönüşmüştür.

Gabriel Weimann, terör örgütlerinin ve teröristlerin yüzey internetini günlük olarak nasıl kullandıklarını şu maddeler ile sıralamıştır:

- **Veri Madenciliği**: İnternet, yapısı itibariyle dijital bir kütüphane gibidir. Teröristler interneti nükleer santraller, havaalanları, kamu kurumları gibi hedefler ile ilgili detayları bulmak ve hatta terörle mücadele önlemleri hakkında temel bilgileri araştırmak adına kullanmaktadırlar. Aslında teröristler, internet üzerinden halka açık yasal olarak erişilebilir kaynakları kullanarak saldırı için ihtiyaç duydukları bilgilere ulaşabilmektedirler.
- **Ağ Oluşturma**: 2000'li yıllarda yüzey interneti, çeşitli terörist grupların faaliyetlerini etkin bir şekilde iletmelerini ve koordine etmelerini sağlamaktadır. Yüzey interneti iletişim maliyetini düşürerek paylaşılabilecek bilginin çeşitliliğini ve karmaşıklığını arttırmaktadır.
- İşe Alma ve Seferberlik: Terör örgütlerinin insan kaynağına ihtiyacı her zaman vardır. Yüzey interneti terör örgütlerinin ideolojilerine veya kuruluş nedenine ilgi duyan veya örgüt için uygun görünen kişilerle iletişim kanalını sağlamakta bunu da sempatizanlar ve terör örgütü ile ilgili sohbet odaları arasında dolaşarak elde etmektedirler.

- **Talimatlar ve Çevrimiçi Kılavuzlar**: 2000'li yıllarda yüzey internetinde, okuyuculara kimyasal ve patlayıcı silahların nasıl oluşturulacağı gibi konuları öğreten kılavuzlar ve el kitapları mevcuttur.
- **Planlama ve Koordinasyon**: Yüzey İnterneti, belirli saldırıların planlanmasında ve koordine edilmesinde teröristler için paha biçilemez bir alan olmuştur. El Kaide terörist grubu dönemin şartlarına göre 9/11 saldırıları için internet iletişimi tercih etmişlerdir. 2000'li yıllarda örgüt içerisindeki tüm üyeler e-posta yoluyla birbirilerine mesaj gönderir saldırı ve eylemlerini koordine etmek için çevrimiçi sohbet odalarını kullanmışlardır.
- **Bağış Toplama**: Teröristler online anket ve sipariş formlarından girilen kişiler bilgilerden elde edilen demografik bilgiler kullanılarak sempatizanlarını belirliyor ve daha sonrada e-posta üzerinden bağış talep ediyorlardı (Weimann, 2010).

Yüzey ağındaki terörist faaliyetlerin terörle mücadele birimleri tarafından izlenebilir olması, ilgili web sitelerinin ve sosyal medya hesaplarının kapatılması ya da saldırıya uğraması terörist grupları yeni arayışlara yöneltmiştir (Weimann, 2018). Güvenlik birimleri tarafından gerçekleştirilen tutuklamalar terörist grupları Dark Web'e yönlendirmeye başlamıştır (Hussain ve Saltman, 2014). Özellikle IŞİD'in interneti ve Dark Web'i etkin bir şekilde kullanması daha fazla terörist grubun dikkatini Dark Web'e çekmiş ve buradaki anonimlik terörist grupların başta iletişim olmak üzere birçok faaliyetini karanlık internete taşımasını sağlamıştır. Terörist grupların yüzey internetinden farklı olarak Dark Web'e geçtiklerinde yaptıkları tüm eylemlerin basit ve yalın açıklaması ise; 'yüzey interneti ile aynı ama daha gizli' şeklinde ifade edilebilmektedir.Anonimlik esaslı faaliyetlerini yürütmeye devam eden terörist gruplar özellikle kripto para birimleri sayesinde finansal olarak takip edilememektedirler. Kripto para birimlerinin Dark Web'deki sanal pazarlarda kabul edilmesi ve Dark Web içerisinde sınırsız olarak elde edilen yasa dışı ürünler terör örgütlerini özgürleştirmiştir. Bununla birlikte kripto paralar sayesinde dünyanın herhangi bir yerindeki kişi bir terör örgütüne finansal olarak yardım edebilmektedir (Glasser, 2015).

15 Kasım 2015 Paris saldırısından sonra IŞİD, propagandalarını yürüttüğü sitesinde ".onion" uzantılı bir adrese yer vermiş ve paylaşımlarını buradan sürdüreceğini açıklamıştır. Sitede yer alan mesajın içeriğinde: "Caliphate_Publications" web sitesine uygulanan ciddi kısıtlamalar nedeniyle Dark Web'e geçiş yaptığımızı duyuruyoruz" ifadelerine yer vermiş ve ilgili adreste de çeşitli terörist materyallerin bulunduğu bir çevrimiçi kütüphane olan Chadwiki gibi bir oluşumu hayata geçirmişlerdir (Weimann, 2010).

Terör örgütlerinin ve teröristlerin Dark Web içerisindeki amaçları Moore ve Rid'e göre ikiye ayrılmaktadır:

- Halka açık faaliyetler: propaganda, militan devşirme ve paylaşım önerileri,
- Halka açık olmayan faaliyetler: İç iletişim ve komuta/kontrol (2016, s.21).

Bu grupların günlük faaliyetlerine bakıldığında ise rutinlerinin gelişimi şu şekilde olmuştur:

- **Veri Madenciliği**: Deep Web ve Dark Web'in yüzey internetinin kabaca 400-500 katı olduğu bilinmekte ve bilgi, belge, veri için devasa bir kaynak olarak değerlendirilmektedir. 2019 yılında yüzey internetindeki birçok bilginin birçok devlet tarafından yasaklanması terörist grupların işini zorlaştırmış ve ihtiyaç duydukları bilgilere kolay erişim sağlayamamışlardır ancak Dark Web üzerinde yalnızca yetkili kişilerin erişebileceği verilere kolayca ulaşabildikleri bilinmektedir.
- **Ağ Oluşturma**: Yüzey internetinde gerçekleştirilen birçok işlemin devletler ve güvenlik birimleri tarafından takip edilmesi terör örgütlerinin faaliyet alanlarını kısıtlamıştır. Ancak anonimliğin ön planda olduğu Dark Web üzerinden gerçekleştirilen iletişimlerin takip edilememesi, örgütlerin saldırı ve eylem planlarını rahatça gerçekleştirebildiklerini ortaya koymaktadır.
- **Militan Devşirmek:** Günümüzde internet üzerinde kişilerin yer tespitleri çok kolay bir şekilde gerçekleştiği için terör örgütleri yasal bir internet sitesi ya da sohbet odasından sempatizanları ile görüşememekte ancak bazı ikircikli tavırlara sahip sosyal medya üzerinden propaganda yapmaktadır. İletişim kanallarını ise daha çok Dark Web üzerinden sempatizanlarının aracılığıyla gerçekleştirdiği bilinmektedir. Konuyla ilgili Birleşmiş Milletler Siyasi İşler Genel Sekreter Yardımcısı Jeffrey Feltman Güvenlik Konseyi ile olan görüşmesinde IŞİD'in bölgedeki askeri baskılara çeşitli şekilde adapte olduğu ve iletişim ve insan devşirme konusunda Dark Web'i kullandığı yönünde bilgi vermiştir (UN News, 2017).
- **Talimatlar ve Çevrimiçi Kılavuzlar**: İnternet üzerinden kimyasal ve patlayıcı silah yapımıyla ilgili konuları öğreten kitaplar ücretsiz şekilde mevcuttur. Google üzerinden "terörizm" ve "el kitabı" anahtar kelimeleriyle yapılan bir aramada 9.210.000 sonuç bulunurken, "silah" ve "patlayıcı yapımı" anahtar kelimeleriyle yapılan bir aramada 1.480.000 sonuç bulunmaktadır. Buraya kadar erişimin kolay olduğu bu bilgilere ulaşılmak istenildiğinde ise güvenlik güçlerinin Siber Suçlar kısmında teröristlerin IP numarasını görme olasılığı çok yüksektir. Dark Web üzerinde Tor ile bu aramaları yaptıklarında ise daha kapsamlı bilgilere ulaşmakla birlikte, anonimlik sayesinde teröristlerin yakalanma olasılığı neredeyse imkansızdır.
- Son dönemlerde anonimliğin avantajlarından önemli ölçüde faydalanan başta IŞİD olmak üzere terörist gruplar Telegram gibi şifreli mobil uygulamaları örgüt üyelerine talimatlarını iletmek adına kullanmıştır. Telegram,

sıradan kullanıcılar tarafından da kullanılan bir mobil program olmakla birlikte, terör örgütleri tarafından Dark Web üzerinden kanalları dağıtılarak anonimliğin üst düzeyde sağlandığı bir uygulamaya evirilmiştir (Weiman, 2010).

- **Planlama ve Koordinasyon**: 11 Eylül sonrasında siber suçlarla mücadelenin daha ciddi ve koordineli bir şekilde gerçekleştirilmesi terör örgütlerini yeni arayışlara yöneltmiştir. Teröristler iletişimi, saldırı eylem ve planlamasını, eylemde kullanılacak maddeleri güvenlik birimleri tarafından takip edilmemek adına Dark Web üzerinden gerçekleştirmeye başlamışlardır. Nitekim 2015 yılında Paris'te İŞID tarafından gerçekleştirilen terör saldırısının DarkWeb üzerinden planlandığına dair görüşler ortaya atılmıştır (Paoli, 2018, s.2).

Planlama ve koordinasyona bir diğer çarpıcı örnek ise, 22 Temmuz 2016 tarihinde Almanya Münih'te Olympia Alışveriş Merkezinde 9 kişiyi vurduktan sonra öldürülen 18 yaşındaki David Ali Sonboly ile ilgilidir. Alman Federal Polisi tarafından sonradan ortaya çıkarılan detaylara göre yalnız kurt olarak isimlendirilen İran kökenli Sonboly işlemiş olduğu eylemde kullandığı 9 mm Glock marka silahı ve 250 mermiyi Dark Web üzerinden satın almıştır. Sonboly'nin saldırıdan önceki rutinlerini takip eden Alman Federal Polisi Dark Web'deki bir satıcı ile temasta olduğunu ve silahı da bu şekilde temin ettiğini duyurmuştur (Paoli vd, 2017, s.3).

- **Bağış Toplama**: Birçok terör örgütü grubu kendi web sitelerinin yanı sıra Twitter, Instagram, Facebook gibi sosyal medya sitelerinden yapmış olduğu propagandalar ile çeşitli faktörlere bağlı olarak –macera arayışı, etnik ve dini unsurlar, uyuşturucu, yoksulluk vb.- insanları terör örgütüne katılmaya sevk etmektedir. Bunun en çarpıcı örneklerinden biri, 2016 yılında Amerikan Tıp Derneği ile gönüllü olarak Ürdün'e giden ve IŞİD'in etkili olduğu Zataari Mülteci kampında 2 hafta kalan ABD'li 27 yaşındaki Zoobia Shahnaz'ın 2017 yılında IŞİD'e finansman sağlamak adına Dark Web'den satın aldığı Bitcoin üzerinden kara para aklaması olmuştur. Shahnaz çeşitli kredi kartlarından farklı miktarda ödemeler yaparak 62.000 $ değerinde Bitcoin satın almış, Çin, Pakistan ve Türkiye'ye deki çeşitli adreslere farklı miktarda fon olarak göndermiştir (Mangan, 2018).

Terör örgütlerinin birbirinden saha da taktiksel anlamda birçok hamleyi öğrendiği bilinmektedir. Bu öğrenme günümüzde propaganda, internet üzerindeki aktif olma gibi değişik alanlarda da kendisini göstermektedir. IŞİD'in Bitcoin ile olan ilişkisi PKK terör örgütünün Suriye'deki silahlı kanadı olan YPG tarafından da taklit edilmeye başlanmıştır. Dark Web kullanıcısı ve Bitcoin kod yazıcısı olduğu bilinen İran asıllı İngiltere vatandaşı Amir Taaki'nin[10] 2015 yılında Suriye'ye gi-

[10] Amir Taaki 2011 yılında Libbitcoin isimli Bitcoin'in çekirdek kodunu yeniden yazmış ve ortaya Dark Wallet'ı çıkarmıştır. Taaki, Silk Road'da kullanılması için tasarladığı Dark Wallet ile Bitcoin'le yasadışı alışveriş yapıldığında izlenmemesi adına bir cüzdana sahip olunmasını he-

derek YPG terör örgütü saflarına katılması ise PKK terör örgütünün Dark Web'deki etkinliğinin arttırmasına yönelik bir hamle olarak değerlendirilmektedir. Taaki, bölgede bulunan YPG'li teröristlere açık kaynaklı kod yazılımı ve Dark Web'de etkin olmaları adına eğitimler vermiştir. Ayrıca Taaki ile birlikte bölgede çalışan İspanyol bir biyolog olan Pablo Prieto, YPG'li teröristlere Dark Web'in ve Bitcoin'in önemini vurgulamış, üst düzey yöneticiler ise Taaki ve Prieto'dan YPG'li teröristler için teknoloji müfredatı hazırlamalarını istemişlerdir (Berg, 2017).

Bu örneklerden ve siber dünyada anonimliğin sağladığı avantajlardan hareketle terör örgütlerinin Dark Web'deki amaçları ve günlük rutinlerine bakıldığında, Dark Web'i ne denli etkin kullandıkları anlaşılmakta bu sahada mücadelenin terör ve terörizmle mücadele bağlamında olmazsa olmaz bir nitelik teşkil ettiği görülmektedir.

Sonuç: Yüzey İnterneti'nin Ötesi, Tehditler ve Öneriler

Terörist grupların evrimleşmesi, interneti aktif olarak kullanması ve anonim olarak Dark Web üzerinden faaliyetlerini sürdürmesi terörizm ile mücadelede yeni bir safhanın açılmasına neden olmuştur. Günümüzde Dark Web hem devlet dışı silahlı aktörler ve bir altbaşlığı olarak terörist gruplar hem de yalnız kurt olarak isimlendirilen teröristler ve tarafından sıkça kullanılmaya başlanmıştır. Bu kişiler Dark Web üzerinden başta silah ve mühimmat kaynağına ulaşmakla birlikte, saldırı planlaması, militan devşirme gibi birçok eylemi anonim olarak gerçekleştirmektedirler (Paoli, vd. 2017, s. 62).

Eski ABD başkanı Barack Obama'nın 2016 yılında Washington'da düzenlenen ve 50 ülke lideri ve dışişleri başkanlarının katıldığı Nükleer Güvenlik Zirvesi'nde Dark Web ile ilgili yapmış olduğu konuşma, tüm dünya liderlerinin dikkatini konunun hassasiyetine çekmiştir. Obama, konuşmasında, teröristlerin Dark Web üzerinden satın aldıkları radyoaktif madde ve drone ile gerçekleştirecekleri eylemin bir senaryosunu çizmiştir. Senaryoda, Obama liderlere, teröristlerin sivil bir alana yüksek oranda radyoaktif madde yaymak adına drone'lar kullandıklarını hayal etmelerini ve sonuçlarının neler olabileceğini düşünmelerini söylemiş, akabinde de takip edilemeyen Dark Web'in potansiyel bir terörist yuvası olduğundan söz etmiştir (Hutton, 2016). Bu senaryo ve terörist grupların Dark Web'deki aktifliği uluslararası sistemde Tor,I2P gibi ağları kullanarak Deep Web içerisindeki karanlık yapı olan Dark Web'e erişimini sağlayan anonimliğin yeniden sorgulanmasına neden olmuştur.

Terörist grupların ve suç örgütlerinin Dark Web üzerinden anonim iletişim sağlama, silah alışverişi, çocuk istismarı gibi eylemlerinin artması devletlerin ilgili güvenlik aygıtlarını zorlayıcı bir mücadelenin içerisine itmiştir. Dolayısıyla

deflemiş ve bunu da başarmıştır. Daha detaylı bilgi için bknz; Jen Copestake, "HiddingCurrency in the Dark Wallet", BBC, 19 Eylül 2014, https://www.bbc.com/news/technology-29283124, (Erişim Tarihi: 26.02.2020).

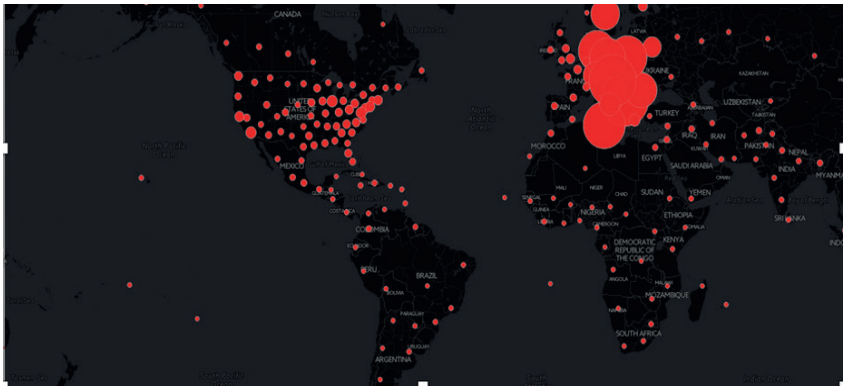
da bu grupların Dark Web üzerinde gerçekleştirmiş oldukları faaliyetleri izleyebilmek ve analiz edebilmek adına yeni yöntemler ve önlemler geliştirilmelidir (Weimann, 2018, s. 43).

2014 yılında yüzey internetindeki insan ticareti, çocuk pornosu ve uyuşturucu tacirlerini takip edebilmek adına ABD'de DARPA[11] (Defence Advanced Research Projects Agency/ Savunma İleri Araştırma Projeleri Ajansı) tarafından yeni bir proje olan MEMEX (https://worldbrain.io/, 2019) hayata geçirilmiştir. MEMEX yüzey internetindeki yasa dışı kullanıcıların izlenmesine yönelik çalışmalara odaklanmıştır. İlk dönemlerinde MEMEX'in yalnızca çocuk pornosu sitelerini, insan kaçakçılarını ve uyuşturucu tacirlerini gözetlemek adına oluşturulduğunu söylemek mümkündür (Brewster, 2018). İnsan hafızasını tamamlayacak bir analog bilgisayar olarak tasarlanan MEMEX, kullanıcıların tüm verilerini hafızasında saklayarak otomatik olarak indeksleme yapmaktadır (https://www.darpa.mil/program/memex, 2019). Bu bağlamda da açık kaynaklı kod olarak tasarlanan MEMEX'in Google'dan daha gelişmiş, daha hızlı bir arama motoru olarak görev yaptığını söylemek mümkündür.

Oluşturulma amacı insan kaçakçılığı, çocuk pornosu ve uyuşturucu tacirlerini gözetlemek olan MEMEX, yüzey internetinin yanı sıra Dark Web'de de terörist faaliyetlerin artmasının akabinde ise birkaç kod eklemesi yapılarak bu alanlarda da terör örgütlerinin takiplerinde kullanılabileceği düşünülmektedir (Weimann, 2010, s.43). MEMEX'in açık kaynaklı koda sahip olması, herkesin onu geliştirmesine katkı sağlarken, baş araştırmacısı Chris Mattmann MEMEX'i "İnsanları, yerleri ve tüm nesneler arasındaki bağlantıları anlayan yeni nesil arama teknolojisi" (Deep Web Search, May Help Scientists, NASA, 2015) olarak tanımlamaktadır. Çalışma prensibine bakıldığında; MEMEX'in yüzey internetinde var olan resim, video ve ses kayıtlarını indekslenmesinden sonra Tor üzerinden MEMEX ile Deep Web'e giriş yaparak yüzey internetindeki resim, video ve ses kayıtlarının aynısının aranması ile Deep Web'in ve Dark Web'in kısmi olarak haritası çıkarılabilmektedir. Anonimliği ortadan kaldıramasa bile atılan adımın terörist grupların Dark Web'de gelecekteki faaliyetlerini engellemek adına umut verici olduğunu söylemek mümkündür.

[11] Pentagon ile birlikte çalışan ve yeni teknolojiler üretmekle görevli ABD'nin Savunma Bakanlığına bağlı bir ajanstır.

Şekil 1. *Dark Web'deki yasadışı ürünler ile ilgili sıcaklık analizi sonucunda MEMEX'in çıkarmış olduğu harita.*



Kaynak: *Christian Mattman, "Searching Deepand Dark: Building A Google For The Less Visible Parts of Web", The Conservation, 9 Ocak 2017, https://theconversation.com/searching-deep-and-dark-building-a-google-for-the-less-visible-parts-of-the-web-58472, (Erişim Tarihi: 01.02.2020).*

Kripto para birimlerinin ve Dark Web'in terör örgütleri tarafından kullanılması terörizmin 21. yüzyıl içerisindeki hızlı, dinamik ve gelişen yapısının önemli bir göstergesidir. Terör örgütlerinin Dark Web'i finansal kaynak, terör eylemlerini planlamak ve sürdürmek adına kullandığı, IŞİD'in Paris saldırısında ve IŞİD ve YPG gibi terör örgütlerinin kripto para birimleri ile işlem yapması sonucunda açığa çıkmıştır. Ulus devletlerin terörizme etkili bir şekilde cevap verebilmesi için Dark Web üzerinden *per se* bir güvenlik riski oluşturmayan kripto paralar ile gerçekleştirilen işlemleri engelleyici kalıcı önlemler üretmesi gerekmektedir. MEMEX projesi her ne kadar terörizmi önlemek adına geliştirilmiş olsa da Tor, I2P gibi ağların anonimliği sağlaması ve kişisel hak ve özgürlükler gibi kavramlar ile Dark Web'in ayrımın yapılamaması şimdilik bu duruma engel teşkil etmiştir. Kısacası Deep Web ile sağlanan anonimliğin Dark Web'de gerçekleştirilen yasa dışı faaliyetlerden ayrılması gerekmektedir. Burada önemli tartışmalardan biri kişisel özgürlükler, verinin korunması ve ifade özgürlüğü gibi başlıkların siber dünyada mücadele bağlamında nasıl şekilleneceğidir. Bu bağlamda ABD'de Defense Advanced Research Program Agency (DARPA), Total Information Awareness (TIA) ve Multi-State Anti-Terrorism Information Exchange (MATRIX) gibi yazılım ve sistemlerin kişisel özgürlükler ve sivillerin verilerinin suiistimali dolayısıyla kullanımdan kaldırıldığını da hatırlamakta fayda vardır. Dolayısıyla devletlerin önümüzdeki süreçte karşılaşacağı en önemli güvenlik meselelerinden biri olan siber güvenlik başlığında hem özel sektörle etkileşimin hem de hukuki sınırların korunmasının önemi ve bunun genel güvenlik-özgürlük ikilemine yansıması, üzerinde önemle durulması gereken başlıkları teşkil etmektedir.

Kaynakça

Adapting to increased military pressure (2017). ISIL Shifts To 'Dark Web,' UN Security Council Told", UN News, 7 Şubat 2017, https://news.un.org/en/story/2017/02/551012-adapting-increased-military-pressure-isil-shifts-dark-web-un-security-council, (E.T. 22 Şubat 2019).

Ball,B., Arthur , C. ve Gabbatt, A. (2013). FBI claims largest bitcoin seizure after arrest of alleged silk road founder, TheGuardian, 2 Ekim 2013, https://www.theguardian.com/technology/2013/oct/02/alleged-silk-road-website-founder-arrested-bitcoin, (E. T. 27 Şubat 2019).

Bartlett, J. (2016). Dark Net: internetin yer altı dünyası, çev. Yasin Konyalı, İstanbul, Timaş Yayınları.

Beckett, A. (2009). The dark side of the internet, 26 Kasım 2009, https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet, (E.T. 26 Aralık 2018).

Berg, A.G. (2017). How an anarchist bitcoin coder found himself fighting ISIS in Syria, Wired, 29 Mart 2017, https://www.wired.com/2017/03/anarchist-bitcoin-coder-found-fighting-isis-syria/, (E. T.26 Şubat 2019).

Bergman M. K. (2001). The Deep Web: surfacing hidden value, Bright Planet, Cilt 7, No 3.

Brewster T. (2018). This Insane Map Shows All The Beauty And Horror of The Dark Web, Forbes, 13 Mart 2018, https://www.forbes.com/sites/thomasbrewster/2018/03/13/dark-web-map-6000-webpages/#4ee4912718e7, (E.T. 27 Şubat 2019).

Chaabane, A., Manils, P. ve Kaafar, K.A. (2010). Digging into anonymous traffic: a deep analysis of the tor anonymizing network, 4th International Conference on Network and System Security (NSS), 1 Eylül 2010, https://planete.inrialpes.fr/papers/TorTraffic-NSS10.pdf. Adresinden Erişilmiştir.

Charlton, A. (2014). Snowden files reveal NSA had 'major problems' tracking tor dark web users and cracking encryption, International Business Times, 29 Aralık 2014, http://www.ibtimes.co.uk/snowden-files-reveal-nsa-had-major-problems-tracking-tor-dark-web-users-cracking-encryption-1481225, (E. T. 30 Aralık 2018).

Clarke, I., (1999). A distributed decentralised information storage and retrieval system, Division of Information University of Edinburgh, https://freenetproject.org/papers/ddisrs.pdf. Adresinden Erişilmiştir.

Clarke, I., Hong T. W., Sandberg, O. ve Wiley, B. (2002). Protecting free expression online with freenet, IEEE Internet Computing, Ocak- Şubat 2002, https://freenetproject.org/papers/freenet-ieee.pdf. Adresinden Erişilmiştir.

Copestake, J. (2014). Hidding currency in the dark wallet, BBC, 19 Eylül 2014, https://www.bbc.com/news/technology-29283124, (E. T. 26 Şubat 2019).

Core, A. (2018). Fighting terrorism on the dark web: new techto fight advantaced enemy tactics, Torres, 10 Ağustos 2018, http://www.torresco.com/fighting-terrorism-dark-web-new-tech-fight-advanced-enemy-tactics/, (E.T. 30 Ocak 2018).

Çelik, E. (2017). Deep web ve dark web: internetin derin dünyası, Cyberpolitik Journal, Cilt 2, No 4.

Deep web search may help scientists, NASA, 22 Mayıs 2015, https://www.jpl.nasa.gov/news/news.php?feature=4595, (E. T. 1 Mart 2019).

Defense Advanced Research Projects Agency, Memex, DAPRA, https://www.darpa.mil/program/memex, (E. T. 27 Şubat 2019).

Dingledine, R. (2014). Tor: The Second-Generation Onion Router, in Proceedings of the 13th USENIX Security Symposium, https://www.usenix.org/legacy/event/sec04/tech/full_papers/dingledine/dingledine.pdf. Adresinden Erişilmiştir.

Financal Analyst Insider (2018). How to spend crytocurrency in the real world, 4 Mart 2018 https://financialanalystinsider.com/use-cryptocurrency-real-world/, (E. T. 23 Aralık 2018).

Finklea, K. (2017). Dark Web, Congressional Research Service, 10 Mart 2017, https://fas.org/sgp/crs/misc/R44101.pdf. Adresinden Erişilmiştir.

Ghaffar H. ve Erin Marie S. (2014). Jihad trending: a comprehensive analysis of online extremism and how to counter IT, QUILLIAM, Mayıs 2014, https://preventviolentextremism.info/sites/default/files/Jihad%20Trending-%20A%20Comprehensive%20Analysis%20of%20Online%20Extremism%20and%20How%20to%20Counter%20it.pdf, Adresinden Erişilmiştir.

Glasser, E. (2015). Paris attackers used 'dark web' to coordinate. What Is It? WTSP-Tv, 16 Kasım 2015, https://www.wtsp.com/article/news/local/paris-attackers-used-dark-web-to-coordinate-what-is-it/67-47820003, (E. T. 19 Şubat 2019).

Henninger, D. (2012). The president that time forgot. *Wall Street Journal.* 28 Haziran 2012. 04 Temmuz 2012, http://online.wsj.com/article/wonder_land.html?mod=WSJ_topnav_europe_opinion#articleTabs=article, Adresinden Erişilmiştir.

Hutton , R. (2016). Nuclear drones from dark web cited by obama in terror scenario, Bloomberg, 2 Nisan 2016, https://www.bloomberg.com/news/articles/2016-04-01/nuclear-drones-from-dark-web-cited-by-obama-in-terror-scenario, (E.T. 26 Şubat 2019).

Internet Live States (2019). http://www.internetlivestats.com/, (E.T. 01 Aralık 2019).

Is FreeNet More Secure and Anonymous than Tor? , https://www.quora.com/Is-Freenet-more-secure-and-anonymous-than-Tor, (E.T. 29 Aralık 2018).

Kelion, L. (2014). Tor project's struggle to keep the "dark net" in the shadows, 22 Ağustos 2014, https://www.com/news/technology-28886465, (E.T. 15 Aralık 2018).

Lee, D. (2017). Defending tor-gateway to the dark web, BBC, 5 Ağustos 2017, https://www.bbc.com/news/technology-40810771, (E. T. 07 Ocak 2019).

Levine, B. N., Liberator, M., Lynn, B. ve Wright, M (2017). Statistical detection of downloaders in freenet, IEEE International Workshop on Privacy Engineering, Mayıs 2017, http://ceur-ws.org/Vol-1873/IWPE17_paper_12.pdf, Adresinden Erişilmiştir.

Macrina, A. ve Phetteplace, E. (2015). The Tor browser and ıntellectual freedom in the digital age, American Library Association, Cilt 54, No 4.

Mangan, D. (2018). New York woman pleads guilty to using bitcoin to launder money for terror group ISIS, CNBC, 27 Kasım 2018, https://www.cnbc.com/2018/11/26/new-york-woman-pleads-guilty-to-using-bitcoin-to-launder-money-for-isis.html, (E. T. 26 Şubat 2019).

Memex (2017). https://worldbrain.io/, (E.T. 27 Şubat 2019).

Mikael Eriksson, et. al., Socail media and ICT during the arab spring, FOI, Temmuz 2013.

Moore, D. ve Rid, T. (2016). Cryptpolitik and The Dark Net. , Surival Cilt 58, No1, Şubat/Mart 2016.

Nakashima, E. (2013). Pentagon to boost cyber security force, The Washington Post, 27. Ocak. 2013,https://www.washingtonpost.com/world/national-security/pentagon-to-boost-cybersecurity-force/2013/01/27/d87d9dc2-5fec-11e2-b05a-605528f6b712_story.html?utm_term=.70f8063d1573 (E.T. 24 Mart 2019).

Owen, G. ve Savage, N. (2015). The Tor dark net, Chatham House The Royal Institute of International Affairs, Eylül 2015, No 20.

Paoli G.P., Aldridge, J., Ryan, N. ve Warnes, R. (2017). Behind the curtain the ıllicit trade of firearms, explosives and ammunition on the dark web, RAND Research Reports.

Paoli, G.P. (2018). The trade in small armsand light weapons on the dark web, UNODA Occasional Papers, No 32.

Peaster W.M. (2019). The best exchanges for trading cryptocurrency, 24 Ocak 2019 https://blockonomi.com/cryptocurrency-exchanges-trading/ adresinde erişilmiştir.

Santos,D. (2017). What the dark web is and isn't, smart data collective, 30 Mart 2017, http://www.smartdatacollective.com/what-dark-web-and-isn-t/, (E.T. 07 Ocak 2019).

Schneier, B. (2013). Attacking tor: how the NSA targets users online anonymity, The Guardian, 4 Ekim 2013, https://www.theguardian.com/world/2013/oct/04/tor-attacks-nsa-users-online-anonymity, (E.T. 12.12.2018).

SecDev Foundation (2018). Syrian regime tightens access to secure online communications, 27 Ocak 2018, https://www.secdev-foundation.org/internet-in-syria-remains-critical/, (E. T. 1 Ocak 2019).

Sigalos, M. (2018). The dark web and how to access it?, CNBS, 23 Ocak 2018, https://www.cnbc.com/2018/04/13/the-dark-web-and-how-to-access-it.html, (E.T.1 Ocak 2019).

Tiwarii, A. (2017). Everything about Tor; what is tor? How tor works?, Foss Bytes, 22 Mayıs 2017.

TOR (2017). Normal people use Tor, https://www.torproject.org/about/torpeople.html.en, (E.T. 31 Aralık 2018).

TOR (2017). Tor sponsor, https://www.torproject.org/about/sponsors.html.en, (E.T. 2 Şubat 2019).

TOR: Overview (2019). Tor project, https://www.torproject.org/about/overview, (E.T. 05 Ocak 2020).

U.S. Department of Justice Office of Public Affairs (2015). Former secret service agent sentenced to 71 months in scheme related to silk road investigation, 7 Aralık 2015, https://www.fbi.gov/contact-us/field-offices/sanfrancisco/news/press-releases/former-secret-service-agent-sentenced-to-71-months-in-scheme-related-to-silk-road-investigation, (E.T. 10 Şubat 2020).

Watson, K. D. (2012). The tor network: a global inquiry into the legal status of anonymity networks, Washington University Global Studies Law Review, No 11.

Weimann, G. (2010). Terror on the internet: the new area, the new challenges, 9 Mayıs 2010, https://www.usip.org/publications/2010/05/terror-internet, (E. T. 4 Şubat 2019).

Weimann, G.(2018). Going darker? The challenge of dark net terrorism, Wilson Center, https://www.wilsoncenter.org/sites/default/files/going_darker_challenge_of_dark_net_terrorism.pdf, Adresinden Erişilmiştir.

Weimanni, G. (2016). Terrorist migration to the dark web terrorism research institute, Cilt 10, No 3.

Yang, I. (2019). Addressing the issue of transnational organized crime in order to combat the growth of terrorist groups,The Hague International Model United Nations Qatar, 22-25 Ocak 2019.

Zantout, B. ve Haraty, R. A. (2011). I2P data communication system, TheTenth International Conference on Networks, 23-28 Ocak 2011.