DEEP WEB VE DARK WEB: İNTERNET'İN DERİN DÜNYASI

Emine ÇELİK[*]

Özet

İnternet şüphesiz insanlık tarihinde devrim niteliğinde bir buluş ve gelişimi de halen devam etmektedir. İnsanların birçoğu iletişim, sosyal medya, alışveriş, siyasi ve sosyal gündem takibi ve daha fazlası için interneti kullanmaktadır. İnternetin devletlerin uluslararası arenada, kamu kuruluşlarında ve insan hayatındaki yeri itibariyle Deep Web ve Dark Web kavramlarının yalnızca bilgisayar, yazılım mühendislerince ele alınmasının eksikliğinden yola çıkarak sosyal bilimler içerisinde incelenmesi büyük önem arz etmektedir. Buradan hareketle çalışma içerisinde Deep Web ve onun karanlık yanı olarak isimlendirilen Dark Web'in ortaya çıkardığı potansiyel tehlikelere değinilmiştir. İki kavramın nasıl ortaya çıktığı ve gelişimi, Deep Web'e erişimin nasıl sağlandığı, iki kavramın birbirinden ince bir çizgiyle ayrıldığı yerler, Dark Web'deki yasadışı faaliyet alanlarının getirmiş olduğu sorunların önemine vurgu yapılmıştır. Akabinde, Dark Web karşısında devletlerin nasıl bir politika izlemesi gerektiğine dair analizler yapılmaya çalışılmıştır.

Anahtar Kelimeler: Deep Web, Dark Web, Tor, Siber Suçlar, Siber Uzay

Abstract

The Internet is undoubtedly still a revolutionary breakthrough in the history of humanity. Many people use the internet for communication, social media, shopping, political and social agenda, and more. Deep Web and Dark Web concepts not only handled by computer, software engineers but also handled by social siciensists because of the role of internet for the States in international arenas, public institutions and human life. By the moving point that very important

[*] Doktora Öğrencisi, Necmettin Erbakan Üniversitesi, Siyaset Bilimi ve Kamu Yönetimi Bölümü, E-mail: eminegvenilir@gmail.com

role of internet for social sicientists, the potential hazards of Deep Web and its dark side referred to Dark Web have been put forth. The emergence and development of deep web and dark web concepts and the acsees of them were handled in the paper. The diffrences between the two concepts which are crucial point of the topic, and the Dark web significance of market are impressed on the paper. Additionally; In the face of Dark Web, an attempt has been made to analyze what kind of policy the states need to follow.
Key Words: Deep Web, Dark Net. Tor, Cybercrime, Cyberspace.

GİRİŞ

İnternet, tasarlanışı itibariyle bilgi paylaşımı ve şeffaflık üzerine inşa edilmiştir. Bu bağlamda da günümüze değin insanlar şeffaflık, bilgiye hızlı ve mekân sınırı olmadan erişim gibi olumlamalar üzerine internet ile olan ilişkilerini geliştirmişlerdir. 21. yüzyılda internetin insan hayatı içerisinde vazgeçilmez bir konuma ulaşması ise çeşitli tartışma alanlarının ortaya çıkmasına neden olmuştur. Sınırları hakkında bilgiye sahip olunmayan internetin ve dolayısıyla siber uzayın insan güvenliği açısından bazı tehlikeler barındırdığı 21. yüzyılda yaşanılan teknolojik gelişmelerin hızlı bir ivme sergilemesi sonucunda fark edilmiştir. Teknoloji dünyasında yaşanılan bu hızlı gelişim internetin bilmediğimiz katmanlarının ulaşılabilir olmasına sebep olmakla birlikte çeşitli güvenlik zafiyetlerinin de ortaya çıkmasına neden olmuştur. 2013 yılında internetin derin dünyası olarak adlandırılan Deep Web ve Dark Web üzerinde faaliyet gösteren Silk Road adı altında yasa dışı ürünlerin satıldığı siteye FBI tarafından gerçekleştirilen bir operasyon sonucunda internetin bazı katmanlarının ne kadar tehlikeli olduğu gözler önüne serilmiştir. Başta devletlerin, güvenlik güçlerinin, akademisyenlerin, düşünce kuruluşlarının ve kamuoyunun dikkatini çeken Silk Road operasyonun akabinde Deep Web ve Dark Web hakkında çeşitli tanımlamalar yapılmaya çalışılsa bile akademik manada doyurucu bir tanım yahut sınır çizilememiştir. Çeşitli parametrelerle izah edilebilecek bu durumun başlıca nedenin ise teknolojik gelişimin sürekli olması, günümüzde internet ve onun derinliği hakkında sağlıklı verilere ulaşılabilecek donanımsal materyallere sahip olunamaması şeklinde ifade edilebilmektedir.

İnternet Kavramı ve Gelişimi

İnternet sözcüğü 20. yüzyılın ikinci yarısı ile ABD ordusunun geliştirme kolu olan İleri Araştırma Projeleri Ajansı tarafından 1960'ların sonlarında yürütülen ve desteklenen küçük bir

bilim projesi olarak hayatımıza girmiş(Barttlet, 2016:15) ve günümüz dünyasında da bireysel olarak yaşamımızın her anında kullandığımız vazgeçilmez bir nesne olmuştur.

İnterneti kullanan 4,8 milyar kişinin varlığının yanı sıra yüzey interneti o1arak adlandırılan kısımda 1,2 milyardan fazla web sitesi bulunmaktadır. Bununla birlikte günde 3,5 milyar Google aramasından söz edilmektedir. Ayrıca "sıradan" bir gün içerisinde ortalama 157 milyar e-mail gönderildiği, 2 milyardan fazla aktif Facebook kullanıcısının olduğu, 500 milyon tweet atıldığı, 4 milyardan fazla YouTube'dan video izlendiği, 47 milyona yakın fotoğrafın Instagram'a yüklendiği araştırmalar sonucunda elde edilmiştir(Internetlivestats, 2018). Rakamsal bu verilerin yanı sıra internet devletler nezdinde ve kamu kuruluşlarında da işleyişin temel aktörlerinden biri haline gelmiştir.

İnternet aslında iletişim ve işbirliğine izin veren açık bir ağ mimari olarak tasarlanmıştır.[12] Tanımlaması yapılacak olur ise ilk başta tasarlandığı gibi birçok kümülatif ağ yapısının bir araya gelmesiyle ortaya çıkan ağ sarmalı olmasıyla birlikte özel standart protokoller kullanarak enformasyon iletmek üzere tasarlanmış devasa bir desantralize bilgisayar ağ şeklinde kavramsallaştırılmaya çalışılmıştır (Schmidt ve Cohen, 2015: 95).

Uzun ve karmaşık tanımlamanın akabinde şu sorular ortaya çıkmaktadır: İnternet sözcüğünü duyduğumuzda zihnimizde ilk olarak ne canlanır? İnternet yalnızca sosyal medya üzerinden etkileşim sağladığımız ağ ya da Google, Bing, Yandex, Yahoo gibi arama motorları ile hayatı kolaylaştıran bilgi kaynağı mıdır?

İnternetin tüm katmanları ele alındığında bilinmezlik ve güvenlik kaygısı taşıyan mimarisi, anonimlik, isnat ve tespitte yaşanan zorluklar -günümüzde devletlerin alt yapılarını oluşturan temel argümanların ağlar üzerinden yönetildiği düşünüldüğünde (Ermiş, 2014) - başta devletlerin olmak üzere, şirketlerin ve bireylerin de yaşamlarını tehdit eder seviyeye gelmiştir. Gelişiminden günümüze kadar uzanan internet yapısı incelendiğinde karşımızda geniş bir alanın olduğu görülmektedir. Düşünülenden fazlasını mevcut ağ yapısının içerisinde barındıran

[12] Deep Web'in spesifikliği ve alanın genişliği bağlamında konuyu karmaşıklaştırmamak adına İnternet yapısının ortaya çıkışı hakkında çalışmada detaylı olarak yer verilmemiştir. İnternetin ortaya çıkışı ve çalışma prensibi hakkında geniş bir bilgiye ulaşmak için bknz: Barry M. Leiner vd. (1997)"Brief History of the Internet ", Internet Society.

internetin ne olduğu aslında insanoğlunun uzay hakkındaki bilgisi kadar olmakla birlikte "Siber Uzay" kavramının karmaşıklığının da ortaya çıkmasıyla sonuçlanmıştır.

Deep Web ve Dark Web Kavramsal Tanımlanması ve Gelişimi

Günümüzde dünyadaki birçok kişi günlük yaşantısında kullandığı internetle siber uzay dünyasında var olan bilgilerin hepsine bahsi geçen arama motorları ile ulaşabileceğini düşünmektedir. Bilinen arama motorların ulaşabildiği bilgilerin çok daha fazlasıysa internetin ağ yapısı incelendiğinde "Deep Web" yani "Derin İnternet" olarak ifade edilen alanda karşımıza çıkmaktadır.

Detaylandıracak olursak; internet olarak adlandırdığımız şey kabaca üç katmana ayrılabilir: yüzey ağ, derin ağ ve karanlık ağ (Santos, 2017). Peki insanların birçoğunun yüzey interneti kullandığı düşünülürse kalan insanların kullanmış olduğu Deep Web neyi ifade etmektedir?

Amerikalı bir akademisyen ve girişimci olan Micheal Bergman "*Deep Web*" ifadesini ilk ortaya atan kişi ve bu konuda önde gelen otoritelerinden biri olarak 90'lı yılların sonlarında derinliğini ölçmek için yaptığı ölçek araştırmasının sonucunda çalışanlarına yüzey internetinin iki yada üç katı büyüklükte olduğunu ifade etmiş ve araştırmanın ilerleyen süreçlerinde tahmin edilen derinliğin daha fazla olduğunu vurgulamıştır. Ayrıca Bergman, Deep Web'i internette bilgilerin en hızlı büyüdüğü alan olarak ifade etmiştir (Beckett, 2009). Deep Web internetin karmaşık ve gizemli bölümü olarak kavramsallaştırılabilmektedir. Deep Web aynı zamanda Hidden Web (Gizli Web) ya da Invisible Web (Görünmeyen Web) olarak da isimlendirilmektedir (Hawkins, 2016: 5-7).

Günümüzdeyse yukarıda bahsi geçtiği gibi kavramsal olarak internetin yer altı olarak tabir edilen Deep Web, var olan yüzey ağının 400-500 katından fazlasının olduğu tahmin edilmektedir. Yüzey interneti olarak adlandırılan (%4 ile %10 aralığını temsil etmektedir) bölüm dışındaki Deep Web'e girmek için ise özel olarak tasarlanmış yazılımsal ürünler, browserler kullanılmaktadır (Epstein, 2014).

Deep Web'in kavramsallaştırılması ve fiziksel olarak ifade edilmesinde popüler olarak kullanılan buzdağı temsilinin yanı sıra yer altı maden işletmeciliği örneği de kullanılmaktadır. Zemin üzerindeki görünür ve bulunabilir her şey yüzey internetini temsil ederken yüzey

altındaki her şey Deep Web'in doğal olarak gizlenmiş, ulaşılması zor ve kolayca görülmeyen yanına atıf yapmaktadır (Cincaglini, vd., 2015:5).

Deep Web dünya çapındaki internetin büyük bir bölümü olmakla birlikte standart arama motorları tarafından indekslenemezler (NCA, 2016:49). Daha açık bir ifade ile Deep Web arama motorlarının ve dizinlerinin doğrudan veri tabanlarına erişimi olmayan geniş bilgi havuzunu ifade etmektedir (Lifewire,2017). Normal şartlarda sınırlı erişim ağları yahut standart bir ağ yapısıyla erişilemeyen Deep Web içerikleri ve barındırılan hizmetler bağlamında kötü amaçlı aktörlerin (terörist gruplar, uyuşturucu satıcıları, eski istihbarat elemanları, çocuk istismarcıları vb…) yasa uygulayıcı aktörler tarafından kısmen ya da tamamen algılanmamasına, görülememesine zemin hazırlamaktadır (Cincaglini, vd., 2015:5). Derin internetin indekslenmemiş bu katmanı ifade etmesiyse güvenlik kaygılarının temelini oluşturmaktadır.

Buraya kadar sorun teşkil etmeyen Deep Web ve Tor benzeri (FreeNet, IP2) yazılımsal sistemlerin kullanımının ortaya çıkardığı asıl sorun ise yasa dışı faaliyetlerin sürdürüldüğü ve bireysel ve devletler nezdinde tehlikeli hala gelen Deep Web'in bir parçası olan ve karanlık katman olarak ifade edilen Dark Web'in kullanımı olmuştur. Deep Web'in tanımlanmasındaki güçlükten yola çıkarak Dark Web'in tam bir akademik tanımının varlığından söz edilememektedir.

Araştırma sonucunda, Dark Web için: Google gibi standart bir web tarayıcısı kullanarak arama motorları tarafından dizine eklenmeyen ve yönlendirilmeyen internette bir bölüm olduğu ve veriye ulaşabilmek için uzman bilgi birikimi ve yazılımsal araçları gerekliliğinden bahsedilmektedir. Ayrıca unutulmamalıdır ki Dark Web, Deep Web değildir, Deep Web içerisinde yasadışı faaliyetlerin yürütüldüğü bir alan olarak belirtilmiştir (Cincaglini, vd., 2015:6). Bu bağlamda da Dark Web genel çerçevede yasadışı faaliyetlerle ilişkilendirilmektedir (Charlton, 2014).

İnternet'in 1990'ların ortasında hemen hemen tüm dünyada popüler hale gelmesinden bu yana var olan "Deep Web" ve onun karanlık yanı olarak nitelendirilen "Dark Web" kavramı uzunca bir süre kamuoyunun dikkatini çekmemiştir. Dark Web'in kamuoyunun tüm dikkatleri üzerine çekmesi ise Ross William Ulbricht'ın tutuklanmasıyla olmuştur. Ulbricht'ın kurmuş olduğu İpek Yolu (Silk Road) sitesi, 2011 yılında faaliyete geçmiş ve bu web sitesi aracılığıyla

satıcıların ve alıcıların internet üzerinden anonim şekilde alışveriş yapabileceği bir platform olması üzerine dizayn edilmiştir (Christin, 2012:3).

Ulbricht'in kurmuş olduğu İpek Yolu'ndaki işlemleri anonimleştirmek için iki türlü yola başvurduğu ortaya çıkmıştır. İlk olarak müşterilerinin anonim olması için Tor ağını kullanmış, ikincisi ise tüm yasa dışı alışverişleri –ilgili bölümde sınıflandırılmasında da bahsedildiği gibi- Bitcoin olarak bilinen ve internette kullanılan, bugün itibariyle herhangi bir yerde fiziksel formda var olmayan, merkezi olmayan elektronik para birimi üzerinden gerçekleştirmiştir. İpek Yolu sayesinde kullanıcılar anonim olarak uyuşturucu ve yasa dışı malların alım ve satımını gerçekleştirilmesini sağlanmıştır. Silk Road yani İpek Yolu Dark Web'de gelişen ilk başarılı anonim pazar olmakla birlikte Amazon tarzında bir yapı benimsediği de görülmüştür(Hawkins, 2016:13). FBI'ın iddiasına göre Ulbright'in bilgisayarına el konulduğunda 150 milyon dolar değerinde 144.000 Bitcoin ele geçirilmiştir. İnternet üzerinden gerçekleştirilen yasa dışı bu faaliyetin FBI tarafından ortaya çıkarılması tüm dünyanın merakını arttırmış ve Deep Web'e ve onun karanlık yönü olan Dark Web'in birçok alanda incelenme ihtiyacını ortaya çıkarmıştır.[13]

Çeşitli güvenlik departmanları ve akademisyenlerce yapılan araştırmalar derinleştikçe İpek Yolu'nun Dark Web'deki en büyük pazar olduğu ancak tek olmadığı anlaşılmıştır. Dark Web'de tamamen yasa dışı faaliyet gösteren bu sitelerin varlığının güvenlik güçleri tarafından takip edilmesi ve akabinde de kapatılmasına rağmen üzerinden çok zaman geçmeden yenilerinin faaliyet göstermeye başlaması ise Dark Web'in işlevselliğini gözler önüne sermektedir (Barttlet, 2016: 152-154).

Tor ve Free Net: Deep Web'in Araçları

Deep Web ve Dark Web hakkında yüzey internet protokollerinden farklı bir çalışma prensipleri kullanması haricinde ilk nasıl kullanılmaya başlandığına dair sağlıklı ve kesin bilgilere ulaşmak zordur. Bunun nedeni ise yukarıda bahsi geçen eylemlerin gerçekleştirildiği platform olmasından ve devletler nezdinde gizlilik arz etmesinden kaynaklandığını söylemek makul bir yaklaşım olabilmektedir. Bunun yanı sıra Deep Web'e giriş için gerekli olan yazılımsal

[13] FBI, "Manhattan U.S. Attorney Announces Seizure of Additional 28$ Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of "Silk Road" Website". https://archives.fbi.gov/, Cadie Thompson, (2015)."Beyond Google: Everything You Need to Know About the Hidden Internet", Business Insider, http://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11.

araçlardan bahsedecek olur isek en popüler ve bilinenleri Tor ve FreeNet olarak sıralanabilmektedir.

Türkiye'de de yaygın olarak kullanılan ve artık girişi yasaklanan (Aydoğan, 2017) The Onion Router yani Tor 2002 yılında bütünüyle ABD Donanma Araştırma Laboratuarı ile kar gütmeyen kuruluş olan Free Haven Projesi arasında ortak bir proje olarak ortaya çıkmıştır. Projenin temel amacı ise ihtiyaç duyanlar tarafından kullanılmak üzere dağıtılmış, isimsiz yani anonim ve kolayca konuşlandırılabilir, şifrelenmiş bir ağ oluşturmak şeklinde açıklanmıştır (Moore and Rid, 2016:11). Bir diğer deyişle Tor'un amacı iletilen verilerin adsız kalmasını sağlayacak bir ağ platformu oluşturmasıdır.[14]

Tor mimarisi tek bir yazılım aracılığıyla anonim tarama ve anonim bilgi alışverişlerinin barındırılması için iki temel hizmet sunmaktadır (Moore and Rid, 2016:9). Tor bağlantısı ile giriş yapılan Deep Web ve Dark Web'de aranılan argümanları bulmak kolay bir iş olarak gözükmemektedir. Bunun temel nedeniyse; Tor ile giriş yaptığınız Deep Web ve Dark Web'de internetin yüzey kısmında bulunan sitelerle buralardaki sitelerin benzerlik göstermesidir. Ancak herhangi bir başka siteyle bağlantısı olmamakla birlikte Tor ile giriş yapılan sitelerde URL adreslerinin anlamsız numaralar ve harflerden oluştuğu görülmektedir. Yüzey internetinde bilinen, sonu "com", "org" ve "com. tr" gibi adreslerin yerine "hy352qdvb21.onion" gibi adreslerle bu platformlarda gezinti yapmak mümkündür. URL farklılığının yanı sıra söz konusu sitelerin adresleri Tor Gizli Servisleri tarafından her gün düzenli şekilde değiştirilmektedir. Ancak Deep Web ve Dark Web kullanıcılarına kolaylık sağlayabilmesi açısından güncel sayfaların indekslendiği bazı siteler yer almaktadır. En popüler olanlarından Hidden Wiki'de Wikipedia mantığı ile çalışarak güncel sitelerin adresleri sıralı şekilde yer aldığı bilinmektedir (Bartlett, 2016:119).

Deep Web ile bağlantılı olarak FreeNet ise Edinburg Üniversitesi'nde Ian Clarke adında bir genç tarafından 1995'te insanların internette anonim olarak yani takip edilmeden kullanması için devrim niteliğinden yeni bir yol haritası öneren bilgisayar bilimi dersi için "Dağıtılmış, Merkezi Olmayan Bilgi Depolama ve Alma Sistemi" adında bir tez olarak hazırlanmıştır. Clarke tezinden yola çıkarak 2000 yılında FreeNet adlı yazılımı yayınlamıştır. Bu yazılım sayesinde anonim bir şekilde internetin yüzey katmanının altına inerek Deep Web'e erişim

[14] Hawking, B. a.g.e. p.15.

sağlanabilmiştir. Tor mantığı ile aynı şekilde anonimliği ön planda tutan Freenet'te standart adres uzantılarına -com, org, gov, gibi bilinen uzantılar yerine rakamlardan oluşan bir uzantı vermişlerdir- sahip olmadıkları ve çalışma prensiplerinin normal internetten farklı olması sebebiyle tamamen bir gizlilik sunmaktadır (Labovitz, 2009:11).

Dark Web'deki Potansiyel Tehlikeler

Klasik yüzey internetinin daha gelişmişi olarak birçok kişinin bazı parametrelerden sıyrılarak edinmeye çalıştıkları bilgi alış verişi olarak ele alınan Deep Web'in kullanımın tamamen yasa dışı olduğundan bahsetmek yanlış bir söylemdir. Birçok siyasi düşünür, gazeteci, bilim adamı, akademisyen ve hatta özel hayat gizliliğine önem veren sıradan vatandaşlar bile Deep Web'i kullanmaktadır.[15]

Arap Baharı sürecinde mevcut hükümetlerce internet kullanımın yasaklanmasına rağmen Twitter ve Facebook üzerinden organize olarak gösteri düzenleyen kitlelerin VPN'in yanı sıra, Tor ile birlikte Deep Web'i aktif şekilde kullandığı bilinmektedir. Deep Web'in güvenli kullanıma dair ABD başta olmak üzere Batı'da birçok bilişim şirketi bu yönde hizmet vermektedir.[16] Lakin kullanımı yasal ya da yasal olmasın Deep Web'e erişim kısıtlı ve kullananlar tarafından kasıtlı bir eylem olduğu belirtilmiştir (Hawkins, 2016:7). Buraya kadar birçok ülkede sorun teşkil etmeyen Deep Web'in temel problematiği; Dark Web'deki kişiler tarafından gerçekleştirilen paylaşımların anonim olması(diğer bir ifadeyle IP adresleri herkese açık olarak paylaşılmadığı için) olarak ifade edilmiştir. Bu bağlamda da bu kişilerin devletler veya şirketlerin müdahalesinden çekinmeden iletişim kurup yasadışı faaliyetlerde özgürce bulunmasıysa Dark Web'in potansiyel tehlikesinin temel argümanı şeklinde ifade edilmektedir (Digital Citizens Alliance, 2017:4). Bu argümandan yola çıkılarak vurgulamak gerekirse internet ortamında yani Dark Web'de bir düğümle diğer düğüm arasında Tor gibi yeterince kimlik gizleyici katmanlar söz konusu ise veri paketlerini kaynağına kadar izlemek kesinlikle olanaksızdır. Geniş bir çerçeve içerisinde bahsedilecek olursa da Dark Web platformunda karşıdaki kişiyi tespit etmek bugün neredeyse imkânsızdır(Smidt ve Cohen, 2015:134).

[15] Bu parametreye örnek olması açısından bknz: Marco, C., "Access The Deep Web And Protect Your Privacy Online With The Anonabox", 29.04.2016. https://www.forbes.com/sites/marcochiappetta/2016/04/29/access-the-deep-web-and-protect-your-privacy-online-with-the-anonabox/#6a922a6440c2

[16] Örnek olması açısından bknz: https://brightplanet.com

Deep Web ve Dark Web arasında ayrım yapılamamasının ve yasa dışılık ve yasalara aykırı olamama tartışmaları olmakla birlikte yasal yargı alanları arasındaki karışıklık ve karışıklıklar nedeniyle siteleri, yasal ya da yasa dışı olarak sınıflandırmanın zor olduğu ifade edilmiştir (Owen ve Savage, 2015:4). Sınıflandırmanın zorluğu üzerine Lüksemburg Üniversitesi'nde Deep Web içerisindeki 40.000 adet sitede yapılan analizin akabinde, sitelerin büyük çoğunluğunun İngilizce olduğu, %17'sinin yetişkin içerikli çocuk pornosu, uyuşturucuların %15'ini, sahte ürünlerin %8'ini, hackleme bilgilerinin %3'ünü, siyasi içerikli sitelerin %9'u, yazılım ve donanım üzerine %7 ve sanat üzerine de %2'lik bir oranın tespit edildiği anlaşılmıştır (Bartlett, 2016:280). Buradan yola çıkarak genel kabul gören sınıflandırma:

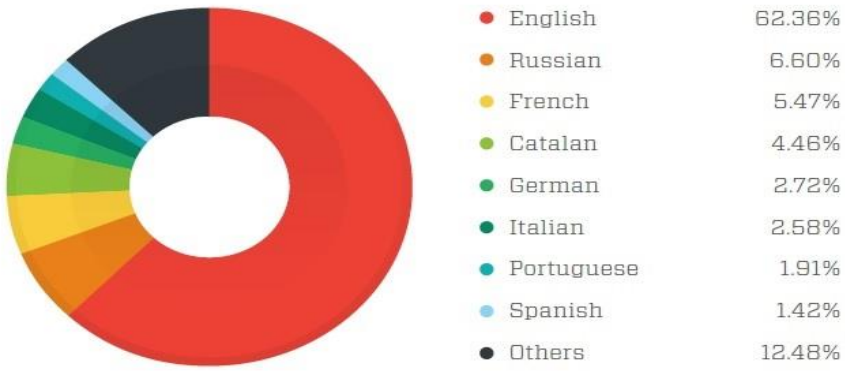
- Kötüye Kullanım: Bu başlıkta altında genel olarak cinsel istismarı gösteren(özellikle küçük çocuklar) ve Batı'da ve dünyanın neredeyse tamamında yasak olan siteler,
- Anonimlik(İsimsizlik): Anonim araçların yahut anonim kültürün tanıtımını veya öğretmeyi amaçlayan siteler,
- Bitcoin: Sanal para birimiyle para vs alış-verişi olarak isimlendirilse bile genel itibariyle kara para aklama hizmetleri,
- Blog: Kişisel yahut toplu blog ve genel itibariyle siyasi, etnik, dini saldırı içerikli,
- Kitaplar: Telif haklarıyla korunan kitapların ücretsiz olarak kullanımına izin verilmesinin yanı sıra yasaklı kitapların paylaşımı,
- Sohbet: Web tabanlı sohbet servisleri,
- Sahtekarlık: Sahte ürünler sunan siteler: Pasaport, kimlik kartları, sahte paralar… vs.
- Dizin: Dark Net içerisinde diğer sitelere bağlantı kuran siteler(genellikle anonim olan alan adlarının bulunmasının yardımcı olması için kullanılmaktadır.),
- Uyuşturucular: Uyuşturucu alışı veya satışı; genel itibariyle alıcılarla satıcıları birbirine bağlayan pazarlar,
- Forum: Birincil amacı başka bir kategoriye sığmayan web tabanlı formlar,
- Dolandırıcılık: Aldatmadan maddi bir amaç sağlayabilen siteler
- Kumar: Kumarı teşvik yada destekleyen siteler,
- Silahlar: Silah satma amaçlı siteler,
- Hacking: Yasa dışı bilgisayar eğitimleri/öğrenimleri sağlayan siteler,
- Hosting: Kullanıcıların başka bir Dark Net sitesine ev sahipliği yapmasına izin veren Dark Net'in barındırma hizmetleri,
- Mail: Dark Net web tabanlı e-posta ve mesajlaşma servisleri (Mail2Tor ve artık kullanımda olmayan TorMail)

- Pazar: Uyuşturucu, silahlar haricinde kalan hizmetleri satan aracı pazar siteleri,
- Haberler: Güncel olaylar ve Dark Net'e özgü haberler,
- Pornografi: Dünya'daki ve özellikle Batı'daki bölgelerdeki yasalarla uyuşmaması,
- Wiki: Gizli Wiki gibi düzenlenebilir içerik (Owen ve Savage, 2015:4-5), şeklinde ifade edilebilmektedir.

Sınıflandırmalara bakıldığında fiziksel dünyada hukuken ağır suç unsurları olan birçok öğenin yer aldığı görülmektedir. Bunun akabindeyse zihinlerde şu soru canlanmaktadır: Bunca yasal olmayan parametreye rağmen peki Dark Web'de kimler bulunmaktadır?

Yapılan araştırmaların neticesinde Dark Web'de kimlerin bulunduğunu söylemek gerçek manada bir durum tespitidir. Ancak Dark Web'in kullanıcılara sunduğu anonimlik seviyesi birçok güvenlik araştırmacısı ve istihbarat servislerinin bile kendi profilini oluşturmalarını zorlaştırmaktadır. Dolayısıyla da elde edilen veriler yalnızca site içeriği ve popülerliğine bakılarak kullanıcı tabanını ölçmeye yaramaktadır. Forward Looking Threat Research Team olarak kendilerini isimlendiren Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle ve Martin Rösler'in iki yıl içerisinde Dark Web'de birçok web sayfasını taramış, analiz etmiş ve kullandıkları dillere göre sayfaları kategorize etmişlerdir.

Tablo 1.1. :Drk Web'de en çok kullanılan diller :



Bu analiz ise Dark Web kullanıcılarının olabileceği olası bölgelerin açığa çıkmasını sağlamıştır (Cincaglini, vd., 2015:9).

Dark Web İçerisindeki Pazarlar

Silk Road baskının akabinde Dark Web içerisinde yapılan araştırmalar neticesinde,2011 yılında kurulan Black Market Reloaded'ın varlığı tespit edilmiş ve Silk Road'un (satabileceği ürünler sınırlı) aksine her türlü yasa dışı ürünün satışının gerçekleştirildiği tespit edilmiştir. Bu alanda tek olmayan bu iki pazarın yanı sıra: Russian Anonymous Market Place (2012), Sheep Market (Şubat 2013) ve Atlantis Online'ın varlığı açığa çıkmıştır (Bartlett, 2016:280). Silk Road'un satıcılar ve alıcılar arasında daha popüler ve güvenlik güçlerine karşı daha anonim olmasından dolayı Silk Road 2.0 yeniden aktive edilmiştir.

Marketplaces (Today)	Drug Listings	Total Listings	Weapons
Silk Road 2.0	13,648	17,192	No
Agora	7,400	9,158	Yes
Pandora Openmarket	5,249	5,812	No
Evolution	2,623	5,523	Yes
BlueSky Marketplace	1,740	1,833	No
New Markets			
Dark Bay	292	329	No
The Pirate Market	247	367	Yes
Outlaw Market	230	246	No
Tor Bazaar Alpha	205	252	Yes
Black Bank Market	201	239	No
White Rabbit Anonymous MarketPlace	194	256	Yes
TOTAL LISTINGS	32,029	41,207	

Tablo 1.2. Dark Web Markets

Tablo incelendiğinde Dark Web'de anonimlik sayesinde eskisi kapatılmış olsa bile her gün yeni bir pazarın aktif edildiği anlaşılmaktadır. Özellikle bahsi geçen ve birçoğunun varlığı tespit edilemeyen bu pazarları kullanan kişilerin Dark Web üzerinde yasadışı malları alıp satarken anonim kalmasını sağlayan üç temel yapı taşından söz edilmektedir. Bunlar: Tor Network, Bitcoin ve her market tarafından idare edilen pazar forumları (Digital Citizens aliance, 2017:3). Tor ve Bitcoin'in yanı sıra temel olarak ele alınan market forumlarında alıcılar ve satıcılar anonimliği ön planda tutarak satın alacakları yahut satacakları malların elde edilmesine yönelik çeşitli yöntemler geliştirmektedirler.

Genel çerçeve ile bakıldığında Deep Web'de: Kişisel bilgilerin deşifre edilmesi yahut izinsiz olarak ikinci şahıslara satılması, devletlerarası gizli anlaşmaların ifşa edilmesi, devlet politikalarına dair bilgilerin ifşa edilmesi, kara para aklama işlemlerinin gerçekleştirilmesi, çocuk pornografisi, uyuşturucu ve silah ticareti gibi yasa dışı her türlü faaliyetin gerçekleştirilmesi Dark Web üzerinden yapılmaktadır. Tehlikeli ve devletler tarafından- Tor kullanımın Türkiye'de yasaklanması da bu bağlamda değerlendirilmedir- şüpheyle yaklaşılan erişim alanı olan Dark Web ile birlikte başta Bitcoin olmak üzere sanal para birimi ile işlem yapılması ise birçok yasadışı faaliyetin izinin takip edilememesiyle sonuçlanmaktadır. Nca'ın raporunda da belirttiği üzere anonim ödeme sistemleri karanlık web ticaretinin tetikleyici durumundadır (NCA, 2016:7).

SONUÇ

Demokratik olan tüm toplumlarda aşırılık yanlısı terörizm, şiddetin teşvik edilmesi, çocukların istismarı, çocuk pornografisi, dolandırıcılık, kara para aklama, uyuşturucu ve sınırsız silah ticareti başta ahlaki değerler olmak üzere hukuk devletlerinin hepsinde yasalara aykırıdır. Bu bağlamda, internet ve ona bağlı yeni teknolojiler bu ahlaki değerleri ve yasaları yerle bir eden mimariler olarak –Dark Web'in- gayri meşruluğu teşvik edebilir mi? (Moore and Rid, 2016:9) Bu sorudan yola çıkarak gelecekte belki de en önemli sorun, bir toplumun internet kullanıp kullanmadığı değil, hangi versiyonunu kullandığı olacaktır (Erik ve Jared, 2015:96). Bu bağlamda da devletlerin, politikacıların ve karar verici kişilerin Deep Web'in güvenli bilgi sahası dışında kalan Dark Web ile mücadelesi büyük bir önem arz etmektedir. Uzaya insanoğlunun müdahalesinin zorluğu ne kadar ise Siber uzayda da aynı şartların var olduğu gerçekliğinden yola çıkarak devletler, özel sektör ve vatandaşlar arasında sağduyulu iş birliğinin önemi ve temel ahlaki, insan hakları ve evrensel prensiplerin oluşturulması ve geliştirilmesi, bu mücadele de temel yapı taşı görevindedir.

Yaşamlarımızın dijital enformasyon sistemleri ve buna bağlı olarak internet ile iç içe geçmesi arttıkça, her tıkla birlikte bireysel ve topumsal kırılganlıklarımız artmaktadır. Yakın gelecekte daha pek çok ülkenin ve insanın online yaşama katılmasıyla birlikte, bu kırılganlık genişleyecek ve şimdikinden daha karmaşık bir hal alacaktır (Erik ve Jared, 2015:118). Dolayısıyla, internet üzerinde gittikçe artan yasa dışı faaliyetlerin önüne geçmek adına atılan adımlar ülke vatandaşlarının internete olan erişimlerini kısıtlamak yerine bilişim sektörü ile karar vericilerin ortaklaşa geliştirecekleri yapıcı adımlar ve vatandaşların Dark Web ile Deep Web arasındaki

ayrım konusunda bilgilendirilmesi ve bilinç eğitimleri günümüz teknoloji şartları içerisinde yapılacak doğru bir hamle olacaktır.

Siber uzayda devletler, devlet dışı aktörler (özel şirketler) ve kişilerin ortak paydaş/aktör halinde bulunması yasal sınırlamaların etkin çözüm olmadığının/olamayacağının göstergesidir. Dolayısıyla, Deep Web ve Dark Web kavramlarının iç içe geçmesinden kaynaklanan çatışmanın önüne geçilmesi adına siber uzay güvenlik anlayışının etik ahlaki temellere oturtularak yasaklardan ziyade devlet politikası geliştirilerek güvenli hale getirilmesi bu soruna bir çözüm olarak düşünülmelidir. Siber uzayda fiziksel dünyanın dışındaki bir çatışma alanına dönüşen Dark Web'deki yasa dışı faaliyetler sürdüren kişilere karşı yalnızca Tor kullanımının yasaklanmasına dair yapılacak hamlelerin kısa sürede aşılabilir olması, etik ahlaki temellerin atılması vurgusunun en büyük makul argümanı şeklinde karşımıza çıkmaktadır.

Son söz olarak ifade edilmesi gerekir ise, çalışma boyunca karşılaşılan en büyük zorluklardan biri akademik manada beslenebilinecek kaynakların yoksunluğu olarak belirtmek mümkündür. Bunun temel nedenlerini üçe ayırabiliriz: İlk olarak Deep Web ve Dark Web hakkındaki bilgilerin birçoğunun internet ortamında asparagas haberlerden ibaret olması; ikinci olarak çalışma alanının genel itibariyle yazılım mühendisleri, bilgisayar mühendisleri ve veri analizcileri tarafından irdelenebileceği yanılgısının ortaya atılması neticesinde akademik olarak yazınsal ürünlerin ortaya koyulamaması ve son olarak ise devletlerin bu konuda gizlilik esasını gütmesi şeklinde sıralanabilmektedir.

KAYNAKÇA

Alistair Charlton (2014). "Snowden Files Reveal NSA had 'major problems' Tracking Tor Dark Web Users and Cracking Encryption", http://www.ibtimes.co.uk/snowden-files-reveal-nsa-had-major-problems-tracking-tor-dark-web-users-cracking-encryption-1481225, E.T: 11.10.2017.

Andy Beckett, (2009) "The Dark Side of the Internet", https://www.theguardian.com/technology/2009/nov/26/dark-side-internet-freenet. E.T: 14.11.2017

Aydoğan, A. "Tor Network Türkiye'de Engellendi", http://www.webtekno.com/tor-network-turkiye-de-engellendi-h23134.html, E. T: 5.09.2017.

Barry M. Leiner, Vinton G. Cerf, David D. Clark, Robert E. Kahn, Leonard Kleinrock, Daniel C. Lynch, Jon Postel, Larry G. Roberts and Stephen Wolff, (1997)"Brief History of the Internet ", Internet Society.

Jamie Bartlett, (2016). "Dark Net: İnternetin Yer Altı Dünyası", Konyalı, Y. (çev.). Timaş Yayınları, İstanbul. s. 15.

Brett Hawkins, (2016). "Under the Ocean of Internet", The Sans Institue

Cadie Thompson, (2015)."Beyond Google: Everything You Need to Know About the Hidden Internet", Business Insider, http://www.businessinsider.com/difference-between-dark-web-and-deep-web-2015-11. E.T: 11.11.2017.

Craig Labovitz, (2009). "The Dark Web Explained", https://witnessthis.wordpress.com/tag/craig-labovitz/. E.T: 23.11.2017.

Daniel Moore and Thomas Rid, "Cryptopolitik and The Dark Net.", Surival Vol.58 No.1 February-March, 2016.

Digital Citizens Alliance, "Busted, But No Broken The State of Silk Road And The DarkNet Market Places" Digital Citizens Alliance Investigative Report.

Eric Schmidt and Jared Cohen, (2015). "Yeni Dijital Çağ: İnsanların, Ulusların ve İş Dünyasının Geleceğini Yeni Baştan Şekillendirmek", Ü. Şensoy (çev).Optimist Yayın, İstanbul.

Ermiş, Uğur. "Saldırganın Geri Dönüşü: 1. Dünya Savaşı'ndan Siber Uzaya", 10.10.2014. ,https://siberbulten.com/makale-analiz/saldir-birinci-dunya-savasindan-siber-uzaya/, E.T: 2.09.2017.

FBI, “Manhattan U.S. Attorney Announces Seizure of Additional 28$ Million Worth of Bitcoins Belonging to Ross William Ulbricht, Alleged Owner and Operator of “Silk Road” Website”. https://archives.fbi.gov/, E.T: 29.11.2017.

Internet Live States, (2018). Internet Usage & Social Media Statistics. http://www.internetlivestats.com. E.T. 01.01.2018.

Marco Chiappetta, (2016).“Access The Deep Web And Protect Your Privacy Online With The Anonabox”, https://www.forbes.com/sites/marcochiappetta/2016/04/29/access-the-deep-web-and-protect-your-privacy-online-with-the-anonabox/#6a922a6440c2, E.T: 9.12.2017.

NCA, ”National Strategic Assessment of Serious and OrganisedCrime 2016”, E.T: 20.11.2017.

Nicolas Christin, (2012). “Traveling the Silk Road: A Measurement Analysis of A Large Anonymous Online Marketplace”, Carnegie Mellon University Pittsburgh.

Gareth Owen and Nick Savage (2015). The Tor Dark Net”,Chatham House The Royal Institute of International Affairs, September.

Debiel Santos, (2017). “What The Dark Web Is And Isn’t”, Smart Data Collective, http://www.smartdatacollective.com/what-dark-web-and-isn-t/, E.T: 4.09.2017.

Vincenzo Ciancaglini, Marco Balduzzi, Robert McArdle, and Martin Rösler (2015). “Below the Sruface: Exploring the Deep Web”, Forward- Looking Treat Research Team, Trend Micro.

Zack Epstein, (2014). “How to Find the Invisible Internet”, BGR, http://bgr.com/2014/01/20/how-to-access-tor-silk-road-deep-web/.