Dr. Serbakov Márton Tibor*

Kriminalitás a dark weben: illegális piacok, pedofil oldalak, terroristák és az ellenük való küzdelem

az internet a gyors technikai fejlődéssel számtalan lehetőséggel bővült, és mind a szervezett bűnözők, mind a terroristák használják ugyanazokat a technikai adottságokat, mint más felhasználók, csak ők a szabadság és határoknélküliség adottságával visszaélve, azokat illegális céljaikra használják.[3] A kibertér és a különféle informatikai eszközök kiváló lehetőséget kínálnak a szervezett bűnözés fejlődéséhez is, mert ezek használatával a szervezett bűnözői csoportok nem csak egymás között tudnak egyszerűbben kommunikálni, hanem a névtelenségüket is könnyebben tudják megőrizni.[4]

Bevezetés

Jelen tanulmányomban az internet dark webnek, dark netnek, magyarul sötét webnek, sötét netnek (a továbbiakban dark web) nevezett rejtett szegmenséhez kapcsolódó kriminalitást vizsgálom. Egy átfogó képet kívánok nyújtani az internetnek e rejtett és legendákkal övezett rétegén jelen lévő bűnözés természetéről, a fellépés lehetőségeiről és a dark webbel kapcsolatos dilemmákról. Tanulmányomban bemutatom az internet rétegeit, a Tor böngészőt, néhány deep és dark web technológiát, a dark web tartalmait, dark weben alkalmazott bűnüldöző technikákat, néhány műveletet a gyermekpornóoldalak ellen, a dark webes illegális piacokat, megvizsgálom a terroristák dark webes jelenlétét, kitérek a dark webbel kapcsolatos dilemmákra. Zárásként javaslatokat fogalmazok meg. Nagy Zoltán András megállapításaival könnyű egyetérteni: „A számítástechnika, különösen az Internet közvetítésével megjelent és egyre szaporodó, egyre veszélyesebb bűncselekmények valamennyi bűnügyi tudomány számára jelentenek kihívást. A számítógépes környezetben elkövetett bűncselekmények, nemcsak az anyagi büntetőjog számára jelentettek új kihívást, hanem a büntető eljárásjog és a kriminalisztika számára is."[1] A legfontosabb kibertérből érkező fenyegetéseket Berki a következőképp csoportosítja: kiberbűnözés, kiberkémkedés, hacktivizmus, kiberterrorizmus, kiberhadviselés.[2] Nagy továbbá rámutat, hogy

1. Az internet rétegei: a felszíni web, a deep web, a dark web

Az internet mérete az utóbbi évtizedekben rengeteget nőtt. 1991-ben még mindössze egy (info.cern.ch), 2014-re 1 milliárd, mára több mint 1,5 milliárd weboldal található a world wide weben, melyből kevesebb mint 200 millió aktív.[5] Az internet rétegekből áll. A felső réteg a keresőmotorok által könnyen hozzáférhető felszíni web (surface web). Az alsóbb rétegek hatalmasak: A deep web (mély web), azaz a nem indexelt weboldalak száma becslések szerint 400-500-szor nagyobb, mint a felszíni web indexelt, keresheto weboldalai.[6] Más szerzők szerint az internetnek 90%-a a deep web.[7] A dark web a deep web része, melynek tartalmai szándékosan rejtettek. Hozzáféréséhez speciális szoftver szükséges, mint a Tor. A dark web legális és illegális tevékenységek elfedésére egyaránt használható. A visszaélés ad okot fejfájásra a ha-

* Doktorandusz, Pécsi Tudományegyetem Állam- és Jogtudományi Kar.

[1] Nagy Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: Homoki-Nagy Mária – Karsai Krisztina – Fantoly Zsanett – Juhász Zsuzsanna – Szomora Zsolt – Gál Andor (szerk.): Ünnepi Kötet Dr. Nagy Ferenc Egyetemi Tanár 70. Születésnapjára. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged 2018. 755. o.

[2] Berki Gábor: A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon. Nemzetbiztonsági Szemle, 2018. 3. sz. 8. o.

[3] Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula – Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII: TANULMÁNYOK „A BIZTONSÁG RENDÉSZETTUDOMÁNYI DIMENZIÓI – VÁLTOZÁSOK ÉS HATÁSOK" CÍMŰ TUDOMÁNYOS KONFERENCIÁRÓL. Pécsi Határőr Tudományos Közlemények XIII. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs 2012. 221. o.

[4] Gyaraki Réka: A kiberbűncselekmények megjelenése és helyzete napjainkban. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont, Budapest–Pécs 2019. 83. o.

[5] Internet Live Stats https://www.internetlivestats.com./total-number-of-websites/ (2020.03.28.)

[6] Sui, Daniel – Caverlee, James – Rudesill, Dakota: The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. Woodrow Wilson International Center for Scholars, Washington, DC 2015. 4. o. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676615 (2020.03.28.)

[7] Rathod, Digvijaysinh: Darknet Forensics. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2017. Vol. 6. No. 4. 78. o.

tóságoknak és törvényhozóknak, de ahogy a bűnözők támaszkodhatnak a dark web biztosította anonimitásra, úgy a bűnüldöző szervek, a katonaság és a hírszerző szolgálatok is.[8] Fontos leszögezni, hogy a dark weben böngészni önmagában még nem illegális (ám könnyen azzá válhat).[9] A Tor böngésző használata nem ütközik törvénybe, sokan azt online magánéletük megóvására használják: katonaság, rendőrség, újságírók, whistleblowerek[10] (pl. Edward Snowden, Julian Assange). A Tor biztosította anonimitás miatt a dark web bűnözői aktivitás melegágya is, többek között kábítószerrel kapcsolatos bűnözésnek, gyermekpornográfiának, fegyverkereskedelemnek, és bérgyilkosok felbérlésének is (több csoport kínál ilyen szolgáltatást, de tényleges létezésükre nincs bizonyíték.[11]).[12] A dark webet övezik még legendák: állítólag léteznek ún. „red roomok" (vörös szobák), ahol embereket és állatokat kínoznak, erőszakolnak vagy ölnek meg élő közönség előtt, pénzért, és néhány vörös szobában a közönség kívánhat is, hogy hogyan kínozzák és öljék meg az áldozatokat.[13] A vörös szobák nagy valószínűséggel nem többek városi legendánál.[14] Mivel a Tor nemcsak anonimitást biztosít, hanem még a tartalomszűröket is kikerüli, így használatával akár Kínából is elérhető – többek közt – az ott feketelistára tett YouTube is.[15] Moore és Rid szerint az illegális és nem illegális Tor weboldalak abban élesen különböznek, hogy a legitim oldalak majdnem mindig azonosították a kezelőiket, miközben az illegális rejtett szolgáltatások majdnem sosem tették azt.[16] 1994-ben Jill Ellsworth alkotta meg az „invisible web" (láthatatlan web) kifejezést, ezzel utalva az információra, ami láthatatlan volt az abban az időben használt konvencionális keresőmotorok keresései számára. Később, 2001-ben a webtudós Michael K. Bergman alkotta meg a „deep web" kifejezést a „The Deep Web: Surfacing the Hidden Value"[17] című tanulmányában. Bergman deep web meghatározása nem különbözött Ellsworth invisible webjétől, de kerülte azt a kifejezést, mert az ő fő célja a deep web oldalak azonosítására és azok keresésre szolgáló automatizált eszközök felfedezése volt, annak érdekében, hogy ezek a láthatatlan oldalak láthatóvá váljanak a felszíni weben. Továbbá fel akarta mérni a deep web méretét és minőségileg jellemezni a tartalmait. Mivel Bergman tanulmánya volt az első átfogó invisible/deep web kutatás, és mivel a tanulmány híressé vált a webkutatók közösségén belül, a deep web kifejezés győzedelmeskedett az invisible web kifejezés felett, a web nem indexelt forrásaira való utalásban.[18] Dilipraj a 'deep web' definícióját a következőképpen határozza meg: „Az információs tartalom az interneten (weboldalak, dokumentumok, fájlok, képek etc.) amik: hozzáférhetetlenek a konvencionális keresőmotorok általi közvetlen kereséseken keresztül; amikhez csak célzott keresésekkel vagy kulcsszavakkal lehet hozzáférni; amelyek nem indexeltek vagy nem indexelhetőek a konvencionális keresőmotorok által; amelyek biztonsági mechanizmusok által védettek, mint a login ID-k, jelszavak, tagsági regisztrációk és díjak. Röviden: „deep webnek" vagy „invisible webnek" vagy „hidden webnek" nevezzük az információs tartalmat az interneten, amely nem hozzáférhető közvetlenül konvencionális keresőmotorokon keresztül, hanem egy célzott megközelítést igényel."[19]

2. A Tor böngésző

A világot az internet egy globális entitássá változtatta. Ez az összeköttetés viszont a magánéletbe kerül. Minden internetkliensnek van egy egyéni azonosítója, Internet Protocol cím (IP cím) formájában, ami lefordítható a lokációjára a helyi internetszolgáltató (Internet service provider ISP) segítségével. A magánélet hiánya komoly implikációkkal jár kifejezetten újságírók, szabadságharcosok és szimpla állampolgárok számára is. A magánélet hiánya vezetett az anomin kommunikációs hálózatok (anonymous communication networks, ACN-ek) használatához, melyek számos technikai megoldással rejtik el a kliens IP címét. Az ACN-ek közé tartozik a Tor, a Java anonymous proxy (JAP), Hotspot Shield és UltraSurf etc. A Tor az egyik legnépszerűbb ACN.[20] Népszerű még az I2P és a Freenet. Ezeknek a

[8] Finklea, Kristin: Dark Web. Congressional Research Service, Washington DC, 2017. 1. o. https://www.fas.org/sgp/crs/misc/R44101.pdf (2020.03.28.)

[9] Kiberbűnözés és a virtuális tér veszélyei – interjú az Internet Világnapja alkalmából. https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja (2020.03.28.)

[10] „Szó szerinti jelentése 'sípfújó', és olyan személyekre használják, akik arra hívják fel a figyelmet, ha egy intézmény vagy szervezet törvénytelenül működik, vagy akár csak rosszul irányítják. A whistleblowerek tipikusan belülről jönnek, bizalmas értesüléseik munkájukból vagy a szervezetben betöltött más szerepükből következően vannak – léteznek azonban kívülről jövő whistleblowerek is, akik hosszas adatgyűjtés, nyomozás után jutnak a leleplező adatokhoz. A whistlerblowereket sok helyen a törvény is védi." Forrás: https://www.nyest.hu/hirek/aki-megfujja-a-sipot (2020.03.28.)

[11] Moore, Daniel – Rid, Thomas: Cryptopolitik and the Darknet. Survival: Global Politics and Strategy, 2016. Vol. 58. No. 1. 24. o.

[12] Tor And The Deep Web: Everything You Secretly Wanted To Know. https://www.whoishostingthis.com/blog/2017/03/07/tor-deep-web/ (2020.03.28.)

[13] What is the Deep Web? The Definitive Guide [2020]. https://www.thedarkweblinks.com/what-is-the-deep-web/ (2020.03.28.)

[14] Harper, Ivy: Dark Web Red Rooms: Urban Legend or Worst Content on the Deep Web? https://darkwebjournal.com/dark-web-red-rooms/ (2020.03.28.)

[15] Devecsai János: Kábítószerek és bérgyilkosok a netről https://www.digitalhungary.hu/konferenciak/evolution/Kabitoszerek-es-bergyilkosok-a-netrol/5056/ (2020.03.28.)

[16] Moore–Rid: i. m. 24–25.o.

[17] Bergman, Michael K.: The Deep Web: Surfacing Hidden Value. The Journal of Electronic Publishing, 2001. Vol. 7 No. 1.

[18] Dilipraj, E.: Terror In The Deep And Dark Web. Air Power Journal, 2014. Vol. 9. No. 3. 126. o.

[19] „The information content on the internet (web pages, documents, files, images, etc) which are: inaccessible through direct queries in the conventional search engines; 1 which can be accessed only through targeted queries or keywords; which are not indexed or which are unable to be indexed by the conventional search engines; which are protected by security mechanisms like login IDs, passwords, membership registrations and fees. In short, the information content on the internet which cannot be accessed directly through conventional search engines but requires a targeted approach is called the 'deep web' or 'invisible web' or 'hidden web'." saját fordítás. Dilipraj: i. m. 126–127. o.

[20] Saleh, Saad – Qadir, Junaid – Ilyas, Muhammad U. Shedding Light on the Dark Corners of the Internet: A Survey of Tor Research. Journal of Network and Computer Applications, 2018. Vol. 114. 1. o.

hálózatoknak az architektúrája miatt nehéz a méretét felbecsülni, de a Tor tűnik a legnagyobbnak, távoli második az I2P, a többi jelentősebb kisebb méretben és népszerűségben.[21] A dark web használatához nem szükséges speciális hardvert vagy szoftvert várásolni. Ahhoz elegendő egy ingyenes böngészőt letölteni, például a Tort.[22] Tor egy ingyenes, nyílt forráskódú (open source) szoftver, ami segít az anonimitást megőrizni az online térben. A Tor böngésző sokban hasonlít egy szokványos webböngészőre, a különbség, hogy a Tor az internethez a Tor hálózaton keresztül csatlakoztatja a felhasználót. A Tor használatával az internetforgalom egy szerverek hálózatán van véletlenszerűen irányítva, mielőtt az eléri a végső célját, azért, hogy a felhasználó lokációja és identitása védve maradjon. A Tor „The Onion Router" (A Hagyma Böngésző) neve arra utal, hogy a Tor úgy védi a felhasználó adatait, hogy több rétegű titkosításba foglalja, mint egy hagymát.[23] Léteznek dark web keresőmotorok is, de a legjobbak is küszködnek a folyamatosan változó színtér miatt, ezért az azokkal való keresés élménye az 1990-es évek netes kereséseire emlékeztet. Még az egyik legjobb keresőmotor, a Gram keresési eredményei is gyakran repetitívek és irrelevánsak. Opció még az link listák használata, mint The Hidden Wiki, de az ilyen listákon található indexek is gyakran hibaüzenetet adnak ki. A leghíresebb dark web keresőmotor jelenleg a Duck Duck Go. A Tor dark web oldalai címei .onion-nal végződnek, és kevert az elnevezési rendszerük, ami miatt a létrejött URL-ek megjegyezhetetlenek.[24] A weboldalak a dark weben tehát nem úgy végződnek, hogy „.com", vagy „.org" vagy más gyakori domainvégződések, hanem „.onion" vagy „.i2p." a domainvégződésük, és gyakran betűk és számok hosszú sorából állnak. [25] Ha valaki bizonyos lépéseket tesz annak érdekében, hogy az online azonosságát elfedje, például Tor használatával, vagy ha egyáltalán utánanéz más lehetőségeknek, mint a Windows operációs rendszer, azzal az NSA (National Security Agency, Nemzetbiztonsági Ügynökség) általi megfigyelést kockáztatja. Ha valaki az Egyesült Államokon, Kanadában, az Egyesült Királyságon vagy az ún. Five Eyes[26] ország egyikén kívül van, amely az NSA-val együttműködik a felügyeleti erőfeszítéseiben, akkor a Tor-webhelyének felkeresése automatikus ujjlenyomatot hoz létre nála. Más szavakkal: a magánélet fokozására szolgáló módszerek szimpla keresése az Egyesült Államokon kívülről olyan ellenőrzésre és felügyeletre méltó cselekedet, amely az NSA XKeyscore-ja futtatását indítja el. Továbbá elég a nyílt forráskódú Linuxnak szentelt Linux Journal fórumot meglátogatása, hogy valakit ujjlenyomatozzanak, függetlenül attól, hogy hol él, mert az XKeyscore forráskódja azt extrémista fórumként jelöli meg. A Tails operációs rendszer keresése is ezzel az eredménnyel jár.[27] 2014-ben egy XKeyscore nevű NSA program forráskódjának vizsgálata (melyet a Snowden leaks fedtek fel), azt mutatta, hogy ha bármely felhasználó szimplán megkísérli letölteni a Tort, az automatikusan ujjlenyomatozva lett, mely lehetővé teszi az NSA számára, hogy megismerhesse a Tor felhasználók millióinak azonosságát.[28] Az NSA az XKeyscore használatával gyűjti be és analizálja az internet adatokat. Ezzel az eszközzel az NSA a felhasználó minden internetes aktivitását felügyelheti.[29]

3. Deep web és dark web techológiák:

Az anonimitás a kiberbűnözés egyik sarokköve, mely ma már szabadon hozzáférhető technológiákkal is megvalósítható.[30] Néhány deep web és dark webhez kötődő technológia a teljesség igénye nélkül: VPN[31] Torral: Azért, hogy elrejtsék, hogy Tort használnak, néhányan VPN-t használnak a Tor mellett, ami egy magasabb szintű biztonságot nyújt. Invisible Internet Project (I2P): Ez egy névtelen átfedő hálózat (overlay network) (hálózat a hálózatban) ami arra való, hogy védje a kommunikációt a dark webes felügyelettel és harmadik személyek (mint az internetszolgáltatók (ISP-k, Internet Service Provider)) megfigyelésével szemben. Az I2P a kommunikáció és online aktivitás titkainak megóvására használatos. Az I2P használható e-mailezéshez, web böngészéshez, blogoláshoz, fórumozáshoz, weboldal hosztolásához, fájlmegosztáshoz és valós idejű chateléshez. Free Anonymous Internet (FAI): A Free Anonymous Internet project (FAI) egy decentralizált deep webszolgáltatás, ami blockchain

[21] Moore–Rid: i. m. 15. o.

[22] Lund, Brady – Beckstrom, Matthew: Casting Light on the Dark Web: A Guide for Safe Exploration. Rowman & Littlefield Publishers, London 2019. 41.o.

[23] https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/ (2020.03.28.)

[24] Razali, Nuruddin Bin – Suradi, Nur Razia binti Mohd: A Nest for Cyber Criminals:The Dark Web. IEEE 2019. 2. o. https://www.academia.edu/40783401/A_nest_for_cyber_criminals_-the_dark_web (2020.03.28.)

[25] Gehl, Robert: Illuminating the 'dark web'. https://theconversation.com/illuminating-the-dark-web-105542 (2020.03.28.)

[26] „Kanada, Ausztrália, Új-Zéland, az Egyesült Királyság (UK) és az Egyesült Államok (USA) tagjai a Five Eyes hírszerző közösségnek, a világ legexkluzívabb hírszerző klubjának. Ez az együttműködési kapcsolat nem monolitikus, de minden bizonnyal összetartóbb, mint általánosságban ismert. A második világháborúban az Egyesült Királyság és az Egyesült Államok közötti hírszerzési együttműködésből nőtt ki, a hidegháború alatttovább érett, és ma továbbra is valamennyi tag nemzeti érdekeinek védelmét szolgálja." Forrás: Cox, James: Canada and the Five Eyes Intelligence Community. Canadian Defence and Foreign Affairs Institute, Calgary 2012. 4. o.

[27] Patrick Tucker: „If You Do This, the NSA Will Spy on You" Defense One, July 7, 2014 https://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/ (2020.03.28.)

[28] Weimann, Gabriel: Going Darker? The Challenge Of Dark Net Terrorism. Wilson Center, Washington, DC 2018. 8. o.

[29] Zetter, Kim: Use privacy services? The NSA is probably tracking you. https://www.wired.co.uk/article/nsa-targeting-tor-users (2020.03.28.)

[30] Szász Antónia: A kiberbűnözés társadalmi kontextusa. In: Kovács Janka – Kökényessy Zsófia – Lászlófi Viola (szerk.): A normán innen és túl. ELTE BTK Történeti Kollégium, Budapest 2017. 105. o.

[31] VPN használatával (a Virtual Private Network, virtuális magánhálózat rövidítése) biztosítható, hogy a számítógép ne legyen követhető. A következőképpen működik: a számítógép az internetszolgáltató helyett egy VPN-kiszolgálóhoz csatlakozik egy biztonságos, titkosított kapcsolaton keresztül. Ezután a VPN-kiszolgáló csatlakozik a keresett webhelyhez. Ott a szokásos módon rögzítik a látogatás adatait, azonban a VPN-kiszolgáló IP-címe, és nem a saját számítógép IP-címe alapján. Forrás: Mire jó a VPN? Valóban anonim böngészést nyújt! https://www.vpnszerver.hu/mire-jo-a-vpn/ (2020.03.28.)

technológiát használ a megszokott World Wide Web egy privát, biztonságos, peer-to-peer alternatívájának létrehozására. A FAI-nak saját digitális fizetőeszköze van, ami a bitcoin kódon alapul; lehetővé teszi a felhasználóinak a saját médiatartalmaik közzétételét és a mások által közzétett tartalom biztonságban történő böngészését. Egy beépített decentralizált piaca is van. Free Net: A Freenet egy ingyenes szoftver, ami lehetővé teszi az anonim fájlmegosztást, „freesite-ok" (weboldalak, amik csak a Freeneten érhetőek el) böngészését és létrehozását, chatelést fórumokon, anélkül hogy a cenzúrától félnie kellene a használónak. A Freenet decentralizált, hogy kevésbé legyen sebezhető a támadásokkal szemben, és rendkívül nehéz lekövetni, ha „darknet" módban használják, ahol a felhasználók csak a barátaikkal lépnek kapcsolatba. A Freenet csomópontok általi kommunikáció titkosítással ellátott, és más csomópontokon továbbítódik, hogy rendkívül nehezen lehessen meghatározni, ki kéri az információt és annak tartalmát. A ZeroNet egy új rendszer, mely torrent technológián alapul, Bitcoin titkosítással kombinálva, mely még nem igazán fejlett, de ígéretesnek tűnik a jövőben.[32] A ZeroNet magyar találmány, megalkotója Kocsis Tamás, aki a következőként fogalmaz a hálózatról: „Olyan hálózatot fejlesztek, amelyben a weboldalakat a látogatók maguk üzemeltetik, nincs szükség szolgáltatókra vagy központi szerverre. Magyarul nem kell fizetni azért, hogy egy oldal felkerüljön a hálózatra. A felhasználó készít egy weboldalt, ami letöltődik a látogatók gépére, innentől pedig ők is teljes értékű kiszolgálói lesznek az oldalnak. A felhasználók egymás rendszeréről töltik le ezeket az oldalakat; még internetkapcsolatra sincs szükség, hogy valaki dolgozzon a saját oldalán. A hálózat előnye, hogy biztonságos, mert a megtámadása nagyon időigényes, és óriási kapacitásra volna szükség hozzá."[33] A koronavírus pandémia miatt sokkal többen dolgoznak otthonról, ezért a biztonságos otthoni munkavégzés miatt VPN-t használók tábora sok országban hatalmas növekedést mutat. A NordVPN VPN szolgáltató adatai szerint 2020. március 11. óta a VPN technológiájának globális használata 165%-os növekedést mutat.[34]

4. A dark web tartalmai

Barratt, Aldridge és Maddox öt kategóriába sorolja a dark web tartalmait: 1. Az első kategóriának „szórakoztatási értéke" van, ezek a tartalmak a felszíni weben szigorúan szabályozottak, mint a pornográfia. 2. Egy másik kategóriába magára a dark webre utaló tartalmak tartoznak: hogy kell használni a Tor-t, a rejtett szolgáltatásokat, hogy kell titkosítást használni a technikai anonimitás eléréséhez, szokások és gyakorlatok a társadalmi anonimitás eléréséhez. 3. A harmadik kategóriába az illegális, vagy szigorúan szabályozott árucikkekre specializálódó piacok és kereskedelmi vállalkozások tartoznak, mint a kriptopiacok, melyek kábítószer-kereskedelmet, fegyverkereskedelmet vagy más digitális árucikkek, lopott hitelkártya adatok vagy hamis magánokiratok kereskedelmét teszik lehetővé. 4. A negyedik kategóriába tartoznak a scam oldalak, adathalász (phishing) oldalak, átverések, csaló szolgáltatások. 5. Az ötödik kategóriába tartoznak a szolgáltatások, melyekben a felhasználók határozzák meg a kommunikáció vagy a Tor használatának céljait és tartalmát, mint az anonim e-mail-programok, chatszolgáltatások, közösségi hálózatok, nyílt témájú fórumok, és peer-to-peer (egyenrangú felek közötti) fájlmegosztás. Ezekben megjelenhetnek az előző pontokban tárgyalt tartalmak, de ezek egy felügyelettől, politikai beavatkozástól vagy cenzúrától mentes teret is jelentenek. Tévhit, hogy a dark web a hatóságok számára áthatolhatatlan lenne, amit az is mutat, hogy egyre több kábítószer kriptopiac és dark web pedofil hálózat résztvevőit és vezetőit tartóztatják le. A hagyományos bűnüldöző technikák, köztük a fedett nyomozó alkalmazása is sikeresek lehetnek a digitális környezetben.[35] Moore és Rid 2015. január és március között egy website keresőrobottal végzett kutatása során 300 000 címet vizsgált meg, és arra az eredményre jutott, hogy a Tor rejtett szolgáltatásain található weboldalak leggyakrabb használata bűnözői irányultságú. Ezek közé tartozik a kábítószer-kereskedelem, a jogosulatlan pénzügyi tevékenység és az erőszakos, a gyermeket és állatokat szerepeltető pornográfia. 2015 eleji kutatásuk során még arra jutottak, hogy majdnem hiányzik az iszlám extremizmus a Tor rejtett szolgáltatásain (2015 után ez változott,[36] erről bővebben később), csupán maréknyi aktív oldalt találtak. Moore és Rid a pénzügyi kategóriát 3 prominens alkategóriára osztja: Bitcoin-alapú pénzmosási módszerek, illegálisan szerzett bankkártyákkal és lopott felhasználói fiókokkal való kereskedelem, és hamis pénzzel való kereskedelem. A Tor dark webén a kábítószerek széles tárháza a leggyakoribb árucikk. Sokféle eladó létezik, az egy oldallal rendelkezőktől a közösségi piacokig, mint a hírhedt Agora. Kapható marihuána, kokain, metamfetaminok, LSD több fajtája, továbbá más specializált piacokon anabolikus szteroidok és Viagra-szerű gyógyszerek. Sok eladó szélhámosnak tűnik Rid és Moore szerint. A pornográf tartalom az egyik legaggasztóbb. Website-ok szolgáltatnak linkeket videókhoz, amik szexuális erőszakot, állatokkal folytatott közösülést és gyemekpornográfiát mutatnak. Több fétisek megvitatására és megosztására szakosodott ak-

[32] Rathod: i. m.: 78. o.

[33] Valahovits Szilvia Éva: Magyar találmány: cenzúrázhatatlan internet. http://valasz.hu/techvilag/egy-magyar-fiatalember-feltalalta-a-cenzurazhatatlan-internetet-123507 (2020.03.28.)

[34] Palmer, Danny: VPN use surges as coronavirus outbreak prompts huge rise in remote working https://www.zdnet.com/article/vpn-use-surges-as-coronavirus-outbreak-prompts-huge-rise-in-remote-working/ (2020.03.28.)

[35] Barratt, Monica – Aldridge, Judith – Maddox, Alexia: The SAGE Encyclopedia of the Internet – Dark Web. SAGE Publications, Ltd., Thousand Oaks 2018. 3-4. o.

[36] Weimann, Gabriel: Going Darker? The Challenge Of Dark Net Terrorism. Wilson Center, Washington, DC 2018. 3. o.

tív közösség található. Más illegális szolgáltatások között találhatók a hamis okiratok, lopott, vagy más illegális módon szerzett felszerelések, lőfegyverek, rosszindulatú szoftverek, amik személyes felhasználói fiókok begyűjtésére specializálódtak vagy denial-of-service (DoS) támadásokra. Több oldal bérgyilkos szolgáltatást kínál, de nincs jele annak, hogy bárki bármikor is sikeresen kapcsolatba lépett volna már velük. Sok oldalt az „egyéb" kategóriába sorolt Moore és Rid, melyek magáról a dark webről szóltak. Ezek a „meta oldalak" közé hoszting szolgáltatások és oktatóanyagok tartoznak a Tor használatáról. Az „egyéb" kategóriába tartoznak még a személyes blogok, újságírók drop site-jai, és más ártalmatlan szolgáltatások. A legtöbb oldal a „none", azaz „semmi" kategórába került. A félresikerült és tartalom nélküli weboldalak tömkelege jól mutatja, mennyire megbízhatatlan egy rejtett-szolgáltatásplatform a legtöbb felhasználó számára. Sok oldal nem volt hozzáférhető a home page-én túl, mert a felhasználó bejelentkezését kérték, ezért ezek legális vagy illegális volta nem tiszta.[37] Mirea, Wang és Jung egy empirikus kutatás során kvalitatív interjúkkal végzett online felmérést a dark weben. A felmérés során a résztvevők 10 kérdésre válaszoltak különböző dark webes fórumonkon. A szerzők elismerik, hogy jobban szerettek volna standard félig strukturált face-to-face interjúkat végezni, de ezt az opciót elvetették, mivel tiszteletben kellett tartani az etikai bizottságuk által felvetett különféle etikai szempontokat és a dark web anonim kultúráját. Mirea, Wang és Jung a 10 interjúkérdést egy online kérdőívvé alakította a Bristol Online Survey (BOS) tool használatával (https://www.onlinesurv eys.ac.uk). A linket a felméréshez egy meghívó levélbe ágyazták be, amit a következő négy dark webes fórumra töltöttek fel: The Hub (thehub7gqe43miyc.onion); Intel Exchange (rrcc5uuudhh4oz3c.onion); Darknet Central (2u7kil26qazmrmb6.onion); DarknetM Avengers (avengerfxkkmt2a6.onion). Azért ezeket a fórumokat választották, mert ezek mindennapi általános társalgásra, és nem specifikus célokra vannak kialakítva.[38] Felmérésük eredményeként arra jutottak, hogy a dark web nem olyan „dark", ahogy az a szakirodalomból tűnik. Úgy vélik, a dark web nem kriminogén. A felmérésben részt vevők arról kovencionális nyílt forrásokból szereztek tudomást, és a dark web használata során a szólásszabadság a fő húzóerő, ami miatt rendszeresen használják azt mindennapi tevékenységek végzésére. Ugyan a szerzők nem tagadják, hogy a dark web komoly biztonsági kockázatot jelent, és komoly kutatást igényel. Úgy gondolják, a darknet nem egy olyan közösség, ahol a bűnözés a norma, hanem egy technológiai platform, amit különböző egyének különböző célokra használnak.[39] Úgy vélem, a dark web fórumain végzett ilyen felmérés, de még a face-to-face interjú sem festhet reális képet a dark web kriminogén vagy nem kriminigén voltáról, mert e fórumok használói természeten nem, vagy kisebb valószínűséggel fognak negatív képet festeni önmagukról, magukat nem fogják inkriminálni. A dark web kriminogén voltáról úgy vélem reálisabb képet kaphatunk például keresőrobotok (web crawler) használatával. Moore és Rid kutatása[40] alapján a dark web egyértelműen kriminogén képet mutat. Véleményem, hogy a dark web kriminogén.

5. Bünüldöző technikák a dark webes kriminalitással szemben

A bűnüldöző szervek számos technika alkalmazásával képesek a dark weben a bűnözőket elkapni: fedett műveletekkel, hackeléssel, OSINT alkalmazásával, tömeges adatgyűjtéssel, a lefoglalt adat átvizsgálásával (pl. dark webes kereskedő letartóztatása vagy piac lefoglalása esetén), a pénzmozgások főleg a Bitcoin útjának) nyomon követésével, a postai rendszer követésével (pl. kábítószer vásárlása esetében).[41] Nyeste és Szendrei beszámol arról, hogy a dark weben való információgyűjtés külön problémát jelent, de itt is megvannak a speciális keresőmotorok és egyéb lehetőségek, amelyek által az információk kinyerhetőek (célszoftverek: például Tor, I2P, Freenet, Deepdotweb.com, Reddit, GRAMS). Az OSINT lehetőséget nyújt a bűnös tevékenységek feltérképezésére, szervezett bűnözői csoportok beazonosítására, bomlasztására, bűncselekmények megelőzésére, korábban elkövetett cselekménnyel kapcsolatos információk beszerzésére, bővítésére, a célszemély kilétének megállapítására, a célszeméllyel kapcsolatos adatok bővítésére, a bűncselekmény elkövetési módjának megállapítására, tanulmányozására.[42] A dark weben végzett munkájuk során a bűnüldöző szerveknek elengedhetetlen fontosságú szakértőket bevonnia.[43] Példák jelenleg használt módszerekre dark webes bűnözők elfogásása során: Memex: A U.S. Defense Advanced Research Projects Agency (DARPA) kifejlesztette a Memex nevű keresőmotort, ami segít a Department of Defense-nek (Védelmi Minisztériumnak) az emberkereskedelem elleni küzdelemben és illegális tevékenységek felfedésében a dark weben. A Memex tradícionális keresőmotorokkal nem hozzáférhető oldalak millióin szánt végig és indexeli azokat, köztük több ezer olyat, melyek csak dark web böngészőkkel találhatóak meg. A Memex nem fedi fel az IP címeket vagy a dark web használók azonosságát, de analizálja a tartalmat, mintákat és kapcsolatokat fedez fel, amiket a bűnüldöző

[37] Moore–Rid: i. m. 18-24. o.
[38] Mirea, Mihnea – Wang, Victoria – Jung, Jeyong: The not so dark side of the darknet: a qualitative study. Security Journal , 2019. Vol. 32. 107. o.
[39] Uo. 114. o.
[40] Moore–Rid: i. m. 7–38. o.
[41] Cox, Joseph: 7 Ways the Cops Will Bust You on the Dark Web. https://www.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web (2020.03.28.)
[42] Nyeste Péter – Szendrei Ferenc: Nyílt forrású információszerzés a bűnüldözésben. Nemzetbiztonsági Szemle, 2019. 7. évf. 2. sz. 66. o.
[43] Kehoe, Shawn R.: The Digital Alleyway: Why the Dark Web Cannot Be Ignored. https://www.policechiefmagazine.org/the-digital-alleyway/ (2020.03.28.)

szervek lekövethetnek és visszanyomozhatnak a használóhoz. A DARPA szerint a Memexszel célja nem a dark web de-anonimizálása, hanem az emberkereskedelem elleni küzdelem. Hálózati nyomozási technikák (Network Investigative Techniques): 2011–2012-ben egy „Operation Tornado" fedőnevű nyomozás során az FBI egy NIT nevű módszert alkalmazott legalább 25 személy IP címének a feldefésére, akik gyermekpornográfiát tartalmazó oldalokat látogattak a dark weben. A nyomozás Hollandiában indult. Hollandia nemzeti rendőrségének szakemberei írtak egy web crawlert (keresőrobotot), ami Tor weboldalak után kutatta át a dark webet. A hatóságok le tudták szűkíteni az oldalakat azokra, amik a gyermekpornográfiához kapcsolódtak, és végül felfedhették egy „Pedoboard" nevű oldalnak az igazi IP címét, Bellevue, Nebraskában. Miután megkapta az információt, az IFB le tudta nyomozni Aaron McGrathot, aki három gyermekpornó oldalnak volt gazdája.[44] A TOR által biztosított anonimitás sűrű rétegeinek áthatolására FBI egy Metasploit nevű applikációt használt az „Operation Torpedo" során.[45] Hagyományos technikák: Az alkotmányos korlátozások ellenére a bűnüldöző szervek szabadon folytathatnak le nyomozást a hagyományos módokon, tradicionális technikákkal. Például a bűnözői körökbe történő beszivárgás fedett nyomozókkal, és személyek követése nyilvános helyeken mind engedélyezett. 2014 novemberében az „Operation Onymous" műveletet rejtett Tor szolgáltatások tucatjainak lefoglalásához vezetett. Miközben ismeretlen, hogy a hatóságok hogyan tudták az oldalakat lekapcsolni, biztonsági szakértők spekulációja szerint kormányzati hackerek „denial-of-service attacks-t" (DDoS támadásokat) alkalmazhattak, amik elárasztják a Tor relay-eket szemétadattal, hogy a célzott oldalakat olyan Tor relay-ek használatára kényszerítsenek, amiket megfigyeltek, ezáltal lekövetve az IP címüket. De lehetséges, hogy a hatóságok a rajtaütéshez tradicionális technikákat, mint informátorokat vagy fedett nyomozókat alkalmaztak. A Silk Road esetében a hatóságok szerint Ulbricht saját hibái vezettek az elfogásához, és nem volt szükség illegális cselekményekre vagy kifinomult beszivárgási módszerekre, a drogbáró elfogásához. [46]

A dark web vizsgálatára a Memex mellett alkalmas az Apache Tika nevű szoftver is.[47] Az Apache Tika toolkit (eszközkészlet) több mint ezer különféle fájltípust (mint PPT, XLS és PDF) észlel és von ki azokból metaadatokat és szöveget. Ezek a fájltípusok egyetlen interfészen keresztül értelmezhetők, így a Tika hasznos lehet a keresőmotorok indexelésében, tartalomelemzésben, fordításban és még sok másban.[48] A BlackWidow egy nagymértékben automatizált moduláris rendszer, mely valós időben és folyamatosan figyeli a dark web szolgáltatásokat, és az összegyűjtött adatokat egyetlen elemzési keretben egyesíti. Gépi fordítási technikák felhasználásával a BlackWidow képes a fórumok és a felhasználók közötti kapcsolatokat vizsgálni, a nyelvi korlátok ellenére is. A fórumok között jelentős átfedés mutatkozik, még különböző nyelveken is. A valós idejű információgyűjtés potenciálját szemlélteti Schäfer, Strohmeier, Liechti, Fuchs, Engel és Lenders egy hét darab dark webes fórumon és a nyílt interneten végzett tanulmány elvégzésével. A tanulmányban megmutatják, hogy a BlackWidow képes threadek, szerzők és tartalmak kinyerésére a Dark Web fórumokból, és tovább dolgozza fel őket a kiberbiztonság szempontjából releváns információ létrehozása érdekében.[49]

6. Műveletek gyermekpornóoldalak ellen

A piacokon kívül a dark web otthona még gyermekpornográfiának is.[50]

A már említett 2011-es Operation Torpedo során Hollandia National High Tech Crime Unitja kezdett nyomozásba dark webes gyermekpornográfia oldalak után. A nyomozás során tudomásukra jutott és arról informálták is az FBI-t, hogy Nebraskában található egy szerver, amely hosztolja ezeket az oldakat. Az FBI lekövette a szerver IP címét Aaron McGrathhoz, akit később le is tartóztattak, és a szervereket lefoglalták.[51] 2013-ban az FBI lefoglalta a Freedom Hosting-ot, ami egy website hoszting szolgáltatás volt a Tor hálózaton, mely több mint 40 gyermekpornóoldalnak, és még további nem gyermekpornóhoz kapcsolódó oldalaknak volt otthona. Amikor az FBI az oldal felett átvette az irányítást, megfertőzte egy malware-rel, amit arra fejlesztettek, hogy a látogatókat azonosítsa. A malware egy Firefox biztonsági rést használt ki, hogy a fertőzött gépek felfedjék a valós IP címüket az FBI számára. Mint az Operation Torpedo esetén, az FBI akciója a Freedom Hosting ellen az összes fűződő weboldal látogatóit célozta, mind az illegális gyermekpornóoldalakét és a legitim vállalkozásokét.[52] Az Operation Pacifier során az FBI egy Playpen nevű közel 215 000 tagot számláló dark weben működő gyermekpornó weboldal után folytatott nyomozást. Az FBI a nyomo-

[44] Vogt, Sophia Dastagir: The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. Santa Clara Journal of International Law, 2017. Vol. 15. No. 1. 114–115. o.

[45] Sui–Caverlee–Rudesill: i. m. 10. o.

[46] Vogt: i.m. 115–117. o.

[47] Mattmann, Christian: Searching deep and dark: Building a Google for the less visible parts of the web. https://theconversation.com/searching-deep-and-dark-building-a-google-for-the-less-visible-parts-of-the-web-58472 (2020.03.28.)

[48] https://tika.apache.org/ (2020.03.28.).

[49] Schäfer, Matthias – Strohmeier, Martin – Liechti, Marc – Fuchs, Markus – Engel, Markus – Lenders, Vincent: BlackWidow: Monitoring the Dark Web for Cyber Security Information. In: T. Minárik – S. Alatalu – S. Biondi – M. Signoretti – I. Tolga – G. Visky (szerk.): 2019 11th International Conference on Cyber Conflict: Silent Battle. NATO CCD COE Publications, Tallinn 2019. 3. o.

[50] What is the Deep Web? The Definitive Guide [2020]. https://www.thedarkweblinks.com/what-is-the-deep-web/ (2020.03.28.)

[51] Finklea, Kristin: Law Enforcement Using and Disclosing Technology Vulnerabilities. Congressional Research Service, Washington DC, 2017. 3. o. https://fas.org/sgp/crs/misc/R44827.pdf (2020.03.28.)

[52] Uo. 4. o.

zás során megállapította, hogy a Playpent hosztoló számítógép szerver Észak–Karolinában volt található. 2015 februárjában az FBI lefoglalta a szervert, és közel két héten át működtette tovább az oldalt egy virginiai szerverről. Egy Virginia District Court (Kerületi Bíróság) bíró kutatási parancsot adott ki, ami lehetővé tette a hatóságoknak, hogy NIT-et alkalmazzanak a Playpen-hez hozzáférő számítógépek tényleges IP címeinek azonosítására. A NIT használatával az FBI kb. 1300 IP címet tudott felderíteni és végül azokat személyekhez visszavezetni.[53] A Welcome to Video pedofil oldal 2015 júniusában indult el, és 2018 márciusáig működött, amíg a hatóságok le nem kapcsolták. Az oldal üzemeltetője a dél-koreai Jong Woo Son volt. Az oldal eltávolítása és Son elleni vádemelés mellett a hatóságok világszinten továbbá még összesen 337 Welcome to Video felhasználót is letartóztattak 23 amerikai államban, Washington DC-ben, és 11 másik országban. Az akció eredményeképpen 23 gyermeket sikerült megmenteni, akiket az oldal résztvevői használtak ki. A hatóságok 8 TB (!) gyermekpornóvideót foglaltak le a nyomozás és az oldal eltávolítása során, amik több mint 250 000 egyedi videót tettek ki. Az oldal Bitcoinban szedte a díjait. Minden felhasználónak egyéni bitcoin wallet címet adott a felhasználói fiók létrehozásakor. Az oldal eltávolítása azért is figyelemre méltó, mert a nyomozás nem hackelésre, vagy titkosított kommunikáció megfigyelésére hagyatkozott, hanem a Bitcoin tranzakciók lekövetésére.[54]

7. Illegális piacok a dark weben

Ugyan egy új bűnözői gazdaságról van szó, de a kiberbűnözés legalább 1,5 trillió USD bevételt generál évente. Ez egy konzervatív becslés, amit McGuire az öt legnagyobb profilú és legjövedelmezőbb kiberbűnözési módszerekből nyert adatokra alapoz. Az illegális online piacok 860 milliárd USD bevételt generálnak évente, mely a legjövedelmezőbb kiberbűnözési fajta, éves összbevételének több mint 50%-át teszi ki. Az üzletititok-lopás, IP-cím-lopás 500 milliárd USD-t generál, ami kb. 35%-át teszi ki a kiberbűnözési bevételeknek. Az adattal való kereskedelem (lopott adatokkal való kereskedelemből generált bevétel, mint hitel- és bankkártya információ, bank bejelentkezési adatok etc.) 1,6 millió USD-t generál, ami kb. 11%-a a teljes bevételeknek. A crimeware, CaaS (Cybercrime-as-a-Service) 1,6 milliárd USD-t generál, ami inkább egyéni kiberbűnözőknek jelenthet magasan jövedelmező bevételi forrást, de 2018-ban kevesebb mint 1%-át tette ki az összbevételnek. A ransomware (zsarolóvírus) 1 milliárd USD bevételt hoz évente.[55]

A dark webnek nagy szeletét uralják az illegális piacok, amik olyanok, mint az Ebay, vagy az Amazon, ahol bármi megtalálható és megrendelhető úgy, mint a szokványos e-kereskedelmi oldalakról. Az Empire Market, Dream Market, WallStreet Market néhány a legnépszerűbb dark web piacok közül, melyeken a követelező szolgáltatásokkal kereskednek: számos kábítószer, fegyverek, hackelt szoftverek, lopott hitelkártyák és banki adatok, hamis közokiratok, mint az útlevelek és vízumok, hackerszolgáltatások, és bérgyilkosok szolgáltatásai.[56] Ezek a fekete piacokat az általuk biztosított anonimitás teszi vonzóvá.[57]

A dark webes piacokon minden elérhető: vásárolható hitelkártyaszámot, mindenféle kábítószer, fegyverek, hamis pénz,[58] lopott feliratkozást igazoló adatok, feltört Netflix fiókok és számítógépek feltörésére alkalmas szoftver. 50 000 USD-s Bank of America fiókhoz bejelentkezési adatok kaphatóak 500 USD-ért. 3000 USD-t kitevő hamis 20 dolláros bankjegyek 600 USD-ért. Vásárolható 7 darab prepaid (előre fizetett) bankkártya, egyesével 2500 USD egyenleggel feltöltve, 500 USD-ért (sürgős kézbesítéssel). Egy „életre szóló" Netflix premium fiók 6 USD-be kerül. Felbérelhetők hackerek számítógépek megtámadására. Vásárolhatóak mindenféle felhasználónevek és jelszavak.[59] A dark weben a zsarolóvírusok széles kínálata érhető el, rendszeres frissítésekkel, technikai támogatással, távoli vezérlő szerverekhez (C&C) való hozzáféréssel és számos fizetési lehetőséggel. A Ranion oldalain vásárolható egyik zsarolóvírus havi vagy éves előfizetéssel is elérhető. Számos lehetőség áll a bűnözők rendelkezésre, egyre alacsonyabb árakon: a legolcsóbb egy hónapos csomag alig 120 USD , és a legdrágább sem kerül többe 900 USD-nél egy teljes évre. Az árak a külön megvásárolt szolgáltatások függvényében akár 1900 USD-ig is felmehetnek. Egy másik fizetési modellben a vásárlók magát a vírust és a C&C infrastruktúrát ingyen kapják, és a beérkező váltságdíjakból kér az eladó részesedést. Szerverhozzáférések: Számos olyan szolgáltatás érhető el a dark weben, amely hitelesítő adatokat kínál a világ különböző pontjain lévő szerverekhez, távoli asztali protokoll (RDP) segítségével. Az árak 8–15 USD között mozognak szerverenként és országonként. Szerverhozzáférések kereshetők operációs rendszer szerint, és az alapján is, hogy melyik fizetési oldal felhasználóinak van hozzáférése az adott szerverhez. Például a Kolumbiában található kiszolgálók esetében 250 szerver áll rendelkezésre. Minden szerverhez különféle adatokat adnak meg. A hoz-

[53] Uo. 4-5. o.

[54] Newman, Lily Hay: How a Bitcoin Trail Led to a Massive Dark Web Child-Porn Site Takedown https://www.wired.com/story/dark-web-welcome-to-video-takedown-bitcoin/ (2020.03.28.)

[55] McGuire, Michael: Into The Web of Profit: Understanding the Growth of the Cybercrime Economy. Bromium, Inc., Cupertino 2018. 15–16 .o.

[56] What is the Deep Web? The Definitive Guide [2020]. https://www.thedarkweblinks.com/what-is-the-deep-web/ (2020.03.28.)

[57] Hardy, Robert Augustus – Norgaard, Julia R.: Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. Journal of Institutional Economics, 2016. Vol. 12. No. 3. 516. o.

[58] A pénz- és bélyegforgalom biztonsága elleni bűncselekményekről lásd: Gál István László: A pénz- és bélyegforgalom biztonsága elleni bűncselekmények. In: Polt Péter (szerk.): Új Btk. kommentár: 7. kötet, Különös rész. Nemzeti Közszolgálati és Tankönyvkiadó Zrt., Budapest 2013. 193–224. o.

[59] Guccione, Darren: What is the dark web? How to access it and what you'll find. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (2020.03.28.)

záférés megvásárlása után ezeket zsarolóvírus futtatására vagy más kártevők, például banki trójai vagy kémprogramok telepítésére használhatják. Infrastruktúrabérlés: Egyes kiberbűnözők, akik botneteket, vagy feltört számítógépek hálózatait hozták létre, bérbe adják a spamek, vagy a DDoS támadások végrehajtásához szükséges számítási teljesítményt. A szolgáltatásmegtagadási támadások esetén az ár a támadás hosszától függ (1–24 óra), és hogy mennyi forgalmat képes a botnet ez idő alatt generálni. Például 60 USD három órán keresztül. Fiatalok gyakran kínálják bérlésre a (kis) botnet hálózatukat, főleg a Fortnite-hoz hasonló online játékok által használt szerverek támadására. A közösségi médiában hirdetik magukat és termékeiket, nem igazán törődve az anonimitásuk megőrzésével. PayPal és hitelkártyafiókok: A sikeres adathalász támadásokat végrehajtó bűnözők általában nem kockáztatnak a lopott fiókok használatával. Számukra az is nyereséges és biztonságosabb, ha a számlákat eladhatják. Ezek ára általában az ellopott számlán található hitelkeret 10%-a. Néhány eladó boldogan mutatja be adathalászatra használt eszközeit és a hamis oldalakat. A (nem is annyira) rejtőzködő kiberbűnözők nyereséges iparágat hoztak létre, amely a marketingtől kezdve az ügyfélszolgálatokon át, a frissítésekig és a felhasználói kézikönyvekig minden hagyományos üzleti ágat magában foglal. Érdemes megjegyezni, hogy bár ezeken a felületeken sok vevő van, az igazi nyereséget azonban a kiterjedt infrastruktúrával és jól működő szolgáltatásokkal rendelkező „nagy halak" realizálják. A kiberbűnözők által kínált szoftverek, termékek és szolgáltatások leginkább az értékesítés, a marketing és a terjesztés révén válnak nyereségessé.[60] 2018. szeptemberben több mint 50 millió Facebook-felhasználó feltört adatait bocsátották áruba a dark web piacain, felhasználónként már 3–12 USD-nek megfelelő értékű Bitcoinért.[61] 2016. július 22-én egy 18 éves elkövető a Münchener Olympia-Einkaufszentrumban 9 embert lőtt le, aztán önmagával is végzett egy „Deutschland im Deep Web" nevű dark webes fórumon szerzett Glock 17 pisztollyal, ami jól mutatja a veszélyt a jelenségben.[62] Az első ismert online kábítószer-kereskedelmi ügylet 1971-ben történt, amikor marihuánával kereskedett egymás között két hallgató a Stanford University-ről és Massachusetts Institute of Technology-ról, akik az ügyletet ARPANET használatával bonyolították le.[63] Adewopo, Gonen Varlioglu és Ozer hipotézise szerint az utcai drogdílerek dark web online kábítószerkereskedőkké válnak, az egyszerű és lekövethetetlen kiszállítás, és a fizetési rendszereik kriptovalutás tranzakciókra való támaszkodása (különösen Bitcoinra) miatt. A kábítószerfüggők pedig hajlamosak a dark webről vásárolni a kábítószert.[64] A Silk Road egy dark weben működő piac volt, melyen kábítószerrel és más csempészárukkal kereskedtek. Alapítóját a használók Dread Pirate Roberts néven ismerték. Az oldal két éven át el tudta kerülni világszinten a bűnüldöző szerveket, több millió USD bevételt termelve a használóinak és adminisztrátorainak. Az FBI 2013 októberében kapcsolta le az oldalt, lefoglalt 3,6 millió USD-t, és letartóztatta Ross Ulbrichtot (álnevén Dread Pirate Roberts).[65] A Silk Road domainneve, a http://silkroad6ownowfk.onion csak Tor böngészővel volt hozzáférhető.[66] Az FBI Ulbricht pere során benyújtott vádirata szerint a Silk Road piaca majdnem 150 000 vevővel és 4000 eladóval büszkélkedhetett. A felhasználói bázis nagy része USA-beli volt, de képviseltették magukat a világ minden részéről. Amellett, hogy az oldalnak magának voltak üzenetküldési lehetőségei, mely lehetővé tette a vevők és eladók interakcióját, a Silk Road-felhasználóknak egy Tor fórumhoz is volt hozzáférése, amin társalgások folytak a kábítószerek hatásairól, a Bitcoinról, eladói értékelésekről és tranzakciós képességekről. Emiatt az oldal nemcsak a csempészáruk szabad kereskedelmének menedékhelye volt, hanem széleskörű információk tárháza és egy globális közösség saját értékrenddel, hiedelmekkel és belső konfliktusokkal.[67] Ulbricht 2013-as letartóztatsa[68] után a Silk Road-ot helyettesítő oldalak tucatjai jelentek meg.[69] 2013 novemberében, körülbelül öt héttel azután, hogy a kormány lekapcsolta a Silk Road-ot, és letartóztatta Ulbricht-ot, megjelent a Silk Road 2.0. Arra tervezték, hogy betöltse a Silk Road után keletkezett űrt, ezért a Silk Road 2.0 jóformán azonos volt az eredeti Silk Road oldallal mind megjelenésében, mind működésében. Ahogy az elődje, a Silk Road 2.0 is kizárólag a Tor hálózaton működött, és tranzakcióit Bitcoinban kellett fizetni, hogy óvják a felhasználók anonimitását és elkerüljék a hatóságok általi felfedezést. A Silk Road 2.0 ajánlatai is főleg kábítószerekből álltak, amiket az oldalon nyíltan hirdettek. 2014. október 17-re a Silk Road 2.0 több mint 13 000 szabályozott anyagot listázott. Többek közt 1783 találatot listázott „pszichedelikumokra", 1697 találatot „ecstasyra", 1707 találatot

[60] Kiberbűnözés a dark weben – Milyen szolgáltatások kaphatók az internet sötét oldalán és mennyit kell fizetni értük? https://www.eset.com/hu/hirek/kiberbunozes-a-darkweben/ (2020.03.28.)

[61] Cuthbertson, Anthony: Facebook Hack: People's Accounts Appear For Sale On Dark Web. https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-hack-data-dark-web-login-details-cost-dream-market-a8564671.html (2020.03.28.)

[62] Vogt, Sabine: Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen? Die Kriminalpolizei, 2017. No. 2. 4. o.

[63] Buxton, J. – Bingham, T.: The rise and challenge of dark net drug markets. Policy Brief, 2015. Vol. 7. 3. o.

[64] Adewopo, Victor – Gonen, Bilal – Varlioglu, Said – Ozer, Murat: Plunge into the Underworld: A Survey on Emergence of Darknet. 6th Annual Conference on Computational Science & Computational Intelligence (CSCI'19), Las Vegas 2019. 5. o.

[65] Lacson, Wesley – Jones, Beata: The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. International Journal of Cyber Criminology, 2016. Vol. 10. No. 1. 40. o.

[66] Uo. 42. o.

[67] Uo. 43. o.

[68] Ulbrichtot tényleges életfogytiglani szabadságvesztésre ítélték 2015-ben. Ulbricht fellebbezéssel próbálkozott, de azt a Second Circuit Court of Appeals elutasította. Forrás: Kerr, Dara: Silk Road founder loses appeal challenging life sentence. https://www.cnet.com/news/silk-road-founder-loses-appeal-challenging-life-sentence/ (2020.03.28.)

[69] Sui–Caverlee–Rudesill: i.m. 9. o.

„kannabiszra" és 379 találatot „opioidokra". Az illegális narkotikumok mellett más illegális árukat és szolgáltatásokat is hirdettek eladásra az oldalon, beleértve hamis személyazonosító okmányokat és számítógépes hackereszközöket és szolgáltatásokat.[70] Az Operation Onymous során 2014 novemberében az FBI és több mint 15 ország az European Cybercrime Centeren (EC3) keresztül dolgozva vizsgált számos dark web piacot. A művelet során eltávolított oldalak között volt a Silk Road 2.0.[71] Az FBI az oldal lekapcsolásának hírét a Twitteren osztotta meg. A vádiratában az FBI arról számolt be, hogy a Silk Road 2.0-t az oldal 2013. októberi elindulása óta nyomon követte, amikor is egy fedett nyomozó a Belbiztonsági Minisztériumtól (Department of Homeland Security) beszivárgott egy online fórumra a Tor hálózaton. A korai fórumos beszélgetésekből kiderült, hogy egy „Defcon" nevű személy az oldal üzemeltetője. A fedett nyomozót a Silk Road 2.0 oldalon moderátornak kérték fel, összesen 16 kifizetést kapott fizetségként meghatározatlan munkáért, melyek több mint 32 000 USD-nek feleltek meg Bitcoin-ban. A hatóságok Benthallt azonosították, mint „Defcon", miután meghatározták egy Silk Road 2.0 szerver helyét tengerentúlon és megerősítésre került, hogy azt a blake@benthall.net e-mail-címet használó személy irányította és menedzselte. Az FBI szerint az oldalnak 8 millió USD havi bevétele és több mint 150 000 aktív használója volt.[72] Ugyan a Silk Roadnak a mérete elhanyagolható volt a teljes nemzetközi kábítószerkereskelemhez képest, a bevételei esetében dollár tízmiliókról, a nemzetközi kábítószerkereskedelem esetén pedig dollár százmilliárdokról beszélünk. A Silk Road jelentősége a jövő kábítószerkereskedelmére való hatásában rejtőzhet. Ahogy a számítógépek megváltoztatták azt, ahogy kezeljük és fogyasztjuk az információt, a kriptopiacokban benne van a lehetőség, hogy a kábítószerpiacok működését úgy változtassák meg, ami évtizedekkel vetheti vissza a szabályozási törekvéseket. A kutatóknak oda kell figyelniük a kriptopiacok méretváltoztató képességére: 15 hónap alatt a Silk Road eladásai is hatszorosára nőttek. További kérdés lesz a kriptopiacok ineternacionalizálódása. A Silk Road lehetővé tette a kábítószerfogyasztóknak, hogy majdnem bármilyik országból rendeljenek. A kriptopiacok jelenthetik az innovációt, ami alapjaiban változtathatja meg a kábítószerkereskedelmet az elkövetkező évtizedekben.[73] 2019. májusban két virágzó dark web piac, a Wall Street Market és Valhalla (más néven Silkkitie), került eltávolításra EU-s bűnüldöző szervek szimultán globális műveletei által. A három legnagyobb piac 2017-es lekapcsolása után a Wall Street volt az egyik legnagyobb megmaradt illegális online piac. Eltávolítása idején több mint 1 150 000 használója és 5400 eladója volt. A Német Szövetségi Bűnügyi Hivatal (BKA), a Holland Nemzeti Rendőrség, az Europol, az Eurojust és néhány amerikai kormányügynökség támogatásával három gyanúsítottat tartóztattak le Németországban. A rendőrök több mint 550.000 EUR-t foglaltak le készpénzben, továbbá Bitcoin és Monero kriptovalutákat hat számjegyű összegű értékben. Az USA-ban letartóztatták a piac két legnagyobb bevételt generáló kábítószer-kereskedőjét is. A finn vámhatóság a francia Nemzeti Rendőrséggel és az Europollal szoros együttműködésben lefoglalta a Valhalla piactér szerverét és annak tartalmát. A művelet eredményeként a finn vámhatóság jelentős összegű Bitcoint foglalt le. A Valhalla volt az egyik legrégebbi és nemzetközileg egyik legismertebb Tor kereskedő oldal.[74] A Wall Street Market működtetéséhez használt szervereket 2019. május 2-án foglalták le. A piac üzemeltetői minden ügylet után az értékesítési ár 2-6 %-a közötti összegnek megfelelő jutalékot szedtek. Az eltávolítása idején a Wall Street Market a második legnagyobb illegális online kereskedelmi platform volt. A hatóságok egy fedett nyomozók közreműködésével folytatott nemzetközi eljárással számolták fel. Az után léptek akcióba, hogy az üzemeltetők 2019. április 23-án a portált karbantartási üzemmódba állították, és elkezdték magukhoz venni a felhasználói számlákon elhelyezett összegeket. Ez „exit scam"[75] néven ismert a színtéren. Az amerikai és holland hatóságokkal és az Europollal közösen folytatott nyomozás révén Los Angelesben elfogtak két gyanúsítottat, akik a hatóságok szerint a portál legnagyobb forgalmat lebonyolító kábítószer-kereskedői közé tartoztak. A gyanúsítottaknál tartott házkutatásokon drogok és számos illegálisan tartott fegyver mellett készpénzt is lefoglaltak több millió EUR értékben.[76] A Wall Street Market lekapcsolása után a T•chka Market lett az egyetlen megmaradt nagyobb piac a dark weben.[77] DreamMarket olyan platformra példa, amihez fórum is tartozik. A piac megközelítőleg 55 000 árut listázott, és nagyjából 20 000 használója volt. Az Alphabay a 2016. június és július közötti időszakban körülbelül 66 000 ajánlatot listázott, több mint 75 000 használó-

[70] U.S. Attorney's Office: Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court. https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court (2020.03.28.)

[71] Finklea, Kristin: Law Enforcement Using and Disclosing Technology Vulnerabilities. Congressional Research Service, Washington DC, 2017. 3. o. https://fas.org/sgp/crs/misc/R44827.pdf (2020.03.28.) 5. o.

[72] Martinez, Fidel – Wile, Rob: Silk Road 2.0 hits dead end with FBI. busthttps://splinternews.com/silk-road-2-0-hits-dead-end-with-fbi-bust-1793842852 (2020.03.28.)

[73] Aldridge, Judith – Decary-Hetu, David: Not an 'eBay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. SSRN Electronic Journal, 2014. 20. o.

[74] Europol The Internet Organised Crime Threat Assesment 2019. Europol, Hága, 2019. 44. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (2020.03.28.)

[75] Exit scam esetében gyakorlatilag arról van szó, hogy az oldal adminjai megszöknek a felhasználók (bűnözők) pénzével, jelen esetben több mint 14,2 millió USD-vel. Forrás: Cimpanu, Catalin: Another dark web marketplace bites the dust – Wall Street Market https://www.zdnet.com/article/another-dark-web-marketplace-bites-the-dust-wall-street-market/ (2020.03.28.)

[76] Felszámolták a darknet második legnagyobb portálját. https://www.digitalhungary.hu/e-kereskedelem/Felszamoltak-a-darknet-masodik-legnagyobb-portaljat/8513/ (2020.03.28.)

[77] Cimpanu, Catalin: Another dark web marketplace bites the dust – Wall Street Market https://www.zdnet.com/article/another-dark-web-marketplace-bites-the-dust-wall-street-market/ (2020.03.28.)

val. Narkotikumok tették ki a kínált áruk többségét (körülbelül. 52 000), továbbá lehetett még vásárolni fegyvereket (kb. 500 ajánlat), hamis pénzt (kb. 300), adatokat és gyógyszereket is.[78] Az Europol Szervezett bűnözés internetes fenyegetettségét (IOCTA) vizsgáló 2019-es éves jelentése szerint a dark web marad a bűnözői termékek és szolgáltatások széles tárháza kereskedelmének a legfőbb online elősegítője, és kiemelt fenyegetést jelent a bűnüldöző szervek számára. Az utóbbi idők koordinált bűnüldöző tevékenységei, kiterjedt DDoS támadásokkal kombinálva a Tor környezetbe bizalmatlanságot hoztak. Miközben van arra mutató bizonyíték, hogy az adminisztrátorok alternatívákat fedeznek fel, úgy tűnik, a felhasználóbarátság, a meglévő piac sokoldalúság és a Tor vásárlói bázisa miatt az új platformokra történő teljes migráció még nem tűnik valószínűnek. Növekedés tapasztalható az egyeladós üzletek és kisebb fragmentált piacok terén a Toron, beleértve azokat is, amelyek specifikus nyelvekre szakosodtak. Néhány szervezett bűnözői csoport is fragmentálja az üzletét online becenevek és piacok skáláján, ami további kihívást jelent a bűnüldöző szervek számára. A titkosítással ellátott kommunikációs alkalmazások erősítik az egyeladós kereskedelmet a dark weben, azáltal, hogy segítenek a használókat szolgáltatásokhoz irányítani, és zárt kommunikációt tesznek lehetővé. Bár nincs bizonyíték a teljes üzleti vándorlásra, fennáll annak a veszélye, hogy a csoportfunkciókat egyre inkább felhasználhatják a tiltott kereskedelem támogatására.[79] Fontos arról a jelenségről beszélni, hogy amint a hatóságok eltávolítanak egy illegális dark web piacot, a helyükön mindig újabbak jelennek meg. A két legnagyobb, a Wall Street Market és a Valhalla eltávolítása után az Empire nevű piacon már nagy volt a nyüzsgés, kínálatában 18 000 termékkel. A Nightmart Market 28 000 illegális áruját kínálja. Egy új, a Reddithez hasonlatos fórum, a Tor rejtett szolgáltatásán hosztolt Dread már helyettesítette is az eltávolított DeepDotWebet, mint közösségi csomópontot, ahol a felhasználók megtárgyalják, melyik oldalt érdemes használni, melyiket távolította el a rendőrség, és melyikeket működtetik csalók. Az FBI és Europol nyomozói szerint ugyan a dark webes kábítószeroldalak ellen vívott háborújuknak messze nincs vége, de a harc szükséges, és már akkor is megéri, ha csak visszafoghatják a dark webes piacok növekedését, és nehezebbé tehetik a veszélyes kábítószerek online vásárlását.[80]

8. A terroristák a dark weben

A témát illetően Finszter Géza szavait bocsátom előre: „Nem véletlen, hogy a terrorizmus és a szervezett bűnözés elleni küzdelmet gyakran nevezik bűnügyi hírszerzésnek, jelezve, hogy az ilyen típusú deliktumok felderítésében csak a titkosszolgálati eszközök lehetnek eredményesek.[81] Ugyan a terroristaszervezetek korábbi intenzív nyilvános webes jelenléte visszaszorult, de a kisebb szervezeteknek még mindig vannak internetes felületeik, gyerekeknek szóló weboldalaik, illetve terrorizmussal szimpatizáló csoportok még mindig megtalálhatók a közösségi média felületein.[82] Bodo és Speckhard rávilágít, hogy kétségtelenül az Iszlám Állam a történelem legsikeresebb technológia-orientált terrorszervezete, mivel ők nem csupán azt értik, hogy használható az internet kommunikációra, hanem azt úgy teszik, hogy közben el tudták rejteni az üzeneteiket és azonosságukat. Az ISIS aktivistái használják a felszíni webet, a deep webet, dark webet, a közösségi médiát és titkosított üzenetküldő alkalmazásokat, propagandájuk terjesztésére, toborzásra, követőiket terrorcselekmények elkövetésének inspirálására vagy terrorcselekmények elkövetésére való közvetlen utasításra, mely komoly fejfájást jelent a bünüldöző szerveknek, a titkosszolgálatoknak és biztonsági szakértőknek, akiknek a feladata lenne egy lépéssel mindig a terrorszervezet előtt maradni,[83] de ahogy Bartkó Róbert rávilágít az egyes terrorszervezetek módszereinek kiismerhetetlenségére: „Az egyes elhárítási eszközök a terrorista akciókkal együtt fejlődnek, így továbbra is alátámasztódni látszik a mára már »közhelynek« tekinthető állítás, miszerint a bűnözők egy lépéssel mindig a bűnüldöző hatóságok előtt járnak."[84] Az ISIS aktivitása a webalapú interneten (Youtube-on, Facebookon, Twitteren etc.) megfigyelhető keresőrobotokkal és keresőmotorokkal, de a bűnüldöző hatóságoknak és titkosszolgálatoknak nehezebb dolga van a titkosított üzenetküldő alkalmazásokon lévő információk megszerzése tekintetében, pedig azok értékesek lehetnek a terrorcselekmények megelőzése és megakadályozása szempontjából.[85] Bodo és Speckhard kísérlete ISIS-támogató Telegram felhasználók azonosítására irányuló kreatív módszerek felfedezésére irányulult. Arra jutottak, hogy lehetséges behatolni a Telegramos ISIS

[78] Vogt, Sabine: Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen? Die Kriminalpolizei, 2017. No, 2. 5. o.

[79] Europol The Internet Organised Crime Threat Assesment 2019., Europol, Hága, 2019. 43. o. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (2020.03.28.)

[80] Greenberg, Andy: Feds Dismantled the Dark-Web Drug Trade – but It's Already Rebuilding. https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/ (2020.03.28.)

[81] Finszter Géza: Rendészettan. Dialóg Campus Kiadó, Budapest 2018. 78. o.

[82] Haig Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest 2018. 301–302. o.

[83] Bodo, Lorand – Speckhard, Anne: Identifying Nefarious Telegram Users without the Help of Telegram Itself: Testing Solutions for Intelligence and Security Professionals in Fighting ISIS in the Encrypted Social Media Space. International Center for the Study of Violent Extremism, London 2017. 2. o.

[84] Bartkó Róbert: A terrorizmus elleni küzdelem kriminálpolitikai kérdései. UNIVERSITAS-GYŐR Nonprofit Kft., Győr 2011. 68. o.

[85] Bodo, Lorand – Speckhard, Anne: Identifying Nefarious Telegram Users without the Help of Telegram Itself: Testing Solutions for Intelligence and Security Professionals in Fighting ISIS in the Encrypted Social Media Space. International Center for the Study of Violent Extremism, London 2017. 2-3.o.

chatszobákba, és azokon belül megtalálni a közösségi médiás felhasználói fiókokat, és OSINT[86] alkalmazásával[87] az ISIS támogatók személyazonosságát felfedni. Közülük legtöbben az ISIS instrukciói ellenére sem teszik meg a megfelelő óvintézkedéseket, mint VPN vagy Proxy hálózat használata. A módszer még a Telegram Secret Chatjében is működik.[88] Moore és Rid 2015. január és március között website keresőrobottal végzett kutatása során 300 000 címet vizsgált meg, és 2015 eleji kutatásuk során még arra jutottak, hogy majdnem hiányzik az iszlám extremizmus a Tor rejtett szolgáltatásain, csupán egy maréknyi aktív oldalt találtak. Moore és Rid szerint a dark neten a propaganda nem ér messzire, főleg azért, mert az újoncokat kezdetben elijesztheti, hogy egy „jogellenes" cselekményt kell véghezvinniük, szemben egy egyszerű, Google-kereséssel. A rejtett szolgáltatások gyakran nem elég stabilak vagy hozzáférhetőek a hatékony kommunikációhoz, más platformok jobban megfelelnek a kommunikációs igényeknek. Iszlamista harcosok azonban gyakran használják a Tor böngészőt a nyílt interneten, a fokozottabb anonimitás miatt.[89] A terroristák dark webes jelenléte azóta jelentősen nőtt: a 2015. novemberi párizsi terrortámadások után hírei és propagandája terjesztése céljából az ISIS a dark web felé fordult, hogy meg kísérelje védeni a terrorszervezet támogatóinak azonosságát és az anyagaikat a hacktivisták tevékenységétől. Ez az után történt, hogy több száz ISIS-hez köthető weboldal került eltávolításra az Anonymous hacker kollektíva által indított Operation Paris (OpParis) kampány részeként. Az ISIS mediaügynöksége, az Al-Hayat Media Center egy ISIS-hez kötődő fórumon közzétett egy linket és instrukciókat arról, hogyan lehet eljutni az új dark webes oldalukra.[90] A felszíni web használata a terroristák számára kockázatosabb: ott felügyelhetőek, lekövethetőek, megtalálhatóak. Ezzel szemben a dark weben decentralizált és anonim hálózatok használatával a lebukás elkerülhető, és a terrorista platformok zártak maradhatnak.[91] A terroristák a dark weben biztonságosabban kommunikálhatnak, mint eddig valaha. 2016 márciusában a francia belügyminiszter, Bernard Cazeneuve a Nemzetgyűlés előtt a terroristák dark web használatára hívta fel a figyelmet. Nyilatkozata szerint napjaink európai terrortámadásainak elkövetői a deep webet használták fel, és titkosított üzenetekkel kommunikáltak. Az utóbbi években az ISIS és más dzsihádista csoportok titkosított üzenetküldő alkalmazások felé fordultak. Egy ilyen alkalmazás például a Telegram, mely egy üzenetek küldésére alkalmas applikáció, Android, iOS, és Windows készülékekre. Egyik fő tulajdonsága a végpontok közötti titkosítás (end-to-end encryption), ami vonzóvá teszi bűnözők, köztük terroristák számára. A dark webet továbbá virtuális fizetőeszközök használatával terroristák és más bűnözők felhasználják összegek rejtett utalására. Korunkban Weimann ezt a trendet tartja a legriasztóbbnak a dark web terroristáknak nyújtott lehetőségei közül. A kriptovaluták a készpénz digitális megfelelői, melyeket gyakran használnak tranzakciókhoz illegális kereskedelem során, zsaroláshoz, pénzmosáshoz. A terroristák is használhatják a webet adománygyűjtésre, pénzátutalásra és virtuális fizetőeszközök használatával robbantószerek, fegyverek vásárlására.[92] Malik 2018-as „Terror in the Dark" című jelentésében a következő trendekre világít rá a terroristák dark web használatát illetően: A terroristák a titkosítást használják rejtőzködésre. A felszíni web a közösségi média cégek és hatóságok általi fokozott felügyelete a közösségi média platformjairól az extremista tartalom gyorsabb eltávolításához vezetett. A terrorcselekmények megtervezésére a dark webes extremista hálózatokat fokozottaban használják. A toborzók a dark webet használják terrorcselekmények megtervezésére és kezdeményezésére, mivel ott kisebb az esély, a lebukásra. Miközben a kezdeti kapcsolatfelvétel a felszíni weben történhet meg, a további instrukciókat gyakran végpontok közötti titkosítással ellátott alkalmazásokon adják arról, hogyan férhetnek hozzá dzsihádista weboldalakhoz a dark weben. A terroristák a dark webet felhasználják toborzásra: a titkosított csatornák mint a Telegram, és a dark web színterei nehezen hozzáférhetőek, emiatt tömeges toborzás ritkán történik ezeken a csatornákon, ehelyett az ISIS emberei az érdeklődő szimpatizánsokat a felszíni web és a közösségi média platformjaimról a biztonságosabb dark net felé irányítják, mint a további interakció és indoktrináció színetere felé. A terroristák a dark webet felhasználják propaganda tárolására: Az extremista és terrorista tartalmak felszíni webről és deep webről való eltávolítása, főleg a mesterséges intelligencia programok által végzett tömeges eltávolítás növeli annak a kockázatát, hogy a tartalmat terjesztő vagy terrorszervezeteknek anyagi támogatást nyújtó személyek bíróság elé állításához szükséges bizonyítékok elveszhetnek. Ezek közül az anyagok közül sok újra előbukkan a felszíni weben. A tech cégek és a bűnüldöző hatóságoknak együtt kell működniük, hogy ezt az anyagot hatékonyan archiválják, hogy a viselkedésminták megérthetők legyenek. A terroristák kriptovalutákat használnak adománygyűjtésre, és a lebukás elkerülése érdekében. A terroristák, mint más bűnözők, kriptovalutákat használnak, melyek ugyanazt a fajta anonimitást biztosítják a pénzügyi környezetben, mint a titkosítás a kommunikációs rendszerekben. A bitcoinnal végzett adománygyűjtéssel és online pénzügyi tranzakciókkal a terroristák és más bűnözők el tudják kerülni a pénzügyi szabályozók és más harmadik személyek általi be-

[86] Az OSINT-ről bővebben: Dobák Imre: OSINT – Gondolatok a kérdéskörhöz. Nemzetbiztonsági Szemle, 2019. 7. évf. 2. sz. 83–93. o.

[87] Bodo–Speckhard: i. m. 6. o.

[88] Bodo–Speckhard: i. m. 10–11. o.

[89] Moore–Rid: i. m. 18–22. o.

[90] Weimann, Gabriel: Going Darker? The Challenge Of Dark Net Terrorism. Wilson Center, Washington, DC 2018. 3. o.

[91] Weimann, Gabriel: Terrorist Migration to the Dark Web. Perspectives on Terrorism, 2016. Vol. 10 No. 3. 40–41. o.

[92] Weimann, Gabriel: Going Darker? The Challenge Of Dark Net Terrorism. Wilson Center, Washington, DC 2018. 4–5. o.

avatkozást, akik lépéseket tennének a műveleteik megakadályozására.[93] A terrorizmus finanszírozása[94] tekintetében Pasca és Orza rávilágít, hogy a terroristacsoportok a műveleteik finanszírozásához szükséges bevételszerzési és pénzátutalási módszerei tekintetében haladnak a modern technológia új trendjeivel (mint a kriptovaluták és a dark net használata), de a tradicionális módszereket is használják (mint a zakat és hawala).[95] Amikor csak külső anyagi forrásokra van szükségük, a terroristák különféle módszerekhez folyamodnak, melyek bonyolultságukban az egyszerűtől a rendkívül összetettig (lásd például az al-Kasszám Brigádok, a Hamász katonai szárnyának felhívását a támogatói számára, bitcoinos közösségi finanszírozásra.[96]) terjednek.[97] Különösen riasztó a tény, hogy „... a terrorizmus finanszírozásával szemben a büntetőjogi eszközök hatékonysága a nullához konvergál".[98] Az internetes pénzügyi tranzakciók száma növekszik. Tóth Dávid arra mutat rá, hogy újabb típusú fizetési eszközök, virtuális fizetőeszközök[99] jelennek meg, mint például a Bitcoin és a Litecoin, melyeknek a jogi státusza nem teljesen tiszta. Az információs technika fejlődése ugyan könnyebbé tette a pénzügyi szolgáltatások használatát, de a technológia a bűnelkövetők számára egyre több lehetőséget nyújt az ezekkel történő visszaélésekre.[100]A „Fund the Islamic Struggle without Leaving a Trace" (Finanszírozd az Iszlám Küzdelmet Nyomok Hagyása nélkül) egy Deep Web oldal, ami egy adott Bitcoin címre adományokat kér dzsihád finanszírozására. Egy Amreeki Witness álnévvel az internetre feltöltött „Bitcoin wa Sadaqat alJihad" című pdf dokumentum, melynek címe lefordítva „Bitcoin és az erőszakos fizikai küzdelem adománya" (Bitcoin and the Charity of Violent Physical Struggle) egy útmutató a Dark Web titkos pénzügyi tranzakciókra való felhasználásához.[101] Az ISIS még terrorcselekmények finanszírozására is használt Bitcoint, melyek közé tartoznak a 2019 áprilisában Srí Lankán elkövetett húsvéti robbantások is.[102]Az ISIS a terrorszervezet hivatalos al-Naba nevű hetente megjelenő hírlevelében egy egész oldalas infografikát tett közzé a COVID-19 fertőzés megakadályozásáról. Az ISIS a hírleveleiben január óta figyelemmel kísérte a koronavírust, és rendszeresen tájékoztatott róla. „Egy új vírus terjeszt halált és rettegést Kínában", jelentette az al-Naba még januárban. Valószínűleg a tagjaira és támogatóira jelentett veszély miatt, ahogy a vírus terjedt, az ISIS egyre jobban kritizálta a kínai kormányt, amiért az titkolta a járvány valódi mértékét. Az ISIS szerint ez a járvány Isten büntetése, amiért Kína sanyargatja az ujgur népességet. A terrorszervezet azt tanácsolja, hogy „helyezzétek a hitetek Istenbe és keressetek Benne menedéket a betegségektől" és „az egészségesek ne lépjenek a járvány földjére, és az az által sújtottak ne távozzanak onnan". (Ehhez képest az ISIS hajt végre műveleteket Algériában, Egyiptomban, Irakban, Afganisztánban, Indiában, a Fülöp-szigeteken és Indonéziában, ahol vannak igazolt esetek.) Az az ISIS szorgalmazza a kézmosást, és azt tanácsolja követőinek, hogy „ásításkor és tüsszentéskor takard el a szádat". Egy hadíszt is idéz a kórokozókról és fertőzésekről. Az al-Naba legújabb számában az ISIS szerint a koronavírus „további nyomást és terhet" ró a kormányokra, csökkenti azok együttműködési képességeit a terrorizmus elleni harc terén és biztonsági szempontból olyan rést jelent, amit a terrorszervezet szerint ki kell használniuk „a párizsi, londoni, brüsszeli és más csapásokhoz hasonló" terrorcselekmények elkövetéséhez, foglyaik kiszabadításaihoz.[103] Úgy vélem a terroristák kihasználhatják az abból adódható biztonsági réseket, hogy az állami szerveket lefoglalják a koronavírus pandémiával kapcsolatos feladatok, és ebben a megváltozott helyzetben fokozottan szükséges a terroristák kommunikációjának, szervezkedésének minden platformon történő fokozott megfigyelése, a terrorcselekmények elkövetésének megakadályozása céljából.

9. A dark webhez kapcsolódó dilemmák

Lehet, hogy a dark webet böngészni önmagában még nem illegális, de nem veszélytelen és könnyen illegálissá válhat. A dark webbel kapcsolatos biztonsági kockázatok a következők: a bűnözői elemek jelenléte, az illegális cselekmények elkövetésének lehetősége, gyanús linkek (amik illegális tartalomhoz vezethetnek), a bűnöldöző szervek jelenléte. Veszélyes lehet még a dark web a vírusok, hackerek és web cam eltérítés

[93] Malik, Nikita: Terror in The Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies. The Henry Jackson Society. London 2018. iv. o.

[94] A terrorizmus finanszírozásról bővebben: Gál István László A XXI. század új bűncselekmény-típusa: a terrorizmus finanszírozása. Rendészeti Szemle: Az Igazságügyi És Rendészeti Minisztérium Szakmai, Tudományos Folyóirata 2009. 57. évf. 6. sz 61–90. o.

[95] Pasca, Viorel – Orza, Daniela Simona: Terrorism: between the need for funding and obtaining funding sources. In: Journal Of Eastern-European Criminal Law, 2019. No. 1. 227. o.

[96] Fanusie, Yaya: Hamas Military Wing Crowdfunding Bitcoin. https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#306575c34d7f (2019. 12. 30.) (2020.03.28.)

[97] Europol's 2019 EU Terrorism Situation and Trend Report (TE-SAT) 17. o.

[98] Gál István László: Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat kiadványa, 2012. 1. sz. 15. o.

[99] A virtuális pénzekkel kapcsolatos visszaélésekről bővebben: Tóth Dávid: A virtuális pénzekkel kapcsolatos visszaélések. Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével, Szerkesztette: Baráth Noémi Emőke, Mezei József, Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya Budapest 2019. 242-250. o.

[100] Tóth, Dávid: Credit card fraud with a comparative law approach. In: International Scientific Conference „Towards a Better Future: Democracy, EU Integration and Criminal Justice", Conference Proceedings, Volume I, Faculty of Law – Kicevo, University „St. Kliment Ohridski" – Bitola, Bitola 2019. 232. o.

[101] Weimann, Gabriel: Terrorist Migration to the Dark Web. Perspectives on Terrorism, 2016. Vol. 10 No. 3. sz. 42. o.

[102] Katz, Rita: Tales of Crypto-Currency: Bitcoin Jihad in Syria and Beyond. https://www.thedailybeast.com/the-bitcoin-jihad-in-syria-and-beyond-tales-of-crypto-currency (2020.03.28.)

[103] Johnson, Bridget: ISIS: Cities Distracted by Coronavirus Should be Hit with Attacks Like Paris, London, Brussels. https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-cities-distracted-by-coronavirus-should-be-hit-with-attacks-like-paris-london-brussels/ (2020.03.28.)

miatt. Az ember könnyen illegális dolgokba keverheti magát, akár egy félreütéssel vagy egy kíváncsi kereséssel, és gyemekpornográfiába botolhat, vagy ha illegális árukat és szolgáltatásokat vásárol. [104]

A dark weben nem minden illegális, annak van legitim oldala is. Található ott például sakk klub, a „Tor Facebookjaként" jellemzett BlackBook nevű közösségi háló is.[105] A The New York Times volt az első fő digitális médiaorgánum, ami megnyitotta az oldalát a dark weben.[106] Weimann szerint mielőtt a dark web elleni fellépést fontolgatnánk, figyelembe kell vennünk annak a nem terrorista felhasználóit és felhasználhatóságát, továbbá társadalmi hasznait is. Sok átlag polgár használja a dark webet, főleg a magánéletük megóvása érdekében. Weimann szerint felmerülnek a kérdések, hogy az állampolgároknak fontosabb-e a magánélet védelme, mint a terrorista fenyegetésektől való biztonság, továbbá a magánélet, a szólásszabadság és a felügyelet nélküli kommunikáció elvesztésének költségei meghaladják-e az előnyöket. A terroristák száma nagyon alacsony a Telegram, Tor, és más titkosított applikációk használóinak túlnyomó többségéhez viszonyítva, akik jó szándékúak és nincs szándékukban terrorcselekményt elkövetni. Weimann szerint a terroristák a dark webbe való behatolása egy illegális és rossz szándékú tevékenységek elleni megoldás utáni nemzetközi kutatást kellene megindítania, de ennek olyannak kell lennie, amelynek nem szabad akadályoznia a legitim, törvényes véleménynyilvánítási szabadságot.[107] Rubasundram szerint a magánéletnek és anonimitásnak helyének is meg kell lennie a társadalomban, de észszerű keretek között. A kulcskérdés, amit fel kell tennünk magunknak, hogy: „Tényleg a biztonságunk árán akarunk magánéletet?"[108] Chertoff szerint a dark web természeténél fogva anonim és képtelen különbséget tenni a bűnözők és rendes felhasználók között. A bűnöldöző hatóságoknak kezelnie kell ezt a kérdést, azáltal, hogy olyan taktikákat alkalmazzanak, ami tiszteletben tartja az átlagos felhasználó adatvédelmét, miközben leleplezi a bűnözőket. A leghatékonyabb módja ennek, ha az illegális oldalakat keresik az illegális felhasználók helyett. Megfelelő legális felhatalmazással kormányhackerek deanonimizáló eszközöket helyezhetnek el az oldalhoz hozzáférő felhasználók számítógépeire. Ha a hatóságok szimplán csak leállítják az oldalt, egy másik fog a helyén felbukkanni. Másrészről, ha a hatóságok vádat emelnek egy illegális oldal felhasználói ellen, a jövőbeli felhasználók, akik illegális oldalakhoz való hozzáférést fontolgatnak, hezitálni fognak, a kockázat miatt, hogy elkaphatják őket. A végső opció az lenne a kormány kezében, hogy megkísérelhetnék feltörni a Tort, más szavakkal, azonosítani minden Tor-felhasználót. Ez a Silk Roadból adódó trend alapján, valószínűleg azt eredményezné, hogy a szolgáltatás egy robusztusabb verzióját alkotnák meg, ezáltal gátolva a kormányzati törekvéseket. Továbbá ez el is pusztítana egy hasznos eszközt a legitim felhasználók kezében. Az USA olyan módokon alkotmányosan elkötelezett az internetes véleménynyilvánítás szabadságának védelme mellett, ahogyan sok ország nem. Néhány ország teljes kontrollt szeretne az internet forgalma felett. Ők a szólászabadságot a hatalmuk fenyegetéseként értékelik, és a dark webet mint eszközt, amely lehetővé teszi a másképp gondolkodóknak, hogy szabadon beszéljenek. Az internet természeténél fogva számítógépek nemzetközi hálózata. Az illetékesség a legjobb esetben is ködös, tehát a kormányoknak meg kell találniuk az együttműködés módjait abban, hogy legalább kölcsönösen elfogadható dark webre irányuló szabályozást dolgozzanak ki. Az online anonimitás egy kétélű kard, amivel finoman kell bánni. Ahogy a politikai döntéshozóknak éberen kell figyelniük a dark web fejlődését, és gondoskodniuk kell arról, hogy a hatóságok rendelkezzenek megfelelő erőforrásokkal és jogi támogatással a dark weben történő sikeres rendfenntartáshoz. A dark webre vonatkozó politikának árnyaltnak és átgondoltnak kell lennie annak érdekében, hogy egyensúlyt lehessen találni az adatvédelmet szem előtt tartó felhasználók igényei és a kormány illegális tevékenységek megállítására irányuló felelőssége között.[109] Egyetértek Jardine véleményével, aki szerint a kényelmetlen valóság az, hogy ténylegesen azoknak a liberális demokratikus nemzeteknek kell foglalkoznia a rendszer negatív következményeivel, amelyek kifejlesztették és hosztolják a Tor network nagy részét, miközben kevés előnyét látják annak. Liberális országokban a technológia használatának lehetősége azt jelenti, hogy szaporodnak a Silk Roadhoz hasonló oldalak, az anonim gyemekpornó website-ok és a trollok, de az előnyök (az állami megfigyelés vagy vállalati tartalom megfigyelés elkerülése és a cenzúra megkerülése) meglehetősen minimálisak. Léteznek más kevésbé nehézkes programok (privát keresőmotorok, mint a Duck Duck Go, és VPN-ek) és nagyjából ugyanaz a hatásuk, mint a Tornak, de nagyobb letöltési sebességgel és kisebb potenciállal a visszaélésre, mivel ezek megőrzik a felhasználók adatait és együtt tudnak működni a hatóságokkal, ha érvényes bírósági végzést kapnak. Ezért, hacsak valaki nem végez konkrétan illegális tevékenységeket, a teljes anonimitást biztosító program, mint a Tor alkalmazásának a liberális demokratikus országokban korlátozott a szükségessége, a polgárjogok alkotmányos

[104] Symanovich, Steve: How to safely access the deep and dark webs. https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html (2020.03.28.)

[105] Guccione, Darren: What is the dark web? How to access it and what you'll find. https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (2020.03.28.)

[106] Paliy, George: What Is The Dark Web ? https://stopad.io/blog/what-is-the-dark-web-and-how-it-is-different-from-deep-web (2020.03.28.)

[107] Weimann, Gabriel: Going Darker? The Challenge Of Dark Net Terrorism. Wilson Center, Washington, DC 2018. 9. o.

[108] Rubasundram, Geetha A.: The Dark Web and Digital Currencies: A Potent Money Laundering and Terrorism Opportunity. International Journal of Recent Technology and Engineering (IJRTE), 2019. Vol 7. No. 5. 481. o.

[109] Chertoff, Michael: A public policy perspective of the Dark Web, Journal of Cyber Policy, 2017. Vol. 2 No. 1. 36–37. o.

és jogi védelme miatt. Ellenben fontos nem alulreprezentálni annak a mértékét, hogy az internet technológiájának gyors fejlődése mennyire meghaladta a jogrendszer azon képességét, hogy képes legyen kezelni a polgárok alapvető jogainak új kihívásait. A fentiek alapján valószínűtlen az a gondolat, hogy a Tor nettó haszonnal jár a liberális demokratikus országok társadalmában. Az nagy valószínűséggel több kárt okoz, mint hasznot.[110] A dark web használata a szabad országokban nem illegális, és Moore és Rid szerint valószínűleg nem is kell, hogy az legyen, de ezek a széles körben abuzált platformok éles kontrasztban a szélesebb nyilvános kulcsú infrastruktúrával (Public Key Infrastructure) szabad prédák, és azoknak is kell lenniük a legagresszívebb hírszerző és bűnüldöző technikákkal szemben, ahogy a beható akadémiai kutatásnak is. Moore és Rid szerint az ilyen tisztán elbarikádolt, szabad-tűz zóna még hasznos is lehet az állam számára, mert a rossz reputáció a rossz biztonsághoz vezet, és a Tor „csúnya" példája a tech vitáknak komoly részét kell képeznie. A dark wet kérdésével nem konfrontálódni szimplán felelőtlenség lenne.[111]

Összegzés

Egyetértek Nagy Zoltán gondolataival: „Az új kockázatokat, akárcsak más számítástechnikai környezetben felmerülő kockázatot, az internet árnyoldalait meg kell ismertetni a képzési formáknak megfelelő szinten, mélységben, középiskoláktól az egyetemi oktatáson át a jogalkotók a jogalkalmazók képzéséig. Jelenleg e körben bőven lenne tennivaló."[112] A titkosszolgálati eszközök alkalmazására kiváló platformot jelentenek a dark web színterei. Véleményem szerint fontos a dark weben folyó kriminalitás, az illegális piacok, a pedofil oldalak, a terrorista oldalak és egyéb bűnözői elemek bűnüldöző szervek általi nyomon követése, felügyelete, tanulmányozása, fedett ügynökök, szakértők alkalmazása. A felbukkanó illegális piacokat és pedofil oldalakat el kell távolítani. A terrorizmus elleni harc, a terrorcselekmények megelőzése és terrorizmus finanszírás elleni küzdelem szempontjából különösen fontosnak tartom a terroristák dark webes aktivitásának nyomon követését. Úgy vélem, a terrorista fenyegetés szempontjából hatalmas kockázatot jelent a COVID-19-pandémia. A terroristák kihasználhatják a világszinten megváltozott helyzetet, az állami szervek leterheltségét és az esetleges ebből adódó biztonsági réseket terrorcselekmények elkövetésére, ezért a járvány idején (is) rendkívül komolyan kell vennünk a terroristák jelentette fenyegetést, és nyomon kell követni a kommunikációjukat minden létező általuk használt platformon a jövőbeli terrorcselekmények megakadályozása érdekében.

[110] Jardine, Eric: The Dark Web Dilemma: Tor, Anonymity and Online Policing. Centre for International Governance Innovation, London 2015. 7. o.

[111] Moore–Rid: i.m. 32-33. o.

[112] Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula – Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII: TANULMÁNYOK „A BIZTONSÁG RENDÉSZETTUDOMÁNYI DIMENZIÓI – VÁLTOZÁSOK ÉS HATÁSOK" CÍMŰ TUDOMÁNYOS KONFERENCIÁRÓL. Pécsi Határőr Tudományos Közlemények XIII. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs 2012. 232. o.

Irodalomjegyzék

- Adewopo, Victor – Gonen, Bilal – Varlioglu, Said – Ozer, Murat: Plunge into the Underworld: A Survey on Emergence of Darknet. 6th Annual Conference on Computational Science & Computational Intelligence (CSCI'19), Las Vegas 2019. 5. o.
- Aldridge, Judith – Decary-Hetu, David: Not an 'eBay for Drugs': The Cryptomarket 'Silk Road' as a Paradigm Shifting Criminal Innovation. SSRN Electronic Journal, 2014. 20. o.
- Barratt, Monica – Aldridge, Judith – Maddox, Alexia: The SAGE Encyclopedia of the Internet – Dark Web. SAGE Publications, Ltd., Thousand Oaks 2018. 3–4. o.
- Bartkó Róbert: A terrorizmus elleni küzdelem kriminálpolitikai kérdései. UNIVERSITAS-GYŐR Nonprofit Kft., Győr 2011. 68. o.
- Bergman, Michael K.: The Deep Web: Surfacing Hidden Value. The Journal of Electronic Publishing, 2001. Vol. 7 No. 1.
- Berki Gábor: A kibertér, annak veszélyei és a kibervédelem jelenlegi helyzete Magyarországon. Nemzetbiztonsági Szemle, 2018. 3. sz. 8. o.
- Bodo, Lorand – Speckhard, Anne: Identifying Nefarious Telegram Users without the Help of Telegram Itself: Testing Solutions for Intelligence and Security Professionals in Fighting ISIS in the Encrypted Social Media Space. International Center for the Study of Violent Extremism, London 2017. 2. o.
- Buxton, J. – Bingham, T.: The rise and challenge of dark net drug markets. Policy Brief, 2015. Vol. 7. 3. o.
- Chertoff, Michael: A public policy perspective of the Dark Web, Journal of Cyber Policy, 2017. Vol. 2 No. 1. 36–37. o.
- Cimpanu, Catalin: Another dark web marketplace bites the dust --Wall Street Market https://www.zdnet.com/article/another-dark-web-marketplace-bites-the-dust-wall-street-market/ (2020.03.28.)
- Cox, James: Canada and the Five Eyes Intelligence Community. Canadian Defence and Foreign Affairs Institute, Calgary 2012. 4. o.
- Cox, Joseph: 7 Ways the Cops Will Bust You on the Dark Web
- https://www.vice.com/en_us/article/vv73pj/7-ways-the-cops-will-bust-you-on-the-dark-web (2020.03.28.)
- Cuthbertson, Anthony: Facebook Hack: People's Accounts Appear For Sale On Dark Web. https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-hack-data-dark-web-login-

details-cost-dream-market-a8564671.html (2020.03.28.)
- Devecsai János: Kábítószerek és bérgyilkosok a netről https://www.digitalhungary.hu/konferenciak/evolution/Kabitoszerek-es-bergyilkosok-a-netrol/5056/
- Dilipraj, E.: Terror In The Deep And Dark Web. Air Power Journal, 2014. Vol. 9. No. 3. 126. o.
- Dobák Imre: OSINT – Gondolatok a kérdéskörhöz. Nemzetbiztonsági Szemle, 2019. 7. évf. 2. sz. 83–93. o.
- Europol's 2019 EU Terrorism Situation and Trend Report (TE-SAT) 17. o.
- Europol The Internet Organised Crime Threat Assesment 2019. Europol, Hága, 2019. 44. o.
- https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019 (2020.03.28.)
- Fanusie, Yaya: Hamas Military Wing Crowdfunding Bitcoin
- https://www.forbes.com/sites/yayafanusie/2019/02/04/hamas-military-wing-crowdfunding-bitcoin/#306575c34d7f (2019. 12. 30.) (2020.03.28.)
- Felszámolták a darknet második legnagyobb portálját
- https://www.digitalhungary.hu/e-kereskedelem/Felszamoltak-a-darknet-masodik-legnagyobb-portaljat/8513/ (2020.03.28.)
- Finklea, Kristin: Dark Web. Congressional Research Service, Washington DC, 2017. 1. o.
- https://www.fas.org/sgp/crs/misc/R44101.pdf (2020.03.28.)
- Finklea, Kristin: Law Enforcement Using and Disclosing Technology Vulnerabilities. Congressional Research Service, Washington DC, 2017. 3. o. https://fas.org/sgp/crs/misc/R44827.pdf (2020.03.28.)
- Finszter Géza: Rendészettan. Dialóg Campus Kiadó, Budapest 2018. 78. o
- Gál István László: A XXI. század új bűncselekménytípusa: a terrorizmus finanszírozása. Rendészeti Szemle: Az Igazságügyi És Rendészeti Minisztérium Szakmai, Tudományos Folyóirata 2009. 57. évf. 6. sz 61–90.
- Gál István László: A pénz- és bélyegforgalom biztonsága elleni bűncselekmények. In: Polt Péter (szerk.): Új Btk. kommentár: 7. kötet, Különös rész. Nemzeti Közszolgálati és Tankönyvkiadó Zrt., Budapest 2013. 193–224. o.
- Gál István László: Új biztonságpolitikai kihívás a XXI. században: a terrorizmus finanszírozása. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat kiadványa, 2012. 1. sz. 15. o.
- Gál István László: Some thoughts about money laundering (Fenyves, Csaba – Herke Csongor – Mészáros Bence (szerk.) Bizonyítékok: tiszteletkötet Tremmel Flórián Egyetemi Tanár 65. Születésnapjára Pécs, 2006 167–173. o.
- Gehl, Robert: Illuminating the 'dark web'. https://theconversation.com/illuminating-the-dark-web-105542 (2020.03.28.)
- Greenberg, Andy: Feds Dismantled the Dark-Web Drug Trade—but It's Already Rebuilding
- https://www.wired.com/story/dark-web-drug-takedowns-deepdotweb-rebound/ (2020.03.28.)
- Guccione, Darren: What is the dark web? How to access it and what you'll find.
- https://www.csoonline.com/article/3249765/what-is-the-dark-web-how-to-access-it-and-what-youll-find.html (2020.03.28.)
- Gyaraki Réka: A kiberbűncselekmények megjelenése és helyzete napjainkban. In: Mezei Kitti (szerk.): A bűnügyi tudományok és az informatika. Pécsi Tudományegyetem Állam- és Jogtudományi Kar, MTA Társadalomtudományi Kutatóközpont, Budapest–Pécs 2019. 83. o.
- Haig Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest 2018. 301–302. o.
- Hardy, Robert Augustus – Norgaard, Julia R.: Reputation in the Internet black market: an empirical and theoretical analysis of the Deep Web. Journal of Institutional Economics, 2016. Vol. 12. No. 3. 516. o.
- Harper, Ivy: Dark Web Red Rooms: Urban Legend or Worst Content on the Deep Web?
- https://darkwebjournal.com/dark-web-red-rooms/ (2020.03.28.)
- https://www.nyest.hu/hirek/aki-megfujja-a-sipot (2020.03.28.)
- https://tika.apache.org/ (2020.03.28.)
- https://www.vpnmentor.com/blog/tor-browser-work-relate-using-vpn/ (2020.03.28.)
- https://www.vpnszerver.hu/mire-jo-a-vpn/ (2020.03.28.)
- Internet Live Stats https://www.internetlivestats.com./total-number-of-websites/ (2020.03.28.)
- Jardine, Eric: The Dark Web Dilemma: Tor, Anonymity and Online Policing. Centre for International Governance Innovation, London 2015. 7. o.
- Johnson, Bridget: ISIS: Cities Distracted by Coronavirus Should be Hit with Attacks Like Paris, London, Brussels
- https://www.hstoday.us/subject-matter-areas/counterterrorism/isis-cities-distracted-by-coronavirus-should-be-hit-with-attacks-like-paris-london-brussels/ (2020.03.28.)
- Katz, Rita: Tales of Crypto-Currency: Bitcoin Jihad in Syria and Beyond
- https://www.thedailybeast.com/the-bitcoin-jihad-in-syria-and-beyond-tales-of-crypto-currency (2020.03.28.)
- Kehoe, Shawn R.: The Digital Alleyway: Why the Dark Web Cannot Be Ignored
- https://www.policechiefmagazine.org/the-digital-alleyway/ (2020.03.28.)
- Kerr, Dara: Silk Road founder loses appeal challenging life sentence. https://www.cnet.com/news/silk-road-founder-loses-appeal-challenging-life-sentence/ (2020.03.28.)
- Kiberbűnözés a dark weben – Milyen szolgáltatások kaphatók az internet sötét oldalán és mennyit kell

fizetni értük? https://www.eset.com/hu/hirek/kiberbunozes-a-darkweben/ (2020.03.28.)
- Kiberbűnözés és a virtuális tér veszélyei – interjú az Internet Világnapja alkalmából
- https://birosag.hu/hirek/kategoria/magazin/kiberbunozes-es-virtualis-ter-veszelyei-interju-az-internet-vilagnapja (2020.03.28.)
- Lacson, Wesley – Jones, Beata: The 21st Century DarkNet Market: Lessons from the Fall of Silk Road. International Journal of Cyber Criminology, 2016. Vol. 10. No. 1. 40. o.
- Lund, Brady – Beckstrom, Matthew: Casting Light on the Dark Web: A Guide for Safe Exploration. Rowman & Littlefield Publishers, London 2019. 41.o.
- Malik, Nikita: Terror in The Dark: How Terrorists use Encryption, the Darknet and Cryptocurrencies. The Henry Jackson Society. London 2018. iv. o.
- Martinez, Fidel – Wile, Rob: Silk Road 2.0 hits dead end with FBI. busthttps://splinternews.com/silk-road-2-0-hits-dead-end-with-fbi-bust-1793842852 (2020.03.28.)
- Mattmann, Christian: Searching deep and dark: Building a Google for the less visible parts of the web
- https://theconversation.com/searching-deep-and-dark-building-a-google-for-the-less-visible-parts-of-the-web-58472 (2020.03.28.)
- McGuire, Michael: Into The Web of Profit: Understanding the Growth of the Cybercrime Economy. Bromium, Inc., Cupertino 2018. 15–16 .o.
- Mirea, Mihnea – Wang, Victoria – Jung, Jeyong: The not so dark side of the darknet: a qualitative study. Security Journal , 2019. Vol. 32. 107. o.
- Moore, Daniel –Rid, Thomas: Cryptopolitik and the Darknet. Survival: Global Politics and Strategy, 2016. Vol. 58. No. 1. 24. o.
- Nagy Zoltán András: A joghatóság problémája a kiberbűncselekmények nyomozásában. In: Homoki-Nagy Mária – Karsai Krisztina – Fantoly Zsanett – Juhász Zsuzsanna – Szomora Zsolt – Gál Andor (szerk.): Ünnepi Kötet Dr. Nagy Ferenc Egyetemi Tanár 70. Születésnapjára. Szegedi Tudományegyetem Állam- és Jogtudományi Kar, Szeged 2018. 755. o.
- Nagy Zoltán András: A kiber-háború új dimenzió – a veszélyeztett állambiztonság (Stuxnet, DuQu, Flame – a Police malware). In: Gaál Gyula – Hautzinger Zoltán (szerk.): Pécsi Határőr Tudományos Közlemények XIII: TANULMÁNYOK „A BIZTONSÁG RENDÉSZETTUDOMÁNYI DIMENZIÓI – VÁLTOZÁSOK ÉS HATÁSOK" CÍMŰ TUDOMÁNYOS KONFERENCIÁRÓL. Pécsi Határőr Tudományos Közlemények XIII. Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport, Pécs 2012. 221. o.
- Newman, Lily Hay: How a Bitcoin Trail Led to a Massive Dark Web Child-Porn Site Takedown https://www.wired.com/story/dark-web-welcome-to-video-takedown-bitcoin/ (2020.03.28.)
- Nyeste Péter – Szendrei Ferenc: Nyílt forrású információszerzés a bűnüldözésben. Nemzetbiztonsági Szemle, 2019. 7. évf. 2. sz. 66. o.
- Paliy, George: What Is The Dark Web ? https://stopad.io/blog/what-is-the-dark-web-and-how-it-is-different-from-deep-web (2020.03.28.)
- Palmer, Danny: VPN use surges as coronavirus outbreak prompts huge rise in remote working https://www.zdnet.com/article/vpn-use-surges-as-coronavirus-outbreak-prompts-huge-rise-in-remote-working/ (2020.03.28.)
- Pasca, Viorel – Orza, Daniela Simona: Terrorism: between the need for funding and obtaining funding sources. In: Journal Of Eastern-European Criminal Law, 2019. No. 1. 227. o.
- Patrick Tucker: „If You Do This, the NSA Will Spy on You", Defense One, July 7, 2014 https://www.defenseone.com/technology/2014/07/if-you-do-nsa-will-spy-you/88054/ (2020.03.28.)
- Rathod, Digvijaysinh: Darknet Forensics. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), 2017. Vol. 6. No. 4. 78. o.
- Razali, Nuruddin Bin – Suradi, Nur Razia binti Mohd: A Nest for Cyber Criminals:The Dark Web. IEEE 2019. 2.o.
- https://www.academia.edu/40783401/A_nest_for_cyber_criminals_-the_dark_web (2020.03.28.)
- Rubasundram, Geetha A.: The Dark Web and Digital Currencies: A Potent Money Laundering and Terrorism Opportunity. International Journal of Recent Technology and Engineering (IJRTE), 2019. Vol 7. No. 5. 481.o
- Saleh, Saad – Qadir, Junaid – Ilyas, Muhammad U. Shedding Light on the Dark Corners of the Internet: A Survey of Tor Research. Journal of Network and Computer Applications, 2018. Vol. 114. 1. o.
- Schäfer, Matthias – Strohmeier, Martin –Liechti, Marc – Fuchs, Markus – Engel, Markus – Lenders, Vincent: BlackWidow: Monitoring the Dark Web for Cyber Security Information. In: T. Minárik – S. Alatalu – S. Biondi – M. Signoretti – I. Tolga – G. Visky (szerk.): 2019 11th International Conference on Cyber Conflict: Silent Battle. NATO CCD COE Publications, Tallinn 2019. 3. o.
- Sui, Daniel – Caverlee, James – Rudesill, Dakota: The Deep Web and the Darknet: A Look Inside the Internet's Massive Black Box. Woodrow Wilson International Center for Scholars, Washington, DC 2015. 4. o. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2676615 (2020.03.28.)
- Symanovich, Steve: How to safely access the deep and dark webs
- https://us.norton.com/internetsecurity-how-to-how-can-i-access-the-deep-web.html (2020.03.28.)
- Szász Antónia: A kiberbűnözés társadalmi kontextusa. In: Kovács Janka – Kökényessy Zsófia – Lászlófi Viola (szerk.): A normán innen és túl. ELTE BTK Történeti Kollégium, Budapest 2017. 105. o.
- Tor And The Deep Web: Everything You Secretly Wanted To Know
- https://www.whoishostingthis.com/blog/2017/03/07/tor-deep-web/ (2020.03.28.)

- Tóth Dávid: A virtuális pénzekkel kapcsolatos visszaélések. Rendészet-Tudomány-Aktualitások: A rendészettudomány a fiatal kutatók szemével, Szerkesztette: Baráth Noémi Emőke – Mezei József, Doktoranduszok Országos Szövetsége, Rendészettudományi Osztálya Budapest 2019. 242–250. o.
- Tóth, Dávid: Credit card fraud with a comparative law approach. In: International Scientific Conference „Towards a Better Future: Democracy, EU Integration and Criminal Justice", Conference Proceedings, Volume I, Faculty of Law – Kicevo, University "St. Kliment Ohridski" – Bitola, Bitola 2019. 232. o.
- U.S. Attorney's Office: Operator of Silk Road 2.0 Website Charged in Manhattan Federal Court. https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/operator-of-silk-road-2.0-website-charged-in-manhattan-federal-court (2020.03.28.)
- Valahovits Szilvia Éva: Magyar találmány: cenzúrázhatatlan internet
- http://valasz.hu/techvilag/egy-magyar-fiatalember-feltalalta-a-cenzurazhatatlan-internetet-123507 (2020.03.28.)
- Vogt, Sabine: Das Darknet – Rauschgift, Waffen, Falschgeld, Ausweise – das digitale „Kaufhaus" der Kriminellen? Die Kriminalpolizei, 2017. No. 2. 4. o.
- Vogt, Sophia Dastagir: The Digital Underworld: Combating Crime on the Dark Web in the Modern Era. Santa Clara Journal of International Law, 2017. Vol. 15. No. 1. 114–115. o.
- Weimann, Gabriel: Going Darker? The Challenge Of Dark Net Terrorism. Wilson Center, Washington, DC 2018. 8. o.
- Weimann, Gabriel: Terrorist Migration to the Dark Web. Perspectives on Terrorism, 2016. Vol. 10 No. 3. 40-41. o.
- What is the Deep Web? The Definitive Guide [2020]
- https://www.thedarkweblinks.com/what-is-the-deep-web/ (2020.03.28.)
- Zetter, Kim: Use privacy services? The NSA is probably tracking you
- https://www.wired.co.uk/article/nsa-targeting-tor-users (2020.03.28.)