Az internet mint nemzetközi tér

Bevezetés

A számítógépes hálózatok kiépítésének lehetőségét a távíró, telefon, rádió és számítógép integrációja készítette elő. J. C. R. Licklider fogalmazta meg az *intergalaktikus hálózat* koncepcióját, amely hasonlít a mai világhálóhoz.

Az internetet is, mint annyi más tudományos felfedezést, így például a rakétatechnikát, a számítógépet, a mélytengeri búvárruhákat, az éjjellátó távcsöveket, a Global Position Systemet (GPS) vagy a mesterséges esőt, valamint további találmányokat, a katonai kutatás hívta életre.

Történetünk a II. világháború előtti évekre nyúlik vissza; a német ipari technológia szinte minden téren évtizedekkel megelőzte a világ technológiai tudását, a légi járművek, tengeralattjárók, harckocsik, a V–1 robotrepülőgépek és a V–2 rakéták jelezték a német haditechnikai fölényt. Közel kerültek az atombomba előállításához, készen voltak a helyből felszálló repülőgép és a 30-40 kilométerre távolhordó ágyúk tervei, és folytak más irányú fejlesztések is. K. Zuse megalkotta az első programvezérelt számítógépet. (Adalékként a német technikai fejlettséghez megemlítjük, hogy az 1936-os berlini olimpia megnyitójáról a német televízió színes adásban közvetített. Az USA-ban több mint másfél, a COCOM-lista miatt [is] Magyarországon közel három évtizeddel később kezdődött a színes televíziózás korszaka.)

Érthető, hogy a háborúban a szövetségesek német vagy Németországban dolgozó, dolgozni kényszerített tudóst, szakembert igyekeztek maguknak megszerezni mindenáron, magas fizetéssel, zsarolással, emberrablással és más módon politikai céljaik szerint. Csak az Egyesült Államokba 1800 tisztet, tudóst, hírszerzőt, más specialistát vittek át, ahol új életet kezdhettek.[1] Pregnáns példa Wernher von Braun esete, aki kollégáival a V–2 rakéta gyakorlati megalkotói között volt. Az egykori SS-tiszt az USA-ban a Holdra szállást célul kitűző Apolló-program egyik vezetője, sőt a NASA (*National Aeronautics and Space Administration* – Nemzeti Repülési és Űrhajózási Hivatal) igazgatója volt 1960–1970 között.[2]

[1] Erich Lichtblau: *The Nazis Next Door: How America Became a Safe Haven for Hitler's Men.* Boston – New York, Houghton Mifflin Harcourt, 2014. 2.

[2] Bob Ward: *From Nazis to NASA: The Life of Wernher Von Braun.* London, Sutton, 2006. 75–85.

https://doi.org/10.36250/01004_01

A szovjet Szputnyik-programban együtt dolgozott Konsztantyin Ciolkovszkij és Herman Oberth, aki Von Braun ellenlábasa volt a náci időkben, a V–2 rakéta egyik elméleti kidolgozója.[3]

A Szputnyik fellövésének második próbája sikeres volt 1957 októberében. Ez a siker azt is üzente a világnak, hogy a Szovjetunió interkontinentális ballisztikus rakéta segítségével gyakorlatiag bárhová bármilyen eszközt eljuttathatott, ami az USA-ban aggodalmat keltett. Válaszként 1958 januárjában létrehozták a NASA-t.

A DARPA (*Defense Advanced Research Projects Agency,* Fejlett Védelmi Kutatási Projektek Ügynöksége), az Egyesült Államok Védelmi Minisztériumának kutatásokért felelős részlege létrehozta az ARPANET-et, egy föld alatti telefonhálózatot, amely a nemzetbiztonsági szempontból fontos intézményeket, később egyetemeket kötötte össze.

1969. szeptember 2-án indult el az ARPANET. 1973-ban a hálózat részévé vált Európa, először a University College of Londont és egy norvég radarállomást kötöttek be.

1982-ben létrejött az EUNET, az első európai internetszolgáltatás Nagy-Britanniában, Hollandiában, Dániában, Svédországban, majd másutt is. Az akkori szocialista országokat természetesen kihagyták az EUNET-ből.

1985–1986-ban az ARPA-Internetet MILNET-re *(military network)* és Internetre *(internet working system)* osztották.

1991-ben a Nemzeti Kutatási Alapítvány (USA) engedélyt adott az internet kereskedelmi célú hasznosítására.

Az internet technikai értelemben „hálózatok hálózata". A hálózat többrétegű. A keresőmotorok által indexált felület a surface web, amely csupán a „jéghegy csúcsa". Ahhoz, hogy a surface web egy meghatározott tartományát elérhessük, ismernünk kell annak domainnevét. A tartománynevek felépítése hierarchikus, az elemek alá vannak rendelve egy másik elemnek.

Például az rtk.uni-nke.hu tartománynév példáján mutatva:

– .hu – a legmagasabb szintű tartománynév,
– .uni-nke – a második szintű tartománynév (főállomás neve),
– .rtk (alállomás neve).

A legmagasabb szintű tartománynevek (*top level domain* – TLD) tipikusan nemzetközi jelzések:

[3] Horvai Ferenc: Ötven éve a világűrben. *Meteor,* 37. (2007), 10. 12.

– a .com (commercial) kereskedelmi tevékenységként;
– a .biz (business) az előbbinél szűkebb körben az üzleti tevékenységként hirdeti magát;
– az .org (organization) különböző szervezetekre;
– a .gov (government) kormányzati szervekre;
– az .edu (eduacation) oktatási tevékenységre, egységekre utal (például egyetemi oldalak jelölése);
– az .info (information), tájékoztatási, informálódási lehetőséget kínál;
– a .net (network) hálózati, operátori tevékenységként hirdeti magát.

Léteznek szponzorált, legmagasabb szintű tartománynevek, így
– a .travel kiterjesztés, amely esetén utazási irodákról, utazási ajánlatokról vagy
– a .museum kiterjesztés esetén múzeumokról, kiállítótermekről nyerhetünk információkat;
– a .jobs kiterjesztés a munkát keresőknek, munkát kínálóknak ad lehetőséget.

Legmagasabb szintű tartománynevek lehetnek országkódok is, ideértve az Európai Unióra történő utalást is, például .hu, .de, .at, .uk vagy az .eu.

A fenntartott legmagasabb szintű tartománynevek:
– a .test elnevezés valamilyen új webes megoldással kísérletező oldalra utal, vagy például
– az .example oldalak webdesigner tevékenységet ígérnek.

A *deep weben* jelszóval, azonosítóval érhetők el a vállalati, intézményi adatbázisok, az e-mail és a közösségi média fiókjainak tartalma és más adatbázisok.

A *dark web* az úgynevezett *Onion Router* rejtett szolgáltatási protokollt használja. A „Tor" szerverek – a *The Onion Router* rövidítése – saját klienssel válnak megismerhetővé. A felhasználók névtelenek maradnak a protokoll által biztosított speciális titkosításoknak köszönhetően.[4]

A dark web ma még „szürke zóna", megtalálhatók a szólás- és véleményszabadságért küzdők által közölt tartalmak és a bűnözők „piaca" is.

[4] Cath Senker: *Cybercrime and the Darknet.* London, Arcturus Publishing Ltd., 2017. 117–140, Lance Henderson: *Tor and the Dark Art of Anonymity.* Amazon Media EU, 2016. 13–98, Jamie Bartlett: *The Dark Net.* London, Windmill Books, 2015. 13–303.

A weboldalak (felső szintű) tartományneve a dark weben mindig .onion.

A bűnözők anonimitásukat – többek között – proxy szervereken keresztül történő aktivitásukkal igyekeznek leplezni.

A ma ismert proxyszerver-típusok:

– anonim public proxy szerver igénybevételével is elrejtőzködhetnek a felhasználók. E szerverek „mögé" rendkívül egyszerűen el lehet bújni. Az anonim public proxynál egy „fokkal" biztonságosabb az úgynevezett
– distorting proxy szerver. Ez a fajta proxy szándékosan hamis IP-t szolgáltat, azaz a proxy szerver helyét is elrejti. A „legbiztonságosabb" mégis a
– high anonimity proxy. Ezek kifelé nem is proxynak mutatják magukat, úgy jelennek meg, mint ha maga a felhasználó hívná a célzott szervert, legfeljebb a TC/IP-szám vagy hamis (nem egyezik meg a földrajzi-matematikai képlettel kiosztott országra), vagy nem létezik.

Jelenleg nehézséget jelent, ha a felhasználó egy publikus router „mögül" lép az internetre, mivel a router nem oszt ki IP-számokat az arra kapcsolódó egyes felhasználók számára. Ebben az esetben maradnak a hagyományos nyomozati megoldások, a felhasználó által hagyott internetes lábnyomok vizsgálata, továbbá a helyszíni webkamerák felvételei, tanúk kikérdezése stb.

Ha valamilyen azonosító szükséges a wifihálózathoz, akkor némileg egyszerűbb a helyzet, de számolhatunk azzal, hogy olyan e-mail-címmel azonosítja magát, amely e-mail-cím olyan ország szerveréről működik, amely ország jellemzően nem partner a nemzetközi nyomozásokban.

A terroristacsoportok[5] saját biztonságuk miatt, valamint a terrorelhárítók működésének megnehezítése céljából úgynevezett „mozgó IP-címet" (moving IP) használnak, amely a szerverek lokalizálását és azok gyors légi vagy szárazföldi beavatkozással történő likvidálását próbálja ellehetetleníteni.

Bűncselekmények az interneten

A számítógépes hálózatokon elkövethető bűncselekményeket kriminológiai közelítéssel két fő csoportba sorolhatjuk:

[5] Jeremiah Jolliff: *Islamic extremism and cybercrime.* Leipzig, Amazon, 2017; Michael Mealer: *Internet Radicalization: Actual Threat or Phantom Menace.* US Government, Department of Defense, Naval Postgraduate School, Monterey, 2012. 7–63.

– A tartalomközlésben megvalósuló bűncselekmények jellemzően olyan tradicionális deliktumok, amelyek java részben verbálisan, de írásban is elkövethetők.
– Olyan támadások, amelyek célzott szerverekben kárt okoznak. A károk keletkezhetnek a szerverek működésének leállásától kezdve a pénzügyi viszonyok sértésén át a zsarolás miatt fizetett anyagi károkig.

1. A tartalomszolgáltatók weboldalain, a közösségi oldalakon, továbbá a felhasználók saját weboldalain, blogokban, fórumrovatokban, közösségi, torrent-, valamint egyéb fájlcserélő oldalakon vagy másutt megjelenített szöveges, képi közléseit, csatolt audio- vagy videófájljait a világ bármely pontján, bárki láthatja, elolvashatja. A közlések címzettje bármely földrészen bárki lehet, akár egyetlen személy, közösség, avagy bárki ismeretlen.

A 2000-as évektől a felhasználók tartalomfogyasztóból tartalom-előállítókká váltak; az egyéni felhasználók *tartalomközléssel is elkövethetnek* bűncselekményeket. Különösen *tiltott a gyermekpornográf, pedofil felvételek terjesztése, megosztása.*

A tradicionálisan tiltott tartalmak között találjuk a felhasználókat pénzügyi kiadásokra ösztönző, megtévesztő csalásra vagy piramisjátékra felhívó közléseket. Néhány ismertté vált megtévesztés:

– *Nigériai levelek,* amelyek ismertek 419-es csalásként is (utalva a nigériai büntető törvénykönyvben a 419. §-ban található csalásra), vagy spanyol lottóként, holland lottóként. Ezen esetekben kilátásba helyezett örökség (megnyílt egy nagy örökség, például egy diktátor vagyona), valamint nem is játszott szerencsejátékban, „kiválasztott, szerencsés" IP-cím miatt nyeremény eléréséhez (ügyvédi díjként, pénzügyi költségként stb.) anyagi hozzájárulást kérnek a csalók.
– Ismert eset az is, hogy a *közösségi oldalakon történő ismerkedést követően* az ismerkedést kezdeményező személy meg kívánja látogatni az általa kiválasztott személyt, majd az utazáskor „felmerült" problémára (ellopták a bőröndjét, pénztárcáját, repülőjegyét stb.) hivatkozva pénzt kér átutalással a meglátogatni kívánt személytől. Természetesen a meghívást kezdeményező személy megtévesztő célzattal, anyagi haszonszerzés végett teszi mindezt. Az utazást meg sem kezdte.

Filmek, zeneszámok, könyvek, kották, albumok és más *szerzők művei illegálisan fel- és letölthetők* torrentoldalakon, surface weben jellemzően warezoldalakon

pénzért, illetve ingyenesen. Különösen a torrenttechnológia kitalálása óta vált ez tömegessé. Napjaink jelensége a *streaming,* – élő vagy rögzített médiatartalom – az interneten keresztül elérhetővé válhat. A közvetítés lehet a rádió- vagy TV-állomás egész napos műsora vagy egy-egy esemény közvetítése, például sportmérkőzés, díjkiosztó ünnepség. A streamelés is lehet jogszerű, ha a rádió- vagy TV-társaság maga sugározza az adását, vagy engedéllyel veszi át a streaminghálózat a műsorát, de lehet jogellenes is, ha például egy fizetős csatorna műsorát vagy egy-egy ott sugárzott eseményt közvetítenek. Jogellenes streamelés esetén nagyon gyakran (másutt tiltott) reklámokat is találunk a program betöltésekor vagy a közvetítés megszakításakor. Az illegális streamingplatformokon vírusok is terjeszthetők.

A torrentezés, az illegális streamelés szerzői jogsértésnek minősül.[6]

A számítástechnika fejlődése tette lehetővé a *3D-s nyomtatás* technológiáját, amely alkalmas bármely, a fizikai térben létező tárgy reprodukálására. A technológiának óriási előnyei vannak: termékek prototípusainak olcsó gyártásától a manuálisan megmunkálhatatlan, létrehozhatatlan, vagy miniatűr (milliméter nagyságú) tárgyak előállításán, a helyszínen történő szervizelés lehetőségén át a gyógyászatban használatos protézisek abszolút pontos elkészítéséig sok minden megoldható. Ugyanakkor e körben az iparjogvédelem körébe tartozó védett tárgyak vagy fegyverek is előállíthatókká váltak. A jogvédett tárgyak „nyomtatásához" szükséges fájlok illegális elérésének tiltása még várat magára.[7] Reális a félelem, hogy a 3D-s fájlok elérhetősége az interneten ugyanúgy ellenőrizhetetlenné válik, mint jelenleg a digitalizált filmek, zenék le- és feltöltése.

Tartalomközlő, egyben támadó ténykedés a megfélemlítő, megalázó (cyberbullying), a társadalmi csoportot célba vevő (cybermobbing) tartalmak közlése, amely zaklatásnak minősül. A törvény főszabályként a Btk. 222. §-ban[8] meghatározott *zaklatás* tényállása alapján rendeli büntetni az ilyen cselekményeket. Szintén elérhetők az interneten *becsületsértő, nyíltan rasszista, holokausztagadó* – horribile dictu náci propaganda – közlések is.

[6] 2012. évi C. törvény a Büntető törvénykönyvről (Btk.) 385. §. Szerzői vagy szerzői jogok megsértése.

[7] Szabó Csaba: A 3D nyomtatási technológiával előállított tűzfegyverek biztonságpolitikai kihívásainak vizsgálata a fegyverrendészet aspektusából I–II. *Nemzetbiztonsági Szemle,* 5. (2017), 4. 91–124.

[8] Btk. 222. §. Zaklatás.

A pénzügyi viszonyok tisztaságát, az adórendszert sérti a *pénzmosás,* amelynek megvalósításához, elleplezéséhez tág teret teremt az internet, így például:

- a bűnszervezet (terroristaszervezet) által létrehozott, működtetett névtelen, azonosíthatatlan alapítványok bűncselekményből származó pénzekkel történő „támogatása", azaz befizetés, ami az alapítványszámlán már legális összegként jelenik meg;
- a bűnszervezet (terroristaszervezet) által létrehozott és működtetett illegális szerencsejátékokban (gambling) való részvétel, ahol a „játékos" mindig csak veszít, jóllehet csak befizet, így a gamblingszervezet számláján ez már legális összeg;
- szabad munkavállalási oldalakon (freelancer oldalak) történő fizetéssel, ahol akár a munkaadó, akár a munkavállaló ugyanaz a személy is lehet, mivel több oldalon elegendő e-mail-címmel regisztrálnia magát a felhasználónak vagy a bűnszervezet egyik, illetve másik tagjának;
- az online játékokban, ahol nem érvényesülnek piaci árak, szabadon vásárolhatók valós vagy virtuális valutában a játékhoz szükséges vagyontárgyak, vagy a játékban maradásért „élet";
- offshore számlák nyitása, azokon pénzek elhelyezése, azokról átutalások kezdeményezése;
- virtuális valutában történő adásvételek, azok átváltása valós valutára stb.

A pénzmosás büntetendő magatartás a Btk. 2012. évi C. törvény a Büntető törvénykönyvről 399. §. Pénzmosás alapján.

Az internet „életben tartója" az e-kereskedelem, színtere az üzleti (*business to business* –B2B), az üzlet és a fogyasztó közötti (*business to consumer* – B2C; *consumer to business* – C2B), valamint a fogyasztók közötti kereskedelemnek (*consumer to consumer* – C2C).[9]

Ez utóbbi üzleti kapcsolatban a felhasználók különböző aukciós, secondhand oldalakon, elektronikus hirdetőtáblákon (*electronic bulletin boards* – más elnevezéssel üzenőfalakon vagy fórumokon), az Airbnb-n és egyéb oldalakon kínálják új vagy használt cikkeiket, szállásaikat, szolgáltatásaikat, vagy kereshetik ezeket.

[9] Eszes István: *Digitális gazdaság. Az e-kereskedelem marketinges szemmel.* Budapest, Nemzeti Tankönyvkiadó, 2012. 61–126.

E körben különböző visszaélések valósulhatnak meg, ezek egy része bűncselekmény, más része polgári jogi felelősséget vet fel:

- a vevő fizetett, de az eladó nem küldte az árut, vagy
- gyengébb minőségű árut küldött;
- bűncselekményből származó (csempészett, hamis) árut kínált vagy küldött az eladó;
- a szállást bérbe vevő a bérbe adott szálláson kárt okozott, onnan
- valamilyen dolgot eltulajdonított, majd a bérbe vevő rágalmazás miatt feljelentést tehet stb.

Az alábbi bűncselekmények valószínűsíthetők: csalás, rossz minőségű termék forgalomba hozatala, fogyasztók megtévesztése, versenytárs utánzása, rongálás, vagy akár rágalmazás.[10]

Létező jelenség a bűnözők egymás között folytatott üzletelése (nevezhetjük Cr2Cr vagy *criminals to criminals* kapcsolatnak) a – fentebb említett – dark weben.

2. A tartalomközlések mellett a technika fejlődésével a társadalomra való veszélyesség korábban nem ismert formáival kerültünk szembe. Feltűnnek a valamennyiünk biztonságát közvetlenül vagy közvetve veszélyeztető visszaélések.

A *hacker* a számítástechnikai rendszerbe történt jogellenes belépését („elektronikus betörés") követően távoli országok szervereinek működését malware-ekkel, adat- vagy programmanipulációval akadályozhatja, kárt okozhat, titkot sérthet, webtartalmat írhat felül.

Hackingtámadással különösen fenyegetetté válnak az Internet of Things hálózatok, mivel minden, az internethez csatlakoztatott eszközt veszélyeztet egy hackertámadás. Minél több eszköz kapcsolódik a hálózathoz, annál inkább kitett nemcsak az eszköz, hanem az egész hálózat egy ilyen támadásnak. A hálózatba történő jogosulatlan belépéssel károk idézhetők elő, a termelési-logisztikai folyamatok megbénításától az okosotthonokban a riasztó kikapcsolásán, a tűzesetek előidézésén át az önvezető járművek baleseteinek okozásáig (fékrendszer, sebesség manipulálásával).

Napjainkban már tipikus, hogy a felhasználók wifihálózaton keresztül kapcsolódnak az internethez. A szolgáltatás publikus hálózaton (közterekben, középületekben stb.) szabadon, publikus-zárt hálózaton (például szállodában,

[10] Btk. 373. §, 415. §, 417. §, 419. §, 371. §, 226. §.

vendéglátóhelyeken stb.) jelszóval, míg magánhálózaton felhasználónév/jelszó megadásával vehető igénybe. A hacking sajátos megvalósulása a *wardriving,* amikor is az elkövető jogellenesen használja a más által előfizetett (publikus-zárt, illetve magán) és használt wifihálózatot.

Hackingtámadás célja lehet az úgynevezett *defacing* is, ami a weboldal eredeti tartalmának jogellenes felülírását jelenti. Tipikusan valamilyen protest támadás eszköze a defacing. Az elkövetők valamilyen politikai, gazdasági vagy más követelés megjelenítését, dezinformáció közlését, konkurencia lejáratását stb. jeleníthetik meg. A defacing is tiltott.[11]

A *malware-támadás* offline módon, a számítógéphez közvetlenül hozzáférve sem kizárt.

Ennek felderítése könnyebb feladatnak látszik, hiszen az elkövető közvetlenül használja a célzott számítógépet, és ennek lehet tanúja, vagy kamera is rögzítheti ezt a ténykedést. Távolról nem célzottan, számítógépeket (szervereket) is veszélyeztethet malware-támadás. A különböző malware-eket warezekben, egyéb alkalmazásokban, fertőzött bannerekben, csomagolt fájlokban és másutt helyezik el, és azokat a felhasználók telepítik eszközeikre.

Amennyiben a malware-támadás a számítástechnikai rendszer működését jogellenesen akadályozza, úgy az elkövető cselekménye büntetendő.[12]

A *zsarolóvírusok* (WannaCry, Petya, NotPetya, Jaff, CryptoLocker stb.) alkalmazása napjaink legveszélyesebb visszaélése, amely irányulhat a vállalati (ideértve a kisvállalati) szféra ellen és a védekezéssel keveset törődő, felkészületlen felhasználók ellen is. A zsarolás, bár többféle módon történik, célja minden esetben jogosulatlan anyagi ellenszolgáltatás.

A zsarolóvírust a felhasználó – figyelmetlensége, gondatlansága révén – maga tölti le és telepíti eszközére, majd a vírus lehetetlenné teszi a felhasználó számára a fájljai, könyvtárai elérését azáltal, hogy titkosítja őket. Azok feloldásáért cserébe – tipikusan – valamilyen kriptovalutát követel a zsaroló. A kifizetést követően vagy megérkezik a feloldó kód (*patch* stb.), vagy a zsaroló nem küld, esetleg hamis kódot küld, és folytatódik a zsarolás. A *police malware* lényege, hogy hatóságok nevében küldött levelek zsarolják a felhasználót egy efféle indokolással: „a felhasználó tiltott tartalmat töltött le, vagy szélsőséges csoportokkal tartott kapcsolatot, és ha fizet, akkor nem indul büntetőeljárás".

[11] Btk. 423. § (2) bekezdés *b)* pont.

[12] Btk. 423. § (1) bekezdés.

Zsarolás végrehajtható terheléses támadással történő fenyegetéssel is, amikor az elkövetők megüzenik, hogy terheléses támadást fognak végrehajtani a szerver ellen, ha nem fizet a szervert üzemeltető. Ez a cselekmény különösen azon esetekben veszélyes, amikor a szervernek 0–24 órában kell működnie, így különösen a kritikus infrastruktúrák vagy a szerencsejáték-oldalak vannak veszélyben.

A zsarolás, mivel relatív állandósággal jelen van a büntető törvénykönyvekben, a magyar Btk. szerint is büntetendő.[13]

A hálózatot irányító személy *botnet* (a robot network rövidítése) vírusokkal több tíz- (vagy akár száz-) ezer számítógép felett szerezheti meg az uralmat, és ezekkel a zombigépekkel terheléses támadásokat (DoS, DDoS) hajthat végre célzott szerver, szerverek ellen. Botnet létrejöttéhez szükséges valamilyen malware, amely a számítógép, mobiltelefon hálózathoz történő csatlakozásakor kapcsolódik a támadó szerverhez; a botnet gazdája így szerzi meg az uralmat több ezer – mit sem sejtő – felhasználó számítógépe felett. Ilyen malware (úgynevezett *exploit kit*) letölthető valamely weboldalról vagy e-mailhez csatolt fájlból, illetve egy másik programban elrejtett trójai vírusként.

A DoS *(denial of service)* támadás célja szolgáltatásmegtagadás: ebben az esetben egy számítógépet (vagy számítógépeket) használnak TCP- és UDP-csomagokkal. A DDoS *(distributed denial of service)* támadás az, amikor több rendszerről egy rendszert céloznak meg az elkövetők terheléses támadással. A célzott hálózatot több helyről származó csomagokkal bombázzák.

A bűncselekmény alapesetben az információs rendszer vagy adat megsértése.[14] Ha jelentős számú információs rendszert érint, akkor a bűncselekmény minősített esete állapítandó meg,[15] ha közérdekű üzem ellen intézik a terheléses támadást, akkor az még súlyosabban minősül.[16]

Terheléses támadás fenyegető kilátásba helyezésével zsarolás is elkövethető. A botnettel spamek is terjeszthetők.

A malware-ek másoknak történő *bitcoinbányászatra* is beállíthatják eszközeinket.

A *kémszoftverek* adatainkat, jelszavainkat, napi ténykedésünket, rutinjainkat rögzíthetik.

[13] Btk. 367. §.
[14] Btk. 423. § (1) bekezdés.
[15] Btk. 423. § (2) bekezdés.
[16] Btk. 423. § (3) bekezdés.

Az *adathalász* technikák rendkívül szofisztikáltak, ahogy az úgynevezett *social engineering* legkülönfélébb imposztori formái is színesítik az adathalászat változatosságát. Tipikusak az egy kiválasztott célcsoporttal szembeni adathalász-támadások (*spear phishing* – szigonyozás), a felső vezetőket célba vevő támadás (*executive whaling* – bálnavádaszat), a hamis címről függelmi viszonyt színlelő úgynevezett BEC, valamint adathalász e-mailek.

Az internet lehetőségeit a szervezett bűnözés is kihasználja kábítószerek, fegyverek, pornográf és pedofil tartalmak[17] pénzért történő elérésétől a hamis okiratok készítésén át a bérgyilkos bérlésén, a botnetek pénzért történő átadásán át a pénzmosásig. A pénzügyi tranzakciók kriptovalutában zajlanak, ami biztosítja a vásárló és az eladó névtelenségét.[18]

A dark weben a bűnözők áru vagy szolgáltatás értékesítőjeként, illetve megrendelőként egyaránt megjelenhetnek.

Az elektronikus kommunikáció jogszerű, vagy annak nem nevezhető *lehallgatására* pedig szinte minden államban rendelkezésre áll a csúcstechnológia.

A bűnözés elterjedtségének okai a *felkészületlen, felelőtlen felhasználók* is, akiknek ismerete sokszor alulmarad az elkövetők tudásához képest. A felhasználók könnyelmű közlései (a vagyoni helyzetükről, tartózkodási helyükről, gyűjtőszenvedélyükről, hobbijukról, szexis szelfik) a bűnözők számára hívószók lehetnek.

A felhasználók naivságát használják ki a *clickjacking-támadók.* Különlegesnek szánt videó- és más tartalom elérhetőségét kínálják, ám az odakattintót meglepetés éri, mivel a felkínált tartalom nem elérhető, azt törölték stb. Találunk

[17] Mezei Kitti – Dornfeld László: Az online gyermekpornográfia elleni küzdelem aktuális kérdései. *Infokommunikáció és Jog,* 14. (2017), 68. 32–37; Mezei Kitti: A szervezett bűnözés az interneten. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont. 2019a. 125–147; Gyaraki Réka: A kiberbűncselekmények megjelenése és helyzete napjainkban. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Budapest – Pécs, Pécsi Tudományegyetem Állam- és Jogtudományi Kar – MTA Társadalomtudományi Kutatóközpont, 2019a. 83–101.

[18] Gazdag Tibor – Kovács Zoltán: Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. *Nemzetbiztonsági Szemle,* 2. (2014), 2. 36–57; Halász Viktor*: Kriptovaluták a bűnüldözésben – új kihívások és lehetséges válaszok.* Diplomamunka. NKE NETK, 2018; Simon Béla: A kriptovaluták és a kapcsolódó rendészeti kihívások. In Mezei Kitti (szerk.): *A bűnügyi tudományok és az informatika.* Budapest – Pécs. PTE ÁJK – MTA Társadalomtudományi Kutatóközpont, 2019. 169–186; Miskolczi Barna – Szathmáry Zoltán: *Büntetőjogi kérdések az információ korában.* Budapest, HVG–ORAC, 2018. 146–165. Mezei Kitti: A kriptovaluták büntető anyagi és eljárásjogi kihívásai. *Pro Futuro,* 9. (2019b), 1. 79–98.

példát a romantikus csalásokra is, amikor érzelmi kapcsolatkeresés céljával férkőznek a másik személy bizalmába, majd valamilyen ürüggyel (pl. utazáshoz, gyógykezeléshez) pénzt kérnek.

Az interneten *a kommunikáció* is leplezhető (például végpontok közötti titkosítással), szöveges, audio- vagy videóchat formájában, számítógépen, mobileszközön. A *titkos üzenet küldésének* kedvelt formája az úgynevezett halott e-mail-fiók, ahová a felhasználók belépnek, majd kilépnek anélkül, hogy az e-mail-fiókot egyetlen adat is elhagyta volna. Ebben az esetben a be- és kilépő felhasználók a Piszkozat mappában hagyott üzenetekkel kommunikálnak.

A bűnözők is hasznát veszik a világ városait, tájait online mutató webkameráknak, vagy a Google Earth (például online) szolgáltatásoknak, amely által a kiválasztott célpont beazonosítható.

A modern technológia lehetőséget kínál a *bűnüldözés* számára is.[19] Az elkövetők tartózkodási helyének megállapításához például a mobiltelefon helymeghatározási szolgáltatása (LoCation Service) révén, vagy mobiltelefon GPS-adatai alapján. A bankkártyás fizetés helyét, idejét, összegét az ATM-ek, POS-ek, az imprinterek rögzítik. A gépkocsiban a GPS, a beépített nyomkövető tájékoztat a gépkocsi földrajzi helyzetéről. A közösségi hálók az elkövető kapcsolati hálóját, aktuális tartózkodási helyét, esetleg vagyoni helyzetét is mutatják.

A számítógépek TC/IP-szám alapján általában lokalizálhatók, feltéve, ha a felhasználó nem VPN (virtuális magánhálózat) vagy egyéb proxy szervert, publikus, publikus-zárt wifihálózat routerét használja, bár ez utóbbi esetben legalább a router helye meghatározható. Publikus-zárt hálózat használója, ha személyére adat utal (például szállodai szobaszáma), akkor nyomonkövethető, ám ha személyére nem utal semmi (például vendéglátóhelyen), akkor az elkövető nehezebben azonosítható.

Meg kell említenünk azt is, hogy az elkövetők egy része megjelenik az interneten vagy akciója előtt, vagy azt követően mintegy dicsekvésként. Mindenképpen fontos az internet monitorozása, és hogy az extrém tartalmakra, a szélsőséges elveket, gondolatokat kifejező tartalmakra, azok készítőire figyelmet fordítsunk. Ezek a közlések ugyanúgy és ugyanott megjelenhetnek, ahol más közlések is az interneten. Érdemes mesterséges intelligenciát alkalmazni a felderítés eredményessége érdekében.

Az interneten a *felhasználó azonosíthatóságát* segítik az azonos érdeklődési oldalakon az azonos nickname-ek, a közlések közös tartalmi elemei (szavak,

[19] Simon Béla: A bűnüldözés előtt álló digitális kihívások. *Magyar Rendészet,* 17. (2017), 5. 83–104.

szófordulatok, a mondatok hosszúsága stb.), vagy azok alaki jellemzői (írásjelek, smiley-k és más jegyek) segítenek az azonosításban.

Ahogy valós térben a grafológia segítheti a nyomozást, úgy az interneten a felhasználók közléseiből is lehetséges a gyanúsítotti kör behatárolására, a konkrét személyre vonatkozó személyiségi jegyek megismerése.[20]

A gyanúsított megismerésére vagy a gyanúsítotti kör szűkítésére segítséget jelent a közlések elemzése; a fogalmazás precizitása, szavak ismételt használata, írásjelek, emojik, más jelzések beszúrása stb. Az esetlegesen leírt szakkifejezések utalnak a szakmájára, hobbijára. A közlésekből kiderülhet az, hogy mennyire hajlamos szélsőséges véleményekre, azokba mennyire lovalja bele magát, extrovertált vagy introvertált személyiségről van-e szó. A közösségi oldalakon az egyes csoport(ok)hoz csatlakozása, valamint más jellemzők is tükrözik személyiségét vagy éppen érintettségét az adott ügyben. Jellemzően a web2 nyilvánosságát használják fel közléseik közzétételére.

Legalább ennyire fontos a gyanúsítottnak, gyanúsítotti körnek a közösségi oldalakon (még) fellelhető kapcsolatrendszere, amelyből baráti, családi és vagyoni viszonyai megismerhetők.

Rendőrségi eljárás hírére a közösségi oldalakon fellelhető ismerősök általában megszüntetik az ismeretséget.

Új problémák a jogban

Digitális környezetben a hagyományos jogi fogalmak, intézmények, szabályok alkalmazhatósága aggályokat vetett fel.

A valós térben elkövetett bűncselekmények nyomai, bizonyítékai közvetlenül érzékelhetők, láthatók a személyi sérülés nyomai, a megrongált vagyontárgyak, vagy éppen hiányoznak ezen dolgok, mert ellopták, elrabolták azokat stb. Azaz mind a bűncselekmény elkövetési tárgyai, mind a bűncselekményre utaló bizonyítékok közvetlenül érzékelhetők.

Ezzel szemben az elektronikus adatok csak más technikai eszköz alkalmazása révén tehetők láthatóvá, nyernek értelmet.

Valós térben a sértett általában közvetlenül és azonnal érzékeli az ellene indított támadást, mert például testi sérülést szenvedett, a dolgát megrongálták,

[20] Ürmösné Simon Gabriella: Miben segítik a nyelvi ujjnyomok a nyomozást? *Magyar Rendészet,* 19. (2019), 1. 65–75.

ellopták. Virtuális térben a sértett korántsem biztos, hogy érzékeli a támadást. A fájlok, könyvtárak, helyükön vannak, ám a fájlok, könyvtárak tartalmát az elkövetők ellopták (le-, illetve kimásolták). Majd e szöveges, fénykép-, audio-, videótartalmakat (például manipulálva vagy anélkül zsarolási, illetőleg lejáratási célzattal) felhasználják a sértettel szemben. Megjeleníthetik közösségi oldalakon vagy másutt az interneten, ami a sértett számára kedvezőtlen, kínos következményekkel járhat.

A felhasználó azt látja, hogy számítógépe működik, minden funkcióját ellátja, tud böngészni, e-mailt írni, rádiót hallgatni stb. De nem kizárt, hogy a felhasználó számítógépe már zombigép, része egy robot networknek, egy másik személy (a botnet gazdagép felhasználója) átvette az uralmat a sértett számítógépe felett, számítógépe, mobiltelefonja már másnak bányászik bitcoint vagy más virtuális valutát. Az átlag felhasználó legfeljebb azt érzékeli, hogy számítógépe lassabb, nehezebben tölti be a kívánt weboldalt, meg-megszakad az internetes rádió, televízió adása stb., valószínűleg nem is gyanakszik arra, hogy a számítógépe egy terheléses támadásban vesz részt, és éppen egy célzott szerver működésképtelenné tételében használják mint eszközt.

Valós térben az elkövető és a sértett sok esetben *face to face* áll szemben egymással, akár személyleírás is van a támadóról, vagy a sértett a bűncselekmény célzata, motívuma (mint a tényállások esetleges alanyi elemei), személyi, üzleti vagy más kapcsolatai alapján tudja, sejti, behatárolhatja a támadó kilétét, ami a nyomozásban fontos szempont, segítség.

Virtuális térben az elkövető az esetek nagy részében ismeretlen marad. A személyiséglopás, a jogtalan vagyoni haszonszerzési cél, egy szerver működésképtelenné tétele nem mutat az elkövetők irányába. Természetesen, ha a támadó ismertté szeretné tenni magát, vagy az elkövetés körülményei miatt ismert lesz (például defacing), akkor az elkövető(k) meghatározható(k).

Továbbmenve a valós és a virtuális térben elkövetett bűncselekmények közötti különbség vizsgálatában: a különbség komoly jogi dilemmát is okozhat. A valós térben elkövetett bűncselekmény elkövetési helye általában *(locus delicti)* adott, ami alapján a joghatóság, a hatásköri és az illetékességi szabályok kijelölik az eljáró hatóságokat. A hálózati tevékenységnek több helyen lehet hatása, nemcsak azon a helyen, ahol a felhasználó használta eszközeit, hanem ott is, ahol aktivitásának eredménye megjelenik. A bűncselekmény tényállási elemei sokszor különböző földrajzi helyeken lokalizálhatók.

A joghatóság problémája jól jelzi a büntetőjogi jogharmonizáció vagy akár europaizálódásának[21] elmaradását, szemben az évszázadok óta a társadalom együttélését, fejlődését biztosító tulajdon-, birtok-, házassági, öröklési, kereskedelmi stb. viszonyokat rendező, precízen kimunkált, utat mutató római joggal.

Ha a számítógépek (szerverek), hálózatok fizikailag elérhetők Magyarországon vagy a zászló-elv szerinti magyar felségterületen, akkor a bizonyítékok megszerzése általában jogilag nem, legfeljebb technikailag okoz nehézséget.

Ha a számítógép (szerver) nem Magyarországon működik, akkor nemzetközi bűnügyi jogsegély igénybevétele a lehetőség.

A nemzetközi bűnügyi jogsegélyről szóló 1996. évi XXXVIII. törvény helyett az Európai Unióba tartozó állam esetében a 2012. évi CLXXX. törvényt kell alkalmazni. A 2001. november 23-án kelt Számítástechnikai Bűnözésről szóló Egyezmény (Egyezmény) bűnügyi jogsegély hiányában is megnyitja az egyezményben részes országok számára az együttműködést.

E szerint „a Szerződő Fél megkeresheti a másik Felet, hogy a területén található számítástechnikai rendszer útján tárolt adatokat átvizsgálja vagy azokhoz más hasonló módon férjen hozzá, foglalja le vagy más hasonló módon szerezze meg, illetőleg adja át".[22]

Izgalmasabb kérdés egy másik állam területén működő számítógépből, számítástechnikai hálózatból történő bizonyítékszerzés lehetősége. Az Egyezmény szerint bármely ország más szerződő állam beleegyezése nélkül:

– a publikusan elérhető *(open source)* adatokhoz hozzáférhet;
– a másik Szerződő Fél területén tárolt számítástechnikai adathoz hozzáférhet, vagy a területén levő számítástechnikai rendszer útján azt megszerezheti, amennyiben a Fél beszerzi az adat számítástechnikai rendszer útján történő átadására jogszabályban feljogosított személy önkéntes és jogszerű hozzájárulását.

Az első esetben a bármely ország felhasználója által szabadon elérhető adatállomány elérése megengedett, másik esetben az adatállományhoz a feljogosított vagy illetékes személy önkéntes és legális hozzájárulásával szerezhet meg adatokat.

[21] Nagy Ferenc: Az európai büntetőjog fejlődési irányairól és jogállami alapjáról. *Acta Universitatis Szegediensis Acta, Juridica Et Politica, Tomus LXI.,* (2002). Szeged. 308.

[22] Számítástechnikai Bűnözésről szóló Egyezmény 31. pont.

Minden más esetben a kölcsönös jogsegély keretében közreműködnek az adatok összegyűjtésében.[23]

A felhőszolgáltatás mint idegen tárhelyek igénybevételének ötlete már az 1960-as évektől felmerült. Ez esetben a jogi kihívás a tárolt inkriminált adatállomány, különösen előállítója adatainak elérhetősége. Nem lokalizálható, hogy mely országban vannak az inkriminált adatot tároló szerverek, mivel az adatok elérésük biztonsága miatt folyamatosan áramolnak. Kérdés, hogy a tárolás éppen aktuális helyén milyen szabályok hívhatók fel (GDPR, az Adatvédelmi Pajzs vagy más szabályok alkalmazhatók?). Egy megoldás marad: a felhőszolgáltatóhoz fordulni, ahol a választ vagy a kérést teljesíthetik vagy elutasíthatják. A megkeresés sikere függ a felhőszolgáltatást alapító cég bejegyzése helyének jogszabályaitól, jellemzően az USA jogi szabályozásától (például a véleménynyilvánítási szabadság megítélésétől). A felhőszolgáltatók a legsúlyosabb bűncselekmények esetében hajlandók megosztani információikat.

Ugyanakkor, ha a szolgáltató nem adja ki a kért adatokat, gyakorlatilag a „koronabizonyítékokat" tagadják el a hatóságok elől. A politikai és nagyvállalati érdekek – jelen pillanatban – nehezítik a nemzetközivé vált bűnözés közös üldözését. A jövő a politikai akarat és a nagyvállalati érdekek metszéspontjában dől el.

A joghatóság kérdésében nyilvánvaló problémát jelent, hogy egy kiberbűncselekmény több államot érint (ahol a törvényi tényállás egy-egy eleme megvalósul, egyik országban lenyomják a billentyűt, egy másik országban keletkezik a kár, egy harmadik országbeli elkövető hajtja végre a bűncselekményt, több országban utaztatják, bújtatják a pénzt, közben több országon keresztül zajlik az internetes kapcsolat; és sorolhatnánk azokat az okokat, amelyek a kiberbűncselekmények joghatóságának megállapítását nehezítik).

Ugyanakkor – horribile dictu – az is előfordul, hogy bármely okból egyetlen ország sem hajlandó (tud) nyomozást indítani.

A probléma megoldása lehetőségének felvillantásához vissza kell nyúlni egy 1926-os esethez, amely a nemzetközi jogi gondolkodásban paradigmaváltást hozott. Az úgynevezett Lotus-ügyben az Állandó Nemzetközi Bíróság kimondta, hogy nincs a nemzetközi jognak olyan szabálya, amely a lobogó államának kizárólagos joghatóságát állapítaná meg, azaz a területi hatályt kiterjesztő lobogó-elv *(flag principle)* is megtörhet.

[23] Számítástechnikai Bűnözésről szóló Egyezmény 33–34. pont.

A bíróság szerint a nem tevés csak igen kivételes esetben lehet szokásjog-keletkeztető (úgynevezett negatív) gyakorlat.[24]

A kiberbűncselekmények nyomozásához alapvetőnek kell(ene) tekintenünk az Eurojust (az Európai Unió Büntető Igazságügyi Együttműködési Ügynöksége) 2003-as Éves Jelentését.[25] Mivel a számítógépes környezetben nemritkán a bűncselekmények megvalósulásának csupán egyetlen eleme detektálható, értelmezhető a nemzeti hatóságok számára, ezért az eljáró hatóságoknak a joghatóság megállapításához figyelembe kell(ene) venniük:

- azt a helyet, ahol a bűncselekmény legnagyobb részét elkövették;
- azt a helyet, ahol a kár vagy veszteség jelentős része keletkezett;
- a gyanúsított vagy vádlott tartózkodási helyét; valamint
- más joghatóságok számára történő átadásának vagy kiadatásának lehetőségeit;
- a gyanúsított vagy vádlott állampolgárságát vagy lakóhelyét;
- a gyanúsított vagy vádlott jelentős érdekeit;
- a sértettek és tanúk jelentős érdekeit;
- a bizonyítékok elfogadhatóságát vagy
- az esetlegesen előforduló késedelmeket.

A felsoroltak egyben sorrendet teremtenek, tehát a versengés – elméletileg – kizárt, mert bármely fent említett körülmény – figyelembe véve azok sorrendjét – megalapozhatja a joghatóságot.

Az európai ügyészek szervezetének iránymutatásában megfogalmazottakat érdemes volna átültetni a magyar jogba.

A kiberbűnözés elleni harcban nemzetközi és hazai szervezetek is részt vesznek, gyakorlati és tudományos iránymutatásokkal. 2004-ben kezdte meg működését az ENISA *(The European Union Agency for Cybersecurity),* amely praktikus tanácsokkal és megoldásokkal szolgál az EU-tagállamok köz- és magánszektorbeli szereplőinek a hálózat- és információbiztonság területén. Az ENISA kiberbiztonsági gyakorlatokat szervez, segíti a tagállamokat kiberbiztonsági stratégiájuk kidolgozásában. A hálózatbiztonságért felelős nemzetközi és nemzeti szervezetek közötti együttműködés megteremtése is céljai közt szerepel.

[24] Dérné Hopoczky Janka: Univerzális joghatóság pro és kontra. *Jogi tanulmányok,* 14. (2010), 2. 339–354.

[25] Online: http://eurojust.europa.eu/doclibrary/corporate/eurojust%20Annual%20Reports/Annual%20Report%202003/Annual-Report-2003-EN.pdf, 62–64.

1999-ben alapították az Europolt, majd azon belül 2013-ban a *European Cyber Crime Centre*-t (EC3). Az EC3 által évről évre kiadott IOCTA *(Internet Organised Crime Threat Assessment)* Jelentés ajánlásokat fogalmaz meg a bűnüldöző szerveknek, törvényhozóknak annak érdekében, hogy hatékony és összehangolt módon reagálhassanak a számítógépes bűnözésre. A Jelentések az interneten szabadon elérhetők, visszamenőleg is.

A Készenléti Rendőrség Nemzeti Nyomozó Irodánál (KR NNI) a nemzetközi bűnügyi együttműködéssel járó feladatok, jellemzően az információcsere és a közös nyomozások feladatai összpontosulnak. Az NNI együttműködése folyamatos a rendőrséggel, a Nemzeti Adó- és Vámhivatallal, az Országos Katasztrófavédelmi Főigazgatósággal és a titkosszolgálatokkal is.