DOI:10.38146/bsz-ajia.2012.v60.i6.pp108-125

NAGY ZOLTÁN ANDRÁS

A szervezett bűnözői jelenségek a számítógépes hálózatokon

A modern technika vívmányait – mintegy a fejlődés árnyoldalaként – a bűnelkövetők is fel-, illetve kihasználják.[1]

A cím azért óvatos, mert nemcsak a szervezett bűnszervezet büntetőtörvény-beli fogalma[2] alapján vizsgáljuk a problémát, hanem a bűnszervezet dogmatikailag egzakt fogalma mellett idevesszük azokat a jelenségeket is[3], amelyekben a szervezettség bizonyos vonásai[4] tetten érhetők. Ezeket a vonásokat, jellemzőket az alábbiakban láttuk, láthatjuk számítógépes hálózaton:

1. *Egyetlen bűncselekmény* elkövetéséhez nem igazán éri meg a befektetés:
   a) Legális, viszonylag bürokratikus tevékenységek szükségesek: doménnév-igénylés, tárhelybérlés, a később pénzmosodának szánt alapítvány létrehozása, esetleg engedélyek beszerzése legális, ám a későbbiekben fedőtevékenységek (szerencsejátékok) lebonyolításához engedély megszerzése.
   b) Anyagi befektetést is igényel: internet-hozzáférés költsége, a weboldalkészítés munkadíja, annak feltöltésének munkadíja, tárhelybérleti díj, weboldal tükrözéséhez vagy TC/IP-szám leplezésére alkalmazás (program) megvásárlása stb.
2. A *munkamegosztás* is szükségszerűen megjelenik e körben, ahogy ez a többek által elkövetett bűncselekmények esetében jellemző. Ennek oka, a számítástechnikai ismeretek sokrétűsége és kapcsolódó tevékenységek:
   a) A weboldal elkészítése: ma az interneten több helyről letölthető (díjmentesen vagy ellenszolgáltatás fejében, regisztrációval vagy anélkül) web-

1 Papp Péter: Hi-tech bűnözés napjainkban. Belügyi Szemle, 2001/11–12., 5. o.; Anamaria Cristina Cercel: Criminologie. Editura Hamangiu, 2009, p. 101.

2 Btk. 137. § 8. pontja szerinti bűnszervezet fogalma: három vagy több személyből álló, hosszabb időre szervezett, összehangoltan működő csoport, amelynek célja ötévi vagy ezt meghaladó szabadságvesztéssel büntetendő szándékos bűncselekmények elkövetése.

3 Guillemette de Vericourt: A maffia. Alexandra Kiadó, Pécs, 1995, 5–9. o.

4 Korinek László: Kriminológia II. Magyar Közlöny Lap- és Könyvkiadó, Budapest, 2009, 338–339. o. A kialakuló munkamegosztás megfigyelhető más jogsértések esetében is. Lásd erről Gyaraki Réka: Az online elkövetett szerzői vagy szerzői joghoz kapcsolódó jogok megsértésének bűncselekménye. Infokommunikáció és Jog, 2010/6., 220. o.

oldalsablon. Ezek egyszerűek, kielégítik a nagyon alapszintű igényeket, átalakításuk azonban már némi szakismeretet igényel. Természetesen megrendelésre a legapróbb igények kiszolgálására is készítenek weboldalt, több-kevesebb díjazás fejében.

b) Weboldal feltöltése: egy-egy weboldal elkészítését, esetleg feltöltését, sőt a tárhelyszolgáltatást – vagy mindezeket együtt – legális gazdasági vállalkozások is elvégzik, elvégezhetik. Ha a (fedő)tevékenység (alapítvány, szerencsejáték folytatása, használt holmik árusítása, vagy az árusítás megszervezése stb.) nem tiltott, akkor a legális vállalkozások elkészítik és fel is töltik a weboldalakat. Némi szakismerettel az elkövetők is megtehetik. Ha a tiltott tartalom megjelenítése már bűncselekmény, akkor a webtartalom feltöltése akár tettesi, akár bűnsegédi magatartásnak is minősülhet, attól függően, hogy a számítógépes hálózaton való megjelenítéshez milyen további tevékenységek szükségesek. A tiltott tartalom (pornográf, pedofil, kábítószer-terjesztés, illegális szerencsejáték stb.) feltöltése azonban már kockázatos a legális vállalkozások számára. Megfelelő díjazás ellenében azonban ezek a vállalkozások is – minden bizonnyal – elkészítik, bár inkább az elkövetőktől várhatjuk a tiltott tartalom feltöltését. A webtartalom elkészítése, karbantartása, a tiltott termékek előállításának, majd árusításuk megszervezése, raktározása, vagy éppen az illegális szerencsejáték kitalálója, szervezője, lebonyolítója, a beérkező pénzekhez bankszámlát nyújtó, majd később a pénzmosó már jellemzően más-más személy.

A munkamegosztás megjelenik más tevékenységek során is.
Az internet hozzáféréséhez szervert nyújtó és a tárhelyszolgáltatóval szerződést kötő tárhelybérlő személye elkülönülhet.

Az internet elérése legálisan a hozzáférést nyújtó szolgáltatón vagy tárhelyszolgáltatón keresztül lehetséges. Ezután kezdődhetnek a trükközések az előfizető vagy a számítógépe (szervere) elrejtésére.

Magyarország határain (vagy óceánon) túl van a szerver. Ez a joghatóság kérdését veti fel: a szerver Magyarországon van, de tartalmát az országon kívüli szerver weboldalára tükrözik. A „tükrözés” nem bonyolult tevékenység, bár némi gyakorlottságot igényel.[5] A joghatóság kérdése általában aggály-

5 Tükrözéshez talán a Teleport Pro, a Wget, a WebWhacker vagy a Webcopier alkalmazások a legnépszerűbbek. Vélhetően a regisztrációmentes programok vannak előnyben. Az igényesebb fizetős alkalmazások akkor, ha a díjfizetés leplezett vagy anonim lehet.

mentes. Bár, ha a tiltott tartalom (rasszista, pornográf, becsületsértő, rágalmazó, személyes adatokat illetéktelenül közlő stb.) a hazai szerveren van, de még nem jelent meg a külföldi weboldalon, akkor a bűncselekmény előkészülete merül fel, már ha a törvény abban a bűncselekményben az előkészületet büntetni rendeli. (A példaként említett esetekben az előkészület nem merül fel.)

Anonim vagy public proxy szerverek „takarhatják ki" a valódi szervert. Ezek a „kalózszerverek" legfeljebb egy-egy cselekmény elkövetésénél játszhatnak szerepet, folyamatos megjelenés elrejtésére nem igazán alkalmasak. Különösen a distorting proxyk a furfangosak, amelyek alapfunkciójukban hamis IP-címet mutatnak a host szervernek.

A proxyláncolás során egyik proxyról a másikra, onnan a harmadikra és így tovább, majd a (például a Magyarországon szerkesztett) weboldal egy távol-keleti vagy karib-szigeteki ország szerveréről kerül az internetre. Hatásosságát rontja a sávszélesség csökkenése. De a sebességcsökkenésből eredő hátránnyal szemben előnye lehet, hogy (utolérhetetlen ország utolérhetetlen szolgáltatója miatt) a weboldal viszonylagos biztonságban jelenhet meg az interneten.

Más programok is léteznek a TC/IP elrejtésére, például a Hyde My IP stb.

De megjelenik a *haszonszerzési cél* a bűncselekmények elkövetésében: a befektetés megtérülése, illetve a megélhetéshez szükséges részbeni vagy teljes összeg előteremtése. Ez elérhető a tiltott tartalom árusításából, szolgáltatásából, hamis áruk, termékek árusításából, kábítószerek eladásából eredő bevételből, vagy a modern technikai zsarolás útján is (DDoS-támadással való fenyegetéssel).

A kommunikáció, a kapcsolattartás lehetősége a számítógépes hálózatokon

A számítógépes hálózatok a hidegháború idején az Egyesült Államokban épültek ki először, mégpedig a sikeres szovjet szputnyik kilövése után, amivel a Szovjetunió „üzent", hogy képes a távolságokat nagy hatótávolságú rakétákkal áthidalni, és a kijelölt célpontba juttatni őket. Az Egyesült Államoknak lépnie kellett, hiszen az „üzenet" világos volt: már nem lehet egyetlen vezetési pontról irányítani a hadsereget, ahhoz több vezetési pontot kell létrehozni, amelyek között egy hálózatot építettek ki. Ha minden igaz, négy vezetési pont létezett a hatvanas években.

Tehát a számítógépes hálózatok kiépülését a gyors kommunikáció indokolta. Mára a kommunikáció eszköztára a technikai elemek fejlődésével fokozatosan bővült. Ezt a technikai repertoárt (e-mail, chat, twitter, Skype, wapolással mobiltelefonról) a bűnözők is minden bizonnyal használják.

Az írott, elektronikus jelekkel létrejövő kapcsolat lehallgatásának van a legkevesebb technikai akadálya. A waphoz használt mobiltelefonénak szintén, így ezek a kommunikációs formák háttérbe szorulnak.

A Skype lehallgatása nehézkes. A Skype-szoftver a szöveget nagyon sok apró csomagra darabolja fel, majd több szerveren keresztül juttatja célba. Nincs tehát közvetlen kapcsolat a hívó és a hívott fél között. A kódolás előtt kell(ene) lehallgatni a beszélgetést. A legutóbbi hírek szerint találtak megoldást a Skype-on keresztül lebonyolított beszélgetés lehallgatására.[6]

A kommunikációt segíthetik az egyoldalú közlendők, közlemények, tájékoztatások, amelyek feltűnhetnek, pontosabban elrejtve jelennek meg weboldalakon, elektronikus hirdetőtáblákon. Ezek megismerése a weboldalak tömegessége miatt nehézkes.

A számítógépes hálózatok alkalmassága tagtoborzásra, hálózatépítésre

Mivel a számítógépes hálózatok alkalmasak kommunikációra, így ezzel az opcióval személyes, közösségi kapcsolatok kialakítására is.

E lehetőséggel a szervezett bűnözői körök is élhetnek. A fekete bárányból biztonságtechnikai szakértővé avanzsált hackerlegenda, *Kevin Mitnick*[7] a könyvében leír egy esetet: egy ismeretlen arra vett rá egy dicsekvő fiatalembert, hogy először a Kínai Műszaki Egyetem hallgatói adatbázisát, később a Lockheed Martinnál a Boeingek biztonságtechnikai rendszerének leírását szerezze be, azaz ezekért a dokumentumokért törjön be a számítógépes rendszerbe. A megbízás teljesítése után a megbízó elérhetetlenné vált. A fiatal hacker egy indiai Boeing elrablásakor szembesült azzal, hogy kivel is állt kapcsolatban. Az Egyesült Államok rendőrsége is megtalálta az összefüggést

6 http://computerworld.hu/lehallgathato-skype.html

7 Kevin Mitnick (1963–) öt évet ült börtönben különböző számítógépes bűncselekmények miatt. A legismertebb és legvédettebb számítógépes hálózatokba tört be, sok tízezer ügyfél adatait szerezte meg. Ma számítástechnikai biztonságtechnikai vállalkozása van. Két könyve jelent meg magyarul: A megtévesztés művészete. Perfect Kiadó, Budapest, 2003; A behatolás művészete. Perfect Kiadó, Budapest, 2006. Ezekben saját ismereteit, tapasztalatait osztja meg az olvasókkal. 2005-ben Budapesten is tartott előadást. Könyvei igen hasznos olvasmányok az e téma iránt érdeklődőknek.

a géprablás és a hacker tevékenysége között, így röviddel a géprablás után elfogták a fiatalembert.[8] A beszervezett hacker „lebukása" után – természetesen – a beszervező eltűnt a kibertérben. E toborzási mód a különös szakismerettel felvértezett, egy-egy részfeladat elvégzésére alkalmas személy beszervezésekor jöhet szóba. Ideális találkahelyek erre a chatszobák.

DoS-, DDoS-támadás zsarolás, terrorcselekmény, szabotázs céljával

A számítógépes környezetben elkövetett zsarolás sem új keletű jelenség: a kilencvenes évek elején *Lewis Popp* vírusos lemezeket küldött szét a világ több országába, mint az AIDS legújabb tudnivalóiról szóló ismertetőt, ám a lemezen lévő vírus 90 nap múltán aktívvá vált, hacsak a gyanútlan felhasználó nem rendelt – persze, jó pénzért – egy másik, a vírust hatástalanító lemezt.[9]

Korábban is ismert voltak vírusok, férgek, logikai bombák által az adatállományban vagy a programokban okozott károk előidézése.

Napjainkban a felhasználók tudtán kívül hálózatba vont terheléses támadás alkalmas zsarolás és más bűncselekmények végrehajtására. Szinte naponta újabb és újabb fogalmakat (botnet, spambot, DoS, DDOS, stuxnet stb.) kell megismernünk, hogy megértsük a ránk leselkedő veszélyeket.

A szervezett bűnözés sem tesz mást, mint felhasználja azokat a lehetőségeket, amelyek destruktív támadások indítására alkalmasak.[10] Ma vírusokkal, egyéb destruktív programokkal történő vagy a weboldal *deface*-elésének (átalakításával, átformálásával, más tartalom feltöltésével) fenyegetésével kívánják céljaikat elérni. A valós térben folytatott bűncselekmények átkerülnek a virtuális térbe is.

Botnet, terheléses támadás – röviden

Hálózati hibakereséskor az ügyfél, az egyéni felhasználó és a (például internet-) szolgáltató szervere kapcsolatuk ellenőrzésére (azonosításra) néhány

8 Kevin Mitnick – William Simon: A behatolás művészete. Perfect Kiadó, Budapest, 2006, 27–59. o.
9 Nagy Zoltán: Bűncselekmények számítógépes környezetben. Ad-Librum, Budapest, 2009, 257. o.
10 Mezey Nándor: Digitalizált bűnözés – digitalizált védelem. Rendészeti Szemle, 2009/5., 40–45. o.; Sebők János: A harmadik világháború. Mítosz vagy realitás. Népszabadság könyvek, Budapest, 2007, 88–93. o.

rövid adatcsomagot vált egymással. A hívó fél számítógépének adatcsomagjára a hívott fél számítógépének válaszolnia kell.

Ezt a technikai megoldást használják fel az úgynevezett terheléses támadás, más néven DoS vagy több számítógép részvételével DDoS-támadás végrehajtásakor. Ezekben az esetekben nagyobb mennyiségű adatcsomag érkezik a megtámadott gépre, mint amennyire a szerver válaszolni képes lenne, illetve amennyi adatcsomagot fogadni tudna. A szerver ilyenkor általában vár (hiába vár) a kliens gép megerősítő válaszára, és amíg vár, addig áll a szerver.

Az egyszerű DoS-támadás esetén a támadó és megtámadott számítógép között nincsenek közbeiktatott, rendszerbe állított számítógépek. DDoS-támadás esetén – mint ahogy az elnevezésből következik – további, a rendszerbe állított számítógéppel történik a támadás, amelynek következtében a megtámadott szerver lebénul. A rendszerbe állított számítógépek az úgynevezett zombigépek[11], amelyeket egy-egy program aktivál az adatcsomagok elküldésére. Ezeket a programokat a felhasználók töltik le, amikor valamilyen alkalmazást, játékot, egyéb programot töltenek le egy-egy weboldalról, vagy fájlcseréléskor stb., majd a letöltött programok kibontásával együtt – tudtukon és akaratukon kívül – betöltik azokat a programokat is, amelyek a számítógépüket terheléses – támadás eszközévé teszik. A botnetbe (százával, ezrével) vont (zombi) számítógépek terheléses támadása (több ezer számítógép pingjére) óriási károkat okozhat azzal, ha megbénítja a célba vett szervert, amely lehet egy erőműnek, egy repülőtérnek, vagy akár egy banknak a szervere is.

Már ismertek olyan esetek, amikor az elkövetők azzal fenyegettek meg internetes vállalkozásokat, hogy ha nem küldenek bizonyos pénzösszeget nekik, akkor terheléses támadást intéznek a szervereik ellen.[12] Az elkövetők olyan weboldalakat választottak célpontul, amelyeknek a folyamatos és zavartalan működés létszükséglet (például online kaszinó oldalak). A célpont tehát nyilván jól megválasztott.

Látható tehát, hogy egy modern technikai megoldásokkal klasszikus vagyon elleni bűncselekmény, nevezetesen a zsarolás (Btk. 326. §) is elkövethető.

A botnet veszélyére figyelmeztet egy 2011-es felmérés, amely szerint Magyarország a botfertőzött számítógépek esetében a kilencedik helyen áll, minden huszonötödik botfertőzött számítógép Magyarországon működik.[13]

11 Sütő János: Spamtelenül – minden a spamről. SZAK Kiadó, Budapest, 2008, 61. o.
12 http://www.sophos.com/pressoffice/news/articles/2006/10/extort-ddos-blackmail.html
13 http://infovilag.hu/hir-17557-symantec_jelentes_kiberbunozesrol_magyar.html

Az adathalász weboldalak származási helyét illetően Magyarország az első tíz között van Európában.[14]

Illegális szerencsejáték szervezése

Az illegális szerencsejáték szervezése tipikusan hosszabb távra szervezett játék. A szervezett csoportok adómentes bevételhez jutnak. Az illegális szerencsejáték mindig is vonzotta azokat, akik el kívánják kerülni az adózási és egyéb kötelezettségeket.[15]

Az illegális pénznyerő automaták valós térben (például vendéglátóhelyen) történő üzemeltetésével szemben a virtuális térben leginkább az elrejtőzés (a sok millió weboldal között), az anonimitás, a bevételek tisztára mosása jelenti azt az előnyt, amelyért ezek a játékok ott szerveződnek.

A számítógépes hálózatokon is, akár a valós térben, elterjedtek a különféle szerencsejátékok (póker, rulett, slotjátékok, blackjack, baccara, craps és más játékok) és fogadási oldalak. A pókerjátékot olyan népszerűvé tették a sportcsatornák, hogy több száz pókeroldal működik az interneten. Az online kaszinókat nem kereső felhasználók is beleütköznek az online kaszinók reklámjaiba egy-egy keresőoldalon vagy bulvároldalakon.

A legtöbb online kaszinó, akár legális, akár illegális, ingyenes, kedvcsináló, demójátékot ajánl a felhasználóknak, és mivel a kaszinó jellemzőit mutatják, megismertetik a felhasználókkal a kaszinót.

Ami ennél fontosabb, az illegális online kaszinók, fogadási oldalak weboldalai megtévesztően hasonlítanak a legális kaszinók weboldalaira. Ez könnyedén tévedésbe ejtheti a tájékozatlan felhasználót. Az illegális kaszinókat tévedésből vagy tudatosan választók vonzó jellemzőkkel találkoznak.

Az oldalak népszerűségének több oka van, így például magasabbak az oddsok, többet lehet nyerni, mivel a nyereményt nem terhelik adók (sem nyereményadó, sem személyi jövedelemadó) és más kiadások. Az illegális online kaszinóban fogadóknak azonban számolniuk kell azzal, hogy a nyereménykifizetés bizonytalan is lehet.

Előfordul, hogy a kaszinó vagy fogadójáték egyben pénzmosás színtere is. Az ismeretlen felhasználókkal korrektnek nevezhető módon játszanak, de a „bennfentes" felhasználók csak vesztenek, azaz csak befizetnek oda.

14 Elegendő lenne a csalás előkészületének büntetni rendeltsége a phishing ellen.

15 Farkas Imre – Jávorszky József: Az illegális pénznyerő automaták felderítése. Rendészeti Szemle, 1993/5., 58–59. o.

A szerencsejáték jogi megítéléséről megállapítható, hogy nem a szerencsejáték minősége teszi tiltottá, illegálissá, hanem az a tény, hogy a játék szervezőjének nincs jogosultsága szerencsejáték szervezésére. A szerencsejáték szervezése általában minden országban állami monopólium. A szerencsejáték lebonyolítása átengedhető koncessziós szerződés alapján. Az engedéllyel bíró ezt a jogosultságot más, mások számára tovább nem engedményezheti (nem adhatja tovább).

A magyar jog (Btk. 267. §) szerint a tiltott szerencsejáték szervezése akkor állapítható meg, ha az rendszeres, azaz több vagy előre meg nem határozott számú játékra irányul, és e játékok között viszonylag rövid idő telik el.

A számítógépes hálózaton szervezett illegális játékra a rendszeresség – már csak a befektetések megtérülése, továbbá a haszonszerzési cél miatt is – mint tényállási elem valószínűleg fennáll.

Szerencsejáték szervezésének, azaz tettesi magatartásnak minősül a játék lebonyolításának kialakítása, a weboldal fenntartása, üzemeltetése, irányítása, a tétek kimunkálása, a tétek elfogadása, a nyeremények kifizetése. A szervezés akkor is megvalósul, ha a szervező részt vesz a játékban.

Illegális szervezésnek minősül az is, ha a személy legális szerencsejáték szervezésére jogosult, de jogosultságát túllépi. Közömbös, hogy végeredményben anyagi hasznot hozott-e a játék, vagy sem.

A szerver nyújtása bűnsegélynek minősül. Irreleváns, hogy ingyenes vagy visszterhes.

A pornográf, pedofil tartalmak közvetítése mint üzleti lehetőség

A számítógépes hálózatok szabadsága mellett a szabadosságuk, ezen belül a szexuális szabadosságuk is jellemző. A felhasználók anonimitásukban bízva (azt kihasználva) eltitkolt (szégyellt) vágyaikat élik ki.

A pedofilok és homoszexuálisok zárkózott emberek, akik a vágyaikkal általában nem léphetnek a nyilvánosság elé, így bűnös tevékenységüket titokban űzik. Az internet elterjedésével olyan kapcsolattartási lehetőséget kaptak, amelynek előnyeit hamar felismerték, és fel is használják a vágyaik titkos kiélésére.[16]

16 Peszleg Tibor: Internet és pedofília. Belügyi Szemle, 2004/11–12. http://www.remet.hu/cms/index.php?option=com_content&task=view&id=16&Itemid=4

A pornográf, ezen belül a pedofil tartalmak megosztása jellemzően négyféleképp történhet: e-mailben, chathálózatokon, weboldalakon vagy élő webkamerás közvetítéssel.

Erotikus, pornográf tartalmú képgalériák (akár híresség, akár kiskorúak képeiről van szó) díjfizetés ellenében tekinthetők meg. Néhány kép elérhető ingyen, ám a többiért már fizetni kell. A webkamerán keresztül közvetített erotikus, sőt pornográf jelenetek elérése szintén díjköteles. Az ilyen tartalmak iránt érdeklődőket az a veszély is fenyegeti, hogy a bankkártyaadataik kiszolgáltatásával az elkövetők könnyedén hozzáférhetnek a bankszámlájukhoz.

Az anonim kommunikáció lehetőséget teremt prostituáltak közvetítésére, így még nagyobb anyagi haszonra lehet szert tenni. A szexturizmus könnyen és titokban megszervezhető, zökkenőmentes az érdeklődők toborzása. Ez is anyagi hasznot hoz, sőt a kliens is megzsarolható. A szervezett bűnözés e téren

– a pornográf, pedofil tartalmak pénzért való árusításával,
– a bankkártyák adatainak megismerése, majd
– a bankkártyák „megcsapolásával”,
– a klienseknek a szexkaland miatti megzsarolásával juthat anyagi előnyökhöz.

Napjainkban jellemzőnek tekinthetjük a perverziók felé fordulást. Erre jó lehetőséget kínálnak a számítógépes hálózatok, és erre a keresletre épít a szervezett bűnözés is. *„Az extrém tartalmakkal szembeni tolerancia arra ösztönzi a kínálati oldalt, hogy a valódi érdeklődőket egyre szélsőségesebb tartalmakkal szolgálja ki.”*[17]

A kiskorúak a leginkább veszélyeztetett sértetti kör, azon belül a gyermekek, de nemcsak a felhasznált személyek, hanem valamennyi kiskorú, sőt a közmorál is.[18]

Számtalan jó szándékú, világos tartalmú, elkötelezett nemzetközi dokumentum, büntetőjogi regula[19] született e tárgykörben, de reális a tendencia a gyermekpornográfia, pedofília dinamikus továbbterjedésére.[20] A szervezett bűnözés e területe is jövedelmező üzleti lehetőség.

A hazai szabályozás (Btk. 204. §) büntetni rendeli a kiskorúakról pornográf felvétel készítését, a forgalomba hozatalt, az azzal való kereskedést, a

17 Parti Katalin: Gyermekpornográfia az interneten. Bíbor Kiadó, Miskolc, 2009, 48. o.
18 Uo. 104. o.
19 A nemzetközi és a hazai büntetőjogi intézmények, regulák kiépülésének szép leírását olvashatjuk Parti Katalinnál. Uo. 112–139. o.
20 Barta Sándor: Gyermek sérelmére elkövetett internetes bűncselekmények. Belügyi Szemle, 2004/11–12., 117–118. o.

nyilvánosságra hozatalt, kínálást, átadást, hozzáférhetővé tételt, az ilyen felvételek megszerzését, tartását.

Kábítószer-kereskedelem és illegális forrásból származó gyógyszerek forgalmazása a számítógépes hálózatokon[21]

A számítógépes hálózatok szabadsága együtt jár némi szabadossággal is. Így a kábítószerekkel összefüggésben megszámlálhatatlan információ elérhető, sőt találunk kifejezetten kábítószerre szakosodott weboldalakat is.

A szervezett bűnözés a számítógépes hálózatokon is megtalálta a kábítószer-kereskedés lehetőségét.

Két fő értékesítési lehetőséget prognosztizálhatunk:

– közvetlenül a fogyasztónak értékesítés chatszolgáltatás útján; a chatszobák érdeklődés szerint szerveződnek, bővülnek. Így az értékesítők nyilván az illegális szerekről vitatkozók, az iránt érdeklődő chatelők között keresnek ügyfeleket;
– kábítószerrel kapcsolatos weboldalakon felkínálják a kábítószerhez jutás lehetőségét.[22]

Az ilyen oldalakon a kábítószer-használat történetéről, a kábítószerekkel kapcsolatos vitákról, a kábítószer-előállítás eszközeiről, fortélyairól, ötleteiről, a termesztésről vagy a házilagos előállításról olvashatunk. Találunk értékesítési lehetőséget, vagy csak cannabismagokat, vagy magát a drogot árusítják.

A kábítószer termesztése, előállítása „receptjének" megosztásának minősítése. A *visszaélés kábítószerrel* tényállás több pontjában szerepel az „termeszt, előállít" elkövetési magatartás.

A *termesztés,* mint a bűncselekmény egyik elkövetési magatartása, magában foglalja mindazokat a tevékenységeket, amelyek a kábítószer alapanyagául szolgáló növény ültetésétől a szaporításán át annak ápolásáig tartanak.

Ha a számítógépes hálózatokon a termesztéshez elengedhetetlenül *szükséges* információk, ismeretek olvashatók – például a vetőmagok beszerzéséről,

21 Nagy Zoltán: i. m. 212–221. o.

22 A kábítószerek népszerűsítéséről (például elektronikus hirdetőtáblákon, chatszobákban, fórumrovatokban vagy egyéb weboldalon: cannabis.net, 420group.com). A kábítószer előállításának technológiájáról, a hozzá szükséges eszközökről, azok beszerzéséről stb. például nepenthes.lycaeum.org/Drugs/THC/Smoke/dual.html. A kábítószer-kereskedelem, -rendelés: cannabisseeds.biz, worldwideseeds.com.

annak rendeléséről, az ültetés technológiájáról, a növény ápolásáról, az öntözés menetéről, idejéről, a nélkülözhetetlen napfény pótlásának módjáról, a melegházi hőmérsékletről (általában ezek együtt olvashatók) –, akkor a cselekmény a „kábítószer-termesztésre irányuló felhívás". A felhívás, mint előkészületi magatartás [Btk. 18.§ (1) bek.] nem más, mint eredménytelen felbujtás, azaz nem szükséges, hogy – adott esetben – a kábítószer termesztése elkezdődjön vagy megtörténjen.

Felhívás esetében nem kívánunk meg az elkövetők (tettesek, bűnrészesek) és a felhívást kibocsátó között konkrét (létező) kapcsolatot.

Az elkövető tisztában van azzal, hogy kábítószer alapanyagául szolgáló növény termesztésére vonatkozó információit meghatározatlan számú felhasználó olvashatja, és annak alapján a növény termesztésére sor is kerülhet. Fontos feltétel, hogy a termesztésre vonatkozó ismeretek, információk valódiak legyenek.

Ebben az esetben a kábítószer termesztésére felhívó személy a *Btk. 282. § (1) vagy (2) bekezdésébe ütköző és a 282. § (3) bekezdés a) pontja szerint minősülő és büntetendő visszaélés kábítószerrel bűncselekményének előkészületéért* felel.

Ha a számítógépes hálózaton közölt, bemutatott, ábrázolt információ *általános ismeret* nyújt a növényről és műveléséről – ami egyébként elérhető például az internet különböző weboldalain is –, akkor a kábítószer-termesztésre történő felhívás nem állapítható meg.

Az *előállítás* magában foglal minden olyan cselekményt, amelynek következtében jogszabályban meghatározott fogyasztásra alkalmas kábítószer jön létre, például a kábító hatású anyag kivonása a növényből szintetikus úton. Nem minősül előállításnak egy már létező kábítószerből egy másik kábítószerfajta készítése, továbbfeldolgozása (például ópium–morfin–heroin), tisztázása, finomítása, kis egységekbe kiszerelése. Közömbös, hogy az előállítás gyári méretű, gyári körülmények között zajlik, vagy házilagos.

Ha a tartalomközlés kábítószer előállításához szükséges technológiai folyamatot bemutat, ábrázol, a gyártáshoz szükséges technikai eszközökről, beszerzésükről, vegyi anyagokról, beszerzésükről, a technikai eszközök vagy vegyi anyagok kábítószer előállítására alkalmassá tételéről szóló információt oszt meg, akkor az „kábítószer előállítására felhívás". Azaz az elkövető a *Btk. 282. § (1) vagy (2) bekezdésébe ütköző és a 282. § (3) bekezdés a) pontja szerint minősülő és büntetendő visszaélés kábítószerrel bűncselekményének előkészületét* valósítja meg.

Kábítószer „rendelése" számítógépes hálózatokon keresztül, nem más, mint a *megszerzés* – Btk. 282. § (1) bekezdésében büntetni rendelt cselekmény – előkészülete.

Az elkövető a kábítószer tényleges birtokbavételére, illetve az azzal való rendelkezés lehetőségének megteremtésére törekedve *„a közös elkövetésben megállapodik"* az elkövetővel. A cselekmény büntetőjogi minősítése *a Btk. 282. § (1) vagy (2) bekezdésébe ütköző és a 282. § (3) bekezdés a) pontja szerint minősülő és büntetendő visszaélés kábítószerrel bűncselekmény előkészülete.*

A Btk. 282. § (1) vagy (2) bekezdésében büntetni rendelt bűncselekmény befejezettségéhez nem szükséges a kábítószer tényleges birtokbavétele. A befejezettség stádiumába jut a cselekmény azzal, ha az elkövető számára a kábítószerrel való rendelkezés lehetősége realitás (például kifizette a kábítószert, vagy mással megszereztette azt, de még nem vette át, illetve ha azt az elkövető „nevében" vagy által fizetve más veszi át, más őrzi meg, mással értékesítteti tovább).

A reális rendelkezési lehetőség hiányában *a Btk. 282. § (1) bekezdésébe ütköző és e szakasz szerint büntetendő visszaélés kábítószerrel bűncselekményének a Btk. 16. §-ában meghatározott kísérlete* valósul meg.

A kábítószer *kínálása* a Btk. 282/A § (1) bekezdésében büntetni rendelt. Ez a tevékenység akkor jöhet szóba, ha az elkövető a számítógépes hálózaton a birtokában, ennek hiányában a rendelkezése alatt (például másnál) lévő kábítószer átvételére hív fel egy konkrét személyt (például e-mail).

Ebben az esetben az elkövető a *Btk. 282/A § (1) bekezdésébe ütköző és e szakasz szerint minősülő és büntetendő cselekményért* felel.

A számítógépes hálózatokon – általában – nem egy konkrét személy számára kínálják fel a kábítószert, így a „kínálásra felhívás", azaz előkészület jöhet szóba.

Ez esetben a *Btk. 282/A § (1) bekezdésébe ütköző és e szakasz szerint büntetendő visszaélés kábítószerrel bűncselekményének a Btk. 18. §-ában meghatározott előkészülete* valósul meg.

Amennyiben a hálózaton a kábítószer forgalmazására, kereskedésére az elkövető „felajánlkozik", akkor a bűncselekmény *a Btk. 282/A § (1)vagy (2) bekezdésébe ütköző és a 282/A § (3) bekezdés a) pontjába ütköző és büntetendő visszaélés kábítószerrel bűncselekmény előkészülete.*

Hamis áruk, szolgáltatások forgalmazása számítógépes hálózatokon

Az elmúlt években az informatika és a gazdasági élet fejlődésének kölcsönhatásából új, az elektronikus kereskedelmi módszerek és azokat támogató alkalmazási rendszerek alakultak ki. Ezek mára nélkülözhetetlenné váltak a mindennapi gazdasági tevékenységben, a beszerzési és értékesítési folyamatokban éppúgy, mint a pénzügyi szektorban.

Az elektronikus kereskedelem *(e-commerce)* egyebek között a számítógépes hálózatok felhasználásával történő áruk, szolgáltatások értékesítését és az ezt kísérő pénzügyi műveletek interneten keresztül történő végzését jelenti. E kereskedelmi folyamat során a felhasználó online egy speciális szerverkapcsolat segítségével juttatja el a megrendelését a kereskedőhöz. A nagy földrajzi távolság vagy az időhiány nem akadálya az elektronikus kereskedelemnek. Ez rendkívül kényelmes és praktikus megoldás a vásárlónak, hiszen az otthonából rendelheti meg a számára szimpatikus termékeket vagy szolgáltatásokat.

A hamis árut gyártók és forgalmazók úgy dolgoznak és szervezik az értékesítést, mint egy nagyvállalat. Ők is az internetet használják a terjeszkedésükhöz és a marketinghez. Így tudják leggyorsabban eladni hamis termékeiket, vagy így találhatnak újabb értékesítőpartnereket szerte a világon.

Az illegális kereskedők ugyanúgy adnak kedvezményeket, ajánlanak pontgyűjtéses akciókat termékeik, szolgáltatásaik megvásárlásához, mint más legális vállalkozás. Tehát ugyanúgy viselkednek az elektronikus kereskedelem piacán, mint más legális, hivatalos kereskedők. Weboldalaik megtévesztően hasonlítanak a legális vállalkozások weboldalaihoz. A márkák megszólalásig azonosak külsejükben vagy elnevezésükben (Loreal kölni, Adidas, Nike, Gucci, Armani, Tokaji bor, Rubik-kocka[23]). Nem ritka, hogy a hamis termékek külsejükben, elnevezésükben hasonlítanak valamely márkára. Könnyen fellelhetők az interneten D & G (Dolce e Gabbana) helyett D & C (azaz az orosz Docha i Cabanov) farmerok, Lacoste helyett Lokasta kölnik, Nokia helyett Nokla mobiltelefonok, Adidas helyett Adios vagy Daiads vagy a négy csíkkal jelzett cipők, ruhák.[24]

23 Magyarországot jelentős presztízs- és anyagi veszteség érte a Rubik-kocka gyártása és értékesítése miatt. Mezei András: Magyar kocka, avagy még mindig ilyen gazdagok vagyunk? Magvető Kiadó, Budapest, 1984

24 Reflex – gazdasági magazin. 2007. december, 20–21. o.

Egyes források szerint az interneten kínált cikkek között a hamisítványok aránya jelenleg körülbelül 37 százalék, a parfümök magasan megelőzik a ruházati termékeket.[25] Ez a szám – bár a számbavétel körülményeit, kiterjedtségét, idejét nem ismerjük[26] – óriási. Bárhogy történt és bármit emeltek ki a kutatást végzők, a kapott eredmény világosan jelzi, hogy a hamis termékek forgalmazása jelentős gazdasági károkat okoz a termékek jogszerű előállítóinak és a hivatalos forgalmazóknak egyaránt.

Tipikus (sajnálatosan „természetes") jelenség, hogy az új termékek piacra kerülése után hamarosan megjelennek a hamis termékek is.

A hamis termékek iránt van kereslet. A megtévesztő márkák és az alacsony árak vonzzák a vásárlókat, ezzel téve népszerűvé az ilyen weboldalakat. Persze az alacsony árhoz alacsony minőség társul. Ezeket a weboldalakat a tájékozatlan felhasználókon kívül a hamis terméket tudatosan (szándékosan) keresők tartják életben.

A hamis termékek forgalmazásának körében is megjelenik a szervezettség és a munkamegosztás. Különösen azokban az esetekben, amikor is a weboldal a hamis termékek forgalmazására rendezkedett be, ideértve az árukínálat teljes vagy részleges hamis voltát. Ebben az esetben ugyanis a termékek előállítása, saját maguk által vagy másokkal való legyártatása, továbbítása, netán országhatáron való mozgatása, raktározása, a pénzügyi műveletek és a postázási, csomagküldési feladatok ellátása több ember munkamegosztáson alapuló együttműködését kívánja meg.

Sőt bizonyos aukciós, használt holmikat árusító oldalakon is elképzelhető a szervezett forgalmazás:

– ugyanazt a terméket, termékcsoportot többször és folyamatosan, vagy
– meghatározott időközönként, más-más felhasználónévvel, de ugyanaz az elkövetői kör értékesítheti a bűncselekményből származó vagy hamis termékeket;

25 A Chanel parfümök 38, a Dior parfümök 29, a Boss, Gucci stb. ruházati termékek 13 százalékát találták hamisnak a vizsgált időszakban vagy időpontban. Uo. 21. o.

26 Hiszen nem tudjuk, hogy az általam is észlelt több száz angol nyelvű kínai weboldalt figyelembe vették-e, vagy csak a legnépszerűbb európai és egyesült államokbeli aukciós, second hand és egyéb (C2C = consumer to consumer = fogyasztótól a fogyasztóhoz) oldalakat. Mit jelent a vizsgálatban, a márkás termék? Bizonyos kiemelt, jól bevezetett, több évtizedes, évszázados márkákra, vagy a frissen bevezetett, még nem vagy nem igazán ismert, de márkajelzéssel ellátott termékekre is kiterjedt-e a vizsgálat? Nem derült ki, hogy egy adott időintervallumban figyelték a hamis termékek forgalmát, vagy egy meghatározott időben, ami szintén differenciálódhat vásárlási, ajándékozási boom idején (karácsony, húsvét stb.), vagy azon kívül esőben.

– tehát az aukciós oldalak ideális terepe a bűncselekményből származó dolgok árusítására, azaz orgazdaság (Btk. 326. §) elkövetésére is.

A hamis terméket értékesítők szerverei lokalizálhatók. Ez nem jelent nehézséget.

A magyarországi és a magyar állampolgárok által külföldön való előállítás és forgalmazás büntetőjogi felelőssége aggálymentesen megállapítható a Btk. 296. §-ában szabályozott *áru hamis megjelölése* bűncselekményben. Akár a jellegzetes külsővel, megjelöléssel, elnevezéssel történő előállítás, akár az ilyen termékek forgalomba hozatala céljából történő megszerzése, tartása, vagy maga a forgalomba hozatala eseteiben a tényállás megvalósul.

Ha bizonyíthatóan bűncselekményből származó dolog értékesítése történik, akkor fő szabályként az orgazdaság (Btk. 326. §), esetleg más járulékos bűncselekmény, például pénzmosás (Btk. 303. §).

Az a nehézség, hogy a TCP/IP-címek hamisak, vagy olyan országban működnek, amelyek részesei a bűnügyi egyezményeknek, vagy azokban az országokban ez nem számít büntetendő cselekménynek (Kína, Vietnam, Törökország, Ukrajna stb.). Kettős kriminalizáció hiányában a bűnügyi jogsegély általában nem vehető igénybe.

A szervezett bűnözés sajátja és célja: a pénzmosás

A bűnelkövetések végső célja a megszerzett vagyoni előny érvényesítése, legális gazdaságba emelése. A pénzmosás nem kötődik kizárólag a szervezett bűnözéshez, de a szervezett bűnözés lételeme a pénzmosás, a szervezet működésének, gazdasági háttérének, illetve az elkövetők későbbi egzisztenciájának a megteremtése. *„Az illegálisan szerzett jövedelmek tisztára mosása napjainkban iparági méreteket öltött."*[27]

A pénzmosás globális jelenség, és az internet rendkívül sok lehetőséget kínál a bűncselekményből származó vagyoni előny legálissá tételében.[28]

A pénzmosás valós térben megvalósuló szakaszai tetten érhetők a virtuális térben is.

27 Bardócz Csaba: Pénzmosási technikák. Belügyi Szemle, 1997/3., 74. o.

28 A „tisztára mosott" pénz összegének becslésére többféle módszer is létezik. Kertész Imre: A bűn európai útjain. Belügyi Szemle, 1999/9., 58. o. Bármelyik számítási módszert fogadjuk el vagy mellőzzük, megállapítható, hogy a bűncselekményből származó pénzek felbecsülhetetlen hányadát igyekeznek a bűnelkövetők a legális gazdaságba visszaforgatni.

A szolgáltatások egy részében elegendő anonimitás, a hamis név, cím eltakarhatja a valódi felhasználót. Ráadásul a pénzügyi műveletek a világ bármely pontjáról, bármikor megvalósíthatók. A felhasználó lehetőségét a banki szféra érdeke is támogatja, egyfelől a bankok a pénzmozgásokat rugalmas szabályokkal, technikai háttérrel, ügyfélbarát módon segítik, másfelől a banki oldal az általa kért költségekben is érdekelt a pénzmozgásokban.[29]

A pénzmosás végrehajtásánál az elhelyezés fázisa dominál a számítógépes hálózatokon.

Lássuk a bűncselekményből származó pénzekkel történő fizetés, átutalás vagy vásárlás néhány lehetőségét!

Egyszeri vagy ismétlődő pénzátutalások más személynek, szervezetnek, alapítványnak. Az utalás jogcíme elvileg bármi lehet (karitatív, személyes, szimpátián alapuló), de ez közömbös is, hiszen ezek mind alibi indokok.

Akár legális, akár illegális szerencsejátékban a „bennfentes játékos" állandó vesztes, azaz gyakorlatilag befizet.

Ezekben az esetekben az elkövetők legálisan fizetnek (utalnak) pénzt, ám onnan a pénz a terrorcsoportokhoz (vagy más szervezett bűnözői csoporthoz) megy. A szakirodalom ezt az esetet „fordított pénzmosás"-nak nevezi.[30]

Csalárd aukciós tevékenység is alkalmas pénzmosásra. Csalárd az aukció

– ha bűncselekményből származó dolog értékesítésére kerül sor (orgazdaság), vagy
– a pénz átutalását nem követi áru mozgása vagy szolgáltatás teljesítése. Lehetőség van az aukció lerövidítésére, azonnali lezárására egy a licitre bocsátó által megállapított úgynevezett villámár elfogadásával. Ilyenkor a licitelő akármilyen magas árat is kifizet a felkínált termékért. A licitálás, majd a pénzátutalás megtörtént, ám ezt árumozgás nem követte, amit a licitáló nem ró fel, ez volt a szándéka, azaz a pénz kifizetése;
– kétes követelés elismerése és teljesítése pénzátutalással;
– Consumer to consumer e-business: műtárgyak, ékszerek, luxustermékek felárral történő vásárlása.

29 Például az átutalás díja, az átvezetés díja, a külföldre utalás több ezer forintos díja, a valuta átváltásának díja, a bankkártyák éves díja, a bankkártyával fizetés díja, amely a vállalkozást terheli, a bankszámlavezetés díja, a hitelkártya díja, a hitelkamatokban rejlő, a betéti kamatokhoz képest harmincötven százalékos kamatkülönbözet, a THM-ek díja stb. Láthatjuk, hogy miért nem kapjuk meg a jogszabályban, munkaszerződésben meghatározott és a jogszabályban előírt közterhekkel csökkentett teljes nettó bérünket.

30 Gál István László: A pénzmosás és a terrorizmus finanszírozása. In: Korinek László – Kőhalmi László – Herke Csongor (szerk.): Emlékkönyv Irk Albert egyetemi tanár születésének 120. évfordulójára. PTE ÁJK, Pécs, 2004, 39. o.

Vagy egyéb, e körön kívül eső termékek, vásárlása, szolgáltatások igénybevételének látszata. (A polgári jog szerint színlelt szerződés teljesítése pénzátutalással.) A pénz átutalását nem követte árumozgás vagy szolgáltatás, vagy nem olyan mértékben. Valószínűsíthető, hogy a bűncselekményből származó jövedelem átutalása történt a „pénzmosónak", aki majd legális bankszámlájára utalja tovább, ahonnan a pénz nagy része visszakerül az első befizetőhöz, vagy értékpapírt vásárol, vagy más legális vállalkozásba forgatja tovább.

Rétegzés (bújtatás) fázisa: a rétegzés során az illegális jövedelem elkülönül az eredeti forrásától. E fázis célja, hogy a bevételhez jutó és az illegális pénz között ne lehessen kapcsolatot találni. Azaz a pénz eredetét kell kideríthetetlenné tenni. A szervezett bűnözői körök többszörösen összetett fiktív tranzakciókat folytathatnak, amíg a bűncselekményből származó pénz legális vállalkozásokban, bank- vagy értékpapírszámlákon landol.

A számítógépes hálózatokon végzett banki műveletek rövid időn belül sok országon áthaladva megkerülhetik a Földet. Vagy olyan ország a cél, ahol a pénzmosás üldözése hagy némi kívánnivalót maga után, vagy a többszörös tranzakcióval, ide-oda utalással, számlákon kisebb címletekben való elhelyezéssel, majd ezek összevonásával, valutaműveletekkel, értékpapír-vásárlásokkal, majd azok eladásával követhetetlenné válik a pénz forrása. Mindez akár bel-, akár külföldi bankok szolgáltatásainak igénybevételével nem ütközik nehézségbe.

A pénzmosás harmadik fázisában a rétegzés során megbúvó pénzek a legális gazdaságban is megjelennek (például a bűncselekményből származó pénz immár legálisan megjelenik az elkövetők bankszámláján).

Zárszó…

…helyett megállapíthatjuk, hogy a számítógépes hálózatok elterjedésével, a felhasználók számának megnövekedésével a szervezett bűnözés is jelen van a hálózatokon. A külön-külön működő bűnözők egymásra találhatnak, a felhasználók számának növekedésével a kevesebb ismerettel felvértezett felhasználók megtéveszthetők, átverhetők, számítógépeik – tudtuk és akaratuk nélkül – feltörhetők, összeköthetők (botnet), majd fel- és kihasználhatók tisztességtelen célokra [például D(D)os-támadások végrehajtására].

Egy pesszimista megállapítás szerint az Egyesült Államok már vesztésre áll a kiberbűnözőkkel szemben.[31]

31 http://tech.cert-hungary.hu/tech-blog/120329/amerika-vesztesre-all-a-kiberbunozok-elleni-harcban

Magyarországon a biztonsági szakemberek és a jogalkalmazók egy szűkebb része már ismeri a jelenséget, veszélyüket, az ellenük való védekezés fontosságát. A jogalkotót, a jogalkalmazók nagyobb részét, az egyéni felhasználók döntő részét pedig fel kell készíteni – mihamarabb.