

A VIRTUÁLIS VILÁGBÓL A VALÓSÁGBA

Az Internet (Internetworking System) nyújtotta lehetőségeket a bűnözők, bűnözői csoportok is fel- és kihasználják. Kérdés az, hogy fellelhetők-e hasonlóságok, illetve különbségek a terrrorszervezet vagy tagjaik és a magányos terroristák Internet használata között? Hasonlóságok mutatkoznak a két elkövetői kör cselekménye között:

- Célok, motivációk tekintetében. Idetartozhat a nemzeti, etnikai, szeparatista törekvések, a neo-náci, a fehérek felsőbbrendűségét hirdető rasszista vagy más szélsőséges politikai, politikai gyökerű ideológia is.
- A célok, motívumok össze is fonódhatnak (neo-náci ideológia nevében alkalmazott erőszak egyaránt lehet politikailag motivált és irányulhat a zsidóság ellen. A muszlim szélsőségesek cselekményei is irányulhatnak a keresztény vallás egyben a nyugati világ (politikai berendezkedésének, életmódjának, értékrendszerének) tagadása ellen.
- Mindkét elkövetői kör potenciális támadásainak helyszíne lehet a valóságos téren kívül, akár on-line vagy off-line hálózatok.

A valós térben végrehajtott támadások esetében az Internet figyelés fontosságának indoka a célpont, a támadás módszere, az elkövetés előtti illetőleg utáni közlések, más azonos célpont ellen, azonos módszerrel elkövetett terrortámadások időbeliségének tisztázása, amelyek más bizonyítékokkal a valós térbeli nyomozást segíthetik. Az on-line vagy off-line térben alkalmazott támadás során a terrrorszervezet és a magányos terrorista is rejtve maradhat. Ténykedésükről a használt azonosítókról (álnév, monogram, trükkök, TC/IP-szám stb.), a hálózati támadás módja, célja utólagos értékelésével tudomást szerezhethetünk, bár beazonosításához e körben is más eszközökre is szükség van. Tipikus hálózati támadások a malware-k alkalmazása, bot-net támadások stb. Felfedezhetők különbségek is.

- A fentebb említett célok és motívumok esetében a politikai és vallási indíttatás mellett, mint hasonló okok és célok mellett, az egyéni céllal, önmagukért végrehajtott támadások, pl. haszonszerzési céllal, emberrablás, egyéni követelés érvényesítése, továbbá a motívum nélküli vagy irracionális támadások a magányos elkövetőkre jellemző. Különösen a pszichopaták veszélyesek.³⁰⁵ Ugyanakkor terrrorszervezetek céljaként jellemezhető a társadalmi – gazdasági – politikai rend megzavarására vagy túszok kicserélésére irányuló akciók.
- A postai küldeményekkel végrehajtott támadások a magányos terroristára jellemző.³⁰⁶

³⁰⁵ Fanatikus pszichopaták nevükben rejtik a veszélyt, de ugyanígy az affektív pszichopaták, akiket az érzelmi hullámvész, a túlzott érzelmi reakció jellemző, hisztériás pszichopaták, akik sokszor rejtőzködnek a világ elől, de társadalmi kapcsolatokat sokszor nem képesek kialakítani stb.

³⁰⁶ Jeffrey Simon: Lone Wolf Terrorism: Understanding the Growing Threat, Prometheus Book, New York, 2013. 87-88. o.

A hálózatokon történő megjelenést tekintve a különbözőségek:

Az Internetes felületen való megjelenésben a nyugati világ által terroristának nyilvánított szervezetek nagyobb személyi és tárgyi potenciállal rendelkeznek:

- Saját szerverek, szerverparkok vagy raid-szerverek fenntartása.
- Hamis, ún. „utazó” TC/IP-számok használata a számítógépek, szerverek bemérése és azok megbénításának megakadályozása céljából.
- Saját web-oldal szerkesztése, karbantartása a gyors, többnyelvű, teljes körű multimédiás tájékoztatás nyújtása céljából. Tevékenységükről szóló propagandájuk sikereiket, felnagyítják, veszteségeiket elbagatellizálják (Ilyen site a csecsen kavkazcenter.com). Ne feledjük, hogy egy nagyon erős vahabbita közösség él a dél-szerbiai Szandzsák tartományban, akiknek törekvése vahabbita testvéreikkel együtt egy Koszovót, Szandzsákot és muszlim Boszniát magába foglaló iszlamista állam létrehozása. A csecsenek és az al-kaidások jó része a muszlim radikális irányzatához tartozó vahabbita.
- Oldalaik mélyen vallásos tartalmukkal, (tipikusan a dzsihadista site-ok ilyenek), a fiatalok irányába fájlcserelés lehetőségével tagtoborzásul is szolgálnak. Nem egy esetben a palesztin oldalakról hamarabb letölthető egy film, mielőtt azt Hollywoodban bemutatták volna.
- A web-oldalakon információk rejtettek el rejtjelezés nélkül (a szteganográfia – ismert, bevett megoldás), amelyek utasításokat, tájékoztatásokat tartalmazhatnak. A web-oldalokról letöltött képek pl. egészen mást tartalmazhatnak.³⁰⁷
- Más opciók is ismertek, például olyan zárt FTP-hálózat, amelyet jelszó vagy más azonosító véd, és ezen a rejtett hálózaton keresztül történik a kommunikáció, vagy olyan e-mail fiók nyitása, amely nem forgalmaz, de a belépők a megírt üzeneteikkel a „piszkozatban” (draft) hagyással kommunikálnak. Érdeemes figyelni azokra a létező e-mail fiókokra, amelyekből nincs adatforgalom kifelé.
- A terrorszervezetekről, létükről, céljairól, tagságáról és más hírek, információk megjelenhetnek legális híroldalokon, tartalomszolgáltatóknál, a baszk és észak-ír oldalak szimpátiája az ETA és az IRA iránt észrevehető.³⁰⁸ Gyakorta nem terrorszervezet neve alatt, de lényegében azok propagandáját hirdető („fedő”) website-ok is feltűnnek.

A magányos terroristák közlési felületei az Interneten lehetnek saját web-oldalak is, ám – ennek viszonylagos bonyolultsága (készítése, üzemben tartása, díjfizetés a szolgáltató irányába és további okok miatt) vélelmezhetően – inkább az egyéb közlésre teret nyújtó opciók használata életszerű. A magányos elkövetőt gyakorta jellemzi a közlékenység, nézeteiket, véleményüket, jövőbeni cselekedeteiket nem képesek magukba tartani, ahhoz másoktól megerősítést várnak vagy kényszert éreznek annak megosztásával, dicsekedni vágnak ötletükkel.³⁰⁹

³⁰⁷ Próbálják ki a Jpg+FileBinder programot. Egy tömörített fájl elrejthető egy képben.

³⁰⁸ Nagy Zoltán András: Bűncselekmények számítógépes környezetben. Budapest, Ad-Librum, 2009. 224-226.o.

³⁰⁹ A most következő eseteken kívül példa az ex-jugoszláv származású Muharem Kurbegovic bűncselekménye, aki a los angelesi repülőtéren az első robbantásos merényletet hajtotta vére (innen a neve: Alphabet Bomber). 1974 augusztusában gyűlékony anyagokat tartalmazó robbanószerkezetet hozott működésbe, amely három ember halálát okozta. A támadásban 36-an sebesültek meg. Kurbegovic magnószalagokra mondta el terveit és megosztotta

Az anonimitás „tálcán kínálja” a személyiség megváltozását. A felhasználók sokszor jelentéktelenségüket, szürkességüket levetve, onnan kitörve új személyiségbe bújnak, és radikális nézeteket hirdethetnek, „rendteremtést”, a társadalom problémáinak megoldásáról írnak, amelyet ő maga fog megoldani vagy a megoldáshoz hozzájárulni. Aztán ez az általa alkotott „magasztos küldetés” fixa ideává válhat, rögzül pszichéjében, amely másoktól is megerősítést nyerhet. Végül jellemzően ez a rögeszme torkollik a való világban elkövetett cselekményben, így a képzetében rögzült ellenséggel leszámoló fegyveres támadásban.³¹⁰ A web-oldalon kívül potenciálisan sok felhasználóhoz juthatnak el a blogok írásai, a blog bejegyzésekhez való hozzászólás, a videómegosztó portálokra való közlés, az azonos tematika köré szervezett „fórum-rovatokban” és az azonos érdeklődés alapján kialakított chat – szobákban kisebb, bár „vájtfülű” (vele vagy cselekedetével rokonszenvező) közönséghez jut el közlése. Az e-mailben pedig kettő vagy néhány személy érheti el a magányos terrorista mondandóját. Nézzünk közelmúltban megtörtént eseteket:

Saját web-oldalon: Az egyesült államokbeli Joseph Stack szoftverfejlesztő mérnök saját honlapján, az *embeddedArt.com*-on 2010. február 18-án egy 6 oldalnyi búcsúüzenet-félén tudatta a világgal, hogy az adózási feltételek változására, mint okra „*az erőszak nemcsak válasz, ez az egyetlen válasz*”. Levelét, mint egy halálának előre kijelölt időpontjával zárta, Joseph Stack (1956-2010). Majd másnap a texasi Austinban, az adóhatóság épületébe vezette kispéját.³¹¹ Az ő öngyilkos egyéni akciója volt az Egyesült Államok több városát érintő 2011. szeptember 11-i összehangolt a-kaidás terrortámadások ötletadója? Az Al-Kaida tanult az esetből, a CIA nem?

A különböző közösségi és videómegosztó portálok alkalmasak a felhasználók – sokszor a szó szoros értelmében vett – kitarukozásának. Colleen LaRose (későbbi nevén Jihad Jane) *myspace.com* profilján jelentek meg először a „Palesztina veled vagyunk”, és „Szimpátia Gázával” közlések, majd egy másik közösségi oldalon a *Dailymotion.com*-on, illetve a *Youtube.com* videómegosztó portálon adott hírt magáról. Ezekben elítélte az arab területek izraeli megszállását, Izrael állam arabokkal szemben tanúsított politikáját, annak eszköztárát, mind e közben utalt Lars Vilks svéd grafikus megölésére, akit ironikus rajzokat készített a mohamedán vallás meghatározó alakjairól.

A blogokban (web-logokban „a háló naplóiban”): a közlések tipikusan tematikusak. Ezért az azonos érdeklődésűek között közösség kialakítására is alkalmasak. Bármilyen fájlformátumban történhet a közlés feltöltése (vannak videó-, zenei-, képblogok). A blogok összehozhatják az azonos gondolkodású felhasználókat. Somogyi Ábel ellen még folyik a büntetőeljárás, bizonyíthatóan több hallgatóságával próbált végezni, majd egy budapesti gyorséteremben lőtt is. Viszont tény az, hogy a *blog.hu*-n „Arszák” álnéven írt gyűlöletkeltő, eszement bejegyzéseket. Most is olvasható irományai gyűlöletről tanúskodnak a blogon meg az *iwiw-en*: „*Határtalan gyűlölet van Bennem minden rohadék iránt, aki előttem áll a sorban.*”³¹²

A fórum-rovatokban is megnyilvánult Breivik, a *Document.no*-n 75 alkalommal adott hangot szélsőségesnek minősíthető véleményét. James von Brunn több ízben több

telefonon egyik közeli ismerősével. Vö: Horváth Attila: A repülőterek és a légiirányítás mint kritikus infrastruktúrák. *Hadmérnök* 2009/4. sz. 90-99. o.

³¹⁰A pszichológiának érdemes volna erre területre is beható vizsgálatokat végezni.

³¹¹http://kitekinto.hu/amerika/2010/02/20/kamikaze-tamadas_erte_az_amerikai_adohivatal/#.UkCgAtIvnSs (Letöltés ideje: 2013.09.20.)

³¹²<http://blog.hu/user/114820/tab/activity>, és <http://iwiw.hu/pages/user/userdata.jsp?userID=9344869> (Letöltés ideje: 2013.09.20.)

fórumon nyíltan antiszemita véleményének adott hangot, zsidógyűlölő web-oldalt működtetett, majd ilyen hangvételű könyvet is írt. Bekerült az FBI látókörébe, de úgy ítélték meg, hogy közlései nem lépik túl a véleménynyilvánítás szabadságának határát. Zsidógyűlölete egy gyilkosságba torkollott, 2009. június 10-én a washingtoni Holocaust Memorial Múzeum egyik örét ölte meg.

Az egyik, szélsőséges ideológiának teret engedő chat-room, a mind mai napig működő Stormfront az, ahol Richard Poplawski is gyakran csevegett, csetelt. Antiszociális magatartására utalt a hadseregtől leszerelésekor kapott legrosszabb minősítés. Poplawski 2009. április 4-én három rendőrt lőtt le kettőt pedig megsebesített.

Az egyesült államokbeli Nidal Malik Hasan, a haditengerészet pszichiáterként dolgozott. Rokonsága a Palesztin Nemzeti Hatóság székhelyén a ciszjordániai Ramallahban él a mai napig. Az Egyesült Államokban abba a muszlim közösségbe járt, amelyiknek tagja volt a 9/11 terrortámadás két elkövetője, Hani Handzsar és Navaf al_Hazmi is. Utóbbi harcolt Boszniában is, az ottani vahabiták és a velük harcoló csecsen és más arab vahabita önkéntesek oldalán. Akkortájt a muszlim közösség vezetőjét Anwar Al-Awlakinak³¹³ hívták, aki 2004-ben elhagyta az USA-t és Jemenbe ment, ahol viszont bebörtönözték. Már a 2001-es terrortámadások idején radikalizálódott Awlaki felfogása, később ez még inkább kiteljesedett. 2008-tól Al-Awlaki és Hasan húsz e-mailt váltottak egymással (ennyit találtak a számítógépén), a mélyen vallásos tartalmú üzenetek hatására 2009. november 5-én a texasi az afganisztáni bevetésre felkészítő Fort Hoodban megölt tizenkettő katonát és egy polgári személyt, valamint megsebesített további tizenkilenc személyt.

Bruce Ivins az amerikai hadsereg fertőző betegségekkel foglalkozó kutatóintézetének orvosa 2001-ben egy e-mailben ajánlott anthraxot (lépfenét) kollégáinak. Abban az évben 5-en haltak az Egyesült Államokban postai levélben küldött anthrax portól. Ivins a vád alá helyezés idején öngyilkosságot követett el. Felvetik Ivins ártatlanságát, de a nyomozó hatóság meg van győződve a szociopátának minősített tudós bűnösségéről. Ivins 18 évig kutatta, tökéletesítette az anthraxot. Talán ki akarta próbálni valóságos közegben a gyilkos hatást? Más erre nem volt hajlandó, akkor ő megtette?

Talán figyelmet érdemel az a vélemény, amely szerint az Internetes kapcsolattartásban, eszmék terjesztésében, rábeszélésnek, meggyőzésnek legveszélyesebb terepe a chat-szoba.³¹⁴ Sajnos, az Internet nemcsak a fegyverek és bombák összeszereléséhez nyújt információt, ad tanácsot, hanem, ahol ez engedélyezett ott a fegyverek, lőszerkeszerezhetők rendelés útján. Ám nem minden terrorista jelenik meg az Internet valamilyen felületén. A magába forduló, introvertált elkövetőkre is találhatunk bőven példát.

Hogyan rejtőzködhettek el a felhasználók? A legkézenfekvőbb, hogy hamis e-mail címmel regisztrálnak, vagy ha olyan levelezőrendszert használnak, amely nem valamely távoli országban, távoli szigeten található, ahol nem fogják utolérni. Az anonimitás céljának megfelelően további lehetőségek is adóttak. A más által bekapcsolva hagyott vagy az azonosítóit megosztó valódi felhasználó számítógépéről, internet kávézókból avagy WiFi - kapcsolat útján. Ebben az esetben a hívott szerver csak a router TC/IP-számát naplózza, ám az, hogy a több felhasználó közül ki kapcsolódott a router jelére (ki van a router mögött),

³¹³ Anwar al-'Awlakī haláláig az egyik legveszélyesebb és leghatásosabb iszlámista hittérítő volt, neve az elkövetőkkel való kapcsolattartása miatt felmerült például a 2005-ös londoni, a 2006-os torontói, a 2007-es fort dixi, a 2010-es new yorki merénylet kísérleteknél és más esetekben.

³¹⁴ Mark Sagemon : Leaderless Jihad: Terror Networks in the Twenty-First Century, University of Pennsylvania Press, Philadelphia. 2008. 115-116. o.

azt már „nem tudhatja” a szerver. A routernek kellene naplóznia, ennek ma még technikai akadályai vannak. Ilyen alkalommal a felhasználók személye más módszerekkel deríthető ki pl. tanúvallomások (pl. helyiségekben, vonatokon, távolsági buszokon) vagy a helyiségek (iskolák, egyetemek, irodaépületek, vendéglátói helyek), közterületek kamerás felvételei. (Ha csak a felhasználók a közterületen meg nem bújnak a kamera holtterében.)³¹⁵ Anonim public proxy szerver igénybevételével is elrejtőzhetnek a felhasználók. E szerverek „mögé” – egyébként - rendkívül egyszerűen el lehet bújni. Az anonim public proxy-nál eggyel „fokkal” biztonságosabb az úgynevezett distorting proxy szerver. Ez a fajta proxy szándékosan hamis IP-t szolgáltat, azaz a proxy szerver helyét is elrejteti. A „legbiztonságosabb” mégis a high anonimity proxy. Ezek kifelé nem is proxynak mutatják magukat, úgy jelenik meg, mintha 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.

A nyomozás során viszont gyakori nehézség az, hogy bár az IP szám alapján az előfizető neve, lakcíme – pillanatok alatt – tisztázható, ám az még mindig kérdés, hogy ki is használta a számítógépet (és az Internetet) az inkriminált időpontban. Ennek kiderítésére a klasszikus kriminalisztikai módszerek, eszközök és fogások alkalmazandók. A TC/IP szám manipulálása (meghamisítása) már komolyabb felkészültséget igényel.

Mit tehetünk a virtuális térből fenyegetők ellen?

A terrorizmus ellen küzdelem, ahogy maga a jelenség is komplex jellegű, egyszerre kell „csatát vívni” a valóságos és a virtuális térben.

1. Elméleti ismeretek a számítástechnikai veszélyekről, visszaélésekről.³¹⁶
2. A védekezés, és a megelőzés részben nem különbözik az elektronikus adatfeldolgozó- és átviteli rendszerek egyébként szükséges fizikai védelmétől.
3. Az antiterrorista stratégia része a nemzeti adatbázisok egyesítése, az információk kölcsönös és gyors cseréje a hálózatokon megjelenő, és elérhető terrorista megnyilvánulásokról.³¹⁷
4. A hálózatok monitorozásnak ki kell(ene) terjednie a destruktív web-oldalakra (blogok, fórum-rovatok), a wap, és a chat-szobákra, különösen a szélsősége nézetekről eszmét cserélők csevegésére. A radikalizálódó felhasználókra figyelmet kellene fordítani, pl. az azonos vagy közel azonos álnevekre más-más fórumokon, blogokban, chat-szobákban. A közlések tartalma az azonos kifejezések, szófordulatok segíthetnek az elkövető profiljának azonosításában.
5. Az Internet megfigyelése, korlátozása demokratikus viszonyok között nem könnyű kérdés. Hans-Peter Friedrich német belügyminiszter a Breivik „ámokfutása” után úgy nyilatkozott, hogy ez merénylet nyilvánvalóvá tette, hogy meg kell szüntetni az internetes blogok, illetve a netes megszólalások általános névtelenségét, mivel az „ordas eszmék” terjesztését valamiképpen vissza kell fogni.³¹⁸

³¹⁵ De lege ferenda: Kívánatos volna az Internet Kávézókat is bekamerázni, amely az internetezők tevékenységét is rögzítené.

³¹⁶ Segítséget jelenthet Nagy Zoltán András: i.m.

³¹⁷ Korinek László: Az antiterrorista harc eszközei, különös tekintettel a büntetőjogra. In: Gál István László – Köhalmi László (szerk.): Emlékkönyv Losonczy István professzor halálának 25. évfordulójára. PTE ÁJK Pécs, 2005. 196. o.

³¹⁸ <http://www.spiegel.de/international/germany/german-interior-minister-german-identity-is-shaped-by-christianity-a-779032.html> (Letöltés ideje: 2013.09.20.)

6. A „jó hackerek” folyamatos képzése, létszámuk növelése a különböző szolgálatoknál, a honvédelemnél, a rendőrségen státuszba helyezéssel. (Kiemelt ösztöndíjak műszaki karokon tanulóknak, az informatikus szakos hallgatóknak.)
7. Pályázatok gyakoribb hirdetése (pl. harc a destruktív oldalak ellen, az Internetes közösség bevonása az ellenük folyó küzdelembe).
8. Nyilvánvaló, hogy a terrorizmus elleni harc a társadalom tagjai feletti fokozott ellenőrzés lehetőségével jár együtt.³¹⁹ Nem létezik a „mi lett volna” kérdés, így azt kérdezni, ha Breivik borzalmas merényletéről hamarabb tudomást lehetett volna szerezni, talán megakadályozható lett volna a tette? Viszont a jövőt illetően komoly, érvelő gondolkodásra van szükség a világhálón rejlő veszélyek (nézetek, káros tartalmak) és veszélyes emberek kiszűrését illetően, az ellenük való jogszabályi keretek megalkotására.
9. Be kell mutatni az Internet eme káros hatását is. Konkrét példákkal, esetekkel kell illusztrálni, miért is fontos az Internet szabadságának finomított szűkítése (blogok szerzőjének hitelt érdemlő, valós regisztrálása, attól még a felhasználó írhatna vagy feltölthetne adatállományokat álneven, fantomnéven). Párhuzamba lehetne állítani, más, bár korlátozó, de a biztonságunkat szolgáló intézkedésekkel pl. a repülőtéri csomagvizsgálattal. Ezek talán segíthetnének a kontroll elfogadásának szabályainak meghozását.

Érdekes kontraszt, amíg a társadalom egy része féltve őrzi, őrzné a személyiségi adatokat, intim szférájához tartozó információkat, addig másik része bőszen és bőven megosztja személyes adatait, horribile dictum – az aktuális tartózkodási helyeiket, segítve a bűnelkövetőket információszerzésben. A felelősségre nevelésre lenne szükség e területen is.

A terrorizmus napjaink realitása, a terroristák itt élnek, járnak - kelnek közöttünk. Csak aljas gondolatainkban, borzalmas pusztításra kész szándékukban különböznek tőlünk. A magányos elkövetők pszichés betegek, személyiségzavarral küszködők, szürke emberek, akik az Interneten találják meg a jelentéktelenségükből kitörni akaró, de gonosz énjüket. Ott kiabálják ki a világnak torz, eszement gondolataikat, ott találnak társakra, akik ugyanolyanok, mint ők vagy egymáshoz közel állnak, és akikkel együtt kiabálhat, ... hogy aztán menjen a végzet felé, gyilkolni magával rántani sokakat a halálba. Ahhoz, hogy a társadalom meg tudja védelmezni önmagát, a kiabálókat le kell leplezni, el kell szigetelni. Ne az árat sajnáljuk érte! Annál sokkal többet, embertársainkat veszthetjük el!

³¹⁹ Korinek László: i.m. 195. o.