Az internethasználat biztonságetikai kérdései – A virtuális lét rejtett veszélyforrásai

Szijártó Lívia[1]

Absztrakt:

Az internethasználat elterjedése azt eredményezte, hogy egyes tudományágak területén egyre több kutatás foglalkozik az internetes jellemzők vizsgálatával. A jelen tanulmány fő kérdése, hogy a webes kultúra sajátosságai mennyiben változtatják meg a kialakult társadalmi és biztonságpolitikai viszonyokat, az internet térnyerése milyen szinten jelent fenyegetést a mindennapi életre vonatkozóan. A szélsőséges csoportok internetes tevékenysége, a kiberbűnözés elterjedése mindenesetre újfajta védelmi megoldásokat igényel, melyhez kapcsolódóan a pszichológiai kutatások hasznos javaslatokkal szolgálhatnak. Az online tartalmak korszerű elemzése, és az így kinyert információk alapján végzett profilalkotó eljárások előnyei nyomon követhetők a nemzetközi felderítő, elhárító szervek munkájában.

Kulcsszavak: Internet, biztonság, kiberbűnözés, szélsőséges csoportok, pszichológiai módszerek,

Abstract:

The expansion of the Internet usage has led to an increasing research activity regarding the characteristics of the Internet in several disciplines. The purpose of this study is to determine the effect of the Internet culture on the already developed social and security policy relations and to analyze whether the virtual community is a serious thread in the everyday life. The online activities of extremist groups and cyber criminality requires new defensive tools, in connection with which the psychological research can provide valuable contribution. The modern analysis of the online contents and its investigation through profiling techniques are important methodologies, which are applied by the international intelligence and anti-terrorism sector in the world.

Keywords: Internet, security, cyber crime, extremist groups, psychological techniques

[1] *Nemzeti Közszolgálati Egyetem, harmadéves doktorandusz*

1. Bevezető

Napjainkban az internet széles körben elterjedt, így a mindennapi életünk szerves részévé vált. Az internet alapú hálózatok – különösen a közösségi oldalak – használata megváltoztatta a hagyományos kapcsolati, kulturális, szakmai és kommunikációs formákat. Egyes vélemények szerint a hétköznapi tevékenységek jellege nem, csak a felülete változott, míg mások nagyobb jelentőséget tulajdonítanak a virtuális lét kiteljesedésének.[2] A 21. században számos társadalomtudományi és infokommunikációs témájú tanulmány foglalkozott az internet elterjedésével járó szociális változásokkal, azok mindennapi életre gyakorolt hatásával. A jelen dolgozat egyik legfontosabb kérdése, hogy az internet mennyiben változtatta meg a fennálló társadalmi viszonyokat, és milyen hatással van a biztonságra nézve.

Az mindenesetre elmondható, hogy az internetforgalom nagy része a hagyományos gazdasági és társadalmi tevékenységek fenntartását szolgálja[3]. A banki műveletek, a kereskedelmi és oktatásbeli szolgáltatások, a kommunikációs csatornák és a közösségi oldalak nagyban megkönnyítik a mindennapi életünket. A webes közeg azonban nemcsak a hétköznapi életben fejti ki a hatását, hanem a biztonságpolitikai szektor területén is. A virtuális világ kiszélesedése miatt az ott folyó tartalmak és interakciók ellenőrzése nagy kihívást jelent, így a hagyományos tevékenységeket megkönnyítő szerepén túl, az internet komoly biztonsági kockázatokat is magában rejt. Kovács Zoltán 2013-as cikkében az internetes kommunikációt biztosító felhő alapú rendszerek (ld. Facebook, Twitter, Skype, Gmail, stb.) törvényes ellenőrzésével foglalkozik: a tanulmány szerzője szerint a felhasználók körében csökkent a hagyományos kommunikációs formák (pl. telefon) használatának igénye az elektronikus úton történő kommunikációval szemben, és erre a tendenciára a rendvédelmi és nemzetbiztonsági szolgálatoknak reflektálnia kell.[4]

Ropolyi szerint[5] *"az internet hasznos eszköz, és az általa kiváltott hatások a beépített társadalmi céloktól függenek",* azonban nem szabad figyelmen kívül

---

[2] *LEE S., KIM J. H., ROSEN D. (2009): A semantic network and categorical content analysis of Internet and online media research, The Open Communication Journal (2009), Vol. 3., 15-28. old.*
WALLACE P.: Az internet pszichológiája. Magyar fordítás: Krajcsi Attila, Osiris Kiadó, Budapest, 2002.

[3] *ROPOLYI L. (2006): Internethasználat és hálólét-konstrukció, Információs Társadalom, Évf. 6.,4. szám, 2006, 39-46. old.*

[4] *KOVÁCS Z. (2013): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I., Hadmérnök, VIII. évf., 3. szám (2013), 184-197. old.*

[5] *ROPOLYI, 2006., 40. old.*

hagyni, hogy ez a haszon destruktív célokra is felhasználható. A modern technikai eszközök használatával kiszélesedett a bűnözői lehetőségek köre, új illegális tevékenységi formák jelentek meg. A kiberbűnözés, a szélsőséges csoportok internetes tevékenysége új típusú kihívások elé állította a védelmi szektorban dolgozó szakembereket. Az ezekhez köthető rendvédelmi és nemzetbiztonsági feladatok közé tartozik az elektronikus kommunikáció figyelése, a lehetséges fenyegetések azonosítása, a terrorista propagandavideók felderítése és a hackertevékenység leleplezése is.

1.1. Az internet működése, használata

Napjainkban az internet egy szinte mindent és mindenkit összekötő rendszer, melyen a teljes emberi tudás és memória könnyen elérhetővé vált.[6] Előtérbe kerültek a multimédiás tartalmak – a hang, a mozgókép, a szöveg, a kép –, továbbá egyre jelentősebbé váltak az internetes interaktív elemek, melyek kétirányú kommunikációt is lehetővé tettek. Mára az internet látszólag egy teljesen nyitott és mindenki számára elérhető rendszerré vált, azonban egyes autokrata hatalmak komoly cenzúrát gyakorolnak felette. Az olyan diktatórikus államokban mint például Észak-Korea vagy Kína több közösségi oldal, internetes keresőfelület és fórum is elérhetetlen az átlagos felhasználó számára.[7] Az előbbi példa mutatja, hogy az említett országokban a virtuális tér meghatározó politikai eszköz, mivel az állam korlátozza az információk, a hatalommal nem összeegyeztethető vélemények, gondolatok elérésének lehetőségét. A demokratikus országok vezetői is használják az internetet politikai célokra, azonban alapvetően nem korlátozás céljából, hanem kampányok népszerűsítésére, véleményformálásra, manipulálásra és tájékoztatásra is.[8]

Az internet alkalmazási területei a szociális és gazdasági szférára is kiterjednek. A szabadidős tevékenység egy nagyobb hányada szintén itt történik: a közösségi oldalak használata, a különböző médiák szolgáltatásainak használata, a böngészés és hírportálok figyelése lassan felváltja a hagyományos eszközöket, továbbá internetes felületet használnak az iskolákban, a könyvtárakban, a pénzügyi cégeknél és a bankokban is.[9]

---

[6] *NÁMESZTOVSZKI ZS.: Az internet fogalma, kialakulása és fejlődési irányvonalai, Újvidéki Egyetem, Szabadka, 2010. Elérhető innen: http://blog.namesztovszkizsolt.com/wp-content/uploads/2009/10/AzInternetFogalmaKialakulasEsFejlodesiIranyvonalai.pdf*

[7] *Top 10 Internet-censored countries. USA Today. 2014. február 5. http://www. usatoday.com/story/news/world/2014/02/05/top-ten-internet-censors/5222385/*

[8] *BURJÁN A. (2010): Internetes politikai kampány, Médiakutató, 2010 ősz, elérhető innen: http://www.mediakutato.hu/cikk/2010_03_osz/08_internet_kampany*

[9] *NÁMESZTOVSZKI, 2010.*

Ropolyi szerint az internet összetett természetű, ezért többféle tulajdonságot és tevékenységformát foglal magában, melyek közül kiemelendők a(z):[10]

- számítógépek és hálóhelyek közötti mindenféle adminisztratív, banki, üzleti, kulturális vagy fogyasztási célú fájltranszferek
- elektronikus levelezés, egyéb postai és kommunikációs szolgáltatások
- önszerveződő csoportok fenntartása (hírcsoportok, fórumok, szerepjátékok, stb.)
- intézményi vagy személyes honlapok, naplók, műsorok szerkesztése, böngészés
- hálózatba kapcsolt számítógépek működésének összehangolása, megaszámítógépek létrehozása stb.

Összességében az internet az elmúlt évtizedek egyik legmeghatározóbb technikai újítása, olyan IP alapon kommunikálni képes eszközök (legjellemzőbb példa a számítógépek) rendszere, melyek egy hálózaton működnek és egymás között gyors információ- és adatcsere lebonyolítására képesek.[11] Azonban Ropolyi szerint ezen kívül az internet az interakciós szituációk egyik fontos szereplője, hiszen internethasználat révén egymástól távol élő személyek képesek hatékonyan kommunikálni. Ezeken túl a net sajátos közegként is értelmezhető, ahol az emberi tervek, célok és gondolatok formát ölthetnek, és ahol az adott személy új lehetőségekkel, értékekkel, tevékenységi formákkal találkozhat.[12]

A fentiekből következik, hogy az internet ma az emberi kommunikáció egyik legfontosabb közvetítő szereplője, így hatással van a társadalmi lét működésére. Az internet által kialakított virtuális tér befolyásolja a szociális és kulturális viszonyokat, és csökkenti a földrajzi távolságot az emberek között.

1.2. Az internet társadalmi szerepe

Az internet társadalomra gyakorolt hatása egyelőre vitatott kérdés, Válas Péter[13] megfogalmazásában például az internet önmagában nem több egy technikai eszköznél, melyet a felhasználók töltenek meg tartalommal. Ebből kiindulva talán a legfontosabb kérdés az, hogy az itt folytatott tevékenység milyen mértékben tükrözi, és milyen mértékben formálja a felhasználó személyiségét. Amennyiben az internet valóban csak technikai eszköz, elvileg nincs hatással a személyiségfejlődésre, de a valós életben gyakran lehet tapasztalni, hogy a fenti állítás

[10] *ROPOLYI, 2006. 41. old.*
[11] *ROPOLYI, 2006.*
[12] *ROPOLYI, 2006.*
[13] *Etika a világhálón. Írta: VÁLAS P., 2009. június 17., letölthető: http://www.ofi.hu/tudastar/internet-mediaetika/valas-peter-etika*

nem teljesen igaz.

A webes tartalmak vizsgálatában nem szabad figyelmen kívül hagyni az anonimitás kérdéskörét. Az internet világában mindenki maga konstruálja meg virtuális entitását, ami lehetőséget ad mind a hamis információk terjesztésére, mind a névtelenség megőrzésére. Wallace szerint a fenyegető üzenetek terjesztői gyakran őrzik meg anonimitásukat, és ilyen helyzetben az egyén hajlamosabb felrúgni a társadalmi konvenciókat, továbbá megfigyelhető, hogy a felhasználó agresszívebb és gátlástalanabb viselkedést mutat a számára névtelenséget – legalábbis reményei szerint – biztosító online térben, mint a valóságban.[14]

A fentiektől függetlenül azt gondolom, hogy alapvetően a mindennapi életben megjelenő együttélési normák határozzák meg az internetes működést is, azonban az elmúlt évtizedben már kialakultak olyan szabályok is, melyek csak a virtuális világban érvényesek. Válas[15] szerint a modern társadalmakat meghatározó jogrendszert valamilyen állami szereplő vagy szerv képviseli, így az egyén viselkedése, a szociális normák betartása kontroll alatt tartható. Ezzel szemben az internet egésze – funkciójából fakadóan - nem ellenőrizhető, a hálózat kiterjedtsége miatt a különböző tartalmak, kapcsolatok követése rendkívül nehézzé, adott esetben lehetetlenné vált. Ezáltal az interneten a normál állampolgárok kevésbé érzik ellenőrizhetőnek magukat, így a jogkövető magatartásuk is lazábbá válhat.

A sajátos virtuális társadalom létrejötte miatt egyedi szaknyelv van kialakulóban, mely reflektál a mindennapi és az internetes közösségek megváltozott szerepeire. A világhálón kialakult normák tekintetében két fontos fogalmat érdemes kiemelni:[16] a netizen az a felhasználó, aki a saját országának állampolgárságán túl az internetes közösség tagja is, a munkája, szociális kapcsolatai és szabadidős tevékenysége révén rendszeres időt tölt el az interneten. A netikett fogalom pedig a belső virtuális szabályrendszert jelöli, ez a szokásrendszer biztosítja az online térben lévők "együttélését". A netikett megsértése erkölcsileg elítélendő, emellett erőforrásban és anyagiakban keletkezett károkat is eredményezhet, de legtöbb esetben büntetőeljárást nem von maga után. Azonban fontos kiemelni, hogy a netikett nem általánosan elfogadott törvények gyűjteménye, hanem inkább erkölcsi szabályrendszer, melynek elutasítása vagy áthágása nem szankcionált.

2. Az internet, mint újtípusú biztonsági kockázat

Az online térre vonatkozó jogrendszer kidolgozása azért is nélkülözhetetlen, mivel a bűnüldözési tendenciák azt mutatják, hogy egyre nagyobb számban jelen-

[14] *WALLACE, 2002.*

[15] *VÁLAS, 2009.*

[16] *VÁLAS, 2009.*

nek meg illegális csoportok az interneten.[17] Az internet segítségével elkövetett bűncselekmények egyik részét képezik azok a tevékenységek, melyek kifejezetten az internetet, az információs rendszereket, az infokommunikációs eszközöket támadják, másik részét pedig a bűnözői csoportok internetes tevékenysége teszi ki.[18] A hackerek például az első típusba tartozó bűncselekményeket követnek el, mellyel céljuk, hogy az internet segítségével védett adatokat szerezzenek meg egyes számítógépekről. A hacktivisták politikai vagy ideológiai célból törnek fel internetes rendszereket, míg a számítógépes bűnözők általában rosszindulatú szoftverek segítségével pénzszerző akciókat hajtanak végre a kibertérben.[19]

Ezzel szemben a "klasszikus" bűnözői csoportok a már meglévő illegális tevékenységet terjesztik ki az internet világába. A pedofil-hálózatok, a terrorista szervezetek, a szervezett bűnözők alapvetően kapcsolatépítésre, pénzügyi tranzakciók végrehajtására, propagálásra, illegális tartalmak terjesztésére és anonimitásuk megőrzésére használják az internetet. Ezek a bűnözői típusok az internet megjelenése és széles körű elterjedése előtt is léteztek, azonban a technikai újítások segítségével soha nem látott méreteket öltenek napjainkban. A két típus között átfedés van, a terrorista csoportok például a kibertér elleni támadásokkal gyengítik az ellenségeiket a hagyományos merényletek mellett.[20] A Nemzeti Közszolgálati Egyetemen készült, 2012-es tanulmányban[21] leírtak szerint a 21. században a terrorszervezetek már hatékonyan használják ki a csúcstechnológia adta lehetőségeket, így a hagyományos terrorizmus és a kiberterrorizmus egymást kiegészítő akciói halmozott fenyegetést jelentenek.

Mint a fentiekből kiderül, az internet térnyerésével egyre nagyobb feladat hárul a védelmi szektorban dolgozó szakemberekre. A 21. századi informatikai és kommunikációs fejlődéssel párhuzamosan a bűnözők, terroristák lehetőségei kiszélesedtek[22], új típusú illegális tevékenységi formák jelentek meg, régiek alakultak át, amelyek napjainkban meghatározó biztonsági kockázatként jelentkeznek. A fentiekből következik, hogy az internetes rendszerek monitorozása minden ország számára nemzetbiztonsági és rendvédelmi kihívást jelent.[23]

---

[17] Risk of Cybercrime and Social Media. By ANJUM Z. I. Corporate Research and Investigations LLC (CRI Group).

[18] HAIG ZS., KOVÁCS L. (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Egyetemi tanulmány. Nemzeti Közszolgálati Egyetem, 2012.

[19] HAIG, KOVÁCS, 2012.

[20] HAIG, KOVÁCS, 2012.

[21] HAIG, KOVÁCS, 2012.

[22] ALFÖLDI Á. D. (2012): A profilalkotás tudományterületi elhelyezkedése és elméleti modelljei, Magyar Tudomány, 2012/8, 980-987.

[23] KOVÁCS, 2013.

2.1. Szélsőséges csoportok internetes tevékenysége

A jelenkorban a nemzetközi terrorizmus, a tömegpusztító fegyverek terjedése, a széteső államok és a regionális konfliktusok jelentik a legnagyobb biztonsági kockázatot.[24] A legújabb tendenciák szerint ezen kockázatok egy része, vagy azok bizonyos aspektusai már az online térben is megjelenik: a különböző terrorcsoportok egyre nagyobb számban használják az internetet tevékenységük bővítésére.[25] Weimann[26] szerint a 2001. szeptember 11-i terrortámadás után nagymértékben megnőtt a szélsőséges szervezetek webes tevékenysége. Ezek a közösségek az internetet politikai céljaik megvalósítására használják, kapcsolatot tartanak fent a szimpatizánsaikkal, fenyegető tartalmú üzeneteket tesznek közzé, toborzó tevékenységet végeznek, és támadják az ellenségüknek tartott hatalmak információtechnológiai struktúráit.[27] A holland kormány 2006-os jelentése szerint[28] a radikális üzenetek internetes terjesztésével lehetővé vált, hogy a dzsihád mozgalmak a nyugati világban is tért hódítsanak. Az elmúlt időszak alátámasztja a feltételezést, miszerint az Európában élő muszlim fiatalok között erőteljes radikalizáció mutatható ki. Az Iszlám Állam tudatosan használja a virtuális teret tanai terjesztésére, és számos bizonyíték van arra vonatkozóan, hogy második generációs, nyugaton élő arabok ezek hatására csatlakoztak a most zajló iraki és szíriai harcokhoz.[29]

Az Iszlám Állam (Islamic State – IS) térnyerése globális fenyegetést jelent, mivel a terrorszervezet nemcsak a közel-keleti térségben tevékenykedik, hanem az internet segítségével az egész világon képes befolyásra szert tenni. Az Iszlám Állam az internetes felületeket mind propaganda, mind kiképzési célokra, használja és az al-Kaidával és más iszlám csoportokkal ellentétben az IS nem rejtett internetes csatornákon jelenik meg, hanem olyan ismert közösségi oldalakon

---

[24] A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, Magyar Közlöny, 2012. évi 19. szám. 1378-1387. old. http://2010-2014.kormany.hu/download/f/49/70000/1035_2012_korm_hatarozat.pdf

[25] WEIMANN G. (2005): Virtual Terrorism: How modern terrorists use the internet. The Journal of International Security Affairs, Spring 2005, Nr. 8.

[26] WEIMANN, 2005.

[27] HAIG, KOVÁCS, 2012.

[28] Ministry of the Interior and Kingdom Relations. Violent Jihad in the Netherlands: Current Trends in the Islamist Terrorist Threat. General Intelligence and Security Service (AIVD), The Hague, Netherlands, 2006.
Letöltve innen (2013. október 15.): http://www.fas.org/irp/world/netherlands/violent.pdf

[29] Az Iszlám Állam internetes tevékenységéről ld.:
Fighting Islamic State in cyberspace. Daniel Cohen, Institute for National Security Studies, 2014. 09. 05. Social networks "in denial" on extremist use: GCHQ chief (Update). phys.org, 2014. 11. 04. http://phys.org/news/ 2014-11-social-networks-denial-extremist-gchq.html

hirdeti eszméit, mint a Twitter és a Facebook.[30] Ezeken a honlapokon a hívek rendszeresen közzéteszik a szervezet tetteit, az ideológiájukat, továbbá az Iszlám Állam az interneten keresztül befolyásolja azokat a potenciális híveket, akik saját hazájuktól elidegenedtek, közvetlen környezetükhöz instabil módon kötődnek, és ezért a terrorszervezet által ajánlott alternatív lét, a valahova tartozás és a büszke identitás ígérete vonzóvá vált a számukra. A sajtóban megjelent hírek szerint már több ezer nyugati országokból származó fiatal csatlakozott az Iszlám Állam harcához a Közel-Keleten, és ez nagyrészt az IS internetes tevékenységének köszönhető.[31]

Az FBI 2009-es tanulmánya[32] szerint a rendvédelemben kiemelt jelentőségűvé vált az internetes tartalmak, iszlám terrorista videófelvételek figyelése. Az IntelCenter nevű terrorizmussal foglalkozó magáncég 2005-ös gyűjteménye alapján a szélsőséges, dzsihadista videók több típusba sorolhatók: kiképző és instruáló felvételek, túszejtő akciókat tartalmazó vagy merényleteket bemutató tartalmak és a propaganda célokra készült videók. Az FBI az IntelCenter vizsgálati anyagát alapul véve megállapította, hogy az elmúlt évtizedben a dzsihád mozgalmak globálissá váltak, melyben nagy szerepe van az internet térnyerésének. A terrorista sejtek különböző internetes honlapokon, fájlmegosztó oldalakon, közösségi adatlapokon és fórumokon teszik közzé a felvételeket, mely mára ezen csoportok kommunikációjának szerves részévé váltak.

2.2. A kiberbűnözéssel járó biztonsági kockázat

Az internet térnyerése az előbbieken túl egy újfajta bűnözési forma kialakulásával is együtt járt:[33] a kiberbűnözés alapvetően az internet, a szoftverek és egyéb technológiai mechanizmusok illegális felhasználását jelenti. A fogalom alatt a különböző hackercsoportok tevékenységét, az adatlopást, az anyagi erőforrások jogtalan megszerzését, vagy ipari és hadi titkok leleplezését értjük, azonban ide tartozhatnak az interneten keresztül folytatott illegális kereskedelmi tevékenységek, pénzügyi csalások és lopások is.[34] Az internet és az ahhoz köthető alkalmazások még inkább felgyorsították a kiberbűnözés terjedését, mivel olyan pénzügyi tranzakciókra adnak lehetőségeket, melyek klasszikus banki háttér nél-

[30] *COHEN, 2014.*

[31] *COHEN, 2014. és phys.org, 2014.*

[32] *REID E. (2009): Analysis of Jihadi Extremist Groups'RVideos, Forensic Science Communications, 2009 július, Vol. 11., Nr. 3. Letöltve innen (2013. október 11.): http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2009/index.htm/research_tech/2009_07_research01.htm*

[33] *Risk of Cybercrime and Social Media. By ANJUM Z. I. Corporate Research and Investigations LLC (CRI Group).*

[34] *HAIG, KOVÁCS, 2012.*

kül zajlanak.[35] A különböző felhő alapú rendszerekben lehetőség van olyan pénzügyi tevékenység végzésére, mely kívül esik az állam ellenőrzésén, így egyrészről lehetőséget ad az adóhatóság elkerülésére, másrészről táptalajt biztosít a szervezett bűnözés és a terrorizmus finanszírozására.[36] Az online játékoldalak sajátos teret képeznek a z internet világában, hiszen a felhasználók gyakran ezeken a felületeken élik ki agresszív energiájukat, virtuális bűncselekmények, erőszak formájában, mely destruktív hatással lehet a valós cselekedetekre is.

Összességében elmondható, hogy az internet a fenti tevékenységek kapcsán mintegy megszüntette a hagyományos nemzeti határokat és geográfiai tényezőket, hiszen már sok esetben nem szükséges a fizikai jelenlét az illegális cselekedetek elkövetésekor. A kiberbűnözés és a kiberterrorizmus nemzetközi hatása miatt a probléma megoldására irányuló tevékenységek is már nemzetközi színen zajlanak.

3. Javaslatok az interneten megjelenő biztonsági kockázat kezelésére

A fentiekből kiderül, hogy a mindennapi életben egyre nagyobb szerepe van az online térnek, emellett megnőtt az internethez köthető illegális tevékenységek száma is, emiatt a rendvédelmi és elhárító szervek munkájában egyre hangsúlyosabb szerepet kap az internetről megszerzett nagy mennyiségű információ elemzése. A szélsőséges szervezetek és a kiberbűnözők virtuális működése új típusú kihívást jelent, melyek megoldásához a lélektani kutatások is hozzájárultak az utóbbi évtizedekben. A pszichológia bekapcsolódása a védelmi szektor munkájába nem új, azonban a korszerű technikai eljárások kidolgozása még viszonylag kiforratlan terület. A jelen tanulmány írója az internetes tartalmak pszichológiai szempontú elemzésével foglalkozik, és arra keresi a választ, hogy ez a módszer miként hasznosítható a felderítési munkában. A továbbiakban az eljárás rövid bemutatása és lehetséges használata következik:

A pszichológiai szempontú tartalomelemzés segítségével azonosítani lehet az internetes tartalmak mögöttes lélektani struktúráit, a felhasználó személyiségjellemzőit. A módszer a rendvédelemben többek között az alábbi területeken adhat hasznos információkat:[37]

- ismeretlen mintázatok feltárása az internetes csalók tevékenységében
- bűnözői csoportok közötti kapcsolatok feltárása az internetes kommunikációjuk alapján

---

[35] GAZDAG T., KOVÁCS Z. (2014): Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. Nemzetbiztonsági Szemle, II. évf., II. szám, 2014., 36-57. old.

[36] GAZDAG, KOVÁCS, 2014.

[37] Mastering new challenges in text analytics. Making unstructured data ready for predictive analytics. Elektronikus jegyzet. Letöltve innen (2014. április 10.): http://public.dhe.ibm.com/common/ssi/ecm/en/imw14301usen/IMW14301USEN.PDF

- lehetséges biztonsági fenyegetések vagy illegális tevékenységek leleplezése

A fenti területek vizsgálata során nagy mennyiségű adatforrás gyors feldolgozása szükséges, mely alapvetően számítógépes módszerekkel lehetséges. Az automatizált feladatmegoldás esetleges hibái miatt azonban érdemes manuális eszközöket is használni a felderítő munka során. Az emberi feldolgozás gyakran kiegészítője a számítógépes szoftvereknek, melynek célja, hogy a kutató a rendelkezésére álló emberi eszközökkel felmérje a vizsgálni kívánt szöveget, majd az elővizsgálat alapján olyan kategóriákat hozzon létre, melyeket be lehet vonni az elemzésbe. A számítógépes programok a pszichológiai dimenziókat és fogalmakat az előre betáplált adatok alapján értékelik, és ezután végeznek statisztikai számításokat, vázolnak fel kapcsolódási pontokat, összefüggéseket tárnak fel és tartalomszűrést is végrehajtanak.[38]

A tartalom- vagy szövegelemzés másik fontos feladata az anonim szövegek szerzőjének azonosítása.[39] Alapvetően manuális eszközökkel nehéz feladat, hiszen az előzetes jellemzők kiválasztása és detektálása nagyban meghatározza a kapott eredményt. Ma már az azonosításra szánt szövegek nagy hányada elektronikus formában jelenik meg, így a kézírás egyedi jellegzetességei sem állnak rendelkezésre. Azonban a gépelt szövegnek is vannak egyedi jellemzői, mint például a tematikus szavak megléte, az esetleges helyesírási hibák, a gyakran használt egyedi kifejezések, a témaválasztás, az írásjelek vagy különböző betűtípusok használata.[40] A korszerű számítógépes programoknak éppen az a legnagyobb előnye, hogy képesek azonosítani ezeket a sajátosságokat, mely nagyban megkönnyíti a felderítő munkát. Wittek tanulmánya[41] szerint a szövegelemzést alapvetően releváns információk kinyerésére, trendek és viszonyok felismerésére (személyek, helyek vagy akár szervezetek között), szövegek tartalmi osztályozására és szervezésére lehet használni.

A webes tartalomelemző módszerek segítségével mind az egyéni, mind a csoportos felhasználókról személyiségprofil készíthető, mely alapján nagy számban kiszűrhetővé váltak a destruktív internetes tartalmak. Lényegében a pszichológiai vizsgálatok arra szolgálnak, hogy a webes tevékenység alapján azonosítani lehessen a potenciális veszélyforrást jelentő csoportokat vagy személyeket. Az

---

[38] Részletesen, ld. EHMANN B., BALÁZS L. (2011): Nyelvtechnológia az űrpszichológiában: ICE-csoportok pszichodinamikájának távoli monitorozása narratív pszichológiai tartalomelemzéssel, Pszichológia, 2011, 31. évf., 1. szám, 63-79. old.

[39] WITTEK P. (2006): A szövegbányászat gyakorlata és nehézségei. IN: Információból üzleti érték – Az információbróker környezete és tevékenysége. Szerk: Mikulás Gábor, Budapest, Magyar Információbrókerek Egyesülete, 2006.

[40] WITTEK, 2006.

[41] WITTEK, 2006.

online térben működő csoportok sajátos pszichodinamikai tulajdonságokkal rendelkeznek, melynek vizsgálata nélkülözhetetlenné vált a felderítő munkában. Napjainkban több eljárás is elterjedt, melyek arra szolgálnak, hogy az internetes tartalmak alapján bejósolják a szélsőséges felhasználók, csoportok várható viselkedését. Ennek egyik példája a klaszterépítő megközelítés[42], mely a csoportprofilt a tagok szociális információira alapozza. Ez az eljárás az egyént és annak demográfiai jellemzőit vizsgálja, és ezekből következtet az adott közeg identitására. Tang és munkatársai szerint[43] a közösségi és webes kapcsolatok elemzése hozzásegít a szociális struktúrák jobb megértéséhez. Egy vizsgálni kívánt csoportról nemcsak a közösségi oldalakról lehet hasznos információt kiszűrni, hanem az internetes beszélgetések, blogok, státuszfrissítések vagy egyéb bejegyzések alapján is.

4. Összegzett következtetések

Az internet létrejötte nagy hatással van mind a hétköznapi, mind a szakmai életre. A pénzügyi folyamatok, a biztonságpolitikai együttműködések ma már nem csak országhatárokon belül, hanem széles nemzetközi palettán mozognak. Az átlagos felhasználó számára az internet egy jól használható technikai eszköz, mely megkönnyíti a mindennapi életet a munka, a szociális kapcsolatok vagy éppen az oktatás területén. Az internet elterjedése azonban újfajta biztonságetikai kérdéseket is felvet, hiszen jellegéből fakadóan alkalmas illegális tevékenységek terjesztésére, végrehajtására is. Az aktív szélsőséges csoportok, terrorista sejtek és kiberbűnözői szervezetek internetes tevékenységének és kommunikációjának felderítése nehéz feladat a szakemberek számára.

A 2000-es években a szélsőséges szervezetek egyre nagyobb területen használják a virtuális szférát. A fenyegető tevékenységek nagy száma, a kormányzati és kritikus infrastruktúrákat érintő hackertámadások elhárítása érdekében az arra illetékes szolgálatoknak szűrni és értékelni kell a keletkezett információt, mely elősegíti a hatékonyabb fellépést. Az interneten megjelenő biztonsági kockázatok új típusú felderítő és elhárító feladatokat hívtak életre, mint például a destruktív internetes tartalmak vizsgálata.

A védelmi szektorban megjelenő lélektani feladatok szükségessé teszik a velük kapcsolatos empirikus kutatások elvégzését is: az újfajta módszerek kidolgozása miként járulhat hozzá a felderítő munka sikeréhez. A szélsőséges felhasználók internetes tevékenységének vizsgálata, a tartalomelemző és profilalkotó

---

[42] CHRISTENSEN I., SCHIAFFINO S. (2014): A hybrid approach for group profiling in recommender systems. Journal of Universal Computer Science, Vol. 20., No. 4. (2014) 507-533.

[43] TANG L., WANG X., LIU H. (2010): Understanding emerging social structures - A group profiling approach, School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tech. Rep. TR-10-002

módszerek használata olyan prediktív szűrést tesznek lehetővé, melyek nagyban lecsökkentik a látókörbe került egyének körét, ezzel megkönnyíti a hivatásos szakemberek munkáját. Az adott vizsgálati forrásban rejlő egyéni sajátosságok - mint a helyesírási hibák, visszatérő motívumok, tematikus szavak, kifejezések - információt adnak mind az üzenet feladójáról, mind motivációjáról, mely alapján bejósolhatóvá válhat a jövőbeni viselkedése. A fent tárgyalt tartalomelemző és profilalkotó eljárások használata eredményesen vizsgálja a terroristák és hackerek által üzemeltetett weboldalakat, a használt kommunikációs stratégiákat és közösségi jellemzőket is.

Felhasznált irodalom

- ALFÖLDI Á. D. (2012): A profilalkotás tudományterületi elhelyezkedése és elméleti modelljei, Magyar Tudomány, 2012/8
- ANJUM Z. I.: Risk of Cybercrime and Social Media. Corporate Research and Investigations LLC (CRI Group). http://www.crigroup.com/wp-content/uploads/2014/01/risks-of-cybercrime-and-social-media-web-.pdf
- BURJÁN A. (2010): Internetes politikai kampány, Médiakutató, 2010 ősz, http://www.mediakutato.hu/cikk/2010_03_osz/08_internet_kampany
- CHRISTENSEN I., SCHIAFFINO S. (2014): A hybrid approach for group profiling in recommender systems. Journal of Universal Computer Science, Vol. 20., No. 4. (2014)
- EHMANN B., BALÁZS L. (2011): Nyelvtechnológia az űrpszichológiában: ICE-csoportok pszichodinamikájának távoli monitorozása narratív pszichológiai tartalomelemzéssel, Pszichológia, 2011, 31. évf., 1. szám
- Fighting Islamic State in cyberspace. Daniel Cohen, Institute for National Security Studies
- GAZDAG T., KOVÁCS Z. (2014): Felhő alapú új pénzügyi tranzakciós lehetőségek és azok veszélyei. Nemzetbiztonsági Szemle, II. évf., II. szám, 2014
- HAIG ZS., KOVÁCS L. (2012): Kritikus infrastruktúrák és kritikus információs infrastruktúrák. Egyetemi tanulmány. Nemzeti Közszolgálati Egyetem, 2012.
- KOVÁCS Z. (2013): Felhő alapú rendszerek törvényes ellenőrzési módszerei vizsgálata I., Hadmérnök, VIII. évf., 3. szám (2013)
- NÁMESZTOVSZKI ZS.: Az internet fogalma, kialakulása és fejlődési irányvonalai, Újvidéki Egyetem, Szabadka, 2010. Elérhető innen: http://blog.namesztovszkizsolt.com/wp-content/uploads/2009/10/AzInternetFogalmaKialakulasEsFejlodesiIranyvonalai.pdf

- REID E. (2009): Analysis of Jihadi Extremist Groups' Videos, Forensic Science Communications, 2009 július, Vol. 11., Nr. 3. http://www.fbi.gov/about-us/lab/forensic-science-communications/fsc/july2009/index.htm/research_tech/2009_07_research01.htm
- ROPOLYI L. (2006): Internethasználat és hálólét-konstrukció, Információs Társadalom, Évf. 6.,4. szám, 2006, 39-46. old.
- TANG L., WANG X., LIU H. (2010): Understanding emerging social structures - A group profiling approach, School of Computing, Informatics, and Decision Systems Engineering, Arizona State University, Tech. Rep. TR-10-002
- VÁLAS P:- Etika a világhálón. 2009. június 17., Letölthető innen: http://www.ofi.hu/tudastar/internet-mediaetika/valas-peter-etika
- WALLACE P.: Az internet pszichológiája. Magyar fordítás: Krajcsi Attila, Osiris Kiadó, Budapest, 2002.
- WEIMANN G. (2005): Virtual Terrorism: How modern terrorists use the internet. The Journal of International Security Affairs, Spring 2005, Nr. 8.
- WITTEK P. (2006): A szövegbányászat gyakorlata és nehézségei. IN: Információból üzleti érték – Az információbróker környezete és tevékenysége. Szerk: Mikulás Gábor, Budapest, Magyar Információbrókerek Egyesülete, 2006.
- Social networks "in denial" on extremist use: GCHQ chief (Update). phys.org, 2014. 11. 04. http://phys.org/news/ 2014-11-social-networks-denial-extremist-gchq.html
- Top 10 Internet-censored countries. USA Today. 2014. február 5. http://www.usatoday.com/story/news/world/2014/02/05/top-ten-internet-censors/5222385/
- A Kormány 1035/2012. (II. 21.) Korm. határozata Magyarország Nemzeti Biztonsági Stratégiájáról, Magyar Közlöny, 2012. évi 19. szám.
- Mastering new challenges in text analytics. Making unstructured data ready for predictive analytics. Elektronikus jegyzet. http://public.dhe.ibm.com/common/ssi/ecm/en/imw14301usen/IMW14301USEN.PDF
- Ministry of the Interior and Kingdom Relations. Violent Jihad in the Netherlands: Current Trends in the Islamist Terrorist Threat. General Intelligence and Security Service (AIVD), The Hague, Netherlands, 2006. http://www.fas.org/irp/world/netherlands/violent.pdf