Közösségi hálózatok hivatali használata

(Social Networks in Government Environment)

A tanulmány a KÖFOP-2.2.2-VEKOP-16-2016-00001

„KÖFOP keretében megvalósuló fejlesztések IT biztonságának növelése, ezáltal rendszerekkel összefüggő korrupciós lehetőségek és kockázatok csökkentése”

című projekt keretében készült.

Tartalom

Absztrakt

A közösségi oldalak napjaink megkerülhetetlen platformjaivá váltak. Használatuk nem korlátozódik csupán a szabadidő eltöltéséhez, az állami szféra különböző területein számos esetben nyújtanak olyan alkalmazási lehetőségeket, amelyek nagyban támogathatják az érintett szervezetek jogszabályban meghatározott tevékenységeik hatékonyabb ellátását. A használatuk azonban egyszerre jelent lehetőséget és kockázatot. Jelen tanulmány a közösségi média biztonságos használatával foglalkozik, kiemelten fókuszálva a közösségi oldalakból fakadó adat- és információbiztonsági kockázatra a hivatali használat tekintetében.

Kulcsszavak

közösségi média, adatvédelem, információbiztonsági tudatosság, kiberbiztonság

Abstract

Social networking sites have become the primary and unavoidable platforms, lately. Their usage is not limited to the spare time, as various fields of the public sector offer opportunities for organisations to utilise their public duties stipulated by law, in an efficient way. This usage can be an opportunity and risk or threat, as well, at once. This study delves into the secure usage of the social media, with a special focus on the data and information security risksk stemming from the social networks running in the government environment.

Keywords

social media, data protection, information security awarness, cybersecurity

1. Bevezetés

Az internet elterjedésével és az infokommunikációs technológiák (a továbbiakban: IKT) fejlődésével a közösségi média is életünk szerves részévé vált. Betört az otthonokba, munkahelyekre, iskolákba, de ugyanúgy a közösségi tevékenységek szereplőjévé vált, ahogy mondjuk utazás közben is egyre többen és egyre gyakrabban használnak valamilyen közösségi oldalt. Lehet szeretni vagy gyűlölni a közösségi oldalakat, olyan társadalmi és szociális változásokat eredményezett, amelyek megkerülhetetlenné tették, így nem vonhatjuk ki magunkat a hatása alól.[1]

A közösségi média használat napjainkra jelentősnek tekinthető. A közösségi média fogalmára tudományterületek függvényében különböző meghatározások születtek, azonban alapvetésként elfogadható az Andreas Kaplan és Michael Haenlein által alkotott definíció, amely szerint a közösségi média internetes alkalmazások olyan csoportja, amely a web 2.0 ideológiai és technológiai alapjaira épül, ami elősegíti, hogy kialakuljon és átalakuljon a felhasználó által létrehozott tartalom.[2] A definíció alapjául a felhasználó által előállított tartalom[3] szolgál, ami egyúttal paradigmaváltást is jelentett internetezési szokásainkban. A közösségi média megjelenése előtt az internetes tartalomszolgáltatást a szolgáltatók végezték, azonban a web 2.0 elterjedésével a tartalom-előállítás a felhasználók irányába tolódott el, míg a szolgáltatók csupán a keretet biztosítják. Ebből következik, hogy a tartalom az internetezők interakciójából jön létre, ami vagy teljesen új tartalom megalkotásából vagy a többi felhasználó által előállított tartalom módosításából, kiegészítéséből keletkezik. Ez egyben azt is jelenti, hogy a tartalom elvileg bármikor megváltozhat, akár az eredeti közléssel teljesen ellentétes tartalmat is magában foglalhat.

A felhasználói tartalomelőállítás azonban jelentősen kibővíti a közösségi média körét, hiszen számos okos mobil eszközre optimalizált alkalmazás is hasonló elven működik, ami a biztonsági kockázatok számának nagyfokú kibővülésével jár együtt.

Növeli a kockázatok számát a közösségi oldalak állandó innovációja is, amelynek oka vélhetően a gazdasági racionalizálás. A közösségi oldalak profitjának döntő részét a reklámbevételek jelentik, így a felhasználók bevonásáért, elköteleződésük növelése érdekében az egyes közösségi oldalak folyamatosan változtatják szolgáltatásaikat. Ez jelentheti az algoritmusuk változtatását, a versenytársak népszerű szolgáltatásainak adaptálását vagy azok felvásárlását és saját szolgáltatásba integrálását. Az a vállalat, amelyik nem képes megtartani a felhasználókat, eljelentéktelenedik, és nem csupán piacvezető szerepének elvesztését kockáztatja, hanem adott esetben a megszűnését is. Erre a magyar fejlesztésű IWIW kiváló példával szolgál.[4]

A közösségi oldalak csoportosítására különböző elméletek léteznek, amelyek a felhasználók, alkalmazástípusok függvényében kategorizálják az egyes oldalakat. Ngai és szerzőtársai például egy olyan konceptuális keretet ajánlanak elfogadásra, amely három egymásra épülő szintet feltételez.[5]

---

[1] Bányász Péter: *A közösségi média térnyerése a védelmi szférában.* PhD értekezés tervezet, Nemzeti Közszolgálati Egyetem, Budapest, 2018.

[2] Kaplan, Andreas – Haenlein, Michael: *Users of the world, unite! The challenges and opportunities of Social Media.* Business Horizons, 2010.

[3] Eredeti szóhasználat szerint User Generated Content, UGC

[4] Mint ismeretes, a 2002-ben létrehozott IWIW 2005 és 2010 között Magyarország legnépszerűbb weboldala volt. 2006-ban a Magyar Telekom Nyrt. tulajdonában álló Origo Média és Kommunikációs Szolgáltató Zrt. felvásárolta, de az új tulajdonos nem volt képes olyan mértékben integrálni az új szolgáltatásokat, mint az időközben egyre népszerűbb külföldi vetélytársak. Bár születtek kísérletek az elszivárgott felhasználók visszacsábítására, de ezeket vagy megkésve vezették be, vagy nem sikerült elfogadtatni a felhasználókkal. Az IWIW aktív felhasználóinak száma folyamatosan csökkent, mígnem az Origo 2014. május 15-én bejelentette, hogy június 30-ától megszünteti az oldalt.

[5] Ngai, E. W. T. – Moon, K. K. – Lam, S. S. – Chin, E. S. K. – Tao, S. S. C.: *Social media models, technologies, and applications.* Industrial Management & Data Systems, 115(5), (2015), 769–802. doi:10.1108/imds-03-2015-0075

Véleményük szerint modelljük adoptálása végül a közösségi médiával kapcsolatos kutatások inter- és multidiszciplináris feldolgozásához vezet.

Az első szint a közösségi médiával kapcsolatos elméleteket, modelleket jelöli. Ide sorolják a szerzők a:

- a magatartáselméleteket (például személyiségjegyek,[6] TAM[7] modell);
- a szociális tanuláselméleteket (például társadalmi tőke,[8] társadalmi identitás[9]);
- a tömegkommunikációs elméleteket (például paraszociális kapcsolatok,[10] használati-juttatási modell).[11]

A második szint a platformokat jelöli. Ide sorolják a szerzők:

- a tartalommegosztó oldalakat (például YouTube, Picasa);
- a közösségi könyvjelző oldalakat (például Pinterest);
- a blogokat, mikroblogokat (Blogger.com, Twitter);
- a virtuális/online közösségeket (például Lonely Planet, Yahoo Answer);
- a közösségi hálózatokat (például Facebook, LinkedIn);
- a virtuális világokat (például Second Life).

A harmadik szint pedig az egyes alkalmazási területeket fedi le, amelyek az előző szintek integrációjából valósulnak meg. Ilyen területek:

- a marketing;
- a tudásmegosztás;
- az ügyfélkapcsolat menedzsment;
- az együttműködésre vonatkozó tevékenységek;
- a szervezeti kommunikáció;
- az oktatás és képzés;
- és az egyebek.

---

[6] Az egyes személyiségjegyek kategóriákba történő sorolásának az oka, hogy ily módon különbséget tudjunk tenni az egyes individuumok között, megértve ezáltal a viselkedésük mögötti motivációt, illetve interperszonális interakcióikat. Bővebben lásd: Pléh Csaba et al.: *Pszichológiai lexikon.* Akadémiai Kiadó, Budapest, 2008. Személyiségtípusok, p. 276. p.

[7] A TAM modell (Technology Acceptance Model), vagyis a technológia elfogadás modellje szerint a felhasználó által érzékelt hasznosság, valamint a technológia könnyed használata határozza meg, hogy a felhasználó az adott technológiát milyen könnyen fogadja el. Az eredeti modell megalkotása Davis nevéhez fűződik, ezt azonban továbbfejlesztették. A TAM2 modell a hasznosság mértékét meghatározó tényezőket is figyelembe veszi, mint például imázs, szubjektív norma, az output minősége, az eredmény bizonyíthatósága és a munkarelevancia. Bővebben lásd: Davis, F.D.: *Perceived usefulness, perceived ease of use, and user acceptance of information technology.* MIS Quarterly, 13(3) (1989), pp. 319–339.; Venkatesh, V. – Davis, F.: *Theoritical extension of the technology acceptance model: four longitudinal field of studies.* Management Science, 46(2), (2000), pp. 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

[8] A társadalmi tőke fogalma a közgazdaságtanból ismert tőke fogalomból eredeztethető. A társadalmi tőke az interperszonális interakciókban megbúvó erőforrás, amely a kapcsolatok mennyiségének, minőségének, illetve azok struktúrájának függvénye. A társadalmi tőke elősegítheti az egyén boldogulását, illetve kollektív cselekvések hatására a társadalom prosperálását. Bővebben lásd: Bourdieu, Pierre: *Gazdasági tőke, kulturális tőke, társadalmi tőke.* In: Angelusz Róbert (szerk.): A társadalmi rétegződés komponense. Új Mandátum Könyvkiadó, Budapest, 1999, pp. 156–177.

[9] A társadalmi identitás az emberek azon motivációját írja le, amely szerint csoporttagságuk hatására pozitív önértékelésre tegyenek szert. Ez alapján a csoporthoz való tartozás más csoportokkal szembeni pozitívabb percepcióját jelenti. Bővebben lásd: Tajfel, Henry: *Social identity and intergroup behaviour.* Social Science Information, Vol. 13, No. 2, 1974, pp. 65–93.

[10] Munk Veronika megfogalmazása alapján paraszociális kapcsolatok alatt azokat a kapcsolatokat értjük, „*amelyekkel fenntarthatjuk magunkban a közösségiség látszatát, részt vállalhatunk a csoportban, közeliként élhetjük meg néhány ember életét, például a celebrityét. A valódi, közeli emberi kapcsolatainkat – jobb híján – paraszociális viszonyokra váltjuk fel*." Bővebben lásd: Munk Veronika: *Sztárság, elméletben.* Médiakutató, 2009 tavasz, http://www.mediakutato.hu/cikk/2009_01_tavasz/01_sztarsag_elmeletben

[11] Blumler, J. G. – Katz, E.: *The Uses of Mass Communications: Current Perspectives on Gratifications Research, Vol. 3.* Sage, Beverly Hills, CA., 1974.

Az elmúlt évek eseményei (gondoljunk csak például a 2016-os amerikai elnökválasztásra vagy a szintén a tárgyévben lezajlott brit népszavazásra az Európai Uniós tagságot illetően) világossá tették, hogy a közösségi média használat egyszerre lehet katonai, nemzetbiztonsági, politikai kérdés, és megkerülhetetlen a téma ilyen irányú vizsgálata.

A közösségi médiával kapcsolatos kutatások inter- és multidiszciplináris jellegűek, amelynek igazolására elég az okos mobil eszközökre optimalizált alkalmazások információgyűjtésben betöltött szerepére gondolni. E téma nem csupán az informatikatudományban fontos, például a szoftverfejlesztésben, de az orvostudományok esetében a függőségekkel kapcsolatban komoly kutatásokat végeznek. Ezeknek az eredménye pedig a katonai, nemzetbiztonsági kutatások tekintetében is fontossá válik, hiszen azok a felhasználók, akik nem engedhetik meg maguknak a nagyobb adatforgalmú mobilelőfizetést, azonban kialakult bennük a függőség a közösségi média és az okos mobil eszköz használattal kapcsolatban, nagyobb arányban fognak nem megbízható, nyilvános Wi-Fi hálózathoz csatlakozni, amivel adataik biztonságát kockáztatják.

2. A közösségi hálózatok biztonságos használata

2.1. A közösségi média használatának általános kockázatai

A kibertámadások száma a vonatkozó statisztikák alapján folyamatosan növekszik.[12] A közösségi média kockázatait első megközelítésben a kibertámadások motivációi oldaláról kell vizsgálnunk. A támadók motivációit illetően a szakirodalom négy kategóriát határoz meg a kiberfenyegetettségekkel kapcsolatban.[13] Ily módon különválasztjuk a kiberbűnözést, a hacktivizmust és kiberterrorizmust, a kiberkémkedést és a kiberhadviselést. A közösségi média mindegyik támadástípus esetén jelentősnek értékelhető, amely az egyes szervezetek esetében természetesen eltérő kockázattal bír. Fontos kiemelni azt is, hogy az egyes támadástípusok gyakran összefolynak, nehéz megállapítani vegytisztán, hogy melyik kategóriába sorolhatjuk. Állami szereplők gyakran alkalmaznak kiberbűnözőket bizonyos tevékenységek elvégzésére, de akár terroristák is vásárolhatnak a Darkneten[14] olyan kibertámadással kapcsolatos szolgáltatást, képességet, amivel egy komplexebb kibertámadást hajthatnak végre. Ahogy a 2016-os amerikai elnökválasztás is mutatta, nemzetbiztonsági szolgálatok hacktivistákat is felhasználhatnak műveleteik sikeres végzésére, akár közvetlenül, akár idegen zászló alatt.

2.1.1. Kiberterrorizmus és hacktivizmus

A kiberterrorizmus fogalmát először a ’80-as években használták,[15] de napjainkban sem találkozhatunk általánosan érvényes definícióval. Egy megfogalmazás szerint *„a kiberterrorizmus olyan bűncselekmény, amelyeket számítógépekkel és telekommunikációs eszközökkel úgy hajtanak végre, hogy azok rombolják és/vagy megzavarják a szolgáltatások működését, zavart és bizonytalanságot keltve ezzel a lakosságban. Ezen akciók célja a kormányzat vagy a lakosság erőszakos befolyásolása a szervezet egyéni politikai, társadalmi vagy ideológiai céljai érdekében.”*[16] Szerencsére elmondható, jelenleg nincsenek a terroristák olyan képességek birtokában, amelyek segítségével komplex kibertámadást lennének képesek elkövetni, csupán terroristák, akik használják a kiberteret. A kibertér és a terrorizmus összefonódását első alkalommal a 2016-os IOCTA jelentés nevesítette. A fogalom nem egyenlő a kiberterrorizmussal, ugyanis ez alatt azokat a tevékenységi köröket értjük, amelyek az internethasználatból fakadnak. A terroristák nemcsak információgyűjtésre használják az internetet, de propagandatevékenységre, kapcsolattartásra, támogatók szerzésére,[17] lélektani műveletek[18][19]

---

[12] Ezzel kapcsolatban a www.hackmageddon.com nevű oldal nyújt használható statisztikákat, amely havonta elemzi a bejelentett kibertámadásokat. Fontos azonban látni, hogy ez csupán a kibertámadások egy szeletét jelentik, hiszen gyakran az áldozatoknak nincs tudomásuk arról, hogy kibertámadás áldozatai (például az általuk használt informatikai eszköz egy botnet hálózat részeként mondjuk bitcoint bányászik, spamet küld vagy túlterheléses támadásban vesz részt), vagy a cégek, félve a felhasználói bizalom csökkenésétől, nem jelentik az őket ért kibertámadásokat.

[13] Krasznay Csaba: *A polgárok védelme egy kiberkonfliktusban.* Hadmérnök, VII/4. szám, 2012, pp. 142–151.

[14] Darknet alatt azoknak a Deep weben fellelhető oldalaknak az összességét értjük, ahol magas szintű titkosítás mellett illegális eszközöket, szolgálatásokat lehet vásárolni, legyen szó fegyverről, kábítószerkereskedelemről, bérgyilkosságról, szexuális szolgáltatásokról stb. A közösségi médiával való kapcsolatát a közösségi oldalakon kicsalt erotikus képek piacával nevesíthetjük, de vásárolhatunk álprofilokat, amelyeket például politikai döntéshozatal befolyásolására lehet használni, malware-eket, amelyeket a közösségi oldalakon alkalmazhatunk, de hozzájuthatunk olyan eszközökhöz is, amelyek segítségével feltörhetjük mások közösségi profiljait. Szintén nagy piaca van a kiszivárgott felhasználói adatbázisoknak.

[15] Luiijf, Eric: *Definitions of Cyber Terrorism.* In: Cyber Crime and Cyber Terrorism Investigator's Handbook, 2014, pp. 11–17.

[16] Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004.
http://www.fbi.gov/congress/congress04/lourdeau022404.htm (2018. 10. 20.)

[17] Ez lehetőséget biztosíthat akár a Darkneten képességek megvásárlására.

[18] *A Lélektani Műveletek (PSYOPS) elsődleges célja, hogy befolyásolja egy kiválasztott célcsoport viselkedését, magatartásformáit és véleményét az elöljáró által elfogadott PSYOPS célokkal összhangban, valamint hogy kiváltsa vagy megerősítse a célcsoport kívánt viselkedését az elöljáró távlati céljainak érdekében. Bővebben lásd:* Ált/57, Információs műveletek doktrína, MH DOFT kód: MD 3.10 (1), 2014. augusztus 5., pp. 1–15.

[19] A lélektani műveletek közösségi médiában történő alkalmazásához soroljuk az álhír-kampányokat, amit napjaink kiemelt kockázataként kell kezelni, különösen a mesterséges intelligencia fejlődésével.

végzésére is nagy hatékonysággal használják fel a közösségi oldalakat. Ezzel kapcsolatban az Iszlám Állam azonosítható paradigmaváltó szervezetként.

A hacktivizmus célja az információk nyilvánosságra hozatala, a széles közvélemény előtti megosztása, ugyanis a hacktivisták szerint az információhoz való szabad hozzáférés alapjogként értelmezhető. Ennek érdekében követik el támadásaikat, amelyek fő iránya az informatikai rendszerekbe történő behatolás információszerzés céljából. Napjainkban azonban paradigmaváltás figyelhető meg a hacktivisták esetében, ugyanis az unatkozó, amatőr fiatalok (lásd például Anonymous) mellett megjelentek a professzionális hackerek, jelentős politikai támogatással, gyakran katonai tevékenység kiegészítéseképpen. Erre kiváló példával szolgálnak az Iszlám Állam hacktivistái vagy a Szíriai Elektronikus Hadsereg harcosai.[20] A kiberhadviselés az államok közti konfliktusokban jelenik meg, amelynek során a konvencionális hadviselés támogatására (vagy akár kiváltására) az ellenfél információs rendszereinek működésképtelenné tételére törekszenek. A hacktivizmus és közösségi média kapcsolata szintén több szempontból azonosítható. Ahogy a fogalom meghatározásakor már fentebb említettük, a hacktivisták célja az információk nyilvánosságra hozatala. Véleményük szerint az információhoz való hozzáférés magasabb rendű jog, mint a nemzetbiztonsági érdek. Ily módon a social engineering támadás, hogy behatoljon védett rendszerekbe, esetükben is használható támadástípus.

2.1.2. Kiberbűnözés

A kiberbűnözés célja informatikai rendszerek felhasználásával az anyagi haszonszerzés, célpontjaik között az üzleti és politikai világ szereplői egyaránt megtalálhatóak.[21] A kiberbűnözés és közösségi média kapcsolatát az Europol által minden évben publikált Szervezett bűnözés internetes fenyegetettségét (Internet Organised Crime Threat Assessment, a továbbiakban: IOCTA) értékelő jelentése felhasználásával vizsgáltuk e tanulmány esetében. A 2017-es évre vonatkozó jelentés az előző évekhez képest új típusú kategorizálást alkalmaz az egyes támadástípusok esetében, azonban ez nem a támadások csökkenésével magyarázható, hanem a prioritások átrendezősédével. A 2016-os IOCTA jelentés 12 területet azonosított,[22] amelyből 10 esetében fedezhetünk fel kapcsolatot a közösségi médiával. A 2017-es jelentés[23] ezzel szemben négy prioritást határoz meg, amelyeket kulcsterületekre bont, illetve további határterületeket jelöl meg. A prioritások ez alapján:

- kibertérrel kapcsolatos bűnözés;
- gyermekek szexuális kizsákmányolása;
- fizetőeszközzel történő visszaélés;
- online bűnözői piacok.

Ezenfelül határterületként azonosítja a jelentés:

- a kibertér és terrorizmus összefonódását;

[20] Caldwell, Tracey: *Hacktivism goes hardcore*. Network Security, Volume 2015, Issue 5, May 2015, pp. 12–17. http://dx.doi.org/10.1016/S1353-4858(15)30039-8

[21] Moskowitz, Sanford L.: *The Global Cybercrime Industry*. In: Cybercrime and Business, Strategies for Global Corporate Security, 2017, pp. 3–22.

[22] Europol The Internet Organised Crime Threat Assesment 2016. Europol, Hága, 2017. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (2018. 10. 28.)

[23] Europol The Internet Organised Crime Threat Assesment 2017. Europol, Hága, 2018. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (2018. 10. 28.)

- a social engineeringet;[24]
- a szolgáltatásszerű bűnözést;
- a bűnözők pénzügyi tevékenységeit.

A malware-ek (malicious software – kártékony szoftver) a rosszindulatú programok gyűjtőneve, ide soroljuk többek között a számítógépes vírusokat, férgeket, reklámprogramokat, zsarolóvírusokat, kémprogramokat. Ahogy a felsorolásból látható, nem véletlen, hogy a kiberbűnözők előszeretettel használnak malware-eket, hiszen segítségükkel kritikus infrastruktúrákat, hálózatokat lehet támadni (például egy olyan vírus segítségével, amely botnethálózat részévé teszi a fertőzött informatikai eszközt, vagy ahogy a NotPetya zsarolóvírus esetében tapasztaltuk, elérhetetlenné tesz egy kritikus infrastruktúrát), illetve az adatlopásnak is fontos eszközei. A közösségi oldalakon gyakran találkozhatunk kártékony kódot tartalmazó alkalmazásokkal. Bár sokszor könnyen kiszűrhetők lennének, az alacsony biztonságtudatossággal bíró felhasználók rendszeresen áldozatokká válnak. A közösségi oldalakon ezek a kártékony kódok privát üzenetekben vagy megosztott tartalomként terjedhetnek, mindkét esetben az emberi kíváncsiságra, kapzsiságra alapoznak, olyan figyelemfelkeltő tartalmaz ígérve, amellyel ráveszik a felhasználót, hogy megnyissák a fertőzött weboldalt, alkalmazást.

A kritikus infrastruktúrák támadásában a közösségi médiának a malware-eken kívül az álhírek terjesztésében, illetve nyílt forrású információgyűjtésben lehet szerepe.[25][26]

Hogyan ismerhetjük fel a közösségi oldalakon terjedő malware-eket? Az azonosításuk bizonyos sémák mentén könnyen megvalósítható, azonban ezeket a jeleket gyakran nem veszik észre a laikusok. Ilyen jel lehet többek között, ha angol nyelven küld üzenetet az ismerősünk, aki egyébként nem beszél angolul, ahogy mi sem. A rövidített URL-el mindig gyanús kell hogy legyen, különösen olyan esetben, amikor a felhasználó, akitől kapjuk, vélhetően nem ismeri az URL rövidítésének eljárását. Gyakori továbbá, hogy valamilyen óriási akciót, híresség ekről szóló botrányt vagy rólunk szóló erotikus videót ígér a link. Ha pedig lekattintottuk, és valamilyen Facebook- vagy YouTube-hasonmás oldalra vagy ismeretlen videomegosztóra keveredtünk, ne kattintgassunk ott tovább, és semmilyen feltáruló adatmezőben, felugró ablakban ne adjunk meg adatokat. Célszerű olyan kiegészítőket telepíteni a böngészőnkbe, amelyek figyelmeztetnek a fertőzött oldalakra, s nem engedik megnyitni őket, hacsak mi jóvá nem hagyjuk (például NoScript Security, illetve a Web of Trust nevű kiegészítők). Emellett célszerű minden olyan alkalmazást mellőzni Facebookon, amelyek valamilyen „vicces” választ adnak, mennyire ismerjük az NDK autóit, hány évesnek nézünk ki stb.

A gyermekek szexuális kizsákmányolásával kapcsolatban négy kulcsterületet fogalmaz meg a jelentés. Az egyik legkomolyabb kockázatot a közösségi oldalak felhasználásával a gyermekek bizalmába történő férkőzést nevesíthetjük, amelynek során gyakran erotikus képeket csalnak ki álprofilok segítségével. Ennek egy komolyabb aspektusát jelenti a gyermekek szexuális abúzusa, ami például a korábban kicsalt erotikus képek felhasználásával valósulhat meg, zsarolást felhasználva. Azt sem szabad elfelejteni, hogy a gyermekek felhasználásával igyekezhetnek a támadók a célszemélytől információt kicsalni, és az ily módon kicsalt erotikus képet felhasználva zsarolják meg a célszemélyt, hogy hozzáférést biztosítson védett rendszerhez, vagy adjon át bizalmas információkat.

[24] A social engineering olyan támadásforma, amelynek során a támadó az emberi tényező kihasználható tulajdonságait használja fel, hogy ily módon férjen hozzá megtévesztéssel, zsarolással a védett információkhoz, rendszerekhez.

[25] Kovács László – Krasznay Csaba: *A digital Mohács: a cyber attack scenario against Hungary*. Nemzet és Biztonság: Biztonságpolitikai Szemle III:(Spec. Issue Winter), 2010, pp. 49–59.

[26] Kovács László – Krasznay Csaba: *Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint*. Nemzet és Biztonság, 2017/1., 2017, pp. 3–16.

2.1.3. Social engineering

Kevin D. Mitnick[27] megfogalmazásában: *„A social engineering a befolyásolás és rábeszélés eszközével megtéveszti az embereket, manipulálja vagy meggyőzi őket, hogy a social engineer tényleg az, akinek mondja magát. Ennek eredményeként a social engineer – technológia használatával vagy anélkül – képes az embereket információszerzés érdekében kihasználni.”*[28]

A social engineering támadásokat humán- és IT alapú támadások alapján szokás megkülönböztetni, annak függvényében, hogy használ-e valamilyen informatikai eszközt a támadás végrehajtása során. Az ilyen jellegű támadások sokszor akkor is hatékonyak lehetnek, ha a megtámadni kívánt rendszert magas fizikai és logikai védelemmel látták el,[29] ilyen esetben a szervezet leggyengébb „láncszemén”, egy nem kellően biztonságtudatos alkalmazotton keresztül kerülik meg a fizikai vagy logikai védelmet. A humán és IT alapú támadásoknak számos vállfaját különböztetjük meg. Humán alapú támadás lehet például az identitáslopás, a segítségkérés, IT alapú támadás lehet például adathalászat, keylogger vagy az alkalmazásengedélyekkel kapcsolatos támadások. Természetesen egy komplex támadás esetében a támadók a különböző technológiákat egymásra építve alkalmazzák. Egy social engineering támadás négy fázisból épül fel:

- információgyűjtés;
- a kapcsolat kiépítése;
- a kapcsolat kihasználása;
- a támadás végrehajtása.

Egy social engineering támadás esetében bárki lehet célpont, nem csupán az a személy, aki fontos adatokat kezel; minél kevésbé biztonságtudatos az alkalmazott, annál nagyobb eséllyel lehet a támadók célpontja. Egy social engineering támadás felépítése során rendkívül fontos a nyílt forrású információgyűjtés, amelynek a közösségi média az aranybányája.[30] *„Az OSINT a katonai felderítés és a hírszerzés rendszerén kívül létező, a publikum (tehát minden egyén) számára nyilvánosan, legális eszközökkel megszerezhető, vagy korlátozott körben terjesztett, de nem minősített adatok szakmai szempontok alapján történő felkutatását, gyűjtését, szelektálását, elemzését-értékelését és felhasználását jelenti*.”[31] Az egyének felderítése mellett az OSINT-nak a trendelemzésben is óriási szerepe van. A nagy közösségi oldalak közel 30 ezer szempont alapján gyűjtenek információt a felhasználókról, amit megfelelő értékelés-elemzés során nagy pontossággal lehet prognosztizálni jövőbeli viselkedéseiket.[32] A mesterséges intelligenciának e tekintetben egyre komolyabb szerepe van, hiszen ezt a fajta adatmennyiséget csakis algoritmusok segítségével lehet hatékonyan értékelni-

[27] Kevin Mitnick, egy legendás hacker sosem tartotta magát igazán kiemelkedő hackernek, elmondása szerint sikereit inkább social engineerként érte el. Letartóztatását követően szakított a rendszerekbe történő illegális behatolásokkal, biztonsági céget alapított, azóta etikus hackerként tevékenykedik.

[28] Mitnick, Kevin D.: *A legendás hacker – A megtévesztés művészete.* Perfact-Pro, Budapest, 2003, p.1.

[29] A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról értelmező rendelkezései alapján fizikai védelem: a fizikai térben megvalósuló fenyegetések elleni védelem, amelynek fontosabb részei a természeti csapás elleni védelem, a mechanikai védelem, az elektronikai jelzőrendszer, az élőerős védelem, a beléptető rendszer, a megfigyelő rendszer, a tápáramellátás, a sugárzott és vezetett zavarvédelem, klimatizálás és a tűzvédelem; logikai védelem: az elektronikus információs rendszerben információtechnológiai eszközökkel és eljárásokkal (programokkal, protokollokkal) kialakított védelem. Bővebben lásd: 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[30] Kenedli Tamás: *A nyílt forrású információszerzés.* In: A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest, 2014, pp. 169–178.

[31] Lévay Gábor: *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* Egyetemi jegyzet. ZMNE, Budapest, 2006, p. 6.

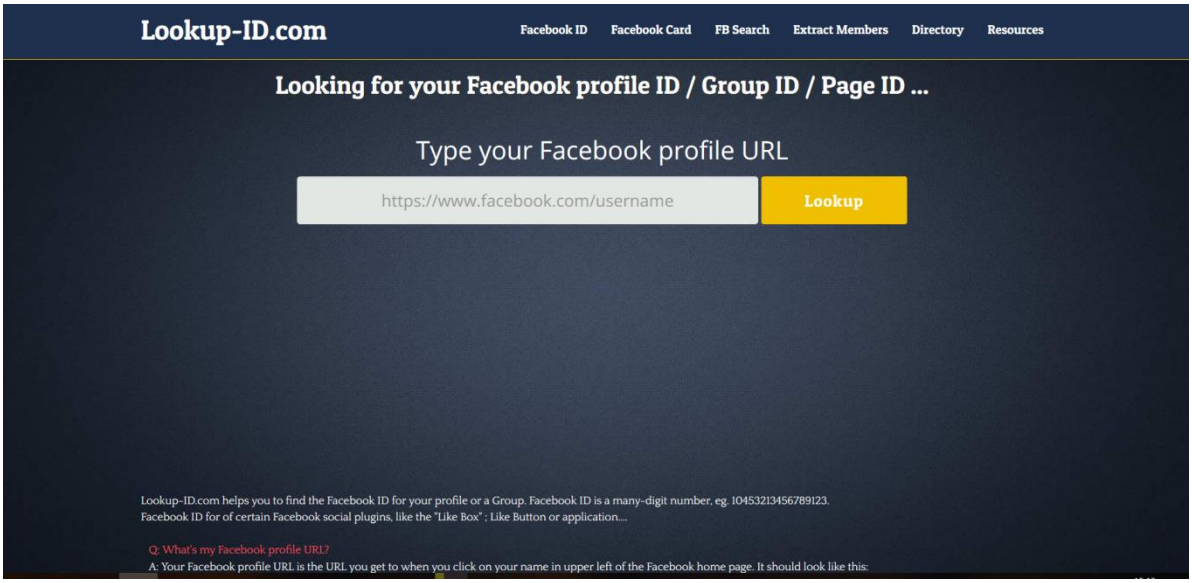
[32] Az értékelés-elemzés természetesen mesterséges intelligencia segítségével történik, amelyek esetében a gépi mélytanulás egyre nagyobb jelentőséget fog kapni, melyek hatására egyre pontosabb prognózisokat kaphatunk.

elemezni. Az egyének felderítésére nyílt forrásból számos ingyenesen, legálisan használható eszköz áll rendelkezésünkre. Ezek az oldalak azért is hasznosak lehetnek, mert ily módon rendszeresen lehetőségünk nyílik önmagunk ellenőrzésére („ön-OSINT").[33] Az ön-OSINT rendszeres végzése rendkívül fontos. A közösségi oldalak gyakran változtatják felhasználói feltételeiket, ilyen esetben az is előfordulhat, hogy a korábbi adatvédelmi beállításainkat felülírták, és amit korábban letiltottunk a nyilvánosság elől, azok ezt követően mégis nyilvánosan hozzáférhetőek. Az ön-OSINT azért is hasznos lehet, mert előfordulhat, hogy olyan helyekre kommenteltünk, vagy olyan véleményt tettünk közzé, amelyre már nem emlékszünk, azonban kellemetlenséget okozhat a megítélésünkkel kapcsolatban. Ily módon törölhetjük az esetleges kellemetlen kommenteket, megosztásokat. Célszerű egyébként a régi megosztások nyilvánosságának korlátozása, az adatok törlése, hiszen csökkenthetjük a profilozásunk pontosságát. Természetesen a törölt adatok továbbra is megmaradnak valamilyen adatbázisban, azonban ezekhez nem férhet akárki hozzá. Nyílt forrású információgyűjtés esetében ezek az adatok nem lesznek elérhetőek. Az adatvédelmi beállításaink, megosztásaink előzményének rendszeres ellenőrzése azért is fontos, mert felfedezhetünk olyan tevékenységeket, amelyeket nem mi végeztünk. Ilyen jellegű tartalmak felfedezése arra utal, hogy valakik hozzáfértek a fiókunkhoz, vagy valamilyen kártékony kóddal fertőződött meg az általunk használt informatikai eszköz. Ha olyan megosztott tartalmakat találunk, amelyeket nem mi osztottunk meg, természetesen nem jelenti feltétlenül, hogy hozzáfértek a fiókunkhoz, előfordulhat az is, hogy nem jelentkeztünk ki a fiókunkból egy olyan eszközön, amelyhez mások is hozzáférnek, és valamilyen tartalom megosztásával tréfálnak meg bennünket. Ennek elkerülése érdekében minden alkalommal jelentkezzünk ki a felhasználói fiókjainkból, és ne adjuk meg hozzáférési adatainkat senkinek. Ezzel kapcsolatban meg kell említeni a jelszavak tárolását, hiszen nemcsak az jelent problémát, ha egy postitre felírva kiragasztjuk a munkaállomáson, hanem a böngésző által történő elmentése is komoly kockázatot rejt. A böngészőkben elmentett jelszavak tárolása azért is kockázatos, mert azok védelme gyenge, és külső támadók is megszerezhetik. Annak ellenőrzése, hogy milyen honlapokat látogattunk meg, milyen keresési előzményeink vannak, azért célszerű, mert ha kirívó sémákat tapasztalunk, felfedezhetjük az eszközünk, hálózatunk kompromittálódását. Ha például a keresési előzményeink között nagy számban találunk olyan kereséseket, amelyeket nem mi indítottunk, utalhat arra, hogy valamilyen kártékony kód indítja ezeket a kereséseket

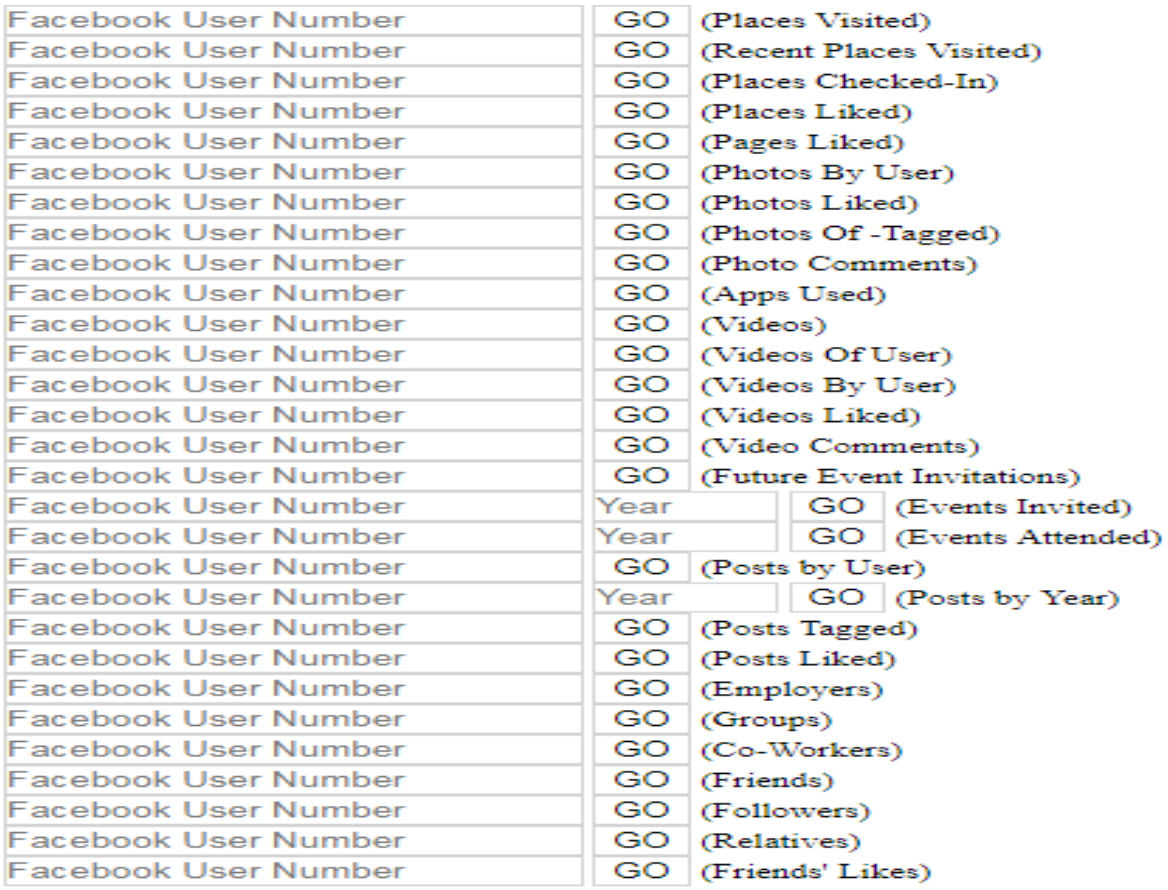
Google keresés során számos olyan oldalt találhatunk, amelyek segítségével percek alatt gyűjthetünk különböző információkat a célszemélyről. Erre szolgál példaként az 1. számú ábrán látható oldal (www.uk-osint.net). Ehhez csupán a célszemély egyedi azonosítójára, vagyis ID Numberére van szükségünk, de ezt egy másik oldal használatával másodpercek alatt megszerezhetjük. (2. számú ábra) Ehhez csupán a Facebook-felhasználó adatlapjának URL-je szükséges. Ezt követően az ID Numbert bemásoljuk a számunkra megvizsgálni kívánt részhez, és az oldal azonnal listázza a nyilvánosan megjeleníthető találatokat. (3. számú ábra) Ez azt jelenti, hogy nem látjuk azokat a megosztásokat, amelyeknek a láthatóságát korlátozta a felhasználó, de számos esetben nincs módunk letiltani a nyilvánosságot. Az általunk követett oldalak, nyilvános csoportok vagy azon ismerőseink, akik nem tiltották le a láthatóságot, meg fogják jeleníteni az azokon végzett tevékenységeinket (kommenteket, megosztásokra adott reakcióinkat). Az oldalon minden olyan nyilvános adat megtalálható, amelyeket nem tiltunk le, például kapcsolatainkat, munkatársainkat, lakóhelyünket stb.

[33] Természetesen egyes oldalak esetében ez csalóka lehet, hiszen az önellenőrzés esetében olyanokat is láthatunk a saját profilunk kapcsán, amelyek láthatóságát más személyek esetében letiltottuk.

1. ábra: Nyílt forrású információgyűjtés pár kattintással a Facebookról (forrás: www.uk-osint.net)

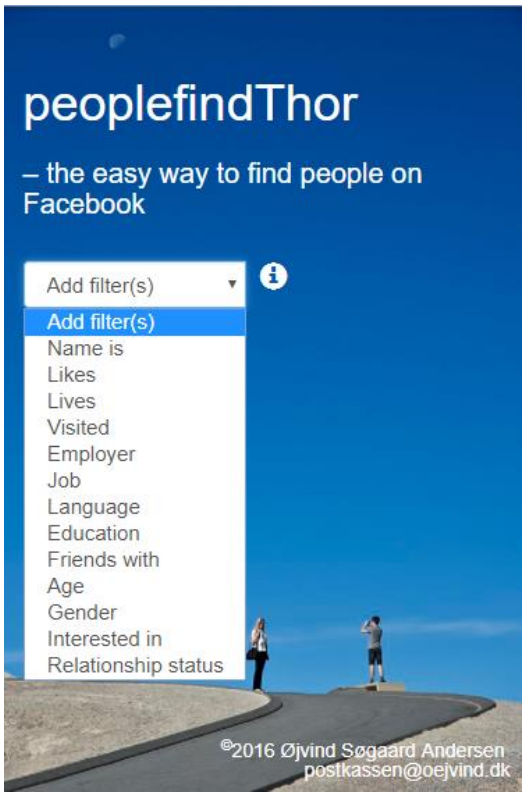


2. ábra: Hogyan szerezzük meg a célszemély Facebook ID Numberét? Forrás: http://lookup-id.com/



3. ábra: Néhány példa, hogy milyen információkat szerezhetünk meg pár perc alatt.
Forrás: https://inteltechniques.com/OSINT/facebook.html

A bemutatott oldalak természetesen csak akkor használhatóak, ha ismerjük a célszemélyt. Ennek hiányában is kereshetünk általunk definiált variánsok alapján, amelynek eredményeképpen azokat a felhasználókat kapjuk meg, akik az általunk megadott keresési feltételeknek megfelelnek, és ezek az adatok róluk nyilvánosan elérhetőek. (Lásd 4. számú ábra) Ilyen variáns lehet például a lakhely, nem, kor, oldalkedvelések, munkahely, iskola, kapcsolati státusz stb. Miután megtaláltuk a számunkra érdekes személyt, akkor az előző módszer segítségével részletesen gyűjthetünk róla információt.



4. ábra: Nyílt forrású keresés különböző variásnok alapján. Forrás: https://www.peoplefindthor.dk/

A bemutatott oldalak vagy a hozzájuk hasonló, egyéb nyílt forrású információgyűjtést támogató oldalak használata azonban ellentmondásos adatvédelmi szempontból. Bár nyílt forrásból dolgoznak, azonban automatizált adatfeldolgozást valósítanak meg, melynek a jogi szabályozása már szigorúbb. Ugyanúgy szürke zóna, hogy milyen célból gyűjtjük az adatokat, hiszen az adatkezelés elveit, mint például a célhoz kötöttség elvét meg kell valósítanunk. A Nemzeti Adatvédelmi és Információszabadság Hivatal (NAIH) által kiadott tájékoztató szerint a munkáltató bizonyos feltételek mellett ellenőrizheti az állásra jelentkezők közösségi profiljait.[34] A tájékoztató kimondja, hogy a munkáltató ellenőrizheti a pályázó közösségi oldalait, ha:

- *„a jelentkező előzetes tájékoztatása a közösségi oldalainak vizsgálatáról;*
- *kizárólag a nyilvánosan elérhető adatokat ismerheti meg a munkáltató, a korlátozottan nyilvános adatokat nem nézheti meg. Korlátozottan nyilvános adat például, ha az érintett egy zárt csoport tagja, és ebben a zárt csoportban oszt meg tartalmat. A munkáltató ilyen esetben nem kérhet meg senkit, aki ennek a zárt csoportnak a tagja, hogy számára információkat osszon meg az érintett tevékenyégéről;*
- *a munkáltató csak azokat a nyilvános adatokat vizsgálhatja, amelyek a pályázattal, a munkakör betöltésével kapcsolatosak. Ebbe a körbe azonban nem tartozhat bele a magánélettel, párkapcsolattal, vallással összefüggő adatok megismerése.*
- *az érintett nyilvános tevékenysége megismerhető, az ily módon megszerzett adatokból következtetéseket vonhatnak le, de minden egyéb adatkezeléssel összefüggő művelet*

[34] A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről, 2016. november 15.
https://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf

jogellenesnek minősül, tehát a profilját nem mentheti le, nem tárolhatja, és nem továbbíthatja harmadik fél részére."

Ez utolsó két pont esetében azonban ellentmondást tapasztalhatunk. Nehéz elképzelni olyan szituációt, amely során a nyilvános megosztásokból akarva-akaratlanul nem szűrünk le következtetéseket az illető magánéletéről, politikai meggyőződéséről. Annak megítélését, hogy a NAIH tájékoztatója alapján sértjük-e az illető magánszféráját, csak akkor tudjuk eldönteni, ha megnézzük az adott megosztásokat, s ezt követően ennek feldolgozása egyúttal következtetések levonásához vezet. Ez alapján nehezen biztosítható, hogy csak a NAIH által engedélyezett tartalmakat vegyék figyelembe. Azt sem szabad elfelejteni, ha valaki a nyílt forrású információgyűjtést egy támadás előkészítése érdekében végzi, nem foglalkozik az adatvédelmi előírásokkal.

Ahogy számos rendőrségi ügy alátámasztja, alapvetésként megállapíthatjuk, támadók, hamis profilok segítségével gyakran pár órás ismertséget követően képesek erotikus tartalmú képeket kicsalni a gyermekektől. Már pedig, ahogy a bemutatott oldalak is igazolják, néhány perc alatt gyűjthetünk olyan információkat, amelyeket a támadók céljaiknak megfelelően felhasználhatnak. Nem nehéz belátni, milyen nehéz döntésre kényszerül az a dolgozó, akit a gyermekétől kicsalt erotikus képpel zsarolnak meg a támadók, hogy rajta keresztül férjenek hozzá egy védett informatikai rendszerhez vagy érzékeny adatokhoz. Az informatikai biztonsági kontrollok segítenek felkészülni a rendszer „nyugalmi", ideális állapotát megzavaró helyzetekre az incidens teljes életciklusa (kialakulása, észlelése, kezelése) alatt. Az incidensre adott válaszok alapján az informatikai védelmi eljárásokat preventív, korrektív vagy reaktív, illetve detektív tevékenységek alapján csoportosíthatjuk. Ezek a kontrollok gyakorlatilag a biztonsági incidensek bekövetkezése elleni védelmet jelentik. Szabó András megfogalmazásában: „*…a preventív funkciók biztosítják a biztonsági incidensek megelőzését, a támadások alapjául szolgáló sérülékenységek megszüntetését, azok kihasználásának akadályozását. A korrektív, reaktív funkciók a támadások bekövetkezte után aktivizálódnak, és próbálják megszüntetik a biztonsági incidens kiváltó okát, minimalizálják a károkat. A detektív funkciók a támadások nyomainak gyűjtését, hiteles rögzítését és megjelenítését végzik az incidens bekövetkezése előtt, alatt és után.*"[35] A közösségi média használatával kapcsolatban a preventív kontroll többek között az adminisztratív szabályozással kapcsolatban tekinthető relevánsnak, továbbá a megfelelő adatvédelmi beállítások használatát, a kétlépcsős azonosítás alkalmazását, illetve tudatos használatát említhetjük. A korrektív, reaktív kontroll tekintetében alapvetően a fiók kompromittálódásával kapcsolatos védelmi eljárásokat nevesíthetjük, mint például a jelszó megváltoztatása. Detektív kontroll a bekövetkezett informatikai támadás felderítése, digitális forenzikus vizsgálata során jelentkezik, amikor például a támadók social engineering támadást alkalmaztak, amelyben felhasználtak valamilyen közösségi oldalt, akár információgyűjtésre, akár kártékony kód célba juttatására.

2.1.4. Kiberkémkedés

Kiberkémkedés alatt az államok, magánszemélyek, piaci szereplők által végzett hírszerzést értjük, amit informatikai eszközön végeznek. A közösségi média nem csak az OSINT esetében játszik fontos szerepet. Ahogy az Edward Snowden által nyilvánosságra hozott dokumentumokból tudhatjuk, az elektronikai felderítéshez (SIGINT) sorolható kommunikációs felderítés (Communications Intelligence, COMINT) esetében is rendkívül jelentős. A COMINT a távközlési- hírközlési kommunikáció felderítésére vonatkozik, írásos üzenetek vagy hanganyagok lehallgatására alkalmazott tevékenység.[36] A Snowden

[35] Szabó András: *Preventív hálózatvédelmi rendszerek alkalmazási lehetőségei a támadások detektálására, valamint a módszerek elemzésére.* Hadmérnök, VI. évfolyam, 2011, 4. szám, pp. 239–249., p. 241.

[36] Béres János: *A hírszerzés feladatrendszere.* In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest, 2014, p. 363.

iratokból tudhatjuk, hogy az amerikai nemzetbiztonsági szolgálatok és partnerszolgálatai[37] a nagy közösségi oldalak adatbázisához teljes mértékben hozzáfértek, valós időben, tömegesen voltak képesek a felhasználók üzeneteit olvasni, informatikai eszközeik fölött átvenni az irányítást, és ezen keresztül megfigyelni őket. Nem véletlen, hogy egyes szerzők a közösségi médiát a hírszerzés önálló ágnak tekintik (SOCMINT).[38]

2.1.5. Kiberhadviselés

A közösségi média Bányász Péter megítélése szerint értelmezhető az információs hadszíntér egy speciális területeként.[39] Azt, hogy a közösségi média jelentős szerepet tölt be az információs műveletekben, több szerző is érintette. Drew Herrick kutatásaiban[40] felvázolta a közösségi média információs műveletekben betöltött szerepét.[41] Herrick azonban csupán a téma egy kis szeletét érintette. Annak érdekében, hogy az információs hadszíntér tartományaként nevesíthessük a közösségi médiát, Bányász Péter kutatásai alapján azonosíthatjuk:

- a tartomány kereteit,
- illetve azokat a területeket, amelyek az információs műveletek végzésében szerepet játszanak.

A tartomány kereteit a közösségi média egyénekkel és a társadalmi alrendszerek viszonyában vizsgálhatjuk. A közösségi média korábban ismertetett fogalmából egyértelműen következik, hogy személyközi kapcsolatokból tevődik össze, amelyek különböző közösségi csatornákon keresztül zajlanak. Eltérő jellemzővel írhatók le azonban az egyes generációk, amelyek egyrészt az attitűdben, a használati szokásokban, adat- és információbiztonsági tudatosságban jelentkeznek. Ez a különbözőség fontos az esetleges műveletek tervezésekor, hiszen a célcsoport azonosítását követően figyelembe kell venni az eltéréseket és adoptálni a tervezéskor.

A NATO információs műveletekkel foglalkozó doktrínáját alapul véve[42] Bányász Péter hét területet azonosított, amelyek megjelennek az információs műveletekben:

- lélektani műveletek;
- megjelenés, viselkedés, arculat (PPP);
- műveleti biztonság (OPSEC);
- információbiztonság (INFOSEC);
- kulcsfontosságú vezetőkkel kapcsolatos tevékenység (KLE);
- számítógép-hálózati műveletek (CNO);
- civil-katonai együttműködés (CIMIC).[43]

Az egyes támadástípusok alapján kijelenthetjük, hogy a közösségi média rendkívül komplex biztonsági fenyegetést jelent. A közösségi oldalak nem megfelelő használata számos területen jelent veszélyt az egyénre, a szervezetekre egyaránt.

---

[37] Partnerszolgálatai alatt elsődlegesen a Big Five Eyes országait, Nagy-Britanniát, Kanadát, Ausztráliát és Új-Zélandot kell érteni.
[38] Omand et al.: *Introducing social media intelligence (SOCMINT).* Intelligence & National Security 27(6) December 2012. https://doi.org/10.1080/02684527.2012.716965}
[39] Bányász 2018. i. m.
[40] Uo.
[41] Herrick, Drew: *The social side of 'cyber power'? Social media and cyber operations*. In: International Conference on Cyber Conflict, CYCON, Cyber Power. N.Pissanidis – H.Rõigas – M. Veenendaal (Eds.) NATO CCD COE Publications, Tallin, 2016.
[42] AJP-3.10 Allied Joint Doctrine for Information Operation, 2009. https://info.publicintelligence.net/NATO-IO.pdf
[43] Bányász 2018. i. m.

3. A közösségi hálózatok hivatali használatának esetei

3.1. A közösségi média használatának feltételei

A 2012. évi I. törvény a munka törvénykönyvéről[44] (a továbbiakban: Mt.) általános magatartási követelmények részénél meghatározza: „*…a munkavállaló a munkaviszony fennállása alatt – kivéve, ha erre jogszabály feljogosítja – nem tanúsíthat olyan magatartást, amellyel munkáltatója jogos gazdasági érdekeit veszélyeztetné. A munkavállaló munkaidején kívül sem tanúsíthat olyan magatartást, amely – különösen a munkavállaló munkakörének jellege, a munkáltató szervezetében elfoglalt helye alapján – közvetlenül és ténylegesen alkalmas munkáltatója jó hírnevének, jogos gazdasági érdekének vagy a munkaviszony céljának veszélyeztetésére. A munkavállaló magatartása a 9. § (2) bekezdésében foglaltak szerint korlátozható. A korlátozásról a munkavállalót írásban előzetesen tájékoztatni kell*.” Az Mt. 11. §-a az alábbiakat írja elő: „*…a munkáltató a munkavállalót csak a munkaviszonnyal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A munkavállaló magánélete nem ellenőrizhető. A munkáltató előzetesen tájékoztatja a munkavállalót azoknak a technikai eszközöknek az alkalmazásáról, amelyek a munkavállaló ellenőrzésére szolgálnak*.” A közösségi média általános használatával foglalkozó alfejezetben a Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről résznél már említettük a szabályozás nehézségét, hiszen rendkívül nehezen alkalmazható a fenti jogszabályi előírás, ha az adott munkahelyen a munkáltató és a munkavállalók ismerősök valamilyen közösségi hálózaton vannak, hiszen akarva-akaratlanul láthatóak lehetnek, ezáltal ellenőrizhetik a munkavállalót szabadidejében is abban az esetben, ha a munkavállaló nem alkalmaz főnökei esetében szigorúbb adatvédelmi beállítást.

A közösségi média használat eltérő kockázatokat jelent az egyes hivatásnemek, beosztások tekintetében. Az általános kockázatok esetében a social engineeringgel foglalkozó résznél már említettük, hogy bárki célpontja lehet a támadóknak az általa kezelt adatoktól, rendszerektől függetlenül, a biztonságtudatosság szintjének növelése így minden szervezet minden munkavállalója esetében elengedhetetlen. A közösségi média használat normatív szabályozásával kapcsolatban még hiátusokat tapasztalhatunk a tanulmány írásának idején.[45] A közösségi média használat általános tiltása nem csak betarthatatlan, egyúttal kontraproduktív is lehet, ha a munkavállalók megpróbálják kijátszani az előírásokat, ily módon lehetőséget teremtve a támadóknak a rendszerekbe történő behatolásra. A közösségi oldalak használatának tiltása általános esetben csupán a munkaidőben történő használatra korlátozódhat, azonban az okos mobil eszközök és mobilinternet használatával a munkahelyen a munkaállomásokon letiltott közösségi oldalak ugyanúgy elérhetőek. Ha maguknak a közösségi oldalaknak a használatát nem is tiltjuk munkaidőben, de ezeket a munkavállaló csak saját okos mobil eszközéről éri el mobilinternetet használva, akkor az esetleges kártékony kódok, amelyek hozzáférést adhatnak az informatikai eszközhöz, nem veszélyeztetik a munkahelyi eszközöket.

Értelemszerűen azonosíthatunk bizonyos területeket, ahol a közösségi média használat korlátozható, tiltható, de ez a munka szenzitivitásának függvénye. Ilyen munkakör egyértelműen a nemzetbiztonsági területeken van. A nemzetbiztonsági szolgálatok esetében a közösségi média használatára vonatkozóan belső szabályozók érvényesek, azok jellegüknél fogva nem nyilvánosak, ennél fogva e tanulmány keretei között a nemzetbiztonsági szolgálatok munkatársainak közösségi média használata szabályaival nem foglalkozunk. Azonban az ezen munkakörökben dolgozók esetében a közösségi média használatának jelentős korlátozása indokolt. Ez persze nem jelenti azt, hogy egyes munkakörökben

[44] 2012. évi I. törvény a munka törvénykönyvéről, https://net.jogtar.hu/jogszabaly?docid=A1200001.TV
[45] A tanulmány 2018 őszén készült.

feladataik ellátása érdekében nem használnak különböző álprofilokat – például pedofilhálózatok, szervezett bűnözők felderítése érdekében –, azonban ezek a profilok a konspirációs szabályok betartása mellett kell léteznek, a használó(k) valódi identitására nem utalhatnak, azokból nem lehet a valódi személyes adataikra következtetést levonni.

A kulcsfontosságú vezetők esetében korlátozottan megengedhető a közösségi média használata, de ez csakis az információbiztonsági előírások szigorú betartása mellett engedélyezhető, ahogy ezt a Hillary Clintont érintő e-mail botrány is hangsúlyosan illusztrálja. Kulcsfontosságú vezetők kapcsán azonban elvárásként is megjelenhet, hogy a közösségi médiát a transzparencia jegyében, illetve a stratégiai kommunikáció eszközeként alkalmazzák. Az Egyesült Államokban erre számos jó gyakorlatot találhatunk, igaz, ezek nem személyes profilok, hanem rajongói oldalak formájában üzemelnek, és professzionális kommunikációs stábok működtetik őket.

A munkáltató megítélésünk szerint jogosan tilthatja meg a közösségi oldalak használatát a munkavállalói számára, ha azok minősített adathoz férhetnek hozzá. Természetesen minősített adatokat nem a közösségi oldalakon keresztül fognak küldeni, de ahogy fentebb láttuk, a közösségi oldalaknak komoly szerepük van a profilozásban, és az ily módon gyűjtött információkat a munkavállalóról akár zsarolásra is felhasználhatják. Azt sem szabad elfelejteni, hogy az amerikai nemzetbiztonsági szolgálatok valós időben képesek megfigyelni a privát beszélgetéseket is, így ha a minősített adathoz hozzáférő személy privát beszélgetései alatt olyan információkat közöl partnerével, amelyeket adott esetben felhasználhatnak ellene, komoly kockázati tényezővé válik. A nemzetbiztonsági szolgálatok mellett azonban kémprogramokat felhasználva bűnözők, terroristák, hackerek, hacktivisták is hozzáférhetnek ezekhez az információkhoz.

A jelenleg hatályos jogszabályok ezekre a kockázatokra nem adnak válaszokat. Megvizsgálva a Magyar Honvédségre és a Rendőrségre vonatkozó, ezekkel kapcsolatos törvényi előírásokat, bár találunk a közösségi média használatával kapcsolatosakat, ezek azonban több kiegészítésre és több terület pontosabb szabályozására szorulnak.

A Magyar Honvédség esetében a 2012. évi CCV. törvény a honvédek jogállásáról[46] (a továbbiakban: Hjt.) és a 72/2011. (VI. 30.) HM utasítás a Honvédelmi Minisztérium és a Magyar Honvédség külső kommunikációjának rendjéről[47] tekinthető irányadónak. Konkrétan egyik norma sem érinti a közösségi médiában való jelenlét szabályait, azonban általuk azonosíthatunk különböző területeket, amelyek indokolttá tennék a közösségi média használatára vonatkozó előírásokat.[48] A Hjt. 5. §-a az „Általános magatartási követelmények” kapcsán érinti a honvédek szolgálatteljesítésen kívüli szabályait, amely rögzíti a Magyar Honvédség iránti közbizalom megóvásának kötelezettségét. A Hjt. rendelkezik egyes alapjogok gyakorlásának korlátozásáról, ami esetünkben például a gyülekezési jogra, párttagságra stb. vonatkozik (21–23. §). Figyelembe véve, hogy a nagy közösségi oldalak, mint például a Facebook is a nyilvánosság színterei, hiába is korlátozzuk a láthatóságot ismerőseinkre, megvan a lehetőség arra, hogy a jogszabályi előírásokat megsértsük. Hiába tiltott politikai rendezvényen való részvétel, ha valamilyen reakciót adunk egy politikai tüntetésről szóló eseményre, az ugyanúgy értelmezhető az azon való részvétel szándékaként. Bonyolultabb a 22. § értelmezése, mert bár egy zárt Facebook csoport nem azonos egy bejegyzett szervezettel, azonban a csoport működése, belső szabályai, céljai lehetnek hasonlóak bejegyzett szervezetekhez. A zárt csoportban pedig a felhasználó a viselkedésével

[46] 2012. évi CCV. törvény a honvédek jogállásáról, https://net.jogtar.hu/jogszabaly?docid=A1200205.TV

[47] 72/2011. (VI. 30.) HM utasítás a Honvédelmi Minisztérium és a Magyar Honvédség külső kommunikációjának rendjéről, http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2011/10.pdf

[48] Személyes beszélgetés során hívták fel a figyelmem a 87/2011 MH ÖHP intézkedésre, amely a közösségi média használattal kapcsolatban fogalmazott meg előírásokat (például geotagging tiltása, az adatvédelmi beállítások alkalmazása stb.), de az intézkedés nyilvánosan nem érhető el, így nem tárgyalhatom az alfejezetben.

könnyen végezhez olyan tevékenységeket, amelyek ütköznek a Hjt-ben megfogalmazottakkal. Legalább ennyire fontos a 23. §, hiszen a közösségi oldalon folytatott aktivitásunk még ha nem is tudatosan, de – a megosztott hírek, vélemények akár kép, videó vagy írott szöveg formájában – alkalmas lehet pártpolitizálásra, a szolgálati fegyelmet sértő tartalmak megosztására stb. Nem nehéz belátni, hogy különböző álhírek megosztásával, legyen szó a Honvédség állapotáról, olyan politikai tartalmakról, amelyek a Honvédség feladatkörébe tartoznak (például migráció, határőrizet stb.), igen komolyan sérthetik az előírásokat. Amitől különösen fontossá válik a 23. §, és indokolja a 72/2011. (VI. 30.) HM utasítás említését a „sajtónyilvánosság" kitétel.

Mai napig nem eldöntött kérdés, hogy a Facebook sajtóterméknek minősül-e. Politikusok, a média szereplői akképpen érvelnek, hogy a Facebook is sajtótermék, amiből kifolyólag a sajtóra vonatkozó szabályokat kell érvényesnek tekinteni rá, de a Facebook egyelőre sikeresen lobbizott ez ellen. Ennek ellenére a magyar lakosság jelentős hányada elsődleges hírforrásként a Facebookot használja, a sajtónyilvánosság ebből következően érvényes rá. Ily módon az idézett HM utasítás a 15. § (1) d) pontjában a Hjt-n felül konkretizálja, hogy a személyi állomány „*a szolgálati rendet és fegyelmet sértő internetes bejegyzést nem tehet*".

Mindez nemcsak indokolja a közösségi média használatra vonatkozó konkrét szabályozás megalkotását, ami a közösségi média felületein megosztott tartalomból a fent idézett előírások tisztázását segíti elő, hanem a használatából fakadó, a felhasználók megfigyelésére alkalmazható eljárások elleni védekezés erősítése is.

A Rendőrség tekintetében a hatályos jogszabályi előírások több esetben hasonlóak a Honvédséggel kapcsolatos szabályozókkal, de itt létezik egy ORFK utasítás a közösségi média használattal kapcsolatban, azonban ez is jelentős kiegészítést kíván meg. A 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról[49] (a továbbiakban: Hszt.) a Hjt-hez szinte szó szerint hasonló megkötéseket alkalmazza a „Véleménynyilvánítás szabadsága" (21. §) résznél. Az országos rendőrfőkapitány 11/2015. (VII. 10.) ORFK utasítása a hivatásos állomány tagjának az internetes felületen a hivatásos állományba tartozására vonatkozó adatok nyilvánosságra hozatalának szabályozásáról[50] rendkívül fontos megállapítást tesz, amikor a védendők körébe beemeli a hivatásos állomány tagjának közeli hozzátartozóit. Ennek az információnak a korlátozását a 2006–2010 között lezajlott politikai tüntetések esetén a szélsőjobboldalhoz kötődő szervezetek[51] tevékenysége is alátámasztja. Mint az közismert, az akkor érvényes jogszabályok lehetővé tették, hogy tüntetéseket biztosító rendőrökről fényképet készítsenek.[52] Olyan weboldalak, mint például a Kuruc.Info, a képeken azonosított rendőröket felkutatva a közösségi oldalakon levő profiljaikat listázta, és erre bíztatta olvasóit is, hogy egészítsék ki új információkkal az általuk ismert rendőrökkel kapcsolatban.[53] Nincs ismeretünk arról, hogy az ilyen listákra felkerült rendőröket atrocitás érte volna, de ettől függetlenül komoly lélektani hatása van, ha az embert egy gyűlöletkeltő listán feltüntetik a széles nyilvánosság előtt. A 11/2015. (VII. 10.) ORFK utasítás így véleményünk szerint legitim módon korlátozza, hogy a hivatásos állomány tagjai internetes felületeken magánszemélyként megosszák a Rendőrség állományába való tartozás tényét, beosztásukat, rendfokozatukat, illetve a Rendőrség

[49] 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról, https://net.jogtar.hu/jogszabaly?docid=A1500042.TV

[50] Az országos rendőrfőkapitány 11/2015. (VII. 10.) ORFK utasítása a hivatásos állomány tagjának az internetes felületen a hivatásos állományba tartozására vonatkozó adatok nyilvánosságra hozatalának szabályozásáról, http://frsz.hu/sites/default/files/docs/11_2015_orfk_ut_internetes_feluleten_a_hiv_allomanyba_tartozasra_vonatkozo_adatok_nyilvanossagra_hozatalanak_szabaloyzasarol.pdf

[51] Például a Kuruc.info.

[52] Az akkor hatályos adatvédelmi törvény alapján az intézkedő rendőr adata közadatnak minősült.

[53] Az akkori szélsőjobboldali tüntetők a rendőröket „AVH"-sokként azonosították.

állományába tartozásukra utaló képet, videót, hangfelvételt. Egyben azt is rögzíti az utasítás, hogy ha korábban nyilvánosságra hozta ezeket az adatokat, úgy köteles utólag törölni azokat. Megengedi azonban a magánvélemény közzétételét, ha „*a szolgálati időn kívül végzett tudományos, oktatói, művészeti, lektori, szerkesztői, a jogi oltalom alá eső szellemi tevékenységével összefüggésben*" valósul meg. Ettől eltekintve úgy véljük, célszerű pontosítani a közösségi média használat szabályait mind a Rendőrség, mind a Magyar Honvédség esetében.

Elengedhetetlen, hogy a közösségi oldalakon a legszigorúbb adatvédelmi beállításokat alkalmazzuk, hiszen ily módon megnehezíthetjük azok dolgát, akik a profilozásunkat végeznék, beleérve a kapcsolati hálónk felderítését is.[54] Ahogy korábban már volt szó róla, nyílt forrású információgyűjtéssel a felhasználó által megosztott tartalmakon kívül számos információt gyűjthetünk. Egy poszt megosztásával, még ha annak tartalma irreleváns is, számos egyéb adatot megosztunk, mint például a geolokációs helymeghatározásunk. Emlékezetes eset volt a 2018 januárjában történt adatvédelmi incidens, amikor egy fitness alkalmazásból nyilvánosságra került a felhasználók útvonala. A több mint háromtrillió GPS-adatból térképen ábrázolni lehetett a felhasználók útvonalát, amiből kutatók visszavezették többek között amerikai katonák csapatlokalizációját, példaként nevesítve az afganisztáni Helmand tartományt, hiszen az ott szolgálatot teljesítők edzés közben használták az alkalmazást.[55] A műveleti biztonság megteremtése érdekében szükséges korlátozni az okos mobil eszközök használatát, különös tekintettel azokra az alkalmazásokra, amelyek geolokációs helymeghatározást használnak.

Egy social engineering támadás esetében például rendkívül hasznos információ lehet, hogy a célszemély milyen alkalmazásokat használ. A Facebook Messenger árulkodó a mobil készülékünkön levő operációs rendszerrel kapcsolatban, amelynek ismeretében célzott támadást indíthatnak, kihasználva az operációs rendszer sebezhetőségeit, alkalmazásengedélyekkel kapcsolatos policyját. Mivel olyan tartalmat egyébként sem lehet megosztani nyilvánosság előtt, amelyet a jogalkotó a Hjt-ben és Hszt-ben is külön nevesített, információbiztonsági szempontból érdemes a szabályzóban felhívni a figyelmet arra, hogy a magánélettel összefüggésben megosztott tartalmat, amely egyébként csak egy szűkebb nyilvánosságra tartozik, azt csupán erre a körre szűkített adatvédelmi beállítás mellett érdemes megosztani. Más személyek profilja esetében a láthatóság ellenőrzésére lehetőségünk van, de ha a fenti kitétel nem valósul meg, úgy nem javasolt a tervezett tartalom megosztása.

A hatályos szabályozók nem foglalkoznak a technológiai adatgyűjtéssel, holott az ezekből származó kockázatok jelentősége miatt indokolt lenne. Az internetes oldalak, közösségi oldalak, okos mobil eszközök használata esetén, amellett, hogy a tevékenységünk nagy mértékben nyomon követhető nyilvános megosztásainkból, ahogy erről már korábban szó volt, privát üzeneteink sincsenek feltétlenül biztonságban. Privát üzeneteinket a nagy közösségi oldalak akár reklám célból is eladják kiemelt üzleti partnereinknek, ahogy ez például a Facebook esetében 2018 decemberében nyilvánosságra került. Ebből következően célszerű ezeken a felületeken kerülni az intim témákat, ha el szeretnénk kerülni annak a lehetőségét, hogy harmadik fél birtokába kerüljenek. Az okos mobil eszköz használatra vonatkozó szabályok kidolgozása is megkerülhetetlen kérdés, amelynek érintenie szükséges az alkalmazások használatával kapcsolatos eljárásokat (figyelembe véve az alkalmazásengedélyeket),[56] a

[54] Heaven, Douglas: *The internet knows you all too well.* New Scientist, Volume 237, Issue 3168, March 2018., pp. 42–43. https://doi.org/10.1016/S0262-4079(18)30444-5

[55] Hern, Alex: *Fitness tracking app Strava gives away location of secret US army bases*. The Guardian, 2018. január 28. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (2018. 10. 27.)

[56] Az okos mobil eszközökre optimalizált alkalmazások számos kockázatot rejtenek, hiszen használatukért cserébe különböző engedélyeket követelnek meg. A tapasztalat, hogy a felhasználók egy alkalmazás telepítésekor ritkán olvassák el, valójában

Wi-fi hálózatok biztonságát, a megfelelő védelmi eljárások használatát (például frissítsük mindig az általunk használt eszközöket, alkalmazásokat, operációs rendszert, lehetőleg használjunk VPN-t, kommunikációs titkosítást használó alkalmazásokat használjunk stb.[57]) Értelemszerűen ezeknek minden informatikai eszköz esetében érvényesnek kell lenniük, akár munkaidőben, akár szabadidőben. Számos lehetőség van, amelyek segítségével növelhetjük a magánszféránkat. Ezzel kapcsolatban a „Privacy by Desing" elvének gyakorlati megvalósulását elősegítő privátszférát erősítő technológiák[58] (a továbbiakban: PET-ek) jó kiindulási alapot biztosítanak. Ilyen megoldás például a Firefox böngészőhöz készült „Track me not"[59] nevet viselő böngészőkiegészítő, amely olyan anonimizáló alkalmazás, amely meghatározott időnként véletlenszerűen indít kereséseket a megadott keresőmotorokon. Ennek a lényege, hogy az általunk indított keresésekből pontosan meg lehet határozni a profilunkat. Azonban, ha ezt felhigítjuk nagy számú, véletlenszerűen indított keresésekkel, ebben elrejthetjük a valódi kereséseinket, ami nehezíti a profilozásunkat.[60]

Az adatgyűjtésekkel szembeni védekezés egyik legegyszerűbb módjának a pszeudonimizálást tekinthetjük. A folyamat lényege, hogy megfosztjuk az adatokat az egyértelmű személyes adatoktól (például felhasználónév, név), és azokat pszeudonim azonosítókra cseréljük, például véletlenszerűen generált számokra. Ezáltal az egyes rekordok érintettel való kapcsolatának visszaállítása bonyolultabb tevékenységet jelent. Ezzel kapcsolatban a később tárgyalásra kerülő Általános Adatvédelmi Rendelet konkrét rendelkezést fogalmaz meg. A pszeudonimizáláshoz hasonló folyamat az anonimizálás, azonban ez tágabb tevékenységi kört jelent. Bár célja azonos a pszeudonimizálással, azonban anonimizálás során további követelményként fogalmazódik meg, hogy az anonimizálás során létrejövő rekordokat ne lehessen az adatot szolgáltató eredeti személyhez kötni.

A weboldalak nyomkövetését támogatják az úgynevezett cookiek. A cookie-kat alapvetően kényelmi funkcióként igyekeznek interpretálni, hiszen ezáltal az oldalak rendszeres látogatói preferenciáinak megfelelően használhatók minden látogatáskor az oldalak. A nyomon követés azonban oldalakon keresztül is megvalósulhat, például a Google azt követően is követi a felhasználót sütik segítségével, hogy elnavigált az Google oldaláról.[61] Mivel a sütik lehetővé teszik a természetes személyek

---

mihez is engednek hozzáférést, ezért több százezerre tehető azoknak az alkalmazásoknak a száma, amelyeket szándékoltan adathalászat céljából írtak meg. A Facebook vagy más nagyobb közösségi alkalmazások több mint harminc engedélyt kérnek a használathoz. Ilyen engedély lehet többek között minden üzenetünk tartalma, geolokációs helymeghatározás, kameránk, mikrofonunk irányítása, a tárolt file-jaink stb. Az egyes operációs rendszerek eltérő kockázatot jelentenek, ugyanis nem egyforma az alkalmazások adatgyűjtésének engedélyezése. A Facebook alkalmazás kapcsán például az Android engedte, hogy a felhasználó telefonkönyvében szereplő kontaktokkal kapcsolatos tevékenységeket is begyűjtse az alkalmazás (kivel beszéltünk, mikor, mennyi ideig), addig az iOS esetében erre nem volt lehetőség. Eltérő emellett a Google Play áruházba és az App Store-ba történő bekerülés lehetősége. Az App Store esetében több körös biztonsági ellenőrzést követően kerülhetnek fel alkalmazások, melynek következtében jelentősen alacsonyabb a problémás alkalmazások előfordulása iOS-es operációs rendszerek esetében. Minden esetben javasolt ellenőrizni az alkalmazásengedélyeket, mielőtt telepítenénk a készülékre. Ebben különböző weboldalak is segítséget nyújtanak, mint például a Privacy Grade (http://privacygrade.org/home). Az oldal biztonsági kategóriákba sorolja az alkalmazásokat annak függvényében, hogy indokolt-e az általa kért alkalmazásengedély. Egy zseblámpa alkalmazás kapcsán indokolatlan a vaku irányításán felül minden egyéb engedély, különösen az üzeneteink tartalma, kamera irányítása stb. Bővebben lásd: Bányász Péter: *Az „okos" mobileszközök jelentette biztonsági kihívások.* In: Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2016. Nemzeti Közszolgálati Egyetem, Budapest, 2016.

[57] Jó példa erre a Signal vagy a Telegram Messenger.

[58] Kiss Attila: *A biztonsági események és az adatvédelmi incidensek kezelésére vonatkozó előírások hazánk és az EU jogában*. In: Incidensmenedzsment – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2017. Dialóg Campus Kiadó, Budapest, 2017.

[59] Magyar fordításban: „Ne kövess".

[60] Személyes példán bemutatva, a bővítmény telepítése előtt átlagosan naponta 20–30 keresést indítottam a Google keresőjében, ez az automatizálást véletlenszerű keresést követően napi 750–800 keresésre növekedett.

[61] Ezt nevezik cross site trackingnek.

azonosítását, így a 2018. május 25-étől hatályos Európai Általános Adatvédelmi Rendelet[62] (a továbbiakban: GDPR) rendelkezései alapján a sütik által gyűjtött adatok kezeléséről egyértelmű és pontos leírást kell adni az adatvédelmi tájékoztatóban, továbbá az érintettnek minden kétséget kizáróan jóvá kell hagyni a sütik használatát. Ahogy Bányász Péter megfogalmazta: „*…annak megállapítása is nyomkövetés, hogy az érintett járt-e korábban az oldalon. Erre két lehetőség van, első esetben az oldalra történt regisztráció során a felhasználó engedélyezi a sütiket, ez esetben a weboldal következő meglátogatásakor nem jelenik meg újból az engedélyezésre vonatkozó tájékoztató. Regisztráció híján, ha jóváhagyja a sütik kezelését, következő alkalommal már nem jelenik meg a tájékoztató. Kivételt képez ez alól, ha a felhasználó törli a korábban engedélyezett sütiket. Ezzel kapcsolatban a GDPR világosan fogalmaz, az érintett bármikor visszavonhatja a korábban engedélyezett sütiket. Erre egyébként a böngészők egyszerű lehetőséget biztosítanak, de ezen kívül számos olyan PET található böngészőkiegészítőként, amelyek automatikusan eltávolítják az oldal vagy a böngésző bezárását követően a nyomkövetőket*."[63]

A jogszabály nyilvánvalóan nem tudja követni a technológiai fejlődést, ráadásul rendszeresen derül fény olyan új típusú sebezhetőségekre, amelyek korábban biztonságosnak hitt eljárásokat semmisítenek meg (gondoljunk csak például a 2017 novemberében megismert WPA2 sebezhetőségre, amely a Wi-Fi titkosítását játszotta ki), ezért elengedhetetlen, hogy az állomány tagjai mindig naprakészek legyenek. Ennek érdekében meghatározott időközönként a témával kapcsolatos tudatosító előadásokon való részvétel előírása célszerű, valamint továbbképzési programok kötelező elemévé kell váljanak az adat- és információbiztonsággal kapcsolatos kurzusok. A 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról az adminisztratív védelem kapcsán megfogalmazza az oktatást a szervezet munkatársainak biztonságtudatosságának növelésével kapcsolatban. A jogszabály alapján az Ibtv. hatálya alá tartozó szervezetek esetében a szervezet vezetője „*gondoskodik az elektronikus információs rendszerek védelmi feladatainak és felelősségi köreinek oktatásáról, saját maga és a szervezet munkatársai információbiztonsági ismereteinek szinten tartásáról*". Ez a gyakorlatban általában az elektronikus információbiztonságért felelős vezetőnek delegálja a szervezet vezetője. A tudatosságnövelésben az oktatásnak kiemelt szerepe van. Az oktatásnak azonban természetesen nem szabad általánosnak lennie, hiszen az egyes generációknak eltérő az eszközhasználattal kapcsolatos attitűdje, azonban kijelenthető, hogy a fiatalabb generáció korántsem biztonságtudatosabb, mint az idősebbek. A fő eltérés a tanulásban azonosítható az egyes generációk esetében. Marc Prensky véleménye szerint az infokommunikációs technológiák használata befolyásolja a tanulási képességeket.[64] Az általa digitális bennszülöttekként definiált generációra jellemző, hogy gyorsan, az utolsó pillanatban tanulnak, számos multimédia forrást használnak a tanuláshoz, szívesebben használnak ehhez képi, videós anyagokat, mint szövegeket, azonnali visszacsatolást várnak el az elsajátított tudásanyag ellenőrzésével kapcsolatban, kedvelik a multitaskingot. Ezzel szemben a digitális bevándorlók korlátozott számú forrásból származó ismeret lassú átadását preferálják a tanulás során, a multitaskinggal szemben egy vagy két feladatra való koncentrálást részesítik előnyben, a videókkal, képekkel szemben a szövegalapú tanulást kedvelik, és inkább a későbbi visszacsatolást várják el. Az oktatás megtervezésekor ezekre nagy hangsúlyt kell fektetni, hogy az sikeres legyen.

[62] Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT vonatkozású szöveg)

[63] Bányász 2018. i. m.

[64] Prensky, Marc: *Digital Natives, Digital Immigrants, On the Horizon.* MCB University Press, Vol. 9 Iss: 5, No. 5, 2001. október, p. 1–6. http://doi.org/10.1108/10748120110424816

Az 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról[65] (a továbbiakban: Kjt.) esetében nem találunk a Hjt.-hez és Hszt.-hez hasonló előírásokat, azonban a 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről[66] (a továbbiakban: Kttv.) Általános magatartási követelmények résznél megtalálható az alábbi kitétel: „*A közszolgálati tisztviselő a munkaidején kívül sem tanúsíthat olyan magatartást, amely – különösen munkakörének jellege, a munkáltató szervezetében elfoglalt helye alapján – közvetlenül és ténylegesen alkalmas munkáltatója helytelen megítélésére, az általa betöltött beosztás tekintélyének, a munkáltató jó hírnevének, a jó közigazgatásba vetett bizalomnak, valamint a közszolgálat céljának veszélyeztetésére*." A Kttv. 12. § értelmében „*a munkáltató a közszolgálati tisztviselőt csak a közszolgálattal összefüggő magatartása körében ellenőrizheti. A munkáltató ellenőrzése és az annak során alkalmazott eszközök, módszerek nem járhatnak az emberi méltóság megsértésével. A közszolgálati tisztviselő magánélete nem ellenőrizhető. A munkáltató előzetesen tájékoztatja a közszolgálati tisztviselőt azoknak a technikai eszközöknek az alkalmazásáról, amelyek a közszolgálati tisztviselő ellenőrzésére szolgálnak*."

Azt gondolom, belátható, függetlenül attól, hogy a magyar jogszabályi környezet az adat- és információbiztonságot szigorúan szabályozza, a közösségi oldalak és az okos mobil eszközök rengeteg lehetőséget biztosítanak támadások végrehajtására, ami indokolja egy olyan, a közösségi oldalakra és okos mobil eszközökre vonatkozó szabályozó megalkotását, amely az alfejezetben tárgyaltak mintájára konkrétabb előírásokat fogalmaz meg a Magyar Honvédség és a Rendőrség, állományába tartozók, illetve a közalkalmazottak és közszolgálati tisztviselők számára. A szabályzókban foglalt előírások megsértése fegyelmi eljárást vonhat, bizonyos esetekben pedig kell maga után vonjon. A közösségi médiában tanúsított magatartásunkra ugyanolyan szabályoknak kell érvényesnek lenniük, mint a nem virtuális térben. Ha olyan munkakört tölt be a munkavállaló, amely esetében megtiltható a közösségi oldalakon történő regisztráció (nem számítva azokat az eseteket, amikor munkavégzés során álprofilt használ a munkavállaló), ennek ellenére mégis regisztrált, súlyosabb szankciókat szükséges alkalmazni.

Egy átlag felhasználó számos különböző online profilt használ, így az azonosság-kezelés kérdése különösen fontos. Azonosságkezelés alatt azokat a szoftveres megoldásokat értjük, amelyek az egyes profilok munkavégzését támogatják. A személyes, munkahelyi profiljaink mellett gyakran IoT eszközökhöz, szervezekhez, mobil készülékekhez, de újabban ügyfelekhez is rendelünk ilyen azonosítókat. Egyes vélemények szerint az adaptív azonosság-kezelés segít a szervezeteknek abban, hogy átlássák és ellenőrizzék az egyes hozzáféréseket.

Egy felhasználóhoz egy közösségi oldalon belül akár több profil is tartozhat, például, ha különböző hivatali oldalak kezelőjévé válik. Ez esetben különösen fontos az azonosság-kezelés, hiszen, ha megmarad a felhasználónak az oldal kezelési jogosultsága azt követően, hogy már nem dolgozik az adott szervezetnél, óriási károkat képes okozni. Növeli a kockázatot, ha az oldal kezelőjének magán profilját törik fel a támadók, azon keresztül hozzáférhetnek az általa kezelt oldalakhoz is. Az ily módon kompromittálódott fiók nem csupán abban jelenthet kockázatot, hogy olyan tartalmakat osztanak meg a támadók, amellyel az érintett szervezet jó hírnevét károsíthatják, de egy célzott támadás során pánikkeltésre is használhatják. Emellett további kockázatot jelenthet, ha az adott hivatali oldal korábban hirdetéseket vásárolt, ugyanis ezt kihasználva a támadók anyagi kárt is okozhatnak. Fiókjaink védelme érdekében ajánlott a kétlépcsős azonosítás használata. Ennek lényege, hogy a fiókunkhoz a jelszavunkon felül egy plusz lépcsőt iktatunk be azáltal, hogy a szolgáltató az általunk választott formában (például sms-ben, e-mailben, telefonhívás vagy valamilyen QR-kód segítségével) egy

[65] 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról, https://net.jogtar.hu/jogszabaly?docid=99200033.TV
[66] 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről, https://net.jogtar.hu/jogszabaly?docid=A1100199.TV

véletlenszerűen generált, rövid ideig élő kódot küld a felhasználó számára, és a bejelentkezéshez a jelszó megadását követően ezt is be kell írnia.

A közösségi média munkahelyen történő használatának engedélyezése szervezetfüggő. A C-generációnak[67] tanulmányok szerint a közösségi média használathoz való hozzáférés munkaidőben különösen fontos szempont. Vitathatatlan, hogy ha tiltanánk, megtalálja a módot a kijátszásra, újabb biztonsági problémákat okozva mindezzel. Hiába tiltjuk le a közösségi oldalak elérését a munkahelyi gépeken, ha munkakezdéskor nem kobozzuk el a mobil készülékeket, akkor azon keresztül ugyanúgy hozzáférhet a közösségi oldalakhoz.[68] Ebből következően megfontolandó bizonyos szervezetek esetében a közösségi média használatának engedélyezése, hogy adott esetben belső feladatok szervezését, kommunikációt ezeken a felületeken keresztül lehessen alkalmazni. A Telegram Messenger ennek például jó eszköze lehet, titkosított adatkapcsolaton keresztül, fórumszerűen, meghatározott felhasználói kör számára jó megoldást jelent.

3.2. A közösség/a lakosság elérése

A közösségi média talán egyik legfontosabb értékeként azonosíthatjuk, hogy a segítségével kiszélesednek a közéletben való részvétel lehetőségei. A közösségi oldalak nemcsak a véleménynyilvánítás lehetőségeit növelik, de a politikai részvétel növelésében is fontos szerep hárulhat rájuk.

Ennek egyik módja az e-kognokrácia elterjedése lehet.[69] Az e-kognokrácia lényege, hogy általa az állampolgárok beleszólhatnak, maguk is részt vehetnek a problémák megoldásában, véleményeikkel és ötleteikkel növelhetik a társadalom tudását a döntéshozatali eljárások során. Természetesen az elmélet kidolgozói sem hiszik, hogy minden politikai döntést ez alapján kell meghozni, de meg lehet határozni azokat a területeket, amelyek esetében alkalmazni lehet, illetve mindenkinek lehet hozzászólása egy témához, míg más ügyekben (különleges ismereteket igénylő ügyekben) csökkenteni lehet a megkérdezett állampolgárok számát. Ha az e-demokrácia azt jelenti, hogy a polgárok az interneten keresztül (e-részvétel) jelennek meg a döntéshozatali eljárásban, ahol véleményüket, észrevételeiket és javaslataikat kínálhatják a képviselőknek, akkor az e-kognokrácia arra utal, hogy az állampolgárok interneten keresztül vonódnak be (e-implication) a döntéshozatali folyamatba.

A közösségi média kommunikációban betöltött szerepe kétirányú. Nem csupán az állami, önkormányzati szervezetek kommunikálhatnak velünk, például az álampolgári részvétel erősítése céljából, hanem nekünk is lehetőségünk nyílik ezeken az eszközökön keresztül kifejezni véleményünket, értékelhetünk folyamatokat, de akár ügyfélszolgálat csatornájaként is működhetnek. A kommunikáció esetében különösen fontos, hogy milyen jellegű tartalmakat oszt meg a felhasználó, hiszen a szerzői jog védelme ebben az esetben is elengedhetetlen. Az Európai Unióban 2017 év végétől komoly vita zajlott az Európai Unió Parlamentje és Tanácsa által benyújtott javaslatról, ami a digitális egységes piac szerzői jogi kérdései szabályozásáról szólt.[70] A javaslat ellen 85 szervezet fogalmazta meg

[67] Connect, create, contribute, communicate, content creating generation, vagyis kommunikáló, létrehozó, hozzájáruló, kommunikáló, tartalomgyártó generáció.

[68] Ugyanezen okból kifolyólag nehezen értelmezhető a közösségi oldalak esetében a DLP prevenció. A DLP olyan informatikai védelmi rendszer, amely azonosítja, monitorozza és megvédi a bizalmas adatokat a végpontok, a hálózat és adattárolók tekintetében.

[69] Merkovity Norbert: *Bevezetés a hagyományos és új politikai kommunikáció elméletébe*. A Pólay Elemér Alapítvány Könyvtára, Hódmezővásárhely, 2012.

[70] Javaslat Az Európai Parlament és a Tanács irányelve a digitális egységes piacon a szerzői jogról, Brüsszel, 2016.9.14. COM (2016) 593 final 2016/0280(COD)
https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52016PC0593&from=HU

tiltakozását,[71] amely véleményük szerint cenzúrához, az emberi jogok és a sajtószabadság indokolatlan korlátozásához vezetne, ami az oktatásban, a technológiai és a tudományos fejlődésben gátolná az Európai Uniót. Emellett a nagyobb közösségi oldalak esetében olyan tarthatatlan követelményeket állítana a szerzői jogok ellenőrzésére vonatkozóan, amit nem lehet betartani. A jelenlegi szabályozás alapján a szerzői jogok betartását a tartalom feltöltése után kell ellenőrizzék a tartalomszolgáltatók, de a javaslat elfogadását követően ezt a feltöltéskor már meg kell tenniük, és csak a szerzői jogot nem sértő tartalmat engedélyezhetik az oldalukon. A javaslatot végül 2018 szeptemberében elfogadták, a közösségi oldalakon felül hatálya kiterjed továbbá a streaming szolgáltatókra, de a hírmegosztó oldalakra és a tudományos publikációkra is.

A 2010-es évek elején az online marketing szakemberek úgy gondolták, a közösségi média az az ingyen felület, ahol nagy felhasználói elkötelezettséget lehet kiépíteni, okos gerillamarketing kampányokkal megsokszorozni a követők számát. Ez az ingyenesség azonban sokszor csak illúzió volt, hiszen ahhoz, hogy a követők érdeklődését fenntartsák, rendszeresen gondoskodni kellett az oldalról, új tartalmat kellett előállítani, illetve szűrni kellett az oda nem illő tartalmaktól. Minél nagyobb követőtáborral rendelkezik egy oldal, annál időigényesebb, komolyabb feladatot jelent mindez. Ha nincs külön személy, aki kezelje az oldalt, akkor más munkakörből von el értékes időt. Az évek során egyre több pénzbe került a megjelenés, a Facebook hírfolyama a gyakori alakítgatások során másképp rendezte az oldalak megjelenését (ahogy jelenleg a híroldalak háttérbe szorítása az aktuális téma, ha nem fizetnek a megjelenésért cserébe), ezért folyamatosan új és új ismeretek elsajátítását követelte az oldalak kezelőitől, és még több időt vont el. Nincs ez másképp a közigazgatási szervek esetében sem.

A közösségi oldalaknak az egyes szervezetekről alkotott kép pozitív percepciójában igen komoly szerepük van. A sikeres online megjelenés nagyban befolyásolja egy szervezet megítélését, így a pozitív percepció növelheti a lakosság körében való elismertségét, támogatását, valamint a toborzást is segíti.

A Magyar Honvédség professzionális közösségi médiajelenlétet épített ki, nemcsak a Magyar Honvédség szervezete, hanem számos egység esetében tapasztalunk aktív Facebook jelenlétet. Ez rendkívül fontos a Magyar Honvédség megítélésének erősítésében. A megítélés mellett jelentős szerepet tölthet be a toborzásban, ami többek között az Önkéntes Területvédelmi Tartalékosok esetében kiemelt prioritás a jelenlegi kormányzat szempontjából. Az US Army esetében több mint ötezer hivatalos közösségi médiaprofilt találunk, amelyek mind az US Army népszerűsítét hivatottak ellátni.[72] Az egyes egységek mindegyike használja a Facebookot, de azonkívül egyéb platformokon is jelen vannak, mint a Twitter, Youtube, Instagram stb. 2016-hoz képest, amikor egy kutatás során vizsgáltam ezeket az oldalakat, összesen 1922 volt, ami két év alatt majdnem háromszoros növekedés. Nyilvánvalóan más a Magyar Honvédség létszáma az amerikai fegyveres erőkhöz képest, de úgy vélem, a Honvédség által elkezdett nagyon pozitív irányt ki lehet terjeszteni és növelni az egyes egységek közösségi média jelenlétét. Természetesen szem előtt kell tartani a megosztott tartalmak esetében a műveleti biztonságot és információbiztonságot, a feltöltött képek, ha nem kellő elővigyázatossággal járunk el, sérthetik ezeket. Erre nem csak a korábban említett példát lehet hozni, amikor a képek tartalmazták a geolokációs adatokat.

Összehasonlítva a Magyar Honvédség és a Rendőrség Facebook jelenlétét, az előbbi esetében közel 80 ezer kedvelőt láthatunk, míg a Rendőrség esetében ez a szám alig éri el az 1200-at, illetve míg a Honvédség Facebook oldalán naponta több bejegyzést találunk, addig a Rendőrség esetében az utolsó bejegyzés 2017 novembere. Ha a szervezet nem fordít nagy gondot a közösségi médiában való

[71] Open Letter in Light of the Competitiveness Council on 30 November 2017 http://copybuzz.com/wp-content/uploads/2017/11/Open-Letter-COMPET-Council-30-Nov-online.pdf
[72] Official U.S. Army Social Media https://www.army.mil/socialmedia/directory/

jelenlétre, jószándékú amatőrök vagy csalók megteszik helyette, mindkettő igen komoly kockázatot jelent. A rendőrség szóra történő rákeresésre például „Rendőrségi Sajtó” néven jelenít meg egy profilt, ami arra utal, hogy a Rendőrség kommunikációjának csatornája, holott nem oldal, hanem személyes profil, a tartalmat csak akkor láthatjuk, ha ismerősnek jelöltük. Az alacsony adat- és információbiztonság tudatosságú felhasználók nem feltétlenül veszik észre a különbséget, és hivatalos oldalként tekinthetnek rá. Nem nehéz belátni, ha egy ilyen profilt használnak dezinformáció küldésére, pánikhelyzet kialakítására, annak milyen következményei lehetnek. A hivatalos profiloknak óriási szerep jut a kríziskommunikációban is, egy rendkívüli esemény bekövetkezése esetén elengedhetetlen, hogy a közösségi oldalakat felhasználjuk.

A közösségi oldalak az önkormányzatok számára a kommunikáció hasznos csatornái lehetnek, de üzemeltetését nem lehet félvállról venni. Már csak azért sem, mert a közösségi média megfelelő használta a település fejlesztésében is komoly szerepet játszhat. Egy élhető település képe nagyban növeli a lakosok elégedettségét, ami jelentős szerepet játszhat a gazdaság növekedésében. Számos tanulmány mutatta ki, hogy az internetnek komoly szerepe van a GDP növekedésében, de a gazdaság növekedésének a közösségi média is motorjává válhat. Egy prosperáló, élhető település nemcsak a befektetőket vonzhatja, hanem a turizmus növekedésében is fontos. Jó példával szolgálhat Budapest VII. kerületének okostelefonokra készített alkalmazása, amely virtuális sétát tesz lehetővé, bemutatva a kerület sokszínűségét. Az alkalmazás egyfajta turisztikai GPS-ként működik, több száz különböző kerületi turisztikai célpontot helyez el a kerület virtuális térképén. A virtuális útikalauzként is értelmezhető alkalmazás fényképekkel és ismertetőkkel szolgál Erzsébetváros múzeumaihoz, éttermeihez, különféle nevezetességeihez, de programajánlóként is funkcionál. A telefon kamerája segítségével felismeri a kerület épületeit, és információval szolgál róluk. Mára majdnem mindenkinek van a zsebében okostelefon, így az ehhez hasonló alkalmazások rengeteg lehetőséget nyújtanak az önkormányzatoknak, akár a közlekedésfejlesztésben, akár turizmus növelésében, akár a városfejlesztésben.

A közösségi média óriási lehetőséget biztosít a rendkívüli események kezelésében. Rendkívüli esemény alatt alapesetben ember vagy természet által okozott katasztrófát értünk, de ugyanúgy ide sorolható egy terrortámadás is. A katasztrófák elleni védekezés jogszabályban rögzített kötelezettsége minden állampolgárnak. Annak érdekében, hogy az állampolgárok a katasztrófák elleni védekezésbe bevonhatók legyenek, elengedhetetlen, hogy ismerjék a védekezés módjait. A közösségi média e tekintetben rendkívül hasznos eszköz, hiszen segítségével

- nemcsak a lakosság felkészítést könnyíthetjük meg,
- de ezek mellett megkerülhetetlen a kríziskommunikációban,
- a felhasználói aktivitás monitorozásának eszköze, ami erősítheti a védekezés tudatosságát,
- a segítségkérés eszköze is lehet,
- valamint hatékony a kárfelszámolásban is.

A lakosság felkészítésnek kettős szerepe van. Egyrészt az általános ismeretek megszerzésében, a rendkívüli események elleni védekezésben, kötelességeik megismerésében. A blogok, kép- és videómegosztó oldalak, közösségi hálózatok, alkalmazások az oktatásban játszhatnak szerepet, differenciálva akár korcsoport, lakóhely, érintettség alapján. Más felkészítésre van szükség mondjuk az árvízzel sújtott területen élőknek, mint akik hegyekben, nukleáris, ipari létesítmények közelében élnek. Másrészt pedig egy közelgő rendkívüli eseményre aktualizált felkészítésre: pl. egy közeledő hurrikán várhatóan hol fog átvonulni, hol találhatóak menedékhelyek, milyen óvintézkedéseket szükséges megtenni stb.

Egy rendkívüli esemény bekövetkezésekor különösen fontos a lakosság megnyugtatása. A közösségi oldalakon rengeteg információ találhat, közvetíthető, azonban nagy számban terjednek az álhírek is, amelyek egy bekövetkezett katasztrófa esetén súlyosbíthatják a következményeket a pánik kitörésével. Éppen ezért fontos, hogy hivatalos, megerősített információk közlésére használják az erre hivatott szervek, illetve blokkolják azokat a tartalmakat, amelyeket szándékosan pánikkeltésre használnak. Természetesen ez nem feltétlenül valósítható meg könnyen. Az álhírek elleni védekezésre a mai napig nem létezik 100%-osan használható forgatókönyv. Egyes országokban, például Franciaországban az országos választások előtt három hónappal korábban lehetőség nyílik az álhíroldalak cenzúrázására.[73] Az internet cenzúrázása rendkívül kényes kérdéskör, azonban egy rendkívüli esemény bekövetkezésekor az emberi élet védelmében a pánikkeltésre szolgáló álhír oldalak blokkolása célszerű lehet. További lehetőség különböző megosztások fizetett hirdetésként történő terjesztése, amely a hivatalos üzenetek célcsoportok számára történő targetálásával hatékony lehet. A nagy közösségi oldalak, így a Facebook és a YouTube is online közvetítést tesz lehetővé, így nincs szükség kiterjedt technikai eszközökre és személyzetre, csak megfelelő mobil internetes kapcsolatra egy élő közvetítés lebonyolításához. Ezek nagyban kielégíthetik a lakosság hírigényét, ami döntő fontosságú lehet. A hashtag-gel ellátott üzenetek segíthetnek továbbá az információk rendszerezésében, könnyebb kereshetőségében.

Egy jelentősebb rendkívüli esemény esetében a segélyhívó vonalak könnyen túlterheltté válhatnak, a közösségi oldalak ez esetben is hasznosak lehetnek. A Facebook például Safety Check néven egy olyan szolgáltatást vezetett be, amely egy katasztrófa esetén üzenetet küld a felhasználónak, amelyben arról kell nyilatkoznia, hogy biztonságban van-e, vagy segítségre szorul. Ha nem érintett, erről a Facebookon egy bejegyzést tesz közzé automatikusan, hogy megnyugtassa ismerőseit. Jelenleg azonban még nem lehet ezen keresztül segítséget kérni baj esetén. Az okos mobil eszközök lokalizációja azonban lehetővé teszi, hogy a bajba jutott személyeket könnyű szerrel kutathassák fel, ha a készüléke nem sérült meg.

A kárfelszámolás fázisában szintén hasznos a közösségi média, hiszen számos közösségi finanszírozású projektet lehet kezdeményezni, amely az adománygyűjtés mellett akár összekötheti azokat az embereket, akik fizikailag segítenének a károk enyhítésében.

Egy rendkívüli esemény kezelése során célszerű, hogy a kommunikáció a közösségi médiában központi irányítás alatt, egy szervezet részéről történjen.

3.3. A közösségi médiahasználat adatvédelmi kérdései

A kibertérben keletkezett adatok nem köthetőek egy adott nemzethez, a fizikai korlátok kibertérben történő lebomlásával az interneten továbbított adatok akár több országon keresztül jutnak el a címzetthez. Ez azonban azzal a kockázattal jár, hogy az adatcsomagok megfigyelése jelentősen eltérő adat- és információbiztonsági szabályozással bíró országokon keresztül vándorolnak, ami az üzenetek monitorozásának eltérő gyakorlatát vonja maga után. A GDPR ebben a tekintetben jelentős előre lépésként értékelhető, azonban hatályoa csupán az EU állampolgáraira terjed ki.

Az interneten továbbított adatokat a könnyebb kézbesítés érdekében úgynevezett csomagokra bontja a rendszer, és ily módon továbbítja a hálózaton. Miután ez megérkezik a fogadó eszközre, újra összeáll egy egésszé. Hálózatbiztonsági okokból ezeket a csomagokat az internetszolgáltatók átvizsgálják, hogy kiszűrjék az esetleges kártékony kódokat. Ezt az eljárást nevezzük mély csomagvizsgálatnak (DPI).[74]

[73] Sz. N.: *Az álhírek ellen hozott törvényeket Franciaország.* SG, 2018. november 22. https://sg.hu/cikkek/it-tech/134010/az-alhirek-ellen-hozott-torvenyeket-franciaorszag (2018. 11. 28.)

[74] Guo. et al.: DPI & DFI: *A Malicious Behavior Detection Method Combining Deep Packet Inspection and Deep Flow Inspection*. Procedia Engineering, Volume 174, (2017), pp. 1309–1314. https://doi.org/ 10.1016/j.proeng.2017.01.276

Emellett azonban az algoritmus beállításának függvényében lehetőség nyílik bizonyos tartalmak kiszűrésére is, amely a bűnüldözésben (például pedofil tartalmak), a nemzetbiztonságban (terrorista tartalmak) is hasznos. Szélsőséges esetben lehetőség nyílik bizonyos politikai vélemények monitorozására is. Európában a DPI-t kizárólag hálózatbiztonsági szempontok alapján alkalmazhatják, de más országokban nincsenek ilyen szigorú megkötések. Az Egyesült Államokban kereskedelmi célból[75] szabadon használhatják a cégek a DPI-t, de vélelmezhetően többek között Kína, Oroszország és Irán is alkalmazza az internetes mély csomagvizsgálatot, ami akár az ellenzéki vélemények elhallgattatására is felhasználható. A DPI használatából így az is következik, hogy azok az országok, amelyeken keresztülhaladnak az általunk küldött adatcsomagok, hozzáférhetnek a tartalmához. Márpedig az európai gyakorlathoz hasonló szigorú adatvédelmi szabályozás nem gyakori. Emellett azt sem tudjuk, hogy az ily módon esetlegesen megszerzett információkat az érintett állam nemzetbiztonsági szolgálata mily módon használja fel.

A GDPR egységes követelményrendszert fogalmaz meg a személyes adatok kezelését illetően az Európai Unió minden tagállamában, továbbá korszerű választ kíván adni a technológiai fejlődésből következő kockázatokra, hogy ennek segítségével növekedjen a felhasználók új technológiákba vetett hite, és ezáltal növekedhessen a Digitális Menetrendben megfogalmazott európai digitális tér. A Rendelet 32. cikke rögzíti az adatbiztonság megteremtésének érdekében elvárt intézkedéseket, és rendelkezik arról, hogy ahol szükséges:

- *„alkalmazni kell a személyes adatok álnevesített[76] kezelését;*
- *alkalmazni kell a technológiai titkosítását;*
- *biztosítani kell az adatkezelőnek vagy adatfeldolgozónak, hogy a személyes adatok kezelésére használt rendszerekben és szolgáltatásokban folyamatos védelmi intézkedések működjenek;*
- *biztosítani kell, hogy fizikai vagy műszaki incidens esetén rendelkezésre álljon a biztonsági mentés vagy tartalékrendszer;[77]*
- *a védelmi intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást kell az adatkezelőnek kialakítania.”*

Tekintettel a nagy közösségi oldalak adatkezelési gyakorlatára, ezek az elvek különösen fontosak, elég csak a Facebook 2018-as nagy adatvédelmi botrányaira, például a Cambridge Analytica ügyre gondolni.

Adatvédelem tekintetében fontos kezdeményezés volt a 2016-ban megkötött „Adatvédelmi Pajzs” nevű keretegyezmény,[78] amely az Európai Unió és az Egyesült Államok esetében az EU állampolgárok adatainak külföldre továbbításával kívánta rendezni, hiszen az amerikai adatvédelmi felfogás majdhogynem az európai ellentéte. A keretegyezmény célja az volt, hogy az EU állampolgárok adatait szigorúbb adatvédelmi előírások alapján kezeljék az amerikai vállalatok. Végül az „Adatvédelmi Pajzs”

[75] Ilyen cél lehet például a digitális jogok védelme vagy személyre szabott reklámok használata.

[76] A 4. cikk alapján az álnevesítés „*a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve, hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni*”.

[77] A 32. cikk alapján „*az arra való képesség, hogy a személyes adatokhoz való hozzáférést és az adatok rendelkezésre állását kellő időben vissza lehet állítani*”.

[78] European Commission Directorate-General for Justice and Consumer: Guide to the EU-U.S. Privacy Shield, 2016, https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf

a GDPR hatálybalépésével nem tekinthető relevánsnak. A GDPR egyfajta kiegészítése lesz az Európai Parlament és Tanács elektronikus hírközlési rendelete,[79] azonban ezt jelenleg még nem fogadták el.

A technikai adatgyűjtés hiányos szabályozásáról már volt szó, de e tekintetben jó kiindulópontot jelenthet a NAIH „A Nemzeti Konzultáció honlapján a Yandex.Metrica analitikai szolgáltatás igénybevételével összefüggésben indított vizsgálatáról" néven kiadott jelentése. A 2017-ben lezajlott online Nemzeti Konzultáció során derült ki, hogy az üzemeltető Yandex.Metrica analitikai szolgáltatás megsérthette a hatályos adatvédelmi szabályozást, ugyanis a felhasználókról a megengedettnél szélesebb körben gyűjtötte, illetve továbbította harmadik fél részére. A vizsgálat kimondta, hogy „*a Yandex.Metrica a felületeken a tömeges mozgásokat elemzi, köztük a kitöltési mezőben végzett mozgást, ezeket az adatokat küldi el. A tömeges mozgásokról az adatokat titkosítva küldi az adatközpontjába, amelyből egy adatsor – a felhasználók e-mail címe – azonban laikusok által nem, de szakemberek számára visszafejthető volt*."[80]

Az adatvédelem kapcsán nem kerülhetjük meg a felhőszolgáltatások kérdését. Többféle felhőalapú szolgáltatást különböztethetünk meg, de közös pontként azonosíthatjuk, hogy a szolgáltatásokat nem egy dedikált hardveren keresztül, hanem a szolgáltató eszközein keresztül érhetjük el. A felhőszolgáltatásokat megkülönböztetjük szolgáltatás, platform és infrastruktúra alapján. A felhőszolgáltatás előnyei közé sorolhatjuk, hogy helyfüggetlenek, magas rendelkezésre állást biztosítanak, méretezhetőek, és egyúttal védelmet is nyújthatnak a bennük tárolt fájljaink számára (például a zsarolóvírusokkal szemben). Ezzel szemben nem lehetünk 100%-osan biztosak abban, hogy a felhőben tárolt adatainkhoz kik férnek hozzá, és azzal mihez kezdenek. A Google Drive üzembe állításakor tartalmazta a végfelhasználói licencszerződés (EULA), hogy a Drive-ban tárolt adatok a Google tulajdonába kerülnek, és szabadon felhasználhatja azokat. Az egyes EULA-k akár több száz oldal terjedelműek is lehetnek, az átlag felhasználó gyakran az okos mobil eszközre optimalizált alkalmazások esetében sem olvassa végig az engedélykérelmeket, nemhogy a több száz oldal jogi szöveget. Az említett Google Drive EULA esetében is adatvédelmi jogászok szúrták ki, hogy a feltöltött file-ok szerzői jogát a Google magáénak vindikálta volna. Végül a tiltakozás hatására kikerült ez a pont az EULA-ból, ez azonban nem jelenti azt, hogy a felhőben tárolt file-okhoz mások ne férhetnének hozzá. Az Edward Snowden iratokból tudjuk, az amerikai Nemzetbiztonsági Ügynökség (NSA) a nagy technológiai vállalatok teljes adatbázisától hozzáfért 2007-től folyamatosan. Márpedig a közösségi hálózatok, e-mail fiókjaink is felhőként funkcionálnak, hiszen képeket töltünk fel, file-okat küldünk át egymásnak stb. Problémát jelenthetnek a különböző munkahelyi e-mail rendszerek, ugyanis ha azokat nem optimalizálják megfelelő módon, használatuk nem praktikus, előfordulhat, hogy a munkavállalók privát magánfiókjára továbbítják a munkahelyi e-mail fiókjukban megkapott dokumentumokat. Ezzel a kérdéssel a szervezeteknek az informatikai szabályzatban kell foglalkozniuk, illetve arra kell törekedniük, hogy a szervezet által használt e-mail rendszer felhasználóbarát legyen. A munkahelyi e-mail fiókban átküldött dokumentumok gyakran tartalmazhatnak bizalmas információkat, így azok magánfiókra történő továbbítása komoly kockázatot jelent. A tiltás ellenére azonban előfordulhat, hogy a munkavállalók átküldik saját maguknak az egyes dokumentumokat, mert például utazás, várakozás, értekezlet közben dolgoznának az okos mobil eszközükön a dokumentumon, azonban a munkahelyi e-mail kliens ezt nem támogatja megfelelően, ellenben számos privát e-mail szolgáltatóval – ez utóbbira jó példát jelentenek a Google vagy a Microsoft szolgáltatásai. Az Európai Parlament vizsgálatából tudjuk, hogy az NSA az Echelon globális megfigyelőrendszer segítségével gyűjtött

[79] Javaslat az Európai Parlament és a Tanács Rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), Brüsszel, 2017.1.10., COM(2017) 10 final 2017/0003(COD)

[80] A Nemzeti Konzultáció honlapján a Yandex.Metrica analitikai szolgáltatás igénybevételével összefüggésben indított vizsgálatáról. In: NAIH, 2017. július 27. https://naih.hu/files/Adatved_jelentes_naih-2017-2088-20-V.pdf (2018. 11. 03.)

információkat az amerikai kormányzat üzletkötéseinek támogatásaira is felhasználta. Az EULA-k esetében gyakori trend az is, hogy a szolgáltatók gyakran módosítják tartalmukat, amelyekről a felhasználók sokszor csak egy felugró ablak által értesülnek. Vélelmezhetően, ha a felhasználó ezt korábban sem olvasta el, a változásokat sem fogja. Márpedig egy-egy ilyen felhasználási feltétel a felhasználók adatainak teljes átértelmezésével is együtt járhat.

4. A közösségi hálózatok hivatali használatának bevezetését célzó stratégiák

4.1. A közösségi média hivatali használatának felmérése a lehetséges kockázatok szempontjából

A közösségi médiából származó veszélyek felmérésére egy átfogó kockázatelemzést kell készíteni. Ehhez használhatók saját, vagy a Nemzeti Elektronikus Információbiztonsági Hatóság által javasolt módszertanok, de azok kiválasztását mindenképp hozzá kell igazítani a szervezet célkitűzéseihez és lehetőségeihez. A legfőbb cél egy jól használható kockázati modell felállítása, ami képes azonosítani az egyes kockázati tényezőket, továbbá segítségével felmérhetők azok lehetséges hatásai. A közösségi média folyamatos fejlődése miatt fontos továbbá, hogy olyan módszertan kerüljön kiválasztásra, ami képes a változások lekövetésére, így a szervezet reagálni tud az aktuálisan fellépő újabb és újabb veszélyekre. Ahhoz, hogy fel tudjuk mérni a lehetséges kockázatokat elsőként fel kell mérnünk, hogy a védendő vagyonelemek közül melyek azok, amiket érinthetik a közösségi hálózatok irányából származó fenyegetések.

Először érdemes megvizsgálni, hogy a közösségi média hivatali használata milyen jellegű információkat érinthet. Ehhez első lépésként célszerű a különböző adatokat típusuk szerint elkülöníteni. Az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény részletesen ír a különböző adattípusokról:

- *„személyes adat: személyes adat: az érintettre vonatkozó bármely információ;*
- *különleges adat: a személyes adatok különleges kategóriáiba tartozó minden adat, azaz a faji vagy etnikai származásra, politikai véleményre, vallási vagy világnézeti meggyőződésre vagy szakszervezeti tagságra utaló személyes adatok, valamint a genetikai adatok, a természetes személyek egyedi azonosítását célzó biometrikus adatok, az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok;*
- *bűnügyi személyes adat: a büntetőeljárás során vagy azt megelőzően a bűncselekménnyel vagy a büntetőeljárással összefüggésben, a büntetőeljárás lefolytatására, illetve a bűncselekmények felderítésére jogosult szerveknél, továbbá a büntetés-végrehajtás szervezeténél keletkezett, az érintettel kapcsolatba hozható, valamint a büntetett előéletre vonatkozó személyes adat;*
- *közérdekű adat: az állami vagy helyi önkormányzati feladatot, valamint jogszabályban meghatározott egyéb közfeladatot ellátó szerv vagy személy kezelésében lévő és tevékenységére vonatkozó vagy közfeladatának ellátásával összefüggésben keletkezett, a személyes adat fogalma alá nem eső, bármilyen módon vagy formában rögzített információ vagy ismeret, függetlenül kezelésének módjától, önálló vagy gyűjteményes jellegétől, így különösen a hatáskörre, illetékességre, szervezeti felépítésre, szakmai tevékenységre, annak eredményességére is kiterjedő értékelésére, a birtokolt adatfajtákra és a működést szabályozó jogszabályokra, valamint a gazdálkodásra, a megkötött szerződésekre vonatkozó adat;*
- *közérdekből nyilvános adat: a közérdekű adat fogalma alá nem tartozó minden olyan adat, amelynek nyilvánosságra hozatalát, megismerhetőségét vagy hozzáférhetővé tételét törvény közérdekből elrendeli.”*

A 2009. évi CLV. törvény a minősített adat védelméről [144] 3. §-a meghatározza továbbá a nemzeti minősített adat fogalmát. Ez alapján:[81]

- *„nemzeti minősített adat: a minősítéssel védhető közérdekek körébe tartozó, a minősítési jelölést az e törvényben, valamint az e törvény felhatalmazása alapján kiadott jogszabályokban meghatározott formai követelményeknek megfelelően tartalmazó olyan adat, amelyről - a megjelenési formájától függetlenül - a minősítő a minősítési eljárás során megállapította, hogy az érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele a minősítéssel védhető közérdekek közül bármelyiket közvetlenül sérti vagy veszélyezteti (a továbbiakban együtt: károsítja), és tartalmára tekintettel annak nyilvánosságát és megismerhetőségét a minősítés keretében korlátozza.*"

A közösségi média használata során ugyan fennállhat a veszélye minősített adatok kiszivárgásának, de ennek kockázati szintje igen alacsonynak tekinthető. A problémát a közösségi hálózatok által kezelt és gyűjtött nagy mennyiségű személyes és adott esetben különleges adathoz való illetéktelen hozzáférés és felhasználás jelentheti. Az ilyen jellegű adatok a munkavállalókra és a szervezetekre egyaránt vonatkozhatnak, megszerzésük során a támadók különböző social engineering technikákat és OSINT-módszereket használhatnak. A megszerzett információkkal később változatos módon hasznosíthatók, megzsarolhatók vagy kompromittálhatók az egyes munkavállalók, ellopható az adott munkavállaló identitása, továbbá lejáratő kampányok indulhatnak a szervezet ellen, mely rontja lakossági megítélését, és társadalmi elégedetlenséget szülhet.

A szervezet számára ezért fontos, hogy az egyes munkavállalók biztonságos és körültekintő módon használják a közösségi hálózatokat, ügyeljenek az esetleges támadási kísérletekre, és észlelve minél előbb jelentsék azokat. Ezért az általános irányelveken túl elengedhetetlen a munkavállalók információbiztonsági tudatosságának fejlesztésével is foglalkozni. A folyamatos képzésekkel elérhető, hogy az állomány tagjai tudatosabban használják az egyes online szolgáltatásokat, erősebb jelszavakat és két faktoros autentikációt használjanak, kevesebb magánjellegű tartalmat osszanak meg, illetve ellenállóbá váljanak az esetlegesen social engineering támadásokkal szemben.

A különleges és személyes adatok esetleges kiszivárgásának megelőzésére érdemes továbbá felállítani olyan új szabályzókat, amelyek a közösségi média használatra vonatkoznak. Az ilyen jellegű adminisztratív kontrollok szabályozhatják a munkavállalók közösségi média jelenlétét, összhangban a közalkalmazottak (Kjt.[82]), köztisztviselők (Kttv.[83]), katonák (Hjt.[84]), valamint a rendvédelmi állomány (Hszt.[85]) jogállásáról szóló eddigi jogszabályokkal, törvényekkel és utasításokkal. Ezek egy része kitér a munka és szolgálati időn kívüli magatartásra – több esetben külön kiemelve a *„a szolgálati rendet és fegyelmet sértő internetes bejegyzések"* kérdését,[86] ám ezek egyrészt nehezen betarthatók, másrészt a fentebb említett kockázatok miatt szükség lenne a közösségi média használatára vonatkozó konkrét szabályzatok megalkotására.

Ezek létrehozása során érdemes kiemelt figyelmet szentelni az információbiztonsági tudatosítás erősítésére, a szervezeten kívüli közösségi média használat korlátozására, melynek keretében meg kell

[81] 2009. évi CLV. törvény a minősített adat védelméről, https://net.jogtar.hu/jogszabaly?docid=A0900155.TV
[82] 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról, https://net.jogtar.hu/jogszabaly?docid=99200033.TV
[83] 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről, https://net.jogtar.hu/jogszabaly?docid=A1100199.TV
[84] 2012. évi CCV. törvény a honvédek jogállásáról, https://net.jogtar.hu/jogszabaly?docid=A1200205.TV
[85] 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról, https://net.jogtar.hu/jogszabaly?docid=A1500042.TV
[86] A 72/2011. (VI. 30.) HM utasítás 15. § (1) d) pontjában a Hjt-n felül konkretizálja a személyi állomány online bejegyzésekre vonatkozó jogait. Bővebben: 72/2011. (VI. 30.) HM utasítás a Honvédelmi Minisztérium és a Magyar Honvédség külső kommunikációjának rendjéről, http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2011/10.pdf

valósítani a különböző beosztások külön kockázati profilokba történő besorolását. A minősített adatokhoz hozzáférő munkavállalókat külön kockázati tényezőként érdemes kezelni, és velük szemben szigorúbb szabályokat kell alkalmazni. Ennek oka a közösségi médiában folytatott információgyűjtésre és profilozáshoz vezethető vissza.

Erre az OSINT-módszereken túl számos más hatásos technika létezik. Az adott felhasználó privát üzeneteinek és egyéb tevékenységeinek különböző kémprogramok segítségével történő megfigyelésével más országok nemzetbiztonsági szolgálatai, terroristák, hackerek, kiberbűnözők vagy hacktivisták is hozzáférhetnek a magasabb hozzáférési szinttel rendelkező munkavállalók személyes adataihoz, mellyel később megzsarolhatják őket, és akár a szervezetre vonatkozó kényes információkat nyerhetnek ki. Összességében fontos megjegyezni, hogy az ilyen szabályok és kontrollok betartatása számos nehézségbe ütközhet, mivel a közösségi oldalakra történő regisztráció nem tiltható meg, az ott folyó tevékenység pedig csak korlátozott mértékben ellenőrizhető. Emellett nem szabad megfeledkezni arról sem, hogy a közösségi oldalakra történő regisztráció nem igényel valós identitást, az egyes munkavállaló által létrehozott rejtett vagy álprofilok ellenőrzése szinte megoldhatatlan feladat.

A közösségi médiát változatos módon, gyakran saját eszközökön keresztül lehet elérni, melyek különböző kockázati tényezőket jelentenek. Ezért a közösségi hálózatokon megjelenő információkon túl célszerű a fizikai vagyonelemekre vonatkozó leltárral és nyilvántartással folytatni a lehetséges kockázatok felmérését. A közösségi hálózatok ugyanis bármilyen okos – mobil – eszközről elérhetők, s ha nem szabályozzuk ezek használatát, a szervezet fokozottan ki van téve a közösségi hálózatok eléréséből származó kockázatoknak. Mindezt tovább fokozza a saját eszközök bevitelére vonatkozó – és napjainkban egyre nagyobb népszerűsége szert tevő – BYOD-politika (Bring Your Own Device) bevezetése.

Ha a szervezet kényelmi vagy költségvetési okokól él ezzel a lehetőséggel, mindenképp számolnia kell azzal, hogy a munkavállalók hozzáférhetnek a közösségi hálózatokhoz, melynek számos biztonsági fenyegetése lehet. Számolni kell vele, hogy okos eszközökön futó – közösségi média – alkalmazások számos – többek között geolokációs – adatokhoz[87] férhetnek hozzá, amelyek megszerzésével a támadók kritikus információk birtokába juthatnak. Emellett további kockázati tényezőt jelent, hogy az okos eszközök szoftveres és egyéb[88] sérülékenységeit kihasználva számos módon feltörhetők, melyen keresztül kritikus információkhoz lehet hozzájutni. Ennek értelmében a szabályozásnak érintenie kell az eszközökön található alkalmazások hálózati hozzáférésének korlátozását, valamint meg kell valósítani az általuk generált hálózati forgalom fokozott ellenőrzését.

[87] Bizonyos közösségi szolgáltatások rögzítik a bejelentkezett felhasználók eszközeinek geolokációs és egyéb információit, amelyeket a támadók esetlegesen megszerezhetnek, és számos módon felhasználhatnak. Bővebben lásd: Marcus, Fiona: *Facebook Messenger May be Sending out More than Just Your Message*. Secure Thoughts, 2018.
https://securethoughts.com/facebook-messenger-may-sending-just-message/

[88] Ilyennek számíthatnak többek között az okos eszközök által használt 4G LTE protokoll sérülékenységeit kihasználó támadások. Ezekről bővebben lásd: Hussain, Syed Rafiul et al.: *LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE, 2018.*
http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_02A-3_Hussain_paper.pdf

Fenyegetések		
Fenyegetési kategória	**Fenyegetés**	**Fenyegetés leírása**
Technikai és eszközalapú fenyegetések	Sérülékenységek kihasználása	Szoftveres sérülékenységek kihasználása, melyek lehetővé teszik az eszközök feltörését és az érzékeny adatokhoz való illetéktelen hozzáférést.
A szervezet megítélését érintő fenyegetések	A szervezetet érintő hamis vagy rosszindulatú információk közzététele	A szervezetet lejárató információk nyilvánosságra hozása a közösségi hálózatokon. Ezek gyakran valamilyen szervezett dezinformációs vagy propagandahadjárat részeként kerülnek végrehajtásra.
	A szervezet közösségi média oldalainak eltérítése	A támadók valamilyen módszert felhasználva illetéktelen hozzáférést szereznek a szervezet közösségi média profiljaihoz, ahol olyan információkat tehetnek közzé, amelyek rombolják a társadalmi megítélést. Emellett a szervezet megítélését rombolhatják az álcsoportok nevében közzétett félrevezető információk, amelyek a gyanútlan felhasználókat megtéveszthetik, és pánikot kelthetnek.
A munkavállalókat érintő fenyegetések	Social engineering támadások	A közösségi médián keresztül a támadók könnyen kapcsolatba tudnak lépni a munkavállalóval, s hiszékenységét kihasználva különböző támadások valósíthatók meg. Ezek segítségével illetéktelen hozzáférést szereznek a munkavállalók közösségi média profiljaihoz, ahol érzékeny információkhoz férhetnek hozzá. Kiemelt figyelmet kell fordítani a különböző online levelezőkliensekre, melyek gyakran össze vannak kötve a közösségi média profilokkal.
	OSINT-alapú információgyűjtés	A szervezetre vonatkozó információk összegyűjtése az egyre bővülő OSINT módszerekkel. A közösségi média jól használható a munkavállalók kilétének megállapítására és a rájuk, valamint a szervezetre vonatkozó információk összegyűjtésére.
	A szervezetet érintő információk szándékos kiszivárogtatása	A munkavállaló által hozzáférhető érzékeny belső információk tudatos kiszivárogtatása a közösségi médiában, ami rombolhatja a szervezet jó hírnevét és társadalmi megítélését.
A műveleti biztonságot érintő fenyegetések	Bejegyzések, képek és videók engedély nélküli közzététele a közösségi médiában	Az állomány tagjai előzetes engedély nélkül tesznek közzé információkat egy művelet végrehajtása során, mellyel veszélyeztetik a műveleti biztonságot.
	Geolokációs adatok nyomon követése	A bekapcsolt eszközökön futó közösségi média alkalmazások által gyűjtött geolokációs adatok nyomon követése. Mindez jelentősen kihathat a műveleti biztonságra.

1. táblázat: A közösségi média fenyegetettségei (saját szerkesztés)

A vagyonelemek fizikai nyilvántartása mellett fontos továbbá az eszközök teljes körű felmérése, amely számba veszi a rajtuk tárolt információkat, alkalmazásokat – beleértve az operációs rendszert – és

technikai paramétereket, amelyek külön-külön kockázati tényezőként jelenhetnek meg. Ennek értelmében elengedhetetlen a megfelelő stratégia és szabályozási környezet kialakítása, ugyanis az okos eszközök és közösségi hálózatok teljes kitiltására vonatkozó szervezeti politika kialakítása nehezen valósítható meg és kontraproduktív.

4.2. A közösségi média hivatali használatából származó fenyegetések

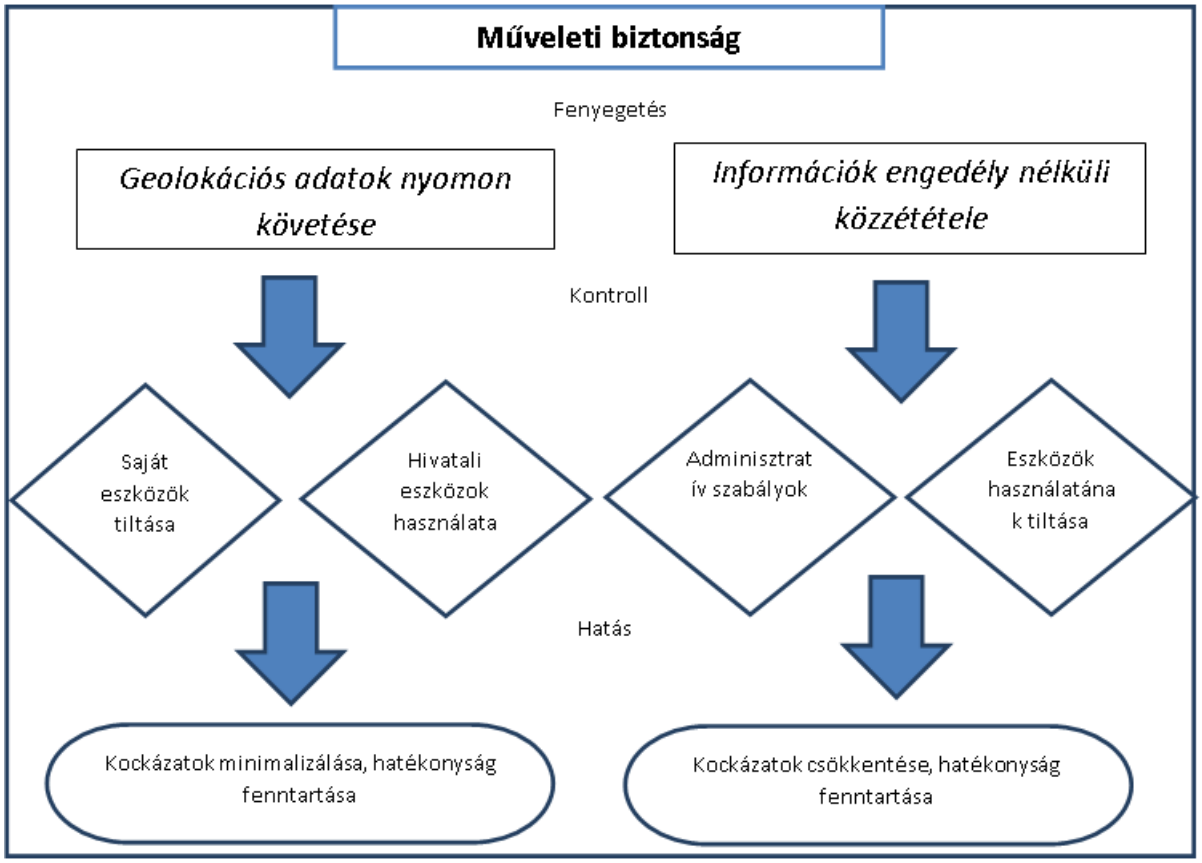
4.2.1. Lehetséges fenyegetések a közösségi médiából

A közösségi hálózatok használatából származó lehetséges fenyegetések felmérése elengedhetetlen a hatékony kontrollok kialakítása szempontjából, ezért az alábbi táblázatban összegyűjtöttünk néhány példát. Ezeket különböző kategóriák szerint csoportosítottuk. Az első kategóriába tartozó fenyegetések magukat az eszközöket érintik, melyek a közösségi hálózatok elérésére szolgálnak. A következő fenyegetési kategória az adott szervezet társadalmi megítélését romboló, szándékos tevékenységeket foglalja össze, végül a harmadik tartalmazza a munkavállalókat célzó – vagy a felőlük érkező – kockázatokat. Az alábbi felsorolás koránt sem teljes körű, csak a közösségi hálózatok kapcsán felmerülő kockázati tényezők illusztrálására szolgál:

A táblázat alapján érdemes az egyes fenyegetési kategóriákat külön megvizsgálni, melyből láthatóvá válik, hogy a közösségi hálózatok használatának milyen további veszélyei lehetnek egy hivatal számára. Ehhez a műveleti biztonságot és a szervezet megítélését érintő fenyegetéseket vizsgáljuk meg részletesebben.

4.2.2. Közösségi média és műveleti biztonság

A rend- és honvédelmi szervezetek feladatrendszerébe tartozó tevékenységek – egy helyszín vagy rendezvény biztosítása, rabok átszállítása, kulcsfontosságú vezetők védelme stb. – végrehajtása során mérlegelni kell a műveleti biztonság kérdését. Az okos eszközök és a közösségi hálózatok használata a műveleti biztonság szempontjából jelentős kockázati tényezőnek számít, ezért célszerű olyan szabályozást kialakítani, amely a műveleti területről teljesen kitiltja a saját eszközöket – helyettük használhatók a biztonsági szempontból ellenőrzött, beállított és megfelelően karban tartott belső eszközök. A közösségi média használatot érintő szabályozásnak ezért a folyamatokra és tevékenységekre is ki kell terjednie, így olyan kontrollok alakíthatók ki, melyek segítségével megvalósítható a kockázati tényezőket és veszélyeket számításba vevő védelem. (Lásd 5. számú ábra) A bevezetett kontrolloknak tehát egyaránt kell tartalmazniuk az eszközöket érintő logikai védelmet és az eszközök használatát érintő adminisztratív szabályozást. Ezek együttes alkalmazásával megelőzhetők a közelmúlt konfliktusaiban látott negatív példák, és egyaránt lehet védeni a személyi állomány, valamint az adott művelet biztonságát.



5. ábra: A műveleti biztonságot érintő kockázatok kezelése (saját szerkesztés)

4.2.3. A szervezet jó hírnevének védelme és az információk kiszivárgásának megakadályozása

A közösségi média szervezeti szintű használatának számos előnye lehet, segítségével olyan kommunikációs csatornák építhetők ki a lakosság felé, melyek javítják a szervezet megítélését, elősegítik a hatékony kommunikációt, ami egy krízis esetén nagyon hasznosnak bizonyulhat. A megfelelő kommunikációs csatornák ugyanis segíthetnek a félrevezető és hamis információkkal szembeni fellépésben, mérsékelve az ártó szándékkal terjesztett dezinformációk által keltett társadalmi feszültség és pánik hatásait. Fontos továbbá, hogy a munkavállalók közösségi média tevékenységeit szabályozza a szervezet, de ennek kapcsán figyelembe kell venni az adott munkavállaló beosztását, továbbá a kontrollokat összhangba kell hozni a Nemzeti Elektronikus Információbiztonsági Hatóság javaslataival, valamint a hatályos jogszabályokkal és belső szabályozókkal. Emellett külön figyelmet kell fordítani a közösségi média használatot szabályozó kontrollok kikényszeríthetőségének nehézségeire, részben ezért is érdemes kerülni a teljes tiltásra vonatkozó szabályokat. Olyan holisztikus szemléletmódra van szükség, mely a kormányzati szervek és a piaci szereplők aktív együttműködésére és információcseréjére épít. A megfelelő stratégia kialakításához és a szervezett lejárató kampányok elhárításához az internetes szolgáltatások (Facebook, Google) és a média bevonása is kulcsfontosságú.[89]

[89] Erre a közelmúltból számos példa akad, a kormányzati és civil szervezetek, kutatóközpontok, valamint a technológiai szektor jelentős képviselői is összefogtak annak érdekében, hogy felderítsék és kiszűrjék a – a nemzetközi terrorszervezetektől vagy állami szereplőktől származó – álhíreket, propagandaanyagokat és az egyéb félrevezető, káros információkat. Bővebben lásd: Newman, Nick: *Overview and Key Findings of the 2017 Report.* Digital News Report, 2017. http://www.digitalnewsreport.org/survey/2017/overview-key-findings-2017/

Minderre azért is szükség van, mert az információs és lélektani műveletek eszközrendszere mára jelentős mértékben kibővült, melynek révén a közvélemény egyre nagyobb része vált az külső állami manipulációk áldozatává.[90] A több milliárd felhasználóval rendelkező Facebook vagy a Twitter már a befolyásolási műveletek legfőbb terepévé vált. További fontos körülményt jelent, hogy a műveletek során anonim módon célba juttatott üzenetek és információk csak komoly nehézségek árán szűrhetők ki. A közösségi média manipulálására – és ezen keresztül a közvélemény befolyásolására – az utóbbi években számtalan technika született, elég, ha csak az államilag támogatott, szervezett trollhadseregek megjelenésére gondolunk.[91] Az ilyen eszközök együttes alkalmazásával a korábbiakban elérhetetlen tömegekhez lehet valós időben és költséghatékony módon eljuttatni a megjeleníteni kívánt – és gyakran egymásnak ellentmondó – narratívá(ka)t, melyek közvetlenül az emberek gondolkodását veszik célba.

Ezek fényében nem meglepő, hogy napjainkban a különböző online közösségi felületek a konfliktusok szerves részévé váltak, a globális információs térben rejlő lehetőségek felismeréséből ugyanis egy olyan új, „kognitív harctér" jött létre,[92] ahol a szemben álló felek kiterjedt műveleteket folytatnak a közvélemény megnyerése és befolyásolása céljából.[93] Ezek növekvő jelentőségét többek között jelzi, hogy a Pentagon Fejlett Védelmi Kutatási Projektek Ügynöksége (Defense Advanced Research Projects Agency – DARPA) az utóbbi években külön kutatási projektet indított (Social Media in Strategic Communication – SMISC) az olyan új eszközök kifejlesztésére, melyek segítségével ellensúlyozhatóvá válhatnak a közösségi térben terjedő propaganda és dezinformációs tevékenységek.[94]

Mindez az állami szervezetek szempontjából is kulcsfontosságú jelentőséggel bír. Ha szervezett propaganda-hadjárat indul az adott ország ellen, az szinte minden esetben érinti a különböző állami szervezeteket, a támadók megpróbálják lejáratni és elhiteltelleníteni azokat, s ezt kihasználva igyekeznek társadalmi feszültségeket és pánikot generálni. Ezért fontos, hogy a lakosság felé kiépüljenek a megfelelő kommunikációs csatornák, melyek kapcsán a közösségi felületek egyre fontosabbá váltak. Számos nemzetközi példát láthatunk arra, hogy egyes fejlett államokban az állami szervek hogyan próbálják meg aktívan kihasználni a közösségi média által nyújtott lehetőségeket, elég, ha csak a brit 77. dandár létrehozására gondolunk. A fenti megállapítások figyelembevételével az alábbi ábrán egy szervezetet érintő lejáratő kampány fenyegetésére tehető esetleges kontrollokat láthatjuk. A lehetséges lépések itt is két elemből tevődnek össze: bizonyos fokig célszerű a munkavállalók közösségi médiában folytatott tevékenységeinek korlátozására építeni, amit ki kell egészíteni egy aktív jelenlét kiépítésével a hatékony stratégiai kommunikáció megvalósítása érdekében:

---

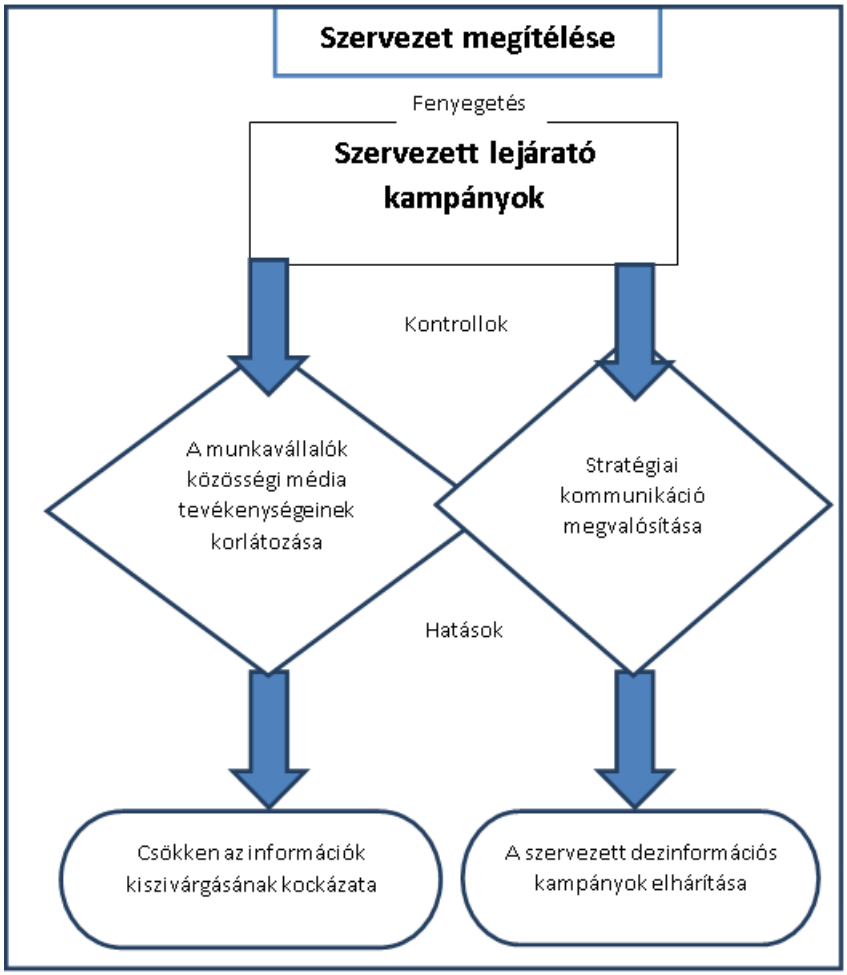
[90] Bővebben lásd: Bányász Péter: *A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében*. Szakmai Szemle 1. sz. 2016.

[91] A provokációt folytató internetes trollokat ma már szervezett formában is alkalmazzák a közösségi médiában annak érdekében, hogy a cikkek alatti kommenteket és az aktuális eseményekről online fórumokban folyó beszélgetéseket az adott kormányzat érdekei szerint manipulálják és megzavarják. Az utóbbi időszakban – online persona management service néven – olyan automatizált szoftvereket is kifejlesztettek, melyek segítségével egy operátor egyszerre több felhasználói fiókot tud szimultán kezelni, biztosítva a vélemények gyors és hatékony befolyásolását. A témáról részletesebben lásd:
Benedictus, Leo: *Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges*. The Guardian, 2016. https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian; Paganini, Pierluigi: *PsyOps and Socialbots.* Infosec Institute, 2013. https://resources.infosecinstitute.com/psyops-and-socialbots/

[92] Ennek ellensúlyozása érdekében az utóbbi években felértékelődött a stratégiai kommunikáció jelentősége, melynek keretében olyan különleges rendeltetésű alakulatokat hoztak létre, mint a brit 77. dandár. Bővebben lásd: *Army sets up new brigade 'for information age'.* BBC, 2015. https://www.bbc.com/news/uk-31070114

[93] Ennek ellensúlyozása érdekében az utóbbi években felértékelődött a stratégiai kommunikáció jelentősége, melynek keretében olyan különleges rendeltetésű alakulatokat hoztak létre, mint a brit 77. dandár. Bővebben lásd: *Army sets up new brigade 'for information age'.* BBC, 2015.

[94] A projekt honlapja az alábbi linken található: http://www.darpa.mil/program/social-media-in-strategic-communication



6. ábra: A szervezet megítélését érintő kockázatok kezelése (saját szerkesztés)

4.3. A közösségi média lehetséges hivatali használatát célzó stratégia szempontjai

A közösségi hálózatokat érintő kockázatok és fenyegetések felmérését követően hivatali használatuk bevezetése előtt célszerű olyan átfogó szabályozást kialakítani, amely tartalmazza az úgynevezett legjobb gyakorlatokat. Ehhez jó alapot nyújthat az Egyesült Államok hadserege által kiadott „*Közösségi média kézikönyv*”.[95] A Kézikönyv nem csupán az műveleti és információbiztonság kapcsán fogalmaz meg az ajánlásokat, de iránymutatást nyújt a közösségi média kríziskommunikációban való felhasználására. A Kézikönyvet alapul véve az alábbi területeken érdemes konkrét szabályozást alkotni a rend- és honvédelmi szervezetek számára:

4.3.1. Az állomány közösségi médiában folytatott tevékenységeinek szabályozása

A szabályozásnak mindenekelőtt korlátoznia kell az állományba tartozás tényének nyilvános közzétételét. Ennek megalkotása során azonban érdemes a minősített információkhoz való hozzáférés függvényében kialakított kockázati profilok esetén más-más követelményt megfogalmazni.

A cél olyan szemléletmód kialakítása, amely tudatosítja a hivatásos állomány tagjaiban, hogy a közösségi térben nem csupán önmagunkat, de a szervezetünket is reprezentálják. Ebből következően magánemberként is olyan közösségi médiajelenlétet kell folytatniuk, amely sem önmagunkra, sem a

[95] *The United States Army Social Media Handbook.* Online and Social Media Division Office of the Chief of Public Affairs, Pentagon, Washington, DC, 2016. április
http://8tharmy.korea.army.mil/site/assets/doc/support/army_social_media_handbook.pdf

szervezetünkre nem hoz szégyent. Kiemelten fontos a kommunikáció stílusa, a megosztott tartalmak jellege, amely egyrészt befolyásolhatja a megítélést, másrészt megkönnyíti egy harmadik fél számára az információgyűjtést és profilozást. Ez utóbbi kapcsán külön figyelmet kell fordítani az okos eszközökön futó alkalmazásokra. Ezek ugyanis rengeteg információt gyűjtenek működésük során, melynek révén olyan információk kerülhetnek illetéktelen kezekbe – helyadatok, ismerősök nevei stb. –, amelyek később felhasználhatók egy támadás során. Erősen javasolt a geolokációs helymeghatározás, Wi-Fi és Bluetooth csatlakozás kikapcsolása, hiszen ezek alapján számos adat összegyűjthető egy adott személyről.

Fontos továbbá az állomány információbiztonsági tudatosságának erősítése és a social engineering típusú támadásokra történő felkészítése. A közösségi média számos lehetőséget biztosít a csalóknak, akik információkat próbálnak szerezni vagy pénzt kicsalni gyanútlan áldozataikból. A támadók a személyes adatok megszerzését követően kiadhatják magukat kollégának vagy távoli ismerősnek, megpróbálva az adott felhasználó bizalmába férkőzni. Emellett akár a családtagokat is felhasználhatják a támadások végrehajtásához, így az ilyen jellegű próbálkozások észlelése során kiemelten fontos, hogy az adott munkavállaló gyorsan jelentse azt az érintett hatóságnál. Az ilyen próbálkozások – főként, ha azok a kiemelt beosztásban lévő tiszteket és köztisztviselőket érintik – egy nagyobb támadás előkészítését is jelenthetik.

4.3.2. A szervezet megítélése és a stratégiai kommunikáció

A szervezeti kommunikáció és a lakosság felé történő kommunikációs csatorna kiépítése szempontjából elengedhetetlen a professzionális közösségi média jelenlétet kiépítése. Ez rendkívül fontos a szervezet megítélésének javítása, a toborzás, valamint a társadalmi támogatottság szempontjából. Emellett a közösségi média felületein terjedő félrevezető és hamis információk ellensúlyozásához elengedhetetlen a megbízható, pontos és hiteles híreken és információkon alapuló szervezeti kommunikáció, melyben a közösségi média kiemelt szerepet játszik.

A médiajelenlét erősítése és a kommunikációs stratégia kidolgozása során fokozottan figyelni kell a közösségi médián keresztül megosztott tartalmak – különösen a kép- és videóanyagok – esetén az információ- és műveleti biztonság követelményeire. A képek ugyanis geolokációs adatokat is tartalmaznak, továbbá a figyelmetlenül megosztott képek felfedhetik a különleges beosztásban szolgáló állomány tagjainak kilétét. Ha a szervezet nem fordít kellő figyelmet a közösségi médiában való aktív jelenlétre, jószándékú amatőrök vagy csalók kihasználhatják a helyzetet, ami komoly kockázatot jelenthet. A rendőrség szóra történő rákeresésre például „Rendőrségi Sajtó” néven jelenít meg egy profilt, ami arra utal, hogy a Rendőrség kommunikációjának hivatalos csatornája, holott nem oldal, hanem személyes profil, a tartalmat csak akkor láthatjuk, ha ismerősnek jelöltük. Az alacsony adat- és információbiztonsági tudatosságú felhasználók nem feltétlenül veszik észre a különbséget, és hivatalos oldalként tekinthetnek rá. Nem nehéz belátni, hogy egy ilyen profilt használhatnak dezinformáció küldésére, pánikhelyzet kialakítására. A hivatalos profiloknak óriási szerep jut a kríziskommunikációban is, egy rendkívüli esemény bekövetkezése esetén elengedhetetlen, hogy a közösségi oldalakat felhasználjuk.

Aktív közösségi média jelenlét		
SWOT	**Pozitív oldal**	**Negatív oldal**
Belső tényezők	**Erősségek** • Az információk nyilvánosságra hozatalának ellenőrzött formája • Egységes arculat • Közvetlen és nyílt kommunikációs csatorna a társadalom felé	**Gyengeségek** • Az információbiztonsági tudatosság alacsony szintje • A közösségi média használatát érintő megfelelő kontrollok hiánya
Külső tényezők	**Lehetőségek** • A társadalmi megítélés javítása • A félrevezető információk és álhírek hatásainak csökkentése • A társadalmi feszültség és pánik megelőzése	**Fenyegetések** • Kritikus információk kiszivárgása • A műveleti biztonság sérülése • A szervezet társadalmi megítélésének romlása

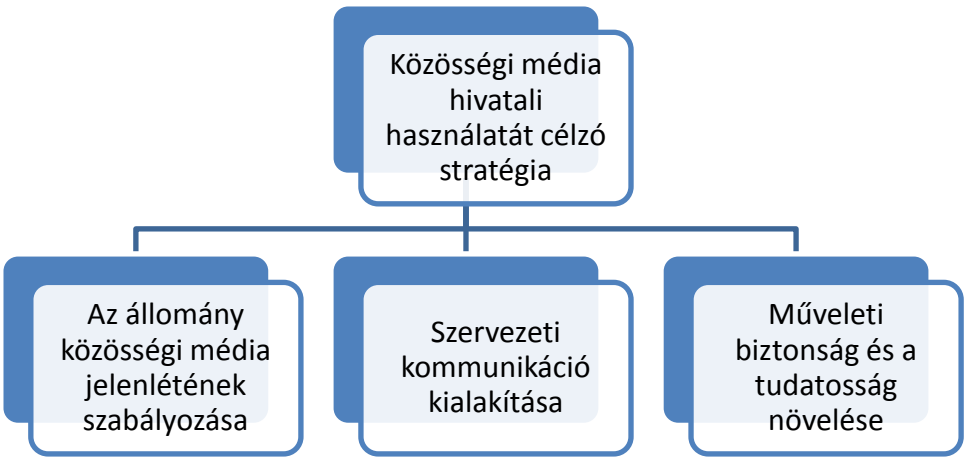
2. táblázat: SWOT analízis az aktív közösségi médiajelenlét kapcsán (saját szerkesztés)

4.3.3. Műveleti biztonság

Célszerű olyan közösségi oldalakat is létrehozni, amelyek segítik a biztonságtudatosság növelését. Ezzel kapcsolatban az amerikai fegyveres erők követendő példával szolgálnak: mind a szárazföldi erők,[96] mind a haditengerészet[97] kapcsán találunk olyan oldalakat, amelyek a műveleti biztonsággal kapcsolatos tudatosságnövelő kampányt folytatnak. A két oldal nemcsak az aktuális eseményekre hívja fel rendszeresen a figyelmet – zsarolóvírus kampányok, sebezhetőségek stb. –, hanem sokszor könnyed formában, mémekkel, videók segítségével tudatosítja az oldalak követőiben a műveleti biztonság fontosságát, és fogalmazza meg a követendő jó gyakorlatokat. A megfelelő szintű műveleti és információbiztonság elérése nem csupán a jogi szabályozáson múlik, legalább olyan fontos, hogy az állományt rendszeresen képezzék ezzel kapcsolatban, aminek egyik aspektusát a közösségi médiában végzett kampányokkal lehet elérni. Mindez jó kiegészítést jelenthet a korábban már kialakított továbbképzési rendszer számára.

A fentiek értelmében a közösségi média hivatali használatát célzó stratégiának mindenképp foglalkoznia kell az állomány közösségi média jelenlétének szabályozásával, a szervezeti kommunikáció megteremtésével és az aktív közösségi média jelenlét kiépítésével, illetve az információbiztonsági tudatosság növelésével, és a műveleti biztonság kérdéseivel.

[96] Army Operations Security (OPSEC), https://www.facebook.com/usarmyopsec/
[97] Naval Operations Security (OPSEC), https://www.facebook.com/NavalOPSEC/



7. ábra: A közösségi média hivatali használatát célzó stratégia főbb területei (saját szerkesztés)

5. Összegzés

A közösségi média használatának komplex kockázatait kevesen ismerik. Az egyes oldalak népszerűségéből következően a támadók előszeretettel használják a közösségi oldalakat támadásaik előkészítése vagy támadások kivitelezése érdekében. A védekezést nehezíti a közösségi oldalak állandó innovációja, amelynek hatására a támadók mindig új és új eljárásokat alkalmaznak. A védekezés egyik legfontosabb elemét az adat- és információbiztonsági tudatosság növelésére vonatkozó oktatások jelentik, amelyek során az állandóan változó fenyegetéseket is ismertetni szükséges. A közösségi oldalak jelentette kockázatok szervezetenként és a szervezeten belül munkakörönként eltérőek, így a képzések ezekre specifikus szervezését igénylik. A közösségi oldalak használata napjainkban komoly kihívás elé állítja a szervezeteket. Bár számos biztonsági kockázatot jelentenek, megfelelő biztonságtudatos használattal a kockázatok minimalizálhatók. A közösségi oldalak számos olyan lehetőséget biztosítanak az egyes szervezeteknek, amelyek segítségével nagyban növelhetik jogszabályban meghatározott feladataik hatékony ellátását. A szervezet és az ott kezeltek adatok függvényében azonban nem csupán célszerű a közösségi oldalak használatának korlátozása, hanem elengedhetetlen. Jelenleg az egyik legjelentősebb kihívást az jelenti, hogy a közösségi média hivatali használatára vonatkozóan nem áll rendelkezésre egységes módszertan. Az információbiztonság szempontjából elengedhetetlen, hogy a különböző szervezetek kitekintsenek saját falaikon túl, és számításba vegyék a munkavállalóik által napi rendszerességgel használt közösségi szolgáltatásokat. Az elmúlt évek azt bizonyítják, hogy a támadók szinte minden esetben felhasználják a közösségi médiából származó információkat egy-egy támadás végrehajtásához. A megváltozott helyzethez történő alkalmazkodás megköveteli, hogy az információbiztonsági tudatosság kialakítására és ezzel együtt a közösségi hálózatok használatát érintő esetleges korlátozásokra konkrét szabályzatok szülessenek a közeljövőben. A szabályozás és a korlátozás mellett a közösségi média használatának számos előnye van egy hivatal szempontjából. Ennek érdekében ki kell dolgozni a közösségi média használatát érintő stratégiákat, melyek kiemelt szerepet kaphatnak a szervezet külső kommunikációjában és az ellenséges propaganda és dezinformációs hadjáratok elhárításában.

Felhasznált irodalom

- 1992. évi XXXIII. törvény a közalkalmazottak jogállásáról https://net.jogtar.hu/jogszabaly?docid=99200033.TV
- 2011. évi CXCIX. törvény a közszolgálati tisztviselőkről https://net.jogtar.hu/jogszabaly?docid=A1100199.TV
- 2012. évi I. törvény a munka törvénykönyvéről https://net.jogtar.hu/jogszabaly?docid=A1200001.TV
- 2012. évi CCV. törvény a honvédek jogállásáról https://net.jogtar.hu/jogszabaly?docid=A1200205.TV
- 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról
- 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról, https://net.jogtar.hu/jogszabaly?docid=A1500042.TV
- 72/2011. (VI. 30.) HM utasítás a Honvédelmi Minisztérium és a Magyar Honvédség külső kommunikációjának rendjéről http://www.kozlonyok.hu/kozlonyok/Kozlonyok/13/PDF/2011/10.pdf
- AJP-3.10 Allied Joint Doctrine for Information Operation, 2009. https://info.publicintelligence.net/NATO-IO.pdf
- *Army sets up new brigade 'for information age'.* BBC, 2015. https://www.bbc.com/news/uk-31070114 (2018. 10. 24.)
- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet) (EGT vonatkozású szöveg)
- Az országos rendőrfőkapitány 11/2015. (VII. 10.) ORFK utasítása a hivatásos állomány tagjának az internetes felületen a hivatásos állományba tartozására vonatkozó adatok nyilvánosságra hozatalának szabályozásáról http://frsz.hu/sites/default/files/docs/11_2015_orfk_ut_internetes_feluleten_a_hiv_allomanyba_tartozasra_vonatkozo_adatok_nyilvanossagra_hozatalanak_szabaloyzasarol.pdf
- A Nemzeti Adatvédelmi és Információszabadság Hatóság tájékoztatója a munkahelyi adatkezelések alapvető követelményeiről, 2016. november 15. https://naih.hu/files/2016_11_15_Tajekoztato_munkahelyi_adatkezelesek.pdf
- A Nemzeti Konzultáció honlapján a Yandex.Metrica analitikai szolgáltatás igénybevételével összefüggésben indított vizsgálatáról. NAIH, 2017. július 27. https://naih.hu/files/Adatved_jelentes_naih-2017-2088-20-V.pdf (2018. 11. 03.)
- Ált/57, Információs műveletek doktrína, MH DOFT kód: MD 3.10 (1), 2014. augusztus 5. pp. 1–15.
- Bányász Péter: *A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében.* Szakmai Szemle, 1. sz. 2016.
- Bányász Péter: *A közösségi média térnyerése a védelmi szférában.* PhD értekezés tervezet, Nemzeti Közszolgálati Egyetem, Budapest, 2018.
- Bányász Péter: *Az „okos" mobileszközök jelentette biztonsági kihívások.* In: Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2016. Nemzeti Közszolgálati Egyetem, Budapest, 2016.

- Benedictus Leo: *Invasion of the troll armies: from Russian Trump supporters to Turkish state stooges.* The Guardian, 2016. https://www.theguardian.com/media/2016/nov/06/troll-armies-social-media-trump-russian (2018. 10. 30.)
- Béres János: *A hírszerzés feladatrendszere.* In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest, 2014, p. 363.
- Blumler J. G. – Katz, E.: *The Uses of Mass Communications: Current Perspectives on Gratifications Research.* Vol. 3, Sage, Beverly Hills, CA., 1974.
- Bourdieu, Pierre: *Gazdasági tőke, kulturális tőke, társadalmi tőke.* In: Angelusz Róbert (szerk.): A társadalmi rétegződés komponense, Budapest, Új Mandátum Könyvkiadó, 1999, pp. 156–177.
- Caldwell, Tracey: *Hacktivism goes hardcore.* Network Security, Volume 2015, Issue 5, May 2015, pp. 12–17., http://dx.doi.org/10.1016/S1353-4858(15)30039-8
- Davis, F. D.: *Perceived usefulness, perceived ease of use, and user acceptance of information technology.* MIS Quarterly, 13(3), 1989, p. 319–339.
- European Commission Directorate-General for Justice and Consumer: Guide to the EU-U.S. Privacy Shield, 2016. https://ec.europa.eu/info/sites/info/files/2016-08-01-ps-citizens-guide_en.pd_.pdf
- Europol The Internet Organised Crime Threat Assesment 2016. Europol, Hága, 2017. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (2018. 10. 28.)
- Europol The Internet Organised Crime Threat Assesment 2017. Europol, Hága, 2018. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017 (2018. 10. 28.)
- Guo. et al.: *DPI & DFI: A Malicious Behavior Detection Method Combining Deep Packet Inspection and Deep Flow Inspection.* Procedia Engineering, Volume 174, 2017, pp. 1309–1314. https://doi.org/10.1016/j.proeng.2017.01.276
- Heaven, Douglas: *The internet knows you all too well.* New Scientist, Volume 237, Issue 3168, March 2018, pp. 42–43. https://doi.org/10.1016/S0262-4079(18)30444-5
- Hern, Alex: *Fitness tracking app Strava gives away location of secret US army bases.* The Guardian, 2018. január 28. https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases (2018. 10. 27.)
- Herrick, Drew: *The social side of 'cyber power'? Social media and cyber operations.* In: International Conference on Cyber Conflict, CYCON, Cyber Power. Pissanidis, N. – Rõigas, H. – Veenendaal, M. (Eds.) NATO CCD COE Publications, Tallin, 2016.
- Hussain, Syed Rafiul et al.: LTEInspector: A Systematic Approach for Adversarial Testing of 4G LTE, 2018. http://wp.internetsociety.org/ndss/wp-content/uploads/sites/25/2018/02/ndss2018_02A-3_Hussain_paper.pdf (2018. 10. 30.)
- Javaslat Az Európai Parlament és a Tanács irányelve a digitális egységes piacon a szerzői jogról, Brüsszel, 2016.9.14. COM (2016) 593 final 2016/0280(COD) https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52016PC0593&from=HU
- Javaslat az Európai Parlament és a Tanács Rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), Brüsszel, 2017.1.10., COM(2017) 10 final 2017/0003(COD)

- Kaplan, Andreas – Haenlein, Michael: *Users of the world, unite! The challenges and opportunities of Social Media.* Business Horizons, 2010.
- Kenedli Tamás: *A nyílt forrású információszerzés.* In: A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Budapest, 2014, pp. 169–178.
- Kiss Attila: *A biztonsági események és az adatvédelmi incidensek kezelésére vonatkozó előírások hazánk és az EU jogában.* In: Incidensmenedzsment – Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2017. Dialóg Campus Kiadó, Budapest, 2017.
- Krasznay Csaba: *A polgárok védelme egy kiberkonfliktusban.* Hadmérnök, VII/4. szám, 2012, pp. 142–151.
- Kovács László – Krasznay Csaba: *A digital Mohács: a cyber attack scenario against Hungary.* Nemzet És Biztonság: Biztonságpolitikai Szemle III:(Spec. Issue Winter), 2010, pp. 49–59.
- Kovács László – Krasznay Csaba: *Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint.* Nemzet és Biztonság, 2017/1., pp. 3–16.
- Lévay Gábor: *OSINT (Open Source Intelligence) – Nyílt információs hírszerzés.* Egyetemi jegyzet. ZMNE,Budapest, 2006, p. 6.
- Luiijf, Eric: *Definitions of Cyber Terrorism.* In: Cyber Crime and Cyber Terrorism Investigator's Handbook, 2014, pp. 11–17.
- Marcus, Fiona: Facebook Messenger May be Sending out More than Just Your Message, Secure Thoughts, 2018. https://securethoughts.com/facebook-messenger-may-sending-just-message/ (2018. 10. 26.)
- Merkovity Norbert: *Bevezetés a hagyományos és új politikai kommunikáció elméletébe.* A Pólay Elemér Alapítvány Könyvtára, Hódmezővásárhely, 2012.
- Mitnick, Kevin D.: *A legendás hacker – A megtévesztés művészete.* Perfact-Pro, Budapest, 2003.
- Moskowitz, Sanford L.: *The Global Cybercrime Industry.* In: Cybercrime and Business, Strategies for Global Corporate Security, 2017, pp. 3–22.
- Munk Veronika: *Sztárság, elméletben.* Médiakutató 2009 tavasz, http://www.mediakutato.hu/cikk/2009_01_tavasz/01_sztarsag_elmeletben
- Newman, Nick: *Overview and Key Findings of the 2017 Report.* Digital News Report, 2017. http://www.digitalnewsreport.org/survey/2017/overview-key-findings-2017/ (2018. 10. 22.)
- Official U.S. Army Social Media https://www.army.mil/socialmedia/directory/
- Omand et al.: *Introducing social media intelligence (SOCMINT).* Intelligence & National Security 27(6) December 2012. https://doi.org/10.1080/02684527.2012.716965
- Open Letter in Light of the Competitiveness Council on 30 November 2017. http://copybuzz.com/wp-content/uploads/2017/11/Open-Letter-COMPET-Council-30-Nov-online.pdf
- Ngai, E. W. T. – Moon, K. K. – Lam, S. S. – Chin, E. S. K. – Tao, S. S. C.: *Social media models, technologies, and applications.* Industrial Management & Data Systems, 115(5), 2015, 769–802. https://doi:10.1108/imds-03-2015-0075
- Paganini, Pierluigi: *PsyOps and Socialbots.* Infosec Institute, 2013. https://resources.infosecinstitute.com/psyops-and-socialbots/ (2018. 10. 22.)
- Pléh Csaba et al.: *Pszichológiai lexikon.* Akadémiai Kiadó, Budapest, 2008. Személyiségtípusok p. 276.
- Szabó András: *Preventív hálózatvédelmi rendszerek alkalmazási lehetőségei a támadások detektálására, valamint a módszerek elemzésére.* Hadmérnök, VI. évfolyam, 4. szám, 2011, pp. 239–249.

- Sz. N.: *Az álhírek ellen hozott törvényeket Franciaország.* SG, 2018. november 22. https://sg.hu/cikkek/it-tech/134010/az-alhirek-ellen-hozott-torvenyeket-franciaorszag (2018. 11. 28.)
- Tajfel, Henry: *Social identity and intergroup behaviour.* Social Science Information, Vol. 13, No. 2, 1974, pp. 65–93.
- Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004 http://www.fbi.gov/congress/congress04/lourdeau022404.htm (2018. 10. 20.)
- *The United States Army Social Media Handbook.* Online and Social Media Division Office of the Chief of Public Affairs, Pentagon, Washington, DC, 2016. április http://8tharmy.korea.army.mil/site/assets/doc/support/army_social_media_handbook.pdf (2018. 10. 30.)
- *Ukrainian bloggers use social media to track Russian soldiers fighting in east.* Stopfake.org, 2015 https://www.stopfake.org/en/ukrainian-bloggers-use-social-media-to-track-russian-soldiers-fighting-in-east/ (2018. 10. 28.)
- Venkatesh, V. – Davis, F.: *Theoritical extension of the technology acceptance model: four longitudinal field of studies.* Management Science, 46(2), 2000, p. 186–204. https://doi.org/10.1287/mnsc.46.2.186.11926

Ajánlott irodalom

- Akhgar, Babak et al.: *Open Source Intelligence Investigation: From Strategy to Implementation.* Springer, 2017.
- Antonello et al.: *Deep packet inspection tools and techniques in commodity platforms: Challenges and trends.* Journal of Network and Computer Applications, Volume 35, Issue 6, November 2012, pp. 1863–1878. http://doi.org/10.1016/j.jnca.2012.07.010
- Bányász Péter: *Social engineering és közösségi média.* Nemzetbiztonsági Szemle 5: (1) (2018), pp. 59–77.
- Bányász Péter: *A közösségi média mint az információs hadszíntér speciális tartománya.* Hadmérnök, 12:(2) (2017), pp. 108–121.
- Bányász Péter: *A közösségi média mint a nyílt forrású információszerzés fontos eleme.* Nemzetbiztonsági Szemle, 2015/2, pp. 21–36.
- Bányász Péter: *A közösségi média szerepe a katasztrófaelhárításban a Sandy-hurrikán példáján keresztül.* In: Horváth Attila (szerk.): Fejezetek a kritikus infrastruktúra védelemből: Kiemelten a közlekedési alrendszer. Magyar Hadtudományi Társaság, Budapest, 2013, pp. 281–292.
- Cavoukian, Ann: *Embed Privacy by Design, or Risk Losing Privacy Forever.* Berkeley Center for Law & Technology, 2016. www.law.berkeley.edu/wp-content/uploads/2016/03/Ann-Cavoukian.pdf
- Esposti et al.: *Aligning security and privacy: The case of deep packet inspection.* In: Čas, J. – Bellanova, R. – Burgess, J. P. – Friedewald, M. – Peissl, W. (eds.): Surveillance, Privacy and Security: Citizens' Perspectives. Routledge, London, 2017, pp. 71–90.
- Greenwald, Glen: *A Snowden-ügy.* HVG Kiadó Zrt., Budapest, 2014.
- Prensky, Marc: *Digital Natives, Digital Immigrants, On the Horizon.* MCB University Press, Vol. 9, Iss: 5, No. 5, 2001. október, p. 1–6. http://doi.org/10.1108/10748120110424816

Ábrajegyzék

Táblázatjegyzék

Rövidítésjegyzék

Rövidítés	Magyar nyelvű megnevezés	Idegen nyelvű megnevezés
CIMIC	civil-katonai együttműködés	Civil-Military Co-operation
COMINT	kommunikációs felderítés	Communications Intelligence
CNO	számítógép-hálózati műveletek	Computer Network Operations, továbbiakban CNO
DLP	adatszivárgás-megelőzés	Data Loss Prevention
DPI	mély csomagvizsgálat	Deep Packet Inspection
EULA	végfelhasználói licencszerződés	End User License Agreement
GDPR	Általános Adatvédelmi Rendelet	General Data Protection Regulation
Hjt.	2012. évi CCV. törvény a honvédek jogállásáról	
Hszt.	2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról	
IKT	infokommunikációs technológiák	Information and Communications Technology
INFOSEC	információbiztonság	Information Security
IoT	Dolgok Internete	Internet of Things
Kjt.	1992. évi XXXIII. törvény a közalkalmazottak jogállásáról	
KLE	kulcsfontosságú vezetőkkel kapcsolatos tevékenység	Key Leader Engagement, továbbiakban
Kttv.	2011. évi CXCIX. törvény a közszolgálati tisztviselőkről	
Mt.	2012. évi I. törvény a munka törvénykönyvéről	
NAIH	Nemzeti Adatvédelmi és Információszabadság Hivatal	
NSA	Nemzetbiztonsági Ügynökség	National Security Agency
OSINT	nyílt forrású információgyűjtés	Open Source Intelligence

OPSEC	műveleti biztonság	Operations Security
PET	privátszférát erősítő technológiák	Privacy Enhancing Technologies
PPP	megjelenés, viselkedés, arculat	Presence, Posture and Profile
SIGINT	elektronikai felderítés	Signals Intelligence
SOCMINT	közösségi médiában folytatott hírszerzés	Social Media Intelligence
UGC	felhasználó által előállított tartalom	User Generated Content
VPN	virtuális magánhálózat	Virtual Private Network