10.17625/NKE.2019.018

PhD értekezés

Bányász Péter

- 2018 -

NEMZETI KÖZSZOLGÁLATI EGYETEM
KATONAI MŰSZAKI DOKTORI ISKOLA

Bányász Péter

A közösségi média lehetőségei és kihívásai a védelmi szférában

Doktori (PhD) Értekezés

Témavezetők:

Dr. Király László CSc
c. egyetemi docens

Prof. Dr. Munk Sándor ny. ezredes DSc
egyetemi tanár

BUDAPEST, 2018.

Tartalom

BEVEZETÉS

A téma aktualitása

Az elmúlt évtizedekben több paradigmaváltás zajlott le a hadtudományban. Az egyik ilyen, kutatási témám szempontjából releváns paradigmaváltás az informatikai eszközök elterjedése nem csupán a mindennapi életben, de a katonai alkalmazás tekintetében is jelentősnek nevezhető. Az internet elterjedésével és az infokommunikációs technológiák (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.

A közösségi médiát számos pozitív dologra használhatjuk, kapcsolattartásra a szeretteinkkel, barátainkkal, növelni az üzletünk bevételét, fontos társadalmi-politikai ügyek népszerűsítésére, de akár életek mentésére is, amennyiben egy katasztrófa esemény során kríziskommunikációra, segítségkérésre használjuk. De ahogy minden éremnek két oldala van, úgy a pozitívumok mellett rengeteg kihívást, kockázatot, fenyegetést is jelenthetnek egyben, amelyek sok esetben kapcsolódnak a honvédelmi, rendvédelmi szervezetek és nemzetbiztonsági szolgálatok működéséhez. A védelmi szféra esetében szintén kettősséget figyelhetünk meg, hiszen míg egyik oldalról a biztonságot veszélyezteti, addig másik oldalról olyan lehetőségeket biztosít a szervezetek számára, amelyekkel a törvényben meghatározott feladataikat láthatják el. Fontos azonban megjegyezni, hogy a védelmi szférának nincs a magyar tudományos szakirodalomban egységesen értelmezett definíciója. Az egyes szerzők a fogalom alá különböző alterületeket rendelnek, mint honvédelem, rendvédelem, nemzetbiztonság, védelmi igazgatás, katasztrófavédelem, védelmi ipar stb. [1] [2] [3] Értekezésemben én alapvetően a honvédelmi, rendvédelmi, nemzetbiztonsági területeket vizsgálom a közösségi média védelmi szférával kapcsolatos kutatásaival összefüggésben. E három terület mellett azonban fontosnak érzem a politikai alrendszer vizsgálatát is, hiszen a katonai, nemzetbiztonsági műveletek célját a politkai döntéshozók határozzák meg, illetve idegen államok politikai döntéshozatalának befolyásolására törekednek.

Az emberi történelem során a technikai fejlődés sok esetben a katonai igények kielégítését szolgálta. Számos találmány haditechnikai fejlesztésből szivárgott át a civil szférába, ahogy ezt az internet példája is igazolja. Az infokommunikációs technológiák innovációja azonban változást eredményezett ebben a trendben, és gyakran a civil élet fejlesztései kerülnek át a védelmi szférába. Erre szolgál példaként a közösségi média, amely alapvetően az interperszonális interakciók ápolására jött létre, azonban megannyi területet meghódított és számtalan felhasználási lehetőséget teremtett.

Az alkalmazás módja nagyban függ a közösségi médiát használó egyén, szervezet céljaitól. A napjainkra már a közel-keleti befolyását egyre nagyobb mértékben elvesztő[1] Iszlám Állam (továbbiakban IÁ) nevű terrorszervezetnél hangsúlyosabban talán egy példa sem bizonyítja, milyen diszfunkciók övezhetik ezeknek az oldalaknak a használatát. Bár a terrorszervezetek viszonylag korán felismerték a propaganda interneten való terjesztésének erejét, ilyen újszerűen, professzionális jelleggel egy szervezet sem kezelte a közösségi oldalakat. Az IÁ elleni nemzetközi koalíció 2014 szeptemberében jött létre. Az IÁ elleni fellépés megítélésem szerint jól példázza, egyetlen tevékenység (a terrorcsoport felszámolása) milyen komplex feladatkör ellátását követeli meg, ebből következően a közösségi média mennyi különböző feladat támogatására alkalmas. Ez alapján a következő tevékenységek sikeres végrehajtását segítheti elő:

- lélektani műveletek (propaganda-ellenpropaganda),
- hírszerzés,
- trendelemzés,
- kommunikáció megfigyelése,
- kapcsolati háló feltérképezése,
- a szervezetbe történő beépülés,
- vezetők megfigyelése, hiteltelenítse,
- terroristák beszervezése,
- oktatás,
- támogatók, szakemberek toborzása,
- politikai döntéshozatal befolyásolása.

[1] Bár az Iszlám Kalifátus 2018-ra jelentősen visszaszorult, azonban Afrikában az Iszlám Állam növelte befolyását.

A felsoroltak nem csupán a terrorizmus elleni harcban alkalmazhatóak, a védelmi szféra különböző területein jelentkező feladatok sikeres ellátását is biztosíthatják.

A megfogalmazott tevékenységek azonban gyakran a másik oldalon megmutatkozó hiányosságok kihasználásából erednek. Elég a nyílt forrású információszerzésre (Open Source Intelligence, továbbiakban OSINT) gondolnunk, hiszen minél kevésbé érzékeny egy felhasználó az adat- és információbiztonságra, annál több információt gyűjthetünk róla. Ha figyelembe vesszük, hogy átlagosan mennyi időt töltünk internetezéssel, ezen belül közösségi oldalak használatával, egy biztonsági szempontból érzéketlen felhasználóról rengeteg értékes információt szerezhetünk, ami többek között egyrészt irányt szabhat titkos információgyűjtés végzésére, de emellett többek között social engineering támadás előkészítésére is alkalmas.

Kutatási témám inter- és multidiszciplináris jellegű, speciális ötvözete számos szakterületnek, amelyek a korszerű hadviselés részét képezik. A Nemzeti Közszolgálati Egyetem (továbbiakban NKE) három doktori iskolájában[2] hirdettek meg olyan kutatási területeket[3] és témákat, amelyekkel kapcsolatba hozható a saját kutatásom, illetve az egyetem több karán oktatnak az alap-, mester- és PhD képzések során olyan tárgyakat, amelyekbe illeszkedik, de ezen felül az Elektronikus információbiztonsági vezető szakirányú továbbképzési szakon is relevánsnak tekinthető. Több doktori kutatást folytatnak a korszerű hírszerzés, az információbiztonság, a kiberhadviselés, terrorizmus, lakosságfelkészítés, létfontosságú rendszerelemek védelme, a civil-katonai együttműködés (Civil-Military Co-operation, továbbiakban CIMIC), lélektani műveletek (Psychological Operations, továbbiakban PSYOPS) témákban, amelyek kapcsán a közösségi média szerepet játszhat. Fontos megemlíteni a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosító számú, ”A jó kormányzást megalapozó közszolgálat-fejlesztés” című kiemelt projekt keretében működő Kiberbiztonsági Kiemelt Kutatóműhelyt, amelynek hat kutatói pilléréből az egyik a „Közösségi média kockázatai” témában folytat kutatásokat. Ezek a kutatások megjelennek továbbá a 2017-ben a Nemzeti Közszolgálati Egyetemen megalakult Kiberbiztonsági Akadémia profiljában is. Dolgozatomban többek között az itt nevesített területek esetében vizsgálom a kapcsolódási pontokat, illetve dolgozok ki eljárásokat, amelyek felhasználhatóak az adott szakterületnél. A doktoranduszokon, doktorjelölteken kívül számos, a témakörökben jártas, nagy tapasztalattal rendelkező szakember foglalkozik e területekkel.

[2] Hadtudományi Doktori Iskola, Katonai Műszaki Doktori Iskola, Rendészettudományi Doktori Iskola.
[3] Védelmi elektronika, informatika, kommunikáció, katasztrófavédelem, védelemgazdaság, védelmi igazgatás, biztonsági tanulmányok, védelem társadalomtudományi kérdései, hadtudomány általános elmélete, nemzetbiztonság és rendvédelem, közmenedzsment.

Kutatómunkám során jelentős szűkítésre kényszerültem a témámat illetően. Kutatásaimat eredetileg védelemgazdasági aspektusból közelítettem meg, de időközben a közösségi oldalak folyamatos átalakulása, illetve új információk láttak napvilágot (pl. az Edwards Snowden által kirobbantott megfigyelési ügy), amelyek átalakították, kibővítették a kutatás irányát, ugyanis megítélésem szerint e szempontok figyelmen kívül hagyása nem eredményezné a téma komplex feldolgozását. Ez azonban azzal járt, hogy számos kapcsolódó területet nem dolgozhattam fel, többek között pl. a kiberbűnözés, ellátási láncok biztonsága, élelmiszerbiztonság stb.

Témaválasztásom indokául az a felismerés szolgált, hogy a közösségi oldalak elterjedése új típusú kihívásokat eredményezett, amelyek a védelmi szférában súlyozottan jelentkeznek. Ez a kihívás egyben lehetőség is a különböző feladatok végrehajtását illetően, azonban hazánkban e terület kevésbé kutatott és nem léteznek olyan kidolgozott eljárások, amelyek útmutatóként szolgálhatnak.

A tudományos probléma megfogalmazása

Jelen értekezés tervezet tudományos problémája a fentebb meghatározott **kettősségből ered**: van egy megkerülhetetlen eszköz, amelyből **számos biztonsági fenyegetés** származik, emellett **rengeteg lehetőséget kínál** egy nemzet **védelmében.**

A közösségi média használatból fakadó kockázatot növeli, hogy különböző eszközökön (PC, tablet, okostelefon, okosszemüveg,[4] okos tv, okosóra stb.) enged hozzáférést, amelyek eltérő módon és mértékben sebezhetőek.[5] Ez a fajta átjárhatóság megnehezíti a biztonsági szabályozást, hiszen különböző eszközökre kell kiterjeszteni, amik esetében eltérő lehetőségek vannak a védelemre, illetve a hordozhatóság alkalmat teremt, hogy a munkahelyen esetlegesen letiltott közösségi média használatot saját eszközről kijátssza a munkavállaló. További szempont, a munkavégzés sajátosságaiból fakadóan (elsősorban a szellemi munkát végzők esetében) a szabadidő összemosódik a munkaidővel: nem csak a munkahelyen élünk

[4] A Google által kifejlesztett Project Glass (közismert nevén Google Glass, továbbiakban GG) egy kiterjesztett valóságot megjelenítő, fejre illeszthető kijelző, ami összekapcsolva egy okostelefonnal a szemüveg kijelzőjén jeleníti meg a különböző információkat. Az eszköz rengeteg módon elősegítheti a katonák, rendőrök munkájának hatékony végzését, többek között pl. adatbázisok megjelenítésével, rejtett és bizalmas kommunikáció folytatásával, több lépcsős azonosítás és jogosultság kezelés, oktatás támogatásával stb. Ez által számos biztonsági kockázatot is magában hordoz, nem véletlen, hogy még megjelenése előtt számos helyen tiltották meg az eszköz viselését (kaszinókban, bankokban, kórházakban, gépjárművezetés közben stb.). A GG kockázatairól bővebben lásd: Török Szilárd: Szemüveggel a biztonságért című tanulmányát [4].

[5] Pl. az Apple termékei védettebbek a rosszindulatú programokkal szemben, mint az Android alapú rendszerek.

magánéletet a közösségi oldalak használatával, de otthon is dolgozunk a családi programot háttérbe szorítva.[6] A technológiai innováció, a különböző közösségi oldalak állandó átalakulása újabb nehézséget okoz, hiszen úgy kell valamilyen szabályozót megalkotni, úgy kell biztosítani az információ- és adatbiztonságot, hogy folyamatosan változik a keret.

Sajnálatos módon az **információ- és adatérzékenység** nem csupán az átlag felhasználók esetében **alacsony**, a politikai döntéshozók, a védelmi szférában dolgozók tekintetében is komoly kockázatot jelent a nem megfelelő szintű felhasználói tudatosság. Már pedig, ahol az információs műveletek egyre nagyobb szerephez jutnak a hadviselésben, ott egyre nagyobb jelentősége van, különösen a védelmi szférában az információ- és adatbiztonságnak. Bár a közösségi oldalak használata megkerülhetetlen, ennek ellenére **jogilag gyengén szabályozott terület**. Nem csupán az adatbiztonsággal kapcsolatban hiányos a közösségi médiával kapcsolatos normatív szabályozás, a használatára vonatkozó korlátozások, etikai szabályozás is fejlesztendő terület.

A közösségi oldalakon zajló **folyamatos változás** egyben azt is jelenti, nem csupán a védekezés metódusait kell naprakészen tartani, hanem azokat az eljárásokat is, amelyek egy adott feladat ellátást támogatják, hiszen új lehetőségek keletkezhetnek, illetve korábban alkalmazott módszerek válhatnak feleslegessé. Mindez az **oktatás** tekintetében rendkívül fontos, ami megítélésem szerint **fejlesztendő terület.**

A képességek, amelyeket a közösségi média megfelelő használatával érhetünk el, különböző szervezeti egységeknél jelentkeznek. A honvédelmi, rendvédelmi, nemzetbiztonsági szervezetek esetében nem újdonság sem az egyes hivatásnemek közti, sem az egyes hivatásnemeken belüli rivalizáció, azonban ahogy a terrorizmus elleni harc esetében is megfigyelhető, **meg kell teremteni a szervezetek közti kooperáció kereteit,** ennek hiányában nem érhető el a kívánt eredmény. A célcsoportok és műveletek függvényében az egyes feladatokat más-más szervezeti egységnek kell ellátnia, de egy komplexebb feladatrendszer esetében ez szoros együttműködést követel meg. A toborzás feladatait pl. a Magyar Honvédség Hadkiegészítő és Központi Nyilvántartó Parancsnokság (továbbiakban MH HKNYP) látja el, de a toborzás megítélésem szerint összefügg a honvédség pozitív percepcionálásával, ami szerepet játszik a hadsereg feladatainak ellátásának támogatásában, az MH érdekérvényesítő képességének növelésében is. Minél komplexebb egy feladat, annál több szervezet lesz érintett. Ha figyelembe vesszük a fenti példát a terrorizmus elleni fellépéssel kapcsolatban, nem igényel

[6] Emellett egy tablet arra is lehetőséget biztosít, hogy utazás közben felváltva dolgozzunk és internetezzünk, ami tovább növelheti a sebezhetőségünket azáltal például, hogy nem védett Wi-fi hálózatra csatlakozunk.

különösebb bizonyítást, milyen szervezeti keretek között kell megvalósítani a kooperációt, illetve kidolgozni a támogató feladatok ellátását.

Kutatásaim során **több olyan területet** vizsgáltam, amelyek esetében a végrehajtó **szerveztek tevékenysége nem nyilvános**, így a normatív szabályozást alapul véve (például 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról [5] (továbbiakban Nbtv)), illetve nyílt forrásból fellelhető információkat felhasználva végezhettem munkámat. A politikai döntéshozatal befolyásolása vagy a különböző hírszerzési eljárások hozhatóak fel ezt illusztrálandó. Edward Snowden nyilvánosságra lépése a magyar nemzetbiztonsági szolgálatok ez irányú működésére is ráirányította a közvélemény figyelmét. Bár hazánkban is szivárogtak ki ezzel kapcsolatos információk, mint ahogy pl. a Nemzetbiztonsági Szakszolgálat (továbbiakban NBSZ) előfizetője a Finfisher nevet viselő kémprogramnak, ez mégsem ölt olyan mértéket, mint az Egyesült Államokban.[7] Feltételezéseket vonhatunk le továbbá a szolgálatok képességéről különböző nyilvános adatokból, pl. a közbeszerzési eljárásokból. Erre szolgál példaként a 2015. június 5-én közzétett tájékoztató a közbeszerzési eljárás eredménytelenségéről [6], amelynek tanulsága szerint az NBSZ 5,25 millió Forint értékben kívánt különböző szoftvereket vásárolni, amelyek többek között weboldalak biztonsági réseinek feltérképezésére, felhasználók IP cím alapján történő beazonosítására vagy hálózatra kapcsolt eszközök, pl. webkamerákhoz való hozzáférést biztosít. Emellett azt is látni kell, a téma tudományos feldolgozása **a nemzetközi releváns szakirodalomban még kevésbé kutatott**, de az elmúlt évek trendjei ebben növekedésre utalnak. A kutatások során gyakran doktrínák, stratégiák jelentették a felhasználható irodalmat, amelyek inkább a szakmai, mint a tudományos feldolgozását erősítették a témának.

A 2016-os brit népszavazási kampányban az Európai Uniós tagságról, de különösen az amerikai elnökválasztási kampány során történtek hangsúlyosan hívták fel a figyelmet a közösségi média politikai döntéshozatal befolyásolásában betöltött szerepére. Bár empirikus úton nem mérhető, hogy a közösségi oldalakon terjedő álhírek mekkora hatással voltak a brit kilépés pártiak győzelmében vagy Donald Trump elnökké választására, a közvélekedésben mégis a közösségi oldalak felelőssége volt az irányadó. A közösségi oldalakon végzett tevékenységeknek, megfelelő tervezés mellett **jelentős hatása lehet**, amely nem csak egy adott **állam életében** járhat következményekkel, hanem **globálisan** is.

A fentieket figyelembe véve, úgy ítélem meg, a közösségi média védelmi szférában való térnyerésének vizsgálata indokolja, hogy komplexen közelítsem meg az általa jelentett

[7] Arról nem is beszélve, hogy a kiszivárgott információkat is kellően kritikusan szükséges értékelni.

tudományos problémát. Értekezés tervezetemben ennek megfelelően bemutatom azokat az egymásra épülő kockázatokat és lehetőségeket, amelyek a közösségi média használatából erednek.

Kutatási célkitűzések

Kutatásom célja azoknak a **védelmi szférában jelenlevő kihívásoknak, kockázatoknak, fenyegetéseknek az azonosítása, amelyek a közösségi médiából származnak**, illetve annak vizsgálata, **milyen lehetőséget biztosít a közösségi média a különböző honvédelmi-, rendvédelmi-, nemzetbiztonsági szervezeteknek céljaik megvalósítása érdekében**.

Ebből következően **kutatásom részcéljainak tartom** a fenyegetések azonosítását követően azon **biztonsági eljárások megalkotását**, amely hatására minimalizálhatóvá válhatnak a közösségi médiából származó fenyegetések. Az azonosítás magában kell foglalja **a védelmi szféra különböző ágainak differenciálását**, ugyanis eltérő módon és mértékben jelentkeznek az adott fenyegetések.

Részét képezi továbbá azon **eljárásoknak a feltérképezése**, amelyek segítségével a **különböző szervezetek hatékonyan láthatják el a meghatározott feladataikat**. Ily módon elemzem a közösségi média szerepét a hírszerzésben (OSINT, elektronikai felderítésben, továbbiakban SIGINT, emberi erőforrással folytatott információszerzésben, továbbiakban HUMINT), megvizsgálom, **hogyan alkalmazható az információs műveletek során**, a terrorizmus ellen fellépés kapcsán, beleértve a civil-katonai műveleteket.

Végezetül feladatomnak tekintem annak **meghatározását, milyen formában, milyen szervezeti keretek között integrálható a közösségi média használata a honvédelmi-, rendvédelmi-, nemzetbiztonsági szervezetek rendszerébe**.

Kutatási hipotézisek megfogalmazása

A kutatási téma feldolgozása során az alábbi hipotéziseket fogalmaztam meg:

H1. A közösségi média új multidiszciplináris szakterület

H2. A közösségi média a kibertérnek, mint hadszíntérnek speciális területe.

H3. A közösségi média használat részben szabályozott területe a magyarországi adat- és információbiztonságra vonatkozó jogszabályoknak, aminek a honvédelmi-, rendvédelmi-, nemzetbiztonsági szervezetek esetében különösen fontos szerepe van.

H4. A biztonságtudatossággal kapcsolatos önpercepciót befolyásolja a nem, az iskolai végzettség, a műszaki-humán tudományok iránti érdeklődés, a korábban a témában hallgatott kurzus, illetve az egyes eszközök használatának ideje.
H5. A közösségi média számos lehetőséget nyújt a honvédelmi-, rendvédelmi-, nemzetbiztonsági szervezeteknek törvényben meghatározott feladatainak ellátásában.
H6. A közösségi média biztosította lehetőségek megfelelő ellátása érdekében szükséges egységesen megfogalmazni a használatra vonatkozó szabályokat és azok feladatai közé integrálni a honvédelmi-, rendvédelmi-, nemzetbiztonsági szervezetekbe.

Kutatási módszerek

Kutatásom alapját tudománymetriai vizsgálatok képezik. A közösségi média megjelenését a tudományos gondolkodásban kulcsszó elemzéssel vizsgáltam. Ez a kutatás egyrészt trendelemzéssel párosult, másrészt az egyes publikációk tudományterületi megjelenését hálózatelemzéssel vizsgáltam.

A kutatásaim során kérdőíves felmérést végeztem a Nemzeti Közszolgálati Egyetem hallgatóinak körében. A felmérés az adat- és információbiztonsági tudatosság humán aspektusát vizsgálta a Tudás Képesség Viselkedés modellt alapul véve. A kérdőív feldolgozása során kereszttábla elemzést végeztem.

Az általam kidolgozott eljárás egyrészt a nemzetközi összehasonlítás alapján feltárja a magyarországi adaptálás lehetőségeit, továbbá a gyakorlati élet során felmerült problémák megoldását végzi el.

A kutatási módszerek megválasztásánál közül többfélét alkalmaztam. A kutatás alapvetően elméleti-logikai kutatási módszereket alkalmaz, ezen belül az analízis, szintézis, összehasonlítás, általánosítás, indukció, dedukció, analógia, hipotézis módszereit használom.

A fent megfogalmazottak érdekében összegyűjtöttem a témával foglalkozó releváns nemzetközi és hazai szakirodalmat, elemeztem a védelem és biztonságpolitikai stratégiai követelményeket, esettanulmányokat dolgoztam fel, interjúkat készítettem, valamint feldolgoztam a tanulmányutak, szakmai konferenciák, tapasztalatcserék során szerzett információkat.

I. FEJEZET

A KÖZÖSSÉGI MÉDIA HELYE ÉS SZEREPE A VÉDELMI SZFÉRÁBAN

1.1. A közösségi média fogalma, alkotói

2013 áprilisában a Forbes magazinban játszott el Keith Loell azzal a gondolattal, hogy a közösségi média eredete egészen a 12. századi céhek kialakulásáig vagy Sir Isaac Newtonhoz eredeztethető vissza [7]. Loell abból indult ki, hogy a céhek az adott szakmán belül zárt közösségeket alkottak, amelyekben a tagok tapasztalatot cseréltek, illetve megvitatták az iparáguk szempontjából releváns kérdéseket, miközben a csoporton belüli nagyobb befolyás érdekében versenyeztek. Az 1660-ban alapított Királyi Természettudományos Társaság[8] Newton vezetése alatt megháromszorozta taglétszámát, emellett felpezsdítette a tudományos közélet. Annak érdekében, hogy bekapcsolódjanak a Társaság keretében folytatott tudományos diskurzusba, akár hónapokat is hajlandóak voltak utazni egyes tudósok, hogy ily módon vitassák meg egyes eredményeiket, csiszolják az elméleteket a vita hatására, és közkinccsé tegyék a végeredményt.

A gazdasági fejlődést illetően utólag kiderült, hogy a céhek gátolták az innovációt és a versenyt, mégis őket tekinthetjük a „társadalmi tőke” megalkotóinak, hiszen a szabályok, információk és a legjobb gyakorlat egymás közt történő megosztásával jelentős iparági és politikai befolyást értek el. Királyi Természettudományos Társaság később pedig folyamatosan a legjobb „contentet”, tartalmat állította elő, olyan fórumokat szervezett, ahol az adott témák legelismertebb szakértőit lehetett elérni. A szerző megállapítása szerint mind a céhek, mind a Királyi Természettudományos Társaság üzleti alapú közösségi média platformok voltak, azelőtt, hogy egyáltalán kialakult volna a közösségi média, ez alapján pedig sikereik (illetve kudarcaik) adoptálhatóak a modern közösségi média stratégiákba:

- rendszeres tartalommegosztás,
- fórumot kell biztosítani a vitára, illetve a megosztásra,
- a beszélgetésekben gondolatvezéreknek is részt kell venniük,

[8] A The Royal Society of London for Improving Natural Knowledge a legősibb angol tudományos társaság. A Társaság rövid időn belül meghatározóvá vált világszerte, ami a politikai és vallási kérdések vizsgálatától való szigorú elzárkózásának tudható be. A Társaságról bővebben lásd internetes elérhetőségét [8].

- biztosítani kell a vitákban résztvevőknek a társadalmi elismertségért folytatott versenyt.

Természetesen Loell gondolatkísérlete csalóka, azonban ez is mutatja, a történelem minden szakaszában a társadalmakat erős közösségszervező igény jellemezte. Ezt az igényt az infokommunikációs technológiák elterjedése kiszélesített az idő- és térbeli korlátok leomlásával. Dolgozatomban bizonyítani fogom, azok a jellemzők, amelyek a közösségi média használatával jelentkeznek, nem napjainkban alakultak ki, pusztán új köntösben jelennek meg.

1.1.1 A közösségi média fogalma

A Loell révén megfogalmazottakat azért is helyesnek tartom, mert segítik az általam elfogadásra javasolt közösségi média meghatározást. A közösségi média definiálására számos kísérlet született, amelyeknek döntő többsége a marketing tudományterületéhez kötődik,[9] amely egyúttal magán viseli annak jegyét, hogy elsősorban a marketinghez kapcsolódó fogalmakkal operál. Az Oxford Dictionaries [10] a közösségi médiát weboldalak és alkalmazások összességeként írja le, amelynek során a felhasználók tartalmat készíthetnek és megoszthatnak a közösségi hálózatokon. Ehhez a definícióhoz köthető Andreas Kaplan és Michael Haenlein által megfogalmazottak, mi 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*” [11].

Elfogadva a Kaplan- Haenlein szerzőpáros által megfogalmazottakat, de mégis kiegészítve a meghatározást, a közösségi média alatt olyan internetes oldalak és alkalmazások összességét értem, amelyeknél a szolgáltató csupán a keretet biztosítja, a tartalmat a felhasználók állítják elő. Ebből következik, hogy a közösségi média elsősorban a felhasználók interakciójából alakul ki, amely a többi felhasználó megosztásából, kiegészítéséből akár részben/teljesen új tartalom előállítását jelentheti. Elméletileg ez a tartalom folyamatosan változhat, kiegészülhet, akár új információk hatására bővülhet. Mindez beleilleszthető Loell ismertetett gondolatkísérletébe.

Látszólag nincs számottevő eltérés Kaplan- Haenlein által ajánlott definíció és az általam használtak között, azonban, ha elfogadjuk az általam javasolt formát, akkor nagymértékben kibővül a közösségi média köre. Ez alapján a közösségi médiához sorolom a különböző okostelefonokra írt alkalmazásokat is, hiszen egyrészt ezek is a felhasználók közti

[9] Heidi Cohen, marketing szakértő gyűjtött össze 30 közösségi média fogalmat, amelyről bővebben lásd a szerző internetes oldalát [9].

interakcióra épülnek, másrészt integratív szerepet töltenek be a különböző közösségi eszközök közt. Az integráció legerősebb példája a Google: a kezdetben keresőszolgáltatóként működő cég mára egy személyben integrálja a különböző közösségi eszközöket (blogszolgáltató, fénykép- és videómegosztó, közösségi hálózat, okostelefon platform stb.).

Az integráció okát elsősorban gazdasági szempontok magyarázzák, ugyanis rendkívül nagy és folyamatosan bővülő reklámpiacról beszélhetünk. Ebből következően óriási verseny van a nagy szolgáltatók közt, állandó innovációra kényszerítve a szereplőket. Az a vállalat, amelyik nem képes folyamatosan megújulni, elveszti piacvezető szerepét. A magyar fejlesztésű IWIW története remekül példázza ezt az állítást, képtelen volt felvenni a versenyt globális szinten a megmerevedett struktúrájából következően. Nem véletlen tehát, hogy a nagy cégek az internet szerepét akarják átvenni. A közösségi média modern gazdaságra gyakorolt hatásával a harmadik fejezetben részletesen foglalkozom.

1.1.2. A közösségi média alkotói

A fogalmi meghatározást alapul véve a közösségi média alkotói tehát olyan oldalak, amelyek megfelelnek a tartalom előállítás-megosztás kritériumának. A közösségi oldalak csoportosítására különböző elméletek léteznek, amelyek a felhasználók, alkalmazás típusok függvényében kategorizálják az egyes oldalakat.

Ngai és szerzőtársai például egy olyan konceptuális keretet ajánlanak elfogadásra, amely három egymásra épülő szintet feltételez [12]. Véleményük szerint modelljük adoptálása végül a közösségi médiával kapcsolatos kutatások inter- és multidiszciplináris feldolgozásához vezet.

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

- a magatartáselméleteket (például személyiségjegyek,[10] TAM [11]modell);

[10] Az egyes személyiségjegyek kategóriákba történő sorolásának az oka, hogy ily módon különbséget tudjunk tenni az egyes individiuumok között, megértve ezáltal a viselkedésük mögötti motivációt, illetve interperszonális interakcióikat [13].

[11] 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 [14]. Az eredeti modell megalkotása Davis nevéhez fűződik, ezt azonban továbbfejlesztették. A TAM2 modell a hasznosság mértékét meghatározó tényezőket is figyelembe veszi [15], mint például imázs, szubjektív norma, az output minősége, az eredmény bizonyíthatósága és a munkarelevancia.

- a szociális tanuláselméleteket (például társadalmi tőke,[12] társadalmi identitás[13]);
- a tömegkommunikációs elméleteket (például paraszociális kapcsolatok,[14] használati-juttatási modell [19]).

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

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

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

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

A közösségi oldalak kategorizálásnak egy másik szempontja a felhasználók típusától függ. Ez alapján beszélhetünk személyes és professzionális oldalakról. Sasvári Péter és Urbanovics Anna megállapítása szerint [20] „*lényegi kérdése az, hogy a regisztrált felhasználók mire használják az adott felületet, így pedig aktív szereplőnek tekinti a felhasználót, aki médiafogyasztási viselkedése nyomán alakítja is az egyes szolgáltatásokat*.” Ennek alapját a

[12] 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 struktúrájnak függvénye. A társadalmi tőke elősegítheti az egyén boldogulását, illetve kollektív cselekvések hatására a társadalom prosperálását [16].

[13] A társadalmi identitáls 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 [17].

[14] Munk Veronika megfogalmazása alapján [18], 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*.”

használati-juttatási modell adja, amely a közönség-centrikus megközelítést alkalmazza. A szerzők ez utóbbira a tudományos közösség által megfogalmazott igényt hozzák fel példának, ami olyan közösségi hálózatok létrejöttéhez vezettek, mint például az Academia.edu, a Google Scholar vagy a Researchgate.net. Ezek az oldalak nem csupán az egyes kutatók publikációjának megosztására használhatóak, de vélhetően a tudománymetriai elemzések alternatívájának is betöltik a későbbiekben a szerepét.

A közösségi média megjelenését a 90-es évek közepére, a fórumok polgári életben való megjelenésére datálom, 1994-ben hoztáklétre a Geocities, 1995-ben pedig a Classmates nevű oldalakat. Az alfejezetben ennek megfelelően ismertetem a nagyobb közösségi oldalakat, amelyek Magyarországon is elterjedtek.

Fontos hangsúlyozni, hogy a bemutatásra kerülő oldalak elsősorban Magyarországon, illetve a nyugati kultúrkörben népszerűek, nem foglalkozok az olyan, elsősorban Kínában elterjedt közösségi oldalakkal, mint pl. Sina Weibo, a Qzone és a Tencent. Ennek okául azon egyszerű megállapítás szolgál, hogy bár a különböző kínai közösségi szolgáltatók bár globálisan akár nagyobb oldalletöltést produkálhatnak, mint az itthon használt egyes oldalak, de hazánkban nem bírnak relevanciával.

A felsorolás azonban természetesen így is hiányos, rengeteg olyan oldal ismertetését mellőznöm kellett, amelyek mind globálisan, mind hazánkban népszerűek. Ennek okául az általam vallott közösségi média fogalom szolgál, amely kiterjeszti a közösségi oldalak számát. Az alfejezetben bemutatott oldalak vizsgálatát azon egyszerű oknál fogva végeztem el, hogy az értekezésben érintett műveletek során relevanciával bírnak. Bár mind világszerte, mind Magyarországon hatalmas tábora van számos közösségi oldalnak, mint például a Music.ly, Academia.edu, a 9gag nevű mém[15] gyűjtő oldalnak, a védelmi szféra tekintetében kevésbé releváns az oldal műveletek tervezése esetében, így a hozzá hasonló oldalak ismertetése nem képezik részét az alfejezetnek.

1.1.2.1. Facebook

A Facebook napjaink legnépszerűbb közösségi oldala. A vállalat 2017. évi negyedik negyedéves jelentés alapul véve [23], a napi átlagos felhasználó szám (Daily Active User,

[15] A mém az interneten rövid idő alatt népszerűvé váló vicces (vagy annak szánt) tartalom, ami vírus szerűen terjed az interneten, adott esetben mutálódik, kereszteződik más mémekkel. A mém szó először Richard Dawkins brit etológus, evolúciókutató 1976-os könyvében, Az önző génben jelent meg. Ez alapján a mém egyfajta gondolatvírus, ami emberi agyakat fertőz meg, a kommunikáció útján terjed, és más mémekkel küzd a tovább öröklődésért. Az „erősebb" fennmarad, az online népművészet, a kultúra részévé válik, a „gyengék" a feledés homályába merülnek [21] [22].

továbbiakban DAU) 1,4 milliárd, ami az előző évhez képest 14%-os növekedést jelent. A havi átlagos felhasználó szám (Monthly Active User, továbbiakban MAU) esetében 2,13 milliárd felhasználóról beszélhetünk, az előző évhez képest 14 %-os növekedéssel számolhatunk. Az oldalt 2004-ben alapította Mark Zuckerberg a Harvard Egyetemen, kezdetben csak a hallgatók körében volt elérhető a szolgáltatás, de a Facebook hamar népszerűvé vált a hallgatók körében, amit a fejlesztők előbb a többi egyetem hallgatói előtt is megnyitott, majd tovább lépve bárki, aki betöltötte 13. életévét, regisztrálhatott. Kezdetben közösségi hálózatként üzemelt, a felhasználók ismerősnek jelölhették egymást, egymással szöveges üzenetet válthattak, különböző tartalmakat (videókat, képeket, szövegeket) oszthattak meg egymással, amelyet kommentelhettek. Az oldal népszerűségével folyamatosan új funkciókkal bővült (pl. videóchat), illetve számos egyéb szolgáltatást integrált magába (például Instagram, Paper). A Facebookot 2012-től a tőzsdén is jegyzik.

1.1.2.2. Instagram

Az eredetileg iOS-ra[16] készített Instagram egy képmegosztó szolgáltatás, amely az általa használt filterek, szűrők, effektek hatására rendkívül népszerűvé vált a fiatalok körében. 2010 októberében indult szolgáltatás decemberre elérte az 1 milliós felhasználói számot, a következő közel egy évben ez 15 millióra, 2013-ra 100 millióra bővült. Az oldal fiatalok körében való népszerűsége időben megegyezett a Facebookról történő elszivárgással, amelynek megállítása érdekében a Facebook 1 milliárd dollárért vásárolt fel 2012-ben az Instagramot.

1.1.2.3. Twitter

A 2006-ban alapított Twitter egy közösségi hálózat és mikroblog szolgáltatás, amelyen a felhasználók maximum 140 karakterben állíthatnak elő tartalmat (úgynevezett tweet-eket). Az oldallal szemben indulása után bár sok kritikát fogalmaztak meg, azonban miután az oldal fejlesztői elérhetővé tették a Twitter alkalmazásprogramozási interfészét[17] (továbbiakban API),

[16] Az iOS az Apple operációs rendszere, nevét az iPhone Operation System rövidítésből kapta.
[17] Az API egy program vagy programrendszer azon eljárásainak és használatainak dokumentációja, amelyet más programok szabadon felhasználhatnak. Egy nyilvános API lehetővé teszi, hogy egy programrendszer anélkül használható legyen, hogy ismernék annak belső működését.

rengeteg olyan fejlesztés és mash up[18] jelent meg, amelyek figyelembe vették a felhasználók igényeit. A Twitter mozgósításban betöltött szerepét a 2010-es „Arab-tavasz" eseményei messzemenően igazolták. A tőzsdei bejegyezésre 2013-ban került sor.

1.1.2.4. Google

Amennyiben elfogadjuk az általam javasolt közösségi média meghatározást, úgy a Google is a részét képezi. A Google 1998-ban indult, eredetileg keresőszolgáltatásként, majd az idő során egyre több területen szerzett dominanciát. Az oldal egy kutatási témából nőtt ki, amely szerint a weboldalak között matematikai analízisen alapuló kapcsolat áll fenn, amit felhasználva jobb keresési eredményeket lehet adni- ez az úgynevezett PageRank.[19] E tézis igazolására hozták létre a Google keresőrendszerének alapjait. Az egyszerű kezelhetőség, a releváns találati eredményeknek köszönhetően gyorsan népszerűvé vált. Napjainkra a Google több tucat különböző szolgáltatással, eszközzel bővítette profilját, mint pl. e-mail (Gmail), blog (Blogger), képmegosztó (Picasa), videómegosztó (YouTube), térkép (Maps), műhold (Earth), 3 dimenziós panorámakép térképhez integrálva (Street View), közösségi hálózat (Orkout, Buzz, Google +), fordító program (Translate), naptár (Calendar), csevegő (HangOuts), szövegszerkesztő (Docs), felhő (Drive)okostelefon platform (Android), kiterjesztett virtuális valóság (GG), internetes böngésző (Chrome), laptop (Chrome OS), autonóm közlekedési eszköz (Driveless Car) stb. Mindezeken kívül számos fejlesztés tekintetében úttörőnek számít, a vállalat titkos laborjában többek között a mesterséges intelligencia, a robotika, az agykutatás, az autonóm eszközök területén elismert kutatók dolgoznak. A szolgáltatások nagy részének használata nem követeli meg, hogy regisztráljunk az oldalra, de amennyiben a regisztrálás mellett döntünk, úgy automatikusan tagjai leszünk a Google közösségi hálózatának, a Google+-nak is.

[18] A fogalmat alapvetően a zenevilágban használják egy olyan szerzemény leírására, amely két vagy több zeneszám összeolvasztásából keletkezik. A webes alkalmazások esetében a mash up több szolgáltatás egy alkalmazásban való összedolgozását értjük.

[19] A szabadalmaztatott PageRank a fontosság számszerűsítése, egy olyan algoritmus, amely hiperlinkekkel összekötött dokumentumokhoz számokat rendel azoknak a hiperlink-hálózatban betöltött szerepe alapján. A feltételezés szerint a weboldalak készítői azokra a weblapokra helyeznek el hivatkozást saját oldalukról, amelyeket relevánsnak gondolnak, ami ez alapján egyfajta szavazatot jelent. Minél több hivatkozás mutat egy weboldalra, annál relevánsabbnak tekinthető. Az algoritmus azonban figyelembe vesz sok egyéb szempontot, mint például a hivatkozó oldal relevanciáját. A PageRank azonban manipulálható (pl. ún. „comment spamek" segítségével, amelyek linkek elhelyezését jelenti hozzászólásokban, vendégkönyvekben vagy ún. linkfarmok alkalmazásával, amelyek olyan weboldalak használatát jelenti, amelyeknek egyetlen célja, hogy a kiválasztott oldalra hivatkozzanak), így folyamatosan csiszolják, a pontos számítási modell nem ismert. Egy weboldal esetében rendkívül fontos, milyen módon szerepel a PageRank szerint, ugyanis a keresőben ennek megfelelően érhető el, ez pedig a hirdetések szempontjából releváns.

1.1.2.5. Google+

A 2011-ben útjára indult Google+ a Google újabb kísérlete, hogy betörjön a közösségi hálózatok piacára. A Google piaci fölényéből eredően és az általa üzemeltett szolgáltatások integrálásából elvileg kedvező feltételek mellett kellene közösségi hálózatot üzemeltetnie, az elmúlt évtizedben mégsem tudott tartós sikert elérni ezen a területen. A felvásárlási kísérletei nem egy esetben kudarcba fulladtak (pl. 2003-ban a Friendster, 2009-ben a Twitter mondott nemet), a nagy várakozással elindított oldalak nem váltották be a hozzájuk fűzött reményt. Az Orkout inkább csak Indiában és Brazíliában vált tartósan népszerűvé, a Buzz vagy a Wave fejlesztését végül megszüntették, annak reményében, hogy a Google+-ba integrálják. Azonban az oldal ismét nem felelt meg a várakozásoknak, a magas felhasználói szám annak tudható be, hogy egy Google fiók regisztrálásához automatikusan Google+ profil kapcsolódik.

1.1.2.6. YouTube

A 2005-ben létrehozott YouTube napjaink legnépszerűbb videómegosztó oldala, ami 1,65 milliárd dollárért történő 2006-os felvásárlása óta a Google leányvállalataként működik. Több mint egy milliárd felhasználóval rendelkezik, a napi megtekintések száma több milliárdra tehető, a feltöltött videók felét mobil eszközökről tekintik meg.

1.1.2.6. Wikipédia

A 2000-ben alapított Wikipédia egy többnyelvű, nyílt tartalmú, közösség által szerkesztett web alapú enciklopédia. Világszerte több tíz millió felhasználó szerkeszti, több mint 30 millió szócikket tartalmaz 286 nyelven. A köznyelvben gyakran „Wiki” -ként használják, ez a kifejezés azonban pontatlan, ugyanis több tízezer wiki rendszerű, a Wikipédiától független oldal létezik. A szabadon szerkeszthetőség nem egy esetben pontatlan információközléssel járhat, de nem egy esetben derült ki, szándékos félrevezetéssel írtak meg egy-egy szócikket.[20]

[20] Erre hozható példaként az 1640-41 közt lezajlott portugál-indiai háború, ami 5 évig szerepelt a Wikipédián vagy a kitalált Jurij Gadjukin szovjet filmrendező szócikke, ami 4 évig volt elérhető az oldalon. Ez utóbbi átverés annyira kifinomult volt, hogy a legnagyobb internetes mozi adatbázisban, az IMDB-n is külön szócikket, illetve Facebook rajongói oldalt is készítettek [24].

1.1.2.7. Reddit

A 2006-ban indított Reddit egy közösségi hírmegosztó oldal, ahol a felhasználók úgynevezett alredditeket segítségével állíthatják elő a tartalmat, ami alapvetően hírek, cikkek, képek megosztásával, moderálásával keletkezik.[21] A felhasználók értékelhetik, kommentelhetik a tartalmat.

1.1.2.8. LinkedIn

A 2003-ban indult LinkedIn egy professzionális, üzleti kapcsolatok ápolására és építésére szolgáló közösségi hálózat. Az oldalt 2016-ban a Microsoft Corporation felvásárolta.

1.1.2.9. 4 Chan

A 2003-ban létrehozott 4 Chan egy fórumszolgáltatás, ahol az alapvetően anonim felhasználók különböző tartalmakat osztottak meg egymással. Az oldal relevanciája a hacktivizmusban ragadható meg, az Anonymous hackercsoport[22] az oldal felhasználóiból rekrutálódott.

1.1.2.10. IWIW

A 2002-ben WIW-ként létrehozott magyar közösségi hálózat a világ egyik legelső közösségi hálózatának tekinthető. Megítélésem szerint iskolapéldája a közösségi média és a gazdaság egymásra ható viszonyának. A 2000-es évek közepén az IWIW annyira sikeres volt, hogy nem egy esetben „az IWIW-et köttettek be”, amikor előfizettek valamelyik szolgáltatónál az internetre. 2005 és 2010 között a leglátogatottabb magyar weboldal 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

[21] Ebből ered az oldal neve is, az angol „read” és „edit”, azaz olvas és szerkeszt szavak összevonásából, illetve a „read it”, elolvasta

[22] Az Anonymous hacktivista közösség decentralizált, egymáshoz lazán köthető csoportok globális hálózata. Kezdetben az internet cenzúrája ellen, az internet szabadásáért harcoltak, később a fennálló világrend megdöntését, politikai és gazdasági rendszerek átalakítását tűzték ki céljuknak. Célpontjuk volt többek között a Szcientológia Egyház, a Sony, a Los Zetas mexikói drogkartell, a WikiLeaks-et bojkottáló pénzügyi vállalatok, az iráni, egyiptomi, tunéziai kormányok, újabban az Al-Kaida és az Iszlám Állam [25].

felhasználók visszacsábítására, de ezeket vagy megkésve vezették be vagy nem sikerült elfogadtassák a felhasználókkal. Ez utóbbira szolgál példaként a mobil platform bevezetése, ami a trendek alapján rendkívül fontosnak tekinthető. Az IWIW aktív felhasználóinak száma folyamatosan csökkent, míg nem az Origo 2014. május 15-én bejelentette, hogy június 30-ától megszünteti az oldalt.

1.1.2.11. Tinder

A Tinder egy 2012-ben létrehozott, tabletre, okostelefonra optimalizált társkereső alkalmazás. A felhasználók száma 2018 áprilisában 46 millióra tehető [26]. Úgy vélem, az alkalmazás alátámasztja, hogy egyes app-okat közösségi média alkotói közé soroljuk. A használatához Facebook regisztráció szükséges, illetve a fejlesztők integrálták az Instagramot a szolgáltatásba. Miután a felhasználók párba állnak, azt követően lehetőségük nyílik szöveges üzenetet váltani egymással.

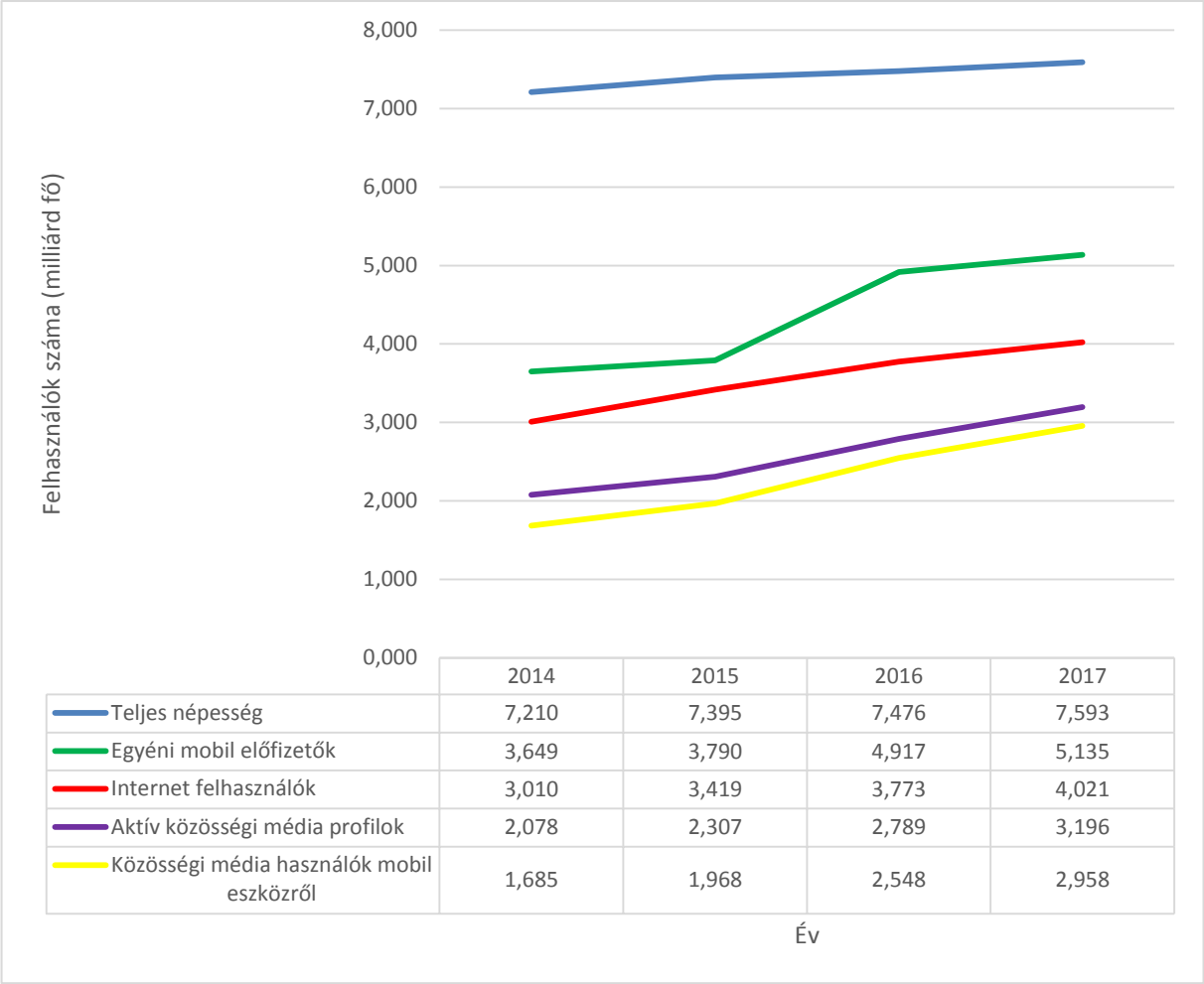
1.1.2.12. Tumblr

A 2007-ben létrehozott Tumblr egy mikroblog szolgáltatás, amelyen képeket, videókat, szövegeket oszthatnak meg egymás között a felhasználók. Az oldal sikere az egyszerűségében rejlik. 2013-ban a Yahoo 1,1 milliárd dollár értékben felvásárolta. 2018 júliusában több mint 402 millió blogot regisztráltak, amelyeken több mint 159 milliárd poszt született [27].

1.2. A közösségi média trendjei

Magyarországon 2018-ban nem végeztek a közösségi média használatra vonatkozó felmérést, így csupán a nemzetközi trendekből vonhatunk le következtetéseket.

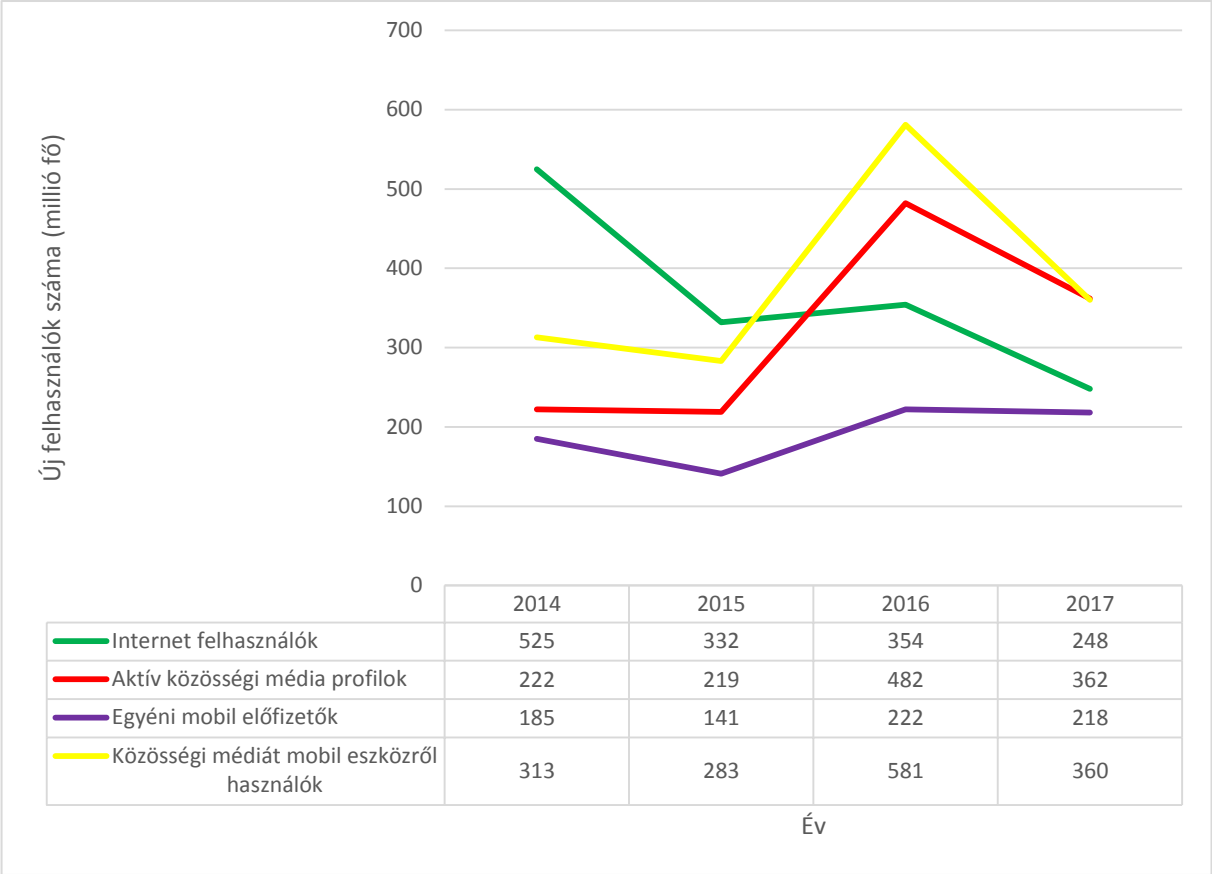
A We are social nevű online marketingre szakosodott reklámügynökség globális felméréseit alapul véve megállapíthatjuk, hogy 2018 januári adatok szerint [28] az aktív internet felhasználók száma meghaladja a négymilliárd főt. A közösségi média profilok száma közel 3,2 milliárd főre tehető, ami 13%-kal magasabb, mint egy évvel korábban. Ebből a mobil eszközről való elérés közel hárommilliárd felhasználói számot jelent, ez 14%-os éves növekedés (lásd 1. számú ábra).



	2014	2015	2016	2017
Teljes népesség	7,210	7,395	7,476	7,593
Egyéni mobil előfizetők	3,649	3,790	4,917	5,135
Internet felhasználók	3,010	3,419	3,773	4,021
Aktív közösségi média profilok	2,078	2,307	2,789	3,196
Közösségi média használók mobil eszközről	1,685	1,968	2,548	2,958

1. ábra Digitális trendek 2014-2017 (saját szerkesztés, forrás: We are social [28])

2017-re a növekedésben visszaesést tapasztalhatunk az új felhasználók számát illetően. Ahogy a 2. számú ábrán is láthatjuk, az egyéni mobil előfizetők számában nem tapasztalunk releváns elmozdulást, 4% az éves növekedés aránya, de az aktív közösségi média profilok (az előző évi 21%-os növekedéshez képest 2017-ben csupán 13%-kal nőtt a felhasználók száma) és az aktív mobil közösségi média profilok esetében az éves növekedés (2016-ban 30%, 2017-ben 14%) üteme jelentősen csökkent.



	2014	2015	2016	2017
Internet felhasználók	525	332	354	248
Aktív közösségi média profilok	222	219	482	362
Egyéni mobil előfizetők	185	141	222	218
Közösségi médiát mobil eszközről használók	313	283	581	360

2. ábra Digitális trendek 2014-2017, Éves növekedés (saját szerkesztés, forrás: We are social [28])

Magyarország közösségi média használatáról az Európai Unió által minden évben publikált Digitális Gazdaság és Társadalom Indexe (továbbiakban DESI) szolgál adatokkal [29]. A DESI különböző indikátorok alapján méri a tagállamok digitális mutatószámait. A 2017-es DESI jelentés alapján hazánk magasan az Európai Unió átlaga fölött teljesít a közösségi média használatot illetően (lásd 1. számú táblázat). A táblázatban látható, hogy az előző évhez képest a hírfogyasztás és online vásárlás esetében figyelhető meg növekedés, a videóhívás és online bankolás esetében csökkenés tapasztalható. Elmondható az is, hogy a közösségi média használat esetében az elmúlt két évben történt változás, Magyarország 83%-os eredményt tudhat magáénak e tekintetben, amivel az Európai Unióban az elsőnek számít, ez az érték 20%-kal magasabb, mint az EU-s átlag.

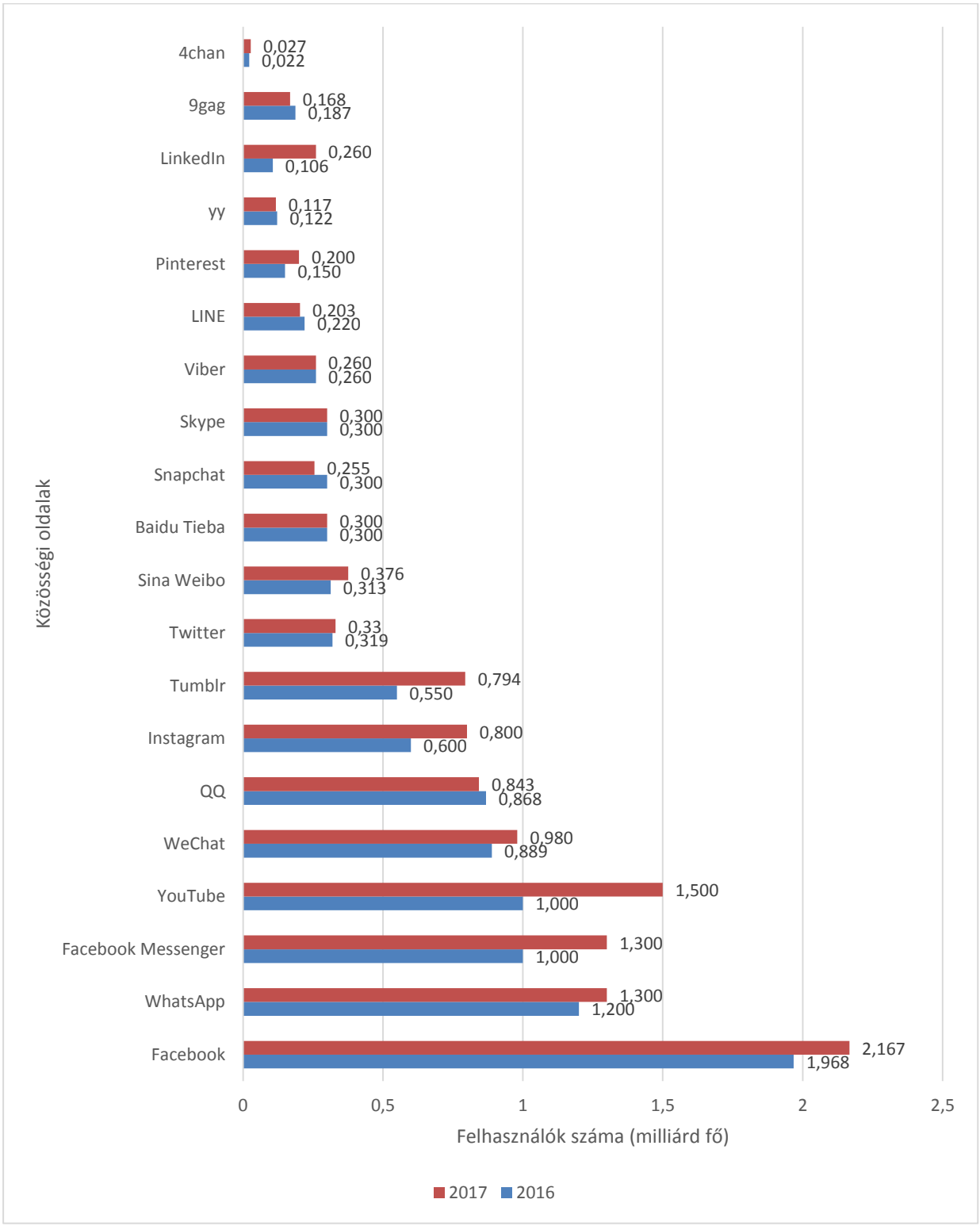
1. táblázat Digitális Gazdaság és Társadalom Index a magyar internethasználatban (saját szerkesztés, forrási: DESI [29])

	Magyarország				EU
	2017		2016		2017
	%	Helyezés	%	Helyezés	%
Hírfogyasztás	88	5	86	7	70
Zene, videó, játékok	81	12	NA		78
VoD[23]	8	24	NA		21
Videóhívás	54	7	55	5	39
Közösségi média	83	1	83	1	63
Online bankolás	44	22	46	20	59
Online vásárlás	48	20	47	20	66

Arra vonatkozóan, milyen arányban használják az egyes közösségi oldalakat Magyarországon, nem készült kutatás az elmúlt években, így a nemzetközi trendeket vehetjük figyelembe. A 3.

[23] Video on Demand olyan tevékenységet jelent, amely során egy korábban streamelt videót utólag is meg lehet tekinteni.

számú ábrán jelenítettem meg a legnépszerűbb közösségi oldalak látogatottságát. Az ábrán feltüntetett adatok a MaU-t veszik alapul.



3. ábra Közösségi oldalak használata globálisan 2016-2017 (saját szerkesztés, forrás: Statista [30], SimilarWeb [31])

Ahogy korábban megfogalmaztam, több olyan, például Kínában népszerű közösségi oldal működik, amelynek felhasználó száma magasabb, mint a nyugati kultúrkörben, ezek azonban kevésbé ismertek Európában.

A We are social 2018-as kutatása [32] a közösségi oldalak használatát Magyarországon 5,81 millió főre teszi, ami 5%-os éves növekedést jelent. Az aktív mobil közösségi média profilok száma 4,8 millió fő, ez 12%-kal magasabb adat 2017 azonos időszakához képest. (lásd 2. számú táblázat)

2. táblázat Magyarországi digitális trendek 2018. (saját szerkesztés, forrás: We are social [32])

	Felhasználók száma (millió fő)	**Penetráció aránya (%)**	**Éves növekedés aránya (millió fő)**	**Éves növekedés aránya (%)**
Teljes népesség	9,71	72		
Internet felhasználók	7,67	79	-208	-2,6
Aktív közösségi média profilok	5,81	60	300	5
Egyéni mobil előfizetők	7,86	81	NA	NA
Közösségi médiát mobil eszközről használók	4,8	49	500	12

A jelentés a magyarországi Facebook felhasználók számát 5,81 millió főre teszi (lásd 3. számú táblázat. Ebből megállapíthatjuk, hogy a 25-34 évesek használják a legnagyobb arányban a Facebookot, az ő számuk 1,35 millió főre tehető. Ezt követi a 35-44 évesek 1,28 milliós, majd a 18-24 évesek 1,11 milliós felhasználói száma. A korosztály vagy nem szerinti megoszlás esetünkben azért tekinthető relevánsnak, mert egy közösségi médiában tervezett művelet esetében az egyes kampányokat az ezekre az adatokra specifikálva szükséges

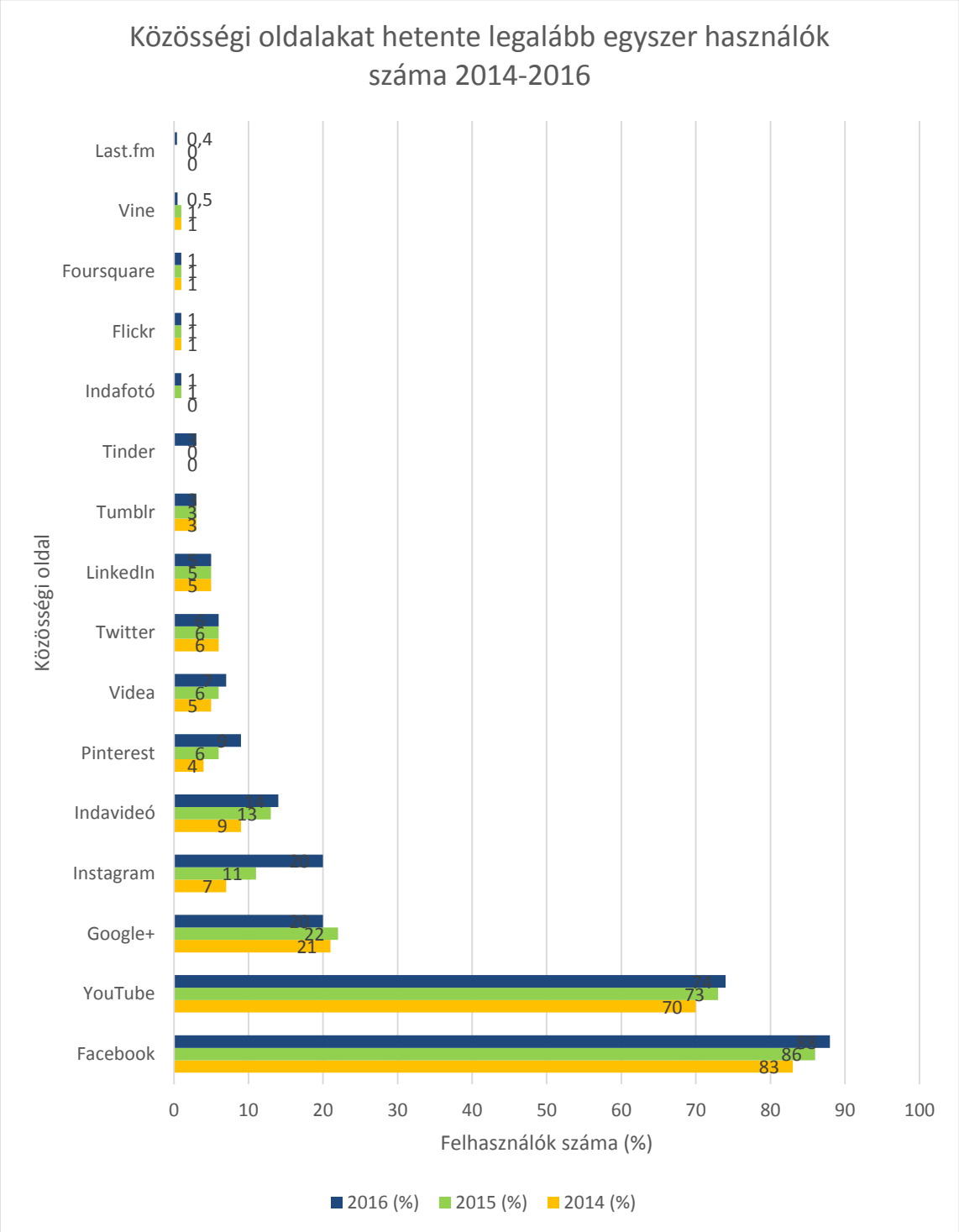
elvégezni. Az adat- és információbiztonsági tudatosság szintje korcsoportonként jelentősen eltér, illetve nemek szerint ez tovább differenciálható.

3. táblázat Magyarországi Facebook felhasználók száma 2018. (saját szerkesztés, forrás: We are social [32])

Korosztály	**Felhasználó szám**	**Ebből nők száma**	**Nők (%)**	**Ebből férfiak száma**	**Férfiak (%)**
Teljes	5801000	3053000	53	2748000	47
13-17	290000	152000	3	138000	2
18-24	1119000	546000	9	573000	10
25-34	1359000	667000	12	692000	12
35-44	1280000	667000	12	613000	11
45-54	831000	465000	8	366000	6
55-64	562000	354000	6	208000	4
65+	360000	202000	3	158000	3

A magyarországi internethasználatról a Nemzeti Média- és Hírközlő Hatóság lakossági internethasználatra vonatkozó 2017-ben publikált, előző évre vonatkozó kutatása tekinthető mérvadónak, az értekezés készítésének idején nincs ennél frissebb hivatalos, magyarországi

felmérés [33]. A 4. számú ábrán látható, hogy a Facebook és YouTube felhasználók száma kimagasló, a többi közösségi oldal nem igazán tekinthető relevánsnak.



4. ábra Közösségi oldalakat hetente legalább egyszer használók száma Magyarországon 2014-2016 (saját szerkesztés, forrás: NMHH [33])

Az NMHH kutatása kitér a közösségi oldalak használatára a motivációk alapján (lásd 4. számú táblázat). Ez alapján a magyarországi felhasználók 78%-a barátokkal, családtagokkal

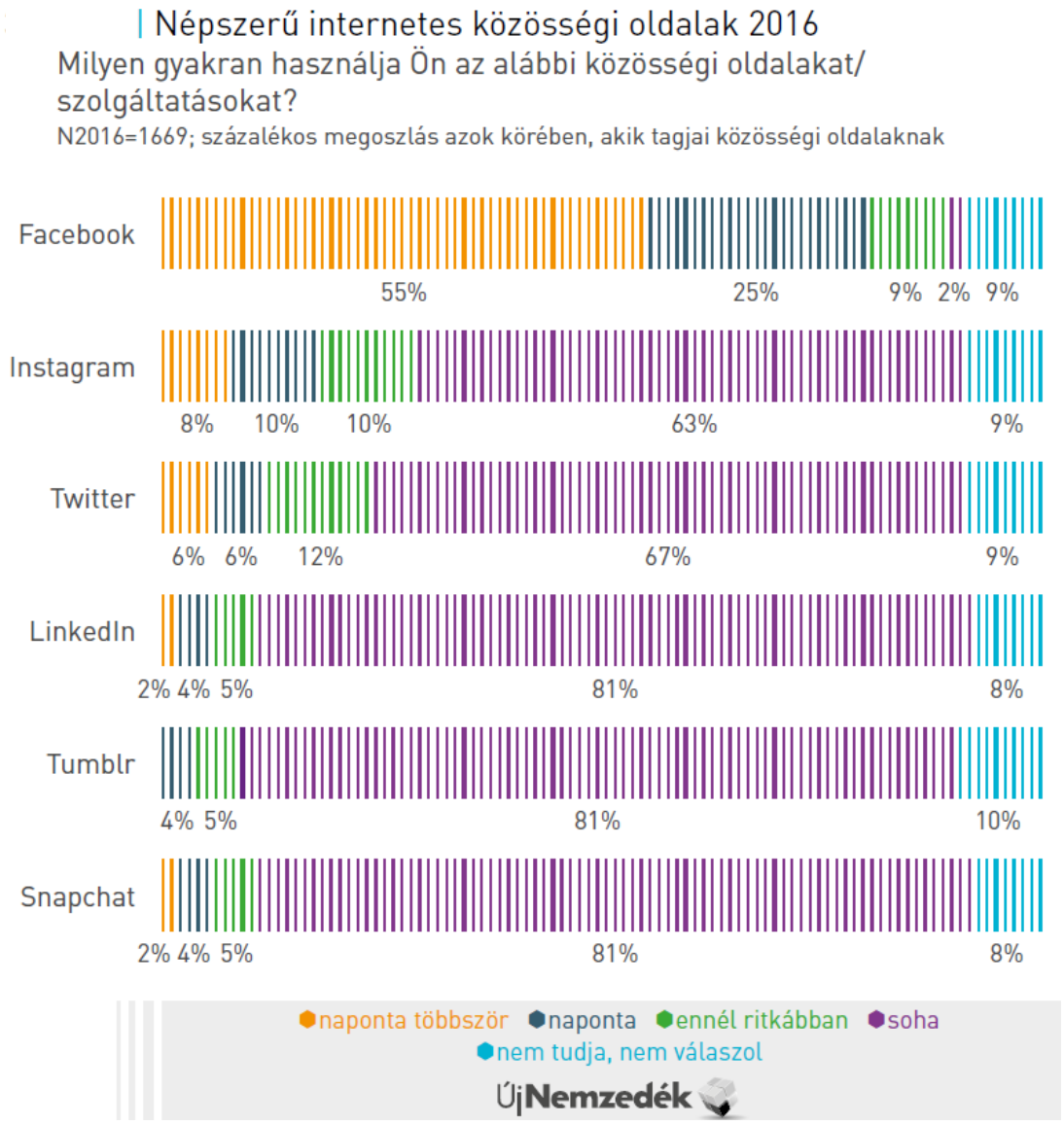
való kapcsolattartást jelölte meg elsődleges szempontként, de a felhasználók valamivel több mint a fele ismerősökkel való kapcsolattartást (54%), érdekességre való rábukkanást (52%), hírfogyasztást (49%) adott válasznak.

4. táblázat A közösségi média használat okai százalékos megoszlás szerint Magyarországon 2016. (saját szerkesztés, forrás: NMHH [33])

Használat célja	**Százalék**
kapcsolatot tartani barátokkal, családtagokkal, más, személyesen ismert emberekkel	78
kapcsolatot tartani olyan ismerősökkel, akikkel személyesen nem vagy nehezen tudok találkozni	54
érdekességekre rábukkanni	52
elolvasni, megtudni a friss híreket az ország-világ dolgairól	49
fotókat, videókat nézni	47
zenét hallgatni	45
kikapcsolódni, szórakozni	42
megtalálni olyan embereket, akikkel elvesztettem a kapcsolatot	26
fotókat, videókat megmutatni, megosztani	25
segítséget, tanácsot, információt kapni nekem fontos dolgokhoz, pl. iskolaválasztás, álláskeresés, gyereknevelés, magánélet	24
üzletek, szolgáltatók, vendéglátóhelyek, rendezvények profilját, saját magukról adott információit elolvasni	23
a tanuláshoz szükséges, hasznos	21
a munkámhoz szükséges, hasznos	19
hasonló érdeklődésű, gondolkodású emberek virtuális közösségéhez tartozni	18
ismerkedni, új embereket megismerni, barátokat szerezni	17
hírt adni saját magamról	13
megmutatni a tevékenységemet (pl. ahogy táncolok, zenélek vagy ha varrtam egy ruhát, készítettem egy tárgyat)	8
kapcsolatot tartani valamely híresség̈gel (pl. színésszel, zenekarral, politikussal)	5

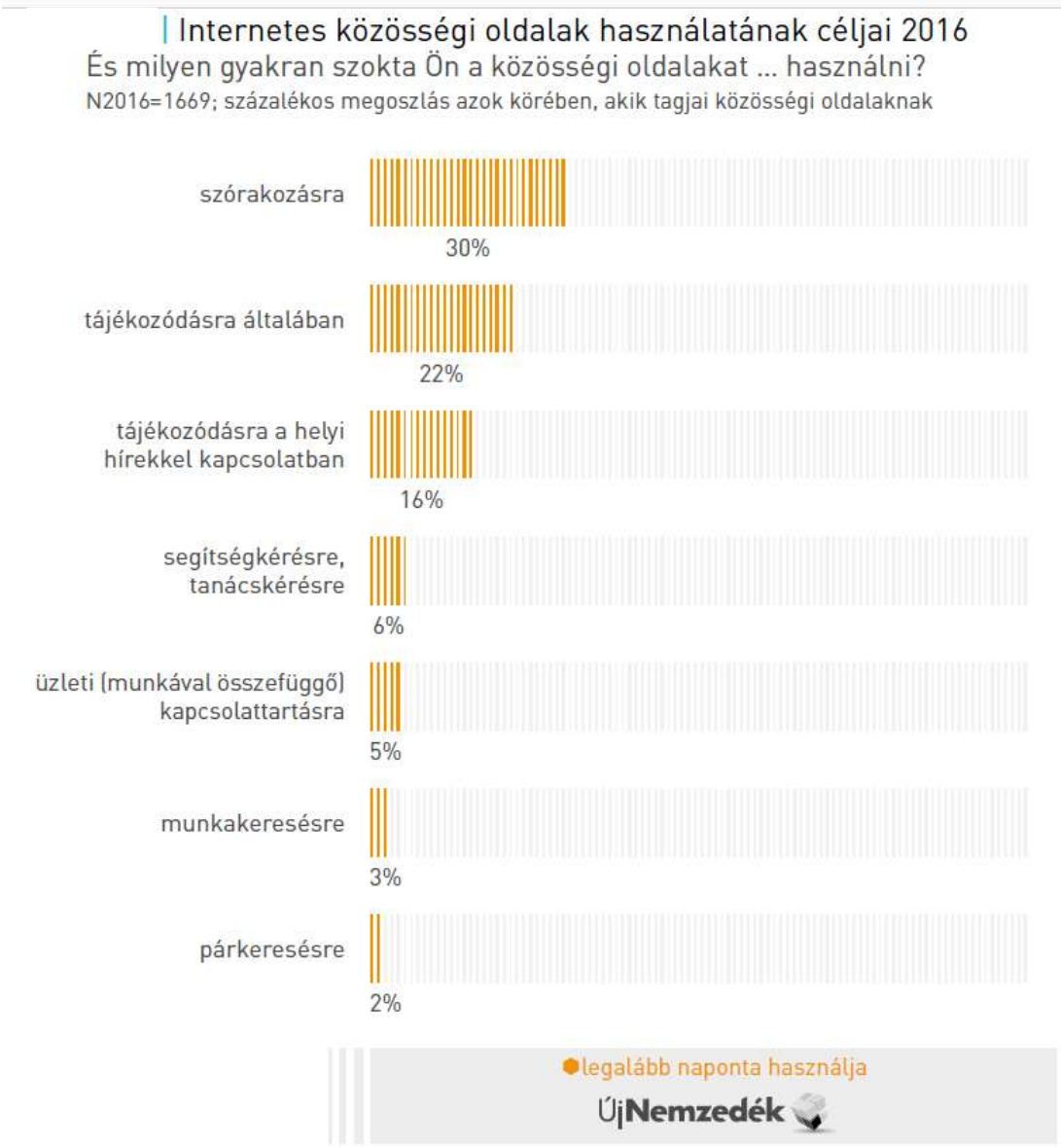
A magyarországi fiatalok felhasználói szokásokairól az Új Nemzedék Központ által 2017-ben publikált Magyar Ifjúság 2016-os kutatása ad iránymutatást, amelyben a 15-29 éveseket vizsgálták [34]. A jelentésből kiolvasható, hogy a 15-29 évesek 79%-a használ valamilyen közösségi oldalt, a 5. számú ábrán ezen oldalak használatának gyakorisága látható. Ebből újfent a Facebook dominanciája állapítható meg a fiatalok körében, 80%-uk naponta

legalább egyszer használja az oldalt. A második leggyakrabban látogatott oldal az Instagram, ez 18%-os eredményt ért el, azonban az Instagram a Facebook tulajdona.



5. ábra Közösségi oldalak használatának gyakorisága Magyarországon, 2016 (forrás: Új Nemzedék Központ [34])

Összevetve az NMHH eredményeit az Új Nemzedék Központ kutatásával, azt tapasztaljuk (lásd 6. számú ábra), hogy a 25-29 közötti fiatalok naponta legalább egy alkalommal szórakozásra (30%), tájékozódásra általában (22%), tájékozódásra helyi hírekkel kapcsolatban (16%) használják a közösségi oldalakat.



5. táblázat Közösségi oldalak használatának céljai Magyarországon 2016. (forrás: Új Nemzedék Központ [34])

1.3. A közösségi média, megjelenése a tudományos gondolkodásban

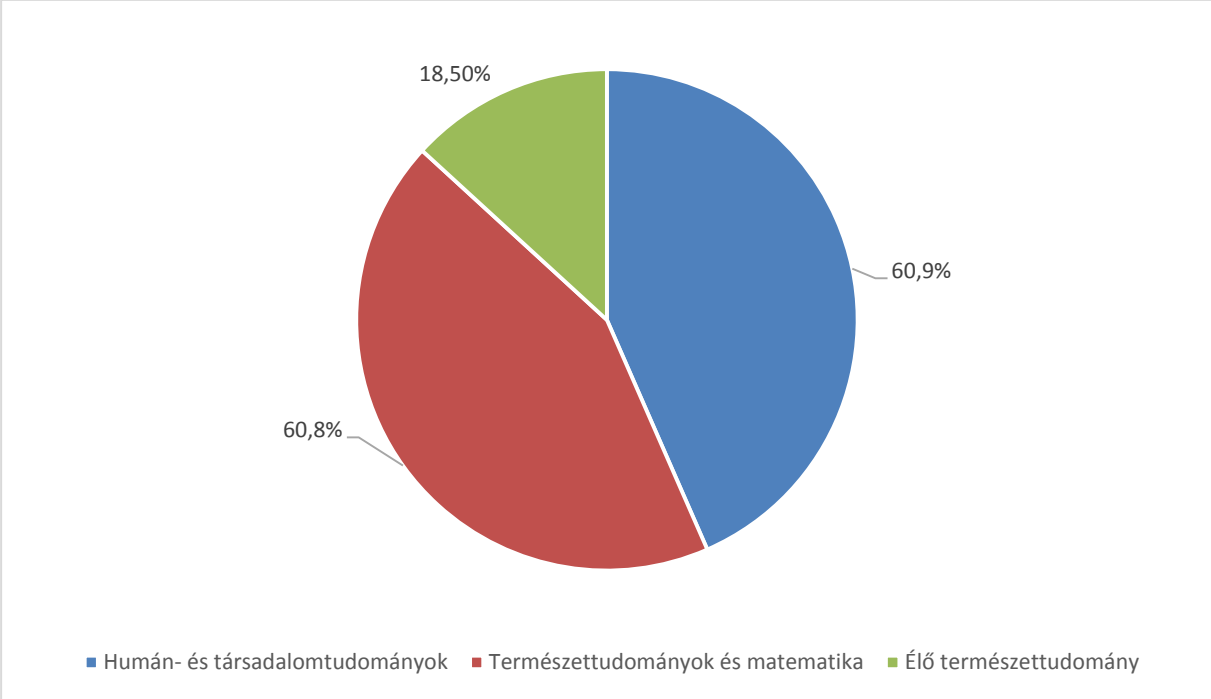
A közösségi média tudományos gondolkodásban való megjelenését három adatbázis segítségével vizsgáltam. A 2004-ben alapított Scopus a lektorált szakirodalom legnagyobb absztrakt és citátum adatbázisa, amely több tízezer folyóirat, könyvsorozat, konferenciakiadvány elemzését teszi lehetővé. A Scopust felhasználva különböző kulcsszavak alapján építettem adatbázist. Ez az adatbázis azonban nem tartalmazta a tudományos közlemények tudományterületi és tudományági besorolását, ennek meghatározásához a SCImago Journal Rank (továbbiakban SJR) adatbázisát vettem alapul. Az SJR számos indikátor

alapján tudománymetriai értékelés alapján osztályozza az egyes tudományos folyóiratokat, konferenciakiadványokat. Fontos kiemelni, hogy egy folyóirat vagy konferencia kiadvány adott esetben több tudományterületen releváns lehet. A harmadik általam használt adatbázis a SciVal volt. A SciVal, hasonlóan a Scopushoz, az Elsevier kiadó gondozásában működik, ennek megfelelően a Scopus adatbázisát felhasználva felérképezhetjük az egyes kutatók tudományos megjelenését, az egyes kutatási szakterületeket. Számomra az utóbbi bír relevanciával, hiszen ily módon lehetőségem nyílt azonosítani a közösségi médiának, mint szakterületnek a kapcsolódási pontjait.

Az I.1. alfejezetben azt az állítást fogalmaztam meg, hogy a közösségi média fogalmát különböző tudományterületek specifikusan értelmezték. Első lépésként megvizsgáltam, a közösségi média keresőkifejezésre milyen találati listát kapok. A keresés vonatkozott minden olyan tudományos közleményre, amelynek a címében, absztraktjában vagy a kulcsszavai között megjelent a közösségi média kereső kifejezés. Az adatbázis, hasonlóan a Google keresésekhez több kulcsszó alapján csak abban az esetben értelmezi a szavak közötti kapcsolatot, amennyiben azok idézőjel között szerepelnek, ellenkező esetben minden olyan találatot megjeleníteni, amelyekben vagy a közösségi vagy a média szavak megtalálhatóak. A keresést én ezzel a szűkítéssel végeztem. A „közösségi média" keresőkifejezésre a Scopus 46311 találatot jelenített meg. A találatok egyaránt tartalmaztak folyóiratokat, konferencia kiadványokat, könyveket és egyéb publikációs formákat. Az így kapott találati listát megvizsgáltam tudományterületi megoszlás szerint. Ez azonban egy módszertani problémához vezetett, ugyanis a nemzetközi tudományos életben az egyes tudományterületek nem azonos területeket fednek le a Magyar Tudományos Akadémia (továbbiakban MTA) által meghatározott tudományterületi nómenklatúrával. Az SJR 27 különböző tudományterületet határoz meg, míg a Magyar Tudományos Akadémia 3 tudományterület különböztet meg. [24]Ez a 3 tudományterület „Természettudományok és matematika", „Élő természettudomány" és „Humán és társadalomtudományok". Ezek bomlanak fel 11 tudomány-részterületre, amelyek az SJR által megkülönböztetett 27 tudományterületnek felelnek meg. A kutatásom során az SJR által nevesített tudományterületeket besoroltam az MTA által meghatározott három tudományterület alá.

[24] Az MTA Doktori Tanácsa 2016-ban felülvizsgálta a korábbi tudományági besorolást, amelynek keretében egy háromszintű osztályozást vezetett be. Az első szint a tudományos osztályok által képviselt tudományterületeket jelöli. A második szintet az osztályokon belül megkülönböztetett tudomány-részterületek adják. Ezek szorosan kapcsolódnak az osztályok tudományos bizottságaihoz, gyakran a megnevezésük is azonos. A harmadik szintet a tudomány-részterületek alá sorolt tudományágak alkotják.

A közösségi média keresőkifejezés tudományterületek alapján az MTA besorolást alapul véve megállapíthatjuk, hogy a Humán- és társadalomtudományok (60,9%) és a Természettudomány és matematika (60,8%) közel azonos arányban oszlanak meg (lásd 6. számú ábra).



6. ábra Közösségi média tudományterületenkénti megoszlása (MTA) (saját szerkesztés, forrás: Scopus [35], SJR [36])

Témám szempontjából a közösségi média teljeskörű vizsgálatának nincs relevanciája, így szűkítettem a keresést. Meghatároztam öt vizsgálati területet, amelyek a védelmi szféra tekintetében számottevőek. Ez az öt terület „military", mint katonai, „law enforcement", mint rendészeti, „national security", mint nemzetbiztonsági, valamint „politics", mint politikai és „governance", mint kormányzás kapcsolatokat vizsgált. Utóbbi két kategóriát azért alkalmaztam, mert a katonai, rendészeti és nemzetbiztonsági területek hatásai a politikai alrendszerben jelentkeznek, és tevékenységeiket a kormányzatok által meghatározottak szerint végzik. A keresést így „social media" + „military", „social media" + „law enforcement", „social media" + „national security", „social media" + „politics", „social media" + „governance" szűkítéssel végeztem, az így kapott találatokból egy 2250 tudományos közleményt tartalmazó adatbázist készítettem. Ebben természetesen előfordulhat átfedés, hiszen például a „social media" + „politics" és a „social media" + „governance" találatok között lehet közös halmaz. A keresés a közösségi média keresőkifejezéshez hasonlóan minden olyan publikációra vonatkozott, amely a keresett kifejezés a címben, absztraktban vagy kulcsszavakban találatként jelentkezett. A 2250 dokumentum megoszlásait területek szerint a 6. számú táblázatban

ábrázoltam, ebből látható, a politika és kormányzat területén született a legtöbb publikáció. A gyűjtést 2018. március elején végeztem, a 2250 találat az ekkori adatokra vonatkozik.

6. táblázat Közösségi média vizsgálati területenként (saját szerkesztés forrás: Scopus [35], SJR [36])

Terület	Darabszám
Politikai	1258
Kormányzás	505
Katonai	219
Rendészeti	194
Nemzetbiztonsági	74

A 7. számú táblázat a publikációk típusonkénti megoszlását tartalmazza, ezen világosan látható, hogy a legmagasabb számban közlemények formájában publikálták a szerzők eredményeiket, ezt követi a konferenciakiadvány, mint publikációs típus.

7. táblázat Közösségi média megoszlása publikáció típusonként az öt vizsgálati területen (saját szerkesztés, forrás: Scopus [35], SJR [36])

Típus	Politikai	Kormányzás	Katonai	Rendészeti	Nemzetbiztonsági	Végösszeg
Közlemény	761	221	84	69	23	1158
Konferenciakiadvány	167	113	65	86	33	464
Könyvfejezet	66	51	13	16	7	153
Könyv	87	26	15	4	3	135
Egyéb	177	94	42	19	8	340

Mind az öt vizsgálati terület esetén megvizsgáltam az 5 legidézettebb közleményt, hogy kiderüljön, a tudományos közösség melyik kutatásokat tekinti relevánsabbnak. A katonai vizsgálati terület eredményeit a 8. számú táblázatban ábrázoltam.

8. táblázat Az 5 legidézettebb tudományos közelmény a közösségi média és katonai keresőkifejezések esetében (saját szerkesztés, forrás: Scopus [35]

Idézetek száma	Szerzők	Közlemény címe
118	Vicario et al.	The spreading of misinformation online
51	Coppersmith et al.	Measuring post traumatic stress disorder in twitter
42	Altheide, D.L.	Media logic, social control, and fear
32	Wulf et al.	Fighting against the wall: Social media use by political activists in a Palestinian village

30	Zeitzoff, T.	Using social media to measure conflict dynamics: An application to the 2008-2009 gaza conflict

A 8. számú táblázatban megjelenített közlemények esetében megállaphítható, a politikai mozgalmak befolyásolásával, a lélektani műveletekkel kapcsolatos és az orvosi jellegű[25] kutatások a legnépszerűbbek.

A 9. számú táblázatban a rendészeti kutatások legidézettebb közleményei olvashatóak. Ebből megállapíthatjuk, hogy a stratégiai kommunikációval kapcsolatos kutatások kiemeltek, legyen szó rendkíüvli események kezeléséről (mint például a Sandy hurrikán vagy zavargások kezelése) vagy a rendőrség lakossággal történő kapcsolattartása.

9. táblázat Az 5 legidézettebb tudományos közelmény a közösségi média és rendészeti keresőkifejezések esetében (saját szerkesztés, forrás: Scopus [35]

Idézetek száma	**Szerzők**	**Közlemény címe**
139	van Dijck, J.	Datafication, dataism and dataveillance: Big data between scientific paradigm and ideology
90	Hughes et al.	Online public communications by police & fire services during the 2012 Hurricane Sandy
55	Denef et al.	Social media and the police-tweeting practices of British police forces during the August 2011 riots
54	Stuesse et al.	Automobility, immobility, altermobility: Surviving and resisting the intensification of immigrant policing
46	Heverin et al.	Twitter for city police department information sharing

A nemzetbiztonsági kutatások legnépszerűbb közleményeit a 10. számú táblázat tartalmazza. A rendészeti kutatásokhoz hasonlóan szintén fontos a stratégiai kommunikáció. A Lee Hughes és szerzőtársai által e témában publikált közleményük jelentőségét az is alátámasztja, hasonló tartalommal máshol is publikálták tanulmányukat, amelyet még 165-en citáltak az eredeti 320 idézeten felül. Az Edward Snowdennel kapcsolatos kutatások népszerűsége véleményem szerint nem véletlen, a legtöbbet idézett tanulmányok közül 2 a Snowden üggyel kapcsolatosak. Fontos továbbá a közösségi médiának a politikai mozgalmakban betölött szerepének vizsgálata.

[25] Például a poszttraumás stressz kezelésére vonatkozó kutatások.

10. táblázat Az 5 legidézettebb tudományos közelmény a közösségi média és nemzetbiztonsági keresőkifejezések esetében (saját szerkesztés, forrás: Scopus [35]

Idézetek száma	Szerzők	Közlemény címe
320	Lee Hughes et al.	Twitter adoption and use in mass convergence and emergency events
117	Cogburn et al.	From networked nominee to networked nation: Examining the impact of web 2.0 and social media on political participation and civic engagement in the 2008 obama campaign
50	Howard et al.	When do states disconnect their digital networks? Regime responses to the political uses of social media
31	Stoycheff, E.	Under surveillance: Examining facebook's spiral of silence effects in the wake of NSA internet monitoring
29	Qin, J.	Hero on Twitter, Traitor on News: How Social Media and Legacy News Frame Snowden

A 11. számú táblázat a közösségi média és politikai keresőkifejezések 5 legnépszerűbb közleményét jelenítik meg. Ezekről elmondható, hogy többségében a politikai mozgalmak, mobilizáció aspektusát vizsgálják.

11. táblázat Az 5 legidézettebb tudományos közelmény a közösségi média és politikai keresőkifejezések esetében (saját szerkesztés, forrás: Scopus [35]

Idézetek száma	Szerzők	Közlemény címe
724	Jenkis et al.	Spreadable media: Creating value and meaning in a networked culture
692	Bond et al.	A 61-million-person experiment in social influence and political mobilization
255	Bennett et al.	The logic of connective action: Digital media and the personalization of contentious politics
250	Bakshy et al.	Exposure to ideologically diverse news and opinion on Facebook
225	Bennett, W.L.	The Personalization of Politics: Political Identity, Social Media, and Changing Patterns of Participation

A közösségi média és kormányzás esetében az 5 legtöbbett idézett közlemény a 12. számú táblázatban kapott helyet. Ez alapján elmondható, hogy alapvetően a transzparencia, a szakpolitikai döntéshozatal esetében kapunk közleményeket, utóbbi esetében az egészségügyi ellátás is fontos kutatási területként jelentkezik.

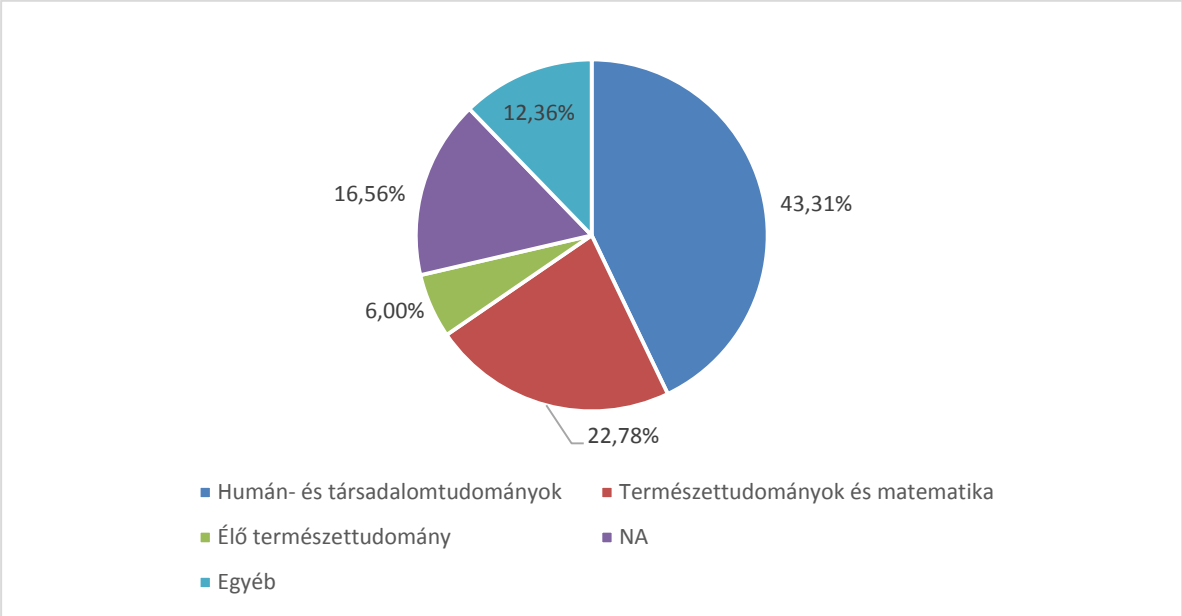
12. táblázat Az 5 legidézettebb tudományos közelmény a közösségi média és kormányzás keresőkifejezések esetében (saját szerkesztés, forrás: Scopus [35]

Idézetek száma	Szerzők	Közlemény címe
725	van Dijick, J.	The Culture of Connectivity: A Critical History of Social Media

386	Batty et al.	Smart cities of the future
323	Bonsón et al.	Local e-government 2.0: Social media and corporate transparency in municipalities
300	Bertot	The impact of polices on government social media usage: Issues, challenges, and recommendations
153	Grajales	Social media: A review and tutorial of applications in medicine and health care

A Scopus adatbázisból letöltött adatok nem tartalmazták az egyes publikációk tudományterületi besorolását, ezért kiegészítettem az SJR által feltüntetett adatokkal. Azonban ezzel együtt sem tudtam minden publikáció esetén meghatározni a kapcsolódó tudományterületeket, ugyanis az SJR csupán az általa jegyzett folyóiratok, konferencia kiadványok esetében szolgál információval, így például többek között a könyvek esetében semmilyen információt nem kaptam, de több folyóirat, konferenciakiadvány nem szerepelt az SJR adatbázisában, ezért „NA”, vagyis nincs adat jelölést alkalmaztak ezen publikációk esetében.

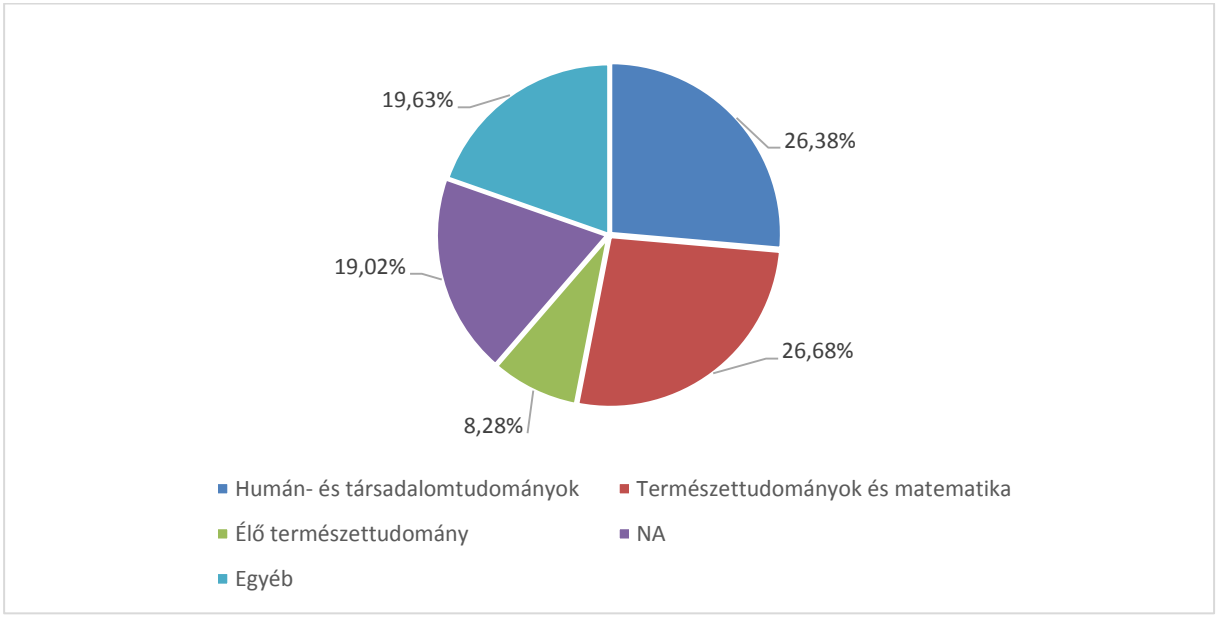
Az öt vizsgálati terület együttes elemzéséből a társadalomtudományok dominanciáját állapíthatjuk meg (lásd 7. számú ábra), a Humán és társadalomtudományok tudományterületén készült publikációk közel kétszer magasabb értéket mutatnak (43,31%), mint a Természettudományok és matematika (22,78%).



7. ábra Közösségi média keresőkifejezések megoszlása tudományterületenként (MTA) (saját szerkesztés, forrás: Scopus [35], SJR [36])

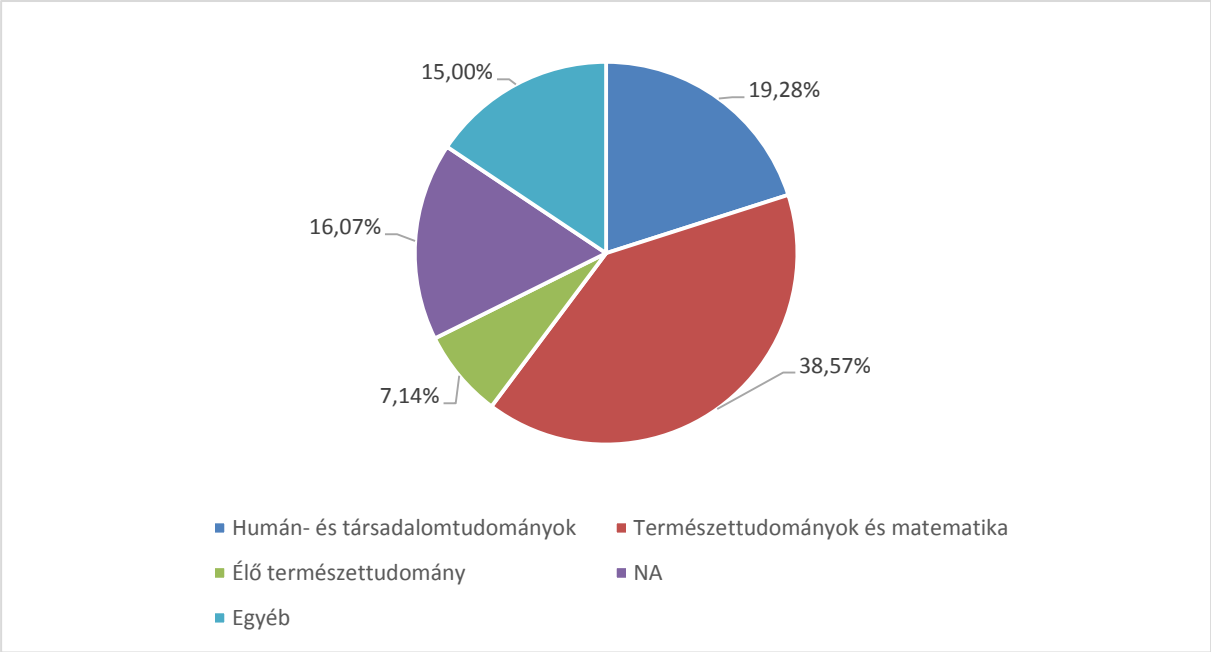
Az öt vizsgálati területet elemezve megállapíthatjuk, a katonai és rendészeti keresőkifejezések esetében megfordul a tendencia, és a műszaki tudományok magasabb

reprezentációját tapasztaljuk. A 8. számú ábrán a közösségi média és katonai kifejezésre kapott találatokat jelenítettem meg, ebből látható, hogy nem csupán kiegyenlítődik a társadalomtudomány és műszaki tudományok aránya, de a műszaki tudományok összességében – bár épp csak– megelőzik a társadalomtudományokat. Az ábráról leolvasható, hogy a Természettudományok és matematika területéről 26.68%-a született a publikációknak, míg a Humán és társadalomtudományok minimálisan alacsonyabb, 26,38%-os értéket jelent.



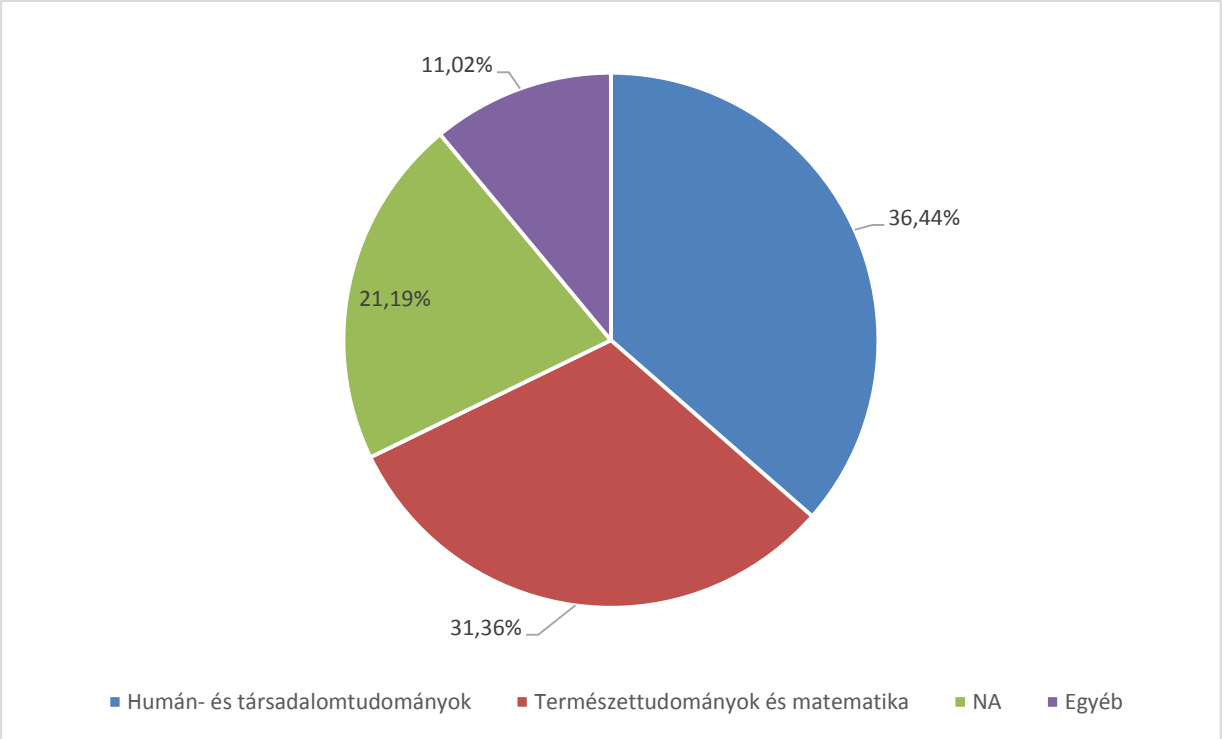
8. ábra Közösségi média és katonai keresőkifejezések megoszlása tudományterületenként (MTA) (saját szerkesztés, forrás: Scopus [35], SJR [36])

Tovább erősödik a műszaki tudományok aránya a rendészeti kutatások esetében. A közösségi média és rendészeti keresőkifejezések esetében a műszaki területek dominanciáját tapasztaljuk, a 9 számú ábrán látható, hogy a Természettudományok és matematika közel kétszeres értéket mutat (38,57%) a Humán- és társadalomtudományokkal szemben (19,28%).



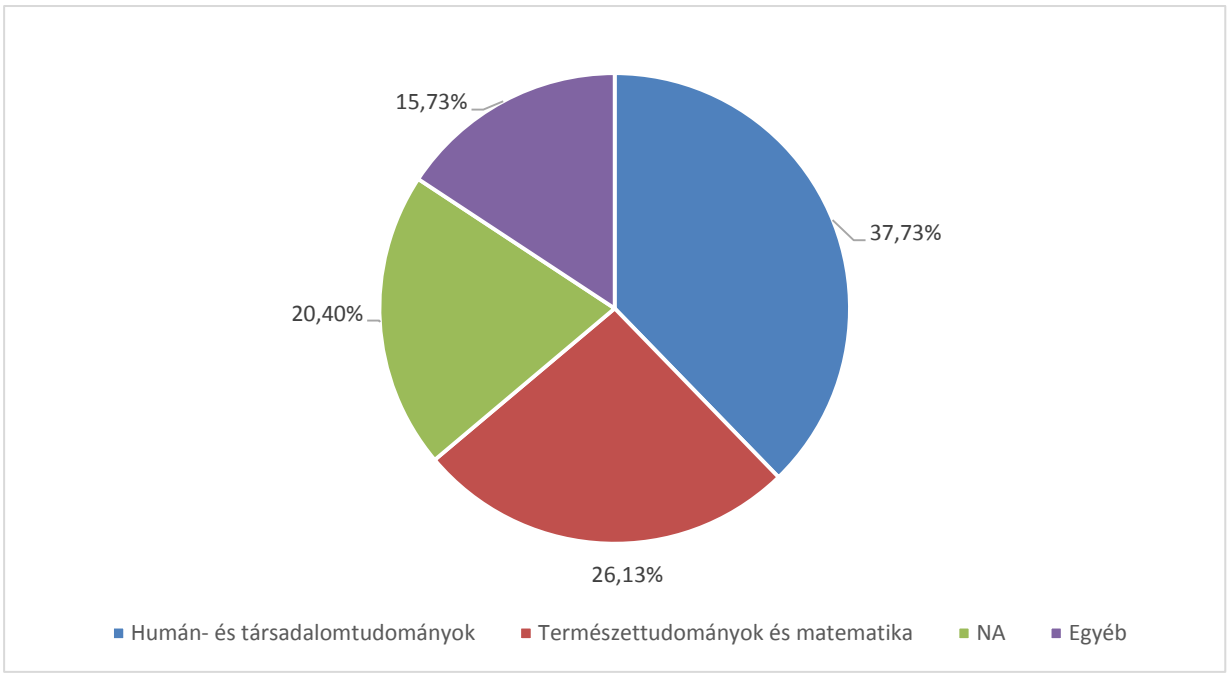
9. ábra Közösségi média és rendészeti keresőkifejezések megoszlása tudományterületenként (MTA) (saját szerkesztés, forrás: Scopus [35], SJR [36])

Az általam vizsgált öt területből a nemzetbiztonsággal kapcsolatos kutatás esetében megállapítható, hogy közel azonos arányban – bár valamelyest magasabb arányban– publikáltak társadalomtudományok és műszaki tudományok területéről. Ezt az eltérést a 10. számú ábrán jelenítettem meg, amin látható, hogy a Humán- és társadalomtudományok, valamint a Természettudományok és matematika esetében alig 5%-os eltérést tapasztalunk a két értéket illetően.



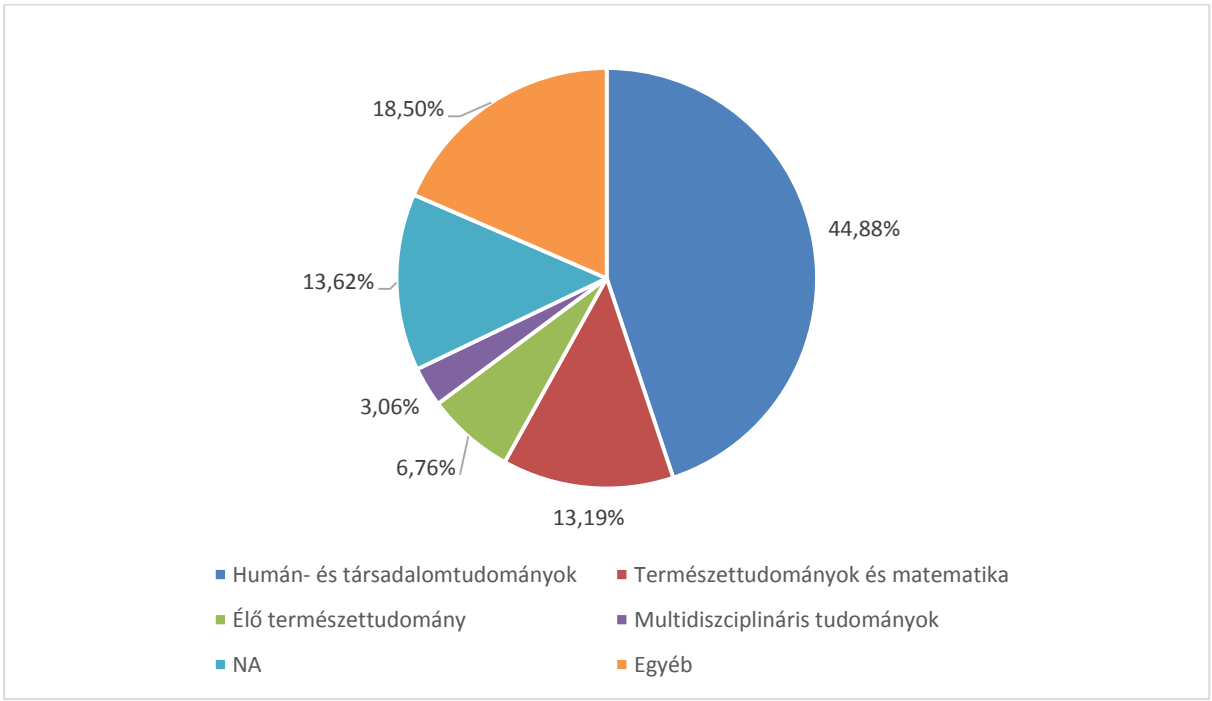
10. ábra Közösségi média és nemzetbiztonsági keresőkifejezések megoszlása tudományterületenként (MTA) (saját szerkesztés, forrás: Scopus [35], SJR [36])

Az öt vizsgálati terület összesített elemzése a társadalomtudományok dominanciáját mutatta, amelyet a katonai, rendészeti, nemzetbiztonsági kutatások nem támasztottak alá, a vizsgálataimból kiderült, a katonai és rendészeti kutatások esetében műszaki tudományterületéről született több publikáció, míg a nemzetbiztonsági területen kis lemaradással, de szintén magas volt arányaiban a műszaki területekről származó publikációk száma. Az összesített eredményben a politikai és kormányzás keresőkifejezéseknél kapott eredmények magyarázzák a társadalomtudományok magas reprezentációját. A 11. számú ábrán a közösségi média és kormányzás tudományterületi megoszlásai láthatóak. Ez esetben még nem figyelhető meg olyan arányú eltérés, mint a politikai tekintetében, de a Humán- és társadalomtudományok valamivel több, mint 10%-os eltérést jelentenek a Természettudományok és matematika tudományterületeihez képest.



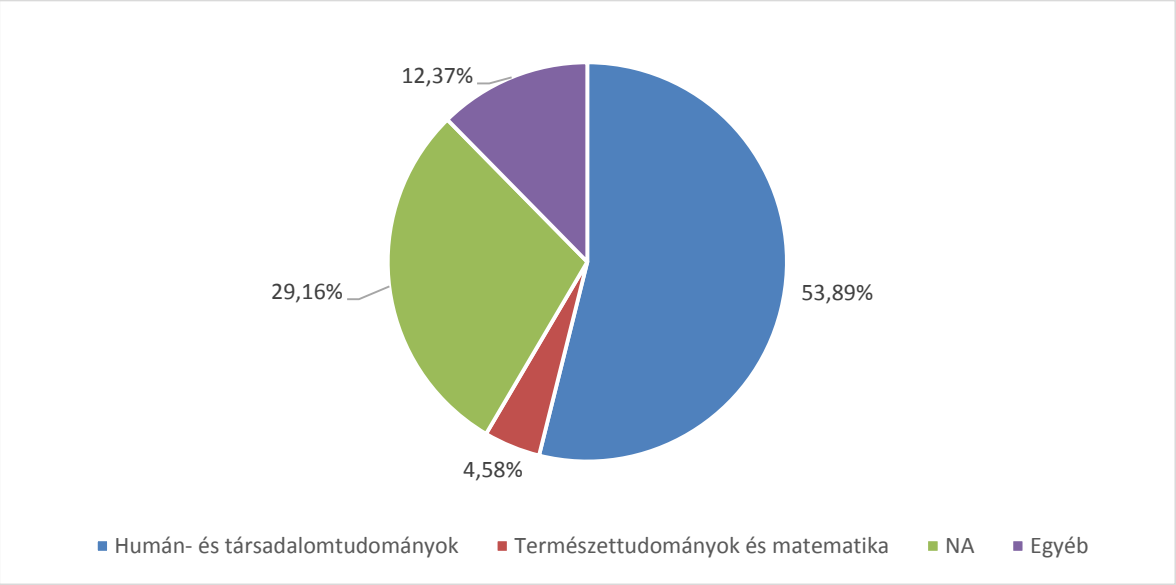
11. ábra Közösségi média és kormányzás keresőkifejezések megoszlása tudományterületenként (MTA) (saját szerkesztés, forrás: Scopus [35], SJR [36])

Arányaiban jelentős ugrást tapasztalunk a közösségi média és politikai kifejezések vizsgálatakor (lásd 12. számú ábra), látható, hogy ez esetben a Humán- és társadalomtudományokhoz köthető kutatások száma 30%-kal magasabb, mint a Természettudományok és matematika területén levők. Ez esetben plusz kategóriaként jelentkezik a Multidiszciplináris tudományok, ezt azonban az MTA nómenklatúrája nem különíti el.



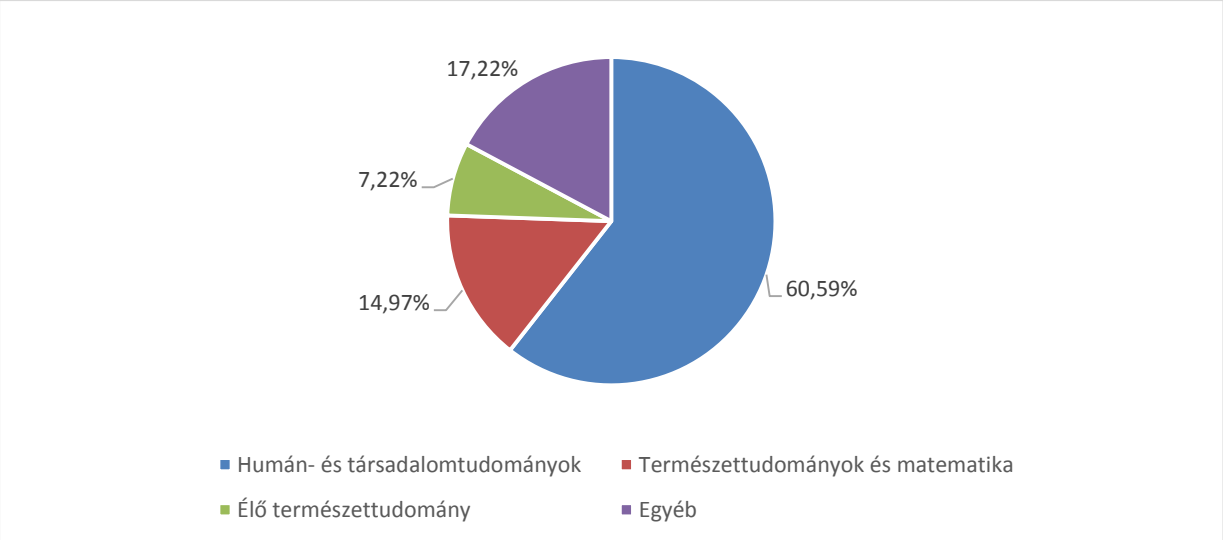
12. ábra Közösségi média és politikai keresőkifejezések megoszlása tudományterületenként (SJR) (saját szerkesztés, forrás: Scopus [35], SJR [36])

Az öt területen megvizsgáltam a tudományos közlemények számának alakulását az egyes publikációs típusokra lebontva. Ez alapján árnyaltabb képet kapunk az egyes tudományterületi megoszlásról. Figyelemre méltó, hogy a konferenciakiadványok vonatkozásában magasan a műszaki tudományterületéről származnak a publikációk. A 13. számú ábrán látható, hogy az Természettudományok és matematika az 53,89%-át jelentik az összes tudományterületnek, míg a Humán- és társadalomtudományok nem érik el az 5%-ot.



13. ábra Konferenciakiadványok megoszlása tudományterületenként (MTA) (saját szerkesztés, forrás: Scopus [35], SJR [36])

A közlemények esetében azonban fordított képet kapunk (lásd 14. számú ábra), ugyanis esetükben magasan a társadalomtudományok felülreprezentáltak, a Humán- és társadalomtudományok négyszeres értéket képviselnek a Természettudományok és matematika területén készült tanulmányokhoz képest.



14. ábra Közlemények megoszlása tudományterületenként (MTA) (saját szerkesztés, forrás: Scopus [35], SJR [36])

Az öt vizsgált területen megfigyelhető eltérést az egyes tudományterületek esetében a kulcsszavak magyarázzák. Összesen 8790 kulcsszavat kaptam, a leggyakoribb kifejezéseket a 13. számú táblázat tartalmazza.

13. táblázat Leggyakoribb kulcsszavak az öt vizsgálati területen (saját szerkesztés, forrás: Scopus [35])

Helyezés	**Kulcsszó**	**Helyezés**	**Kulcsszó**	**Helyezés**	**Kulcsszó**	**Helyezés**	**Kulcsszó**
1	közösségi média	11	közösségi mozgalom	21	Kína	31	Arab tavasz
2	Twitter	12	big data	22	fiatal	32	e-demokrácia
3	politika	13	web 2.0	23	YouTube	33	etika
4	Facebook	14	választások	24	közösségi hálón való kommunikáció	34	identitás
5	közösségi hálózat	15	új média	25	demokrácia	35	újságírás
6	internet	16	részvétel	26	e-részvétel	36	megfigyelés
7	e-kormányzás	17	véleményelemzés	27	kommunikáció	37	technológia
8	politikai kommunikáció	18	média	28	adatbányászat	38	állampolgárság
9	politikai részvétel	19	aktivizmus	29	nem	39	civil elköteleződés
10	kormányzás	20	mikro blog	30	hálózat	40	tiltakozás

Bizonyos kulcsszavak szorosabban kapcsolódnak bizonyos tudományterületekhez. A 14. számú táblázatban jelenítettem meg a leggyakoribb kulcsszavakat a katonai (összesen 755 kulcsszó), rendészeti (összesen 767 kulcsszó), illetve nemzetbiztonsági (összesen 315 kulcsszó) vizsgálati területekről.

14. táblázat Leggyakoribb keresőkifejezések a közösségi média és katonai, rendészeti, illetve nemzetbiztonsági keresésekre (saját szerkesztés, forrás: Scopus [35])

Helyezés	Katonai		Rendészeti		Nemzetbiztonsági	
	kulcsszó	**darab**	**kulcsszó**	**darab**	**kulcsszó**	**darab**
1	közösségi média	53	közösségi média	63	közösségi média	28
2	katonai	12	Twitter	18	Twitter	8
3	Facebook	8	rendészeti	13	nemzetbiztonság	5
4	Twitter	5	rendőrség	10	mikro blog	5
5	identitás	5	big data	10	biztonság	3
6	terrorizmus	4	kiberbűnözés	10	közösségi hálózat elemzés	3
7	közösségi hálózat	4	nyílt forrású hírszerzés	9	vészhelyzet	3
8	veteránok	4	mikro blog	7	big data	3
9	ellenálló képesség	4	természetes nyelvek feldolgozása	7	megfigyelés	3
10	információs műveletek	4	közösségi rendőrség	7	adatbányászat	3

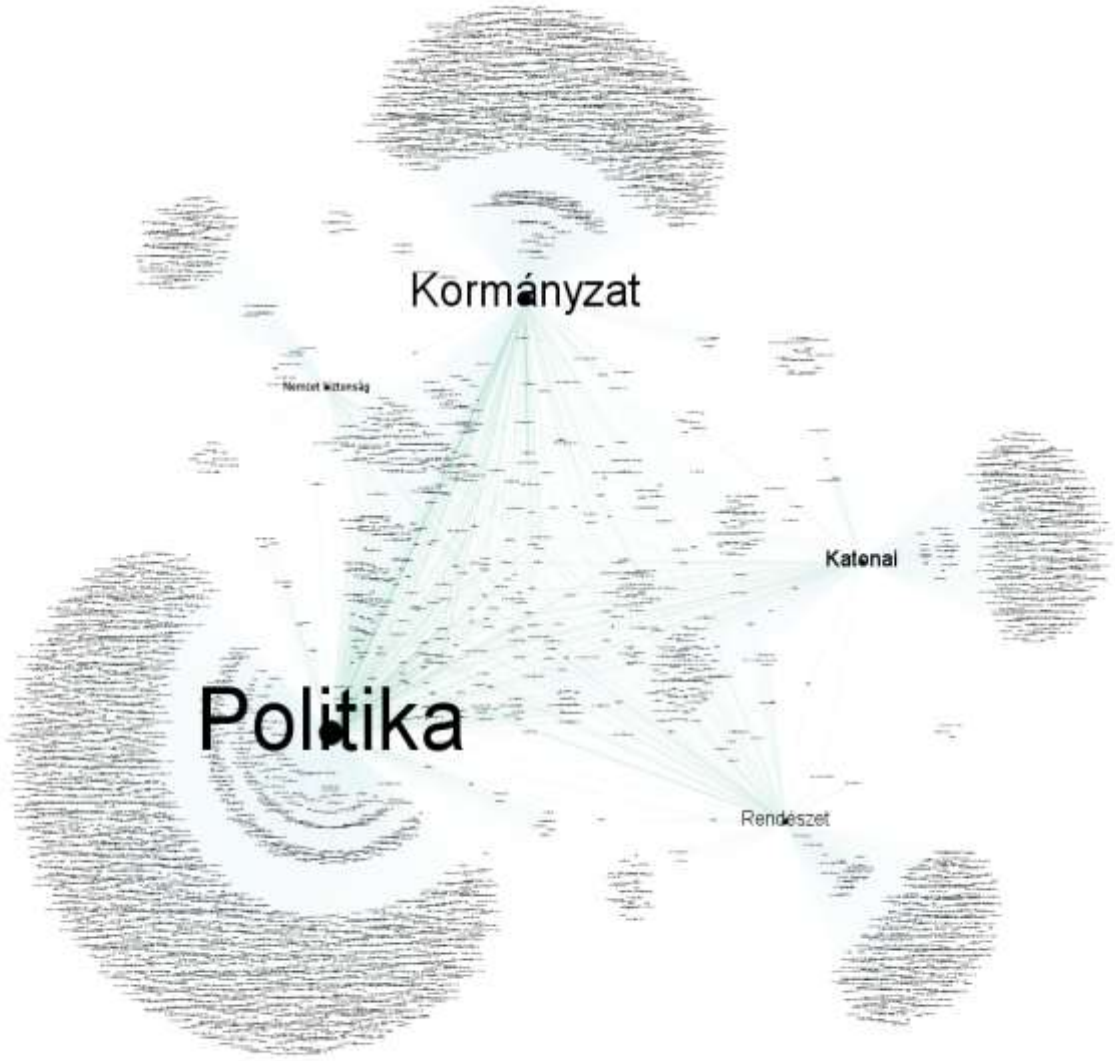
15. táblázat Leggyakoribb keresőkifejezések a közösségi média és politikai, illetve kormányzás keresésekre (saját szerkesztés, forrás: Scopus [35])

Helyezés	Politikai		Kormányzás	
	Kulcsszó	**darab**	**Kulcsszó**	**darab**
1	közösségi média	492	közösségi média	159
2	Twitter	145	e-kormányzás	41
3	politikai	137	kormányzás	40
4	Facebook	65	közösségi hálózat	18
5	Internet	50	Twitter	17
6	politikai kommunikáció	46	e-részvétel	15
7	politikai részvétel	44	web 2.0	15
8	közösségi hálózat	40	Facebook	13
9	választások	31	részvétel	9
10	közösségi mozgalmak	29	IKT	9

A 15. számú táblázat hasonló elven a kormányzás (összesen 1945 kulcsszó) és politikai (összesen 5008 kulcsszó) kulcsszavakat veszi alapul. A 14. és 15. számú táblázat összehasonlításából kiolvashatjuk, hogy míg a kormányzás és politikai esetében kapott kulcsszavak, például politikai részvétel, politikai kommunikáció, e-kormányzás, közösségi

mozgalmak stb. inkább társadalomtudomány kérdésekkel kapcsolatosak, addig a katonai, rendészeti, nemzetbiztonsági területen például a big data, természetes nyelvek feldolgozása, adatbányászat inkább a műszaki területeken kutatott témák.

Érdemes megvizsgálni, hogy az egyes kulcsszavak milyen gyakorisággal jelentkeznek az általam vizsgált öt kutatási területen. Ennek érdekében hálózatelemzés alá vetettem a kapott 8790 kulcsszót, aminek az ábrázolását a Gephi nevű alkalmazással végeztem el (lásd 15. számú ábra). Az ábrán az öt kutatási terület látható, mint a háló csomópontjai, illetve a hozzájuk kapcsolódó kulcsszavak adják a háló éleit. Az egyes kutatási területek erősségét a hozzájuk kapcsolódó kulcsszavak száma adja, ebből látható, hogy a politikai és kormányzati kutatási területek estében tapasztaljuk a legtöbb kulcsszót. Több kulcsszó esetén találunk olyan kulcsszavakat, amelyek mind az öt kutatási terület esetében előfordulnak, ezek kapcsolatát a háló közepén láthatjuk. Azokat a kulcsszavakat, amelyek csak az egyik kutatási területhez kötődnek, a csomópontok körül láthatjuk. Mindez az egyes kulcsszavak vizsgált területek szerint megoszlásában érdekes, melyek azok a területek, amelyek az egyes vizsgált területek esetében közös kutatásként azonosíthatóak, hiszen feltételezhetjük ez alapján az adott téma relevanciáját.



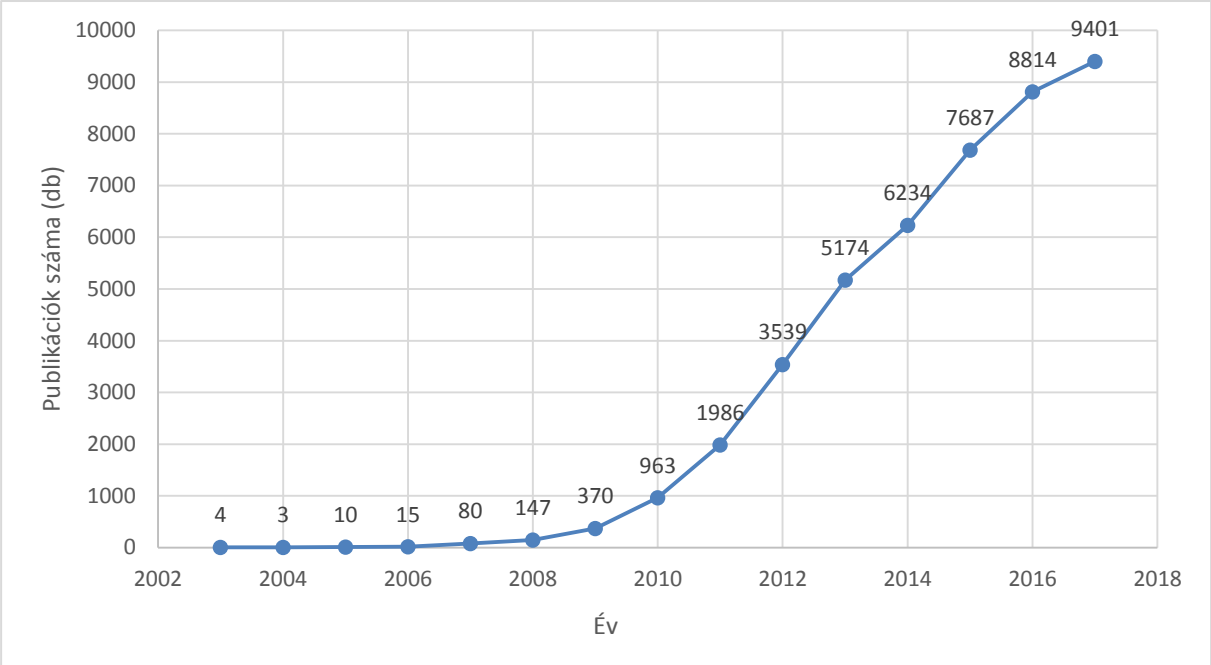
15. ábra A kulcsszavak kapcsolódása az öt vizsgálati területen (saját szerkesztés, forrás: Scopus [35])

A 15. számú ábrán a nagyszámú kulcsszavak okán az egyes kulcsszavak nem olvashatóak ki, csupán a megoszlásukat jelzik, ezért a 16. számú táblázatban feltüntettem a 10 leggyakoribb kulcsszót, amely mind az öt vizsgálati terület esetén releváns. A táblázat érdekessége, hogy a Facebook nem szerepel rajta. Ahogy a 14. és 15. számú táblázatok esetében is megfigyelhető volt, a Twitter gyakoribb kulcsszó (a katonai kutatásokat leszámítva) a vizsgálati területek esetében. Ez azért is figyelemreméltó, mert a Facebook napi elérést illetően jelentősen magasabb statisztikai adatokat mutat globálisan, mint a Twitter.

*16. táblázat A 10 leggyako**ribb kulcsszó az öt vizsgálati területen (saját szerkesztés, forrás: Scopus [35])***

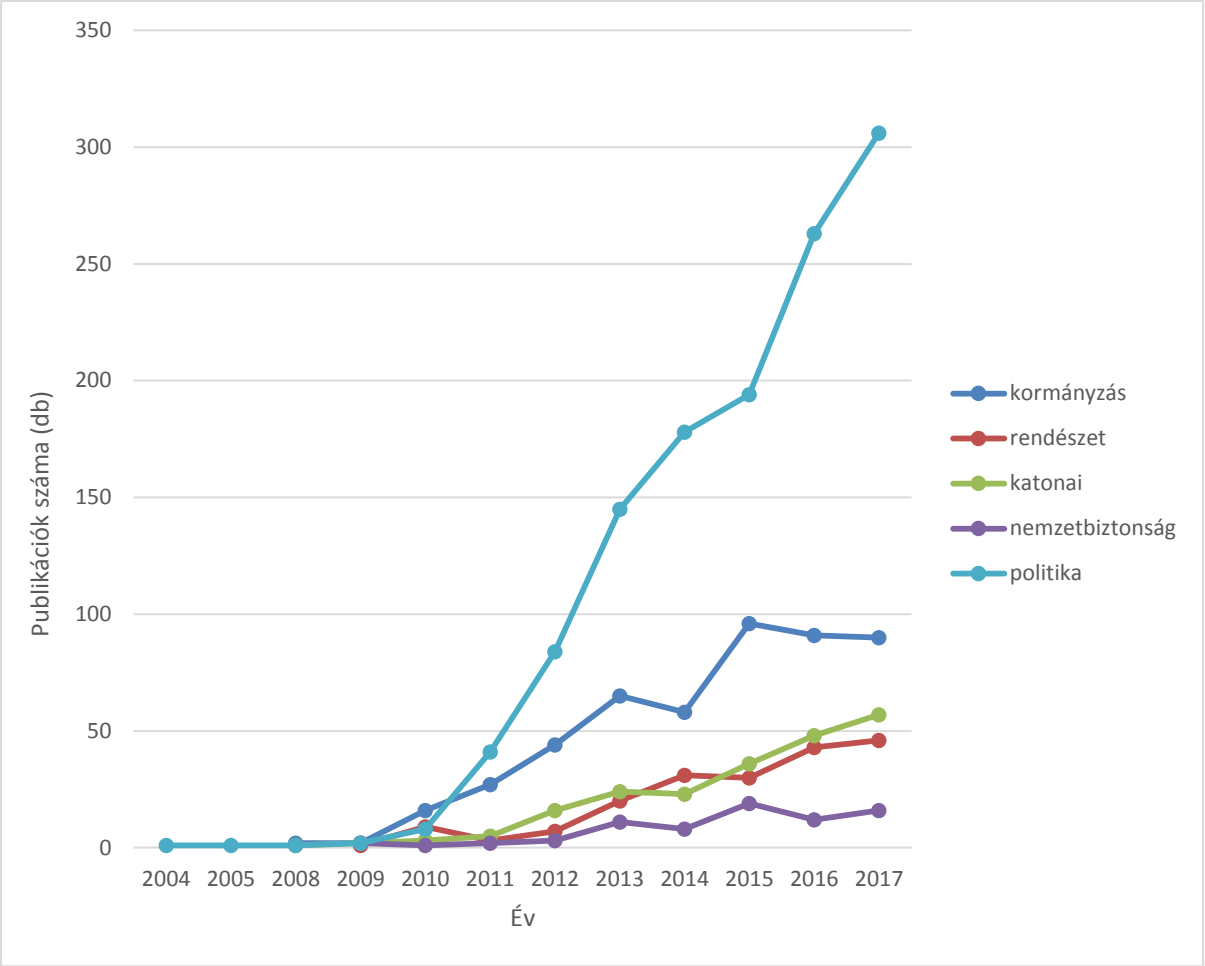
	Politika	**Kormányzás**	**Katonai**	**Rendészeti**	**Nemzetbiztonsági**	**Végösszeg**
Közösségi média	492	159	53	63	28	795
Twitter	145	17	5	18	8	193
Közösségi hálózat	40	18	4	4	2	68
Internet	50	6	2	4	1	63
Közösségi mozgalom	29	7	1	1	1	39
Big Data	16	8	1	10	3	38
Youtube	18	3	1	2	1	25
Adatbányászat	10	1	3	4	3	21
Megfigyelés	6	2	1	6	3	18
Újságírás	13	2	1	1	1	18

A H1 hipotézisem, hogy a közösségi média új multidiszciplináris szakterület. Úgy gondolom, hogy a téma multidiszciplináris jellegét alátámasztottam tudománymetriai elemzésekkel. Vizsgálatom következő fázisa az újszerűségére vonatkozik. A Scopus adatbázisa a 46311 találatot a közösségi keresőkifejezésre 1941-ig vezeti vissza, azonban ez, illetve a következő évtizedekben használt social media fogalom nem egyezik meg az általam vizsgált definíció tartalmával. Először ezzel kapcsolatos tanulmányt 1998-ban jelenít meg az oldal, „Social Media and the New Organization of Government Communications: An Empirical Analysis of Twitter Usage by the Dutch Police" címmel, ami azonban téves, hiszen a Twittert 2006-ban alapították. Szintén hibás a következő releváns találat, a 2000-es publikációs dátummal megjelenített, egyébként japán nyelven készült „Design of testimony Archives with users' activity of information sharing on Social Media" című tanulmány, ugyanis a felhasznált irodalomban 2010-es és 2012-es művek szerepelnek. Kiszűrve az ehhez hasonló téves találatokat, az első valóban releváns tudományos közlemény a 2003-ban megjelent „Someone: A cooperative system for personalized information exchange" címet viselő konferencia kiadvány. Ennek megfelelően 2003-tól vizsgáltam az egyes publikációk trendjeit. A 16. számú ábrán látható, hogy 2003 és 2006 között egy kisebb stagnálás volt megfigyelhető, de 2007-től kezdve 2013-ig minden évben duplázódott a publikációk száma az előző évhez képest- kivéve 2010-ben, ekkor megháromszorozódott. 2014-től továbbra is éves szinten ezernél nagyobb növekedés figyelhető meg.



16. ábra Közösségi média publikációk száma 2003-2017. (saját szerkesztés, forrás: Scopus [35])

Megvizsgáltam a publikációk számának alakulását az öt általam vizsgált területen. A 17. számú ábrán látható, hogy az első publikáció a témában 2004-ből származik a politikai vizsgálati területéről. Katonai és kormányzás vizsgálati területről 2008-ban, míg rendészeti és nemzetbiztonsági vizsgálati területén 2009-ben jelentek meg az első tudományos közlemények. Az eredmények azt mutatják, hogy a témával foglalkozó kutatások, leszámítva a politikait, egy évtizedes múltra tekintenek vissza, ami értékelésem szerint újként nevesíthető.



17. ábra Publikációk számának alakulása az öt vizsgálati területen (saját szerkesztés, forrás: Scopus [35])

A H1 hipotézisem harmadik megállapítása a szakterületre vonatkozik. A Scopus tudományterületi és tudományági besorolása között nem található meg a közösségi média, ebben a SciVal nevű adatbázis nyújtott segítséget. A SciVal a közösségi médiát kutatási szakterületként határozza meg. Az adatbázis kataszterekbe sorolja azokat a kutatási szakterületeket, amelyek együtt jelennek meg. Egy-egy kataszter 3 szakterületből áll egybe. Ily módon 220 tételből álló adatbázist kaptam. Kiszűrtem belőle azokat a kataszterekt, amelyekből a másik két szakterület nem kapcsolódik semmilyen módon az általam vizsgált öt területhez. Ez alapján 20 tételből álló listát kaptam (lásd 17. számú táblázat). Az egyes kataszterek esetében nem láttam értelmét, hogy hozzárendeljem az öt terület egyikéhez, ugyanis több esetben átfedés állapítható meg. A lista egyik fő érdekessége, a politikai rendszerváltások felülreprezentáltsága, négy esetben az Arab-tavasszal kapcsolatos kataszterekt találunk, illetve egy esetben az ukrajnai változások jelennek meg, ami a teljes lista egynegyede. A szakterületi kataszterek száma, igazolja, hogy a közösségi médiával és a védelmi szférával kapcsolatos kutatások nem csak újnak tekinthetőek, de legitimálják is az ezzel kapcsolatos kutatásokat.

17. táblázat Közösségi média és a kapcsolódó kutatási szakterületek (saját szerkesztés, forrás: SciVal [37])

Sorszám	Kutatási szakterület
1	arab; arab világ; közösségi média
2	arab; közösségi média; forradalom
3	bűnözés; közösségi médián való kommunikáció (online); közösségi média
4	krízis; oktatás; közösségi média
5	katasztrófa; szétterjedés; közösségi média
6	Egyiptom; arab; közösségi média
7	munka; közösségi média; politikai gazdaságtan
8	jog; adatbiztonság; közösségi média
9	katonaság; közösségi média; technológia
10	biztonság; demokrácia; közösségi média
11	Szerbia; biztonság; közösségi média
12	közösségi média; forradalom; civil társadalom
13	közösségi média; twitter; választási kampány
14	spanyol polgárháború; poszterek; közösségi média
15	technológia; közösségi média; adatbiztonság
16	Tunézia; arab; közösségi média
17	Ukrajna; tüntetés; közösségi média
18	erőszak; kriminológia; közösségi média
19	VIP; politika; közösségi média
20	háború; kép; közösségi média

KÖVETKEZTETÉSEK

A fejezetben bemutattam a közösségi média kialakulását és trendjeit. A közösségi média használatra vonatkozó trendek igazolták a témával kapcsolatos kutatások relevanciáját. Megvizsgáltam tudománymetriai elemzést alkalmazva a közösségi média megjelenését a nemzetközi tudományos publikációk tekintetében. Az elemzés alátámasztotta a kutatási szakterület inter- és multidiszcuplináris megközelítésének fontosságát. A vizsgálatomat leszűkítettem a védelmi szféra általam meghatározott öt területére: katonai, rendészeti, nemzetbiztonsági, politikai és kormányzás részekre. Elemeztem, hogy a különböző tudományos közlemények milyen tudományterületekhez kapcsolódnak. Ez alapján **igazoltam, hogy a közösségi média a humán- és műszaki tudományterület közös szakterülete, amely a hadtudományi kutatásokban dominánsan a műszaki tudományterülethez kapcsolódik.** Mindezt erősítette a tudományos közleményekhez kapcsolódó kulcsszavak analízise, amelyek segítségével megállapítottam azokat az egyes vizsgálati területekhez kapcsolódó főbb kutatási témákat, amelyek a közösségi média védelmi szférával kapcsolatos kutatásaisban jellemzőek. A kulcsszóanalízis egyben az öt vizsgálati terület közti kapcsolatot is meghatározta. Ez egyben

a tudományos problémák között megfogalmazott kettősséggel is összefüggésbe hozható, hiszen egy adott kutatási téma több diszciplína kapcsán lehet releváns. Ennek 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 fontos.

II. FEJEZET

A KÖZÖSSÉGI MÉDIA, MINT AZ INFORMÁCIÓS HADSZÍNTÉR SPECIÁLIS TERÜLETE

Az I. fejezet eredményei értelmezésem szerint alátámasztják a közösségi médiának a védelmi szférában történő elhelyezését, és ilyen irányú vizsgálatának szükségességét. Jelen fejezetben a közösségi média egy újszerű interpretálására teszek kísérletet. A kulcsszó elemzés azért is hasznos, mert trendelemzés segítségével kimutatható, milyen kutatási témák jelentik a fő sodort, amiből feltételezhetjük, azok a témák aktuálisak valamilyen okból kifolyólag. Egy, a kiberbiztonsággal kapcsolatos másik kutatásomban például érdekes volt látni, 2013 után, vagyis a Snowden-iratok nyilvánosságra hozatalát követően hogyan nőtt meg az adatbiztonsággal kapcsolatos kutatások száma. Az általam elvégzett kulcsszó elemzés a 219 „social media” és „military” találatra a 10 év vonatkozásában nem tekinthető nagy mintának, így nem jelzi olyan élesen az évenkénti változást, de így is találunk bizonyos gyakrabban előforduló kulcsszavakat, pl. 2012-t követően az „arab tavasz” vagy 2014-től az „Ukrajna” keresőkifejezés gyakoribb előfordulását. A 9. számú táblázatban bemutattam a 10 leggyakoribb keresőkifejezést a „social media” és „military” párosításban, amely felsorolásban az „információs műveletek” négy alkalommal is előfordult.

E fejezet célja, hogy a közösségi média új típusú megközelítését adjam, bizonyítani kívánom, hogy a közösségi média felfogható az információs hadszíntér egy speciális területeként. Azt, hogy a közösségi média jelentős szerepet tölt be az információs műveletekben, több szerző is érintette. A témában megítélésem szerint Drew Herrick jutott a legközelebb a 8. CyCon konferencián tartott előadásában, amelyben felvázolta a közösségi média információs műveletekben betöltött szerepét [38]. A fejezetben egy Herricknél komplexebb interpretációt kívánok adni.

2.1. A kibertér, mint hadszíntér kialakulása

A közösségi médiát, mind hadszínteret nem értelmezhetjük önmagában, szükséges a kibertérnek, mint hadszíntérnek a komplex vizsgálata, hogy ebből levezethessük azokat a speciális jellemzőket, amelyek a közösségi médiára, mint speciális tartományra érvényesek.

Doktori értekezésem prekoncepciója, hogy a közösségi média az információs hadszíntér speciális tartományaként is értelmezhető, ami az általa végrehajtható műveletekkel egyúttal kijelöli kereteit. Ennek igazolásához azonban első ízben értelmezni szükséges magának a kibertérnek a kereteit, illetve a hadtudományban, katonai műszaki tudományokban való megjelenését. A hadtudomány vagy katonai műszaki tudmányok önálló diszciplínaként a Magyar Tudományos Akadémia tudományági besorolásában jelenik meg önálló tudományágként, a nemzetközi tudományos nómenklatúrában – például az SJR által alkalmazott felosztásban- nem találhatóak meg önálló tudományágként, az ezzel kapcsolatos tudományos kutatások gyakran más tudományágak részterületei.

A kibertér kifejezés először William Gibson sci-fi író munkásságában jelent meg 1982-ben az Izzó króm című novellájában, de az 1984-es Neurománc című regénye volt az, amelyik a közbeszéd részévé tette. Gibson a kibertér fogalma alatt hálózatba kapcsolt számítógép-terminálokról közvetlenül elérhető digitális teret értett. Maga a kibertér kifejezés a görög kyber (hajózni) szóból származik, és hajózásra alkalmas teret jelent. Gibson regényei óta különböző fogalmi meghatározások születtek a kibertérre, de földrajzi értelemben az infokommunikációs technológiákban megnyilvánuló térfogalmat jelent, nem pedig a technológiára utal [39].

A kibertér térszerkezetének leírására számos kísérlet született geometriai, formai, szerkezeti jellemzőinek meghatározásával. A térgeometriai jellemzők feltárása azonban nem egyszerű, hiszen a kibertér számos különböző, eltérő funkciójú tartományból tevődik össze, illetve mindegyike mesterségesen konstruált. A különböző térfelfogásokat az alapján alkották meg, hogy a fogalom használói a kibertér mely csoportjával foglalkoztak [40]. Ez alapján beszélünk:

- koncepcionális térfelfogásról, ez esetben az IKT önálló belső terét értjük, az internetet és annak alkotó térrészeit, pl. e-mailek tere, a fájl átvitel tere. Ebben az értelmezésben az internet az abszolút kibertér.
- infrastrukturális térfelfogásról, e felfogás alapján a kibertér leginkább fizikai megközelítése áll, azokat a háttérben meghúzódó infrastrukturális elemeket értik, amelyeken a virtuális interakciók lezajlanak- szerverek, gerincvezetékek, optikai kábelek stb.
- oldal térképek terei, nagyban hasonlatos a könyvekben található tartalomjegyzékekhez. Az oldal térképek egyfajta modellezési eljárások, a honlapokon elhelyezett útmutatók, amelyek a honlap tartalmában segítenek

eligazodni a felhasználóknak. Ez esetben már nem beszélhetünk semmiféle fizikai leképzésről, földrajzi lokalizációról, kizárólag a virtuális térben értelmezhető azáltal.

- a sajátos „páva" modellek terei, az egyik legelvontabb térfelfogás, amelynek a lényege, hogy egy nyomkövető eljárással az információs csomagok útvonalát követik a hálózatban (kiindulási ponttól a célig), majd ezeket vizuális módon faszerkezethez vagy pávatollhoz hasonló ábrán jelenítik meg. Az eljárás célja, hogy az internet belső szerkezetét térképezze fel. Maga a páva térkép az internethez hasonlóan folyamatosan változik, hol bővül, hol szűkül, így a teljes feltérképezés megoldhatatlan feladatnak bizonyul. A páva modell térszerkezet már önálló belső teret alkot, híján minden fizikai kapcsolatnak.
- virtuális világok, maga a fogalmom egy erőteljes szűkítés az internethez képest, digitális technológiával létrehozott világot jelent, az általa képzett perceptualitást értjük alatta. Megalkotása mögött az az egyszerű igény húzódik meg, hogy az információ könnyebben kezelhetővé váljon. Sajátosságának tekinthető, hogy a digitális környezetben a felhasználó is jelen van. A virtuális valóság eszköze lehet pl. az okosszemüveg.

A kibertér szakít a klasszikus térfelfogással, hiszen nem képes értelmezni számos fizikai alapvonást, amelyek hatására a tér halmazt alkot, azonban bizonyos térszerkezeti elemek mégis kimutathatóak benne, ami által teljesen új interpretációt jelent a virtuális térben. Ilyen kategóriaként értelmezhető a külső és belső tér, a hely, a helyzet, a távolság, az irány, a határ, illetve a különböző szintek.

Mészáros Rezső A kibertér társadalomföldrajzi megközelítése [39] című munkájában különböző viszonyrendszereket jellemez, a kibertér és az egyén, a társadalom, a politikai-, gazdasági alrendszerek kapcsolatában. Az elmúlt évtizedben azonban kialakult a kibertér, mint hadszíntér értelmezése.

A kibertér fogalmának a meghatározására a magyar stratégiai gondolkodásban viszonylag korán születtek kísérletek. A magyar kormányzat az Európai Unió tagállamainak élmezőnyébe tartozott, amikor a 2010-es évek elején megalkotta azokat a stratégiákat, jogszabályokat, amelyek a kibertérrel kapcsolatos kockázatok felmérését, kezelését hivatottak ellátni. A 2012-ben megalkotott Magyarország Nemzeti Kiberbiztonsági Stratégiája új alapokra helyezte Magyarország kibervédelmét [41]. A stratégia a következő megfogalmazást

tartalmazza: „*A kibertér globálisan összekapcsolt, decentralizált, egyre növekvő elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti*.” [42] A Magyar Honvédség Kibervédelmi Szakmai Koncepciója megfogalmazásában a kibertér: „*az elektromágneses spektrum használatával meghatározató, dinamikusan változó tartomány, mely összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál*” [43].

Komplexebb megközelítését adja a kibertérnek Haig Zsolt. A szerző megállapítása szerint „*egyértelműen kijelenthetjük, a kibertér fontos jellemzője, hogy abban az elektromágneses spektrumot felhasználva és/vagy vezetékes kapcsolaton keresztül hálózatba kötött infokommunikációs rendszerek működnek, amelyek különböző elektronikus információkezelési tevékenységeket (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, adattárolás, kommunikáció stb.) végeznek. A különböző hálózatba kapcsolt infokommunikációs rendszerek az információs környezet azon tartományát használják, amelyben e rendszerek működnek, léteznek (fizikai dimenzióban), a különböző elektronikus információkezelési folyamatok zajlanak (információs dimenzióban), valamint e rendszerek elleni tevékenység és védelem megvalósul (fizikai és információs dimenzióban). Ebből következően tehát a kibertér az információs környezet fizikai és információs dimenziójában értelmezhető.*” [44] A kibertér jellegének, összetevőinek, szereplőinek vizsgálatát látja el Munk Sándor A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései című munkájában [45], amely rávilágít a fogalom eltérő használatából fakadó problémákra. Az egyes szereplők eltérő fogalmi készlete nehezíti a kibertérből fakadó kockázatok együttes kezelését, ezért fontos lenne a fogalmi interoperabilitás megteremtése.

Véleményem szerint, hogy mit értünk a kibertér fogalma alatt, milyen térfelfogásként gondolkodunk róla, miket azonosítunk az összetevőiként nagyban kapcsolódik a kibertér védelméhez. Teljesen más védelmi mechanizmusokat kell alkalmaznunk a koncepcionális, illetve az infrastrukturális térfelfogás esetében, hisz míg előbbi alapvetően az internetet érti a kibertér alatt, addig az infrastrukturális értelmezés esetében a védendő entitások a fizikai térben is jelentkeznek, amely teljesen eltérő védelmi megoldásokat követel meg. Ennek igazolására az óceánok fenekén megtalálható távközlési kábelek kiváló példával szolgálnak, ezek védelme több alkalommal a NATO nyugtalanságát idézte elő, amikor orosz tengeralattjárók rendszeresen megközelítették 2017 decemberében. Az Atlani-óceán északi részén lefektett kábelek felelnek Észak-Amerika és Európa között az internetes kommunikáció biztosításáért.

Nem nehéz belátni, egy célzott támadással, ami diszfunkciót okoz a távközlési kábelekben, óriási károkat lehet okozni.

Az Észak- Atlanti Szövetség (továbbiakban NATO) esetében a kibervédelem hangsúlyos megjelenése a stratégiaalkotásban első alkalommal a Lisszabonban 2010. novemberében megtartott csúcstalálkozóhoz köthető [46]. Az Afganisztánban folytatott háború kezdetétől visszatérő kérdés, hogyan biztosítsák a NATO cselekvőképességét azokon a területeken, amelyek bár nem tartoznak a Szövetség illetékessége alá, de a mindennapok, különösen a műveletek során nagy mértékben függ tőle [47]. A Szövetséges Transzformációs Parancsnokság (továbbiakban ACT) parancsnoka, Abrial vezérezredes utasítást adott ki a stratégiai elemzőrészlegnek egy tanulmány elkészítésére, amelyben feltárja a NATO sebezhetőségét a globális közös tereken. A 2011 áprilisában megjelent „Assured Access to the Global Commons" [48] címet viselő tanulmányt a Szövetséges Transzformációs Parancsnokság parancsnoka, Mark Barett vezérőrnagy, Dick Bedford, Elizabeth Skinner és Eva Vergles jegyzik. Az igazán jelentős lépésnek azonban a 2016-os varsói csúcstalálkozó jelentette a NATO stratégiaalkotási folyamatában, ugyanis a kiberteret a Szövetség az ötödik hadszíntérként ismerte el, valamint a kibervédelmet beemelte a NATO kollektív védelmi feladatai közé [49] [50].

A NATO által használt globális közös tereket a nemzetközi jog szabadon használható terület, avagy res communis omnium usus fogalmával írja le. Ennek lényege, hogy az államok felségjoga csak bizonyos távolságig terjed, ha meghaladják ezt a meghatározott távot, nem érvényesíthetik joghatóságukat. A szabadon használható terek hatályába tartozik a világűr, az Antarktiszt, a tengerfenék és a nyílt tenger.[26] A hivatkozott tanulmányban azonban a korábbi földrajzi kategóriák, mint a tengerek és óceánok, légtér és világűr kibővülnek a virtuális dimenzióval, a kibertérrel. A globális közös terekben tehát nem értelmezhető az államok szuverenitása, azonban számos olyan biztonsági kockázat forrását jelentik, amelyek jelentősként értékelhetőek a NATO és tagállamai szempontjából.[27] Azonban nem csupán a globális közös terekből fakadó biztonsági kihívások miatt fontos a megfelelő szintű védelme, a NATO a különböző műveletei során aktívan használja e területek mindegyikét, legyen szó pl. csapatok mozgatásáról szárazföldön, tengeren, levegőben, kommunikáció biztosításáról, a vezetés-irányítás fenntartásáról a kibertérben, a világűrben. Fontos szempont továbbá a

[26]A tengerparti államhoz tartozik a partja mentén elterülő sáv, ami a parttól számított 12 tengeri mérföldet (kb. 22,2 km) foglalja magába.
[27] A megállapítás természetesen érvényes minden olyan államra is, amely nem tagja a NATO-nak.

tagállamok érdekeinek védelme, ami többek között a kutatás-fejlesztésben, távközlésben vagy a kereskedelemben jelenik meg. Annak érdekében, hogy a NATO képes legyen a globális közös terekben ellátni feladatait, jelentős felderítő, stratégiai elemző, tervező, vezetési, képességfejlesztési, logisztikai és műveleti előkészítő tevékenység ellátását, összehangolását követeli meg. Bár mind a négy közös tér esetében találunk azonosságot, ezért összekapcsolódnak, átfedik egymást (lásd pl. a vezetés-irányítás fenntartását), de mindegyik egyben rendszerspecifikus jellemzőkkel is leírható. Jelenleg a NATO nem rendelkezik a globális közös terekre vonatkozó egységes stratégiai elképzeléssel, de az egyes dimenziók tekintetében már megfogalmaztak eseti állásfoglalásokat, irányelveket.

Az információs tevékenységek, annak okán, hogy mindent átszőnek az infokommunikációs technológiák, az információs környezetben, vagyis az úgynevezett információs színtéren zajlanak. Az Egyesült Államok összhaderőnemi információs műveletek doktrínájának megfogalmazása alapján „*az információs környezet mindazon egyének, szervezetek és rendszerek összessége, akik és amelyek az információ gyűjtésével, feldolgozásával, szétosztásával foglalkoznak*.” [51] Az információs környezet megjelenése a katonai műveletek kibővítésével járt, ami új tartományokkal egészítette ki [52]. Ebből következően a hadszíntér fizikai dimenziója kiegészült egy nem földrajzi dimenzióval, ami létrehozta a katonai információs környezet, vagyis kialakult az információs hadszíntér. Az információs hadszíntér nem egyenlő a kibertérrel. Ezen a hadszíntéren végzett műveleteket, amelyek az információ megszerzéséért, megtartásáért, hatékony felhasználásáért folytatnak, információs műveleteknek nevezzük. A fogalmat korábban információs hadműveletként is használták, civil szóhasználatban mai napig jellemző, azonban a katonai szakterminológia a NATO esetében az információs műveletekként nevesíti a tevékenységet. A médiában az információs hadviselés és információs műveletek közti különbséget az elérendő célban választják el általában, az információs hadviselés civil célok elérésére (például gazdasági, politikai célok), addig az információs műveletek katonai célok elérésére vonatkozik. Ez azonban véleményem szerint nem mérhető kategória, nem azonosíthatjuk az egyes célokat önmagában, hogy civil vagy katonai célok megvalósítására végzik-e a tevékenységet. Gazdasági, politikai nyomásgyakorlás ugyanúgy lehet katonai cél, ebből következően én egységesen az információs műveletek fogalmát használom értekezésemben, összhangban a NATO szakterminológiájával.

Maga az információs jelző nem csupán arra a tevékenység ellátásra utal, hanem arra is, hogy a hagyományos katonai műveleteket végzése az infokommunikációs technológiák

használatával valósul meg. Az információs hadszíntér magában foglalja a valós és virtuális tereket, eszközöket, helyeket, rendszereket, amelyekben az információ megszerzésével, előállításával, felhasználásával, értékelésével, elemzésével, felhasználásával, védelmével foglalkoznak.

Ebből következően az információs hadszíntér a hadszíntér egy speciális tartománya, amelyen belül a szemben álló felek az információ birtoklásáért, a másiknál hatékonyabb felhasználásáért versengenek. Ily módon az információs műveletek célja egyrészt az információs fölény kialakítása, végül a vezetési fölény megszerzése,[28] másrészt pedig az időcsökkentés elérése a saját oldali vezetési folyamat számára, addig az ellenfél számára az időnövelés.

Az információs műveletek tevékenységi körét hat részre osztjuk:

- lélektani műveletek;
- elektronikai hadviselés;
- dezinformáció;
- információs célpontok fizikai pusztítása;
- műveleti biztonság;
- számítógép-hálózati műveletek [53].

Megvizsgáltam a NATO információs műveletekkel foglalkozó doktrínáját (továbbiakban AJP-3.10) [54], ami az alábbi képességeket, eszközöket és eljárásokat határozta meg az információs célkitűzésekkel kapcsolatban:

- PSYOPS;
- megjelenés, viselkedés, arculat (Presence, Posture and Profile, továbbiakban PPP);
- műveleti biztonság (Operations Security, továbbiakban OPSEC);
- információbiztonság (Information Security, továbbiakban INFOSEC);
- megtévesztés (Deception, továbbiakban MILDEC);

[28] Haig Zsolt megfogalmazását kölcsönözve: „*Az információs fölény a két szembenálló fél közötti relatív viszonyt jelenti, amely felhasználható a saját célok, érdekek másik félnél eredményesebb érvényesítésére. […] a végcél a vezetési folyamatban jelentkező vezetési fölény elérése. Az információs fölény alapvető funkciója tehát, hogy kedvező információs helyzetet, tudástöbbletet teremtsen a vezetési fölény kialakításához. A vezetési fölény egyrészről a szembenálló felek vezetési folyamatai között minőségi különbséget jelent: az egyik fél tevékenységét meghatározó intézkedések, utasítások tartalma és időbelisége lényegesen jobban tükrözi a kialakult helyzetet és az ahhoz alkalmazódó célszerű cselekvésmodellt, mint a másiké. Másrészről azt az állapotot fejezi ki, amikor ugyanezen fél végrehajtói eltökéltsége az utasítások teljesítésére azonos vagy nagyobb, mint a másik fél (társadalom) tagjaié.*” [52]

- elektronikai hadviselés (Electronic Warfare, továbbiakban EW);
- fizikai pusztítás (Physical Destruction, továbbiakban PD);
- kulcsfontosságú vezetőkkel kapcsolatos tevékenység (Key Leader Engagement, továbbiakban KLE);
- számítógép-hálózati műveletek (Computer Network Operations, továbbiakban CNO);
- CIMIC.

Az információs műveleteket egyaránt alkalmazzák támadó vagy védelmi célból, annak érdekében, hogy hatást váltson ki a katonai, gazdasági, politikai alrendszerben. A támadó jellegű információs művelet esetében a cél, hogy a speciális érdekekre vagy speciális fenyegetésekre választ adva gyakoroljanak hatást az ellenfélre, akár békében, válságban vagy konfliktus idején. Ezzel szemben a védelmi információs művelet során a cél, hogy megvédjék a saját információkat, valamint fenntartsák az információkhoz való hozzáférést, illetve elősegítsék az információs rendszerek hatékony használatát.

2.2. A kibertér nemzetközi és hazai stratégiai fejlődése

A kibertér, mint ötödik hadszíntér NATO által történő elismeréséhez relatíve hosszú út vezetett. A terület jogilag szabályozatlan mivoltára a 2007-ben lezajlott orosz-észt kiberháború hívta fel a figyelmet. Azonban nem ez volt az első eset, amikor a NATO vagy egy tagállam ellen követtek el kibertámadást, az első eset 1999-re nyúlik vissza, amikor az ENSZ Biztonsági Tanácsának felhatalmazása ellenére a NATO katonai műveletek végrehajtásába kezdett. Válaszul a Fekete Kéz nevű szerb hackerek a NATO weboldalai ellen szolgáltatásmegtagadással járó támadásokat (továbbiakban DoS) indítottak, nem egy esetben elérhetetlenné téve így azokat. Emellett politikai üzeneteket helyeztek el feltört kormányzati honlapokon. A NATO parancsnoki szervereibe való betörési kísérletük egy alkalommal eredménnyel járt, amikor is a légierő informatikai hálózatába sikerrel behatoltak, bár ekkor sem sikerült minősített adatokhoz hozzáférniük. A támadások a belgrádi kínai nagykövetség bombázása után kibővültek kínai és orosz hackerek csatlakozását követően.

Ezek a tapasztalatok indították útjára a NATO kibervédelmi politikájának fejlődését [55]. A 2007-ben a NATO tagállam Észtországot ért kibertámadás felgyorsította az eseményeket [56]. Észtország kormánya úgy döntött 2007 áprilisában, hogy eltávolít Tallinból

egy második világháborús szovjet hősi emlékművet. Észtországban nagy számú orosz kisebbség él, amely körében a lépés nagyfokú tiltakozást váltott ki, tüntetések, zavargások törtek ki. Április 26-27-én túlterheléses támadásokat indítanak Észtország kormányzati rendszerei ellen, beleértve a Parlament, az elnök és a miniszterelnök rendszereit és oldalait is. A kormányzati rendszerek mellett az észt pénzügyi rendszer, valamint a média is a támadók célkeresztjébe kerül. A közel egy hónapig zajló támadássorozatban 128 túlterheléses támadás történt, 2-10 órás időtartamú túlterheléses támadásokkal. A legsúlyosabb támadás a 100 Mbps sávszélességet is elérte, ami kiterjedt botnethálózatra utal. Az észt Parlament 4 napig internet nélkül maradt, a bankrendszer esetében pedig 24 órás teljes vagy részleges kimaradások történtek. A támadásban használt botnethálózatban több mint 170 országból tevődtek össze a támadó informatikai eszközök.

A támadás felkészületlenül érte a NATO döntéshozóit, így igyekeztek nem katonai támadásként értelmezni a történteket, hogy ne kelljen életbe léptetni a kollektív védelemről szóló 5. cikkely rendelkezéseit.

A 2008-ban lezajlott orosz-grúz konfliktus során a konvencionális hadviselés támogatására alkalmazott kiberhadviselés ráirányította a figyelmet az információs műveletek jelentőségére. 2008 januárjában elfogadták a NATO Kibervédelmi irányelvét, majd az április bukaresti csúcson foglalták először dokumentumba az informatikai biztonság fontosságát [57], illetve ezzel összhangban 2008 májusában megalapították a NATO Kooperatív Kibervédelmi Kiválósági Központját (továbbiakban CCD CoE), amelyhez Magyarország 2010-ben csatlakozott.[29] A CCD CoE nem a kibertámadással kapcsolatos feladatokat látja el, alapvetően kutató és oktató szerepe van. A Központ feladatai közé sorolhatjuk:

- a kiberhadviselés jogi szabályozásának támogatása, a nemzetközi jogba történő megvalósításának elősegítése;
- a tagállami kiberképességek kialakításának támogatása;
- a tagállami doktrínák, stratégiai koncepciók kidolgozásának támogatása;
- információbiztonsági tudatosság növelésére vonatkozó képzések, gyakorlatok[30] szervezése.

[29] A Központ székhelyéül Tallinnt választották, az Észtországot ért kibertámadás szimbólumaként.
[30] Ilyen például a Locked Shields gyakorlat, amelynek tesztgyakorlatában évek óta a Nemzeti Közszolgálati Egyetem Hadtudományi- és Honvédtisztképző Kar hallgatói is részt vesznek.

A CCD CoE mellett létrehozták a Kibervédelmi Hatóságot (továbbiakban CDMA), amelynek feladata többek között a sérülékenységvizsgálat, a feltárt hálózati sérülékenységek elhárításában való közreműködés, illetve a stratégiai együttműködés kialakítása az EU és a NATO társszervezetei között [58]. A CDMA a Kibervédelmi Tanács (továbbiakban CDMB) alárendeltségébe tartozik. A CDMB-hez kapcsolódva a Számítógépes Incidenskezelő Képesség Technikai Központnak (továbbiakban NCIRC TC) alárendelve alakították ki az ún. gyorsreagálású csapatot, amelyekhez nemzeti szinten kapcsolódnak a Számítástechnikai Sürgősségi Reagáló Egységek (továbbiakban CERT).[31]

A kibervédelmi politika szabályozásában a következő nagy lépcsőfok a már említett 2010-es stratégiai koncepció volt. Ezzel kapcsolatban indult el párhuzamosan az említett globális közös terek projekt kidolgozása. A Stratégiai Koncepciót kiegészítendő fogadták el a 2011-es brüsszeli védelmi miniszteri találkozón a Kibervédelmi Irányelvet, valamint a Cselekvési Tervet.

A NATO szervezeti változásával összhangban a kibervédelemmel foglalkozó szervezetek esetében is változások következtek be: legfontosabb politikai döntéshozó szervnek továbbra is az Észak-Atlanti Tanács maradt, azonban a megelőzéssel és incidensmenedzsmenttel kapcsolatos feladatok ellátásának döntő többségét a Kibervédelmi Hatósághoz utalták. A kibervédelemmel kapcsolatos technikai és végrehajtáshoz kapcsolódó feladatok végzéséért a 2012-ben létrehozott NATO Kommunikációs és Információs Ügynökség felel.[32] A kibervédelem integrált részét képezi a NATO védelmi tervezési feladatainak.

A 2012-es chicagói NATO csúcson a kibervédelemmel kapcsolatos feladatok továbbra is hangsúlyosak maradtak, az ezzel összefüggő képességek fejlesztését létfontosságúként ítélték meg. A két évvel később megrendezett walesi NATO csúcs egyik legfontosabb döntése a kibervédelmi képességek fejlesztése volt. A döntés értelmében a kibertámadást a jövőben a kollektív védelem hatálya alá tartozó cselekményként értékelik, mert értékelésük szerit lehet olyan mértékű, ami kiváltja a kollektív védelem elvét [59]. Ez alapján az Atlanti Tanács eseti alapon fog dönteni, hogy érvénybe lép-e az 5. cikkely kollektív védelméről szóló elve [60]. A walesi csúcson megerősítették továbbá, hogy a kibervédelmi képességek növelése érdekében szükséges az ipari együttműködés továbbfejlesztése is. A NATO 20 területet fejlesztését határozta meg a minimum képességeket illetően a kibervédelem tekintetében. Ilyen terület

[31] Hazánkban ezt a feladatot a Kormányzati Eseménykezelő Központ (továbbiakban GovCERT-Hungary) látja el
[32] A szervezet létrehozása egy újabb jelentős képességfejlesztés eredményeként valósult meg.

például a stratégia alkotás, az együttműködés, az oktatás, információbiztonság stb. Ahogy az előző alfejezetben már volt szó arról, a 2016-os varsói csúcson ezt a NATO hivatalosan is deklarálta. A varsói csúcs azonban fontos volt abban a tekintetben is, hogy megállapodás született az NATO és EU közötti együttműködésről [61], amelyben a kiberbiztonság hangsúlyosan is megjelent.

2016-ban a NATO tagállamok az úgynevezett „Cyber Defence Pledge" keretében kifejezték azt is, hogy elkötelezettek a kiber képességek fejlesztését illetően. Említeni szükséges továbbá a „Domain roadmap" PO (2017)0072-AS1 címet viselő dokumentumot, ami a kibertér hadszíntérnek a támadó kapacitásáról szól, ez a dokumentum azonban nem nyilvános. A varsói csúcson született döntés a Cyberspace Operations doktrína, vagyis az AJP-3.20-as kidolgozásáról, ami várhatóan 2018-ban készül el [62]. 2017 novemberében egy új, NATO Cyber Operations Centre létrehozásáról is döntés született [63].

A stratégiai dokumentumok mellett fontos azonban a nemzetközi jogi fejlődést is érinteni. Az Észtországot 2007-ben ért kibertámadást követően a NATO felkérésére kezdték el szakértők kidolgozni azt az ajánlást, amely a genfi egyezményt értelmezné a kibertérben. Így született meg a Tallini Kézikönyv, ami azonban nem egy hivatalos NATO dokumentum és nem is jogszabály, egyelőre csak irányelvek gyűjteménye, amelyet egyébként a Cambridge University Press adott ki [64]. Jelenleg még nem ratifikálták az országok, nem kerültek be a benne megfogalmazott irányelvek a nemzetközi szerződésekbe. A Tallini Kézikönyv több mint 300 oldalon, 95 fő szabályra lebontva részletesen tárgyalja az informatikai hadviselés szabályait, többek között kitérve arra, hogy a hagyományos fegyveres konfliktusokhoz hasonlóan el kell kerülni a civil áldozatokat, ennek jegyében például tilos a civil célpontok, különösen kórházak, atomerőművek, vízierőművek vagy gátak támadása, ezt egyébként a genfi egyezmények most is tiltják a hadviselő felek számára. A különösen nagy anyagi kárral járó kibertámadást is „casus belliként" tekinti a kézikönyv, illetve a támadó hackereket kombattásként, azaz legitim célpontként határozza meg [65]. 2017-ben jelent meg a Kézikönyv 2.0-s változata [66], amely kiegészítette az első kiadást többek között a szuverenitás, az államok felelősségének kérdésével, emberi jogi kérdésekkel stb [67].

A NATO kiberbiztonság stratégiájának fejlődése mellett fontos az Európai Unió ez irányú stratégiaalkotás folyamatának vizsgálta is, már csak azért is, hiszen jelentős előzményei azoknak az európai jogszabályoknak, amik az adat-, információ- és hálózatbiztonság szempontjából Magyarország normatív szabályozási környezetében is szerepet kap. A 2008-

ban kitört gazdasági és pénzügyi válság, a kibertérből származó fenyegetéseknek,[33] különösen a kiberbűnözés nagy arányú növekedése az Európai Unió döntéshozói számára is világossá tette, hogy a kibertérből származó új típusú kihívásokra erőteljes választ kell adni. Ez alapján készült el az Európa 2020 foglalkoztatási és növekedési stratégia [68], amely a 2020-ig tartó időszak intézkedéseinek alapdokumentumának tekinthető. Ennek keretében az Európai Bizottság hét kiemelt szabályozási területet azonosított, aminek a megvalósítása érdekében elkészítette az Európai Digitális Menetrend 2014–2020 stratégiáját [69]. [34] Az Európai Digitális Menetrend az alábbi célok megvalósulását tűzte ki:

- *„az egységes digitális piac megteremtése,*
- *az uniós adatvédelmi szabályozási keret felülvizsgálata,*
- *a távközlési szolgáltatások egységesítése,*
- *a fokozott interoperabilitás és szabványok,*[35]
- *a készülékek, alkalmazások, adattárolók, szolgáltatások és hálózatok átjárhatóságának növelése,*
- *a bizalom és az internetes biztonság megerősítése,*
- *a nagy sebességű és szupergyors internet-hozzáférés biztosítása,*
- *befektetés a kutatásba és az innovációba,*
- *a digitális jártasság, a digitális készségek és a digitális integráció előmozdítása,*
- *a technológia intelligens használatából eredő előnyök hasznosítása a társadalom számára.”*

A Digitális Menetrend hét beavatkozási pontja közül a „Biztonság és bizalom intézkedési területével” szükséges foglalkoznom. Ez alapján hat cél megvalósítását azonosíthatjuk, mint:

[33] Ne feledjük, nem sokkal a 2007-es észt-orosz kiberháború után vagyunk.

[34] Bár nem tartozik szorosan a kiberbiztonsági stratégiai fejlődés kérdésköréhez, azonban hatását illetően mégis fontos megemlíteni azt a 2017 év végétől zajló vitát az Európai Unió Parlamentje és Tanácsa által benyújtott javaslatról, ami a digitális egységes piac szerzői jogi kérdéseit szabályozná. [70] A javaslat ellen 85 szervezet fogalmazta meg tiltakozását [71], amely véleményük szerint cenzúrához, az emberi jogok és 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 javaslat ezen felül kiterjed a streaming szolgáltatókra, de a hírmegosztó oldalakra, de a tudományos publikációkra is.

[35] Az interoperabilitás az Európai Uniós kiberbiztonsági stratégiáiban történő megjelenéséről bővebben lásd Munk Sándor témában készült tanulmányát [72].

- *„javaslattétel az információs rendszerek elleni számítógépes támadások leküzdésére irányuló szigorúbb jogszabályokra, illetve a számítógépes bűnözésre vonatkozó joghatósággal kapcsolatos európai és nemzetközi szintű szabályokra;*
- *a számítógépes támadások elleni gyorsreagálású európai rendszer és ennek részeként a számítógépes szükséghelyzeteket kezelő csoportok hálózatának létrehozása, az Európai Hálózat- és Információbiztonsági Ügynökség szerepének megerősítése;*
- *javaslattétel olyan tagállami forróvonalak létrehozására, ahol a gyermekek és szüleik bejelentést tehetnek a jogellenes internetes tartalmakról;*
- *a tudatosságnövelés, a biztonságos internethasználat iskolai oktatása;*
- *a gyermekbántalmazással, a személyazonosság-lopással és a számítógépes bűnözéssel kapcsolatos válaszmechanizmusok kidolgozása;*
- *a magánélethez és a személyes adatok védelméhez való jog érvényesítése az interneten és azon kívül egyaránt [69].*"

Következő lépésként az Európai Parlament, a Tanács, az Európai Gazdasági és Szociális Bizottság és a Régiók Bizottsága által 2013-ban megalkotott az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér című uniós stratégiáját nevesíthetjük. A stratégia hat stratégiai prioritást és intézkedést fogalmazott meg:

- *„kibertámadásokkal szembeni ellenálló képesség megteremtése;*
- *a számítástechnikai bűnözés és a kibertámadások visszaszorítása;*
- *kibervédelmi politika kidolgozása és a kiberképességek fejlesztése;*
- *a kiberbiztonsághoz szükséges ipari és technológiai erőforrások biztosítása;*
- *a kibertérre vonatkozó egységes, nemzetközi szakpolitika kidolgozása, valamint az alapvetőuniós értékek terjesztése;*
- *számítógépes bűnözéssel foglalkozó nemzeti kiválósági központok hálózatának kialakítása és finanszírozása [73].”*

A kibervédelmi stratégiák meghatározzák az országok kibervédelmi feladatköreit, szervezeti rendszereit, illetve, hogy milyen célokat, irányokat követ. A NATO CCD CoE gondozásában megjelent nemzeti kiberbiztonsági keretrendszert bemutató kézikönyve az alábbi ajánlásokat fogalmazza meg a stratégiaalkotást illetően [74]:

- minden ország más, tehát egyéni kibervédelmi stratégiát kell kidolgozni;
- a stratégia csatlakozzon más szervezetek ajánlásaihoz, stratégiáihoz;
- kockázatelemzés;

- kockázatelemzés eljárásainak kidolgozása;
- információmegosztás a kormányzati szereplők között;
- kritikus infrastruktúrák és szolgáltatások beazonosítása;
- kibertudatosság megteremtése, elsősorban a jogszabályalkotók szintjén;
- információ áramlás biztosítása formális és informális keretek között;
- közös fogalmi rendszer kidolgozása;
- tiszta jogszabályi környezet megteremtése;
- rugalmas szervezeti reagálás kialakítása;
- jogszabályokban levő lyukak befoltozása;
- kötelező jogkövetés;
- elavult szabályozások megszüntetése;
- hatékony együttműködés kialakítása;
- az információáramlás és az adatvédelem kapcsolatának tisztázása;
- a digitális írástudatlanság felszámolása;
- a nemzetközi kötelezettségvállalásokat a helyükön kell kezelni;
- az alapvető információbiztonsági követelmények megvalósításának megkövetelése;
- törekedni kell a nemzetközi interoperabilitás megteremtésére;
- más országok tapasztalatainak megismerése, beépítése.

A NATO-n kívül más nemzetközi szervezetek is készítettek ajánlásokat a kiberbiztonsági stratégiák alkotására vonatkozóan. Ide sorolhatjuk a Nemzetközi Távközlési Egyesület (International Telecommunications Union, továbbiakban ITU) által 2011-ben megfogalmazottakat, amelyek az alábbi területre vonatkoznak:

- legmagasabb szintű kormányzati szintű kiberbiztonsági felelősség meghatározása;
- nemzeti kiberbiztonsági kiberkoordinátor kinevezése;
- nemzeti kiberbiztonsági tanács létrehozása;
- jogszabályalkotás;
- nemzeti kiberbiztonsági keretrendszer kidolgozása;
- Computer Incident Response Team (CIRT) felállítása;
- kiberbiztonsági tudatosság és oktatás megszervezése;
- köz- és magánegyüttműködés a kiberbiztonság területén;
- humán képességek fejlesztése a kiberbiztonság területén;

- nemzetközi együttműködés [75].

Magyarország szempontjából az Európai Unió Hálózat- és Információbiztonsági Ügynökségének (továbbiakban ENISA) van jelentősége még. Az ENISA ajánlása az alábbiak szerint épül fel:

- vízió, hatókör, célok, prioritások meghatározása;
- nemzeti kockázat-felmérési szempontrendszer megalkotása;
- meglevő jogszabályok, szabályzók felülvizsgálata;
- tiszta irányítási struktúra felállítása;
- fontos szereplők azonosítása, bevonása;
- megbízható információ átadási eljárások kidolgozása;
- a kiberbiztonságot számbavevő folytonosság megteremtése;
- kibervédelmi gyakorlatok szervezése;
- alapvető biztonsági követelmények meghatározása;
- incidensjelentési eljárások kidolgozása;
- állampolgári tudatosság növelése;
- kutatás-fejlesztés támogatása;
- szakértői oktatások és tréningek indítása;
- incidenskezelési képességek kialakítása;
- kiberbűnözés visszaszorítása;
- részvétel a nemzetközi együttműködésekben;
- köz- és magánegyüttműködés kialakítása;
- biztonság és adatvédelem közös összhangjának kialakítása;
- a kibervédelem rendszerének értékelése;
- a nemzeti kibervédelmi stratégia finomhangolása [76].

Mindhárom szervezet által kiadott ajánlás bizonyos minimumkövetelményeket és elveket fogalmaz meg, amelyeket célszerű a nemzetek kiberbiztonsági stratégiáiba adoptálni. Célszerű azonban mérni a stratégiában foglaltak megvalósulását valamilyen indikátorrendszer segítségével. Ebben mind az ENISA, mind az ITU dolgozott ki értékelőrendszert. Míg az ENISA 6 fő és 21 alkategória alapján értékeli az adott államok kiberbiztonságát, elsősorban a stratégiák megvalósulásán keresztül adja meg a mérőszámot, addig az ITU által megalkotott Global Cybersecurity Index öt pillér (jogi, műszaki, szervezeti, képességnövelés,

együttműködés) alapján vizsgálja, hogy szervezetet tömörítő 134 állam kiberbiztonsági indexe milyennek tekinthető [77]. Ez alapján lehetőség nyílik az egyes államok eredményeinek összehasonlítására [78].

Magyarország az Európai Unióban élenjárt a kiberbiztonsággal kapcsolatos stratégiaalkotásban. Az előző alfejezetben említett Nemzeti Kiberbiztonsági Stratégia 2012-es megalkotása mellett fontosnak tekinthetőek az Országgyűlés által 2011-ben elfogadott az információs önrendelkezési jogról és információszabadságról szóló törvény (továbbiakban Infotv.) [67], 2012-ben a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény [80] (továbbiakban Lrtv.), illetve egy évvel később az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényt [81] (továbbiakban Ibtv.). Az Infotv. és az Ibtv bővebb ismertetését a harmadik fejezetben végzem el.

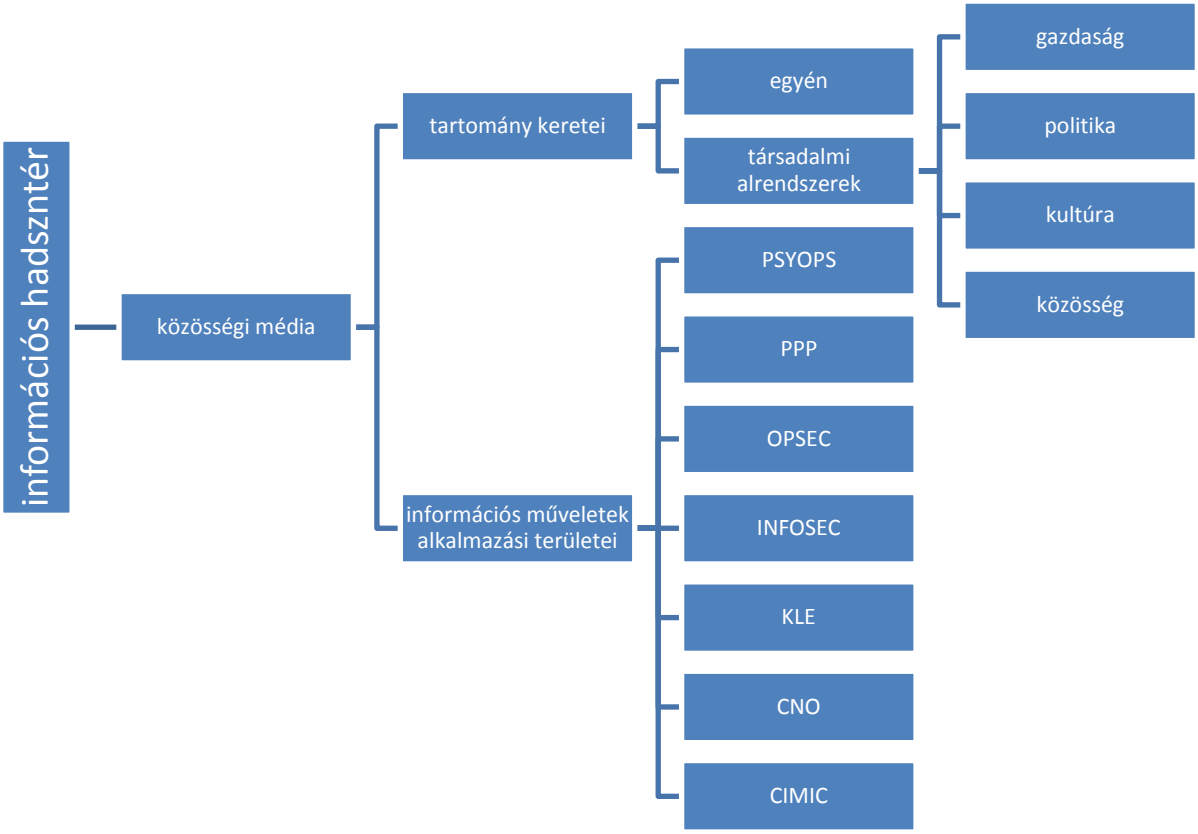
A Nemzeti Kiberbiztonsági Stratégia értékelése nem képezi e dolgozat részét, azonban a törvényhozók is belátták annak szükségét, hogy a 2012 óta végbement változásokra reflektáljon a dokumentum, ezért új Stratégia készült, ami az értekezéstervezet írásának idején elfogadás alatt áll.[36]

2.3. A közösségi média, mint az információs hadszíntér területe

Ahogy a bevezetőben már többször megfogalmaztam, a közösségi média számos lehetőséget nyújt a honvédelmi-, rendvédelmi-, nemzetbiztonsági szervezetek számára, amelyek mind támadó, mind védekező feladatot elláthatnak, de vannak esetek, amikor nem lehet ilyen jellegű megkülönböztetést alkalmazni. Említettem azt is, hogy az egyes támadó jellegű feladatok a másik fél hiányos védekezésből eredhetnek. Úgy vélem, magától adódik annak belátása, hogy a közösségi média a kibertér egy területe, hiszen rajta keresztül zajlanak az interperszonális interakciók. Annak érdekében, hogy az információs hadszíntér tartományaként nevesítjük (lásd 18. számú ábra) a közösségi médiát, azonosítanunk kell

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

[36] A Stratégia értékeléséről bővebben lásd Beláz Annamária témába készült diplomamunkáját [82].



18. ábra A közösségi média, mint az információs hadszíntér speciális tartománya (saját szerkesztés)

A tartomány kereteit a közösségi média egyénekkel és a társadalmi alrendszerek viszonyában vizsgálhatjuk. A közösségi média fogalmából egyértelműen következi, hogy interperszonális interakciókból áll, ami különböző közösségi csatornákon keresztül realizálódik. Eltérőek a jellemzővel írhatóak le azonban az egyes generációk, amelyek egyrészt az attitűdben, a használati szokásokban jelentkeznek. Ez a különbözőség fontos az esetleges műveletek tervezésekor, hiszen a célcsoport azonosítását követően figyelembe kell venni az eltéréseket és adoptálni a tervezéskor.

A generációk demográfiai jellemzőit alapesetben a születési év szerint szokás meghatározni, azonban találkozunk ettől eltérő interpretációkkal is. Bár születési évhez kapcsolódik, azonban más aspektusát adja a Marc Prensky által megalkotott digitális bennszülöttek- digitális bevándorlók kategóriája [83]. Prensky az amerikai oktatási rendszer vizsgálatából jutott el mérföldkőnek számító tanulmánya publikálásáig. A kutatása az oktatási rendszer minőségének romlásával foglalkozott, arra volt kíváncsi, van-e valamilyen összefüggés a digitális technológiák elterjedése és a fiatalok teljesítménye között. Bár maga a kutatás az oktatási rendszerre vonatkozott, de a megállapításai egyéb területeken is érvényesek. A szerző megítélése szerint a minőségromlás kiváltója a fiatalok radikális megváltozásában

keresendő, ez pedig összefügg az infokommunikációs technológiák elterjedésével. Prensky úgy véli, ez az új generáció, eltérően az előzőktől, nem fokozatosan formálódott, s mint ilyen, nem csupán az értékrendjük, öltözködésük, nyelvezetük tér el. A szerző szerint a mai diákok[37] a technológiai szingularitás[38] első generációjának tekinthetőek. Ebből következően a mindent átszövő IKT, az azokon folytatott interakciók alapjaiban változtatták meg ennek a generációnak az információ feldolgozását, valamint a gondolkodásukat. Prensky tanulmányában idézi Dr. Bruce D. Berryt, a Baylor College of Medicine professzorát, akinek állítása szerint „az eltérő tapasztalatok eltérő agyi felépítést eredményeznek". Ezt a megállapítást mai napig sokan vitatják, valóban bekövetkezett-e fizikai valójában, vagyis szervi elváltozásokat is eredményezett vagy csupán a kognitív szinten mutatható ki a változás.[39] Akár eredményez fiziológiai változást, akár csak a gondolkodásban érhető tetten, célszerű a digitális eszközök használata szempontjából külön kezelni az egyes generációkat. Ettől eltekintve célszerű az IKT használata szempontjából megkülönböztetni a különböző generációkat. E megkülönböztetésre vezette be Prensky a digitális bennszülöttek és digitális bevándorlók fogalmát. A digitális bennszülöttek alatt az új generáció tagjait értjük, akik „anyanyelvi szinten" beszélik a digitális környezetet. A digitális bevándorlók, szemben a digitális bennszülöttekkel nem születtek bele a digitális világába, rákényszerültek, hogy használják ezeket az eszközöket. A digitális bevándorló bár folyamatosan tanulja, igyekszik elsajátítani a digitális nyelvet, azonban mindig megmarad az „akcentusa", ami az internet szerepének másodlagos értelmezéséből származik.[40] A digitális bennszülöttekre egy másik megközelítés szerint C-generációként[41] hivatkoznak. A C-generáció tagjai tehát életmód alapján szerveződnek, nem úgy, mint a születési év alapján nevesített "X", „Y" vagy "Z"[42] generációk. Jellemzője e C- generációnak, hogy életük nagy részét online töltik, ezeken az eszközökön tartják elsődlegesen a kapcsolatot másokkal, valamint ezeken fogyasztják a tartalmakat. Egyfajta elvárás részükről, hogy azok a közösségi alapelvek, mint a hozzáférés, transzparencia, hozzászólás, megoszthatóság, elkötelezettség az élet egyéb területein is érvényesüljenek. A különböző generációk különböző szintű adat- és

[37] A tanulmány 2001-ben jelent meg, így az állítást ekkorra kell értelmezni.
[38] A technológiai szingularitás a sci-fi irodalomban és a jövőkutatásban egy olyan lehetséges jövőbeli eseményt ír le, amelyben a technológiai fejlődés olyan mértékben felgyorsul, hogy az elszakad társadalmi változásoktól, és a szingularitás bekövetkezte előtt élők képtelenek értelmezni.
[39] Gondoljunk csak az emberi evolúcióra, amely nem kifejezetten évtizedek alatt következik be.
[40] Például kinyomtatja az e-maileket, vagy telefonon érdeklődik azok kézbesítéséről stb.
[41] Connect, create, contribute, communicate, content creating generation, vagyis kommunikáló, létrehozó, hozzájáruló, kommunikáló, tartalomgyártó generáció
[42] Az „X" generáció alatt 1965 és 1980 között, „Y" generáció alatt 1980 és 1995 között, „Z" generáció alatt pedig az 1996-tól születetteket értjük.

információérzékenységgel rendelkeznek, de összességében elmondható, egyikük esetében sem túl magas.

A digitális bennszülöttek és bevándorlók közti eltérés nem csupán az iskolában jellemző, a családok, munkahelyek esetében is egyaránt probléma forrása lehet. A C-generáció az internetet, az okos mobil eszközöket és a közösségi médiát készség szinten használja, gyakran az eszközökhöz való hozzáférés igénye a Maslow-féle szükséglet hierarchia alsó szintjén jelentkezik, ami a fiziológiai szükséglet színtere. Egyre több kutatás az okos mobil eszközök és közösségi média használatból eredő függőségre hívja fel a figyelmet, ami különösen a fiatal generáció körében tapasztalható. 2018 elején az Apple két részvényese nyílt levélben hívta fel a figyelmet erre a jelenségre, kérve az Applet, fordítson több figyelmet a gyermekek védelmére [84]. A nyílt levélben több kutatásra hivatkoztak, amelyek szerint aggasztó mértékben okoznak mentális betegségeket a túlzott mobil eszköz és közösségi média használat, amelyek a figyelemhiányhoz, depresszióhoz, alváshiányhoz és az ebből származó egészségügyi problémákhoz, valamint öngyilkossághoz vezetnek [84] [85]. A függőség kialakulásáért a gyártók is sokat tesznek, nem egyedi eset, hogy a fejlesztők pszichológiai kutatásokat végeznek, hogyan lehet a felhasználókat rávenni, hogy minél több ideig használják szolgáltatásaikat. Pszichológusok írták le a „Fear of Missing Out”, vagyis a „félelem, hogy kimaradunk” fogalmát [86] [87]. Kutatók a Facebook „like” gombjának kialakításával szokták illusztrálni a szolgáltatók, gyártók addikcióra történő kondicionálását. E szerint a „like” gomb kifejlesztésében egyfajta pavlovi reflex kialakulását tűzték ki. Kutatások kimutatták, hogy a „like” gomb az agyunk dopamintermelését felelős részeit ingerli, azáltal, hogy az azonnali visszajelzések instant örömöt okoznak, aminek újból átélésére törekszünk, ezért is folyamatosan ellenőrizzük, hogy születtek-e újabb és újabb likeok az általunk megosztott tartalmakra. Pozitív visszajelzés hatására az agyunkban megindul a dopamin termelés, ami az örömérzetét felel, akár csak az alkohol vagy drogfogyasztás esetében. Akár csak egyéb addikciók esetében, hogy folyamatos legyen a dopamintermelés, újabb és újabb ingerekre van szükség, azonban a kialakuló tolerancia miatt egyre több ilyen ingerre van szükségünk. Így tehát még többet posztolunk, még többször ellenőrizzük a visszajelzéseket. Ezek elmaradása esetén szorongás, rossz közérzet alakul ki. A függőség növelésének egy másik, egyes gyártók által szintén alkalmazott eszköze az úgynevezett váratlan jutalom elve, ami azt jelenti, az értesítéseket véletlenszerűen jelenítik meg, ily módon ösztönözve a felhasználót, hogy minél gyakrabban ellenőrizze az eszközét. A pszichológiai problémákon túl ezek egyúttal komoly adat- és információbiztonsági kockázatot is jelentenek, hiszen a felhasználókban nem alakul ki

erős adat- és információbiztonsággal kapcsolatos érzékenység. Az oktatásban szerzett tapasztalatom azt mutatja, hiába vannak tudatában a különböző adat- és információbiztonsági kockázatokkal a hallgatók, a viselkedésük ezzel szemben gyakran szöges ellentétben áll. A harmadik fejezetben ismertetett, általam elvégzett kérdőíves felmérés éppen ezért a Tudás-Képesség-Viselkedés modell alapján mérte a felhasználói tudatosságot.

Az IKT eszközök használatából fakadó eltérések azonban nem csak a generációk közti különbségből fakadnak. Digitális szakadéknak nevezzük azt a jelenséget, amikor emberek csoportját szakadék választja el az IKT szempontjából. Maga a metafora a társadalmi csoportok digitális írástudásában tetten érhető jelentős eltérésekre utal, amelyben élesen elhatárolódnak a digitális analfabéták és digitális írástudók. Előbbiek fokozatosan szorulnak ki a társadalmi alrendszerek azon területéről, amelyeken egyre komolyabb hatást fejtenek ki az infokommunikációs technológiák. Mindez tartós lemaradást okoz, aminek egzisztenciálisan is komoly hatása van [88] [90]. A digitális szakadékot hozzáférési és használati megosztottság alapján különböztetjük meg. Előbbi esetében a társadalmi csoportok nem rendelkeznek infokommunikációs eszközökkel, és ez vezet a lemaradásukhoz. Ennek oka gyakran az anyagiakban mutatható ki, de az újítástól való félelem is szerepet játszhat a kialakulásában. A használati megosztottság nem feltétlenül jelenti azt, hogy az egyes csoportok nem rendelkeznek digitális eszközökkel, inkább nem fogalmazódik meg bennük az igény a használatra. A digitális szakadék kialakulásának oka között így a generációs különbségek és gazdasági körülmények mellett társadalmi,[43] kulturális[44] és tartalmi[45] tényezőket is találunk.

A társadalom és közösségi média kapcsolatát a társadalmi alrendszerek szempontjából szükséges vizsgálni. Talcott Parsons munkássága alapján a társadalom alrendszereit a célelérési politikai rendszerre, adaptív gazdasági rendszerre, mintafenntartó kulturális rendszerre, illetve integratív alrendszerét a szocietális közösségre[46] osztjuk [91]. Parsons szerint az egyes rendszereket funkciók szerint határolhatjuk el a másiktól, ezek azonban nem alkotnak egy szilárd egységet, a határok összemosódhatnak, úgynevezett interpenetrációs zónákat kialakítva. Azt gondolom, különösebb indoklás nélkül megállapítható, hogy a kibertér nem csupán

[43] Például eltérő iskolai végzettség, lakóhely stb.
[44] Például nem érzi szükségét, hiányzik a kulturális minta stb.
[45] Például nem találkozik őt érdeklő tartalommal.
[46] A szocietális közösség alatt Parsons a társadalom normatív szerveződéseket érti, amik az emberek tagsági viszonyai alapján szerveződnek.

befolyásolja, de egyben meghatározza az egyes társadalmi intézményeket, folyamatokat, térszerkezeteket.

A kibertérben eltűnnek a fizikai határok, ami egyben azt is jelenti, hogy valós időben követhetünk más országokban lezajló eseményeket, de adott esetben ezen túllépve aktív alakítói is lehetünk az ottani történéseknek.[47] A 90-es években visszatérő toposz volt az internettel kapcsolatban, hogy elidegeníti egymástól az embereket, a társadalmi szerkezetek felbomlásához fog elvezetni, ami antiszociálisabb társadalmat fog eredményezni. A közösségi média elterjedése azonban ezeket az aggodalmakat megcáfolta, bár egyúttal úgy tűnik, egy másik közkedvelt vélekedést is megdönt. Sokáig úgy tekintettünk az internetre, mint a demokrácia mélyítésének egy csatornájára, ahol a szólásszabadság, a véleménynyilvánítás szabadsága és az anonimitás által erősödnek a demokratikus hagyományok. Mára azonban ez az anonimitás egyre inkább elvészni látszik, az internet, és ezen belül a közösségi média a széleskörű megfigyelés eszközévé vált.

A közösségi média mozgósításban betöltött szerepét számos esemény igazolja, ebből csupán néhány jelentősebbet elevenítek fel. Az első a Stop Online Piracy Act (továbbiakban SOPA) elleni fellépés. A szerzői jogvédelemmel foglalkozó lobbicsoportok kiharcolták 2011-ben, hogy az amerikai Törvényhozás elé kerüljön a SOPA, ami az online kalózkodással szemben egy korábbiakban nem létező kiterjesztett jogkörrel és szigorral lépett volna fel. Magát a törvénytervezet a Kongresszus számos tagja mellett Barack Obama elnök is támogatta. Velük szemben határozták meg magukat a nagy technológiai cégek, mint a Google, Facebook és egyebek, akik támogatókat szereztek az Anonymous hacktivista csoportok, valamint a világ számos internetezőjének körében. Az egyre növekvő, közösségi oldalakon zajló tiltakozások hatására fokozatosan hátráltak ki a Kongresszusban korábban támogató képviselők, beleértve Obama elnököt is. Mindez végül a törvénytervezet bukásához vezetett, ami azt gondolom egy igen fontos fordulópontot jelentett. Egy, az Amerikai Egyesült Államok területén hatályos jogszabályt azért nem fogadott el az amerikai Törvényhozás, mert az amerikai állampolgárokon felül világszerte támadtak az internetezők. Véleményem szerint ez jogi értelemben az amerikai szuverenitás csorbulását eredményezte, ami természetesen nem csupán az Egyesült Államokat veszélyezteti, hanem minden szuverén állam esetében kockázatot jelent. Az eset másik

[47] Ezzel kapcsolatban elég felidézni a 2011-es egyiptomi vagy tunéziai forradalmakat, amikor az országok kormányzatai lekapcsolták az internetet, hogy így vegyék elejét többek között a további tüntetések szervezését, a hírek terjesztését. Válaszlépésként az Anonymous hacktivista csoport alternatív kapcsolatokat hozott létre és tartott fenn, hogy támogassa a tüntetőket.

tanulsága a technológiai vállalatok ereje, ami a politikai döntéshozatalban betöltött szerepüket is mutatja.

A közösségi média mozgósításban betöltött szerepét az Arab-tavasz néven ismert események is erősítik. A közösségi média ily módon politikai rendszerek bukását segítette elő, amelyek hatása nem egy közel-keleti államban a mai napig fegyveres konfliktusok realizálódik.

A határok nélküliség azonban egyfajta globalitás kritika is, amely szerint a közösségi média a globális kultúra képviseletével gyengíti a hagyományos kulturális mintákat, tradíciókat és kapcsolatokat, továbbá az amerikai érdekeket, világrendet terjeszti, szélsőséges esetben erőlteti rá az eltérő kulturális fejlődésen átesett társadalmakra.

A tartomány keretei mellett vizsgálni szükséges azokat a területeket, amelyeken az információs műveletek zajlanak. Ennek érdekében az AJP-3.10-ben szereplő eljárásokat és eszközöket vizsgáltam, és meghatároztam azokat a területeket, amelyek esetében közvetett vagy közvetlen módon a közösségi média támogatja az információs műveletek végzését. Az alfejezetben csupán a területeket azonosítom, részletes vizsgálatukra később kerül sor, azonban röviden szükségesnek érzem a fentiek esetében a közösségi média alkalmazási területeit ismertetni.

Lélektani műveletek

A lélektani műveletek Pix Gábor a témában írt doktori értekezést alapul véve olyan tevékenysége, amelyek során a szembenálló felek céljaik megvalósítása érdekében tudatos lélektani ráhatást alkalmaznak [92]. Lélektani műveleteket már a hadviselés kezdetétől alkalmaztak, azonban maga a fogalom ebben a formában csak a 20. században jelent meg, tudományos igényű tervezése pedig az 1960-as évektől datálható. A PSYOPS célcsoportjai ugyanúgy lehet az ellenség mellett a semleges, el nem kötelezett országok, a szövetségesek, de akár a saját lakosság is. A 2014-ben a Magyar Honvédség által kiadott Információs műveletek doktrína alapján: „*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 [93].”*

A lélektani műveletekre a köznyelvben gyakran propagandaként hivatkoznak, azonban ez a fogalom úgy gondolom, csupán egy szűkítés a lélektani műveletek teljes spektrumához

képest. Ettől függetlenül a propaganda valóban a lélektani műveletek eszköztárába tartozik. A propagandát alapvetően három kategória mentén csoportosítjuk:

- fehér propaganda jellemzője, hogy ismert, ki közvetíti, gyakran valósághű, a hírforrása hiteles, így a terjedését könnyű megakadályozni, cáfolni a valótlanságokat. Eszköztárának egyik jellegzetes példánya a vicclapok, karikatúrák, amelyekkel az ellenséget teszik nevetségessé.
- fekete propaganda a valóságtól eltérő hírközlést jelent, alkalmazói gyakran álcázzák önmagukat, megtévesztve a célközönséget, mintha az nem az ellenségtől származna, hanem a saját kormánytól.
- szürke propaganda esetében nem ismert a hír forrása. Fő célja az ellenség demoralizálása olyan hamis, alapvetően az ellenség helyzetéről szóló hírek terjesztésével, amivel csökkentik a harci kedvet, morált. Ide tartozhat például a hátországból származó álhírek terjesztése, amelyben a katonák családjainak pusztulásáról, vagy éppen feleségeik, barátnőjük hűtlenségéről szólnak.

A NATO lélektani műveli doktrínája [94] a célzott információközlést fogalmazza meg alapvető gyakorlatként, aminek egyik fő oka, hogy a propaganda a közvélekedésben rendszerint összemosódik valamilyen politikai ideológiával [95]. A célzott információközlés rendkívül széles skálán mozoghat.

A technikai és technológiai innovációval párhuzamosan bővültek az információterjesztés médiumai. Napjainkban az egyik legjelentősebb csatorna az internet és azon belül a közösségi média [96] [97]. A különböző közösségi hálózatok, blogok, fórumok, de kép és videómegosztó oldalak mind lehetőséget biztosítanak propaganda-ellenpropaganda végzésére, amelyekre az egyes államok kiterjedt szervezeteket tartanak fenn. Ennek egyik legismertebb eljárása a közösségi oldalakon való álhírek terjesztése, ami a kormányzati szereplők mellett az egyénekre, üzleti szereplőkre is fenyegetést jelent [98].

Megjelenés, Viselkedés, Arculat

A megjelenés, viselkedés, arculat tervezése minden szervezet számára fontos, hiszen ezáltal mutatja be az általa képviselt célokat. Aktívan használja a PPP-t a NATO is a közösségi oldalakon, hogy ezáltal is erősítse a nyitott, együttműködő, barátságos szervezet imázsát. A 2010-ben elfogadott Stratégiai Koncepció e tekintetben előrelépés volt, hiszen a dokumentum által megfogalmazott „nyitott ajtók politikája” (open door policy) nem csak egy jól hangzó szólam volt, hanem valódi, széles társadalmi párbeszéd eredményeképp formálódott, szemben

a korábbi bizalmas stratégiaalkotási gyakorlattal. Mindez a NATO által képviselt nyilvános diplomácia (public diplomacy) keretébe integrálódik. A PPP-nek fontos szerep jut az egyes NATO műveletek stratégiai kommunikációjában is [99]. A stratégiai kommunikáció olyan vállalati és intézményi kommunikációs elemeket és/vagy eszközöket használ, amelyek a „cél- vagy kulcshallgatóság" (célcsoport) körében kedvező véleményt alakít(hat)nak ki a vállalati és intézményi célkitűzések lehető leghatékonyabb elérése érdekében [100].

A PPP szempontjából a Magyar Honvédség pozitívan értékelhető. A Honvédség közösségi média jelenléte, elsősorban Facebookon professzionális, évek óta magas színvonalon történik. A sikeres PPP nagyban befolyásolja egy szervezet megítélését, így a pozitív percepció növelheti a lakosság körében való elismertségét, támogatását, valamint a toborzást is segíti.

Műveleti biztonság

Az IKT nagy fokú használata számos új lehetőséget teremtett az digitális eszközökbe történő behatolásra, hogy ily módon szerezzenek információt az ellenfél tevékenységeiről. Ebből következően ezeknek a rendszereknek a védelme, a műveleti biztonság megteremtése elengedhetetlen az információs hadszíntéren, hiszen ennek hiányában az ellenfél ismeri az információs képességeinket, a rendszereink működési folyamatát, terveinket, úgy képes csökkenteni a saját vezetési folyamataink sikerességét [101]. Az OPSEC alatt olyan folyamatok, tevékenységek és rendszabályok összességét értjük, amely aktív és passzív eszközök alkalmazásával megfelelő biztonságot nyújt az adott tevékenység számára azáltal, hogy megakadályozza az ellenséget, hogy hozzáférjen a számára releváns információkhoz [102]. A közösségi média a műveleti biztonságot közvetetten befolyásolja, ami a nem megfelelő adat- és információbiztonságból eredhet. Több esetben fordult elő, hogy műveleteket kellett elhalasztani, mert a katonák közösségi oldalon tárgyalták meg az adott művelet[48] vagy olyan információkat posztoltak, amelyekhez való hozzáféréssel támadást indítottak a katonák ellen.[49] A kelet-ukrajnai konfliktus során is számos esetben a közösségi oldalakra posztolt tartalomból sikerült beazonosítani az orosz katonai egységek mozgását, illetve 2015-ben Szíriában is orosz katonák által feltöltött fényképek hatására ismerte el Oroszország, hogy katonai segítséget nyújt Asszad elnök számára.

[48] Pl. egy izraeli katona egy ciszjordániai tervezett akció helyét és idejét osztotta meg [103].
[49] Pl. egy iraki bázisra új helikopterek érkeztek egy repülőegység számára, és az ott szolgálatot teljesítő katonák a róluk készült képeket feltöltött közösségi oldalakra. A képek azonban a geolokációs adatokat is tartalmazták, amelyet visszafejtettek az iraki ellenállók és sikeresen lokalizálták a helikopterek elhelyezkedését, amelynek következtében négy AH-64-es Apache helikoptert semmisítettek meg aknavetős támadással [104].

Információbiztonság

Az információbiztonság bár kapcsolódik a műveleti biztonsághoz, de sokkal szélesebb spektrumban értelmezendő. A köznyelvben gyakran szinonimaként használják az információbiztonságot az informatikai biztonsággal, azon a két fogalom eltér egymástól. Az informatikai biztonság egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg[105]. Célja, hogy az információ megőrizze és fenntartsa a biztonsági tulajdonságait, az úgynevezett „CIA" hármasát, amiben alapján C, mint confidentiality a bizalmasságot, az I, mint integrity a sértetlenséget, valamint az A, mint availability a rendelkezésre állást jelenti. Ezzel szemben az információbiztonság egy folyamat jelöl, aminek során megvédjük az információt a nem engedélyezett megzavarástól, hozzáféréstől, használattól, módosítástól, megsemmisítéstől, vagy kiszivárgástól. Az információbiztonságnak négy szintjét különböztetjük meg, ami a személyi, fizikai, adminisztratív és elektronikus információbiztonság [81].

Az internet és közösségi média használat adat- és információbiztonság szempontjából rengeteg veszélyt jelent. Nem kell szakembernek lenni ahhoz, hogy a közösségi oldalakat vizsgálva információt gyűjt a célszemélyekről nyílt forrásból. Egy minimális tudással nagyban felgyorsítható az információszerzés. Fejlettebb informatikai tudással azonban jelentősen megnőhet a megszerezhető információknak a száma, ami sokszor egyfajta szürke zónában mozog a nyílt forrású információgyűjtés szempontjából. Egy okos mobil eszközre készített alkalmazás vagy egy közösségi oldalon futó alkalmazás rengeteg olyan adatot is megszerezhet a felhasználókról, amely nem feltétlenül felel meg az adatkezelési szabályoknak, de a nem tudatos felhasználó engedélyt ad ezen információk gyűjtésére- ahogy történt például a később részletesen ismertetésre kerülő Cambridge Analytica (továbbiakban CA) esetében is. Minél alacsonyabb valaki adat- és információbiztonsági tudatossága, annál több információt oszt meg magáról a közösségi oldalakon, amelyek összegyűjtése rendkívül fontos lehet a hírszerzés szempontjából. Már pedig, ahogy a digitális bevándorlók és bennszülöttek már megfogalmaztam, az egyes generációk eltérő mértékben érzékenyek az adataik védelmére, azonban egyik esetében sem nevezhető ez magasfokúnak. A közösségi oldalakon rengeteg információ gyűjthető be a célpontokról nyílt forrásban, ami titkos információgyűjtéssel ki lehet egészíteni. Titkos információgyűjtés végzésére fő szabály szerint legálisan csak a nemzetbiztonsági szolgálatok hivatottak bírói vagy igazságügyiminiszteri engedély alapján, azonban az internet, a közösségi oldalak, az okos mobil eszközök számos lehetőséget

biztosítanak hasonló tevékenység végzésére illegálisan. Ennek eszközei lehetnek többek között például kémprogramok, billentyűzetnaplózó programok, adathalász technikák, amelyek segítségével megszerzik a célszemélyek profiljainak bejelentkezési adatait vagy olyan alkalmazásengedélyek, amelyek számos adathoz adnak hozzáférést a célszemély eszközén. Utóbbira kiváló példát jelentenek az egyes, elsősorban Androidos alkalmazások, amelyek célzottan adathalászatra készítettek. Ennek működési elve a nem tudatos felhasználókon alapul, akik az engedélyek elolvasása és értékelése nélkül engednek hozzáférést a készülékükön tárolt adatokhoz. Az alkalmazások eszközünkre történő telepítésekor hozzáférési engedélyt kell adnunk bizony adatokhoz, rendszervezérlőkhöz. A gond akkor van, ha egy alkalmazás indokolatlan engedélyeket is kér. Egy zseblámpa alkalmazás esetében legitim a vakuhoz való hozzáférés, hiszen ennek ki-be kapcsolásával tudjuk a telefonunkat „zseblámpaként" használni. Azonban, ha az alkalmazás ezek mellett az üzeneteinket is olvasni kívánja, hozzáférne a kamera, mikrofon vezérléséhez, geolokációs helymeghatározásunkhoz és egyéb adatainkhoz, minden bizonnyal adathalász céllal írták meg [106].

Kulcsfontosságú vezetőkkel kapcsolatos tevékenység

Kulcsfontosságú vezetőkkel kapcsolatos tevékenység alapvetően a vezetők által használt közösségi oldalak, okos mobil eszközök védelmével függ össze. Katonai művelet során[50] a szolgálatot teljesítő katonai vezetőknek kiemelten fontos, hogy a jó kapcsolatot ápoljanak a műveletei területen élő kulcsfontosságú politikai, gazdasági és katonai vezetőkkel. Ezért elengedhetetlen, hogy a elengedő információval rendelkezzenek ezekről a vezetőkről, hogy magas szintű bizalmas kapcsolatot építhessenek ki velük. Ahogy az INFOSEC esetében már megfogalmaztam, a közösségi oldalakról, okos mobil eszközökről számos információ szerezhető a célszemélyekről, és ahogy Hillary Clinton példa is illusztrálja, azért, mert valaki magas beosztásban levő vezető, egyáltalán nem jelenti, hogy az információvédelmet a protokoll szerint használja. Clinton külügyminiszterként, a tiltás és protokollok ellenére saját mobil eszközét és magánszerverét is használta a hivatalos levelezésre, amelyhez hackerek végül hozzáfértek. Az amerikai Szövetségi Nyomozó Iroda (Federal Bureau of Investigation, továbbiakban FBI) előtt tett vallomásában úgy védekezett, kalapáccsal szétverték a Blackberry

[50] Napjainkban a katonai műveletek jellemzően békeműveleti tevékenységek körébe tartoznak. Háború indítására a nemzetközi jog csupán az Egyesült Nemzetek Szövetségének (továbbiakban ENSZ) Biztonsági Tanácsa (továbbiakban ENSZ BT) általi felhatalmazására van lehetőség, ennek ellenére mégis gyakoriak a katonai konfliktusok. Minden ilyen esetben a NATO az ENSZ BT felhatalmazása alapján vesz részt valamilyen béketámogató műveletben, amely vonatkozhat megelőző diplomáciára, béketeremtésre, békefenntartásra, békeépítésre, béke kikényszerítésre, válság diplomáciára [107].

készülékeket, hogy minden adat eltűnjön belőlük. Úgy gondolom, ez is rávilágít, milyen jelentős kockázatokat jelent a nem megfelelő szintű adat- és információbiztonsági tudatosság.

További kockázatot jelent, ha a vezetők az általuk birtokolt eszközöket mások is használják, például a kisgyerekük telepít valamilyen alkalmazást, ami magában hordozza annak a lehetőségét, hogy adathalász alkalmazás kerüljön az eszközre, ily módon pedig az esetleg azon tárolt szenzitív információk harmadik fél birtokába kerülhetnek. Éppen ezért a kulcsfontosságú vezetőkkel kapcsolatos tevékenységek két oldalról értelmezhetőek, míg egyrészt a saját vezetőink esetében ezen eszközök védelme, addig a másik oldalról a szembenálló felek kulcsfontosságú vezetők által használt közösségi eszközök feltérképezése információszerzés reményében elengedhetetlen [108].

Számítógép-hálózati műveletek

Számítógép-hálózati műveletek esetében a közösségi média támogató szerepet tölthet be. A számítógép-hálózati műveletek kettős célt szolgálnak. Egyrészt alkalmazzák a hálózatok felderítéséhez, illetve adatok megszerzésére, másrészt a megszerzett adatok módosításában, befolyásolásában, tönkretételében, valamint a hálózatok működésében diszfunkció elérésére [109].

Egyes közösségi oldalak, kiváltképp a Facebook rendkívül hasznos olyan kártékony programok terjesztésére, amelyek hozzáférést biztosítanak a támadóknak a fertőzött eszközhöz. A Facebookon gyakran kampány szerűen jelennek meg bizonyos rosszindulatú alkalmazások, amelyek végig söpörnek a felhasználókon. Annak ellenére, hogy maguk a támadások gyakran ismétlődő mintákkal bírnak, mégis újra és újra sikerrel járnak. A Facebookon terjedő kártékony alkalmazások alapvetően két módon fertőznek: privát üzenetben vagy a felhasználó üzenőfalán. A fertőzött eszközöket a támadók motivációjuknak megfelelően tudják a későbbiekben használni, ami ugyanúgy realizálódhat adatok megszerzésében vagy hálózatok, rendszerek támadásában például egy botnet hálózat segítségével végrehajtott túlterheléses támadással.

Civil- katonai együttműködés

A Civil- katonai együttműködés harctámogató tevékenység, aminek feladata, hogy támogassa a végrehajtó erőket a parancsnok rendelkezésére álló erőkkel és eszközökkel a harcfeladatok sikeres ellátása érdekében. Ennek érdekében a CIMIC három fő tevékenységet végez: a támogatást, a lakossággal történő kapcsolattartás elősegítését és a civil környezet támogatását [110] [111]. A nem háborús feladatok sikeres ellátása érdekében létfontosságú a civil környezet

támogatásának megnyerése. A civil környezet nagyban megkönnyítheti vagy megnehezítheti a feladat végrehajtását. A civil környezet műveleti területenként eltérő lehet, de minden esetben magában foglalja a terület lakosságát, a kormányzati, nem kormányzati szereplőket. Annak érdekében, hogy a civil környezet megkönnyítse a katonai feladatok végzését, rendkívül fontos a támogatásuknak az elnyerése, amelynek egyik eszközéül a CIMIC csoportok szolgálnak. Úgy vélem, a közösségi média megfelelő használata segíthet növelni az együttműködést a civil környezet és a katonai erők között, ezáltal nagyobb mozgásteret biztosíthat a parancsnoknak morális, materiális, környezeti, stratégiai, hadműveleti, harcászati előnyök kihasználása érdekében, illetve hosszútávon segíthet kialakítani egy olyan civil környezetet, amely növeli a konfliktus békés lezárását, a nemzetközi erők kivonása után a béke fenntartását. Értelemszerűen a közösségi média alkalmazási területe ez esetben a civil környezet támogatásának megnyerése, a beavatkozó nemzetközi erők részvételének legitimálása.

KÖVETKEZTETÉSEK

A fejezetben megvizsgáltam a kibertérnek, mint új hadszíntérnek a kialakulását, valamint bemutattam a nemzetközi és hazai stratégiai fejlődést. A stratégiai dokumentumok vizsgálatából megállapítottam, hogy a hazai stratégiai gondolkodás az európai viszonylatban is előremutató volt. Megvizsgáltam a közösségi média használat egyéni és társadalmi használatával kapcsolatos jellemzőit. Ezek alapján megállapítottam az egyének és az egyes társadalmi alrendszerek esetében jelenlevő, használatból fakadó kockázatokat. Mindez összhangban áll az előző fejezetben is megállapított használatból fakadó kettősséggel, hiszen a közösségi oldalak biztonságtudatos használata vagy éppen annak hiánya nagyban befolyásolja a katonai vagy nemzetbiztonsági alkalmazását. Ezt követően a NATO információs műveletekkel foglalkozó doktrínája alapján azonosítottam a közösségi médiának az alkalmazási területeit, amelyek közvetett vagy közvetlen módon támogatják az információs műveletek végrehajtását. Ez alapján hét területet határoztam meg, amelyek tekintetében a közösségi média megfelelő alkalmazása jelentősen növelheti vagy csökkentheti a műveletek hatékony végrehajtását. Az ily módon azonosított alkalmazási területeket megvizsgálva **meghatároztam a közösségi médiának, mint az információs hadszíntér speciális területének kereteit, eljárásait**.

III. FEJEZET
A KÖZÖSSÉGI MÉDIA SZEREPE AZ ADAT- ÉS INFORMÁCIÓBIZTONSÁGI TUDATOSSÁGBAN

Napjainkra már-már közhelynek tekinthető a mondás, amely szerint az adat az új olaj. Dolgozatom korábbi fejezeteiben visszatérő pont volt a közösségi oldalakról gyűjthető adatok nagy száma, jelen fejezet keretén belül alaposabb vizsgálat alá vetem a közösségi oldalak adat- és információbiztonsággal kapcsolatos összefüggéseit. A téma egyúttal szorosan kapcsolódik a magánszféra kérdésköréhez is, hiszen a technikai eszközök olyan széleskörű megfigyelést tesznek lehetővé, amelyben adat- és információbiztonság véleményem szerint felértékelődik. A fejezetben ennek megfelelően vizsgálom az adat- és információbiztonság kibertérben betöltött szerepét, bemutatom az adat- és információbiztonsággal kapcsolatos jogszabályokat, értékelem az esetleges hiányosságokat, amelyek a közösségi média használatával kapcsolatosak. Végül az általam elvégzett kérdőíves felmérés elemzését ismertetem.

3.1. Az adat és információbiztonság szerepe a kibertérben

Az internet hőskorszakára az anonimitás volt jellemző, amit sokan a demokrácia biztosítékaként láttak. A közösségi média elterjedésével azonban az anonimitás egyre inkább a háttérbe szorult. A 21. század új típusú kockázatai az államokban is megerősítették azt az igényt, hogy az internetet nagyobb kontroll alá vessék. Ennek mértéke államonként eltérő, Oroszországban például a terrorizmus és szervezett bűnözés elleni harc jegyében teljes egészében felszámolnák az anonimitást az interneten. Benjamin Franklin mondotta, „*Azok, akik feladnák alapvető szabadságukat egy ideiglenes biztonságért, nem érdemelnek sem szabadságot, sem biztonságot.*” Ez a gondolat véleményem szerint soha nem volt ennyire aktuális.

A magánszféra és kibertér kapcsolata

George Orwell 1984 című regényében egy olyan totalitárius állam disztópiáját festi le, amelyben az állampolgárok életének minden percét ellenőrzik, amelyben a magánszféra fogalma nem értelmezhető. A totális állami kontroll azonban a kognitív dimenzióban is megjelenik, egyes fogalmak száműzése a nyelvből, a „gondolatbűn” megjelenése mind-mind

azt a célt szolgálták, hogy az állampolgárok öncenzúrát gyakorolva elkerüljenek minden nem kívánatos cselekedetet.

Összehasonlítva a bennünket körülvevő technikai eszközöket, illetve azok magánszférára gyakorolt hatásukat, az 1984 világa nem tűnik túlságosan távolinak. Egy okos mobil eszköz már majdnem mindenki zsebében megtalálható, amelyen keresztül pontosan követhető, mikor hol van, megvan a technikai lehetőség arra, hogy távolról vezéreljék a készülék kameráját és mikrofonját, amelynek bekapcsolásával igény szerint hallgathatják, adott esetben láthatják a célszemélyt. Magán vagy munkahelyi levelezésünk jelentős részét ezeken az eszközökön keresztül végezzük, barátainkkal, családtagjainkkal szintén rendszeresen ezeken kommunikálunk.

Az internet, az okos mobil eszközök és a közösségi média a magánszféra erőteljes korlátozását hozta magával, ami az adat- én információbiztonság tekintetében óriási kihívás is egyben.

A magánszféra nem csupán igény, de egyben jog is, amelynek gyakorlása mentén magunk határozunk arról, ki milyen információhoz férhet hozzá velünk kapcsolatban, valamint ellenőrzési helyzet is, amely során döntünk, kikkel osztjuk meg személyes, intim információinkat. Nem egyszerű azonban annak a meghatározása, hogy mi tartozik bele a magánszféra érvényességi körébe, hiszen az információ és információvédelem vagy az elrejtőzés és figyelem középpontjába való kerülés összetett kérdéseihez szorosan kapcsolódik. Az államok funkciójából egyenesen következik, hogy feladataik hatékony elvégzése érdekében a lehető legtöbb információt kívánják megszerezni, hogy azokat értékelését követően hozhassák meg a döntéseket. Az információszerzés eljárásait, az információ feldolgozásának, felhasználásának, tárolásának szabályait jogszabályok határozzák. A probléma, hogy a mindent körülvevő infokommunikációs technológiák olyan mértékű adatgyűjtést tesznek lehetővé, amelyek nem feltétlenül felelnek meg a normatív előírásoknak. Különösen igaz ez a megállapítás a magáncégek által gyűjtött adatokra. Egyes szerzők, mint például Kirstie Ball, a tömeges megfigyelést a kormányzat és a magánszféra érdekeként írják le, amelynek okait gazdasági szempontokra vezetik vissza [112].

Az interneten a fizikai korlátok lebontásával a keletkezett adatok nem csak egy állam területén „vannak jelen”. A közösségi oldalak üzemeltetői globális vállalatok, ezeket a közösségi oldalakat a világ különböző pontjain használják. Nagyon eltérőek azonban az egyes országok adat- és információbiztonsággal kapcsolatos szabályozásai, ráadásul a jogszabályok nem képesek megfelelően követni a technológiai változást, amely az adat- és

információbiztonságot nagyban meghatározza. A 2018. május 25-étől hatályos Európai Általános Adatvédelmi Rendelet (General Data Protection Regulation, továbbiakban GDPR) e szempontból komoly változást fog jelenteni, azonban ez csupán az Európai Unió állampolgáraira érvényes szabályzó, azonban elképzelhető, hogy a GDPR-nak való megfelelés érdekében hozott változásokat nem csak az EU területén, de azon kívül is használni fogják.

Nem szabad elfelejteni azt sem, hogy az interneten továbbított adatok különböző országokon keresztül érnek el a címzetthez. Az 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. Ezek a csomagok több rétegből állnak össze, amelyek különböző információkat tartalmaznak. Annak érdekében, hogy a küldött csomag a megfelelő helyre érkezzen, az internetszolgáltató át kell vizsgálja a csomagok felső rétegét (ezt nevezzük felszíni csomagvizsgálatnak), hiszen ezek tartalmazzák azokat az információkat például, hogy ki az üzenet címzettje. A felszíni csomagvizsgálat mellett azonban a többi réteget is átvizsgálják hálózatbiztonsági szempontok érdekében, ugyanis ennek segítségével lehet kiszűrni az adatcsomagokba elrejtett kártékony kódokat. Ezt az eljárást nevezzük mély csomagvizsgálatnak (Deep Packet Inspection, továbbiakban DPI) [113] [114] [115]. Maga a folyamat automatizált vizsgálatot jelent, amely során algoritmusok segítségével kiszűrik a hálózatbiztonságra veszélyes kódokat. Az, hogy mi jelent fenyegetést, és mit kell kiszűrni nem csak a kártékony kódokra lehet alkalmazni hálózatbiztonsági szempontokból, hanem a bűnüldözésben is hasznos lehet. A megadott paraméterek alapján a DPI segíthet például a pedofil tartalmak vagy más bűncselekmények detektálásában is. A kulcsszavas keresés azonban olyan tartalmakat is kiszűrhet, amelyeket valamilyen oknál fogva károsként értékelnek, így szűkíthető többek között a politikai nyilvánosság kerete, hogy cenzúrázzák a technológia segítségével a nem kívánatos politikai véleményeket. Európában a DPI-t kizárólag hálózatbiztonsági szempontok alapján alkalmazhatnak, de más országokban nincsenek ilyen szigorú megkötések. Az Egyesül Államokban kereskedelmi célból[51] szabadon használhatják a cégek a DPI-t. Ismereteink szerint többek között Kína, Oroszország és Irán is alkalmazza az internetes mély csomagvizsgálatot, ami, mint láttuk, adott esetben az ellenzéki vélemények elhallgattatására is felhasználható. Azáltal, hogy az általunk küldött adatcsomagok a világ különböző országain keresztül haladhatnak át, megvan a lehetőség arra, hogy olyan országok is érintettek legyenek, ahol az adatvédelem sokkal megengedőbb, mint az európai gyakorlat,

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

illetve nem tudjuk, hogy az adott állam nemzetbiztonsági szolgálatai az ily módon megszerzett adatokat miképpen használják fel.

Ha eltekintünk az államok adatvédelemmel kapcsolatos gyakorlatától, még mindig ott van a nagy technológiai cégek gyakorlata, amely gyakran álszent attitűdről árulkodik. A Facebook, a Google vezetői több alkalommal fejtették ki azt a véleményüket, hogy a magánszféra fogalma a 21. századra elavulttá vált, nem értelmezhetőek, de a magánéletben mégis komolyan ragaszkodnak hozzá. Mark Zuckerberg, a Facebook alapítója Palo Alto-i házának a szomszédos házait is megvette, de a Google egyik vezérigazgatója megtiltotta a munkatársainak, hogy nyilatkozzanak egy informatikai újságnak azt követően, hogy a folyóirat egyik szerzője nyílt forrású információgyűjtést használva megírta, hol lakik.

A közösségi oldalak szerepe az adatgyűjtésben

Az, hogy a nagy közösségi oldalak a magánszférát, és ebből következően az adat- és információvédelmet meghaladott gondolatnak értékelik, nem véletlen, hiszen ahogy az első fejezetben már bemutattam, a felhasználókról gyűjtött adatok minél pontosabb profilozásával jelenítik meg a bevételeik jelentős hányadáért felelős hirdetéseket.

Ahhoz, hogy ennek jelentőségét megértsük, tisztázni szükséges az adat és információ közti különbséget. Az adat objektív tények összessége, mérési eredmény, amely egy adott helyzetre vonatkozik egy adott időpontban [116]. A gyakorlatban, ha semmit nem teszünk, akkor is keletkezik valamilyen adat. Ha alszunk az ágyunkban, az éjjeli szekrényen mellettünk elhelyezett okos mobil készülék geolokációs helymeghatározása alapján gyűjti a tartózkodási helyünket. A fejlettebb készülékek egy okosóra segítségével adatokat gyűjthetnek az alvás közbeni élettani jeleinkről (például a pulzusunkról, vérnyomásunkról), a REM fázisunkról stb. Napi tevékenységeink végzése közben az általunk előállított adatok száma exponenciálisan növekedik. Kikkel tartózkodunk egy helyiségben, milyen ideig, milyen helyszíneket keresünk fel, mikre keresünk rá, éppen hol fizetünk elektronikusan stb, mind-mind hozzájárulnak a pontos profilunk megrajzolásához.

Az adatok minél sokrétűbb megszerzésében az okos mobil eszközök különösen sok lehetőséget rejtenek. A Facebook például olyan szabadalmat nyújtott be, ami arra vonatkozik, egy adott helyen huzamosabb ideig merre irányulnak a telefonok kamerájának giroszkópjai [117]. Ez azért érdekes, mert alapból már geolokációs helymeghatározás során tudja rólunk a Facebook, hol vagyunk, de ha adott esetben ez egy szórakozóhelyen történik, és két kamera huzamosabb ideig, rendszeresen egymásra néz, akkor feltételezi, hogy az a két személy

beszélget egymással, ha pedig nem ismerősei még egymásnak, akkor javasolhatja, hogy bejelöljék egymást.

Ez vezet el bennünket az információ fogalmához, ami az adatok értelmezését jelenti. Az információ tehát nem más, mint új ismeretté értelmezett adat [118]. Az által, hogy folyamatosan adat keletkezik, megnehezedik az adatok feldolgozása és értelmezése. A cégek, magányszemélyek, intelligens hálózatok által napi szinten előállított nagy mennyiségű adatot nevezzük big data-nak, ami azonban strukturált és strukturálatlan adathalmaz is egyben [119]. Ezeknek az adatoknak a strukturált feldolgozása és elemzése nagy hasznot jelent a cégek és ügyfeleik számára [120], de nem lehet megkerülni a közszférában sem [121].

Az adatok feldolgozásában az automatizáció nagy szerepet tölt be. A nagy technológiai vállalatok úttörő szerepet töltenek be a mesterséges intelligencia kutatásokban. A Facebook gépi mélytanulással kapcsolatos kutatásai többek között a DeepFace nevű, biometrián[52] alapuló képfelismerő szoftvere segítségével 97,25%-os pontossággal képes felismerni, hogy két feltöltött fényképen ugyanaz a személy szerepel-e [122]. A technológia megalkotásakor azonban nem fordítottak kellő gondot az adatvédelemre. A 2011-ben bevezetett „Tag Suggestions" funkció automatikusan bejelölte a feltöltött fényképeken szereplő személyeket. A funkciót számos támadás érte, Európában például a szigorúbb adatvédelmi szabályozások okán fel is függesztették, az Egyesült Államokban az alapértelmezett beállításból választható funkcióvá sorolták vissza. A Facebook ellen csoportos pert kezdeményeztek a felhasználók, azzal vádolva a közösségi oldalt, hogy - megszegve a biometrikus adatgyűjtésre vonatkozó jogszabályt- törvénytelenül gyűjtöttekék és tárolták a felhasználók biometrikus azonosítóit. 2018 áprilisában a San Franciscó-i szövetségi bíróság úgy határozott, a felhasználók jogosan indíthatnak pert a Facebook ezen gyakorlata ellen [123].

2018 tavasza a Facebook adatkezelési gyakorlatának botrányaitól volt hangos. Ennek hátterében a Cambridge Analytica nevű big data elemző cég áll, amely politikai kampányokban vállal tanácsadói szerepet, elsősorban lélektani műveleteket használva. A CA hírnevét a 2016-os amerikai elnökválasztási kampány alapozta meg, azonban már a szintén 2016-ban lezajlott, az Európai Unióból való brit kilépésről szóló népszavazás végeredményében is komoly szerepet vállaltak [124].

[52] Biometrikus jelzővel olyan rendszereket illetünk, amelyek személyek mérhető fizikai jellemzőit használják a személyek azonosítására, kategorizálására. Ilyen azonosító többek között az ujjlenyomat, az arcvonás, retina véredénystruktúrája, DNS, esetleg a test szag, de egyedi viselkedési jellegzetességek is ide tartozhatnak, mint például a hang, a testtartás stb.

A 2012-ben megalapított CA „viselkedésalapú kommunikációs” kampánytanácsadóként hirdette szolgáltatásait, amelynek alapját Aleksandr Kogan, a Cambridge-i Egyetem kutatójának munkássága jelentette. Kogan megalkotta a This is your digital life (vagyis Ez a digitális életed) nevet viselő Facebook alkalmazását, amely egy személyiség-teszt volt. A Facebook akkori adatvédelmi gyakorlata lehetővé tette az ilyen alkalmazások fejlesztését, azonban meghatározta, kik férhetnek hozzá az így gyűjtött adatokhoz. Az alkalmazás tudatta a felhasználókkal, hogy adatokat gyűjtenek róluk, a kitöltésért még fizetett is. Végül körülbelül 270 ezer felhasználó töltötte ki a személyiség-tesztet, de az alkalmazás nem csak a kitöltő adatait gyűjtötte, hanem az ismerőseinek adataihoz is ugyanúgy hozzáfért.[53] Pontosan nem tudjuk, összesen hány felhasználó adatait gyűjtötte össze az alkalmazás, ugyanis a fokozatosan napvilágra kerülő információk hatására egyre bővült ennek a száma, a kezdeti 50 millióról először 87 millióra. Brittany Kaiser, a CA egykori vezetője a brit parlament bizottsági meghallgatásán azonban azt a vallomást tette, hogy ennél jelentősen több lehet az adatvédelmi botrányban érintett felhasználók száma. A meghallgatáson Kaiser egyebek mellett arról is beszélt, hogy „*Az adatvédelem (privacy) mítosszá vált, az emberek viselkedésének a nyomon követése pedig mára a közösségi média, sőt magának az internetnek a lényegi része”,* valamint „*a kormányok, magánvállalatok és gazdag személyeknek régóta megvan a lehetősége, hogy megvásárolják, birtokolják és összegyűjtsék az adatainkat. Az elmúlt évtized féktelen növekedést hozott az adatgyűjtésben és modellkészítésben, a termékek, szolgáltatások és politikai ideológiák egyénekre targetált eladásában [126]*”

2015-ben a Facebook felfedezte, hogy Kogan harmadik fél részére továbbadta az általa gyűjtött adatokat, ekkor eltávolította az alkalmazást az oldalról, valamint kötelezte Kogant, hogy a begyűjtött adatokat megsemmisítse. Több jel utal azonban rá, hogy bár Kogan igazolta, hogy minden eszközről törölte az adatokat, ez azonban mégsem következett be. A Facebookot ért vádak elsősorban arra vonatkoznak, hogy elhallgatta az esetet 2015-ben, és nem tájékoztatta a felhasználókat, hogy az adataikat nem jogszerűen kezelik.

Önmagában, hogy egy cég megszerzi az adatainkat, nem következik, hogy azok felhasználásából törvénytelen módon történne. Az sem következik belőle, hogy képesek hatékonyak kiértékelni őket. 2011-ben a Facebookon néhány nap alatt közel 800 ezer magyar felhasználó töltötte ki a „Mi az indián neved?” nevet viselő tesztet. Nem sokkal később derült ki, hogy az alkalmazás mögött egy online ékszer üzlet állt, ami ezzel a kis gerilla kampányból

[53] Meg kell jegyezni, ez a gyakorlat más alkalmazások esetében is jellemző. A témáról bővebben lásd Symeonidis és szerzőtársai kutatását [125].

építette ki Facebook oldalának követőit, amit marketing célokra használt. Természetesen a Facebook hirdetési rendszere már ekkor célzott hirdetéseket forgalmazott, ami alapján a hirdető meghatározta, milyen célcsoportoknak kívánja megjeleníteni hirdetéseit (például 19-25 év közötti, budapesti, felsőfokú intézménybe járó fiatalok, akik egyebek mellett kedvelnek bizonyos típusú oldalakat). A minőségi ugrást az jelenti, amikor az adatokból nem csupán a személyiségünket képesek leképezni, hanem egyes, jövőbeli viselkedésmintáinkra is képesek következtetéseket levonni.

Az Aleksandr Kogan által kidolgozott személyiség-teszt az úgynevezett „Big Five" személyiségmodelljén alapult, amely szerint bizonyos jellemzők alapján faktoranalízis segítségével öt különböző faktorcsoportba, mint Extraverzió, Barátságosság, Lelkiismeretesség, Érzelmi stabilitás, Kultúra/Intellektus sorolhatóak az egyének [127]. A Facebook aktivitás és az egyén személyisége közötti kapcsolatról számos kutatás látott napvilágot, amelyek azt igazolták, hogy kimutatható a „Big Five" személyiségmodell alkalmazásával az egyes likeok személyiségünkkel összefüggő kapcsolata [128] [129] [130]. Ha az adatok alapján sikerül megrajzolni az egyén profilját, akkor a targetálás segítségével meg pontosan lehet olyan hirdetést megjeleníteni számára, amely nagyobb valószínűséggel segíti elő a hirdetésre való kattintást és a vásárlást. Ez az eljárás a választási kampányokban kiválóan működik. Amennyiben a felhasználót egy párt potenciális szavazójának értékel az algoritmus, a személyiségének megfelelő hirdetést jelenít meg számára. Amennyiben neurotikus személyiségzavarra utaló személyiséget állapít meg a felhasználónál, olyan típusú tartalmakat jelenít meg, amelyek erőszakos cselekményekkel függenek össze, míg, ha családcentrikus az egyén, akkor inkább a családi hagyományokkal, értékekkel összefüggő hirdetéseket lát.

Értelemszerűen, minél több adat áll a felhasználóról rendelkezésre, annál pontosabban lehet megrajzolni a profilját. A Facebook, a Google, de egyéb közösségi oldalak (vagy éppen a CA-hoz hasonló cégek) számos szempont alapján gyűjtenek adatokat a felhasználókról. Az első fejezetben a Facebook esetében már írtam, hogy több ezer szempont alapján értékeli a felhasználókat. Ezek a cégek nem csak maguk gyűjtik az adatokat, de harmadik féltől, adatbrókerektől is szereznek be további adatokat. Így például a Facebook nem csak azokról az internetezőkről tárol adatokat, akik regisztráltak az oldalra, hanem olyanokról is, akik sosem voltak a közösségi oldal tagjai. Ennek tényét a Facebook sokáig tagadta, de a CA botrány hatására Mark Zuckerberg a 2018 áprilisi kongresszusi meghallgatáson elismerte [131]. Ezek az úgynevezett árnyék profilok Zuckerberg szerint azért szükségesek, amennyiben regisztrálnak a Facebookra, akkor az oldal rendelkezésére álljanak ezek az információk.

Ezeknek az adatoknak a forrása nem csak adatbrókerektől származik, hanem azon oldalak technikai adatgyűjtéséből is, amelyek integrálták az egyes Facebook scripteket, mint például az azonnali megosztáshoz használható „tetszik” gombot. Nem tekinthetünk el a nem tudatos felhasználóktól sem, akik olyan képeket töltenek fel a Facebookra, amelyeken olyan ismerőseik is megtalálhatóak, akik nem regisztráltak az oldalra. A fényképek mellett a telefonkönyv vagy e-mail fiókok szinkronizálása is további kockázatot rejt. A CA botrány hatására ismét napirendre került az adatbiztonság, aminek következtében rengeteg, a témára érzékeny internetező töltötte le a Facebook róla tárolt adatait. Ennek során derült fény arra, hogy Androidos készülékek esetében a Facebook gyűjtötte a felhasználó telefonhívásaihoz, sms-eihez kötődő adatokat, kivel beszélt, mikor, mennyi ideig stb. Ezt a fajta adatgyűjtést az Apple nem engedélyezte az iOS-re optimalizált Facebook alkalmazás esetében [132].

Technikai adatgyűjtés a fentieken kívül számos módon támogathatja a profilozást. Ennek megfelelően az egyes oldalak figyelik az eszközeink hardveres és szoftveres jellemzőit (többek között milyen operációs rendszert használunk, milyen böngészőt, hol tartózkodik az egér mutatónk, ha telefonról használjuk az oldalt, milyen az akkumulátor töltöttsége stb.).
Ezeket az adatokat a cégek jogszerűen gyűjtik. A Kogan által használt adatok is jogszerűen kerültek a birtokába, a törvénysértés akkor valósult meg, amikor ezeket az adatokat értékesítette. Más a helyzet a szándékosan adathalászatra épülő alkalmazásokkal. Facebookon várhatóan a CA botrány hatására szigorúbban fognak fellépni az ilyen alkalmazásokkal, azonban Androidos okos mobil eszközök esetében még nem következett be az a fordulópont, amikor a Google Play áruház biztonságosabbá válik. Bár rendszeresen számolnak be arról, hogy eltávolítottak nagy számú adathalász alkalmazást, ennek ellenére a bekerülés feltételei nem szigorodnak jelentősen. Az Apple alkalmazásboltjába több körös ellenőrzést követően tölthetnek fel a fejlesztők alkalmazásokat, szigorúan ellenőrizve az adatkezeléssel kapcsolatos gyakorlatot is. Ez hiányzik a Google Play áruházból, így rengeteg alkalmazás kifejezetten adathalász céllal kerül be. Ezek az alkalmazások a felhasználók nemtörődömségét használják ki, és úgy kérnek hozzáférést az egyes adatokhoz, hogy a felhasználó nem olvassa el, mihez ad engedélyt.

Mindez elvezet bennünket a felhasználói tudatosság kérdéséhez. Elvárható-e az internetezőktől, az informatikai eszközöket kezelőktől, hogy tisztában legyenek az adat- és információbiztonságukat fenyegető támadásoktól. Könnyen rávághatjuk, hogy igen, azonban véleményem szerint ez nagyban leegyszerűsíti a kérdést. Az internet a polgári felhasználásba csupán az 1990-es években került be, a nagy közösségi oldalak a 2000-es évek közepén jelentek

meg, általános elterjedésük alig egy évtizedre tehető. Úgy gondolom, ilyen rövid idő alatt nem alakulhatott ki az a fajta digitális immunitás, ami megfelelő védelmet nyújt. A társadalmi evolúció során jóval hosszabb időre volt szükség, míg megtanultuk, milyen helyeket kell elkerülünk a túlélésünk érdekében, azonban ehhez olyan tapasztalatok vezettek, amelyek során gyakran emberéleteket követelt. A történelmi emlékezet segített a későbbiekben csökkenteni a ránk leselkedő veszélyeket. Ez a kollektív tudás azonban jelenleg hiányzik az oktatásból. Az adat- és információbiztonságra vonatkozó oktatást a lehető legkorábban, már az óvodában szükséges lenne elkezdeni, azonban gyakran teljes egészében hiányzik a közoktatásból vagy a graduális képzésből. A társadalom jelentős része azonban már befejezte tanulmányait, így esetükben szintén lehetetlen elvárni, hogy felismerjék az ilyen típusú kockázatokat. Megoldást jelenthetne számukra, ha a munkahelyeken részesülnének ilyen jellegű oktatásban, azonban a gyakorlatban ez sem jellemző. Fontosak lehetnek a biztonságtudatosság növelésére vonatkozó kampányok. A Digitális Jólét Program (továbbiakban DJP) keretében működik a Digitális Immunerősítő Program (továbbiakban DIP), amely alapvetően az „X", „Y" és „Z" generáció számára adat- és információbiztonsági tudatosságának erősítése érdekében szervez országos kampányokat, azonban véleményem szerint az idősebb generáció számára is ugyanilyen fontosak lennének.

Hatványozottan igaz a megállapítás az idős internetezőkre, akik ugyanolyan kitetettek a kibertámadásokkal szemben, mint a kisgyerekek, az ő védelmükre azonban még sincsenek ilyen kampányuk. Részt vettem a DIP keretében két munkacsoportban is, amelyek során azonosítottuk azokat a főbb kockázatokat, amelyek az internet és a közösségi média használatból fakadnak. A munkacsoportokban számos terület szakértői vettek részt, többek között pedagógusok, pszichológusok, média szakemberek, jogászok voltak a rendvédelmi szervek munkatársai, valamint kiberbiztonsági szakértők mellett. A kockázatok azonosítását követően fogalmaztuk meg azokat a stratégiai célokat, illetve üzeneteket, amelyekre a digitális immunerősítő kampány épül. A kampány több lépésből áll, nagy befolyású „youtubereket",[54] úgynevezett influencereket, véleményvezéreket kérnek fel az üzenetek nyilvánosság előtti képviseletére, de ezen felül kitelepülések során is népszerűsítik a stratégiai célokat. [55]

[54] Azok a személyek, akik a YouTubeon vezetnek videóblogot. Egy-egy „youtuber" több százezer követővel rendelkezik. Az egyik legismertebb magyar „youtuber" a 400 000 feliratkozóval rendelkező Szirmay Gergely például a korábban említett SOPA törvénytervezet idején szintén kampányolt követői körében, hogy írják alá azt a petíciót, ami a törvénytervezet visszavonásáért indítottak.

[55] Erre szolgál példával többek között a 2018 márciusában Budapesten megrendezett V4 országok e-sport bajnoksága vagy a 2018. április 21-ei VIII. Országos Rendőr- és Tűzoltónap.

Ahogy Bodó Attila Pál fogalmazza, *„Az adat és az információ eltérő jelentéstartalommal felruházott fogalmak, amelyek tartalmukat tekintve eltérő védelem és biztonság fogalommal rendelkeznek, különösen akkor, ha elfogadjuk azt az alapvetést, hogy védelem az a tevékenység, amely a biztonság állapotának elérésére szolgál [133].”*

Ebből következően adatvédelem alatt az adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét értjük [80]. Ezzel szemben az adatbiztonság fogalma az adatok jogosulatlan megszerzése, módosítása, megsemmisítése ellen alkalmazott műszaki és szervezési megoldások összességét takarja [133].

Az információvédelem célja, az adatvédelemhez hasonlóan, hogy megvédjük az információkat a jogosulatlan hozzáféréstől, megsemmisítéstől, módosítástól. Az információvédelemhez kapcsolódik az információt hordozó eszközök, az elektronikus információs rendszerek adminisztratív, fizikai és logikai védelme, az irat- és dokumentumvédelem, valamint a személyi védelme [133]. Az információbiztonság, ahogy a második fejezetben is már megfogalmaztam, egy követelményrendszer, amelynek középpontjában az információk sértetlenségének, bizalmasságának, rendelkezésre állásának megőrzése áll.

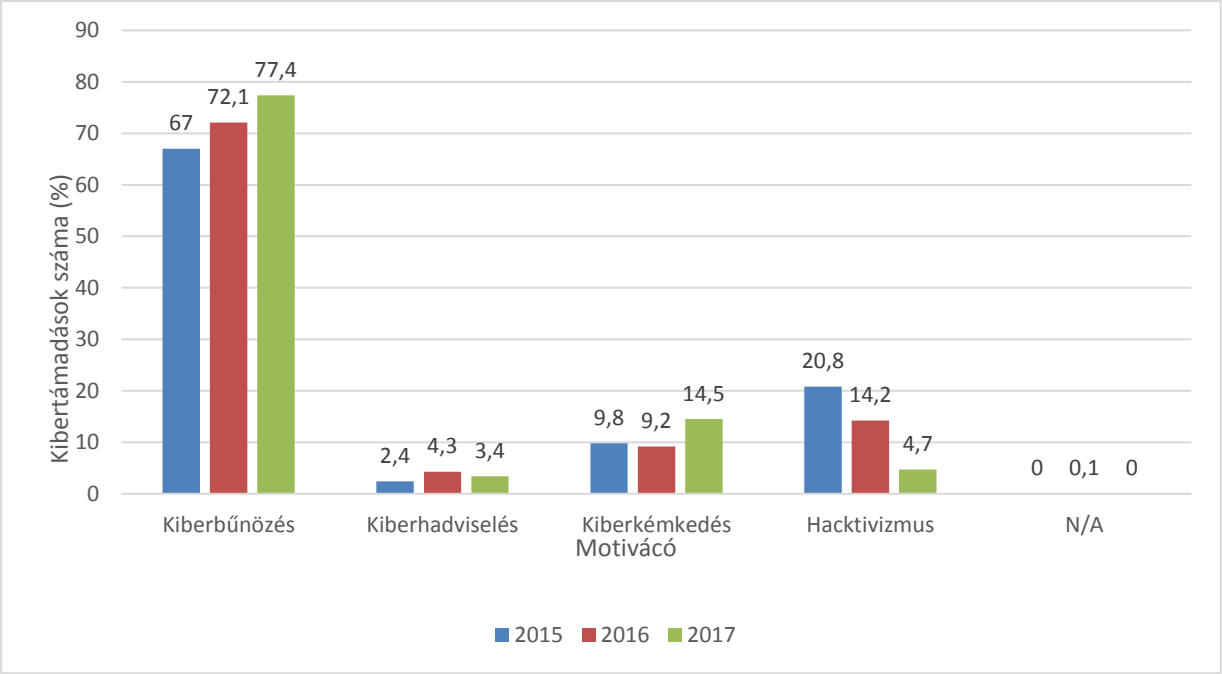
Az adat- és információvédelem/biztonság kiemelten fontos a közszférában, legyen szó katonai, rendészeti, nemzetbiztonsági, államigazgatási, közigazgatási szervezetről. Azok a személyek, akik ezen szervezetek valamelyikében dolgoznak, a támadók kiemelt célpontjai, hiszen általuk rendkívül értékes információkat szerezhetnek meg. Nem szükséges a célpontnak olyan információ birtokában lennie, aminek a megszerzése egyébként a támadók célja, azonban rajta keresztül hozzáférhetnek azokhoz a védett rendszerekhez, amelyek tartalmazzák az értékes információkat. Ilyen esetekben a támadók igyekeznek megkeresni azt a legkevésbé adat- és információbiztonsági tudatossággal rendelkező személyt, akinek a bizalmába férkőzve vagy őt akár megzsarolva hozzáférhetnek ezekhez a rendszerekhez. Minél kevésbé érzékeny valaki ezeknek az adatoknak a védelmére, annál könnyebben szerezhetik meg a támadók. Ezeknek az eljárásoknak a bemutatását a következő fejezetben végezem el részletesen.

A kiberfenyegetettségek fajtái és trendjei

A kibertámadások száma folyamatosan növekszik. Motivációk tekintetében négy csoportját különböztetjük meg a kiberfenyegetettségeknek [134]. Ez alapján beszélhetünk (1) kiberbűnözésről, (2) hacktivizmusról és kiberterrorizmusról, (3) kiberkémkedésről és (4) kiberhadviselésről.

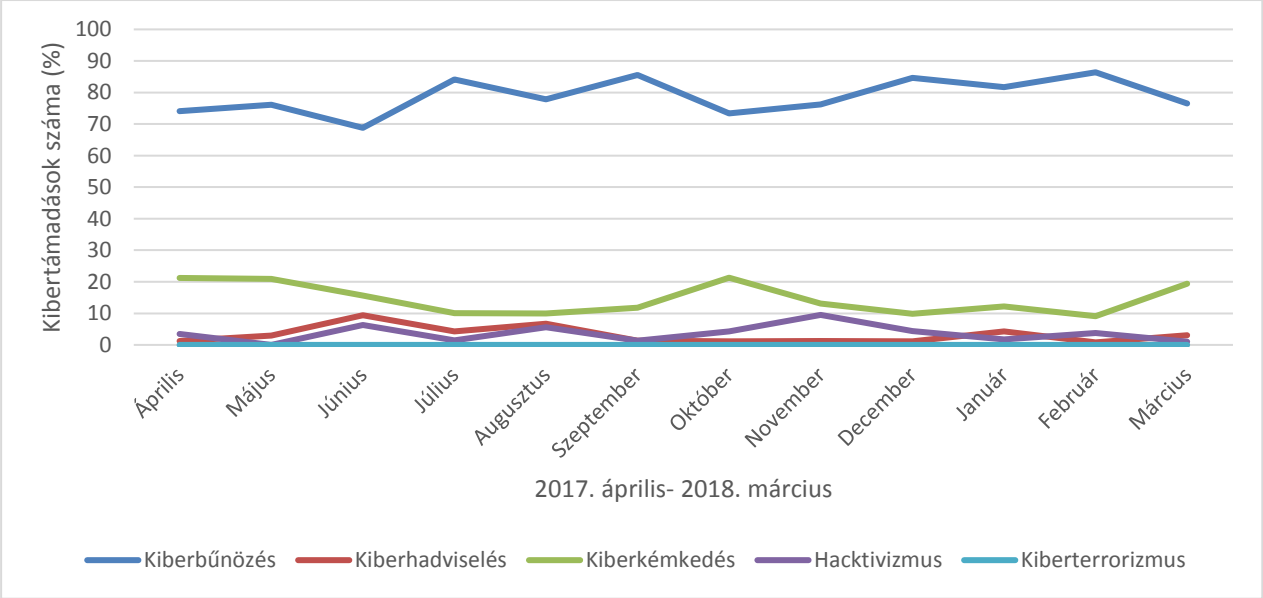
A kiberbűnözés célja informatikai rendszerekkel felhasználásával az anyagi haszonszerzés, célpontjaik között az üzleti és politikai világ szereplői egyaránt megtalálhatóak [135]. Bár a hacktivizmus és kiberterrorizmus fogalmilag két eltérő jelenség, azonban több közös pont határozható meg. Mindkét esetben decentralizált, kis létszámú csoportokról beszélhetünk, amelyek célja az általuk vallott ideológia minél nagyobb médiafigyelem előtti képviselete. A hacktivisták alapvetően az információhoz való szabad hozzáférést gondolják az egyik legfontosabb értéknek, és ennek érdekében követik el támadásaikat. A kiberterrorizmus fogalmát először a 80-as évek közepén használták, de azóta sincs egy általánosan elfogadott definíció rá [136]. Keith Lourdeau megfogalmazásában "*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 [137].”* A hacktivizmus esetében is paradigmaváltás figyelhető meg, az unatkozó és amatőr fiatalok helyett erős politikai támogatással működő profik élnek ezzel az eszközzel, akik gyakran katonai célból támadnak, mint például az Iszlám Állam hacktivistái vagy a Szíriai Elektronikus Hadsereg harcosai [138]. Elmondható azonban szerencsére, hogy jelenleg még nincsenek kiberterroristák, azonban vannak terroristák, akik használják az internetet. Kiberkémkedés alatt az államok, piaci szereplők, de akár magánszemélyek informatikai eszközön végzett hírszerző tevékenységét értük, a kiberhadviselés az államok közti konfliktusokban jelenik meg, amelynek során a konvencionális hadviselés támogatására (vagy akár kiváltására) az ellenfél információs rendszereinek működésképtelenné tételére törekszenek.

Az elmúlt évek trendjeit megvizsgálva megállapíthatjuk, hogy a bejelentett támadások jelentős többségéért a kiberbűnözők feleltek. 2015-2017 adatait vizsgálva megállapíthatjuk (lásd 19. számú ábra), hogy a kiberbűnözéssel összefüggő támadások száma fokozatosan emelkedik, a 2017-es évben az összes támadás 77,4%-át kiberbűnözők követték el. A trendek a kiberkémkedéssel összefüggő cselekmények számának növekedését mutatják, míg a hacktivizmus jelentős visszaszorulását jelzik. A kiberhadviselés, mint a támadások mögött meghúzódó motiváció az elmúlt években csupán néhány %-át jelentette a támadásoknak.



19. ábra Kibertámadások megoszlása motivációk szerint 2015-2017. (saját szerkesztés, forrás: Hackmageddon [139])

Megvizsgáltam az elmúlt 12 hónap változásait a fenyegetettségek tükrében. A 20. számú ábrán látható, hogyan változott az egyes támadástípusok aránya. A kiberbűnözés, mint motiváció 2017 júniusát leszámítva 70% fölötti értéket adott, a vizsgált 12 hónap alatt öt esetben 80% fölött volt az ilyen jellegű támadások száma, 2018 februárja volt a rekord, ekkor a támadások 86,4%-áért a kiberbűnözők feleltek.

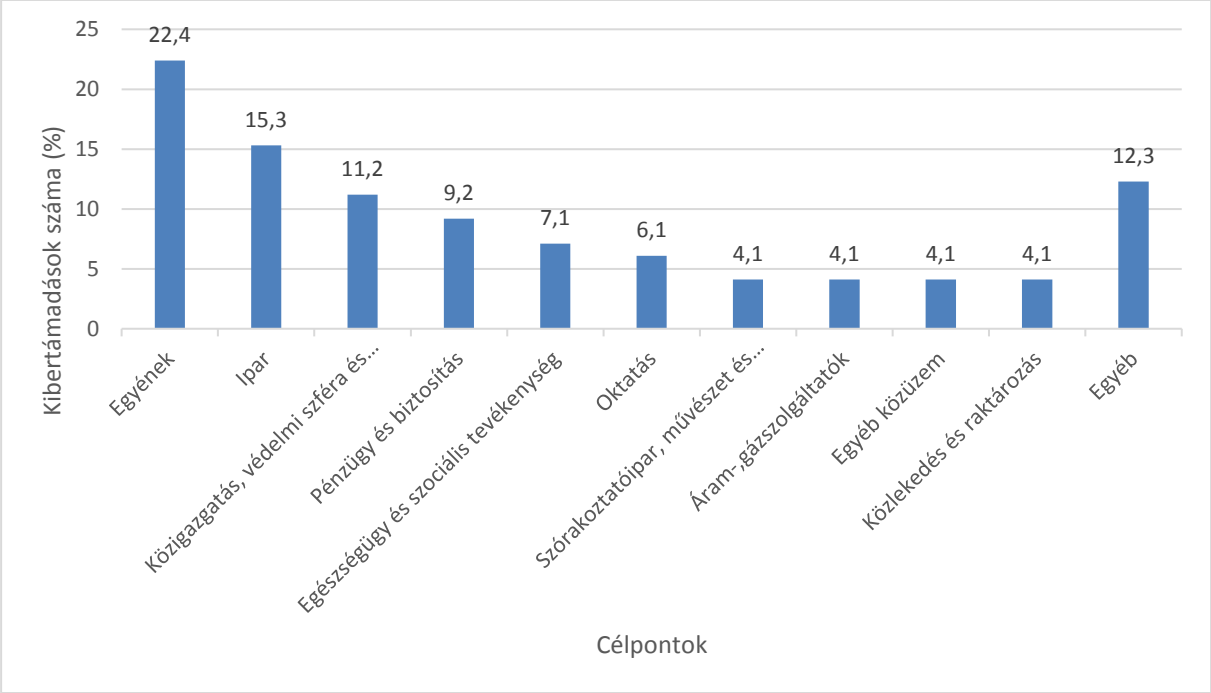


20. ábra Kibertámadások motivációk alapján 2017. április-2018. március között (saját szerkesztés, forrás: Hackmageddon [139])

A kiberhadviseléssel összefüggő támadások az elmúlt egy évben nem mutattak számottevő értéket, egyedül 2017 júniusában tapasztalunk kiugrást, ekkor a támadások 9,4%-ánál

azonosíthattuk, de összességében nem éri el az 5%-os értéket havi bontásban. A kiberkémkedés esetében kisebb ingadozást állapíthatunk meg, a támadások 10 és 20% közötti értéket mutatnak. A hacktivizmus esetében sem beszélhetünk jelentős növekedésről, három hónapot leszámítva 5% alatt volt az ilyen típusú támadások száma.

Érdemes megnézni a támadások célpontjait is. 2018 márciusának adatait figyelembe véve azt tapasztaljuk (lásd 21. számú ábra), hogy az egyének mellett az ipari szereplők, a közigazgatás és védelmi szféra szereplői állnak a legtöbb támadás célkeresztjében. Úgy gondolom, ezek az adatok is alátámasztják a korábban megfogalmazottak, mely szerint a közszférában dolgozók kiemelt célpontnak tekinthetőek.

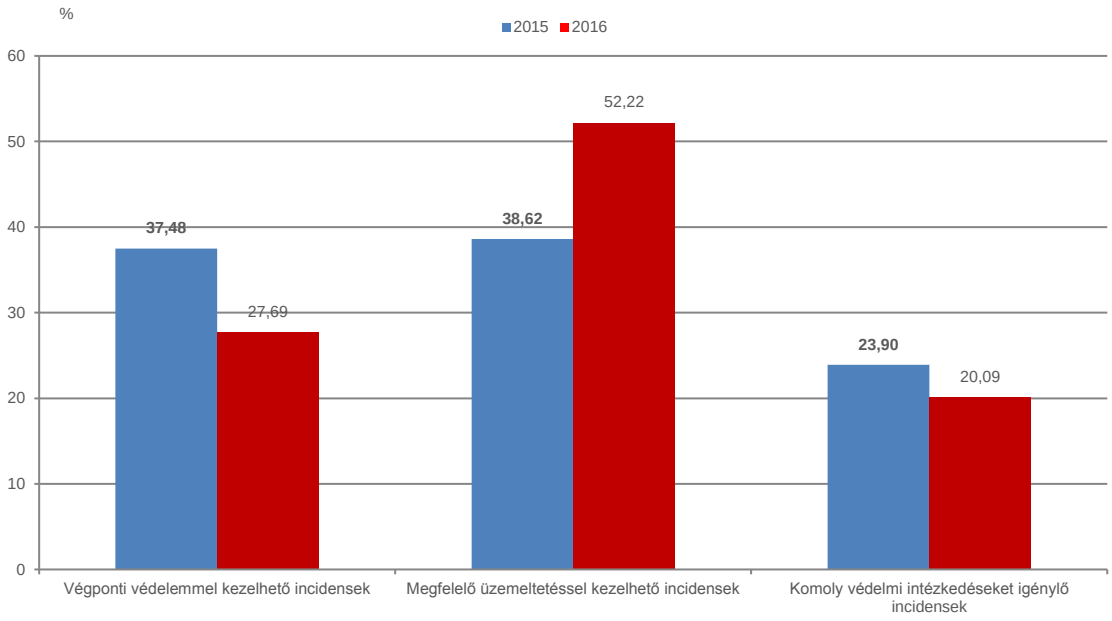


21. ábra Kibertámadások célpontjai 2018. március (saját szerkesztés, forrás: Hackmagaddon [139])

A Nemzeti Közszolgálati Egyetem gondozásában évente megjelentő Jó Állam Jelentés keretében 2017-ben Krasznay Csabával közösen megvizsgáltuk a magyar közigazgatás kiberfenyegetettségét.[56] Ennek felméréséhez a Nemzeti Kibervédelmi Intézet (továbbiakban NKI) által részünkre kiadott 2015-2016 évekre vonatkozó adatait használtuk. Tanulmányunkban kidolgoztunk három mutatótípust, amelyek alapján azonosítottuk a közigazgatás kiberfenyegetettségét. Ez alapján „Végponti védelemmel kezelhető incidensek”-nek neveztük azokat a támadástípusokat, amelyek a legalapvetőbb védelmi technikákkal kezelhető incidensnek minősülnek.[57] Második csoportnak a „Megfelelő üzemeltetéssel

[56] A tanulmány 2018 áprilisában még nem jelent meg.
[57] Például spamek, kártékony programok, botnetek.

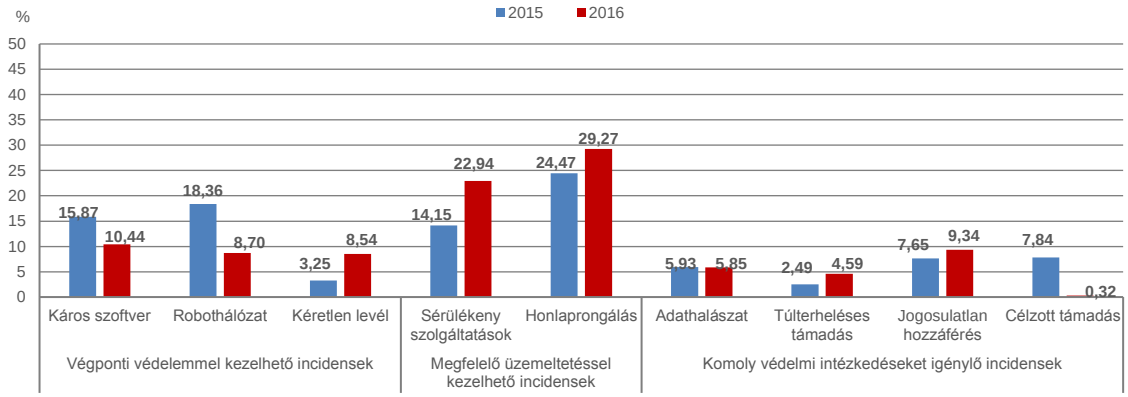
kezelhető incidensek”-et határoztuk meg, amelyek a rendszer-üzemeltetéshez, jellemzően az intézmény elektronikus szolgáltatásaihoz, szerverkörnyezetéhez kapcsolódnak.[58] A harmadik csoportba a „Komoly védelmi intézkedéseket igénylő incidensek” tartoznak, amelyek általában nehezen észlelhetők, kezelésükhöz jelentős infrastruktúra-beruházás, illetve a felhasználók részéről komoly biztonságtudatossági fejlesztés szükséges.[59] Az NKI részére a magyar közigazgatási szervezetek által bejelentett incidenseket figyelembe véve a 22. számú ábrán tüntettem fel a három incidens csoport 2015-2016-os években előfordulásának százalékos megoszlását.



22. ábra Kiberbiztonsági incidensek százalékos aránya kategóriák alapján 2015-2016 (szerkesztette NKE ÁKFI, Forrás: NKI)

A 23. számú ábrán tüntettem fel az egyes incidenstípusokat a három csoport alapján. Látható, hogy a „Végponti védelemmel kezelhető incidensek” számában 2016-ra csökkenés tapasztalható, aminek az okaként nevesíthető többek között a kormányhivatalok elterjedése, ami a munkaállomások központi üzemeltetésével és a hatásos védelmi technikák beszerzésével függ össze.

[58] Például honlaprongálással kapcsolatos támadások (defacement) vagy a sérülékeny szolgáltatások.
[59] Például túlterheléses támadás, adathalászat, célzott támadás, jogosulatlan hozzáférés.



23. ábra Incidenstípusok 2015-2016. (szerkesztette: NKE ÁKFI, forrás: NKI)

A „Megfelelő üzemeltetéssel kezelhető incidensek” megnövekedett számának hátterében elsősorban a megfelelő szakértő és szakértelem-hiány mutatkozik, ez a probléma napjainkra sem oldódott meg, és kérdéses, hogyan tudja az oktatás pótolni hiányukat [140]. A „Komoly védelmi intézkedéseket igénylő incidensek” számában kisfokú csökkenés következett be. Ezek a támadások jelentik a legnagyobb biztonsági kockázatot, gyakran azonban mégis észrevétlenek maradnak. Ez egyben azt is jelenti, hogy elképzelhető, a célpontok nem is érzékelik, hogy áldozatokká váltak.

Védekezés tekintetében a cél egyértelműen az, hogy „Végponti védelemmel kezelhető incidensek” és a „Megfelelő üzemeltetéssel kezelhető incidensek” kategóriájába sorolható támadások aránya csökkenjen a „Komoly védelmi intézkedéseket igénylő incidensek” számához képest, hiszen ennek megvalósulásával növelni lehet a közigazgatás kibervédelmi képességeit. Ennek oka, hogy a kisebb kockázatokat jelentő incidensek ellen meghozzuk azokat a rövidtávú fejlesztéseket, amik csökkentik a támadások számát, miközben kiépülnek azok az infrastruktúrák, amelyek lehetővé teszik a komolyabb incidensek észlelését, majd azok kezelését.

E célok értelemszerűen nem csak a közigazgatásra érvényesek, hanem a védelmi szféra egyéb területeire is. Ennek megvalósításához azonban elengedhetetlen a jogszabályi háttér, amelynek bemutatását a következő alfejezetben végzem el.

3.2. Az adat- és információbiztonságra vonatkozó normatív szabályozási környezet

Magyarországon a magánszféra védelmében az Alaptörvény jelenti a legfontosabb igazodási pontot a jogszabályi környezetben. Ez alapján:

„*(1) Mindenkinek joga van ahhoz, hogy magán- és családi életét, otthonát, kapcsolattartását és jó hírnevét tiszteletben tartsák.*

(2) Mindenkinek joga van személyes adatai védelméhez, valamint a közérdekű adatok megismeréséhez és terjesztéséhez.

(3) A személyes adatok védelméhez és a közérdekű adatok megismeréséhez való jog érvényesülését sarkalatos törvénnyel létrehozott, független hatóság ellenőrzi [141].”

Ebből bár következik, hogy a magánszféra védelme alkotmányos alapjog, ettől eltekintve mégsem sorolhatjuk az abszolút alapjogok körében, hiszen bizonyos tényezők megléte esetében, más alapjogok védelmében korlátozható, például a közbiztonság védelme érdekében.

Az Alaptörvényen felül a személyiségi jogok érvényesülésével a Polgári Törvénykönyv [142], illetve a személyes adatainkkal kapcsolatos bűncselekményekkel a Büntető Törvénykönyv [143] foglalkozik.

Az adat- és információvédelem biztosítása érdekében szükséges annak vizsgálata, hogy a közösségi oldalak használatával milyen adatokat állítunk elő. Az adatokat típusaik függvényében kategorizáljuk. Az Infotv. értelmező rendelkezéseit (3§) alapul véve megkülönböztetjük az alábbi adatfajtákat [80]

- *„személyes adat: az érintettel kapcsolatba hozható adat - különösen az érintett neve, azonosító jele, valamint egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző ismeret -, valamint az adatból levonható, az érintettre vonatkozó következtetés;*
- *különleges adat: (a) a faji eredetre, a nemzetiséghez tartozásra, a politikai véleményre vagy pártállásra, a vallásos vagy más világnézeti meggyőződésre, az érdek-képviseleti szervezeti tagságra, a szexuális életre vonatkozó személyes adat, (b) az egészségi állapotra, a kóros szenvedélyre vonatkozó személyes adat, valamint a bűnügyi személyes adat;*
- *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 és a külföldi minősített adat fogalmát. Ez alapján:

- *„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;*
- *külföldi minősített adat: az Európai Unió valamennyi intézménye és szerve, továbbá az Európai Unió képviseletében eljáró tagállam, a külföldi részes fél vagy nemzetközi szervezet által készített és törvényben kihirdetett nemzetközi szerződés vagy megállapodás alapján átadott olyan adat, amelyhez történő hozzáférést az Európai Unió intézményei és szervei, az Európai Unió képviseletében eljáró tagállam, más állam vagy külföldi részes fél, illetve nemzetközi szervezet minősítés keretében korlátozza."*

Nyilvánvalóan a közösségi média használatával minősített adatot nem állítunk elő, ahogy nem is férünk hozzá ilyen jellegű adatokhoz. Ettől eltekintve személyes és különleges adatok tömkelegét gyűjtik rólunk az egyes oldalak, telefonos applikációk. Személyes adat, amikor Facebookon megadjuk, mikor születtünk, hogy a barátaink soha ne felejtsenek el felköszönteni születésnapunkon. Személyes adat körébe tartozik rokonainak neve, az iskolák, amiket elvégeztünk, munkahelyünk stb. Felsoroltokon kívül megadhatjuk politikai, vallási meggyőződésünket, szexuális preferenciánkat, amelyek a különleges adat kategóriájába tartoznak. Azonban, ha nem is adjuk meg ezeket az adatokat, az általunk megosztott tartalmak alapján következtetni lehet ezekre. Szintén következtetéseket lehet levonni megosztásaink alapján a kórós szenvedélyeinkről (például minden héten vagy akár minden nap bejelentkezünk egy pubból). A különleges adatok körébe tartoznak az egészségügyi adataink, amelyekre nem csak a geolokációs helymeghatározásból gyűjtött adatok alapján lehet következtetni, például rendszeresen meglátogatjuk az Országos Onkológiai Intézetet, hanem a különböző egészségmegőrzéssel kapcsolatos alkalmazások, okos eszközök által gyűjtött adatok megszerzésével is. A telefonunkon tárolhatjuk az egyes mérési eredményeket, mint például pulzusszám, vérnyomás, vércukorszint stb., de feltölthetjük az egészségügyi dokumentumainkat is. Mindez egyébként rendkívül hasznos funkció lehet megfelelő védelem mellett. Egyes okos órák például 85%-os pontossággal előre jelezhetik a cukorbetegség kialakulását az általuk gyűjtött adatok elemzésével [145].

Mindezek miatt különösen fontos ezeknek az adatoknak és információknak a védelme, hiszen, ha nem teljesítik a „CIA" követelményeket, vagy nem megfelelő módon kezelik őket, igen komoly következményekkel járhat.

Az Infotv. alapján az adat kezelője és feldolgozója köteles megfelelő intézkedéseket tennie a fent megfogalmazottak megvalósulása érdekében. Az Infotv. 3§-a alapján az [80]:

- érintett: „*bármely meghatározott, személyes adat alapján azonosított vagy - közvetlenül vagy közvetve - azonosítható természetes személy*;
- adatkezelő: *„az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely önállóan vagy másokkal együtt az adat kezelésének célját meghatározza, az adatkezelésre (beleértve a felhasznált eszközt) vonatkozó döntéseket meghozza és végrehajtja, vagy az adatfeldolgozóval végrehajtatja*";
- adatkezelés: *„az alkalmazott eljárástól függetlenül az adaton végzett bármely művelet vagy a műveletek összessége, így különösen gyűjtése, felvétele, rögzítése, rendszerezése, tárolása, megváltoztatása, felhasználása, lekérdezése, továbbítása, nyilvánosságra*

hozatala, összehangolása vagy összekapcsolása, zárolása, törlése és megsemmisítése, valamint az adat további felhasználásának megakadályozása, fénykép-, hang- vagy képfelvétel készítése, valamint a személy azonosítására alkalmas fizikai jellemzők (pl. ujj- vagy tenyérnyomat, DNS-minta, íriszkép) rögzítése";

- adattovábbítás: „*az adat meghatározott harmadik személy számára történő hozzáférhetővé tétele*";
- adatfeldolgozás: „*az adatkezelési műveletekhez kapcsolódó technikai feladatok elvégzése, függetlenül a műveletek végrehajtásához alkalmazott módszertől és eszköztől, valamint az alkalmazás helyétől, feltéve hogy a technikai feladatot az adaton végzik*";
- adatfeldolgozó: „*az a természetes vagy jogi személy, illetve jogi személyiséggel nem rendelkező szervezet, aki vagy amely szerződés alapján - beleértve a jogszabály rendelkezése alapján kötött szerződést is - adatok feldolgozását végzi*";
- adatállomány: „*az egy nyilvántartásban kezelt adatok összessége*";

Az adatvédelmi incidens fogalmát 2015-től tartalmazza az Infotv.,[60] ez alapján „*személyes adat jogellenes kezelése vagy feldolgozása, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés*". Maga a fogalom összhangban áll az Ibtv-ben megfogalmazott biztonsági esemény fogalmával, amely Bodó Attila Pál megfogalmazásával „*együttes értelmezésével az elektronikus információs rendszerek által kezelt személyes adatokra vonatkozóan bekövetkezett jogsértések azonosítása – jogi szempontból – könnyebben elvégezhető [133].*"

Az Infotv. 15§-ának rendelkezése alapján, amennyiben az érintett kéri, a személyes adatot kezelő köteles az érintettet tájékoztatni a személyes adatainak kezeléséről, az esetleges adatvédelmi incidensekről, azok kezeléséről, következményeiről. Összefoglalva kijelenthetjük, hogy az Infotv. adatvédelem alatt a személyes adatok információbiztonságát érti.

Személyes adat kezelése az Infotv. 4§-a alapján kizárólag „*meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie.* [80]"

[60] Az Infotv 2015-ös módosítása a GDPR nyilvánosságra került szövegtervezetének ismeretében történt meg, annak érdekében, hogy megkönnyítse az új szabályzóra való átállást.

A közösségi oldalak az adatfeldolgozást gyakran automatizált folyamatként végzik. Az automatizált adatfeldolgozás különösen a profilozás esetében történik. Az Infotv 7§ alapján „*A személyes adatok automatizált feldolgozása során az adatkezelő és az adatfeldolgozó további intézkedésekkel biztosítja*

- *a jogosulatlan adatbevitel megakadályozását;*
- *az automatikus adatfeldolgozó rendszerek jogosulatlan személyek általi, adatátviteli berendezés segítségével történő használatának megakadályozását;*
- *annak ellenőrizhetőségét és megállapíthatóságát, hogy a személyes adatokat adatátviteli berendezés alkalmazásával mely szerveknek továbbították vagy továbbíthatják;*
- *annak ellenőrizhetőségét és megállapíthatóságát, hogy mely személyes adatokat, mikor és ki vitte be az automatikus adatfeldolgozó rendszerekbe;*
- *a telepített rendszerek üzemzavar esetén történő helyreállíthatóságát és*
- *azt, hogy az automatizált feldolgozás során fellépő hibákról jelentés készüljön [80].*"

E mellett az Infotv. 7§-a rendelkezik arról is, hogy „*az adatkezelőnek és az adatfeldolgozónak az adatok biztonságát szolgáló intézkedések meghatározásakor és alkalmazásakor tekintettel kell lenni a technika mindenkori fejlettségére. Több lehetséges adatkezelési megoldás közül azt kell választani, amely a személyes adatok magasabb szintű védelmét biztosítja, kivéve, ha az aránytalan nehézséget jelentene az adatkezelőnek*" [80].

2018. május 25-étől az Európai Unió tagállamaiban egységesen az Európai Általános Adatvédelmi Rendelet lép hatályba [146], és a GDPR rendelkezéseit kell alkalmazni tagállamokban korábban hatályos adatvédelmi szabályok helyett.[61] A Rendelet alapjául az Európai Parlament és a Tanács 95/46/EK irányelve szolgált [147]. Bár az irányelv rögzítette a személyes adatok kezelésének elveit, azonban nem határozta meg az adatvédelmi incidensek megsértésének következményeit. Az új adatvédelmi rendelet egyrészt az a hiátust pótolja, másrészt 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 [69].

[61] Az Infotv. tekintetében nem változnak például a közérdekű és közérdekből nyilvános adatok szabályozása vagy az Általános Adatvédelmi Rendelet által nem rendezett adatvédelmi előírások. Utóbbira példa a Nemzeti Adatvédelmi és Információszabadság Hatósággal (továbbiakban NAIH) kapcsolatos előírások.

A GDPR számos változást hoz az adatvédelem és adatbiztonság tekintetében, amelyre a felkészülést a magyar jogalkotók, ahogy fentebb is megfogalmaztam, már 2015-ben megkezdték, de az Infotv. módosítása csak 2018. július 26-án, a NAIH adatkezelési engedélyezési eljárására vonatkozó és akkreditációval kapcsolatos módosító rendelkezései [148] augusztus 25-én léptek hatályba[62]. A GDPR az adatvédelem megfogalmazását kiegészíti a kockázatok értékelésével, valamint a védekezés költségeinek mértékével „*a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja [146]*".

A Rendelet 32. cikke rögzíti továbbá az adatbiztonság megteremtésének érdekében elvárt intézkedéseket, és rendelkezik arról, hogy ahol szükséges:

- *„alkalmazni kell a személyes adatok álnevesített[63] 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;[64]*
- *a védelmi intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást kell az adatkezelőnek kialakítania."*

Az Infotv. -hez hasonló módon határozza meg a GDPR az adatvédelmi incidens fogalmát, amely ez alapján „*a biztonság olyan sérülése, amely a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását, jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi [146]*." Ebben a megfogalmazásban az Ibtv. -ben is megfogalmazott elvek jelennek meg, amelyek a vétlen

[62] Az Infotv. GDPR-al összefüggő változásairól bővebben lásd dr. Halász Bálint és szerzőtársai összefoglalóját. [149]

[63] 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*"

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

vagy jogellenes magatartásra vonatkoznak [133]. A GDPR adatvédelmi incidensre vonatkozó fogalma azonban csupán a személyes adatok biztonságára vonatkozik. Fontos azonban, hogy akár egyetlen egy érintett személyes adatainak sérelme esetén megvalósul az adatvédelmi incidens, abban az esetben is, ha az érintett magánszféráját csupán minimálisan sérti. Ez azt jelenti, hogy nem csak azok a tömeges adatvédelmi incidensek tartoznak bele, mint például a Cambridge Analytica botrány súlyos adatkezelési incidense, de azok az úgynevezett „soft" esetek is, amelyek során az üzemeltetésből fakadó, technikai vagy emberi hibákra visszavezethető incidensek is, ami például abból fakadhat, hogy tévesen másnak küldünk egy olyan e-mailt, amiben személyes adatok szerepelnek.

A GDPR, miután az adatkezelőnek tudomására jutott, 72 órás bejelentési kötelezettséget ír elő adatvédelmi incidensek bekövetkezése esetén a felügyelő hatóság részére.[65] [66] A bejelentési határidő elmulasztását igazolnia kell a késedelem okát. Kivételt képeznek a bejelentés alól azok az adatvédelmi incidensek, amelyek „*valószínűsíthetően nem jár[nak] kockázattal a természetes személyek jogaira és szabadságaira nézve*."

A GDPR legfontosabb változásai a kiszabható büntetésekben figyelhető meg. A 2018. május 25-ig hatályos magyarországi szabályozás alapján a kiszabható büntetés összege maximum 20 millió Forint. A GDPR hatálybalépését követően bejelentési és nyilvántartási kötelezettség megsértése esetén az eljáró adatvédelmi hatóság az adatkezelőt vagy -feldolgozót 10 millió euróig terjedő közigazgatási bírsággal, vagy vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 2 százalékát kitevő összeggel sújthatja. A két összeg közül a magasabbat kell kiszabnia a hatóságnak. Az adatkezelés (például hozzájárulás), az érintett jogainak, illetve a jóváhagyott adattovábbítási mechanizmusok alapelveinek megsértéséért 20 millió euróig terjedő közigazgatási bírsággal vagy a vállalkozások esetében az előző pénzügyi év világpiaci forgalmának legfeljebb 4 százalékának megfelelő mértékű bírság szabható ki- ugyancsak a magasabb összegre vonatkozó büntetést kell érvényadónak tekinteni. Figyelembe véve az igen magas büntetési tételeket, várhatóan növekedni fog a közösségi oldalak adatvédelmi gyakorlata. Mark Zuckerberg a már idézett Kongresszusi meghallgatásán azt nyilatkozta, fontolgatják, hogy a GDPR elveit nem csak az európai felhasználók esetében fogják betartani, hanem a többi Facebook felhasználó esetében is. Figyelembe véve, hogy 2017-ben az éves árbevétele 40,65 milliárd dollár volt, aminek a 4%-a 1,6 milliárd dollár, belátható, nem kevés pénzről van szó.

[65] Érdemes összevetni a CA adatkezelési incidensével 2015-ben, amit a Facebook 3 évvel később ismert csak el.
[66] Magyarország esetén a felügyelő hatóság a NAIH.

A GDPR-ban megjelenik a „Privacy by Design” elve, amelyet beépített adatvédelemként fordíthatunk [150]. Az elv lényege, hogy az adatbiztonságnak már az adatkezelési eljárások meghatározásakor fontos szempontnak kell lennie, nem a termék, szolgáltatás piacra lépése után kell foglalkozni vele. Kiss Attila megfogalmazásában, *„A kanadai „Privacy by Design” filozófiájának európai jogba ültetését megkísérlő rendelkezés értelmében az érintett magánszférájának védelmét és az adatvédelmi szabályozás elveit integrálni kell a különböző adatkezelő technológiák követelményrendszerébe, amely így a számítástechnikai és üzleti alkalmazások integráns részévé válik anélkül, hogy azok funkcionalitást korlátozná. Az elméletet kialakító volt adatvédelmi biztos elismeri a biztonság jelentőségét, de úgy kíván eredményeket elérni, hogy közben nem sérti szükségtelenül az érintettek széles körének magánszféráját, kölcsönös előnyökre törekszik [151].”* A „Privacy by Design” elv gyakorlati megvalósulásának egyik legfontosabb elemének az úgynevezett privát szférát erősítő technológiák (Privacy Enhancing Technologies, továbbiakban PET) fejlesztését, alkalmazását és terjedésük támogatását tekinthetjük [152]. A PET-ekre számos példát lehetne sorolni, a teljesség igénye nélkül csupán egyet említek. A Firefox böngészőhöz készült „Track me not”[67] nevet viselő böngészőkiegészítő egy 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.[68]

A weboldalak nyomkövetését segítik az úgynevezett sütik, eredeti terminológia szerint cookiek. Mivel a sütik lehetővé teszik a természetes személyek azonosítását, így a 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. Azonban 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

[67] Magyar fordításban „Ne kövess”.
[68] 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.

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.

A GDPR mellett gyakran említik a 2016-ban megkötött „Adatvédelmi Pajzs" nevű keretegyezményt [153], ami az Európai Unió és az Egyesült Államok esetében az EU állampolgárok adatainak külföldre továbbításával foglalkozik. A keretegyezmény azt volt hivatott rendezni, hogy az európai és amerikai adatvédelmi gyakorlat jelentős eltérése okán az EU állampolgárok adatait szigorúbb adatvédelmi előírások alapján kezeljék az amerikai vállalatok. Végül az „Adatvédelmi Pajzs" nem képezi a GDPR részét.

A GDPR egyfajta kiegészítése lenne az Európai Parlament és Tanács elektronikus hírközlési rendelete [154], azonban az értekezésem írása idején ezt még nem fogadták el.

A GDPR mellett fontos változást jelent a szintén 2018 májusától érvényes hálózati és információs rendszerek biztonságáról szóló irányelv (Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, továbbiakban NIS irányelv) [155]. A NIS irányelv megalkotásának előzményei a 2. fejezetben ismertetett európai stratégiai fejlődésre vezethetőek vissza. Az irányelv célja, hogy az EU tagállamai képesek legyenek a kibertér jelentette fenyegetések ellen hatékonyan védekezni, ily módon pedig létrejöjjön egy egységes hálózati- és információs rendszerek biztonságára vonatkozó, általános uniós szint. Ennek megvalósítása érdekében a tagállamok:

- *„kidolgozzák saját, nemzeti szintű kiberbiztonsági stratégiájukat;*
- *elektronikus információbiztonságért felelős hatóságot jelölnek ki;*
- *kijelölnek egy vagy több biztonsági eseménykezelő csoportot;*
- *azonosítják és kijelölik a NIS irányelv hatálya alá tartozó adatkezelőket [137].”*[69]

Mivel irányelvként fogadták el a jogszabályt, így a tagállami jogalkotók maguk határozhatják meg, hogy milyen módon implementálják az irányelvben megfogalmazottakat a tagállami joganyagokba. Az irányelv[70] hatálya kiterjed az alapvető szolgáltatást nyújtó szereplőkre és azokra a digitális szolgáltatókra, amelyeknek a szolgáltatásait az alapvető szolgáltatók is igénybe veszik. Nem terjed ki a hatálya „(1)*a mikro- és kivállalatokra, (2) más*

[69] Magyarországon ezt a szerepet a Kormányzati Eseménykezelő Központ látja el 2016-tól.
[70] Ez alapján az energiaszolgáltatás, közlekedés, banki szolgáltatás, pénzügyi piaci infrastruktúrák, egészségügy, ivóvízellátás és ivóvízelosztás, továbbá a digitális infrastruktúra ágazatában működő – tagállami szinten kijelölt- közjogi vagy magánjogi szervezet [137].

EU-szintű, az IT-biztonságot érintő ágazati szabályozás hatálya alá (is) tartozó szereplőkre, (3) a nemzeti ágazati kijelölési kritériumokat nem teljesítő, alapvető szolgáltatást nyújtó szereplőkre, (4) hardvergyártókra és szoftverfejlesztőkre [137]."

A NIS irányelv 4. cikke hálózati és információs rendszerek biztonsága alatt a rendszer azon képességét érti, amely szerint *„adott bizonyossággal ellenálljon az olyan cselekményeknek, amelyek veszélyeztetik a rajtuk tárolt, továbbított vagy kezelt adatok vagy az említett hálózati és információs rendszeren nyújtott vagy rajta keresztül elérhető, kapcsolódó szolgáltatások rendelkezésre állását, hitelességét, sértetlenségét és bizalmasságát [155]".*

A NIS irányelv az Ibtv. -hez hasonlóan a kockázatokkal arányos alapevet deklarálja, amely szerint a védelem mértékének arányosnak kell lennie az adott rendszert érintő kockázatokkal. Az Ibtv. hatálya alá eső szervezeteket biztonsági osztályba és szintbe kell sorolni. Az Ibtv alapján biztonsági osztálynak nevezzük „az elektronikus információs rendszer védelmének elvárt összességét [81]". A biztonsági osztályba sorolás „*a kockázatok alapján az elektronikus információs rendszer védelme elvárt erősségének meghatározása [81]".* Ennek megfelelően a biztonsági osztályokat 1-től 5-ig számozott fokozatok alapján kell elrendelni, a számozás emelkedésével párhuzamosan szigorodnak a megvalósítandó védelmi követelmények. Biztonsági szint *a szervezet felkészültsége az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére*. Biztonsági szintbe sorolás: „*a szervezet felkészültségének meghatározása az e törvényben és a végrehajtására kiadott jogszabályokban meghatározott biztonsági feladatok kezelésére*" [81].

Az Ibtv. -ben meghatározott biztonsági osztályok és szintekbe történő sorolás témám szempontjából a kockázatokkal arányos védelem megteremtésében játszik szerepet, ami az adat- és információbiztonsági tudatosság közösségi média használatából fakadó kockázataival, illetve a használat szabályozásával függ össze.

A jogszabályi környezet vizsgálatakor szükséges röviden a technikai adatgyűjtés szabályozásáról is szólni. E tekintetben a NAIH jelentése iránymutató, amelyet „A Nemzeti Konzultáció honlapján a Yandex.Metrica analitikai szolgáltatás igénybevételével összefüggésben indított vizsgálatáról" néven fogalmazott meg [156]. 2017 nyarán indított online Nemzeti Konzultáció során derült ki, hogy az üzemeltető Yandex.Metrica analitikai szolgáltatás sértheti az adatvédelmi szabályozást az által, hogy nem megengedett módon gyűjti a felhasználók adatait, és azt harmadik fél részére továbbítja. A vizsgálat megállapította, 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 [156]." Ahogy korábban volt szó róla, ily módon nem csak az e-mail cím fejthető vissza, de olyan technikai adatok is, mint például a felhasználók IP címe, amelyből, ha nem használ különböző védelmi eljárásokat, egyértelműen helyreállítható a természetes személlyel a kapcsolat. Az adatkezelés módját a jelentés alapján nem csupán a személyes adatok technikai feldolgozására érti, hanem a feldolgozás módjára is. Ebbe beletartozik a technikai feldolgozáshoz kapcsolódó eljárások átruházásának lehetősége az adatfeldolgozó részére. Az adatfeldolgozónak vizsgálnia kell, hogy a tervezett tevékenységük ellátása érdekében szükséges-e a személyes adatok kezelése. Amennyiben a tervezett cél megvalósítható anélkül, hogy nem kezelik a személyes adatokat, úgy e szerint kell eljárni. Megítélésem szerint ez az elv különösen fontos a közösségi oldalak, illetve az okos mobil eszközökre optimalizált alkalmazások tekintetében.

3.3. Adat- és információbiztonság közösségi médiával kapcsolatos szabályozása a honvédelmi-, rendvédelmi- és nemzetbiztonsági szervezetek esetében

Az előző fejezetben igazoltam, hogy az adat- és információbiztonsággal kapcsolatos magyarországi szabályozás Európai Uniós viszonylatban is előrehaladott. Az Infotv. sok tekintetben a május 25-étől hatályos GDPR-ral összhangban áll, így akik betartották az Infotv. rendelkezéseit, nem lesz nagy változás az adatkezelési gyakorlatukban.

A közösségi média használattal kapcsolatban azonban véleményem szerint a jogszabályalkotás hiányos. Irányadónak tekinthetjük a NAIH által kiadott tájékoztatást a munkahelyi adatkezelések alapvető normáiról [157], amelyben a munkáltatók álláspályázók közösségi oldalának előzetes megtekintésének szabályait tisztázza. A Hatóság elismeri, hogy a munkáltatónak joga van megtekinteni a jelentkező közösségi oldalait, azonban ezt csupán bizonyos korlátozások mellett hajthatja végre. Ilyen korlátozás:

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

Ez utolsó két pont azonban úgy gondolom, ellentmondás. Valakinek a nyilvános Facebook profiljának a megtekintése során a megosztásaiból, főleg, ha minél több adat áll rendelkezésre, olyan következtetéseket vonhatunk le, amely a magánéletére, de akár párkapcsolati, vallási meggyőződésére, politikai nézeteire is utal. Azt gondolom, életszerűtlen az a fajta vizsgálat, hogy miközben megtekintjük valaki nyilvános profilját, a szemünk átugorja például azokat a megosztásokat, amelyek a hétvégi szórakozásról, hírek, politikai vélemények közzétételéről szól. Ha be is tartjuk ezt, csak úgy tudjuk megállapítani, hogy valami magánszférára, párkapcsolatra, vallási meggyőződésre, politikai nézeteire vonatkozik, ha beleolvasunk például a megosztott hír címébe, látjuk a feltöltött fényképet stb. Ezek akarva- akaratlanul következtetések levonására alkalmasak, ily módon annak betartása, hogy a nevesített adatokkal kapcsolatban nem végezhető a megismerés, véleményem szerint nem biztosítható.

Egy személy nyilvánosan megosztott tartalmainak a megismerésére, mint ahogy korábban már utaltam rá, nem szükséges hosszadalmas adatgyűjtés, bizonyos oldalak segítségével percek alatt strukturáltan kaphatjuk meg a számunkra releváns adatokat. A módszer ismertetését a negyedik fejezetben látom el, itt csupán azért szükséges megemlíteni, mert segítségével a honvédelmi-, rendvédelmi-, nemzetbiztonsági szolgálatok alkalmazottairól, de akár családtagjairól is könnyű nyílt forrásból információkat gyűjteni, ezért különösen fontos annak szabályozása, e személyek milyen formában lehetnek jelen a közösségi oldalakon.

Azt gondolom, alapvetően nem tiltható a közösségi oldalakon való regisztráció, leszámítva bizonyos munkaköröket. Ilyen munkakör egyértelműen a nemzetbiztonsági területekhez kapcsolódik. Arra vonatkozóan civil kutatóként értelemszerűen nem találtam belső utasításokat, határozatokat, ami a nemzetbiztonsági szolgálatok munkatársainak közösségi médiában való jelenlétnek szabályozásával kapcsolatos, de az ezeken a területeken dolgozókkal folytatott beszélgetéseim során megerősítették azt a feltételezésemet, hogy számukra nem engedélyezett a közösségi oldalon történő regisztráció. Ez persze nem jelenti azt, hogy egyes munkakörökben feladataik ellátása érdekében nem használnak különböző álprofilokat – például

pedofilhálózatok, szervezett bűnözők felderítése érdekében-, azonban ezek a profilok a konspirációs szabályok betartása mellett léteznek, a használó(k) valódi identitására nem utalnak, azokból nem lehet a valódi személyes adataikra következtetést levonni.

Korlátozott módon a kulcsfontosságú vezetők esetében megengedhető a közösségi média használata, azonban az információbiztonság szabályainak szigorú betartása mellett. Esetükben fontos tényező lehet az is, hogy egyes katonai vagy rendőri vezetők beosztásuknál fogva a közösségi médiát a stratégiai kommunikáció eszközeként használják a transzparencia jegyében. Az Egyesült Államok katonai vezetői úgy vélem jó példával szolgálnak e tekintetben, hiszen különböző közösségi média profilokat használnak. Ide sorolhatjuk többek között James Mattis tábornokot, aki az értekezésem írásának idején védelmi miniszteri beosztást tölt be vagy Mark A. Milley tábornokot, a szárazföldi erők vezérkari főnökét. Természetesen ezeket a profilokat nem az érintett személyek kezelik, hanem kommunikációs stábok, és nem is személyes profilok, hanem oldalak.

Annak függvényében, hogy a Magyar Honvédség vagy a Rendőrség állományában szolgálatot teljesítő személy milyen típusú adatokhoz fér hozzá, szintén célszerű a minősített adatokhoz hozzáférő személyek esetében megtiltani a közösségi oldalak használatát. Ennek oka egyrészt a profilozáshoz vezet vissza, hiszen róla is gyűjthetők olyan adatok, amelyekkel akár zsarolni is lehet. Ehhez nem csupán nyílt forrású információgyűjtés használható, hanem az esetleges privát beszélgetéseihez történő hozzáférés is. Edward Snowdentől tudjuk, hogy az amerikai nemzetbiztonsági szolgálatok valós időben tudták megfigyelni a felhasználók privát üzeneteit is, de rajtuk kívül különböző kémprogramok segítségével más országok nemzetbiztonsági szolgálatai, hackerek, kiberbűnözők, terroristák, hacktivisták is hozzáférhetnek ezekhez az információkhoz.

Az ilyen típusú kockázatok kezelésére a jelenleg érvényben levő hazai szabályozás nem ad válaszokat. Megvizsgáltam a Magyar Honvédségre és a Rendőrségre vonatkozó ezekkel kapcsolatos törvényi előírásokat, és bár találunk a közösségi média használatával kapcsolatos előírásokat, ezek azonban véleményem szerint több kiegészítésre, és több terület pontosabb szabályozására szorulnak.

A Magyar Honvédség esetében a 2012. évi CCV. törvény a honvédek jogállásáról [158] (továbbiakban Hjt.) és a 72/2011. (VI. 30.) HM utasítás a Honvédelmi Minisztérium és a Magyar Honvédség külső kommunikációjának rendjéről [15] 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.[71]

A Hjt. az „Általános magatartási követelmények" kapcsán az alábbiak szerint fogalmaz:

„*5. § (1) A szolgálati viszonyban a szolgálat érdekének elsődlegességét, valamint a Honvédség iránti közbizalom megóvását szem előtt tartva kell eljárni.*

(1a) Az állomány tagja szolgálatteljesítési időn kívül sem folytathat olyan tevékenységet, nem tanúsíthat olyan magatartást, amely a honvéd etika szabályait sérti, a szolgálati viszonyhoz méltatlan, vagy amely a pártatlan, befolyástól mentes tevékenységét veszélyeztetné [158]."

„Az egyes alapvető jogok gyakorlatának korlátozása" rész pedig az alábbiakról rendelkezik:

„21. § (1) A honvédségi szervezet területén a gyülekezési jog alapján nyilvános rendezvény csak a munkáltatói jogkört gyakorló engedélyével tartható.

(2) Nem engedélyezhető a rendezvény, ha az

a) politikai célt szolgál,

b) a szolgálati feladat, a szolgálati rend és fegyelem ellen irányul, vagy azt bírálja,

c) a Honvédség iránti közbizalom megingatására alkalmas vagy

d) a Honvédség feladataival ellentétes célra irányul.

22. § (1) Az állomány tagja nem csatlakozhat olyan szervezethez, amelynek tevékenysége a Honvédség feladataival ellentétes.

(2) A szolgálati viszonyhoz nem kapcsolódó szervezettel fennálló, vagy újonnan létesülő tagsági viszonyát az állomány tagja köteles írásban haladéktalanul bejelenteni a munkáltatói jogkört gyakorlónak. A tagsági viszony nem tartható fenn, vagy nem létesíthető, ha azt a munkáltatói jogkört gyakorló írásban megtiltja, mert az a katonai szolgálattal vagy a szolgálati beosztással nem egyeztethető össze, a szolgálat érdekeit sérti vagy veszélyezteti.

(3) Az (1) és a (2) bekezdést alkalmazni kell a politikai célt szolgáló szerveződéshez való csatlakozásra és az abban történő részvételre is, függetlenül attól, hogy annak tevékenysége vagy programja utólag válik ismertté.

(4) A szerződéses állomány tagja a szolgálati viszonya idejére a párttagságát köteles felfüggeszteni.

23. § (1) Az állomány tagja

a) párt nevében vagy érdekében közszereplést kizárólag a szolgálati viszonyának szüneteltetése idején vállalhat,

[71] Személyes beszélgetések során hívták fel a figyelmem a 87/2011 MH ÖHP intézkedésre, ami 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 tárgyalom az alfejezetben.

b) a parancsot nem bírálhatja, arról jog- és érdekérvényesítő tevékenysége körén kívül véleményt nem mondhat,

c) a szolgálati rendet és a fegyelmet sértő nyilatkozatot nem tehet,

d) a sajtónyilvánosság igénybevételével hivatalos eljárásban magánvéleményt nem nyilváníthat,

e) nem állíthat elő, nem terjeszthet, nem tehet közzé, nem jelentethet meg, és nem hozhat nyilvánosságra a szolgálati rendet és fegyelmet veszélyeztető sajtóterméket, ilyen tartalmú kiadványt, plakátot, hirdetményt, emblémát, más szöveges vagy képi adatot [158].”

Tekintettel arra, hogy a nagy közösségi oldalak, mint például a Facebook is a nyilvánosság színterei, még akkor is, ha ez a nyilvánosság korlátozott, és csak ismerőseink előtt valósul meg, lehetőséget teremtenek arra, hogy az idézett jogszabályi előírásokat a felhasználó megsértse. A kibertérben zajló interperszonális interakciók nem követelik meg, hogy például politikai tüntetésen vegyen részt a fizikai dimenzióban, a tüntetésre létrehozott eseményre adott reakcióval már megvalósulhat mindez. Nem ennyire egyértelmű a helyzet a 22. § esetén, hiszen attól eltekintve, hogy egy zárt Facebook csoport nem tekinthető bejegyzett szervezetnek, a csoport működése, belső szabályai, céljai lehetnek hasonlóak bejegyzett szervezetekhez. Ezen belül pedig tanúsíthat a felhasználó olyan viselkedést, ami ellentétes a Hjt-ben megfogalmazottakkal. Az egyik legizgalmasabb kérdés véleményem szerint a 23. §, ugyanis 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.

Ahogy korábban is utaltam már rá, vita zajlik arról, hogy a Facebook minek tekinthető. A törvényhozók és a média szereplői szeretnék, ha maga a közösségi hálózat is sajtóterméknek minősülne, és ez alapján a sajtóra vonatkozó jogszabályok legyenek érvényesek rá. Tekintettel arra, hogy a Facebookra a magyar lakosság jelentős része elsődleges hírforrásként tekint, a megosztások nagy része hírekkel kapcsolatos, azt gondolom, mindenképpen érvényes rá a sajtónyilvánosság fogalma. 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*” [159].

Véleményem szerint nem csak az 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.

Mielőtt konkrét javaslatokat fogalmaznék meg, úgy gondolom, a Rendőrség esetében is érdemes megvizsgálni a hatályos jogszabályi előírásokat, mert egyrészt számos közös pontot határozhatunk meg, amik az információbiztonság esetében érdemes azonosként kezelni, másrészt a Rendőrség esetében van egy előremutató ORFK utasítás, azonban ez is jelentős kiegészítést kíván meg.

A 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról [160] (továbbiakban Hszt.) a Hjt-hez szinte szó szerint hasonló megkötéseket alkalmazza a „Véleménynyilvánítás szabadsága" résznél. A 21. § előírása szerint

„*1) A hivatásos állomány tagja a részére kiadott parancsot, intézkedést - a 103. §-ban meghatározott esetet kivéve - nem bírálhatja, arról a jog- és érdekérvényesítő tevékenysége körén kívül véleményt nem mondhat, a szolgálati rendet és a fegyelmet sértő nyilatkozatot nem tehet, a sajtónyilvánosság igénybevételével hivatalos eljárásban magánvéleményt nem nyilváníthat.*

(2) A szolgálati rendet és a fegyelmet veszélyeztető sajtóterméket a hivatásos állomány tagja nem állíthat elő és nem terjeszthet, ilyen tartalmú plakátot, hirdetményt vagy emblémát nem függeszthet ki.

(3) Az országos parancsnok és az országos főigazgató közjogi szervezetszabályozó eszközben megtilthatja, hogy a hivatásos állomány tagja az internetes felületen magánszemélyként való megnyilvánulásakor, magánvélemény nyilvánításakor a hivatásos állományba tartozására vonatkozó adatot hozzon nyilvánosságra [160]."

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 [161] rendkívül fontos megállapítást tesz, amikor a védendők körébe beemeli a hivatásos állomány tagjának közeli hozzátartozóit. A Rendőrség esetében a hivatásos állományba tartozásra vonatkozó adat nyilvánosságra hozatala azért is fontos, mert a 2006-2010 között lezajlott politikai tüntetések esetén a szélsőjobboldalhoz kötődő szervezetek[72] a tüntetéseket biztosító rendőrökről az akkori jogszabályok szerint

[72] Például a Kuruc.info.

törvényesen készítettek fényképeket, [73] és a közösségi profiljaik felkutatásával listázták őket, és olvasóikat bíztatva igyekeztek új információkkal kiegészíteni az általuk csak „AVH" -sok listáját. Bár az ilyen listákra felkerült rendőröket nem érte atrocitás, nem nehéz belátni ennek lélektani súlyát. A 11/2015. (VII. 10.) ORFK utasítás tehát indokoltan tiltja meg, hogy a hivatásos állomány tagjai internetes felületeken magánszemélyként megosszák a Rendőrség állományába való tartozás tényét, beosztásukat, rendfokozatukat, illetve a Rendőrség állományába tartozásukra utaló képet, videót, hangfelvételt. Az utasítás azt is rögzíti, amennyiben az állomány tagja nyilvánosságra hozta korábban ezeket az információkat, és magánszemélyként kíván megnyilvánulni, úgy köteles törölni az erre vonatkozó információkat. Kivételt képez ez alól, ha a magánvélemény közzététele „*a szolgálati időn kívül végzett tudományos, oktatói, művészeti, lektori, szerkesztői, a jogi oltalom alá eső szellemi tevékenységével összefüggésben*" valósul meg [161].

Legyen szó a Magyar Honvédség vagy a Rendőrség állományba tartozó személyről, mindkét esetében véleményem szerint helyes annak tilalma, hogy az állományba tartozás tényét a regisztrációs adatok között feltüntesse. Bár az ORFK utasítás megengedi, hogy az állományba tartozás tényének elfedését követően magánvéleményét megossza a nyilvánossággal, ahogy azt a Hjt. és a HM utasítás kapcsán is írtam, ennek szabályait célszerű pontosítani az ott megfogalmazottak alapján.

Fontos, hogy a közösségi oldalakon alkalmazható adatvédelmi beállítások során a legszigorúbb beállításokat alkalmazzák. Ez nem csak azért fontos, mert ennek hiányában az egyén profilozását könnyíthetjük meg, de ugyanúgy segíthet kapcsolati hálójának feltérképezésében, ami értelemszerűen a kollegiális viszonyok kapcsán külön kockázatot jelent [162].

Nyílt forrású információgyűjtéssel nem csak a felhasználó által megosztott tartalmakat szerezhetjük meg, de Facebookon többek között például az általa használt alkalmazásokat, csoportokhoz való tartozását, oldalak kedvelését, meglátogatott helyeket, más személyek által megosztott fényképekhez, tartalmakhoz való hozzászólásaikat. Komoly adatvédelmi kockázatot jelent ez utóbbi, hiszen a saját megosztásaink kapcsán dönthetünk a korlátozott nyilvánosságról, de ismerőseink esetében erre nem nyílik módunk. Amennyiben olyan személy megosztásához szólunk hozzá, kedveljük, aki nem korlátozza a nyilvánosságot, úgy a mi hozzászólásaink is nyilvánosak lesznek, ezáltal kereshetőek. Mivel olyan tartalmat egyébként sem lehet megosztani nyilvánosság előtt, amit a jogalkotó a Hjt-ben és Hszt-ben is külön

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

nevesített, információbiztonsági szempontból érdemes a szabályzóban felhívni a figyelmet arra, hogy a magánélettel összefüggésben megosztott tartalom, 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, amennyiben a fenti kitétel nem valósul meg, úgy nem javasolt a tervezett tartalom megosztása.

Egyik hatályos szabályozó sem foglalkozik a technológiai adatgyűjtésből származó kockázatokkal, ezért a kiegészített szabályozókban mindenképpen szükséges az ezekkel kapcsolatos eljárások rögzítése. Az okos mobil eszközök, internetes oldalak, közösségi oldalak használata, ahogy az előző alfejezetekben is írtam, számtalan olyan lehetőséget biztosít, amelyekkel valós időben, akár tömegesen figyelhetőek meg a személyek. Fontos rögzíteni, attól, hogy egy beszélgetés privát módon is történik meg, nincs garancia arra vonatkozóan, hogy az érintetteken kívül harmadik fél nem fér hozzá a beszélgetés tartalmához. Ez egyben azt jelenti, hogy ezeken a felületeken célszerű kerülni az intim témákat, hiszen azok harmadik fél kezében akár befolyásolásra, akár zsarolásra is használhatóak. Szükségesnek tartom az okos mobil eszköz használatra vonatkozó szabályok kidolgozását is, amelyek vonatkoznak az alkalmazások használatára (figyelembe véve az alkalmazásengedélyeket), a Wi-fi hálózatok biztonságára, a megfelelő védelmi eljárások használatára (az operációs rendszer és az alkalmazások rendszeres frissítése, lehetőség szerint VPN, titkosítást alkalmazó kommunikációs alkalmazások használata stb.). Nyilvánvalóan az ilyen jellegű védelmet nem csupán okos mobil eszközök esetében kell alkalmazni, hanem minden olyan informatikai eszközön, amit az állomány tagjai használnak szabadidejükben. Ebben a korábban ismertetett PET-ek jó kiindulási alapot jelentenek. A jogszabály nyilvánvalóan nem tudja követni a technológiai fejlődést, ráadásul rendszeresen derül fény olyan új típusú sebezhetőségekről, amelyek korábban biztonságosnak hitt eljárásokat semmisítenek meg (gondoljunk csak például a 2017 novemberében megismert WPA2 sebezhetőségre, ami a Wi-Fi titkosítását játszotta ki), ezért elengedhetetlen, hogy az állomány tagjai mindig naprakészek legyenek. Ennek érdekében véleményem szerint meghatározott időközönként a témával kapcsolatos tudatosító előadásokon való részvétel előírása célszerű, valamint továbbképzési programok kötelező elemévé kell váljanak az adat- és információbiztonsággal kapcsolatos kurzusok.

Az eddig megfogalmazottak az általános használatra vonatkoztak, azonban nem szabad elfejteni, hogy műveleti területen is használnak közösségi oldalakat a hozzátartozókkal való kapcsolattartás okán, valamint használnak okos mobil eszközöket, amiket különböző telepített alkalmazások a technikai adatgyűjtés miatt még komolyabb kockázatot jelentenek. Mi sem

igazolja ennek fontosságát jobban a 2018 januárjában történt esetnél, amikor egy fitness alkalmazás által nyilvánosságra hozott több mint háromtrillió GPS-adatból, ami a felhasználók útvonalát rögzítette, sikerült lokalizálni az amerikai katonai bázisokat (példaként az afganisztáni Helmand tartományt nevesítve), hiszen az ott szolgálatot teljesítők edzés közben használták az alkalmazást [163]. A műveleti biztonság érdekében szükséges az okos mobil eszköz használatának korlátozása, tiltva minden olyan alkalmazás használatát, ami geolokációs helymeghatározást alkalmaz, a kapcsolattartásra pedig magas szintű titkosítást alkalmazó program használatát javasolt engedélyezni.[74]

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, ami az alfejezetben tárgyaltak mintájára konkrétabb előírásokat fogalmaz meg a Magyar Honvédség és a Rendőrség állományába tartozók számára.

3.4. Adat- és információbiztonsági tudatosság felsőoktatási hallgatók körében

Értekezésem egyik kulcskérdése az adat- és információbiztonsági tudatosság, amelyben a közösségi média használatának rendkívül nagy szerepet tulajdoníthatunk. Ahogy korábban megfogalmaztam, a megfelelő digitális immunitás megteremtésében az oktatás különösen fontos. A Nemzeti Közszolgálati Egyetem hallgatói e tekintetben úgy vélem, megkerülhetetlenek, hiszen az egyetem elvégzését követően az állami szféra különböző területein fognak elhelyezkedni. Amennyiben hallgatóink nem részesülnek olyan, az adat- és információbiztonsági tudatossággal kapcsolatos oktatásban, amelynek segítségével felismerhetik a fenyegetéseket, magas fokú kockázatot jelentenek az őket foglalkoztató szervezet számára. Ezek a szervezetek, jogszabályban meghatározott feladatainak elvégzése közben különböző típusú adatokat kezelnek, amelyek megszerzése nem csak az idegen államok nemzetbiztonsági szolgálatainak, de kiberbűnözőknek, terroristáknak és hacktivistáknak is egyaránt értékes.

A hírszerzés történelemben nem egyedi elgondolás, hogy idegen államok nemzetbiztonsági szolgálatai azokat a pályájuk elején álló személyeket tartják beszervezésre

[74] Például a Signal nevű alkalmazást.

érdemesnek, akik vélhetően a karrierjük során fontos beosztásokba fognak kerülni. Egy, az egyetemi éveit töltő fiatal kevésbé óvatos, nem feltétlenül tartja fontosnak az adat- és információbiztonságot, így róluk több kompromittáló adat gyűjthető. Az ilyen jellegű beszervezésre Kim Philby és társai, az úgynevezett Cambridgei Ötök szolgálnak a legjobb példával [164]. Nevezett eset az 1930-as években vette kezdetét, amikor Alexander Mihajlovics Orlov ezredes a cambridge-i Trinity College hallgatóit környékezte meg, és sikeresen szervezte be szovjet ügynöknek Kim Philbyt és társait. Az ideológiai meggyőződés mellett azért nagy szerep jutott annak is, hogy Guy Burgess és Anthony Blunt bizonyítottan homoszexuálisok voltak, Donald Duart Maclean pedig biszexuális volt, ami ebben az időben Nagy-Britanniában igen komoly bűnnek számított. Cambridgben végzett hallgatók rendszerint fontos beosztásba kerülnek a politikai, katonai, gazdasági területen. Nem volt ez másképp Philbyvel és társaival sem, Philby az MI-6 tisztjeként fokozatosan lépett előre, mígnem az amerikai Központi Hírszerző Ügynökség és az MI-6 összekötő tisztje nem lett. Ily módon a szovjetek nem csak a brit titkokhoz férhettek hozzá, hanem az amerikaiakhoz is.

Az eset tanulságait úgy vélem, a Nemzeti Közszolgálati Egyetem hallgatói tekintetében is érvényesnek kell tekintenünk. Ennek alapján végeztem el az Egyetem hallgatóinak körében egy kérdőíves felmérést, hogy az adat- és információbiztonsági tudatossággal kapcsolatos ismereteiket értékelve a konzekvenciákat beépíthessük az adat- és információbiztonsági tudatossággal kapcsolatos képzésekbe.

A kérdőívem elkészítésekor áttanulmányoztam az információbiztonsági tudatosság humán aspektusával foglalkozó nemzetközi szakirodalmakat, és e-mailben megkerestem azokat a szerzőket, akik a témában kérdőíves felméréseket végeztek [165] [166] [167] [168] [169] [170] [171] [172]. A kérdőívem megalkotásakor végül a Parsons és szerzőtársai által 2017-ben újra lefolytatott vizsgálatainak kérdéseit vettem alapul [173], és reprodukáltam a szerzők engedélyével. A kérdőív alapjául a Tudás- Képesség- Viselkedés modell (Knowledge– Attitude– Behaviour) szolgált, amely a kompetenciafejlesztés területén használt eljárás. Ez alapján a „Tudáshoz” soroljuk az ismeret jellegű elemeket (elvek, elméletek, tények ismeretét). A „Képesség” a „Tudás” alkalmazásának képességét jelöli, amelynek során az egyén megoldja a felmerülő problémákat. A „Viselkedés” a tényleges viselkedésformákat jelenti. Ennek megfelelően az adott kérdéseket a kompetencia felmérésekor általánosan használt megfogalmazások szerint fordítottam le. A tudásra vonatkozó kérdések esetében a „tudom”, „ismerem”, „megértem”, „azonosítom”, „felismerem” jellegű állításokat, a képességre vonatkozó kérdések esetében a „képes vagyok felismerni”, „képes vagyok figyelembe venni”

stb. jellegű állításokat, míg a viselkedésre vonatkozó kérdések esetében „tudatosan használom”, „törekszem” stb. típusú állításokat fogalmaztam meg. A kitöltők öt fokozatú skálán adhatták meg a válaszokat, amelyen a skála első foka az „egyáltalán nem értek egyet vele”, míg az ötödik foka a „teljes mértékben egyetértek vele” válasz volt.

A kérdőívet a Nemzeti Közszolgálati Egyetem alap-, mester- és doktori képzésében, nappali és levelező képzési formában résztvevők körében, valamint az Ibtv. által az Egyetemre delegált Elektronikus információbiztonsági vezető (továbbiakban EIV) szakirányú továbbképzés jelenlegi és végzett hallgatói körében végeztem el. Az EIV-s hallgatókat külön kezelem, ugyanis ők a képzés során kifejezetten adat- és információbiztonsággal kapcsolatos kurzusokat hallgatnak. Esetükben azonban alacsony kitöltési számot értem el (n=25), így azt nem vizsgáltam végül. A kérdőív megalkotása során feltételeztem, hogy minél több adat- és információbiztonsági tudatossággal kapcsolatos órát, kurzust hallgat a kitöltő, annál magasabb szintű tudatosság jellemezi. A kérdőívek kitöltésének idején több megkeresést kaptam személyesen és e-mailben, amelyek a kérdőív kiértékelése előtt erősítették a feltételezésemet. Egy végzett EIV-s hallgató például a kérdőív anonimitásával kapcsolatban keresett meg, feltételezve, hogy az általam anonimként aposztrofált kérdőív csupán beugratás, hiszen hiába nem kérdezek olyan adatokra, mint e-mail cím, név és egyéb személyes adatok, véleménye szerint, ha egy végzett EIV ezt elhinné, megbukna, hiszen technikai adatgyűjtéssel (például IP cím megszerzésével) visszaállítható a kapcsolat a kitöltővel, és ily módon beazonosítható az érintett. Azt gondolom, ez a fajta biztonságtudatosság lenne célravezető a graduális vagy doktori képzésben résztvevő hallgatók esetében is.

Összesen 415 képzésben résztvevő hallgató töltötte ki a kérdőívemet (n=415). Természetesen nem minden válasz esetében kaptam választ minden kitöltőtől. A kitöltő hallgatók 57,8%-a nő volt. A Karok, Intézetek, Doktori Iskolák tekintetébenaz Államtudományi- és Közigazgatási Kar hallgatói érték el a legmagasabb kitöltési arányt, az összes kitöltő 63,4%-a az ÁKK-hoz kötődik. Ezt követi a Nemzetközi és Európai Tanulmányok Kar (9,2%), a Hadtudományi és Honvédtisztképző Kar (9%), a Katonai Műszaki Doktori Iskola (5,1%), a Rendészettudományi Kar (3,6%), a Katasztrófavédelmi Intézet (3,4%), a Hadtudományi Doktori Iskola és Közigazgatás-tudományi Doktori Iskola (1,7-1,7%), Nemzetbiztonsági Intézet (1,5%), a Rendészettudományi Doktori Iskola (1), valamint a Víztudományi Kar (0,5%). A kitöltők 71,8%-a érettségivel, 14,5%-a mesterszakos diplomával, 9,9%-a alapszakos diplomával rendelkezik, továbbá 3,9%-a korábban posztgraduális képzésben vett részt. A kitöltők jelenleg 77,2%-a alapképzésben, 14,5%-a doktori képzésben, 7%-a

mesterképzésben, valamint 1,2%-a szakirányú továbbképzésen vesz részt. A kitöltők döntő többsége (73,4%) államilag finanszírozott képzési formában vesz részt. A kitöltők 57,5%-a nyilatkozott úgy, hogy korábban hallgatott információbiztonsággal kapcsolatos kurzust. Azok, akik hallgattak már ezzel kapcsolatos kurzust, önbevallásuk szerint 40,8%-a biztonságtudatosabb lett, 20,9%-a korábban is biztonságtudatos volt, 8,6%-a nem lett biztonságtudatosabb, illetve a kitöltők 2,1%-át elmondásuk szerint nem érdekli a biztonságtudatosság. A kitöltők 63,1%-a biztonságtudatosnak gondolja magát, 18,3%-uk pedig nem tudják megítélni, hogy biztonságtudatosak-e. A kitöltők 64,3%-a alapvetően humán, 16,2%-uk műszaki érdeklődésűként jellemezte önmagát, míg 19,6%-uk mindkettőnek. Egy átlagos napra vonatkozó internet, közösségi média és okos mobil eszköz használatával kapcsolatos adatokat a 18. számú táblázat adatai tartalmazzák.

18. táblázat Internet, közösségi média, okos mobil eszköz használata egy átlagos napon a képzésben részt vevő hallgatók esetében (saját szerkesztés)

Idő	Internet	Közösségi oldalak	Okos mobil eszköz
Kevesebb, mint 10 percet	0,0%	9,0%	5,8%
11-30 percet	0,2%	9,5%	3,2%
Fél-egy órát	5,1%	17,3%	9,7%
1-2 órát	20,5%	25,9%	20,4%
3-4 órát	36,1%	25,4%	23,4%
5-6 órát	17,1%	6,3%	14,4%
6 óránál többet	21%	6,6%	23,1%

A kérdőívben vizsgált területeket hét fókuszpont alapján kategorizáltam, mindegyik területen belül három-három kérdéskör alapján állításokat fogalmaztam meg. Az állítások megfogalmazását a Tudás-Képesség-Viselkedés modellt alapul véve végeztem el, és az azokra adott válaszok alapján vizsgáltam a kitöltők adat- én információbiztonság tudatosságát. Az alábbi területeket határoztam meg:

- jelszóhasználat;
- e-mail használat;
- internethasználat;
- közösségi média használat;
- mobil eszköz használat;
- információkezelés;
- incidensek jelentése.

A megfogalmazott állításokat az 1. számú melléklet tartalmazza. Az adatokat az IBM SPSS Statistics 25 programcsomag segítségével értékeltem ki kereszttábla elemzéssel, a kiértékelés statisztikai fogalmaihoz a Sajtos László és Mitev Ariel által írt SPSS kutatási és adatelemzési kézikönyvet használtam fel [174]. A kereszttábla elemzés célja, hogy megállapítsa, két vagy több változó között van-e összefüggés, illetve megmutatja ezek kombinált eloszlását. A kereszttábla elemzésből megállapíthatjuk tehát, hogy a két nominális változó[75] kapcsolatban áll-e egymással. A kereszttábla elemzés eredményeinél a Pearon-féle Khí-négyzet értékét vettem figyelembe, ami a két változó összefüggéseinek statisztikai szignifikanciáját határozza meg. A Khí- négyzet az egyik leggyakoribb elemzési forma, könnyen értelmezhető módszer, ami azonban rendkívül érzékeny a mintanagyságra- előfordulhat, hogy azonos jelenés elemzésekor eltérő eredményt kapunk eltérő elemszámú minta esetén. A Khí- négyzet próbát nominális vagy ordinális[76] változók esetében alkalmazhatjuk, a két változó közti kapcsolat elemzésére szolgáló statisztikai próba. A Khí-négyzet fogalma összefügg az asszociációs kapcsolat fogalmával, ami a Khí- négyzet próba során alkalmazott változók megnevezése. A Khí- négyzet próba alkalmával a cellák megfigyelt esetszámait hasonlítjuk össze azzal az elvárt esetszámmal, amit akkor kapnánk eredményképp, ha nem lenne kimutatható a kapcsolat a két változó között. Amennyiben nevezett kapcsolat egyértelmű, akkor függvényszerű kapcsolatként nevesítjük, amennyiben csupán valószínűsíthető, akkor sztochasztikus kapcsolatnak nevezzük. Ha nem mutatható ki kapcsolat a két változó között, akkor a két változó független. A Khí- négyzet próba egyik feltétele, hogy az elvárt gyakoriság minden egyes cellában legalább 5 legyen. Ha ez nem teljesül, akkor az összes cella maximum 20%-ában lehet az elvárt gyakoriság száma kevesebb, mint 5. Abban az esetben, ha ez az érték nem haladja meg a 0,05-öt, akkor beszélhetünk a két változó közti összefüggésről. Ezt követően a kapcsolat erősségét kell vizsgálnunk.

Az eredményekre vonatkozó részletes adatokat a 2. számú melléklet tartalmazza.

A H3 hipotézisem azon a feltételezésen alapul, hogy a biztonságtudatossággal kapcsolatos önpercepciót befolyásolja a nem, az iskolai végzettség, a műszaki-humán

[75] A nominális változó a legegyszerűbb skálatípus, amely a statisztikai elemzések eredményeinek kategóriákba sorolására szolgál. A skálaértékek között nem feltételezünk matematikai kapcsolatot, pusztán kódszámokként értelmezzük. Nominális változó például a nem, a kategóriák között nem állapítható meg mennyiségi összefüggés.

[76] Az ordinális változó hasonló a nominális változóhoz, azonban ebben az esetben már kvantitatív alapon rendezhetjük az egyes kategóriákat. Ilyen változónak tekinthetjük például a rendfokozatokat, hiszen az egyes rendfokozatok között megállapítható a mennyiségi eltérés értéke.

tudományok iránti érdeklődés, a korábban a témában hallgatott kurzus, illetve az egyes eszközök használatának ideje.

A biztonságtudatossággal kapcsolatos kérdés a kitöltő önmagával kapcsolatos percepciójára vonatkozott, hogy biztonságtudatosnak gondolja-e magát. Kereszttábla analízissel megvizsgáltam, hogy a hipotézisben megfogalmazott tényezők befolyásolják-e a kitöltők önpercepcióját. Az első vizsgálatom arra vonatkozott, van-e összefüggés a nem és a biztonságtudatossággal kapcsolatban (n=406). A vizsgálat Khí-négyzetének (X^2) megfigyelt értéke 7,063, amelynek kétoldali szignifikanciaszintjének értéke 0,029, tehát megállapíthatjuk, hogy a két változó között az összefüggés szignifikáns. A kapcsolat erősségét Cramer's V (C V) segítségével vizsgáltam, ugyanis ez tekinthető az egyik legmegbízhatóbb mutatónak. A C V egy asszociációs együttható, amely két nominális változó közötti szorosságot mutatja meg. A C V értéke 0 és 1 közötti intervallum közötti, a 0-hoz való közelség függetlenséget, az 1-hez való közelség erős kapcsolatot jelent. Vizsgálatomban a Cramer's V mutató megfigyelt értke 0,132, kétoldali szignifikanciaszintjének értéke szintén 0,029. A 0,132-es érték azonban alacsony korrelációra utal a két változó esetében.

A nemek közti válaszarány eredményeit a 19. számú táblázaton ábrázoltam.

19. táblázat Saját biztonságtudatosságnak a megítélése nemek szerint a képzésben részt vevők alapján (n=415) (saját szerkesztés)

	Férfiak	**Nők**
Kitöltők száma	171	235
Igen	68,4%	59,6%
Nem	19,3%	17,9%
Nem tudom	12,3%	22,6%

A táblázatból látható, a férfiak magasabb aránya gondolja biztonságtudatosnak magát, mint a nők, azonban a bizonytalanok körében a nők magasabb számban találhatóak.

A második vizsgálatom a kitöltők azon megállapításra vonatkozott, hogy önmagukat humán, műszaki érdeklődésűként határozzák-e meg, esetleg mindkettőt relevánsnak gondolják magukkal kapcsolatban. A kérdést az indokolja, a kiberbiztonsággal kapcsolatos attitűdöket tapasztalatom szerint gyakran befolyásolja, hogy az érintett önmagát e felosztás szerint hová sorolja be. Az oktatás során visszatérő érv a hallgatóktól, hogy ők nem értenek a kiberbiztonsághoz, mert ők humán érdeklődésűek, míg a kiberbiztonság alapvetően műszaki kérdés véleményük szerint. A Nemzeti Kiberbiztonsági Stratégiában megfogalmazott definíció azonban a politikai, gazdasági, oktatási, stratégiai, jogi területeket is a kiberbiztonsághoz

sorolja, így nem kötődik egyértelműen humán vagy műszaki területekhez. A kérdést ismét a nemek alapján vizsgáltam (n=410). A vizsgálat Khí-négyzetének megfigyelt értéke 33,238, amelynek kétoldali szignifikanciaszintjének értéke 0,000, ami a két változó között szoros összefüggésre utal. A Cramer's V mutató megfigyelt értéke 0,285, kétoldali szignifikanciaszintjének értéke szintén 0,000, ami szoros korrelációt jelent a két változó esetében. A 20. számú táblázatban ábrázoltam a nemek szerinti megoszlást. A válaszokból látható, a nők jelentősen többen tekintenek magukra humán érdeklődésűként, közel 23%-al többen jelölték ezt a választ, mint a férfiak.

20. táblázat Humán vagy műszaki érdeklődés megoszlása nemek szerint a képzésben részt vevők alapján (n=415) (saját szerkesztés)

	Férfiak	**Nők**
Kitöltők száma	173	237
Műszaki	22,7%	8,0%
Humán	50,3%	73,8%
Mindkettő	22,0%	18,1%

A következő vizsgálat szintén a biztonságtudatossággal kapcsolatos önpercepcióra vonatkozott, de ez esetben azt néztem meg, kimutatható-e összefüggés a biztonságtudatosság megítélése és aközött, hogy korábban hallgatott-e valamilyen adat- és információbiztonsággal kapcsolatos kurzust az Egyetemen (n=406). A vizsgálat Khí-négyzetének megfigyelt értéke 6,002, amelynek kétoldali szignifikanciaszintjének értéke 0,05, tehát megállapíthatjuk, hogy van összefüggés a két változó között. A Cramer's V mutató megfigyelt értke 0,122, kétoldali szignifikanciaszintjének értéke szintén 0,05, ami közepes korrelációt jelent a két változó esetében. A biztonságtudatosságra vonatkozó önpercepció és a témával kapcsolatos kurzus közti kapcsolatot a 21. számú táblázatban tüntettem fel.

21. táblázat Biztonságtudatosság önpercepciója és korábban kurzus látogatása közötti összefüggés (n=415) (saját szerkesztés)

	Kurzust	
	Hallgatott	**Nem hallgatott**
Biztonságtudatos	61,5%	56,6%
Nem biztonságtudatos	15,6%	21,7%
Nem tudja	16,0%	21,7%

Ezt követően megvizsgáltam, hogy van-e összefüggés a legmagasabb iskola végzettség, illetve a biztonságtudatosságra vonatkozó önpercepció között (n=98,8). A vizsgálat Khí-négyzetének megfigyelt értéke 4,897, amelynek kétoldali szignifikanciaszintjének értéke 0,557, vagyis két változó között nincs statisztikai összefüggés. Ettől eltekintve érdekes megnézni,

hogy iskolai végzettség szerint az önpercepciót (lásd 22. számú táblázat). Látható, hogy végezettségtől függetlenül a válaszadók több mint a fele biztonságtudatosnak gondolja önmagát, de a mesterszakos diplomával rendelkezők esetében ez az arány a kétharmadot is eléri.

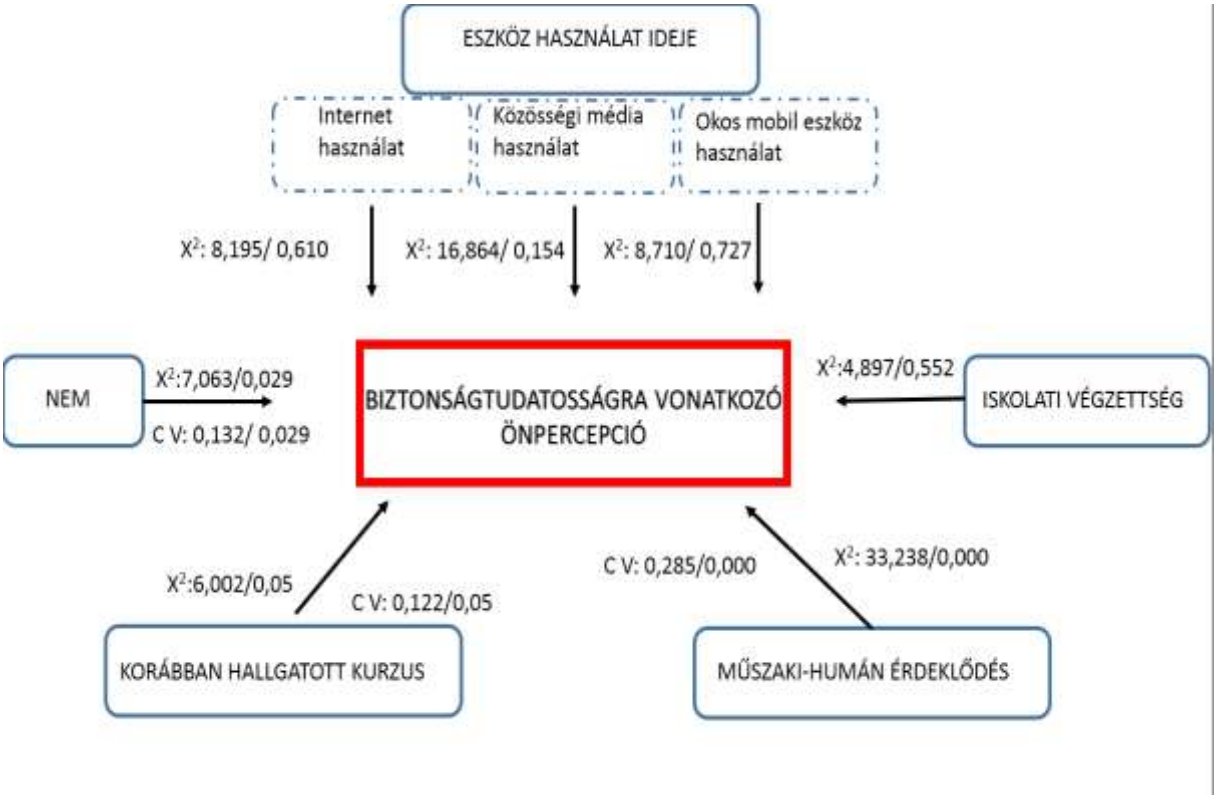
22. táblázat Biztonságtudatosság önpercepciója és legmagasabb iskolai végzettség közötti összefüggés (n=415) (saját szerkesztés)

	Legmagasabb iskola végzettség			
	Érettségi	**BSc. /BA**	**MSc. /MA**	**Posztgraduális**
Biztonságtudatos	61,1%	58,5%	75,0%	66,7%
Nem biztonságtudatos	19,5%	19,5%	13,3%	20,0%
Nem tudja	19,6%	22,0%	11,7%	13,3%

A biztonságtudatosságra vonatkozó önpercepciót az eszközhasználat idejének függvényében is vizsgáltam. Mindhárom eszköztípus esetében lefuttattam a kereszttábla analízist, de mindegyik esetben a Khí-négyzet kétoldali szignifikanciaszintjének értéke jelentősen meghaladta a 0,05-ös értéket,[77] így egyik esetében sem állapíthatunk meg szignifikanciát az eszközhasználat ideje és a biztonságtudatosságra vonatkozó önpercepció tekintetében.

[77] Internethasználat esetében a Khí-négyzetének megfigyelt értéke 8,195, amelynek kétoldali szignifikanciaszintjének értéke 0,610, közösségi média használat esetében a Khí-négyzetének megfigyelt értéke 16,864, amelynek kétoldali szignifikanciaszintjének értéke 0,154, okos mobil eszköz használat esetében Khí-négyzetének megfigyelt értéke 8,710, amelynek kétoldali szignifikanciaszintjének értéke 0,727.

Az öt vizsgált területet a 24. számú ábrán jelenítettem meg. Ez alapján kijelenthetjük,



24. ábra A biztonságtudatosságra vonatkozó önpercepciót befolyásoló tényezők (saját szerkesztés)

hogy a nem, a műszaki-humán érdeklődés, illetve, hogy korábban hallgatott-e a témában kurzust, befolyásolja a kitöltők biztonságtudatosságra vonatkozó önpercepcióját, azonban sem az iskolai végzettség, sem az eszközhasználat ideje esetében nem mutatható ki összefüggés.

KÖVETKEZTETÉSEK

A fejezetben megvizsgáltam az adat- és információbiztonság szerepét a kibertérben, illetve bemutattam azokat az adatgyűjtő eljárásokat, amelyek jelentősen befolyásolják a magánszféra minőségét. Megvizsgáltam továbbá a kibertámadásokkal kapcsolatos trendeket. Ennek segítségével megállapítottam, hogy a védelmi szféra kiemelt célpontja a különböző kibertámadásoknak, így elengedhetetlen a megfelelő normatív szabályozás, ami az adat- és információbiztonságra vonatkozik. Ezt követően elemeztem azokat a hazai és nemzetközi jogszabályokat, amelyek az adat- és információbiztonságra vonatkoznak, illetve vizsgálat alá vetettem azokat a szabályozókat, amelyek a Magyar Honvédség és Rendőrség állományába tartozók esetén a közösségi média használat szabályozását látják el. Az elemzést során **azonosítottam az adat- és információbiztonságra vonatkozó magyarországi normatív szabályozók közösségi média használattal kapcsolatos szabályozásra**

vonatkozó hiányosságait. Ezek alapján javaslatot fogalmaztam meg a közösségi média használattal kapcsolatos szabályozás honvédelmi-, rendvédelmi- és nemzetbiztonsági szempontú kialakítására.

A megfelelő jogszabályi háttér mellett elengedhetetlen az adat- és információbiztonsági tudatosságra vonatkozó képzés. A Nemzeti Közszolgálati Egyetem hallgatóinak többsége az egyetem elvégzését követően hivatásnemüknek megfelelően az állami szféra különböző területén fognak elhelyezkedni. Ebből következően kiemelten fontos, hogy milyen adat- és információbiztonsági tudatosság jellemzi őket, hiszen a munkavégzés során olyan rendszerekhez és információkhoz férhetnek hozzá, amelyek rendkívül értékesek mind idegen államok nemzetbiztonsági szolgálatainak, mind kiberbűnözőknek, terroristáknak vagy hacktivistáknak. Véleményem szerint az NKE hallgatói esetében kiemelt szerepet kell fordítani az adat- és információbiztonsági tudatosságot növelő oktatásnak, amely csökkentheti, hogy kibertámadás áldozataivá váljanak a hallgatók. Az egyetem hallgatói körében végzett kérdőíves felmérés során kereszttábla analízis segítségével **bizonyítottam, hogy a biztonságtudatosságra vonatkozó önpercepciót befolyásolja a nem, a műszaki-humán érdeklődés, illetve, hogy korábban hallgatott-e a témában kurzust. A kutatásom azonban cáfolta, hogy az iskolai végzettség és az eszköz használattal töltött idő befolyásolja a biztonságtudatosságra vonatkozó önpercepciót.**

IV. FEJEZET

A KÖZÖSSÉG MÉDIA ALKALMAZÁSI LEHETŐSÉGEI ÉS INTEGRÁLÁSA A VÉDELMI SZFÉRA EGYES TERÜLETEIN

Az első fejezetben a védelmi szférát öt kutatási területre szűkítettem le. A közösségi média katonai alkalmazásban betöltött szerepét a második fejezetben mutattam be, e fejezet keretében a nemzetbiztonsági, rendészeti és politikai aspektusát vizsgálom a témának. Az alkalmazási területek mellett megvizsgálom annak módját, milyen szervezeti keretekben integrálható a közösségi média a Magyar Honvédség, Rendőrség és nemzetbiztonsági szolgálatok esetében.

4.1. A közösségi média szerepe a nemzetbiztonsági szolgálatoknál

A közösségi médiának a hírszerzésben betöltött szerepét a nemzetbiztonsági szolgálatok korán felismerték. A 3.1-es alfejezet úgy vélem, kellően alátámasztja, milyen mértékben használható a közösségi média az adatgyűjtésre. Az alfejezetben az Edward Snowdenhez köthető információk alapján bemutatom, hogyan használják a nemzetbiztonsági szolgálatok a közösségi médiát a hírszerzésre. E mellett vizsgálni fogom a közösségi média terrorizmusban és a terror ellenes harcban betöltött szerepét is. A lélektani műveleteket, mint egy másik fontos irányát a a nemzetbiztonsági szolgálatok közösségi médiával kapcsolatos tevékenységének az államok politikai döntéshozatalának befolyásolásával foglalkozó alfejezetben tárgyalom.

A 21. századra a nemzetbiztonsági szolgálatok számos kihívás előtt állnak. Ezek közül a fontosabbak Kis-Benedek József megállapítása szerint [175]:

- *„globális terrorizmus;*
- *a tömegpusztító fegyverek proliferációja;*
- *sikertelen államok megjelenése (ezzel együtt gazdasági és szociális destabilizáció);*
- *a válság következtében a menekülthullám, illetve az illegális migráció kialakulása;*
- *a szervezett bűnözés, mint a globalizáció negatív kísérője és az ehhez kapcsolódó pénzmosás;*
- *emberkereskedelem, szervkereskedelem;*
- *a hagyományos kábítószer-kereskedelem, a védelmi pénzek;*
- *kibertér jelentette fenyegetések.”*

Az egyes kihívások önmagukban is komplex fenyegetést jelentenek, de ezek gyakran összekapcsolódnak egymással. Ez által érthető, hogy az államok minél szélesebb körben kívánják erősíteni a nemzetbiztonsági szolgálatok megfigyeléssel kapcsolatos képességeit, azonban ezek együtt járhatnak a magánszféra folyamatos szűkülésével. Nem kérdés, hogy az őrzőket is őrizni kell, ezért fontos garanciális biztosítékokat kell beépíteni a normatív szabályozásba. Amennyiben egy nemzetbiztonsági szolgálat tömegesen, bírói vagy miniszteri felhatalmazás nélkül végzi az állampolgárai megfigyelését, azzal igen komolyan veszélyezteti a demokratikus normákat, hiszen ez által olyan túlhatalmat szerezhet, amely szélsőséges esetben totális diktatúra kiépítéséhez vezethet. A 3. fejezetben bizonyítottam, hogy a közösségi média ezt a fajta totális megfigyelést elősegítheti.

A hírszerzés Izsa Jenő megfogalmazásában *„… az állam egyik funkciója, amelyet a nemzeti érdekek érvényre juttatása és védelme érdekében, kizárólag erre a feladatra létrehozott, közvetlen kormányzati irányítás alatt működtetett szervezetek végeznek, nyílt és titkos forrású információk beszerzésével [176]*.” A fogalom azonban így is csak egy szűk metszetét jelenti a hírszerzés összetett tevékenységrendszerének. Maga a hírszerzés legalább három fogalmi elemet testesít meg:

- az információt, amely a hírszerzés tárgyát, célját képezi;
- a szervezetet, amely a hírszerzést végrehajtja;
- valamint magát a tevékenységet, amely kiterjed a titkos információk megszerzésére, feldolgozására, hasznosítására, illetve a titkos és fedett hírszerző műveletek végrehajtására [192].

A hírszerzésnek két funkcióját különböztetjük meg: egyrészt az ország értékeinek és érdekeinek a védelmét, másrészt az ország érdekeinek érvényre juttatásának a támogatását. A hírszerzés alapvetően külföldre irányul, a külföldi eredetű nyílt és titkos információk megszerzése érdekében folytatják.

Ezzel szemben, Ádám László megfogalmazása szerint az elhárítás „*az ellenérdekelt titkosszolgálatok tevékenységének felderítése, megakadályozása, logisztikai hátterének felfedése, módszereik megismerése; előre jelezni azokat a területeket, aktuális vagy hosszú távú feladatokat, melyek a jelzett szervezetek érdeklődési körébe kerülhetnek, ezáltal a célpontjává válhatnak. Ezen kívül feladata a demokratikus intézményrendszerek rendeltetésszerű működésének védelme, azok megzavarására alkalmas, nemkívánatos külső és belső behatások ellen [178]*.” Ebből következik, az elhárító tevékenység alapja a megelőzés, ami csak akkor

lehet sikeres, ha a meghozott intézkedések hatására az ellenérdekelt nemzetbiztonsági szolgálatok el sem jutnak a védendő személyekhez, intézményekhez.

Napjainkban kilenc fő adat- és információgyűjtő módszert különböztetünk meg, amelyek további alterületekre bonthatóak. Ilyen adatgyűjtő módszer az

- ember erőforrással végzett hírszerzés;
- nyílt forrású információgyűjtés;
- elektronikai felderítés;
- kiber/digitális hálózati hírszerzés, (Cyber Intelligence/Digital Network Intelligence, CYBINT/DNINT);
- képfelderítés (Image Intelligence, IMINT);
- mérés- és jelmeghatározó hírszerzés, (Measurement and Signature Intelligence, MASINT);
- technikai hírszerzés, (Technical Intelligence, TECHINT);
- pénzügyi hírszerzés (Financial Intelligence, FININT);
- orvosi hírszerzés (Medical Intelligence, MEDINT).

Ez a típusú felosztás nem kőbe vésett, egyes szerzők eltérő módon kategorizálják az adatgyűjtő eljárásokat, de új módszereket is alkothatnak. Utóbbira példa Alfred Rolington, aki külön módszerként azonosítja a közösségi médiában folytatott hírszerzést (Social Media Intelligence-t, továbbiakban SOCMINT) [179].

Az emberi erőforrással végzett hírszerzés a legősibb adat- és információgyűjtő eljárás [180]. Ide soroljuk a nyílt, legális pozícióban végzett hírszerzést[78] és az ügynöki, fedett hírszerzést. Előbbi esetében a hírszerzést végző személyek neve, beosztása, hovatartozása nyíltan felvállalt. Az ügynöki, fedett hírszerzést végzők esetében a hovatartozást, illetve a tevékenységet konspiráltan, fedésben végzik. Ez a fajta hírszerzés minden országban illegálisnak minősül.
A nyílt forrású információgyűjtés dinamikusan növekvő ágát jelenti a hírszerzésnek [181]. „*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 [182]*.” Az OSINT-ot gyakran az internettel azonosítják, azonban sokkal szélesebb kör tartozik alá, tv-, rádióműsorok,

[78] Például diplomaták vagy a katonai missziók hír- és információszerző támogatást hírszerző elemekkel biztosított hírszerző tevékenysége.

újságok, szürke anyagok, konferencia előadások, könyvtárak, tanulmányok, de akár kocsmai beszélgetések is ide sorolhatóak. Nyílt forrású információgyűjtés viszonylag alacsony költségek mellett végezhető, mégis nagy mennyiségű adat szerezhető általa. Ferenczy Gábor szerint „a *nyílt információforrások a 70-90%-át elégítik ki a teljes felderítő igényeknek. Olyan összefüggéseket tárhat fel, amelyek rámutathatnak egy adott téma lényegére, illetve segíthetik azt, hogy a minősített anyagokban milyen irányban kell összpontosítani a keresést*" [183]. A nyílt forrású információgyűjtés az egyénekről gyűjtött információk mellett a trendelemzésben is fontos, valós időben vizsgálhatóak bizonyos folyamatokra adott reakciók, mi több, megfelelő számú adat megléte esetén nagy valószínűséggel prognosztizálhatunk jövőbeli eseményeket is. Kertész János, magyar hálózatkutató és szerzőtársai tanulmányukban például kimutatták, hogy egy film Wikipedia oldalának trendelemzésével 85%-os pontossággal előre lehet jelezni, hogy az első hétvégén milyen jegyeladást fog elérni a mozikban [184].

Az elektronikai felderítés különböző, alapvetően vezetékes vagy rádiós úton folytatott, titkosított, vagy nem titkosított kommunikációhoz és jelekhez kapcsolódó felderítő, információgyűjtő tevékenység [185].

Annak érdekében, hogy eljussunk a közösségi média hírszerzésben betöltött szerepének vizsgálatához, tisztázni szükséges az Edward Snowden-ügyet [186]. 2013. június 6-án még kevesen sejtették, hogy a The Guardian és The Washington Post által publikált, Verzion telekommunikációs céget érintő megfigyelési ügy egy hónapokig tartó tömeges megfigyelésekkel kapcsolatos botránysorozat nyitánya. Az első hírek szerint az amerikai Nemzetbiztonsági Ügynökség (National Security Agency, továbbiakban NSA) egy április 25-én hozott bírósági határozat[79] felhatalmazása alapján rögzíti a Verzion több millió előfizetője által kezdeményezett telefonhívásokat [187]. A jogalapot a rendkívül sokat vitatott, 2001. október 26-án aláírt Patriot Act biztosította. Az adatgyűjtés kiterjedt a hívó és a hívott fél telefonszámára, a két fél aktuális földrajzi pozíciójára, a hívás időtartamára, a telefonok IMEI-azonosítójára, magára a beszélgetésre, de nem képezte részét a beszélő személyek azonosítása.

A tömeges megfigyelés, bár a média újdonságként interpretálta, egyáltalán nem nevezhető egyedi esetnek. Snowden színrelépése előtt kereken 25 évvel korábban, 1988. augusztusában publikálta Duncan Campbell a Somebody's Listening [188] (Valaki figyel) címet viselő írását egy olyan témában, amit már évek óta pletykáltak: öt angolszász ország

[79] Az engedélyt a The United States Foreign Intelligence Surveillance Court (továbbiakban FISC) nevű szövetségi bíróság adta ki, amely elsősorban megfigyelésekkel kapcsolatos kérelmek elbírálásával foglalkozik.

hírszerző szolgálata[80] a világ telekommunikációs forgalmának majdnem teljes egészét lehallgatja, elemezi. Az Echelon rendszer, amiről Campbell írt egy régi együttműködés eredményeképpen valósult meg. Az Egyesül Államok és Nagy-Britannia 1943. május 13-án írta alá a BRUSA- egyezményt [190], amely a két állam hírszerző szervezeteinek az ellenséges országok kommunikációjának lehallgatására[81] vonatkozott. A második világháború lezárultával a BRUSA egyezményt az UKUSA váltotta fel, ami egyrészt képességfejlesztésben, másrészt a résztvevő államok körével bővítette a BRUSA egyezményt. A ’80-as évekre az Echelon a rádióelektronikai eszközökön továbbított üzenetek tömeges megfigyelésére volt képes, illetve kulcsszavak alapján egy algoritmus segítségével a lehallgatott üzenetek értékelését is elvégezte.

Ahogy az Echelon példája is mutatja, Snowden színrelépése egyáltalán nem egyedi. A nemzetbiztonsági szolgálatok mindig is igyekeztek a technológiai lehetőségeket felhasználni annak érdekében, hogy a törvényben előírt kötelezettségeiket hatékonyan végezhessék. Az internet és a közösségi média megjelenése ebben csupán újabb és újabb platformokat hozott. Snowden hozzávetőlegesen 58 ezer feljegyzést adott át, ezeknek azonban csupán töredéke látott napvilágot. Témám szempontjából az egyik legfontosabb információ, amit a kiszivárgott dokumentumokból megismerhettünk az úgynevezett PRISM megfigyelőrendszer. A PRISM a SIGAD[82] US-984XN kódnevű titkos tömeges megfigyelésre képes elektronikus adatbányász rendszer, ami a több tucat tömeges megfigyelésre használt rendszer egyike csupán. A közzétett dokumentumok alapján [177] az NSA 2007 óta fér hozzá a PRISM által Microsoft, 2008 óta a Yahoo, 2009 óta a Google, Facebook, PalTalk, 2010 óta a YouTube, 2011 óta a Skype, AOL, 2012 óta az Apple által tárolt adatokhoz. Az érintett cégek természetesen tagadták a megjelent információkat, azonban 2013 augusztusában az is kiderült, hogy az NSA Google-nek, a Microsoftnak, a Yahoo-nak és a Facebooknak is fizetett a lehallgatásokhoz szükséges infrastruktúra kiépítéséért [193].

A kiszivárgott adatok alapján arra is fény derült, az NSA az amerikai jogszabályokat megkerülve, bírói felhatalmazás nélkül figyelt meg amerikai állampolgárokat. Ennek egyik eszköze az XKeyscore nevű program volt [194], hogy bármilyen bírósági felhatalmazás nélkül, egy személyes adat felhasználásával (akár név, akár e-mail cím, akár IP cím) bármelyik állampolgárt alapos megfigyelés alá vonhatják. Az XKeyscore hozzáfért a felhasználók minden

[80] Az úgy nevezett „Big Five Eyes” országai, vagyis az NSA, továbbá a brit Government Communications Headquarters, azaz a GCQH, a kanadai Communications Security Establishment, azaz CSE, az ausztrál Defense Signals Directorate, azaz DSD, illetve az új-zélandi Government Communications Security Bureau, azaz GCSB [189]

[81] Az együttműködés eredményei közé sorolhatjuk többek között a VENONA-projektet. [191])

[82] SIGINT Activity Designator, vagyis elektronikai felderítő tevékenységet meghatározó alfanumerikus azonosító

privát beszélgetéséhez, közösségi oldalainak profiljaihoz, keresési előzményeihez stb. Hogy mindezt bírói engedély nélkül végezhessék, egy olyan jogi kiskaput használtak ki, aminek az volt a lényege, ha a megfigyelni szándékozott amerikai állampolgár kapcsolatba hozható egy megfigyelt külföldivel, úgy elvégezhető az adatgyűjtés bírói engedély nélkül is. Mint kiderült, több ezer alkalommal sértették meg az adatvédelmi törvényeket, illetve a megszerzett információkat megosztották engedély nélkül hazai (például a Drug Enforcement Administrationel, a DEA-vel [195]) és külföldi partnerszervezetekkel (például az Israeli SIGINT National Unittal [196]). A bírói engedély kijátszásának másik módja a brit partnerszervezetének hasonló képesség kiépítését jelentette 100 millió font értékben, hogy a GCHQ segítse az internetforgalom figyelését [197].

A PRISM és az XKeyscore működése az elektronikai felderítéshez sorolható. Jelenleg nincs ismeretünk arra vonatkozóan, hogy más országok használnak-e ehhez hasonló rendszereket, azonban joggal feltételezhetjük, hogy igen. Értelemszerűen a Facebook, Google, Apple esetében ilyen képességet kiépíteni csak az amerikai nemzetbiztonsági szolgálatok tudnak kiépíteni, de vélhetően a VKontakte esetében az orosz szolgálatok, a Weibo és más kínai oldalak esetében a kínai szolgálatok hasonló képességgel rendelkeznek. Ez persze nem jelenti azt, hogy különböző módszereket alkalmazva nem kísérelnének meg hozzáférni idegen államok nemzetbiztonsági szolgálatai az amerikai cégek adatbázisaihoz vagy a felhasználók privát beszélgetéseihez. Ennek egyik módja legális keretek között zajlik, az egyes államok adatszolgáltatásra vonatkozó kérelmet nyújthatnak be állampolgáraival kapcsolatban. A benyújtott kérelmeket a közösségi oldalak üzemeltetői minden esetben megvizsgálják, és amennyiben úgy ítélik meg, hogy jogszerű a kérelem, rendelkezésre bocsájtják az adatokat. 2017 első félévében például 78900 kormányzati adatbekérés érkezett a Facebookhoz, ebből Magyarországról 234 kérvényt nyújtottak be 390 felhasználó adataival kapcsolatban [198].[83] Az sem szokatlan az államok részéről, hogy nyomást gyakorolnak a közösségi oldalakra, hogy így szerezzék meg a számukra fontos adatokat. Természetesen ezt kevés állam kormánya engedheti meg magának. Ilyen állam például Kína, aki a Facebook kínai piacra történő lépésének engedélyezéséért cserébe olyan garanciákat követel meg, amiket kénytelen a Facebook is engedi. Ilyen engedmény például, hogy egy olyan tartalomblokkolásért felelős alkalmazást fejlesztenek Kínának, amelynek üzemeltetését egy harmadik félnek, egy kínai hatóságnak adná át [199]. Nincs információnk arra vonatkozóan, hogy ezen felül egyéb

[83] A 243 esetből 4 volt sürgősségi adatbekérés, ezekből 1 esetben adták ki az adatokat, a 230 esetében pedig 54%-os volt a pozitív elbírálás aránya.

megállapodáshoz kötötték-e a piacra lépés engedélyezésével kapcsolatban, azonban Kína igénye a kínai internetezők teljes megfigyelésére tényként kezelendő (gondoljunk csak a kínai „nagy tűzfalra", a virtuális magánhálózatok, továbbiakban VPN-ek betiltására, a cenzúrára), ahogy az is, a Facebook, ha csak ki nem szivárogna, nem ismerne be egy ilyen megállapodást, ahogy ezt a PRISM esetében is tapasztalhattuk.

Azok az államok, amelyek nem tudják kikényszeríteni a közösségi oldalakat, hogy számukra hozzáférést engedélyezzenek az adatbázisaikhoz, megpróbálhatnak behatolni a rendszerbe, hogy ily módon gyűjtsenek adatokat. Az ilyen típusú informatikai támadást általában a nemzetbiztonsági szolgálatok államilag támogatott hackerekkel végeztetik.

Az elektronikai felderítés mellett a nyílt forrású információgyűjtés a másik fontos területe a közösségi média segítségével végzett hírszerzésnek. Ennek egyik legfontosabb oka az alacsony adat- és információbiztonsági tudatosság, hiszen minél kevésbé vagyunk érzékenyek adataink védelmére, annál több mindent osztunk meg magunkról. A közösségi oldalakon eltelt idő függvényében ezek az adatok pontosabb profilozást tesznek lehetővé még azok számára is, akik az adatok elemzését nem algoritmusok segítségével végzik. Nyílt forrású információgyűjtés természetesen végezhető automatizált folyamatként is, ekkor elsősorban trendelemzés céljából alkalmazzák. Ahogy Kertész János kutatása alapján is írtam, megfelelő módszertannal nagy pontossággal prognosztizálható a közeljövő. A strukturálatlan adatok kiértékelése rendkívül értékes. Big data analízissel, a mesterséges intelligencia megjelenésével lehetséges a közösségi oldalakon folytatott kommunikáció, tartalommegosztás valós időben történő, automatizált elemzése. 2014-ben az amerikai Titkos Szolgálat (Secret Service)[84] túllépve a közösségi média felületeken keletkező nagy mennyiségű tartalom szintetizálására és vizuális ábrázolására képes analitikus programon, egy olyan alkalmazás kifejlesztését tűzte ki céljául, amely többek között automatizálja a közösségi médiát monitorozó műveleteket, valamint felismeri a szarkazmust[85] a megosztott tartalmakban [200]. Azt gondolom, nem vitás, a mesterséges intelligencia, a gépi mélytanulás fejlődése alapjaiban fogja átalakítani az adatfeldolgozást.

[84] A Secret Servicet kezdetekben a pénzhamisítás elleni harcra hozták létre a 19. században, majd az FBI megalapításáig gyakorlatilag azt a feladatrendszert hivatott elvégezni, mint amivel később a Szövetségi Nyomozóirodát ruházták fel. A Secret Service fő feladata napjainkban az elnök és családjának védelme. A szervezet 2003-ig a Pénzügyminisztérium (United States Department of the Treasury) irányítása alá tartozott, azonban a frissen megalakított Belbiztonsági Minisztériumhoz (United States Department of Homeland Security) került. A Secret Service nem klasszikus titkosszolgálat, mint ahogy a neve utal rá, hanem egy szövetségi bűnüldöző hatóság.

[85] Mindez a mesterséges intelligencia egy nagyon fejlett szakaszaként értelmezhető, hiszen rendkívül bonyolult kognitív folyamatokat szükséges ennek érdekében lemodellezni. Ehhez azonban szükséges ismerni az emberi elme működési mechanizmusainak módját.

A trendelemzés mellett az OSINT arra is hasznos, hogy egyes célszemélyekről a lehető legtöbb információt megszerezzük. Ahogy korábban több alkalommal írtam, ehhez nem szükséges sem sok idő, sem komolyan informatikai tudás. Egy egyszerű Google-ös keresés a „Facebook Open Source Intelligence" keresőszavak alkalmazásával több olyan oldalt is ajánl, amelyek használatával percek alatt megszerezhetünk rengeteg nyilvánosan elérhető adatot a célszemélyünk Facebook aktivitásáról. Ilyen oldal például a 25. számú ábrán látható (www.uk-osint.net). Az oldal használatához szükségünk van a célszemélyünk ID Numberére, az oldalon található több ID Number generáló oldal segítségével szerezhetünk meg (26. számú ábra). Ehhez be kell másoljuk a célszemély profiljának az url-jét. Amint megvan az ID Number, csupán a kiválasztott részhez kell bemásolni, és az oldal azonnal listázza a találatokat (27. számú ábra). Az oldal nem adja ki találatnak azokat az adatokat, amiknél a felhasználó korlátozza a láthatóságát oldal, egyedül a nyilvánosan látható adatokat kapjuk meg. Ettől eltekintve kereshetünk minden egyéb nyilvános adat között: milyen oldalakat kedvel, honnan szokott bejelentkezni, milyen fényképeken jelölték meg, milyen kommenteket szokott írni, kik a munkatársai stb. Természetesen ezek jelentős részét szintén letilthatjuk, hogy látható legyen, de ha mondjuk olyan helyre kommentelünk, ahol az ismerősünk nem tiltotta le a láthatóságot, meg fogjuk találni.

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

26. ábra Hogyan szerezzük meg a célszemély Facebook ID Numberét (forrás: http://lookup-id.com/)

Facebook User Number	GO		(Places Visited)
Facebook User Number	GO		(Recent Places Visited)
Facebook User Number	GO		(Places Checked-In)
Facebook User Number	GO		(Places Liked)
Facebook User Number	GO		(Pages Liked)
Facebook User Number	GO		(Photos By User)
Facebook User Number	GO		(Photos Liked)
Facebook User Number	GO		(Photos Of -Tagged)
Facebook User Number	GO		(Photo Comments)
Facebook User Number	GO		(Apps Used)
Facebook User Number	GO		(Videos)
Facebook User Number	GO		(Videos Of User)
Facebook User Number	GO		(Videos By User)
Facebook User Number	GO		(Videos Liked)
Facebook User Number	GO		(Video Comments)
Facebook User Number	GO		(Future Event Invitations)
Facebook User Number	Year	GO	(Events Invited)
Facebook User Number	Year	GO	(Events Attended)
Facebook User Number	GO		(Posts by User)
Facebook User Number	Year	GO	(Posts by Year)
Facebook User Number	GO		(Posts Tagged)
Facebook User Number	GO		(Posts Liked)
Facebook User Number	GO		(Employers)
Facebook User Number	GO		(Groups)
Facebook User Number	GO		(Co-Workers)
Facebook User Number	GO		(Friends)
Facebook User Number	GO		(Followers)
Facebook User Number	GO		(Relatives)
Facebook User Number	GO		(Friends' Likes)

27. ábra Néhány példa, hogy milyen információkat szerezhetünk meg pár perc alatt (forrás: https://inteltechniques.com/OSINT/facebook.html)

Az általam bemutatott oldal vagy a hozzá hasonló oldalak használata azonban ellentmondásosak adatvédelmi szempontból. Bár nyílt forrásból dolgozik, azonban automatizált adatfeldolgozást valósít meg, aminek 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. Felidézve a korábban idézett NAIH tájékoztatót a munkáltatók álláspályázatra jelentkezők közösségi oldalának ellenőrzéséről, egy ilyen oldal segítségével percek alatt tájékozódhatnak a jelentkezőről, azonban szűrniük kell az idézett elvek mentén. Amennyiben az információgyűjtést valaki egy támadás előkészítése érdekében folytatja, úgy nyilvánvalóan nem fogja érdekelni az adatkezelés jogi kötöttsége. A trendek szerint a támadások egyre nagyobb része köthető social engineering alapú támadásokhoz.

A social engineering egy olyan támadásforma, amely során a támadó az emberi tényező kihasználható tulajdonságait[86] használja fel, hogy ily módon férjen hozzá megtévesztéssel, zsarolással a védett információkhoz, rendszerekhez [201]. Kevin D. Mitnick[87] 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 [202].*"

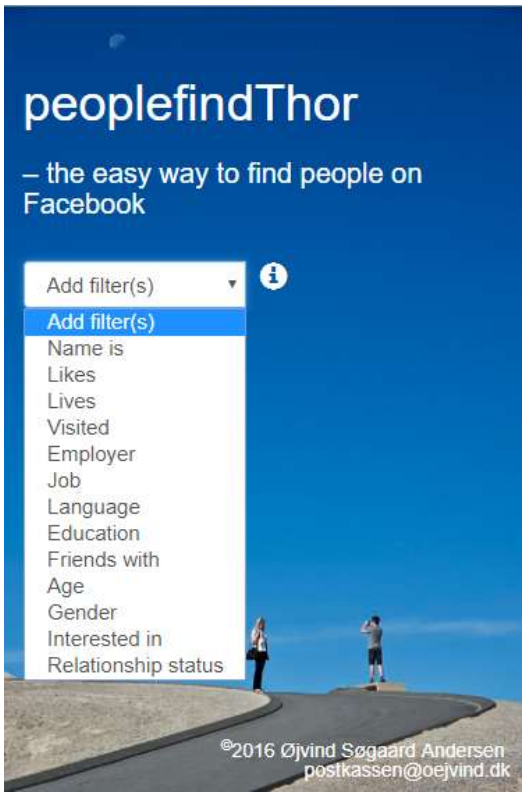
A social engineering támadásokat humán- [203] és IT alapú [204] támadások alapján szokás megkülönböztetni, annak függvényében, hogy használ-e valamilyen informatikai eszközt a támadás végrehajtása során. Az ilyen jellegű támadások sokszor akkor is hatékonyak lehetnek, ha a megtámadni kívánt rendszert magas fizikai és logikai védelemmel látták el.[88]
Egy social engineering támadás négy fázisból épül fel:

- információgyűjtés;
- kapcsolat kiépítése;
- kapcsolat kihasználása;

[86] Naivitás, hiszékenység, segítségnyújtás, kíváncsiság, biztonságtudatosság hiánya, figyelmetlenség, szexualitás stb.
[87] 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.
[88] Az Ibtv 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 [81].

- támadás végrehajtása.

Természetesen egy támadás előkészítésénél akkor hasznos az általam bemutatott oldal, ha tudjuk, ki a célszemély. Az ismertetett oldalon azonban másik hasznos oldalra is átnavigálhatunk, ami különböző, általunk megadott variánsok alapján végzi a keresést (lásd 28. számú ábra). Ezek a variánsok lehetnek 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. Természetesen csak akkor jeleníti meg az oldal a találati listában az adott variáns alapján, ha az arra vonatkozó adat nyilvánosan elérhető róla. Visszautalva az 11/2015. (VII. 10.) ORFK utasításra, amely tiltja, hogy a Rendőrség állományába tartozók nyilvánosan feltüntessék az állományhoz való tartozásuk tényét, azt gondolom, a Rendőrség részéről nem ellenőrzik az utasítás betartását, ugyanis a „rendőrség" -re vonatkozó keresés több száz profilt jelenített meg.



28. ábra Nyílt forrású keresés különböző variásnok alapján (forrás: https://www.peoplefindthor.dk/)

A technológiát felhasználva, kellő informatikai tudással rendelkező támadók az alábbiak szerint is gyűjthetnek információkat a célszemélyekről:

- közösségi oldal feltörése;

- álprofil létrehozása;
- játékok, kvízek, Facebook alkalmazások létrehozása;
- közösségi oldalakon folytatott kártékony kód kampányok segítségével;
- okos mobil eszközökre írt alkalmazások használatával;
- adathalász oldalak felhasználásával;[89]
- rosszindulatú alkalmazások egyéb úton történő fertőzésével;
- Wi-Fi hálózat feltörésével és lehallgatásával.

Az adatgyűjtő eljárások kapcsán az emberi erőforrással végzett hírszerzést kell még megemlítenem. Ebben az esetében értelemszerűen a közösségi média csupán támogató funkcióval bír, az általa gyűjtött adatok segíthetnek egy legenda megalkotásában, a célszeméllyel történő kapcsolat kialakításában stb.

4.2. A közösségi média szerepe a bűnüldözésben

A rendévelemben a közösségi média egyik legfontosabb alkalmazása a bűnügyi felderítés területéhez kötődik. Az eljárásokat a hírszerzéssel kapcsolatos alfejezetben már ismertettem, így itt alapvetően egy másik megközelítést kívánok vizsgálni. A kiberfenyegetettség trendjeinek bemutatása során megállapítottam, hogy a bejelentett támadások jelentős többségénél a kiberbűnözés azonosítható motivációként. Ahogy Simon Béla kiválóan összefoglalja, „*korábban a számítógépes bűncselekmények a cybercryme fogalomkörébe tartoztak a biztonsági előírások megváltoztatásai, hobbi hacker-ek, honlap megváltoztatások, egyedi vírusok, szórványos támadások, egyfajta technikai érdeklődés az informatikai rendszerek biztonsági rései irányába. Legújabban azonban ezek kiegészültek a valóban kriminális szervezett bűnelkövetői csoportokkal, személyiség lopással, tervezett, irányított támadásokkal, kémkedéssel, szabotázzsal, felbérelhető profi hacker-ekkel, növekedő spam áradattal*” [205]. A szakirodalomban az ilyen típusú bűncselekményekre nem találunk egységes fogalmi meghatározást, egyes szerzők csúcstechnológiás bűnözésként, mások információ technológiai bűnözésként vagy számítógépes bűnözésként nevesítik. A definíció választás azért is érdekes, mert például egy bankkártyával való visszaélés informatikai eszközök felhasználásával is történhet, de mégsem feltétlenül számítógépes bűnözés, ahogy mondjuk egy okos mobil eszközön egy kémprogram segítségével ellopott adatok sem számítógép

[89] A kevésbé biztonságtudatos felhasználók gyakran ugyanazt az egy jelszót használják minden profiljuk esetében, így egy megszerzett jelszó jó eséllyel a többi fiókhoz is hozzáférést jelent.

segítségével valósulnak meg. A kiberbűnözés fogalmát én a kibertér komplex megközelítése miatt használom. Kijelenthető, hogy a kiberbűnözők mindig újabb és újabb eljárásokat találnak tevékenységük végzésére, ezért az ellenük folytatott harc különösen nehéz, hiszen gyakran egy lépéssel előbbre járnak, mint akik a védelmet kell biztosítsák [206].

Elsőre a kiberbűnözés és közösségi média kapcsolatát nem feltétlenül gondoljuk relevánsnak, hiszen a köztudatban olyan bűncselekményekhez kötik, mint például közösségi oldalakra feltöltött információk alapján tudják az elkövetők, mikor nem vagyunk otthon, és ekkor törnek be. Ennél azonban jelentősen szélesebb támadási felületet jelent, amelyek igen súlyos következményekkel járnak. A szakirodalom a kiberbűnözés típusait különböző módszerek alapján kategorizálja,[90] de én a kiberbűnözés és közösségi média kapcsolatát az Europol által minden évben publikált Szervezett bűnözés internetes fenyegetettségét (Internet Organised Crime Threat Assessment, továbbiakban IOCTA) értékelő jelentése felhasználásával vizsgálom. A 2017-es évre vonatkozó jelentés az előző évekhez képest egyfajta szűkítést alkalmaz a támadástípusokat illetően, ez azonban nem azt jelenti, hogy csökkent a támadások típusának száma, csupán prioritások alapján rendszerezi azokat. A 2016-os IOCTA jelentés 12 területet azonosított [208], amelyből 10 esetében állapítottam meg kapcsolatot a közösségi médiával. A 2017-es jelentés [209] 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.

Ezen felül határterületként azonosítja a jelentés:

- a kibertér és terrorizmus összefonódását;
- a social engineeringet;
- a szolgáltatás szerű bűnözést;
- a bűnözők pénzügyi tevékenységeit.

A kibertérrel kapcsolatos bűnözés esetén a malwarekkel kapcsolatos támadásokat, a kritikus infrastruktúrák támadását és az adatlopást, adatszivárgást, hálózatok támadását nevesíti a jelentés. Mindhárom esetében azonosíthatjuk eszközként a közösségi médiát. Malwarek (malicious software kártékony szoftver) a rosszindulatú programok gyűjtőkifejezése, körébe

[90] Például John Sammons és Michael Cross a Kiberbiztonság alapjai című könyvben [207].

tartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit) és az egyre inkább globális méreteket öltő zsarolóvírusok (ransomware). A közösségi médiából szinte kiírthatatlanok. Kampányszerűen terjednek, akár privát üzenetekben, akár felhasználók üzenőfalán. Viszonylag könnyen azonosíthatóak, de az alacsony biztonságtudatossággal rendelkező felhasználók gyakran áldozatokká válnak. A közösségi oldalakon terjedő malwarek alapvetően idegen nyelven, valamilyen figyelemfelkető megosztással terjednek (híresség vagy a felhasználóval kapcsolatos erotikus tartalom, akciós termékek stb.). Malwarek típustól függően okozhatnak kárt. Kémprogramok, trójai programok segítségével a rendszerben tárolt adatokhoz férhetnek hozzá, de akár az adatok sérthetetlenségét, rendelkezésre állását és bizalmasságát is sérthetik. Malwarek segítségével botnet hálózatok hozhatóak létre, amelyek hálózatok, kritikus infrastruktúrák támadására használhatóak. Ahogy a 2017 nyarán elterjedt NotPetya zsarolóvírus is igazolta, nem csak anyagi haszonszerzésre, de kritikus infrastruktúrák megbénítására is lehet alkalmazni a ransomwareket. A kritikus infrastruktúrák támadásában a közösségi médiának a malwereken kívül az álhírek terjesztésében, illetve nyílt forrású információgyűjtésben lehet szerepe [210] [211].

A gyermekek szexuális kizsákmányolásával kapcsolatban négy kulcsterületet fogalmaz meg a jelentés. A közösségi média használatával kapcsolatban elsősorban a gyermekek bizalmába férkőzését azonosíthatjuk álprofilok segítségével, aminek gyakran erotikus képek kicsalása a célja. Súlyosabb eset a bizalom kiépítését követően a gyermekek szexuális abúzusa, ami megvalósulhat akár a korábban kicsalt erotikus képpel történő zsarolással vagy a gyermekek meghatározott helyszínre történő odacsalogatásával. Egy másik aspektusát jelentik a streaming szolgáltatások növekvő száma, amelyek mindenféle komoly technológiai ismeret nélkül teszik lehetővé cselekmények élő közvetítését. Ez irányulhat szexuális együttlétek közvetítésére, ami nyilvánvalóan nem a Facebook és YouTube oldalain valósul meg, de gyermekek fizikai és szexuális megalázását élőben már közvetítették Facebookon az áldozatok ismerősei.

A fizetőeszközökkel történő visszaélés elsősorban bankkártyával elkövetett csalásokhoz kapcsolódó tevékenység (például visszaélés, hamisítás stb., de az e-kereskedelem elterjedésével a visszaéléseknek egyre nagyobb arányban az egyéni vásárlók közötti (consumer to consumer, vagyis C2C) üzleti tevékenységekkel függ össze [212]. Az e-kereskedelem népszerűségét a

nagy közösségi oldalak is felismerték, és igyekeznek integrálni szolgálatásaik körébe, ahogy tette például a Facebook is.

Az online bűnözői piacok az esetek többségében Darknethez kapcsolódnak. Darknet alatt azoknak az Deepweben fellelhető oldalak 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 piacát nevesíthetjük, de vásárolhatunk álprofilokat, amelyeket például politikai döntéshozatal befolyásolására lehet használni, malwareket, amelyekkel a közösségi oldalakon alkalmazhatunk, de hozzájuthatunk olyan eszközökhöz is, amelyek segítségével feltörhetjük mások közösségi profiljait. Szintén nagy piaca van a kiszivárgott felhasználói adatbázisoknak.

A kibertér és terrorizmus összefonódását első alkalommal a 2016-os IOCTA jelentés nevesítette. A fogalom nem egyenlő a kiberterrorizmussal, ugyanis ez alatt azokat a tevékenységi köröket értjük, amelyeket az internethasználatból fakadnak. A terroristák az alábbi tevékenységek végzésére használják az internetet, ahogy az Iszlám Állam nevű terrorszervezet a kibertámadást leszámítva a felsoroltak mindegyikében professzionálisan alkalmazott:

- információgyűjtés;
- social engineering;
- kapcsolattartás,
- propaganda;
- új tagok toborzása;
- támogatók szerzése,
- pszichológiai és információs hadviselés;
- komplex kibertámadás.

A terroristáknak jelenleg még nincs meg az a humán és technikai képesség, amivel egy kritikus infrastruktúrát lennének képesek támadni a kibertérben, de vélhetően törekszenek a kialakítására.

A social engineering kérdéskörét korábban már bemutattam, így itt nem ismétlem meg. A határterületek között nevesíti a jelentés a szolgáltatás szerű bűnözést (Crime as a Service, továbbiakban CaaS, ami arra utal, hogy bűnözők bizonyos képességeket, legyen szó technikai eszközök biztosításáról vagy támadások végrehajtásáról, szolgáltatásként forgalmaznak a Darkneten. A CaaS széles körben igénybe vehető, a kiberbűnözők gyakran online

ügyfélszolgálatot is biztosítanak a call centerek mintájára. Ez például terroristák esetében jelenthet óriási kockázatot, hiszen, ha ők nem is képesek egy komolyabb kibertámadás megvalósítására, ha rendelkezésükre áll a megfelelő összeg, megvásárolhatják a szolgáltatást.

A bűnözők pénzügyi tevékenységek kapcsán példaként a bitcoin bányászatot nevesíthetjük, ami közösségi oldalakon alkalmazott malwerek segítségével valósulhat meg, vagy olyan FinTech megoldásokat azonosíthatunk, amelyek közösségi adakozás álcájával pénzmosásra vagy terrorizmus finanszírozásra használnak.

A felsorolt területek vizsgálata azért fontos, mert a bűnüldözőknek ezekre választ kell adni, és olyan jellegű képességeket kell kialakítsanak, amelyek minimalizálják az ilyen jellegű bűncselekmények bekövetkezését, és elősegítik a felszámolásukat. A kiberbűnözés kapcsán ez különösen nehéz, hiszen az egyes bűncselekmények határokon is átívelhetnek. Nem csak az bonyolítja a kiberbűnözés elleni harcot, hogy rendkívül nehéz a felderítése, hanem az egyes országok eltérő jogszabályi környezete is akadályt jelenthet a vádelemelések során. Ezen a felismerésen alapul a 2001-ben Budapesten aláírt Cybercrime egyezmény, aminek a célja a jogharmonizáció megkönnyítése. Hasonló nehézségekbe ütközik egyébként a kiberterrorizmus elleni fellépés is a jogharmonizáció nehézsége okán, amit csak globális összefogással lehet elérni [213]. Az Európai Unió élen jár jogharmonizációs tekintetben, de fontos, hogy minél több állam ratifikálja az egyezményt.

4.3. A közösségi média, mint az államok politikai döntéshozatalának befolyásoló eszköze

Carl von Clausewitz A Háborúról című könyvében fogalmazta meg, „*a háború a politika folytatása más módszerekkel*”. A tétel érvényessége nem változott a digitális térben sem, a kiberhadviselés célja ugyanúgy a politikai döntéshozatal befolyásolása. Nem véletlen tehát, hogy a közösségi média ilyen célú felhasználását korán felismerték politikusok, civil, de katonai és nemzetbiztonsági szervezetek egyaránt.

A közösségi média politikai döntéshozatalának befolyásolására különböző módszereket nevesíthetünk, azonban az elérni kívánt cél nagyságától függően egyre komplexebb eljárásokat azonosíthatunk. A harmadik fejezetben a CA kapcsán már foglalkoztam annak kérdésével, milyen módon lehet pontos célzás eredményeképpen olyan tartalmat megjeleníteni a felhasználók előtt, amellyel egy adott terméket, esetünkben politikust, ideológiát értékesíthetnek magas fokú hatékonysággal.

Egy társadalmi, politikai kérdés közösségi médiában történő megjelenése, illetve annak terjedése létfontosságú az üzenet közvetítőjének, hiszen ahogy az első fejezetben elemzett statisztikai adatokból is kiderült, rendkívül sokan használják napi szinten a közösségi oldalakat, illetve egyre nagyobb arányban elsődleges hírforrásként tekintenek ezekre az oldalakra. A közösségi médiában a politikusok által megosztott tartalmak, különösen választási kampányban komoly szerepet játszanak a választók befolyásolásában. A 2016-os amerikai elnökválasztási kampányban Donald Trump és Hillary Clinton például a Twitteren folytatott háborút a tartalommegosztás tekintetében [214]. A közösségi oldalak a hírközlést alapjaiban változtatták meg az által, hogy egy hír, beszámoló megosztásához nem szükséges komolyabb technikai felszereltség, egy okos mobil eszközzel a zsebében bárki újságírónak érezheti magát, hiszen, ha jól időben van jó helyen, egy fénykép, videó, élő közvetítés segítségével akár milliókhoz is eljuthat a közvetítése.[91] Ez a fajta valós idejű közvetítés egyúttal magában hordozza annak a veszélyét, hogy az információk ellenőrizetlen módon terjedhetnek, elvesznek a hagyományos újságírói eljárások, mint a szerkesztés, tényellenőrzés, forrásellenőrzés. A közösségi médiában megjelenő hírek, információk az azonnaliság miatt az éles hírversenyben gyakran oda vezettek, hogy a mainstream média a közösségi médiában megosztott beszámolókat, híreket vette át, és az alapján közvetített. A hírközlésben mára már oda jutottunk, nem egy szimpla közösségi médiában megjelenő bejegyzésből lehet a mainstream médiában hír, hanem a bejegyzés alatt született kommentből.

Nem nehéz belátni, minél többen osztanak meg valamilyen hírt, annál többen látják, annál könnyebb a megosztott hír relevanciájára hivatkozni. Nem véletlen tehát, hogy az államok katonai, nemzetbiztonsági szolgálatai nem bízzák a véletlenre a hírek terjedését. 2011 februárjában egy tényfeltáró újság figyelt fel az US Air Force által kiírt pályázatra, ami egy „online identitásmenedzselő szoftverre" (továbbiakban OIMSZ) vonatkozott [215]. Az OIMSZ egy olyan botnethálózat lett volna, amely a közösségi médiában létrehozott álprofilok segítségével politikai döntéshozatal befolyásolására alkalmaztak volna. Értelemszerűen a szoftver meg kellett feleljen olyan kritériumoknak, mint például a geolokációs helymeghatározás kijátszása, hiszen például egy Közel-Kelet ellen irányuló művelet esetén nem célszerű, ha a profilok helymeghatározása mondjuk Coloradoba, az US Air Force Akadémiájához vezet. A VPN mellett az álprofiloknak az adott célterületre testreszabott legendával is kellett rendelkezzenek. Az OIMSZ-hez hasonló botnethálózatokat az elmúlt

[91] Például 2011-ben egy pakisztáni állampolgár Twitteren élőben közvetített egy szomszédjában zajló katonai akcióról, de csak másnap derült ki, Osama bin Laden elleni rajtaütés pillanatairól tweetelt.

években vélelmezhetően több állam épített ki. Az e célra létrehozott bontnetek különösen Twitteren népszerűek [216].

A közösségi médiában szervezett politikai mozgalmak jelentőségét a 2010 év végén kibontakozott, a köznyelvben „Arab-tavaszként" hivatkozott eseménysorozat véleményem szerint alátámasztja [217] [218]. Nem véletlen, hogy a SciVal adatbázis segítségével végzett kataszteranalízis az „Arab-tavaszt" olyan magas számban adta eredményként. Mint az köztudott, a 2010 év végén tüntetések kezdődtek Tunéziában, amit közösségi oldalakon szerveztek az elsősorban városokban lakó fiatalok, de ez a térség többi országára is átterjedt. A kezdeti békés tüntetésekre a kormányok erőszakos választ adtak, azonban az ezekről készült képek, videók bejárták a közösségi oldalakat, bekerülve a globális mainstream médiába is, amely nem csak a tüntetők elszántságát, de a nemzetközi közvélemény szimpátiáját is erősítette. Ha egy pillanatra eljátszunk a gondolattal, hogy egy OIMSZ-hez hasonló szoftvert használ egy ilyen esemény során egy idegen állam, akkor értjük meg igazán a szoftver lényegét. Az egyébként is meglevő elégedetlenséget egy nagy számú, de arra a műveleti területre felépített álprofilokból álló botnet hálózat támogat, növelve az azzal kapcsolatos tartalmak megosztását, gondoskodva arról, hogy olyan jelentőségű hírértéke legyen, amit – akár kis segítséggel- a nemzetközi közvélemény elé is lehet tárni, felhasználva a mainstream médiát, beláthatatlan következményei lehetnek. Ezt mi sem példázza jobban, mint egy 2014-es eset, amelyben Oroszország Magyarországot azzal vádolta, hogy T-72-es harckocsikat szállít Ukrajnának, megszegve az európai uniós fegyver export tilalmat. A vádakat az orosz Külügyminisztérium egy, a szélsőjobboldali Magyar Nemzeti Arcvonalhoz[92] köthető Hídfő.neten[93] megjelent beszámolóra alapozta. A Hídfő.netet Magyarországon alig ismerték, marginális oldal volt, mégis, véletlenül kiszúrta az orosz Külügyminisztérium. A tiltakozás természetesen hirtelen a nemzetközi közvélemény figyelmébe került, a diplomáciai jegyzéktől volt hangos a nemzetközi mainstream média. Viszonylag hamar fény derült azonban arra, hogy a Hídfő.net mögött az orosz nemzetbiztonsági szolgálatok áll, a tiltakozásnak alapot szolgáltató hírt is vélelmezhetően hozzájuk kötődő személyek írták meg.

A botnet hálózatok mellett az egyes államok úgynevezett „troll hadseregeket" is alkalmaznak. Az egyik legismertebb „troll hadsereg" Oroszországhoz köthető. Egykori tagok beszámolói alapján ezek a műveletek szigorúan szabályozott keretek között működnek [220].

[92] Az európai szélsőjobboldali pártok és Oroszország viszonyáról bővebben lásd a Political Capital „Eurázsiai vagyok" címen készített elemzését [219].
[93] Azóta az oldal a sokkal őszintébb, .ru domain végződésen érhető el.

A Szentpéterváron található Internet Research Agency nevű, online kutatással foglalkozó cégnél e szerint váltott műszakban,[94] hármas csoportokban[95] eltérő bérkategóriába[96] sorolva dolgoznak, becslések szerint ezren, hogy nyugatellenes, Kreml-barát híreket osszanak meg hazai és külföldi portálokon.[97] A témákat az adott nap elején jelölik ki, és meghatározott számú kommentet[98] kell meghatározott számú profillal elhelyezni. Ezeket nagyban meghatározzák az aktuális kül- és belpolitikai történések. Természetesen nem csak Oroszország, aki ilyen „troll hadseregeket" tart fenn, Kína esetében több millió személyből álló csoportokról beszélhetünk [221], de vélelmezhetően nyugati államok is építettek ki ehhez hasonló képességet.

A politikai döntéshozatal befolyásolásának egyik legfontosabb eszköze a közösségi médiában az álhírek terjesztése, aminek sikerességét az úgynevezett „post truth" jelenséggel írják le [222]. A fogalom egy olyan helyzetet ír le, amikor a közvéleményre nem a tények, hanem az érzelmek, a meggyőződésen alapuló hitek hatnak. Álhírek alatt azokat a híreket értjük, amelyek kitaláción alapulnak, nem támasztják alá tények. Az álhíreknek azonban széles spektrumát különböztethetjük meg. Melissa Zimdars gyűjteményét alapul véve [223] az alábbi kategóriákat azonosíthatjuk:

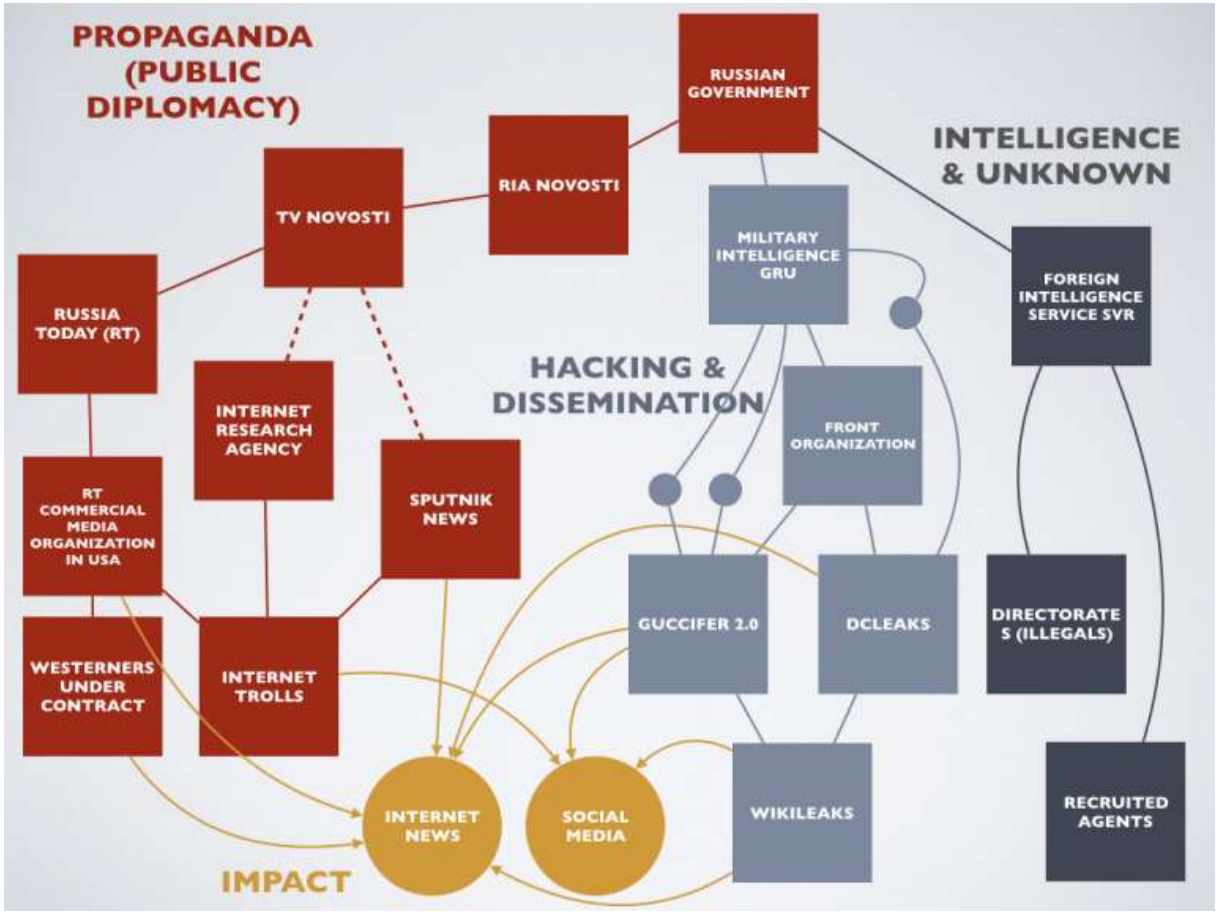
- álhírek;
- elfogult hírek, a megjelenő hírek egy bizonyos politikai oldal, ideológia mellett súlyosan torzított formában, egyoldalúan jelennek meg;
- áltudományos hírek, tudományosan nem alátámasztott, súlyosabb esetben a tudományos eredményeknek ellentmondó hírek, például az oltásellenességgel kapcsolatos hírek;
- összeesküvés elméletek;
- szatirikus hírek, olyan humorosan megírt hírek, amelyek bár álhírek, céljuk azonban a szórakoztatás;
- kattintásvadász hírek, olyan hírek, amelyek mind címükben, mind tartalmukban félrevezetőek, céljuk, hogy minél többen kattintsanak az oldalra, hogy ily módon növeljék a reklámbevételeket.

[94] Helyiségenként hozzávetőlegesen 20 fő dolgozott 3 szerkesztő alá sorolva.
[95] Ebből volt egy témafelvető, akihez később csatlakoztak a többiek vitát generálva, megerősítve a hírt stb.
[96] 2015-ben ez 45 ezer rubelnek (219 ezer forintnak) megfelelő havi bérezést, angol nyelvű kommentek esetében 65 ezer rubelt (316 ezer forint) jelentett.
[97] A leggyakoribb visszatérő elem, hogy a Nyugat, az európai civilizáció a vesztébe rohan a dekadencia, a liberalizmus, újabban a menekültek, a gyenge vezetők miatt, az egyetlen mentsvár az erőskezű, feddhetetlen Vlagyimir Putyin.
[98] 12 órás műszakban 135 kommentet.

Az egyes kategóriákat politikai döntéshozatal befolyásolására egyaránt használják, hiszen a kitűzött célt nem csak akkor lehet elérni, ha az olvasók igaznak tekintenek egy hírt, hanem akkor is, ha más jellegű hírekkel bizonytalanságot keltenek, a hivatalosnak tekinthető híreket megkérdőjelezik.

A 2016-os amerikai elnökválasztás óta Oroszországot rendszeresen éri az a vád, hogy a kiberteret, de azon belül a közösségi médiát aktívan használja idegen államok belpolitikai döntéshozatalának befolyásolására, aminek egyik fő eszköze az álhírek terjesztése. Ennek hatására jelentősen bővült a témával foglalkozó szakirodalom száma [224] [225]. Az orosz lélektani műveletek felerősödése a 2014-re, az ukrajnai konfliktus kialakulásához vezethető vissza, de aktívan 2008-tól, a grúziai háborútól használják [226]. A kibontakozó orosz-ukrán konfliktusra a szakirodalom hibrid háborúként hivatkozik. Hoffmann fogalmi meghatározását kölcsönözve: „*Hibrid fenyegetések a hadviselés számos formáját magukban foglalják, beleértve a konvencionális képességeket, irreguláris harceljárásokat és képződményeket, valamint a válogatás nélküli erőszakot alkalmazó terrorista akciókat és bűnözői tevékenységeket. Hibrid háborúkat egyaránt folytathatnak állami és a legkülönfélébb nem állami szereplők. Az egymástól elszigetelten működő egységek, vagy akár ugyanaz a csoport is folytathat „multimodális" tevékenységeket, de ezek általános, műveleti, valamint harcászati irányítása és koordinálása a fő hadszíntéren megy végbe, annak érdekében, hogy a szinergikus hatások bekövetkezzenek a konfliktusok pszichológiai és fizikai dimenzióiban. Ezen hatások a háború valamennyi szintjén jelentkezhetnek [227]*." Nem nehéz belátni, hogy a közösségi média a rajta folytatott hírszerzéssel, az álhírekkel kapcsolatos lélektani műveletekkel a hibrid hadviselés fontos elemeit képezi.

Egy, az amerikai nemzetbiztonsági szolgálatok által nyilvánosságra hozott jelentés különböző szereplőket azonosít az orosz lélektani műveletek végrehajtóiként. A 29. számú ábrán Edward M. Roche foglalta össze ezeket az aktorokat, akik között hírszerző szolgálatok, hackerek, illetve a propagandáért felelős entitásokat találhatunk. Ez alapján három részre oszthatjuk a szereplőket, a pirossal jelölt, propagandában érintetteket, ide sorolva többek között az internetes trollokat, az említett Internet Reseach Agencyt, az RT-t, a Sputnik Newst, világosabb kékkel jelölve a hackereket és a terjesztésért felelős csatornákat, ide értve többek között a WikiLeakset vagy a katonai hírszerzést, továbbá sötétebb kékkel jelölve a hírszerző szolgálatokat. Az ábrán sárgával látható az egyes szereplők hatása a közösségi oldalakon, illetve a hírodalakon.



29. ábra Az orosz lélektani műveletek szereplői (Forrás: cyberarmscontrolblog [228])

Oroszországot rendszeresen éri az a vád, hogy lélektani műveleteivel komoly hatást gyakorol az európai migrációs válság kezelésében, de a 2016-os BREXIT névszavazás és a szintén ebben az évben lezajlott amerikai elnökválasztás eredményében. A RAND Corporation az orosz propaganda sikerét négy tényezőre vezeti vissza [226]:

- számos csatornán közvetítik;
- gyors, ismétlődő formában terjesztik;
- hiányzik belőle az objektivitás;
- nem következetesek.

A BREXIT kampány esetében 2017 novemberében vádolta meg Oroszországot Theresa May brit miniszterelnök, hogy egyrészt anyagi támogatásban részesítette a kilépéspárti formációkat, másrészt a választást megelőző napokban orosz Twitter fiókok különböző információkkal és álhírekkel igyekeztek társadalmi feszültségeket kelteni, alapvetően a bevándorlás ellenességet felhasználva.

A Belbiztonsági Minisztérium és az FBI messzebb ment Maynél, közös, JAR-16-20296A jelzésű elemzésükben [229] konkrétan Oroszországot nevesítették már a címében. Ahogy Kovács László és Krasznay Csaba megfogalmazza, „*az amerikai védelmi szakterminológiában különleges szerepe van az úgynevezett attribution fogalmának, mely azt jelenti, hogy megalapozott gyanú alapján nevesítik az elkövetéssel vádolt országot. A jelentés ki is emeli, hogy korábban egyetlen ilyen dokumentum sem nevesített konkrét országot a kibertérben elkövetett tevékenységekért. Éppen ezért arra lehet következtetni, hogy mind a műszaki, mind a hírszerzési bizonyítékokat elégségesnek tartja az amerikai hírszerző közösség ahhoz, hogy az orosz kormányt és név szerint Vlagyimir Putyint nevezzék meg felelősnek a kibertámadások elrendeléséért. Az attribution viszont mindig politikai döntés, ami jelzi, hogy Obama elnök döntött arról, hogy Oroszországot nevesíteni fogják [230]*.”

Donald Trump megválasztásában természetesen számos ok játszott közre, de tagadhatatlan, Oroszország befolyásolási kísérlete jelentős következményekkel járt. A Kovács-Krasznay szerzőpáros Mert övék a hatalom című, idézett tanulmányukban rendkívül alapos kronológiai összefoglalását adják a történéseknek, témám szempontjából két releváns eseményt szükséges kiemelnem:

- több informatikai támadás érte a Demokrata Nemzeti Konvenciót, illetve demokrata politikusokat, közte Hillary Clinton elnökjelöltet. Az ily módon megszerzett információkat a WikiLeaksen publikálták. A DNK mellett a Republikánus Nemzeti Konvenciót is érik informatikai támadások;
- a nemzetbiztonsági szolgálatok szerint az orosz kormányzathoz köthető csoportok álhírekkel igyekeztek befolyásolni a szavazókat.

Hillary Clinton e-mailjeinek feltörését és a megszerzett levelek WikiLeaksnek történő kiszivárogtatását egy magát Guccifer 2.0-nak[99] nevező személy vállalta magára. Guccifer 2.0 magán román állampolgárnak adta ki, de számos jel utalt arra, hogy valójában a Fancy Bear[100] által kreált legenda volt. Julien Assange, a WikiLeaks vezetője, az oldal „arca” tagadta, hogy az általa nyilvánosságra hozott adatok Oroszországból kerültek volna a birtokába, azonban ez több dolog is cáfolta. A Clinton e-mailekkel kapcsolatban egy másik botrány is kibontakozott, amikor a Facebookon nem lehetett megosztani azokat a WikiLeakre mutatkozó hivatkozásokat,

[99] A név utalás egy Guccifer nevű erdélyi magyar hackerre, Lázár Marcellre.
[100] A Fancy Bear hackercsoportot a már említett GRU-hoz kötik, ami nem összekeverendő a Cozy Bear nevű hackercsoporthoz, utóbbiak ugyanis az orosz Szövetségi Biztonsági Szolgálathoz (FSZB), a KGB jogutódjához tartoznak. A Fancy Bear tehát katonai, a Cozy Bear pedig polgári kötődésű.

amelyek a Clinton e-mailekre mutatott. A Facebook a botrány hatására azt nyilatkozta, csupán technikai probléma miatt történt mindezt, de az eset megalapozott azoknak a vádaknak, amelyek szerint a Facebook jelentős támogatást nyújt a demokrata elnökjelöltnek. Mindezt erősítette a Facebook egykori dolgozóinak a vádja, amit végül a Facebook is kénytelen volt elismerni. Az eset lényege, hogy az Egyesült Államokban bevezették az úgynevezett „Trending topics", azaz felkapott hírek nevet viselő szolgáltatást, amelyben egy algoritmus válogatja össze a legtöbbet megosztott, ez által feltehetően releváns tartalmakat. Kiderült azonban, hogy ebbe gyakran beavatkoztak mesterségesen a Facebook dolgozói, és a népszerű, ámbár republikánus oldalhoz kapcsolódó híreket kivettek a „Trending topics" közül, amiket alig vagy egyáltalán nem megosztott demokratákhoz kapcsolódó hírekre cseréltem, elősegítve ezzel a magasabb olvasói elérést. Az elnökválasztást követően rendszeresen vádolták a Facebookot, hogy megakadályozhatta volna az álhírek ilyen mértékű elterjedését, azonban a „Trending topics" ügy miatt nem mert beavatkozni az álhírek szűrésébe, ugyanis azok nagy többsége a republikánus kampányt segítették.

A Facebook 2017 szeptemberében elismerte, hogy 2015 júniusa és 2017 májusa között mintegy 470, feltehetően Oroszországból való, hamis profillal vagy oldallal bejelentkező felhasználó mintegy százezer dollárt költött közel háromezer hirdetés megjelentetésére [231]. A hirdetések nem csupán politikai tartamúak voltak, akár csak a BREXIT esetében a bevándorlóellenességre építő álhírek, tartalmak jelentek meg, úgy itt is a társadalmat megosztó kérdésekről szóltak, fegyvertartás, polgárjogi mozgalmak stb. A Facebook belső vizsgálata azt is megállapította, hogy a közösségi oldalon 29 millió amerikai felhasználó került közvetlenül interakcióba a vonatkozó tartalmakkal, és összesen 126 millió amerikai felhasználóhoz jutottak így el a hirdetések, bejegyzések. Ezen felül a Facebook 170 Oroszországhoz köthető Instagram-fiókot törölt, melyek nagyjából 120 ezer témába vágó bejegyzést tettek közzé.

De nem csak a Facebook volt az egyetlen, amely fizetett hirdetések formájában segítette az orosz lélektani műveleteket. A Twitter 2752 Oroszországhoz köthető csatornát, illetve további 50 ezer automatikusan tweetelő álprofilt azonosított, amelyek összesen 1,4 millió bejegyzést tettek közzé a kampány során [232]. A Google is érintett volt ez ügyben, a YouTube-ra 1108 darab vonatkozó videót töltöttek föl, 43 órát kitevő tartalommal. Ezek terjesztését bizonyíthatóan 4700 dollárnyi hirdetéssel indították be [233]. Ezek a hirdetések azért voltak annyira sikeresek, mert a CA képes volt az általa kidolgozott módszertannal a lehető legpontosabban célozni a felhasználókat.

A Facebook a 2016-os választásokra egyébként egy kifejezetten kampányszakemberek részére is állított össze hirdetési csomagot. Ennek a lényege az volt, hogy a Facebook algoritmusa azonosította a politikailag legaktívabb felhasználókat, hogy őket célozzák politikai hirdetésekkel. Ennek során nem fizetett hirdetésként látták az egyes politikai reklámokat, hanem megosztott tartalomként. Mindezt arra a megfigyelésre alapozták, hogy a felhasználók jobban hisznek egy ismerősük, barátjuk által megosztott tartalomba, mintha ezt hirdetésként látnák. Ezzel gyakorlatilag a megrendelők úgy hirdethettek, hogy a felhasználók számára nem derült ki, valójában politikai reklámot olvasnak, nem kötötték össze egy párttal, csupán a hírfolyamukban egy ismerősük tartalommegosztásaként látták. Ez azért is fontos, mert a politikai hirdetések szigorúan szabályozottak, utalni kell benne többek között a megrendelőre, bizonyos etikai-erkölcsi szabályok is kötik. Ezek azonban ily módon teljesen kijátszhatóak voltak.

Kutatások azt bizonyították, hogy a Facebook képes a választási részvételt befolyásolni. 2010 novemberében lezajlott amerikai választások alatt végzett az oldal egy olyan pszichológiai kísérletet, amelyben egy, a hírfolyamban elhelyezett „Szavaztam" gomb aktivizálásával a felhasználók jelezhették, hogy éltek a választójogukkal, és a profilképük mellett megjelent a „Szavaztam" felirat [234].[101] A vizsgálat célja az volt, kiderüljön, kialakul-e egyfajta közösségi nyomás, és azok a felhasználók is elmenjenek szavazni, akik egyébként nem terveztek. A kutatás megerősítette ennek a létét, azok a felhasználók, akiknek a hírfolyamában megjelentek ezek a profilok, 0,39%-kal nagyobb arányban mentek el szavazni, mint azonos időszakban tették. Ez összességében 340 ezerrel több szavazatot jelentett, ami az Amerikai Egyesült Államok választásra jogosultak számához képest csekélynek tűnik, de figyelembe véve George W. Bush 2000-ben történt újraválasztását, ez a 340 ezer szavazó igen is jelentős lehet, hiszen Bush Floridában 537 szavazattal kapott többet, mint kihívója.

Ez a kísérlet nem avatkozott be irányítottan a választás menetébe, nem alkalmaztak célzott manipulációt, amire egyébként a Facebooknak megvan a lehetősége, hiszen ahogy fentebb bemutattam, ismeri preferenciáinkat, és ez alapján válogatja ki az elénk kerülő tartalmakat. Egy 2012-ben végzett kísérlet azonban azt is igazolta, a Facebook képes az érzelmeinket is befolyásolni [235]. 700 ezer felhasználót vontak be a tudtuk nélkül a kísérletbe, amelynek során az alanyok felének egy héten keresztül csak pozitív, míg a másik felüknek csak negatív tartalmakat jelenítettek meg, vizsgálva, hogyan hat a tartalommegosztási szokásaikra. A kísérlet igazolta, hogy azok, akik csak pozitív tartalmakat láttak, ők is pozitív tartalmakat kezdtek

[101] Hasonlóra volt lehetőség a 2018. április 8-ai magyarországi országgyűlési választások alkalmával is.

megosztani, míg akik negatív tartalmakat láttak a hírfolyamunkban, ők hajlamosabbak voltak negatív tartalmakat megosztani.

Mindennek óriási jelentősége van. Ezek a kutatások azt jelentik, nem csupán a mozgósításra képes a Facebook, de a hírek szelektálásával, adott esetben az érzelmeik manipulálásával azt is képes lehet befolyásolni, kire szavazzanak a felhasználók. A szakirodalom ezt nevezi digitális gerrymanderingnek, ami a körzethatár-átrajzolás virtuális változatát takarja, amely során nem valójában nem a körzethatárokat befolyásolják, hanem a megjelenített tartalmakat manipulálják oly módon, hogy hatást fejtsenek ki a felhasználókra [236].

Azt gondolom, az a képesség, amivel a Facebook rendelkezik a politikai döntéshozatal befolyásolásában, az egyik legerősebb entitássá teszi a politikai alrendszerben. Hiába törekednek államok a Facebook és a közösségi oldalak felhasználásával a politikai döntéshozatal befolyásolására, soha nem lesz meg az a lehetőségük és erejük, amivel a Facebook és egyéb közösségi oldalak bírnak. Ebből következően úgy vélem, igen fontos ezeknek az oldalaknak az államilag történő szabályozása, hiszen ahogy például a nemzetbiztonsági szolgálatok esetében is felmerül az „őrzők őrzésének" problémája, úgy a Facebook esetében is reális ez az igény. 2017-ben egyre többen beszéltek arról, hogy 2020-ban Mark Zuckerberg, a Facebook alapítója aspirál az elnöki hivatalra. Természetesen Zuckerberg tagadta ezeket, de úgy vélem, semmilyen garancia nincs arra vonatkozóan, ha mégis úgy döntene, elindul a választásokon, a Facebook adta lehetőségeket ne aknázná ki, ami a fentieket figyelembe véve majdhogynem 90 fokos szögben döntené a pályát számára.

Donald Trump győzelmét követően rengeteg bírálat érte a Facebookot, hogy nem tett meg mindent, hogy kiszűrje az álhíreket, ami óriási nyomás alá helyezte a közösségi oldalt. Ennek egyik oka a fentebb említett „Trending topics" botrány volt, azonban látni kell azt is, hogy rendkívül nehéz az álhírek szűrése. A Facebook 2015-től kezdve igyekszik szelektálni az álhíreket, de ez nem csak nem hatékony, de a sajtószabadságot is veszélyezteti, ezért különösen fontos, milyen elvek mentén szűrik az álhíreket. 2015-től a felhasználók jelenthetik a szerintük álhíreket tartalmazó megosztásokat, azonban ez egyben azzal is jár, hogy a tényekkel alátámasztott híreket is álhírnek jelölik meg és jelentik, ami bizonyos politikai hangok elhallgattatásának lehet az eszköze. 2016-tól a kattintásvadász híreket igyekeztek szűrni mesterséges intelligencia használatával, illetve a Google-el és Twitterrel közös kezdeményest indítottak az álhírek szűrésére.

Ahogy az álhírek kategorizálásánál említettem, több típusukat használják a lélektani műveletek végzésére. Az álhírek terjesztését nem csak politikai elkötelezettség vagy a választások befolyásolásának szándékával alkalmazhatják, sok esetben anyagi haszonszerzés azonosítható a motivációk mögött. Egy montenegrói városban, Valesben például 140 Trump-párti álhír oldalt üzemeltettek egyetemisták, akik felismerték, minél nagyobb képtelenséget írnak Trumpról vagy ellenfeléről, Hillary Clintonról, annál többen kattintanak az oldalra és osztják meg a híreket. Az oldalakra történő kattintás pedig a reklámbevételeket növelték az oldalakon elhelyezett nagy számú „pay per click", vagyis kattintás alapú hirdetésekkel. Ezen a felismerésen alapult a Facebook és Google elhatározása, 2017 év végén, hogy az álhír közvetítőként azonosított oldalak esetében tiltani fogja a hirdetési rendszerének az integrálását. A műhelyvita és a doktori védés közti időpontban végül az is kiderült, hogy mégsem csupán anyagi haszonszerzés motiválta a montenegrói fiatalokat, ugyanis az oldalak mögött egy Trajcse Arszov nevű médiajogász állt, aki kapcsolatban volt két, a republikánus párthoz köthető amerikai személlyel, Ben Goldmannel és Paris Wade-del, akik a Liberty Writers News nevű konzervatív összeesküvés elméletekkel foglalkozó oldalt üzemeltették [237]. Az amerikai elnökválasztás orosz befolyásolásának vizsgálatával megbízott Robert Mueller különleges ügyész vizsgálatai egy, az Internet Research Agencyvel kapcsolatba hozható személyt is azonosítottak a montenegrói álhírgyárral kapcsolatban, azonban jelenleg még nem bizonyított az együttműködés az orosz kormány és Arszov között.

et volt, hogy a megosztott hírek esetében álhírként jelölnék meg a kifogásolt tartalmakat, de ez sem aratott sikert. Az elgondolás lényege abból állt, hogy felhasználók jelentik a szerintük álhíreket tartalmazó megosztásokat, amelyeket a Facebook külső vállalkozók alkalmazásával tényellenőrzés alá vetette volna, akár csak a hagyományos újságírásnál bevett szokás. Amennyiben a vizsgálat arra az eredményre jut, hogy a cikkben megfogalmazott állítások nem valósak, úgy ez az információ megjelent volna a megosztott tartalomnál. Ezzel, megítélésem szerint az a probléma, hogy rendkívül nehéz meghatározni a különbséget a vélemény és a hír között, előbbinek nem feltétele a tényszerűség, az elfogulatlanság, így annak eldöntése egy vélemény esetében, hogy hazugság-e, értelmetlen. Arról nem is beszélve, ha valaki hisz egy adott véleményben, akkor nem garantálja semmi, hogy az álhírként jelölt tartalmat ne az ellenkező véleményt hangoztatók ármánykodásaként értékelje, amelynek során így akarják az igazságot elhallgattatni, ezért álhírnek hazudjál azt.

Az álhírek elleni harcban az egyik legjelentősebb lépést Németország lépte meg. 2017 nyarán egy olyan jogszabályt fogadtak el, ami maximum 50 millió eurós büntetést szabhat ki a

közösségi oldalakra, ha a bejelentést követő 24 órán belül[102] nem távolítják el a gyűlöletkeltésre alkalmas tartalmakat. A jogszabály 2018. január 1-től vált hatályossá, és minden olyan közösségi oldal esetében kötelező alkalmazni, amelyiknek legalább 2 millió német felhasználója van. Amennyiben a felhasználó németországi IP-címről keresi fel ezeket az oldalakat, annak látnia kell egy olyan felületet, amin bejelentést tehet, ha gyűlöletkeltésre alkalmas, a német alkotmányt sértő vagy bűncselekményre buzdító posztot lát. Összesen húsz német jogszabály alapján nyílik mód egy bejegyzés jelentésére, beleértve az önkényuralmi jelképek tiltásáról szóló jogszabályt, az alkotmányos rend felforgatásának kísérletét egyaránt. Annak érdekében, hogy a közösségi oldalak eleget tudjanak tenni a törvényi rendelkezésnek, bővítették a moderátorok számát, akiknek el kell dönteni, hogy a jelentett tartalom valóban jogsértő-e, és amennyiben igen, törölniük kell. A jogszabállyal kapcsolatban számos kritikát fogalmaztak meg a német pártok, illetve jogvédők. A legjelentősebb érv az ítélkezés privatizálása, hiszen annak megállapítása, hogy valami törvénytelen vagy sem, megfelelő eljárás keretében a bíróságok feladata. Ezt a feladatot nem vehetik át vállalatok. Ehhez kapcsolódik, hogy rendkívül szoros határidőt szab a döntés meghozatalára, így nincs garancia arra vonatkozóan, hogy az esetlegesen nagy számban jelentett tartalmaknál nem törlik szinte automatikusan a büntetés elkerülése érdekében, így pedig indokolatlan cenzúra valósulhat meg. Németország mellett Nagy-Britannia is hasonló jogszabály bevezetésén, „büntetőadó" megalkotásán gondolkodik, valamint Emmanuel Macron, Franciaország elnöke is bejelentette, hogy felül fogják vizsgálni a francia médiaszabályozást, hogy felvegyék a harcot közösségi médiában terjedő álhírekkel szemben. Talán nem meglepő, az Egyesült Államokban is törvényjavaslatot nyújtottak be Honest Ad Act, azaz Őszinte Reklám Törvény elnevezéssel, ami a közösségi média, elsősorban a Facebook politikai felelősségével foglalkozik. A jogszabály előírná:

- választási kampánykommunikációnak minősül az online hirdetés is, ez eddig nem volt nevesítve néhány vonatkozó törvényben;
- bizonyos összeghatár felett archiválni kell minden politikai reklám adatait;
- ezekbe beletartoznak a megrendelő adatai, a hirdetés pontos szövege és formája, a célcsoport, az ár, az elért emberek mennyisége és demográfiai összetétele, a publikálás időpontja;

[102] Nem egyértelműen megállapítható tartalmak esetén egy héten belül.

- a közösségi platformoknak mindent meg kell tenniük, hogy külföldi állampolgárok és csoportok ne adhassanak fel az amerikai választók befolyásolására alkalmas politikai hirdetéseket.

2018 januárjában jelentette be Mark Zuckerberg, hogy ismét átalakítják a Facebook hírfolyamát az álhírekkel szembeni harci jegyében. A változások előtérbe helyeznék az ismerőseink életével kapcsolatos tartalmakat, és háttérbe szorítanák a híroldalakat. Ez a lépés azonnal számos kritikát hozott, hiszen ily módon nem csak az álhíreket terjesztő oldalak elérhetősége csökkenne radikálisan, hanem azoké az oldalaké is, amelyek nem fizetnek a megjelenésért.

Nem kérdés, hogy valamilyen módon fel kell lépni az álhírek, a gyűlöletkeltő tartalmak ellen. Ezek nyilván nem csak politikai tartamúak lehetnek, ugyanúgy káros többek között az oltásellenességgel kapcsolatos álhírek terjedése, a zaklatásokkal kapcsolatos tartalmak megjelenése is. De hogy milyen módon lehet hatékonyan szabályozni államilag a közösségi oldalakat, összetett és nehéz kérdés, amire még nem született egyöntetűen jó válasz. Ha csökken az anonimitás, ami az internet egyik alapja volt a kezdetekben, a kormányok, a közösségi oldalak egyre több mindent fognak tudni a felhasználókról, ami a szólásszabadság, a véleménynyilvánítási szabadság kárára válhat, és nem csak a vállalatok, kormányok által alkalmazott cenzúra nőhet meg, de az öncenzúra is egyre jellemzőbbé válhat. Azt sem szabad elfelejteni, hogy a közösségi oldalaknak, annak ellenére, hogy egy adott országhoz köthetőek, gyakran globális hatásuk van, és így például az amerikai gyakorlat nagy mértékben beavatkozhat más, szuverén nemzetek életébe. Visszautalva a német szabályozásra, a közösségi oldalak egyre kevésbé lesznek érdekeltek abban, hogy a felhasználók anonim legyenek jelen, ez pedig az internet nagy fokú szabályozását, állami ellenőrzésének lehetőségét vetíti elő.

A német szabályozás megalkotása mögött nem csak az idegen államok befolyásoló kísérlete azonosítható, hanem terrorszervezetek által végzett lélektani műveletek is. A politika tér alakítói nem csak hivatásos politikusok lehetnek, hanem civil szervezetek, magánemberek, politikai elemzől. E megállapítás különösen érvényes a terroristákra, hiszen az ő céljuk is valamilyen politikai hatás elérése. Az Iszlám Állam több tekintetben nevesíthető paradigmaváltónak, hiszen egyrészt önálló államot, kalifátust kiáltott ki, amelyben az állami funkciókat egyedül gyakorolta, másrészt, a kiberteret is professzionálisan használta lélektani műveletekre [238].

A terrorizmus nem létezhet propaganda nélkül, hiszen ezzel hívják fel a figyelmet a szervezet által képviselt célokra, az akciójuk kiválasztásában jelentős szerepet játszik a minél

nagyobb médiafigyelem elérése [239]. A propagandának kettős célja van, amellett, hogy növeli a szervezet reputációját, komoly hatása van az új tagok, pénzügyi támogatók megnyerésében, ami nélkül a szervezet működésképtelenné válhat [240]. Az Iszlám Állam propagandájának első állomása maga a névválasztás volt, 2003-as megalakuásától kezdve 2014-ig, a Kalifátus kikiáltásáig.[103] Az Iszlám Állam a propagandát mesteri szinten valósította meg. Szemben az Al-Kaida rossz minőségű propagandavideóival az Iszlám Állam HD minőségben, filmes vágásokkal, angol nyelven, arab felirattal a közösségi média számos felületén terjesztette hashtagekkel [241] [242] [243].

Margitics József tanulmányában vizsgálta az Iszlám Állam közösségi oldalakon alkalmazott propagandáját. Ez alapján az alábbi elemeket azonosíthatjuk [244]:

- Dzsihád Média Platform weblap, amin a regisztrált felhasználók oszthatják meg a híreket, kommentelhetik. 2015-ben a regisztráltak száma a tagok száma meghaladta a 3000 főt, akik több mint 400 ezer kommentet írtak. Az oldalon regionális bontásban is szerepeltek hírek, friss hírek- mindezek több nyelven, beleértve az angol, francia, német nyelveket. Korán értelmezésekkel kapcsolatos topikok, propaganda fotók és videók, de emellett családi, egészségügyi témákban is születtek írások.
- Iszlám Állam Arhívum weblap, amin az Iszlám Államhoz köthető beszámolók, fényképek, videók szerepelnek, beleértve harcosok üzeneteit, amit toborzásra, propagandára használtak.
- Facebookon számos oldalt és csoportot üzemeltettek, ide sorolható többek között Iszlám Állam friss hírei, Mudzsahed hírek, Abu-Bakr Baghdadi stb. Csoportok: Az „Iszlám Erő Csoport" Hálózata, Az Umma Dzsihád a csúcsra kerül, Az Iszlám Állam médiasejtje stb.
- Twitteren 2017 első felében mintegy 300 ezer terrorista propagandát terjesztő fiókot töröltek. A fiókok törlését 2014 augusztusától kezdték intenzíven, ami James Foley, amerikai újságíró akkora datálható lefejezéséhez köthető.

[103] 2003-ban Iraki Al-Kaida néven alakult meg, 2011-ben, amikor a szomszédos Szíriában kitört a polgárháború, ott is megjelent, Iraki és Levantei Al-Kaida-ra cserélte a nevét, kifejezve azt, hogy Kelet-Szíriára és Irak északi részére egyként tekint. A szíriai polgárháború során mutatkozott meg az ideológiai különbség az Al-Kaidával, ami alapvetően a Nyugat elleni harcot tekinti szervező elemként, addig az Iraki és Levantei Al-Kaida iszlám Kalifátus megvalósításán fáradozik. Persze az Al-Kaida ideológiájában is megjelent a kétezres évek elején a globális Kalifátus gondolata, amit egy 20 éves terv végeredményeként terveztek megvalósítani, de 2010-es évek elején ezt az Iszlám Állam képviselte. Ez az ideológiai különbség vezetett végül a szakadáshoz az erőszakosság mellett, és végül 2013-ban az Iraki és Levantei Iszlám Állam (ISIS) nevet vették fel az ismert 2014-es névváltozásig.

- YouTubeon is számos csatornát üzemeltettek, amelyek kiképzésektől, fogvatartottak üzenetéig bezárólag, a mindennapi élet bemutatásán át sok mindenre kiterjedtek. Emellett, hogy megszólítsák a fiatalok, olyan tartalmakat is nagy számban állítottak elő, ami a dzsihád „menő” oldalát mutatta be, például a népszerű GTA V-öt alapul véve a játékba integrálták a terrorcselekményeket, Iszlám Államos zászlókkal, ruhákkal, ezeket pedig filmszerű történettel forgatták le.
- Dabiq és a Rumiyah nevű online újságokban szintén hírek, taktikai írások és propaganda található.
- Mobilalkalmazásokat nem csak a kapcsolattartásra használtak, mint például a Telegram Messengert, hanem propaganda terjesztésére is. Amikor 2014 augusztusától az említett James Foley kivégzése hatására nagy számban kezdték törölni az Iszlám Államhoz köthető profilokat a közösségi oldalak, létrehozták a Dawn of Glad nevű alkalmazást. Az alkalmazás sokáig letölthető volt a Google Play áruházból is. A letöltők hozzáférést engedélyeztek, hogy nevükben az alkalmazás az általa használt közösségi oldalakon híreket tegyenek közzé. Ez által lényegében szinte kiírthatatlanná téve az Iszlám Államot a közösségi oldalakról.
- Blogok, köztük az Iszlám Kalifátus, Iszlám Állam a fentiekhez hasonlóan híreket, propaganda üzeneteket közvetített.

Az Iszlám Állam napjainkra szerencsére rengeteget vesztett befolyásából, azonban az megállapítható, az út, amire rálépett a propaganda ilyen magas szintű használatával, az ezután következő terrorista szervezetek esetében követendő példával fog szolgálni. A propaganda mellett természetesen számos egyéb módon is használták a közösségi oldalakat, mint ahogy a kiberbűnözés esetében már megfogalmaztam. A hatékony propaganda pedig megadhatja azt a pénzügyi forrást, amivel kiberbűnözőket alkalmazva komplex kibertámadást hajtsanak végre.

4.4. A közösségi média integrálása a védelmi szféra egyes területein

Dolgozatom korábbi részében megvizsgáltam, milyen feladatok végzésére használhatják a közösségi médiát a védelmi szféra különböző területein. Azonosítottam azokat az eljárásokat, amelyek a honvédelmi-, rendvédelmi- és nemzetbiztonsági szolgálatok jogszabályban meghatározott feladatait támogatják, növelik azok hatékony végzését. A következőkben megvizsgálom, ezeket a feladatokat milyen szervezeti megoldások szerint lehet integrálni a védelmi szféra különböző szereplői esetében. Bizonyos esetekben azzal a módszertani

nehézséggel szembesülök, hogy a téma minősített voltából kifolyólag civil kutatóként nem rendelkezem információkkal arról, hogy az általam megfogalmazottakat egyébként alkalmazzák-e, és ha igen, milyen módon, de természetesen, ha rendelkeznék információkkal, ugyanúgy nem írhatnám le. A közösségi média nemzetbiztonsági szolgálatok körében történő felhasználása tipikusan ide sorolható. Meg tudom határozni, az egyes eljárásokat melyik szervezet esetében tartom indokoltnak kiépíteni, azonban jellegénél fogva elképzelhető, hogy az adott képességet már korábban létrehozták. Ennél fogva fordított megközelítést alkalmazok: az egyes alkalmazási területekből kiindulva vizsgálom, melyik szervezetek esetében azonosíthatunk kapcsolódást.

Legyen szó bármilyen képesség kialakításáról, mindegyik azt a célt szolgálja, hogy a jogszabályban meghatározott feladatát ellássa az érintett szervezet. Éppen ezért elsődlegesen a megfelelő jogi környezet kialakítása szükséges. A harmadik fejezetben az adat- és információbiztonságra vonatkozó jogszabályok vizsgálatakor javaslatot fogalmaztam meg, milyen szempontok alapján célszerű kiegészíteni a Magyar Honvédség és Rendőrség állományába tartozók közösségi média, okos mobil eszköz használatának szabályait. A jogszabályok elemzése során megállapítottam, egyfajta ellentmondás mutatható ki a közösségi médiában végezhető nyílt forrású információgyűjtés és az adatkezelés szabályozása között, ahogy erről a vizsgált NAIH tájékoztató rendelkezett. Véleményem szerint indokolt lenne ezt az ellentmondást feloldani, mert életszerűtlen az alkalmazása. A közösségi média számos támadás esetében jelent kiindulási pontot. Jelenleg a gyakorlatban azonban nem kezelik kellő prioritással a felhasználásával elkövetett bűncselekményeket. Szükséges kialakítani azt a környezetet, ami az elkövetett bűncselekményeket kivizsgálja. Egy Facebook profil az életünk szerves részét képezi, az online identitásunk a fizikai térben is hatással van. Ennek a profilnak a feltörésével nem csak adatainkat szerezhetik meg, de a nevünkben közzétett tartalmak segítségével a jó hírnévhez fűződő viszonyunkat sérthetik, a nevünkben zaklathatnak másokat vagy további bűncselekményekhez használhatják. Megítélésem szerint ez hasonló a „betört ablak” elvéhez [245], ami a kriminológiában arra utal, egy jelentéktelennek tűnő cselekmény, mint egy ablak betörése is, ha nem kezelik a bekövetkezésekor, egy olyan negatív spirált indít el, aminek a vége a bűnözés megnövekedésével, az érintett terület közbiztonságának jelentős csökkenéséhez vezet. A társadalmi bizalom megszerzésének megítélésem szerint egy nagyon fontos pontja, hogy az ilyen jellegű bűncselekményeket, mint egy Facebook, e-mail fiók feltörése is kivizsgáljanak a nyomozók.

A jogszabályalkotáshoz kapcsolódik megítélésem szerint a legjobb gyakorlat kidolgozása az OPSEC és INFOSEC területén. Jó alapot jelent erre a US Army által kiadott „Közösségi média kézikönyv" [246]. A Kézikönyv nem csupán az OPSEC és INFOSEC kapcsán fogalmaz meg az ajánlásokat, de a fegyveres erők pozitív percepcionálására vonatkozó kommunikációs tanácsokkal is foglalkozik, illetve iránymutatást nyújt a kríziskommunikáció közösségi médiában való folytatására. Alapul véve a Kézikönyvet, javaslatom szerint az alábbi területekre célszerű ajánlásokat megfogalmazni a Magyar Honvédség, Rendőrség esetében egyaránt:

- az állomány tagjának közösségi médiában való jelenléte. Ahogy a harmadik fejezetben már megfogalmaztam, nem javasolt az állományba tartozás tényét nyilvánosan közzétenni. Kivételt jelenthet ez alól az idézett ORFK utasításban megfogalmazott kitétel, amikor „*a szolgálati időn kívül végzett tudományos, oktatói, művészeti, lektori, szerkesztői, a jogi oltalom alá eső szellemi tevékenységével összefüggésben*" [161] nyilvánul meg. Fontos azt megérteni, a közösségi médiában való jelenlétünk az „én-marketing" szempontjából kiemelt jelentőségű. A hivatásos állomány tagjaként azonban nem csupán önmagunkat, de a szervezetünket is reprezentáljuk. Ebből következően magánemberként is olyan közösségi média jelenlétet kell folytatnunk, ami sem önmagunkra, sem a szervezetünkre nem hoz szégyent. Még ha nem is tesszük publikussá, hogy mivel foglalkozunk, hol dolgozunk, az ismerőseink tisztában lehetnek mindezzel, így nem jelent védettséget, ha az erről szóró információkat nem adjuk meg. Kerülni kell a közösségi oldalakon minden olyan cselekedet, amit egyébként a fizikai dimenzióban sem tennénk, például kerüljük mások zaklatását, ne osszunk meg szerzői jog alá eső tartalmat illegálisan stb. Kiemelten fontos, hogy milyen stílusban kommunikálunk, milyen tartalmakat osztunk meg, hiszen azok alapján ítélnek meg.
- A tartalommegosztás esetében különösen fontos, milyen információkat osztunk meg magunkról, és mindezt milyen mértékű nyilvánosság előtt. Kerülni kell minden olyan információt, ami harmadik fél számára megkönnyíti a profilozásunkat. Hangsúlyozottan érvényes ez az okos mobil eszköz használatra is, hiszen a telepített alkalmazások függvényében akaratlanul is olyan adatokat adhatunk ki magunkról harmadik félnek, amit felhasználhatnak ellenünk. Ha nem használjuk, minden esetben kapcsoljuk ki a geolokációs helymeghatározást, a Wi-Fi csatlakozást, a Bluetooth-t, hiszen ezek alapján számos adatot gyűjthetnek rólunk.

- A közösségi média népszerű terepe a csalóknak, akik azon keresztül próbálnak információkat vagy pénzt kicsalni. Ne jelöljünk vissza ismeretlen személyeket, ha valakit nem tudunk beazonosítani, kérdezzük meg, honnan ismerjük, ha vannak vele közös ismerőseink, érdeklődjünk náluk is. Fontos megérteni, a támadók akár családtagjainkat is felhasználhatják annak érdekében, hogy a bizalmunkba férkőzzenek vagy tőlük csaljanak ki olyan adatokat, amelyeket ellenünk használnának fel. Amennyiben azt tapasztaljuk, hogy bennünket vagy családtagunkat ilyen célból közelítettek meg, jelentsük az érintett hatóságnál.
- A Magyar Honvédség, ahogy a második fejezetben említettem, professzionális közösségi média jelenlétet épített ki, nem csak 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 média profilt találunk, amelyek mind az US Army népszerűsítét hivatottak ellátni (lásd 23. számú táblázat) [247]. Az egyes egységek mindegyik használja a Facebookot, de azon kívül egyéb platformokon is jelen vannak, mint 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.

23. táblázat US Army közösségi média jelenléte (saját szerkesztés, forrás: US Army [247])

Típus	**Egység száma**
Leaders	95
Installation	322
Active Duty Army Units	2591
Army Reserve Units	304
Army National Guard Units	353
Army Recruiting Commands	283
Family Matters	373
Joint	48
Other	1477
Összesen	***5846***

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. Erre nem csak a korábban említett példát lehet hozni, amikor a képek tartalmazták a geolokációs adatokat. A Nemzeti Közszolgálati Egyetem Karainak honlapján rendszeresen beszámolnak az egyetemi eseményekről, ami fontos dolog, úgy gondolom, de ezt nem minden esetben teszik körültekintően, találkozhattunk már olyan megosztott hírrel, ami a felderítő szakirányos hallgatók csapatgyakorlatáról számolt be, a hallgatókról készült csoportképpel illusztrálva, amin az arca minden hallgatónak kivehető volt. Vélelmezhetően nem csak az Egyetem munkatársai követik a honlapot, hanem idegen államok nemzetbiztonsági szolgálatainak munkatársai is, akiknek ezek az információk nem érdektelenek. Összehasonlítva a Magyar Honvédség és a Rendőrség Facebook jelenlétét, előbbi esetében közel 80 ezer kedvelőt láthatunk, míg a Rendőrség esetében ez a szám alig éri el az 1200-at, illetve a Honvédség Facebook oldalán naponta több bejegyzést találunk, addig a Rendőrség esetében az utolsó bejegyzés 2017 novembere.[104] Ha a szervezet nem fordít nagy gondot a közösségi médiában való jelenlétre, jószándékú amatőrök vagy csalók megteszik helyette, mindkettő igen komoly kockázatot jelentve. 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. A hivatalos profiloknak óriási szerep jut a kríziskommunikációban is, amelye egy rendkívüli esemény bekövetkezése esetén elengedhetetlen, hogy a közösségi oldalakat felhasználjuk.

Kapcsolódva a műveleti biztonság és információbiztonság kérdésköreihez, szintén javaslom olyan közösségi oldalak létrehozását, amelyek a biztonságtudatosság növelésének feladatait látják el. Ezzel kapcsolatban az amerikai fegyveres erők ismét példával szolgálnak, hiszen mind az Army [248], mind a Navy [249] esetében találunk olyan oldalakat, amelyek a műveleti biztonsággal kapcsolatos tudatosságnövelő kampányt folytatnak. Véleményem szerint

[104] A mintavétel ideje 2018. április 30.

a két oldal gyakorlata, amely nem csak az aktuális eseményekre hívja fel rendszeresen a figyelmet (például éppen terjedő zsarolóvírus kampány), 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 OPSEC és INFOSEC elérése nem csupán a jogi környezeten múlik, legalább olyan fontos, hogy az állományt rendszeresen képezzék ezzel kapcsolatban, aminek egyik aspektusát a közösségi médiában végzett kampányokkal lehet elérni, de ez megítélésem szerint csupán kiegészítése lehet a kialakított továbbképzési rendszernek. Ide tartozik a kulcsfontosságú vezetőkkel kapcsolatos tevékenységek végzése is. Ahogy a második fejezetben megfogalmaztam, e tevékenységek első sorban az információgyűjtésben és a személyek eszközhasználatának védelméhez kötődik. Annak függvényében, hogy milyen aspektusból foglalkozunk a kérdéssel, a hírszerzésért vagy elhárításért felelős szervezet hatáskörében kell gondoskodni a közösségi média és okos mobil eszköz használatának módjaival.

A műveleti biztonság és információbiztonság megteremtése míg egyik oldalról védelem körébe esik, addig a hírszerzés sikerességét növeli, ha az OPSEC és INFOSEC szintje alacsony. Ahogy az alfejezet elején már megfogalmaztam, a közösségi média hírszerzésben betöltött szerepét bár meghatározhatjuk, azt azonban nem lehet megállapítani, milyen képességeket építettek ki a katonai-, polgári- nemzetbiztonsági- vagy bűnüldöző szervezetek. Kenedli Tamás megállapítása szerint „*a hírszerző, felderítő szervezetek számára az OSINT tulajdonképpen egy adatszerző szervezet olyan távoli térségek esetében, ahol nem rendelkezünk egyéb adatszerző képességekkel, az egyetlen nemzeti adatszerző erő, amely azonnal és lényegében kockázatok nélkül képes az információgyűjtésre. Igaz ez egy válságkezeléssel érintett missziós terület vagy akár egy nemzetközi szinten működő bűnszervezet esetében is [181]*.” Nem véletlen tehát, hogy a nyílt forrású információszerzést az Információs Hivatal például a hírszerzés forrásai között nevesíti. Úgy vélem, az OSINT minden szervezet esetén megkerülhetetlen, akár katonai-, polgári nemzetbiztonsági vagy akár rendészeti vonalon.

Az elektronikai felderítés esetében értelemszerűen Magyarország nem rendelkezik olyan lehetőséggel, mint az amerikai partnerszolgálatok, hiszen nincs meg az az érdekérvényesítő képessége, amely hatására rá tudná venni a nagy közösségi oldalakat, hogy a PRISM-hez vagy az XKeyscorehoz hasonló megfigyelési képességet tudjon kiépíteni. Ennek ellenére a szolgálatok természetesen törekednek kormányzati kémprogramok beszerzésére. Erre vonatkozóan 2014-ben bizonyítékot szolgáltattak a Gamma nevet viselő cég birtokából kiszivárgott dokumentumok, hogy a Nemzetbiztonsági Szakszolgálat előfizetett a cég FinSpy

nevű kémprogramjára, de az olasz Hacking Team dokumentumainak nyilvánosságra kerüléséből azt is tudjuk, hogy 2008 óta az Információs Hivatal és a Nemzetbiztonsági Szakszolgálat is a megrendelőik között van [250]. A FinSpy képessége többek között weboldalak és szoftverek feltörésére, e-mailekhez való hozzáféréshez, VoIP hívások lehallgatására, személyek beazonosítására vonatkozott [251]. Feltételezhető, hogy az ilyen képességet, mint megrendelők, kiépítettek a hazai szolgálatok, ez pedig elképzelhetetlen, hogy a közösségi médiára ne vonatkozna.

A hírszerzés mellett a másik kiemelt terület a lélektani műveletekkel kapcsolatos tevékenység kell legyen. Ezzel kapcsolatban támadó és védekező képességet egyaránt fejleszteni szükséges. A politikai döntéshozatal befolyásolása, mint láthattuk, az álhírek terjesztésével rendkívül hatékony tud lenni. Magyarország Kormánya bizonyos témákban az érdekérvényesítő képességéhez viszonyítva sokkal hatékonyabban tud tematizálni, és akár világpolitikai tényezőként megjelenni. A Kormány törekszik arra, hogy politikájában az Európai Unió jövőjének egyik fontos alakítója legyen. Ezen vagy akár egyéb jellegű célok képviselete érdekében így akár európai, akár regionális szinten fontos, hogy Magyarország érdekeinek megfelelő üzenetek jelenjenek meg. Ahogy az álhírekkel foglalkozó alfejezetben bemutattam, ezt a képességet mind humán, mind robot felhasználók segítségével hatékonyan lehet növelni. A Magyar Honvédség szervezetén belül működő MH Civil-katonai Együttműködési és Lélektani Műveleti Központ egyik dedikált feladata a „*Magyar Honvédség alaprendeltetésével összhangban CIMIC-, illetve PSYOPS-műveletek végrehajtása hazai területen vagy külföldön.*” Véleményem szerint az álhírek terjesztésével kapcsolatos képesség kiépítését e szervezet hatáskörében célszerű elvégezni. Szintén a Központ hatáskörében javasolt az álhírek elleni elhárító képesség megteremtése. A közösségi média lélektani műveletekben betöltött szerepét az elmúlt években több ország felismerte, és kezelését katonai feladatok körébe sorolta. Nagy-Britannia 2015-ben például dandár szintű egységet hozott létre a közösségi médiából származó fenyegetések kezelésére [252]. A brit 77-es dandárhoz mérhető képességet értelemszerűen a Magyar Honvédség nem tud kiépíteni, hiszen a 77-es dandár a megalakításkor közel 1500 katonával kezdte meg a működését. A létrehozandó szervezeti egységnek a feladatai ily módon lélektani műveletek végzése, a Magyarország ellen folytatott műveletek elleni ellentevékenység végzése. Az álhírek ellen bár a közösségi oldalak is megpróbálnak fellépni, de az egyes országoknak is szükséges, kiépítsenek olyan képességeket, amelyekkel csökkentik hatásukat. Erre példa lehet az Európai Unió által üzemeltett „EU vs Disinformation” [253], ami a közösségi médiában terjedő álhíreket hivatott cáfolni, a cáfolatot

tényekkel alátámasztani. A Civil-katonai együttműködéshez kapcsolódó közösségi médiában végezhető tevékenységeket értelemszerűen szintén az MH Civil-katonai Együttműködési és Lélektani Műveleti Központ keretében célszerű erősíteni.

A várhatóan 2018 végén elfogadásra kerülő új Nemzeti Kiberbiztonsági Stratégia megfogalmazza a Magyar Honvédség kibertámadással kapcsolatos képességének kiépítését. Ennek a képességnek a kognitív dimenzióban való megjelenését az előző bekezdésben tárgyalt lélektani műveletekkel kapcsolatos feladatok jelentik, de a kibertérben kapcsolatos műveletek esetében is fontos szerepet tölt be a közösségi média. Az alfejezet elektronikai felderítésével kapcsolatban már említettem azokat a kormányzati kémprogramokat, amelyeknek nem csak a hírszerzésben, de egy kibertámadás előkészítésében is fontos szerepe lehet. A 2016-os amerikai elnökválasztás esetében a kiszivárgott e-maileket informatikai támadás során szerezték meg, és adták át a WikiLeaksnek, de ezen felül a támadók megkísérelték az elektronikus választási rendszerbe történő behatolást is [230]. Kritikus infrastruktúrák, hálózatok támadásában a közösségi média kártékony kódok terjesztésében, adathalászatban kiemelt jelentőségű.

Az eddigi feladatok szervezeti megoldásai többségében a Magyar Honvédséghez kapcsolódtak, azonban ahogy a bűnüldözéssel kapcsolatos alfejezetben bemutattam, a kiberbűnözés és közösségi média kapcsolata is jelentős. A szervezett bűnözéssel, terrorizmussal kapcsolatban jelentkező feladatok szempontjából alapvetően a bűnügyi felderítés hatáskörébe tartoznak, így a hírszerzéssel kapcsolatos részt nem tárgyalom újra.

A Rendőrség preventív jelleggel rendszeresen indít országos kampányokat különböző tevékenységekkel kapcsolatban, legyen szó ittas vezetésről, kábítószerhasználatról stb. A közösségi oldalak, ahogy korábban bemutattam, rendkívül hatékonyak üzenetek célba juttatásával. Gyakran éri az a kritika a Rendőrséget, hogy kampányai elavultak, nem kezeli megfelelően az egyes célcsoportokat. Ennek kiküszöbölésére a közösségi oldalak, elsősorban a Facebook, hiszen Magyarországon ezt a platformot használják a legtöbben, megoldást jelenthetnek. A kiberbűnözés esetében azonosított kockázatok, mint például kártékony kódok terjesztésével, pénzmosással, terrorizmus finanszírozással, adathalászattal, social engineeringel, de akár pedofilok jelenlétével kapcsolatban az egyes célcsoportokra optimalizáltan lehet tudatosító kampányokat folytatni. Nem nehéz belátni, az egyes korosztályok esetében más-más üzeneteket kell megfogalmazni a siker érdekében, és ahogy a CA botrány egyik tanulsága megmutatta, oly módon lehet közvetíteni az üzeneteket, hogy azok a lehető legnagyobb hatást fejtsék ki a felhasználók körében.

KÖVETKEZTETÉSEK

A közösségi média népszerűségéből és jellegéből fakadóan számos dologra használható. Erősíthetjük interperszonális interakcióinkat, részesei lehetünk társadalmi és politikai szerveződéseknek, hatékonyabban alkalmazhatjuk üzleti tevékenységeink támogatására. Mindez nem csak a civil tevékenységek végzésében jelentkezik, a honvédelmi-, rendvédelmi-, nemzetbiztonsági szervezetek esetében is azonosíthatunk olyan feladatokat, amelyek a közösségi média megfelelő használatával hatékonyabban láthatóak el. A fejezetben megvizsgáltam, hogyan használható a közösségi média a nemzetbiztonsági szolgálatok és a rendészeti szervek esetében, illetve milyen szerepet tölt be a politikai döntéshozatal befolyásolásában. A hírszerzés kapcsán megállapítottam, hogy a közösségi média több adatgyűjtő módszer esetében tekinthető relevánsnak, mint a nyílt forrású információgyűjtés vagy az elektronikai felderítés, de önmagában önálló adatgyűjtő módszerként is értelmezhető. Mindez azonban nem csupán a nemzetbiztonsági szervezetek esetében alkalmazható, a kiberbűnözők és terroristák is használják a közösségi médiát hírszerzésre. A kiberbűnözés kapcsán azonosítottam azokat a területeket, amelyek esetében a bűnüldözőknek reagálniuk szükséges. A politikai alrendszer vizsgálatával elemeztem a közösségi média választásokban, politikai döntéshozatalban betöltött szerepét. Megállapítottam, hogy a közösségi média ez irányú felhasználása nem csupán egy adott államra lehet hatással, azok globális következményekkel járhatnak. A politikai döntéshozatal befolyásolását nem csupán az adott állam politikai aktorai végezhetik, idegen államok nemzetbiztonsági szolgálatai is aktív szerepet játszhatnak a közösségi média felhasználásával. Mindezek figyelembevételével **azonosítottam a honvédelmi-, rendvédelmi-, nemzetbiztonsági szolgálatok törvényben meghatározott feladatainak ellátását támogató, a közösségi médiához kapcsolódó feladatainak rendszerét.** Ehhez kapcsolódóan megvizsgáltam a magyarországi katonai, nemzetbiztonsági és rendészeti szervezetek tekintetében, hogyan adaptálható a külföldi modellek alapján a közösségi média alkalmazása, amelyek alapján **javaslatot fogalmaztam meg közösségi médiához kapcsolódó feladatok szervezeti megoldásaira a Magyar Honvédségben, a nemzetbiztonsági szolgálatoknál, és a Rendőrségnél**.

ÖSSZEGZETT KÖVETKEZTETÉSEK

Értekezés tervezetemben a közösségi média védelmi szférában betöltött szerepét vizsgáltam. Tettem ezt abból a felismerésből, hogy relatíve rövid idő alatt a közösségi média használat megkerülhetetlenné vált nem csak a magánéletben, de a munkavégzésben is. A közösségi média az állandó innováció terepe, aminek hatására számos új funkcióval bővülnek az egyes oldalak. Az innováció egyben rendkívül erős kutatás-fejlesztésre is irányul, a Facebook vagy a Google többek között a mesterséges intelligencia, az autonóm közlekedési eszközök élen járó kutatói. Az oldalak népszerűsége, alkalmazási lehetőségei véleményem szerint a védelmi szféra szereplői számára is figyelemre méltóak.

Az első fejezetben megvizsgáltam a közösségi média fogalmát, megjelenését, illetve ismertettem néhány, témám szempontjából jelentősebb közösségi oldalt. Elemezve a használattal kapcsolatos trendeket, megerősítést nyert, hogy nem lehet figyelmen kívül hagyni a közösségi média nyújtotta alkalmazási lehetőségeket.

A Scopus és Scimago Journal Ranking adatbázisokat felhasználva megvizsgáltam, hogyan jelent meg a közösségi média a nemzetközi tudományos közleményekben, illetve leszűkítettem öt vizsgálati területre, a katonai, rendészeti, nemzetbiztonsági, kormányzati és politikai témájú kutatásokra. Kulcsszó elemzéssel megvizsgáltam, hogy a közösségi médiával kapcsolatos kutatások ezen az öt vizsgálati területen milyen tudományterületekhez köthetőek. **Megállapítottam, hogy a katonai és rendészeti kutatásokban alapvetően a műszaki tudományterület esetében jelentősebbek, a nemzetbiztonsági kutatások esetén közel azonos arányban tapasztalunk műszaki és társadalomtudományhoz kapcsolódó tudományos közleményeket, míg a politikai, kormányzati kutatásokban döntően a társadalomtudományi megközelítésből vizsgálják a közösségi médiát.** Megvizsgáltam továbbá a közösségi médiával kapcsolatos publikációk számának az alakulását, és **megállapítottam**, hogy egy relatíve **új kutatási szakterület.** A SciVal adatbázis segítségével elvégzett kataszterelemzés azt is igazolta, hogy a közösségi média, mint kutatási szakterület számos tudományterülethez kapcsolódik, amely között az általam elemzett öt vizsgálati terület is nagy számban fordult elő, ami alátámasztja a közösségi média védelmi szférával kapcsolatos kutatásait.

A második fejezetben megvizsgáltam a kibertérnek, mint hadszíntérnek a kialakulását, illetve a kiberbiztonsági stratégiák fejlődését nemzetközi és hazai környezetben. Tekintettel a közösségi média felhasználási területeire, az elemzett stratégiai dokumentumok alapján

megállapítottam, hogy a közösségi média értelmezhető az információs hadszíntér speciális területeként. Ez alapján **azonosítottam azokat az alkalmazási területeket, valamint eljárásokat, amelyek az információs hadszíntér részeként nevesíthetők**.

A harmadik fejezetben **megvizsgáltam az adat- és információbiztonság szerepét a kibertérben. Megállapítottam, hogy a közösségi média használat a magánszféra jelentős szűküléséhez** vezet azon eljárások okán, amelyek a felhasználók megfigyelését teszik lehetővé. Véleményem szerint egyértelműen **kijelenthető, az alacsony adat- és információbiztonsági tudatossággal rendelkező felhasználók kitettebbek a kibertér fenyegetettségeivel szemben**. Tekintettel arra, hogy a közösségi média használat milyen mértékben befolyásolja a magánszféránkat, bizton állíthatjuk, hogy **a megfelelő normatív szabályozás elengedhetetlen**. Ennek érdekében megvizsgáltam az adat- és információbiztonsággal összefüggő hazai jogszabályokat, kitérve a 2018 májusától hatályba lévő Európai Uniós irányelvekre. A magyarországi jogszabályok elemzésből megállapítottam, hogy a hazai normatív környezet kialakítása a 2010-es évek elejétől egyértelműen progresszívként nevesíthető, a döntéshozók az Európai Unió tagállamai között az elsők között voltak, akik felismerték a kibertér jelentette fenyegetéseket, és korszerű válaszokat fogalmaztak meg a stratégia és jogszabályalkotásban. A vonatkozó jogszabályok, mint az Ibtv., Infotv. vagy az Lrtv. egyértelműen a 2018 májusától hatályos európai irányelvek szabályozási irányába mutatnak. Ennek ellenére a közösségi média használattal kapcsolatos szabályozás nem ennyire egyértelmű. Vizsgálataim során **megállapítottam, hogy a közösségi médiára vonatkozó adatvédelmi tájékoztató ellentmondást tartalmaz**. A kibertámadások trendjeinek vizsgálata során **megállapítottam, hogy a védelmi szféra a támadók kiemelt célpontja**. Ez alapján megvizsgáltam a Magyar Honvédség és Rendőrség esetében azokat a nyilvánosan elérhető jogi szabályzókat, amelyek a közösségi média használatra vonatkoznak. Ezek értékelést követően **megállapítottam**, **hogy a Hjt. és Hszt. által megfogalmazott előírásokat a közösségi média nem megfelelő használata nagy mértékben sértheti**, azonban **nem készült olyan szabályozó, amely figyelembe véve ezeket megnyugtató módon rögzítené**. Tekintettel erre **javaslatot fogalmaztam meg a Magyar Honvédség és Rendőrség kapcsán a közösségi média használatára vonatkozó szabályozására**.

Úgy gondolom, a megfelelő **normatív szabályozás mellett legalább olyan fontos az oktatás**, amely növeli a digitális immunitást. Ennél fogva kérdőíves felmérést végeztem a Nemzeti Közszolgálati Egyetem hallgatói körében az adat- és információbiztonsági tudatosságukkal kapcsolatban. A kapott eredmények alapján **megállapítottam, hogy a**

hallgatók biztonságtudatossággal kapcsolatos önpercepciójukat több tényező is befolyásolja, amelyek közül az egyik, hogy korábban hallgattak-e adat- és információbiztonsággal kapcsolatos kurzusokat.

A negyed fejezetben megvizsgáltam, a katonai alkalmazáson kívül a védelmi szféra melyik területein alkalmazható a közösségi média. Ez alapján **azonosítottam azokat a területeket, amelyek a nemzetbiztonság és rendvédelem esetében jelentőséggel bírnak**. A vizsgálat területek alapján **megállapítottam** (beleértve a katonai alkalmazást is), **alapvetően a politikai célok megvalósítása érdekében alkalmazzák a közösségi médiát**. Ebből kiindulva megvizsgáltam a közösségi média politikai döntéshozatalban betöltött szerepét. **Megállapítottam, a nagy közösségi oldalak olyan mértékben képesek befolyásolni államok politikai döntéshozatalát, ami mindenképpen indokolttá teszi szabályozásukat.**

Tekintettel arra, hogy a **közösség média számos területen hatékonyan támogatja a honvédelmi-, rendvédelmi- és nemzetbiztonsági szolgálatok jogszabályban meghatározott feladatainak ellátását, javaslatokat fogalmaztam meg a közösségi médiához kapcsolódó feladatok szervezetei megoldásaira a Magyar Honvédség, a Rendőrség és nemzetbiztonsági szolgálatok esetében**.

ÚJ TUDOMÁNYOS EREDMÉNYEK

Tudományos eredményeim

T1. Igazoltam, hogy a közösségi média a humán- és műszaki tudományterület közös szakterülete, amely a hadtudományi kutatásokban dominánsan a műszaki tudományterülethez kapcsolódik.

T2. Meghatároztam a közösségi médiának, mint az információs hadszíntér speciális területének kereteit, eljárásait.

T3. Azonosítottam az adat- és információbiztonságra vonatkozó magyarországi normatív szabályozók közösségi média használattal kapcsolatos szabályozásra vonatkozó hiányosságait. Ezek alapján javaslatot fogalmaztam meg a közösségi média használattal kapcsolatos szabályozás honvédelmi-, rendvédelmi- és nemzetbiztonsági szempontú kialakítására.

T4. Bizonyítottam, hogy a biztonságtudatosságra vonatkozó önpercepciót befolyásolja a nem, a műszaki-humán érdeklődés, illetve, hogy korábban hallgatott-e a témában

kurzust. A kutatásom azonban cáfolta, hogy az iskolai végzettség és az eszköz használattal töltött idő befolyásolja a biztonságtudatosságra vonatkozó önpercepciót.

T5. Azonosítottam a honvédelmi-, rendvédelmi-, nemzetbiztonsági szolgálatok törvényben meghatározott feladatainak ellátását támogató, a közösségi médiához kapcsolódó feladatainak rendszerét. Mindezek alapján javaslatot fogalmaztam meg közösségi médiához kapcsolódó feladatok szervezeti megoldásaira a Magyar Honvédségben, a nemzetbiztonsági szolgálatoknál és a Rendőrségnél.

A KUTATÁSI EREDMÉNYEK GYAKORLATI FELHASZNÁLHATÓSÁGA

Értekezés tervezetemben megfogalmazott eredményeim alkalmasak arra, hogy:

- az adat- és információbiztonsággal kapcsolatos jelenleg érvényben levő szabályzókat kiegészítsék az általam javasolt szempontok alapján;
- az általam azonosított alkalmazási területeket integrálják a Magyar Honvédség, Rendőrség és nemzetbiztonsági szolgálatok szervezetébe a képességfejlesztése érdekében;
- a témával kapcsolatos további kutatások megalapozására;
- a Nemzeti Közszolgálati Egyetem hallgatóinak adat- és információbiztonsági tudatosságának növelésére az oktatásban.

AJÁNLÁSOK

Dolgozatomban a közösségi média védelmi szférában történő alkalmazását vizsgáltam, ily módon eredményeim felhasználását:

- elsődlegesen a Magyar Honvédség, a Rendőrség és a polgári-, katonai nemzetbiztonsági szolgálatok kiberbiztonsággal foglalkozó szakemberei számára;
- a Nemzeti Közszolgálati Egyetem adat- és információbiztonság tudatossággal kapcsolatos kurzusok fejlesztésében történő felhasználására;
- a témakörrel foglalkozó kutatók, oktatók részére;
- az adat- és információbiztonsággal kapcsolatos fejlesztési stratégiák kidolgozói, vezetői számára ajánlom.

TÉMAKÖRBŐL KÉSZÜLT PUBLIKÁCIÓIM

Könyvfejezet

1. A közösségi média szerepe a katasztrófaelhárításban a Sandy - hurrikán példáján keresztül, In: Horváth Attila (szerk.) Fejezetek a kritikus infrastruktúra védelemből: Kiemelten a közlekedési alrendszer. 319 p., Budapest: Magyar Hadtudományi Társaság, 2013. pp. 281-292., (ISBN:978-963-08-6926-3)
2. A közlekedést támogató alkalmazások biztonsági aspektusai, In: Horváth Attila-Bányász Péter (szerk.) Fejezetek a létfontosságú közlekedési rendszerelemek védelmének aktuális kérdéseiről. 152 p., Budapest: Nemzeti Közszolgálati Egyetem, 2014. pp. 47-60. (ISBN:978-615-5305-30-6)
3. Az ellátási lánc kiberfenyegetettsége, különös tekintettel a közlekedési alrendszer biztonságára, a szervezett bűnözés hatásai, In: Csengeri János, Krajnc Zoltán (szerk.), Humánvédelem - békeműveleti és veszélyhelyzet-kezelési eljárások fejlesztése. 791 p., Budapest: Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, 2016. pp. 643-673. (ISBN:978-615-5305-35-1)

Egyetemi jegyzet

1. Bányász Péter, Orbók Ákos: Bevezető az "okos" eszközök világába, In: Bányász Péter, Orbók Ákos (szerk.) Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára. (Nemzeti Közszolgálati Egyetem) Budapest: Nemzeti Közszolgálati Egyetem, 2016. pp. 5-31.
2. Az "okos" mobileszközök jelentett kiberbiztonsági kihívások, In: Bányász Péter, Orbók Ákos (szerk.) Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára. (Nemzeti Közszolgálati Egyetem), Budapest: Nemzeti Közszolgálati Egyetem, 2016. pp. 76-108.

Nemzetközi, vagy országos tudományos pályázaton elfogadott anyag (tanulmány)

1. Terroristák és terrorelhárítók a közösségi médiában, Technikai és technológiai fejlődés új kihívásai a terrorelhárításban, Terrorelhárítási Központ Tudományos Tanácsa által 2014. évben meghirdetett pályázata, első helyezés

Külföldi idegen nyelvű folyóiratban

1. How the social media may be used to paralyse the critical infrastructure? Economics and Management 2013:(4) pp. 7-14. (2013), ISSN 1802-3975

Külföldön idegen nyelvű konferenciakiadványban

1. Spies Act as a Spy: The Edward Snowden Case, In: Milan Sopóci, Mária Petrufová, Miroslav Školník, Viera Frianová, Jaroslav Nekoranec, Lubomír Belan Jirásková, Milota Kustrová, Stanislavmorong (szerk.), Manažment - teória, výučba a prax 2014: zborník príspevkov z medzinárodnej vedecko-odbornej konferencie. Liptovský Mikuláš. 380 p., 2014. pp. 194-201. (ISBN:978-80-8040-496-3)
2. The Role of the Cybersecurity in the Economy, In: Milan Sopóci, Lubomír Belan (szerk.) Manažment, teória, výučba a prax 2013: zborník z príspevkov z medzinárodnej vedecko-odbornej konferencie: 25. - 27. septembra 2013, Liptovský Mikuláš. 398 p. (ISBN:978-80-8040-477-2)

Magyarországon megjelenő idegen nyelvű folyóiratban

1. Dangers of social media through the example of the Arab Spring, Európai Szellem / European Spirit 4: pp. 20-32. (2013)

Magyar nyelvű mértékadó folyóiratban

1. Az okos mobil eszközök biztonsága, In. Hadmérnök 13:(2) pp. 360-377. (2018)
2. Social engineering és közösségi média, In. Nemzetbiztonsági Szemle 5: (1) pp. 59-77. (2018)
3. Kiberbűnözés és közösségi média, In. Nemzetbiztonsági Szemle 4:(4) pp. 55-74. (2017)
4. A közösségi média, mint az információs hadszíntér speciális tartománya, In. Hadmérnök, 12:(2) pp. 108-121. (2017)
5. A közösségi média szerepe a lélektani műveletekben az elmúlt időszak válságainak tükrében, In. Szakmai Szemle 13:(1) pp. 61-81. (2016)
6. A közösségi média, mint a nyílt forrású információszerzés fontos eleme, Nemzetbiztonsági Szemle, 2015/2, pp. 21-36. (2015) ISSN 2064-3756
7. Egy terrortámadás visszhangja a közösségi médiában, In. Belügyi Szemle (2010-) 63:(10) pp. 71-85. (2015)

8. A közösségi média használat biztonsági kérdései a védelmi iparban, Hadtudomány (Online) 24:(1) pp. 49-67. (2014), ISSN 1588-0605
9. Gondolatok Horváth L. Attila: A terrorizmus csapdájában című könyve kapcsán, Hadtudomány (Online) 24:(1) pp. 205-209. (2014) ISSN 1588-0605
10. Horváth L. Attila: A terrorizmus csapdájában, Sereg Szemle: A Magyar Honvédség Összhaderőnemi Parancsnokság Folyóirata XII:(3) pp. 159-161. (2014) ISSN 2060-3924
11. Bányász Péter- Orbók Ákos: A katonai logisztika időszerű kérdései, In. Hadtudomány 23:(1-2.) pp. 163-167. (2013) ISSN 1215-4121
12. Bányász Péter- Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, Hadtudomány (Online) XXIII:(1 elektronikus) pp. 188-209. (2013) ISSN 1588-0605
13. A közösségi média szerepe a települések életében, kiemelten a rendkívüli események kezelésében, Településföldrajzi Tanulmányok 2:(2) pp. 137-145. (2013) ISSN 2063-4315
14. A közösségi média szerepe a 21. század hadseregeiben, In. Hadtudomány 22:(1-2) pp. 152-161. (2012)
15. A tábori postaszolgálat szerepe a harctéri morál fenntartásában: A tábori postaszolgálatok története a XX. század első felében, In. Hadtudomány 22:(1) pp. 1-12. (2012)

Egyéb közlemények

1. A terrorizmus jelenléte a közösségi médiában, In: Bányász Péter, Kiss Dávid, Orbók Ákos (szerk.), Hadszíntér előkészítés, létfontosságú rendszerelemek védelme, honvédelmi érdekek érvényesítése: Poszterkiadvány, Budapest, Magyar Hadtudományi Társaság, 2015. p. 12. (ISBN:978-963-12-1507-6)
2. The Islamic State in the Social Media, In: Kiss Dávid, Orbók Ákos (szerk.), A haza szolgálatában 2014 konferencia rezümékötet. 170 p., 2014. p. 152. 1 p. (ISBN:978-615-5491--88-7)

FELHASZNÁLT IRODALOM

[1] Király László- Medveczky Mihály: Védelemgazdasági ismeretek önkormányzati válságmenedzserek (védelmi igazgatási referensek) számára, Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2009. 197 p

[2] Szenes Zoltán: A védelempolitika fogalma, tartalma és határai, In. Nemzet És Biztonság: Biztonságpolitikai Szemle 1:(2) pp. 27-34. (2008)

[3] Haig Zsolt- Kovács László: Kritikus infrastruktúrák és kritikus információs infrastruktúrák, Budapest: Nemzeti Közszolgálati Egyetem, 2012. 298 p.

[4] Török Szilárd: Szemüveggel a biztonságért In. Hadmérnök, IX. /1. szám, 2014., pp. 264-276.,

[5] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

[6] Tájékoztató eljárás eredménytelenségéről, Közbeszerzési Hatóság, 2015/63, 2015. június 5., 9487/2015, http://kozbeszerzes.hu/ertesito/megtekint/portal_9487_2015/ (2015. június 23.)

[7] Loell, Keith: Did Sir Isaac Newton Invent Social Media? In. Forbes, 2013. április 18., http://www.forbes.com/sites/gyro/2013/04/18/did-sir-isaac-newton-invent-social-media/ (2018. március 23.)

[8] The Royal Society of London for Improving Natural Knowledge, https://royalsociety.org/

[9] Cohen, Heidi: Social Media Definitions, In. Heidi Cohen, 2011. május 9., http://heidicohen.com/social-media-definition/ (2018. március 23.)

[10] Definition of social media in English, In. Oxford Dictionaries, http://www.oxforddictionaries.com/definition/english/social-media (2018. március 23.)

[11] Kaplan, Andreas- Haenlein, Michael: Users of the world, unite! The challenges and opportunities of Social Media, Business Horizons, 2010. http://doi.org/10.1016/j.bushor.2009.09.003

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

[13] Pléh et al: Pszichológiai lexikon, Budapest, Akadémiai Kiadó, 2008. Személyiségtípusok 276. p.

[14] Davis, F.D.: Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 1989., p. 319–339.

[15] 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

[16] Bourdieu, Pierre: Gazdasági tőke, kulturális tőke, társadalmi tőke. In: Angelusz Róbert (szerk.), A társadalmi rétegződés komponense, Budapest, Új Mandátum Könyvkiadó, 1999., 156-177.

[17] Tajfel, Henry- Social identity and intergroup behaviour, In. Social Science Information, Vol. 13, No. 2, 1974., pp. 65-93.

[18] Munk Veronika: Sztárság, elméletben, Médiakutató 2009 tavasz, http://www.mediakutato.hu/cikk/2009_01_tavasz/01_sztarsag_elmeletben

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

[20] Sasvári Péter- Urbanovics Anna: Kutatói közösségi hálózatok használata a Nemzeti Közszolgálati Egyetemen, In. Államtudományi Műhelytanulmányok, 2018:(9) pp. 1-14.

[21] Marosán György: Mém elmélet – a posztmodern szintézis alapvonalai, Gondolatok, vázlatok, http://marosan.hu/gondol/mem-elmelet.doc (2018. március 23)

[22] Kiss Tibor- Parti Katalin: A mém vajon mi? Mémekért való felelősség megállapíthatóságának kérdései és lehetőségei, In. Infokommunikáció és Jog 2016/2:(66-67) pp. 39-47. (2017)

[23] Facebook Reports Fourth Quarter and Full Year 2017 Results, In. Facebook Investor Relations, 2018. január 31., https://s21.q4cdn.com/399680738/files/doc_financials/2017/Q4/Q4-2017-Press-Release.pdf (2018. március 16.)

[24] Index: Leleplezték a Wikipedia legnagyobb átverését, In. Index, 2013. május 5., http://index.hu/tech/2013/05/01/lelepleztek_a_wikipedia_legnagyobb_atvereset/ (2018. március 23.)

[25] Berki Gábor: A kibertéri konfliktusok változása, In. Hadmérnök, VIII/1. szám, pp. 173-185., 2013.

[26] Tinder Information, Statistics, Facts and History, In.Dating Sites Reviews, https://www.datingsitesreviews.com/staticpages/index.php?page=Tinder-Statistics-Facts-History (2018. március 16.)

[27] About Tumblr, https://www.tumblr.com/about (2018 március 16.)

[28] Kemp, Simon: Global Digital Report 2018., We are social, 2015. január 21., https://digitalreport.wearesocial.com/ (2018. március 17.)
[29] Európa digitális fejlődéséről szóló jelentés (EDPR), 2017 – Országprofil Magyarországról, In. Európai Bizottság, https://ec.europa.eu/digital-single-market/en/scoreboard/hungary (2018. március 17.)
[30] Social media - Statistics & Facts, In. Statista, https://www.statista.com/topics/1164/social-networks/
[31] Digital Market Intelligence & Website Traffic, In. Similar Web, https://www.similarweb.com/
[32] Kemp, Simon: Digital in Eastern Europe, In. We are social, 2018. január 29., https://www.slideshare.net/wearesocial/digital-in-2018-in-eastern-europe-part-2-east-86865266 (2018. március 17.)
[33] NMHH: Lakossági internethasználat- Online piackutatás 2016., Ariosz Kft., NRC Kft., In. Nemzeti Média- és Hírközlő Hatóság, http://nmhh.hu/dokumentum/187704/lakossagi_internethasznalat_2016.pdf (2018. március 17.)
[34] Bauer et. al.: Ezek a mai fiatalok! Magyar ifjúságkutatás 2016., Új Nemzedék Központ Nonprofit Kft, 2017.
[35] Scopus, In. www.scopus.com
[36] Scimago Journal and Country Ranks, In. http://www.scimagojr.com/journalrank.php
[37] SciVal Suite, In. https://www.scival.com/
[38] 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.
[39] Mészáros Rezső: A kibertér társadalomföldrajzi megközelítése, In. Magyar Tudomány, 2001/7., 2001., pp. 769-779.
[40] Jakobi Ákos: A virtuális világ terei- Reflexiók Mészáros Rezső „A kibertér társadalomföldrajzi megközelítése” című tanulmányához, In. Magyar Tudomány, 2002/11., 2002., pp. 1482-1491.
[41] Rajnai Zoltán- Fregan Beatrix: Új alapokon a magyarországi kibervédelmi stratégia, In. Műszaki Tudományos Közlemények, 2017, pp. 351-354.
[42] 1139/2013, (III. 21.) Korm. határozat Magyarország Nemzet Kiberbiztonsági stratégiájáról, In. Magyar Közlöny, 2013/47.

[43] 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról, In. Honvédelmi Közlöny, CXL évfolyam 10. szám, 2013.
[44] Haig Zsolt: Információ- Társadalom- Biztonság, NKE Szolgáltató Kft., Budapest, 2015.
[45] Munk Sándor: A kibertér fogalmának egyes, az egységes értelmezést biztosító kérdései, In. Hadtudomány, 28:(1), 2018., pp. 113-131.
[46] Varga Gergely: A NATO új, lisszaboni stratégiai koncepciója, In. Nemzet és Biztonság, 2010/10, 2010., pp. 79-86.
[47] Babos Tibor: „Globális közös terek" a NATO-ban, In. Nemzet és Biztonság, 2011/3.,2011., pp. 34-46.
[48] Barett et. al.: Assured Access to the Global Commons, Supreme Allied Command Transformation, North Atlantic Treaty Organization, Norfolk, Virgina USA, April 2011.
[49] Alatalu, Siim.: NATO's new cyber domain challenge, In. 2016 IEEE International Conference on Cyber Conflict, CyCon U.S. 2016, http://doi.ieeecomputersociety.org/10.1109/CYCONUS.2016.7836609
[50] Tumkevič, A: Uncertain security community: Building western cybersecurity order, In. European Conference on Information Warfare and Security, ECCWS, 2017., pp. 497-504.
]51] Joint Publication 3-13, Information Operations, 27 november 2012 by United States Government
US Army, p. I-1.m
[52] Haig et. al.: Elektronikai hadviselés (szerk. Németh András), Nemzeti Közszolgálati Egyetem, Budapest, 2014.
[53] Haig Zsolt- Várhegyi István: Hadviselés az információs hadszíntéren, Zrínyi Kiadó, Budapest, 2005.
[54] AJP-3.10 Allied Joint Doctrine for Information Operation, 2009., https://info.publicintelligence.net/NATO-IO.pdf (2018. március 18.)
[55] Szentgáli Gergely: A NATO kibervédelmi politikájának fejlődése, In. Bolyai Szemle, XXI/2., 2012., pp. 79-94.
[56] Bányász Péter- Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében, In. Hadtudomány online, XXII évfolyam, 2013/1. elektronikus lapszám, 2013., pp. 188-209.
[57] Bucharest Summit Declaration, In. NATO Press Relaese, 2008. április 3., http://www.nato.int/cps/en/natolive/official_texts_8443.htm?selectedLocale=en (2018. március 11.)

[58] Cyber Defence Management Authority, In. Nemzeti Biztonsági Felügyelet, http://nbf.hu/cdmaoszt.html (2018. március 11.).
[59] Wales Summit Declaration, In. NATO Press Release, Issued on 05 Sep. 2014., https://www.nato.int/cps/ic/natohq/official_texts_112964.htm (2018. március 14.)
[60] Szenes Zoltán: Új bor a régi palackban? A walesi NATO csúcs, In. Hadtudomány, 2014/3-4, 2014., pp. 3-21.
[61] Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, In. NATO Press Release, Issued on 08 Jul. 2016., https://www.nato.int/cps/ic/natohq/official_texts_133163.htm (2018. április 8.)
[62] MacKenzie, Paul J.: NATO Joint Air Power and Offensive Cyber Operations, The Joint Air Power Competence Centre, November 2017., https://www.japcc.org/wp-content/uploads/JAPCC_OCO_screen.pdf
[63] Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers, In. NATO, 2017. november 8., https://www.nato.int/cps/en/natohq/opinions_148417.htm (2018. április 8.)
[64] Tallinn Manual on the International Law Applicable to Cyber Warfare, Cambridge University Press, 2013.
[65] Pipyros et. al.: A new strategy for improving cyber-attacks evaluation in the context of Tallinn Manual, In. Computers & Security, Volume 74, May 2018, pp. 371-383., https://doi.org/10.1016/j.cose.2017.04.007
[66] Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations, Cambridge University Press, 2017.
[67] Liu, Ian Yuying: The due diligence doctrine under Tallinn Manual 2.0, In. Computer Law & Security Review, Volume 33, Issue 3, June 2017, pp. 390-395., https://doi.org/10.1016/j.clsr.2017.03.023
[68] Európa 2020- Az intelligens, fenntartható és inkluzív növekedés stratégiája, Brüsszel, 2010., http://ec.europa.eu/eu2020/pdf/1_HU_ACT_part1_v1.pdf (2018. április 15.)
[69] Európai Digitális Menetrend 2010-2020: A Bizottság akcióterve az európai jólét fellendítésére. Brüsszel, 2010.
http://infoter.eu/attachment/0003/2807_com2010_0245hu01.pdf (2018. április 15.)

[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
[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] Munk Sándor: Kiberbiztonsági célok, jövőképek, szabályozók az EU-ban és kapcsolatrendszerük az interoperabilitással, In. Hadmérnök XIII. :(K1), 2018., pp. 205-217.
[73] Közös közlemény az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának Az Európai Unió kiberbiztonsági stratégiája: Nyílt, megbízható és biztonságos kibertér /* JOIN/2013/01 final */, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52013JC0001&from=HU (2018. április 15.)
[74] Klimburg, Alexander (szerk.): National Cyber Security Framework Manual, 2012., https://ccdcoe.org/multimedia/national-cyber-security-framework-manual.html (2018. április 8.)
[75] Wamala, Frederick: The ITU National Cybersecurity Strategy Guide, 2011., http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf (2017. július 8.).
[76] Liveri, Dimetria -Sarri, Anna: An evaluation Framework for National Cyber Security Strategies, 2014. https://www.enisa.europa.eu/publications/an-evaluation-framework-for-cyber-security-strategies (2017. július 8.).
[77] GCI 2017, In. ITU, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI-2017.aspx (2018. március 14.)
[78] GCI Interactive Comparison Tool, In. ITU, http://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI_GLO_Graphics.aspx (2018. március 14.)
[79] 2011. évi CXII. törvény az információs önrendelkezési jogról és információszabadságról, https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (2018. április 8.)
[80] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről, https://net.jogtar.hu/jogszabaly?docid=a1200166.tv (2018. április 8)

[81] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról, http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158 (2018. április 8)
[82] Beláz Annamária: A magyar kibervédelmi szabályozás továbbfejlesztésének lehetőségei- Különös tekintettel a stratégiaalkotásra, Diplomamunka, Nemzeti Közszolgálati Egyetem, 2017
[83] 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
[84] Open Letter From Jana Partners And Calstrs To Apple Inc., In. Think Differently about Kids, 2018. január 6., https://thinkdifferentlyaboutkids.com/index.php?acc=1 (2018. február 10.)
[85] Gao et. al.: Neuroticism and quality of life: Multiple mediating effects of smartphone addiction and depression, In. Psychiatry Research, Volume 258, December 2017., pp. 457-461., http://doi.org/ 10.1016/j.psychres.2017.08.074
[86] Casale, Silvia- Fioravanti, Giulia: Why narcissists are at risk for developing Facebook addiction: The need to be admired and the need to belong, In. Addictive Behaviors, Volume 76, January 2018, pp. 312-318., https://doi.org/10.1016/j.addbeh.2017.08.038
[87] Wolniewicz et. al.: Problematic smartphone use and relations with negative affect, fear of missing out, and fear of negative and positive evaluation, In. Psychiatry Research
Volume 262, April 2018, pp. 618-623, https://doi.org/10.1016/j.psychres.2017.09.058
[88] Oberst et. al.: Negative consequences from heavy social networking in adolescents: The mediating role of fear of missing out, In. Journal of Adolescence, Volume 55, February 2017, pp. 51-60., https://doi.org/10.1016/j.adolescence.2016.12.008
[89] Cruz-Jesus et. al.: The education-related digital divide: An analysis for the EU-28, In. Computers in Human Behavior, Volume 56, March 2016, pp. 72-82., http://dx.doi.org/10.1016/j.chb.2015.11.027
[90] Leaning, Marcus: Digital Divides: Access, Skills and Participation, In. Media and Information Literacy- An Integrated Approach for the 21st Century, 2017, pp. 101–114.
[91] Parsons, Talcott: Theoretical Orientations, In. The system of modern societies, Englewood Cliffs, New Jersey, Prentice-Hall, 1971.
[92] Pix Gábor: A lélektani műveletek jellemzőinek vizsgálata, Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest, 2005.
[93] Ált/57, Információs műveletek doktrína, MH DOFT kód: MD 3.10 (1), 2014. augusztus 5., p. 1-15.

[94] AJP-3.7. NATO Military Policy on Psychological Operations, 2003., https://info.publicintelligence.net/NATO-PSYOPS-Policy-2003.pdf (2018. március 19.)
[95] Miller, David: Sociology, Propaganda and Psychological Operations, In. Stretching the Sociological Imagination, Palgrave Macmillan, London, 2015., pp. 163-188.
[96] Briant, Emma L.: Pentagon Ju-Jitsu – reshaping the field of propaganda, In. Critical Sociology, 1 March 2018., pp. 1.18., https://doi.org/10.1177/0896920517750741
[97] Dudatyev, A.V: Complex method of informational-psychological operations counteraction, In. Journal of Automation and Information Sciences
Volume 49, Issue 1, 2017., pp. 76-83., http://dx.doi.org/10.1615/JAutomatInfScien.v49.i1.70
[98] Traylor et.al.: PSYOP, deception, and cyberspace in the open: Analysing fake news in a cyber new normal communications environment, In. European Conference on Information Warfare and Security, ECCWS, 2017., pp. 488-496.
[99] Jones, Jefferey B: Strategic Communications: Amandateforthe United States.Joint Forces Quarterly, (39), 2007., pp. 108-114.
[100] Németh József Lajos: A (stratégiai) kommunikáció és a háború kapcsolata napjainkban, In. Hadtudomány, XXIII/1-2. szám, 2013., pp. 129-139.
[101] Andress, Jason: Operations Security, In. The Basics of Information Security-Understanding the Fundamentals of InfoSec in Theory and Practice, 2011., pp. 81–95.
[102] Muha et. al.: Az informatikai biztonság kézikönyve (szerk. Szenes Katalin), Verlag Dashöfer, Budapest, 2007.
[103] MTI: Izrael lefújt egy katonai akciót a Facebook miatt, In. Metropol, 2010. március 3., http://www.metropol.hu/cikk/535056 (2018. március 19.).
[104] Rodewig, Cherryl: Geotagging poses security risks, In. Army.mil, 2012. március 7., http://www.army.mil/article/75165/Geotagging_poses_security_risks/ (2018. március 19.)
[105] Munk Sándor: Információbiztonság vs. informatikai biztonság, Hadmérnök, 2007/különszám,
[106] Adatokat eltulajdonító androidos zseblámpa alkalmazás, In. GovCERT, 2013. december 6., http://tech.cert-hungary.hu/tech-blog/131206/adatokat-eltulajdonito-androidos-zseblampa-alkalmazas (2018. április 21.)
[107] Resperger István: A „diadal” és egyéb módszerek alkalmazása a nemzeti válságkezelési feladatok megoldásánál, In. Hadtudományi Szemle, 5. évfolyam 1-2. szám, pp. 141-165., 2012., http://archiv.uni-

nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2012/2012_1/2012_1_br_resperger_istvan_141_165.pdf
[108] Kovács Zoltán: Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára, In. Hadmérnök, IX/3. szám, 2014., pp. 182-190.
[109] Andress, Jason- Winterfeld, Steve: Cyber Warfare (Second Edition), Techniques, Tactics and Tools for Security Practitioners, Elsevier Inc., 2014.
[110] AJP-3.4.9 Allied Joint Doctrine for Civil-Military Cooperation, 2013., https://www.cimic-coe.org/wp-content/uploads/2014/06/AJP-3.4.9-EDA-V1-E1.pdf
[111] Ankeresen, Christopher (editor): Civil-Military Cooperation in Post-Conflict Operations: Emerging Theory and Pratice, Routledge, New York, 2007.
[112] Ball et.al.: The Surveillance Industrial Complex: Towards a Political Economy of Surveillance, Routledge, New York, 2013.
[113] Guo. et. al.: DPI & DFI: A Malicious Behavior Detection Method Combining Deep Packet Inspection and Deep Flow Inspection, In Procedia Engineering, Volume 174, 2017, pp. 1309-1314., https://doi.org/ 10.1016/j.proeng.2017.01.276
[114] Esposti et.al.: Aligning security and privacy: The case of deep packet inspection. In: Čas, J, Bellanova, R, Burgess, JP, Friedewald, M, Peissl, W (eds) Surveillance, Privacy and Security: Citizens' Perspectives. London: Routledge, 2017., pp. 71–90.
[115] Antonello et. al.: Deep packet inspection tools and techniques in commodity platforms: Challenges and trends, In. Journal of Network and Computer Applications
Volume 35, Issue 6, November 2012., pp. 1863-1878., https://doi.org/ 10.1016/j.jnca.2012.07.010
[116] Davenport T.H. - Prusak, L.: Tudásmenedzsment, Kossuth Kiadó, 2001.
[117] Chen, Ben: Systems and Methods for Utilizing Wireless Communications to Suggest Connections for a User, In. US Patent and Trade Mark Office- Patent Application Full Text an Image Database, United States Patent Application 20160014677, Kind Code A1, 2016. január 14.,
[118] Halassy Béla: Az adatbázis tervezés alapjai és titkai- Avagy az út az adattól az adatbázison át az információig, Budapest, IDG Hungary, cop. 1994.
[119] Chen et. al.: Big Data: A Survey, In. Mobile Networks and Applications, April 2014, Volume 19, Issue 2, pp. 71–209., http://dx.doi.org/10.1007/s11036-013-0489-0

[120] Chen et. al.: Business Intelligence And Analytics: From Big Data To Big Impact, In. MIS Quarterly Vol. 36 No. 4, December 2012., pp. 1165-1188.
[121] Rajnai Zoltán- Nyikes Zoltán: A Big Data alkalmazása a nemzeti digitális közműben, In. Szakmai Szemle, 2015:(4) pp. 103-118.
[122] Taigman, Yaniv: DeepFace: Closing the Gap to Human-Level Performance in Face Verification, In. Facebook Research, 2014. június 24., https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/ (2018. április 16.)
[123] United States District Court Northern District Of California: Acebook Biometric Information Privacy Litigation, Case 3:15-cv-03747-JD Document 333 Filed 04/16/18 Page 1 of 15, https://assets.documentcloud.org/documents/4438920/Donato-Fb-Class.pdf (2018. április 21.)
[124] The Guardian: The Cambridge Analytica Files, In. The Guardian, https://www.theguardian.com/news/series/cambridge-analytica-files (2018. április 21.)
[125] Collateral damage of Facebook third-party applications: a comprehensive study, In. Computers & Security, In. Volume 77, August 2018., pp. 179-208.
[126] K.Á.: A fél világról gyűjthetett törvénytelenül adatokat a Facebook, In. Index, 2018. április 17., https://index.hu/tech/2018/04/17/a_fel_vilagrol_torvenytelen_adatokat_gyujthetett_a_facebook/ (2018. április 21.)
[127] Norman, Warren T.: Toward an adequate taxonomy of personality attributes: Replicated factor structure, In peer nomination personality ratings". Journal of Abnormal and Social Psychology. 66 (6), 1963., pp. 574–583.
[128] He et. al.: Predicting self-monitoring skills using textual posts on Facebook, In. Computers in Human Behavior, Volume 33, April 2014., pp. 69-78., https://doi.org/10.1016/j.chb.2013.12.026
[129] Eşkisu et. al.: An investigation of the relationship between Facebook usage, Big Five, self-esteem and narcissism, In. Computers in Human Behavior, Volume 69, April 2017., pp. 294-301., http://dx.doi.org/10.1016/j.chb.2016.12.036
[130] Azucar et. al.: Predicting the Big 5 personality traits from digital footprints on social media: A meta-analysis, In. Personality and Individual Differences, Volume 124, 1 April 2018., pp. 150-159., https://doi.org/10.1016/j.paid.2017.12.018

[131] Brandom, Russel: Shadow profiles are the biggest flaw in Facebook's privacy defense, In. The Verge, 2018. április 11., https://www.theverge.com/2018/4/11/17225482/facebook-shadow-profiles-zuckerberg-congress-data-privacy (2018. április 21.)
[132] Warren, Tom: Facebook has been collecting call history and SMS data from Android devices, In. The Verge, 2018. március 25., https://www.theverge.com/2018/3/25/17160944/facebook-call-history-sms-data-collection-android (2018. április 21.)
[133] Bodó Attila Pál: Biztonsági eseménykezeléssel kapcsolatos elvárások a hazai és a nemzetközi jogban, In. Incidensmenedzsment- Éves továbbképzés az elektronikus információs rendszer biztonságával összefüggő feladatok ellátásában részt vevő személy számára 2017, Dialóg Campus Kiadó, Budapest, 2017.
[134] Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban. Hadmérnök, VII/4. szám, pp. 142-151., 2012.
[135] Moskowitz, Sanford L.- The Global Cybercrime Industry, In. Cybercrime and Business, Strategies for Global Corporate Security, 2017., pp. 3–22.
[136] Luiijf, Eric: Definitions of Cyber Terrorism, In. Cyber Crime and Cyber Terrorism Investigator's Handbook, 2014., pp. 11–17.
[137] 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. március 18.).
[138] Caldwell, Tracey: Hacktivism goes hardcore, In. Network Security, Volume 2015, Issue 5, May 2015., pp. 12-17., http://dx.doi.org/10.1016/S1353-4858(15)30039-8
[139] Information Security Timelines and Statistics, In. Hackmageddon, https://www.hackmageddon.com/category/security/cyber-attacks-statistics/ (2018. április 22.)
[140] Rajnai Zoltán: Információbiztonsági tudatosság, In. Műszaki Tudományos Közlemények, 2017., pp. 37-42.
[141] Magyarország Alaptörvénye, Szabadság és Felelősség VI. cikk (1-3) bekezdés
[142] 2013. évi V. törvény a Polgári Törvénykönyvről, https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300005.TV (2018. március 11.)
[143] 2012. évi C. törvény a Büntető Törvénykönyvről, https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV (2018. március 11.)

[144] 2009. évi CLV. törvény a minősített adat védelméről, https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0900155.tv (2018. március 11.)
[145] Ballinger et. al.: DeepHeart: Semi-Supervised Sequence Learning for Cardiovascular Risk Prediction, In. Thirty-Second AAAI Conference on Artificial Intelligence, New Orleans, February 2018.
[146] 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), http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=HU (2018. április 12.)
[147] Az Európai Parlament és a Tanács a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló 95/46/EK irányelve, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:31995L0046&from=HU (2018. április 12.)
[148] 2018. évi XXXVIII. törvény az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvénynek az Európai Unió adatvédelmi reformjával összefüggő módosításáról, valamint más kapcsolódó törvények módosításáról
[149] Halász et al.: Az Infotv. változásai a GDPR-ra tekintettel történt módosítást követően, In. Twibirdsideas, 2018. július 31., https://twobirdsideas.hu/wp-content/uploads/2018/09/Infotv-GDPR-modositas-BirdBird-2018-07-31.pdf (2018. szeptember 15.)
[150] 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 (2018. április 20.)
[151] 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.
[152] Székely Iván: Privátszférát erősítő technológiák. Információs Társadalom, 8. évf. 1. sz., 2008., pp. 20–34.
[153] 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

[154] 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), https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:52017PC0010 (2018. április 29.)
[155] Az Európai Parlament és a Tanács a hálózati és információs rendszereknek az egész unióban egységesen magas szintjét biztosító intézkedésekről szóló 2016/1148 irányelve, https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016L1148&from=HU (2018. április 22.)
[156] 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. április 22.)
[157] 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
[158] 2012. évi CCV. törvény a honvédek jogállásáról, https://net.jogtar.hu/jogszabaly?docid=A1200205.TV
[159] 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
[160] 2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról, https://net.jogtar.hu/jogszabaly?docid=A1500042.TV
[161] 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
[162] Heaven, Douglas: The internet knows you all too well, In. New Scientist, Volume 237, Issue 3168, March 2018., pp. 42-43., https://doi.org/10.1016/S0262-4079(18)30444-5
[163] Hern, Alex: Fitness tracking app Strava gives away location of secret US army bases, In. 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. április 27.)

[164] Heffernan, Michael: The interrogation of Sándor Radó: geography, communism and espionage between World War Two and the Cold War, In. Journal of Historical Geography Volume 47, January 2015, pp.74-88., http://dx.doi.org/10.1016/j.jhg.2014.12.004
[165] Jang-Jaccard, Julian- Nepal, Surya: A survey of emerging threats in cybersecurity, In. Journal of Computer and System Sciences, Volume 80, Issue 5, August 2014, pp. 973-993., https://doi.org/10.1016/j.jcss.2014.02.005
[166] He, Wu: A survey of security risks of mobile social media through blog mining and an extensive literature search, In. Information Management & Computer Security Vol. 21 No. 5, 2013., pp. 381-400., https://doi.org /10.1108/IMCS-12-2012-0068
[167] Fokes, Elizabeth- Li, Lei: A Survey of Security Vulnerabilities in Social Networking Media – The Case of Facebook, In. Proceedings of the 3rd annual conference on Research in information technology, Atlanta, USA, 2014., pp. 57-62.
[168] Imgraben et. al.: Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users, In. Behaviour & Information Technology, Vol. 33, No. 12, 2014., pp. 1347–1360., http://dx.doi.org/10.1080/0144929X.2014.934286
[169] Stanton et. al.: Analysis of end user security behaviors, In. Computers & Security, Volume 24, Issue 2, March 2005., pp. 124-133., https://doi.org/1016/j.cose.2004.07.001
[170] Parsons et. al.: Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), In. Computers & Security, Volume 42, May 2014, pp. 165-176., http://dx.doi.org/10.1016/j.cose.2013.12.003
[171] Das et. al.: Increasing Security Sensitivity With Social Proof: A Large-Scale Experimental Confirmation, In. ACM Conference on Computer and Communications Security, Scottsdale, USA, 2014.
[172] Oehri, Caroline- Teufel, Stephanie: Social Media Security Culture- The Human Dimension in Social Media Management, In. Information Security for South Africa (ISSA), 2012.
[173] Parsons et. al.: The Human Aspects of Information Security Questionnaire (HAIS-Q): Two further validation studies, In. Computers & Security, Volume 66, May 2017, pp. 40-51., http://dx.doi.org/10.1016/j.cose.2017.01.004
[174] Sajtos László- Mitev Ariel: SPSS kutatási és adatelemzési kézikönyv, Alinea Kiadó, Budapest, 2007.
[175] Kis-Benedek József: A nemzetbiztonsági szolgálatok együttműködése, Hadtudomány, XXIII:(1-2) pp. 100-114., 2013.

[176] Izsa Jenő: A hírszerzés céljáról és rendszeréről. Hadtudomány, 2009/1-2.
[177] Béres János: A hírszerzés feladatrendszere, In. A nemzetbiztonság általános elmélete. 363 p., Nemzeti Közszolgálati Egyetem, Budapest, 2014., pp. 117-128.
[178] Ádám László: Az elhárítás feladatrendszere, In. In. A nemzetbiztonság általános elmélete. 363 p., Nemzeti Közszolgálati Egyetem, Budapest, 2014., pp. 129-145.
[179] Rolington, Alfred: Hírszerzés a 21. században- A mozaik módszer, Antall József Tudásközpont, Budapest, 2015.,
[180] Kis-Benedek József: Az emberi erőkkel folytatott információszerzés: HUMINT - Human Intelligence, In. A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Budapest, 2014., pp. 153-163.
[181] Kenedli, Tamás: A nyílt forrású információszerzés, In. A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Budapest, 2014., pp. 169-178.
[182] Lévay, Gábor: OSINT (Open Source Intelligence) – Nyílt információs hírszerzés. ZMNE, Egyetemi jegyzet, Budapest, 2006. p. 6.
[183] Ferenczy, Gábor: Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása, PhD értekezés, ZMNE, p. 17.
[184] Mestyán et. al.: Early Prediction of Movie Box Office Success Based on Wikipedia Activity Big Data, In. PLOS One, 2013. augusztus 21., https://doi.org/10.1371/journal.pone.0071226
]185] Dobák Imre: Elektronikai eszközökkel végzett felderítés, In. A nemzetbiztonság általános elmélete (szerk. Dobák Imre), Nemzeti Közszolgálati Egyetem, Budapest, 2014.
[186] Greenwald: Glen: A Snowden-ügy, HVG Kiadó Zrt., Budapest, 2014.
[187] Greenwald, Glenn: NSA collecting phone records of millions of Verizon customers daily, In. The Guardian, 2013. június 6., http://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order (2018. április 28.)
[188] Campbell, Duncan: Somebody's Listening, In. New Statesman, 1988. augusztus 12., http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf (2018. április 28.)
[189] Campbell, Duncan- HONIGSBAUM, Mark: Britain and US spy on world, In. The Guardian, 1999. május 23., http://www.duncancampbell.org/menu/journalism/guardian/britain.pdf (2018. április 28.)

[190] NSA: UKUSA Agreement Release 1940-1956, In. National Security Agency: Public Information, Declassification and Transparency, http://www.nsa.gov/public_info/declass/ukusa.shtml (2018. április 28.)
[191] NSA: VENONA, In. National Security Agency: Public Information, Declassification and Transparency, http://www.nsa.gov/public_info/declass/venona/ (2018. április 28.)
[192] The Guardian: NSA Prism program slides, In. The Guardian, 2013. november 1., http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (2018. április 28.)
[193] Macaskill, Ewen: NSA paid millions to cover Prism compliance costs for tech companies, In. The Guardian, 2013. augusztus 23., http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid (2018. április 28.)
[194] Greenwald, Glenn: XKeyscore: NSA tool collects 'nearly everything a user does on the internet', In. The Guardian, 2013. július 31., http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (2018. április 28.)
[195] Gellman, Barton: NSA broke privacy rules thousands of times per year, audit finds, In. The Washington Post, 2013. augusztus 16., http://www.washingtonpost.com/world/national-security/nsa-broke-privacy-rules-thousands-of-times-per-year-audit-finds/2013/08/15/3310e554-05ca-11e3-a07f-49ddc7417125_print.html (2018. április 28.)
[196] Greenwald, Glenn- POITRAS, Laura- MACASKILL, Ewen: NSA shares raw intelligence including Americans' data with Israel, In. The Guardian, 2013. szeptember 11., http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents (2018. április 28.)
[197] Hopkins, Nick- Borger, Julian: Exclusive: NSA pays £100m in secret funding for GCHQ, In. The Guardian, 2013. augusztus 1., http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden (2018. április 28.)
[198] Facebook Trancparency: Magyarországi adatbekérések 2017. január- 2017. június, In. Facebook, 2017., https://transparency.facebook.com/country/Hungary/2017-H1/ (2018. április 28.)
[199] Horváth Balázs: A Facebook ördögi tervvel férkőzne be Kínába, In. 24 Tech, 2016. november 23., https://24.hu/tech/2016/11/23/a-facebook-ordogi-tervvel-ferkozne-be-kinaba/ (2017. április 19.)

[200] Zezima, Katie: The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work., In. Washington Post, 2014. június 3., http://www.washingtonpost.com/blogs/the-fix/wp/2014/06/03/the-secret-service-wants-software-that-detects-social-media-sarcasm-yeah-sure-it-will-work/ (2017. december 29.)
[201] Deák Veronika: Biztonságtudatosság az információs környezetben, In. Szakmai Szemle- A Katonai Nemzetbiztonsági Szolgálat Tudományos- Szakmai Folyóirata, 2017/3., pp. 59-77., 2017.
[202] Kevin D. Mitnick: A legendás hacker- A megtévesztés művészete. Perfact-Pro, Budapest, 2003.
[203] Deák Veronika: A social engineering humán alapú támadási technikái, In. Biztonságpolitika, 2017. április 10., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai
[204] Deák Veronika: A számítógép alapú social engineer támadási technikák, In. Biztonságpolitikai, 2017. április 28., http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai
[205] Simon Béla: Rendészeti szervek együttműködése a kiberbűnözés ellen, In Nemzetbiztonsági Szemle, VI. /1., 2018., pp. 36-58.
[206] Eddolls Matt: Making cybercrime prevention the highest priority, In. Network Security, Volume 2016, Issue 8, August 2016., pp. 5-8., https://doi.org/10.1016/S1353-4858(16)30075-7
[207] Sammons, John- Cross, Michael: Cybercrime, In. The Basics of Cyber Safety- Computer and Mobile Device Safety Made Easy, 2017., pp. 87–116.
[208] 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. április 28.)
[209] 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. április 28.)
[2010] Kovács László- Krasznay Csaba: A digital Mohács: a cyber attack scenario against Hungary, In. Nemzet És Biztonság: Biztonságpolitikai Szemle III:(Spec. Issue Winter), 2010., pp. 49-59.
[211] Kovács László- Krasznay Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, In. Nemzet és Biztonság, 2017/1., 2017., pp. 3-16.

[212] Krasznay Csaba- Simon Béla: Kiberbűncselekmények az online kereskedelemben, In. Hadmérnök, XII. Évfolyam KÖFOP különszám - 2017.
[213] Tehrani et. al.: Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime, In. Computer Law & Security Review, Volume 29, Issue 3, June 2013., pp. 207-215., https://doi.org/10.1016/j.clsr.2013.03.011
[214] Lee, Jayeon- Xu, Weiai: The more attacks, the more retweets: Trump's and Clinton's agenda setting on Twitter, In. Public Relations Review, Volume 44, Issue 2, June 2018., pp. 201-213., https://doi.org/10.1016/j.pubrev.2017.10.002
[215] Webster, Stephen C.: Revealed: Air Force ordered software to manage army of fake virtual people, In. The Raw Story, 2011. február 18., http://www.rawstory.com/rs/2011/02/18/revealed-air-force-ordered-software-to-manage-army-of-fake-virtual-people/ (2018. január 20.)
[216] Abokhodair et. al.: Dissecting a social Botnet: Growth, content and influence in twitter, In. CSCW 2015 - Proceedings of the 2015 ACM International Conference on Computer-Supported Cooperative Work and Social Computing, 2015., pp. 839-851.
[217] Spier, Shaked: Tehran, Tunis, Tahrir: Social Media and the Formation of Collective Action, In. Collective Action 2.0- The Impact of Social Media on Collective Action- A volume in Chandos Information Professional Series, 2017., pp. 33–51.
[218] Khondker, Habibul H.: New Media, Political Mobilization, and the Arab Spring, In. International Encyclopedia of the Social & Behavioral Sciences (Second Edition), 2015., pp. 798-804.
[219] Juhász et. al.: „Eurázsiai vagyok" - A magyar szélsőjobboldal kapcsolata a Kremllel, In: Political Capital, 2015. március, http://www.politicalcapital.hu/wp-content/uploads/PC_SDI_Boll_tanulmany_EurazsiaiVagyok.pdf (2018. április 29.)
[220] Walker, Shaun: Salutin' Putin: inside a Russian troll house, In: The Guardian, 2015. április 2., http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house (2018. április 29.)
[221] Yang, Yuan: China's Communist party raises army of nationalist trolls, In. Financial Times, 2017. december 30., https://www.ft.com/content/9ef9f592-e2bd-11e7-97e2-916d4fbac0da (2018. április 29.)
[222] Lewandowsky et. al.: Beyond Misinformation: Understanding and Coping with the "Post-Truth" Era, In. Journal of Applied Research in Memory and Cognition, Volume 6, Issue 4, December 2017., pp. 353-369., https://doi.org/ 10.1016/j.jarmac.2017.07.008

[223] Zimdars, Melissa: 'False, Misleading, Clickbait-y, and Satirical “News” Sources', 2016., https://docs.google.com/document/d/10eA5-mCZLSS4MQY5QGb5ewC3VAL6pLkT53V_81ZyitM/edit
[224] Figueira, Álvaro- Oliveira, Luciana: The current state of fake news: challenges and opportunities, In. Procedia Computer Science, Volume 121, 2017., pp. 817-825., https://doi.org/10.1016/j.procs.2017.11.106
[225] Jang, S. Mo- Kim. Joon K.: Third person effects of fake news: Fake news regulation and media literacy interventions, In. Computers in Human Behavior, Volume 80, March 2018., pp. 295-302., https://doi.org/10.1016/j.chb.2017.11.034
[226] Paul, Christopher- Matthews, Miriam: The Russian "Firehose of Falsehood" Propaganda Model- Why It Might Work and Options to Counter It, In. RAND Corporation, 2016., https://www.rand.org/content/dam/rand/pubs/perspectives/PE100/PE198/RAND_PE198.pdf
[227] Hoffman, Frank G.: Conflictin the 21st Century: The Rise of Hybrid Wars.Wars. 2007., p. 8.
[228] Roche M., Edward: Comments on “Assessing Russian Activities and Intentions in Recent US Elections”, In. Cyberarmscontrolblog, 2017. január 8., https://cyberarmscontrolblog.com/2017/01/08/comments-on-assessing-russian-activities-and-intentions-in-recent-us-elections/ (2018. április 29.)
[229] JAR-16-20296. Agrizzly Steppe –Russian Malicious Cyber Activity. US Department of Homeland Security and Federal Bureau of Investigation [online] 2016. 12. 16., https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (2018. április 29.)
[230] Kovács László- Krasznay Csaba: „Mert övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során, In. SVKK elemzések, 2017/9., pp. 1-11., 2017.
[231] Stamos, Alex: An Update On Information Operations On Facebook, In. Facebook Newsroom, 2017. szeptember 6., https://newsroom.fb.com/news/2017/09/information-operations-update/ (2018. április 29.)
[232] Swaine, Jon: Twitter admits far more Russian bots posted on election than it had disclosed, In. The Guardian, 2018. január 20., https://www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed (2018. április 29.)

[233] Timberg, Craig- Dwoskin, Elizabeth: Russian content on Facebook, Google and Twitter reached far more users than companies first disclosed, congressional testimony says, In. The Washington Post, 2017. október 30., https://www.washingtonpost.com/business/technology/2017/10/30/4509587e-bd84-11e7-97d9-bdab5a0ab381_story.html?noredirect=on (2018. április 29.)

[234] Zittrain, Jonathan: Facebook Could Decide an Election Without Anyone Ever Finding Out- The scary future of digital gerrymandering—and how to prevent it, In. New Republic, https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering (2018. április 29.)

[235] Adam et. al.: Experimental evidence of massive-scale emotional contagion through social networks, In. PNAS, 2014., vol. 111., no. 29., http://www.pnas.org/cgi/doi/10.1073/pnas.1412583111

[236] Zittrain, Jonathan: Engineering an Election: Digital gerrymandering poses a threat to democracy. Harvard Law Review, 127(8), 2014., pp. 335-341.

[237] Cvetkovska et al.: The Secret Players Behind Macedonia's Fake News Sites, In. OCCRP, 2018. július 18., https://www.occrp.org/en/spooksandspin/the-secret-players-behind-macedonias-fake-news-sites (2018. október 2.)

[238] Kis-Benedek József: Dzsihádizmus- Radikalizmus- Terrorizmus, Zrínyi Kiadó, Budapest, 2016.

[239] Horváth L. Attila: A terrorizmus csapdájában, Zrínyi Kiadó, Budapest, 2014.

[240] Robinson, Leonard C.: Just Terror: The Islamic State's Use of Strategic "Framing" to Recruit and Motivate, In. Orbis, Volume 61, Issue 2, 2017., pp. 172-186., https://doi.org/10.1016/j.orbis.2017.02.002

[241] Cragn, Kim R.- Weil, Ari: "Virtual Planners" in the Arsenal of Islamic State External Operations, In. Orbis, Volume 62, Issue 2, 2018., pp. 294-312., https://doi.org/10.1016/j.orbis.2018.02.007

[242] Thompson, Gareth: Extremes of Engagement: The post-classical public relations of the Islamic State, In. Public Relations Review, Volume 43, Issue 5, December 2017., pp. 915-924., https://doi.org/10.1016/j.pubrev.2017.03.014

[243] Galloway, Chris: Media jihad: What PR can learn in Islamic State's public relations masterclass, In. Public Relations Review, Volume 42, Issue 4, November 2016., pp. 582-590., https://doi.org/10.1016/j.pubrev.2016.03.014

[244] Margitics József: Az ISIS által használt internetes propaganda eszközök áttekintése, In.Nemzetbiztonsági Szakkollégium Kiadványkötete, Budapest, 2017.
[245] Wilson, James Q- Kelling, George L.: Broken Windows: The police and neighborhood safety, In. The Atlantic, retrieved, 1982.
[246] 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
[247] Official U.S. Army Social Media, https://www.army.mil/socialmedia/directory/
[248] Army Operations Security (OPSEC), https://www.facebook.com/usarmyopsec/
[249] Naval Operations Security (OPSEC), https://www.facebook.com/NavalOPSEC/
[250] H4xXx0R: Magyarország 600 milliót fizetett a világ legostobább hekkereinek, In. Index, 2015. július 7., https://index.hu/tech/2015/07/07/600_milliot_fizettunk_a_vilag_legostobabb_hekkereinek/ (2018. április 30.)
[251] Best Regards Zoltan: Mit tud a magyar titkosszolgálat által használt kémprogram?, In. Index.hu, 2014. augusztus 14., https://index.hu/tech/2014/08/14/a_magyar_titkosszolgalat_siman_lehallgat/ (2018. április 30.)
[252] MacAskill, Ewen: British army creates team of Facebook warriors, In. The Guardian, 2015. január 31., https://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade (2018. április 30.)
[253] EU vs Disinformation, https://www.facebook.com/EUvsDisinfo/

FÜGGELÉK/MELLÉKLETEK

Táblázatok jegyzéke

Ábrák jegyzéke

1. számú melléklet (Kérdőíves felmérés kérdései)

	Tudás	**Attitűd**	**Viselkedés**
Jelszóhasználat			
Ugyanazon jelszó használata	Tudom, hogy lehet ugyanazt a jelszót használni több profil esetében (akár munkahelyen is). <>	Biztonságosnak tartom ugyanazt a jelszót használni a különböző profilok esetében (akár munkahelyen is) <>	Eltérő jelszavakat használok a különböző profiljaim esetében.
Jelszavak megosztása	Tisztában vagyok vele, hogy megengedhető a jelszavak megosztása másokkal. <>	Nem tartom jó ötletnek másokkal megosztani a jelszavainkat, még ha kérdezik is	Megosztom a jelszavaim másokkal. <>
Erős jelszó használata	Tudom, hogy egy jó jelszó betűk, számok és szimbólumok keverékéből áll.	A csak betűkből álló jelszót biztonságosnak tartom. <>	Betűk, számok és szimbólumok keverékből álló jelszót használok.
E-mail használat			
Ismerősök által küldött e-mailben	Tisztában vagyok vele, hogy meg lehet nyitni az ismerőstől	Biztonságosnak tartom az ismerőstől	Nem nyitok meg minden esetben

linkekre való kattintás	kapott mindenféle linkeket. <>	kapott linkek megnyitását. <>	ismerősöktől kapott linkeket.
Ismeretlenek által küldött e-mailben linkekre való kattintás	Tudom, hogy az ismeretlenektől kapott linket meg lehet nyitni. <>	Úgy gondolom, semmi baj nem lehet abból, ha ismeretlenektől kapott linket megnyitok. <>	Amennyiben egy ismeretlentől kapott link érdekesnek tűnik, megnyitom. <>
Ismeretlenek által küldött e-mailben a csatolmány megnyitása	Tisztában vagyok vele, hogy egy ismeretlen által küldött e-mailben meg lehet nyitni a csatolmányt. <>	Kockázatosnak tartom egy ismeretlentől kapott e-mail esetében a csatolmány megnyitását.	Sosem nyitok meg ismeretlenek által küldött e-mailben csatolmányokat.
Internethasználat			
Fájlletöltés	Tudom, hogy bármilyen fájlt le lehet tölteni az általunk használt számítógépre, ha az segít a tanulásban, munkavégzésben. <>	Azt gondolom, kockázatos lehet a fájlok letöltése az általam használt számítógépekre.	Letöltök minden fájlt az általam használt számítógépekre, ha az segít a tanulásban, munkavégzésben. <>
Megbízhatatlan oldalakhoz való hozzáférés	Tisztában vagyok vele, hogy tanulás, munkavégzés közben nem kell hozzáférnem bizonyos weboldalakhoz.	Azt gondolom, attól, hogy hozzáférhetek egy weboldalhoz, az még nem jelenti, hogy az biztonságos is.	Ha csatlakozom az internethez, olyan oldalakat keresek fel, amilyet csak akarok. <>
Információk online közlése	Tudom, hogy rendben levő mindenféle információ közlése a különböző weboldalon, amennyiben az segít a tanulásban, munkavégzésben. <>	Azt gondolom, amennyiben segít a tanulásban, munkavégzésben, nem lényeges, hogy milyen információt közlök egy weboldalon. <>	Mindig ellenőrzöm egy weboldal megbízhatóságát, mielőtt információt közölnék azon.
Közösségi média használat			
SM adatvédelmi beállítások	Tisztában vagyok vele, hogy rendszeresen ellenőriznem kell az adatvédelmi beállításaimat a közösségi média profiljaimban.	Jó ötletnek tartom rendszeresen ellenőrizni az adatvédelmi beállításaimat a közösségi média profiljaimban	Nem ellenőrzöm rendszeresen a közösségi média profiljaimban az adatvédelmi beállításaimat. <>

Következmények megfontolása	Tisztában vagyok azzal, hogy kirúghatnak amiatt, amit a közösségi médiában közzéteszek.	Azt gondolom, nincs jelentősége, ha olyat posztolok a közösségi médiában, amit egyébként nem mondanék nyilvánosan. <>	Semmit nem osztok meg a közösségi médiában anélkül, hogy ne fontolnám meg az esetleges negatív következményeket.
Iskoláról, munkáról való posztolás	Tudom, hogy azt posztolhatok a közösségi médiában az iskolámról, munkahelyemről, amit csak akarok. <>	Kockázatosnak tartom bizonyos információk posztolását a közösségi médiában az iskolámról, munkahelyemről.	Azt posztolok a közösségi médiában, amit csak akarok az iskolámról, munkahelyemről. <>
Mobil eszköz használat			
Mobileszköz fizikai biztonsága	Tisztában vagyok azzal, ha nyilvános helyen tanulok vagy dolgozok, mindig magamnál kell tartanom a laptopom.	Azt gondolom, ha kávézóban tanulok vagy dolgozok, nyugodtan őrizetlenül hagyhatom a laptopom néhány percre. <>	Ha nyilvános helyen tanulok vagy dolgozok, őrizetlenül hagyom a laptopom. <>
Érzékeny információ továbbítása Wi-Fi-n	Tudom, hogy rendben levő érzékeny információ továbbítása nyilvános Wi-Fi hálózatról. <>	Kockázatosnak tartom érzékeny információk továbbítását nyilvános Wi-Fi hálózatról.	Továbbítok érzékeny információt nyilvános Wi-Fi hálózatról. <>
Shoulder surfing	Tisztában vagyok vele, hogy amennyiben érzékeny dokumentummal dolgozom, figyelnem kell rá, hogy idegenek ne láthassák a képernyőt.	Kockázatosnak tartom érzékeny információkat megnyitni a laptopon, ha idegenek is láthatják a képernyőt.	Ellenőrzöm, hogy ismeretlenek láthatják-e a képernyőt, ha érzékeny dokumentummal dolgozok.
Információ kezelése			
Érzékeny adatot tartalmazó dokumentumokat megsemmisítése	Tudom, hogy érzékeny adatot tartalmazó dokumentumokat ugyanolyan módon dobhatunk ki, mint a nem érzékeny adatokat tartalmazókat. <>	Azt gondolom, hogy biztonságos érzékeny adatot tartalmazó dokumentumokat a szemetesbe dobni. <>	Amikor érzékeny adatot tartalmazó dokumentumokat kell kidobnom, meggyőződök róla, hogy azt felaprítják vagy megsemmisítik teljesen.

Hordozható eszközök csatlakoztatása	Tisztában vagyok vele, hogy nyilvános helyen talált pendriveot nem szabad a számítógépembe dugni.	Úgy vélem, nyilvános helyen talált pendrive esetén semmi rossz nem történhet, ha bedugom a számítógépembe. <>	Nyilvános helyen talált pendriveot nem dugok be a számítógépembe.
Érzékeny adatok kezelése	Tisztában vagyok vele, hogy érzékeny adatokat tartalmazó dokumentumok őrizetlenül hagyhatok. <>	Kockázatosnak tartom az érzékeny adatokat tartalmazó dokumentumokat őrizetlenül hagyását.	Őrizetlenül hagyok érzékeny adatokat tartalmazó dokumentumokat. <>
Incidensek jelentése			
Gyanús viselkedés jelentése	Tisztában vagyok vele, ha gyanúsan viselkedő személyt látok az iskolámban vagy a munkahelyemen, jelentenem kell.	Úgy vélem, ha nem veszek tudomást egy gyanúsan viselkedő személyről az iskolámban vagy munkahelyemen, semmi baj nem történhet. <>	Ha gyanúsan viselkedő személyt látok az iskolámban vagy a munkahelyemen, tennem kell ezzel kapcsolatban.
Az alacsony bizontságtudatosságú iskolatársak, kollégák figyelmen kívül hagyása	Tudom, hogy nem hagyhatom figyelmen kívül azokat az iskolatársaim, munkatársaim, akik nem követik a biztonsági szabályokat.	Azt gondolom, nem történhet semmi rossz, ha figyelmen kívül hagyom azokat az iskolatársaim, munkatársaim, akik nem követik a biztonsági szabályokat. <>	Ha észreveszem, hogy az iskolatársaim, munkatársaim nem követik a biztonsági szabályokat, nem teszek semmit. <>
Incidensek jelentése	Tisztában vagyok vele, hogy szabadon eldönthető, hogy jelentsük-e a biztonsági incidenseket. <>	Kockázatosnak tartom figyelmen kívül hagyni a biztonsági incidenseket, még akkor is, ha úgy gondolom, nem jelentősek.	Amennyiben észlelek egy biztonsági incidenst, jelentem azt
A kérdések végén szereplő <> jelzés a helytelen válaszokat jelöli.			

2. számú melléklet (Kérdőív kiértékelése)

Crosstabs

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Biztonságtudatosnak gondolja-e Önmagát? * Neme?	406	98,1%	8	1,9%	414	100,0%

Biztonságtudatosnak gondolja-e Önmagát? * Neme? Crosstabulation

			Neme?	
			Férfi	Nő
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	117	140
		Expected Count	108,2	148,8
		% within Biztonságtudatosnak gondolja-e Önmagát?	45,5%	54,5%
		% within Neme?	68,4%	59,6%
		% of Total	28,8%	34,5%
	Nem	Count	33	42
		Expected Count	31,6	43,4
		% within Biztonságtudatosnak gondolja-e Önmagát?	44,0%	56,0%
		% within Neme?	19,3%	17,9%
		% of Total	8,1%	10,3%
	Nem tudom	Count	21	53
		Expected Count	31,2	42,8
		% within Biztonságtudatosnak gondolja-e Önmagát?	28,4%	71,6%
		% within Neme?	12,3%	22,6%
		% of Total	5,2%	13,1%
Total		Count	171	235
		Expected Count	171,0	235,0

	% within Biztonságtudatosnak gondolja-e Önmagát?	42,1%	57,9%
	% within Neme?	100,0%	100,0%
	% of Total	42,1%	57,9%

Biztonságtudatosnak gondolja-e Önmagát? * Neme? Crosstabulation

			Total
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	257
		Expected Count	257,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Neme?	63,3%
		% of Total	63,3%
	Nem	Count	75
		Expected Count	75,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Neme?	18,5%
		% of Total	18,5%
	Nem tudom	Count	74
		Expected Count	74,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Neme?	18,2%
		% of Total	18,2%
Total		Count	406
		Expected Count	406,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Neme?	100,0%
		% of Total	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7,063[a]	2	,029
Likelihood Ratio	7,318	2	,026

Linear-by-Linear Association	5,896	1	,015
N of Valid Cases	406		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 31,17.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,132	,029
	Cramer's V	,132	,029
	Contingency Coefficient	,131	,029
N of Valid Cases		406	

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Alapvetően műszaki vagy humán érdeklődűnek gondolja Önmagát? * Neme?	410	99,0%	4	1,0%	414	100,0%

Alapvetően műszaki vagy humán érdeklődűnek gondolja Önmagát? * Neme? Crosstabulation

			Neme?		
			Férfi	Nő	Total
Alapvetően műszaki vagy humán érdeklődűnek gondolja Önmagát?	Műszaki	Count	48	19	67
		Expected Count	28,3	38,7	67,0
		% within Alapvetően műszaki vagy humán érdeklődűnek gondolja Önmagát?	71,6%	28,4%	100,0%
		% within Neme?	27,7%	8,0%	16,3%
		% of Total	11,7%	4,6%	16,3%
	Humán	Count	87	175	262
		Expected Count	110,6	151,4	262,0
		% within Alapvetően műszaki vagy humán érdeklődűnek gondolja Önmagát?	33,2%	66,8%	100,0%

		% within Neme?	50,3%	73,8%	63,9%
		% of Total	21,2%	42,7%	63,9%
	Mindkettő	Count	38	43	81
		Expected Count	34,2	46,8	81,0
		% within Alapvetően műszaki vagy humán érdeklődűnek gondolja Önmagát?	46,9%	53,1%	100,0%
		% within Neme?	22,0%	18,1%	19,8%
		% of Total	9,3%	10,5%	19,8%
Total		Count	173	237	410
		Expected Count	173,0	237,0	410,0
		% within Alapvetően műszaki vagy humán érdeklődűnek gondolja Önmagát?	42,2%	57,8%	100,0%
		% within Neme?	100,0%	100,0%	100,0%
		% of Total	42,2%	57,8%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	33,238[a]	2	,000
Likelihood Ratio	33,394	2	,000
Linear-by-Linear Association	7,015	1	,008
N of Valid Cases	410		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 28,27.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,285	,000
	Cramer's V	,285	,000
	Contingency Coefficient	,274	,000
N of Valid Cases		410	

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Biztonságtudatosnak gondolja-e Önmagát? * Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	406	98,1%	8	1,9%	414	100,0%

Biztonságtudatosnak gondolja-e Önmagát? * Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa? Crosstabulation

			Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	
			Igen	Nem
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	158	99
		Expected Count	146,2	110,8
		% within Biztonságtudatosnak gondolja-e Önmagát?	61,5%	38,5%
		% within Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	68,4%	56,6%
		% of Total	38,9%	24,4%
	Nem	Count	36	38
		Expected Count	42,1	31,9
		% within Biztonságtudatosnak gondolja-e Önmagát?	48,6%	51,4%
		% within Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	15,6%	21,7%
		% of Total	8,9%	9,4%
	Nem tudom	Count	37	38

	Expected Count	42,7	32,3
	% within Biztonságtudatosnak gondolja-e Önmagát?	49,3%	50,7%
	% within Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	16,0%	21,7%
	% of Total	9,1%	9,4%
Total	Count	231	175
	Expected Count	231,0	175,0
	% within Biztonságtudatosnak gondolja-e Önmagát?	56,9%	43,1%
	% within Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	100,0%	100,0%
	% of Total	56,9%	43,1%

Biztonságtudatosnak gondolja-e Önmagát? * Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa? Crosstabulation

			Total
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	257
		Expected Count	257,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	63,3%
		% of Total	63,3%
	Nem	Count	74
		Expected Count	74,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	18,2%
		% of Total	18,2%
	Nem tudom	Count	75
		Expected Count	75,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%

	% within Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	18,5%
	% of Total	18,5%
Total	Count	406
	Expected Count	406,0
	% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
	% within Volt-e valamilyen információbiztonsággal kapcsolatos kurzusa?	100,0%
	% of Total	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6,002[a]	2	,050
Likelihood Ratio	5,985	2	,050
Linear-by-Linear Association	4,945	1	,026
N of Valid Cases	406		

a. 0 cells (,0%) have expected count less than 5. The minimum expected count is 31,90.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,122	,050
	Cramer's V	,122	,050
	Contingency Coefficient	,121	,050
N of Valid Cases		406	

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent

Biztonságtudatosnak gondolja-e Önmagát? * Mi az Ön legmagasabb iskolai végzettsége?	409	98,8%	5	1,2%	414	100,0%

Biztonságtudatosnak gondolja-e Önmagát? * Mi az Ön legmagasabb iskolai végzettsége? Crosstabulation

			Mi az Ön legmagasabb iskolai végzettsége?	
			Érettségi	Alapszakos diploma
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	179	24
		Expected Count	184,8	25,9
		% within Biztonságtudatosnak gondolja-e Önmagát?	69,4%	9,3%
		% within Mi az Ön legmagasabb iskolai végzettsége?	61,1%	58,5%
		% of Total	43,8%	5,9%
	Nem	Count	57	8
		Expected Count	54,4	7,6
		% within Biztonságtudatosnak gondolja-e Önmagát?	75,0%	10,5%
		% within Mi az Ön legmagasabb iskolai végzettsége?	19,5%	19,5%
		% of Total	13,9%	2,0%
	Nem tudom	Count	57	9

Biztonságtudatosnak gondolja-e Önmagát? * Mi az Ön legmagasabb iskolai végzettsége? Crosstabulation

			Mi az Ön legmagasabb iskolai végzettsége?	
			Mesterszakos diploma	Posztgraduális képzés
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	45	10
		Expected Count	37,8	9,5

		% within Biztonságtudatosnak gondolja-e Önmagát?	17,4%	3,9%
		% within Mi az Ön legmagasabb iskolai végzettsége?	75,0%	66,7%
		% of Total	11,0%	2,4%
	Nem	Count	8	3
		Expected Count	11,1	2,8
		% within Biztonságtudatosnak gondolja-e Önmagát?	10,5%	3,9%
		% within Mi az Ön legmagasabb iskolai végzettsége?	13,3%	20,0%
		% of Total	2,0%	0,7%
	Nem tudom	Count	7	2

Biztonságtudatosnak gondolja-e Önmagát? * Mi az Ön legmagasabb iskolai végzettsége? Crosstabulation

			Total
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	258
		Expected Count	258,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Mi az Ön legmagasabb iskolai végzettsége?	63,1%
		% of Total	63,1%
	Nem	Count	76
		Expected Count	76,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Mi az Ön legmagasabb iskolai végzettsége?	18,6%
		% of Total	18,6%
	Nem tudom	Count	75

Biztonságtudatosnak gondolja-e Önmagát? * Mi az Ön legmagasabb iskolai végzettsége? Crosstabulation

		Mi az Ön legmagasabb iskolai végzettsége?

			Érettségi	Alapszakos diploma
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	53,7	7,5
		% within Biztonságtudatosnak gondolja-e Önmagát?	76,0%	12,0%
		% within Mi az Ön legmagasabb iskolai végzettsége?	19,5%	22,0%
		% of Total	13,9%	2,2%
Total		Count	293	41
		Expected Count	293,0	41,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	71,6%	10,0%
		% within Mi az Ön legmagasabb iskolai végzettsége?	100,0%	100,0%
		% of Total	71,6%	10,0%

Biztonságtudatosnak gondolja-e Önmagát? * Mi az Ön legmagasabb iskolai végzettsége? Crosstabulation

			Mi az Ön legmagasabb iskolai végzettsége?	
			Mesterszakos diploma	Posztgraduális képzés
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	11,0	2,8
		% within Biztonságtudatosnak gondolja-e Önmagát?	9,3%	2,7%
		% within Mi az Ön legmagasabb iskolai végzettsége?	11,7%	13,3%
		% of Total	1,7%	0,5%
Total		Count	60	15
		Expected Count	60,0	15,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	14,7%	3,7%
		% within Mi az Ön legmagasabb iskolai végzettsége?	100,0%	100,0%

	% of Total	14,7%	3,7%

Biztonságtudatosnak gondolja-e Önmagát? * Mi az Ön legmagasabb iskolai végzettsége? Crosstabulation

			Total
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	75,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Mi az Ön legmagasabb iskolai végzettsége?	18,3%
		% of Total	18,3%
Total		Count	409
		Expected Count	409,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Mi az Ön legmagasabb iskolai végzettsége?	100,0%
		% of Total	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4,897[a]	6	,557
Likelihood Ratio	5,137	6	,526
Linear-by-Linear Association	2,712	1	,100
N of Valid Cases	409		

a. 2 cells (16,7%) have expected count less than 5. The minimum expected count is 2,75.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,109	,557
	Cramer's V	,077	,557
	Contingency Coefficient	,109	,557
N of Valid Cases		409	

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használja aktívan az internetet?	404	97,6%	10	2,4%	414	100,0%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használja aktívan az internetet? Crosstabulation

			Egy átlagos napon mennyi ideig használja aktívan az internetet?		
			11-30 percet	Fél-egy órát	1-2 órát
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	0	12	50
		Expected Count	,6	12,6	52,4
		% within Biztonságtudatosnak gondolja-e Önmagát?	0,0%	4,7%	19,6%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	0,0%	60,0%	60,2%
		% of Total	0,0%	3,0%	12,4%
	Nem	Count	1	3	14
		Expected Count	,2	3,7	15,4
		% within Biztonságtudatosnak gondolja-e Önmagát?	1,3%	4,0%	18,7%

		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	100,0%	15,0%	16,9%
		% of Total	0,2%	0,7%	3,5%
	Nem tudom	Count	0	5	19

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használja aktívan az internetet? Crosstabulation

			Egy átlagos napon mennyi ideig használja aktívan az internetet?		
			3-4 órát	5-6 órát	6 óránál többet
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	93	45	55
		Expected Count	92,8	44,2	52,4
		% within Biztonságtudatosnak gondolja-e Önmagát?	36,5%	17,6%	21,6%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	63,3%	64,3%	66,3%
		% of Total	23,0%	11,1%	13,6%
	Nem	Count	31	11	15
		Expected Count	27,3	13,0	15,4
		% within Biztonságtudatosnak gondolja-e Önmagát?	41,3%	14,7%	20,0%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	21,1%	15,7%	18,1%
		% of Total	7,7%	2,7%	3,7%
	Nem tudom	Count	23	14	13

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használja aktívan az internetet? Crosstabulation

			Total
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	255
		Expected Count	255,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%

		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	63,1%
		% of Total	63,1%
	Nem	Count	75
		Expected Count	75,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	18,6%
		% of Total	18,6%
	Nem tudom	Count	74

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használja aktívan az internetet? Crosstabulation

			Egy átlagos napon mennyi ideig használja aktívan az internetet?		
			11-30 percet	Fél-egy órát	1-2 órát
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	,2	3,7	15,2
		% within Biztonságtudatosnak gondolja-e Önmagát?	0,0%	6,8%	25,7%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	0,0%	25,0%	22,9%
		% of Total	0,0%	1,2%	4,7%
Total		Count	1	20	83
		Expected Count	1,0	20,0	83,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	0,2%	5,0%	20,5%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	100,0%	100,0%	100,0%
		% of Total	0,2%	5,0%	20,5%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használja aktívan az internetet? Crosstabulation

			Egy átlagos napon mennyi ideig használja aktívan az internetet?		
			3-4 órát	5-6 órát	6 óránál többet
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	26,9	12,8	15,2
		% within Biztonságtudatosnak gondolja-e Önmagát?	31,1%	18,9%	17,6%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	15,6%	20,0%	15,7%
		% of Total	5,7%	3,5%	3,2%
Total		Count	147	70	83
		Expected Count	147,0	70,0	83,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	36,4%	17,3%	20,5%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	100,0%	100,0%	100,0%
		% of Total	36,4%	17,3%	20,5%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használja aktívan az internetet? Crosstabulation

			Total
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	74,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	18,3%
		% of Total	18,3%
Total		Count	404
		Expected Count	404,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	100,0%
		% within Egy átlagos napon mennyi ideig használja aktívan az internetet?	100,0%
		% of Total	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8,195[a]	10	,610
Likelihood Ratio	7,109	10	,715
Linear-by-Linear Association	1,283	1	,257
N of Valid Cases	404		

a. 5 cells (27,8%) have expected count less than 5. The minimum expected count is ,18.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,142	,610
	Cramer's V	,101	,610
	Contingency Coefficient	,141	,610
N of Valid Cases		404	

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	405	97,8%	9	2,2%	414	100,0%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat? Crosstabulation

	Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?

			Kevesebb, mint 10 percet	11-30 percet
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	31	25
		Expected Count	22,7	24,6
		% within Biztonságtudatosnak gondolja-e Önmagát?	12,2%	9,8%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	86,1%	64,1%
		% of Total	7,7%	6,2%
	Nem	Count	3	7
		Expected Count	6,8	7,3
		% within Biztonságtudatosnak gondolja-e Önmagát?	3,9%	9,2%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	8,3%	17,9%
		% of Total	0,7%	1,7%
	Nem tudom	Count	2	7

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?		
			Fél-egy órát	1-2 órát	3-4 órát
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	40	69	59
		Expected Count	44,1	65,5	65,5
		% within Biztonságtudatosnak gondolja-e Önmagát?	15,7%	27,1%	23,1%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	57,1%	66,3%	56,7%
		% of Total	9,9%	17,0%	14,6%
	Nem	Count	15	13	26
		Expected Count	13,1	19,5	19,5
		% within Biztonságtudatosnak gondolja-e Önmagát?	19,7%	17,1%	34,2%

		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	21,4%	12,5%	25,0%
		% of Total	3,7%	3,2%	6,4%
	Nem tudom	Count	15	22	19

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?		
			5-6 órát	6 óránál többet	
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	17	14	255
		Expected Count	16,4	16,4	255,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	6,7%	5,5%	100,0%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	65,4%	53,8%	63,0%
		% of Total	4,2%	3,5%	63,0%
	Nem	Count	6	6	76
		Expected Count	4,9	4,9	76,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	7,9%	7,9%	100,0%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	23,1%	23,1%	18,8%
		% of Total	1,5%	1,5%	18,8%
	Nem tudom	Count	3	6	74

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	
			Kevesebb, mint 10 percet	11-30 percet
	Nem tudom	Expected Count	6,6	7,1

Biztonságtudatosnak gondolja-e Önmagát?	% within Biztonságtudatosnak gondolja-e Önmagát?	2,7%	9,5%
	% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	5,6%	17,9%
	% of Total	0,5%	1,7%
Total	Count	36	39
	Expected Count	36,0	39,0
	% within Biztonságtudatosnak gondolja-e Önmagát?	8,9%	9,6%
	% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	100,0%	100,0%
	% of Total	8,9%	9,6%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?		
			Fél-egy órát	1-2 órát	3-4 órát
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	12,8	19,0	19,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	20,3%	29,7%	25,7%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	21,4%	21,2%	18,3%
		% of Total	3,7%	5,4%	4,7%
Total		Count	70	104	104
		Expected Count	70,0	104,0	104,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	17,3%	25,7%	25,7%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	100,0%	100,0%	100,0%
		% of Total	17,3%	25,7%	25,7%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?		
			5-6 órát	6 óránál többet	
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	4,8	4,8	74,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	4,1%	8,1%	100,0%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	11,5%	23,1%	18,3%
		% of Total	0,7%	1,5%	18,3%
Total		Count	26	26	405
		Expected Count	26,0	26,0	405,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	6,4%	6,4%	100,0%
		% within Egy átlagos napon mennyi ideig használ aktívan közösségi oldalakat?	100,0%	100,0%	100,0%
		% of Total	6,4%	6,4%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	16,874[a]	12	,154
Likelihood Ratio	18,434	12	,103
Linear-by-Linear Association	3,503	1	,061
N of Valid Cases	405		

a. 4 cells (19,0%) have expected count less than 5. The minimum expected count is 4,75.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,204	,154
	Cramer's V	,144	,154
	Contingency Coefficient	,200	,154
N of Valid Cases		405	

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	406	98,1%	8	1,9%	414	100,0%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	
			Kevesebb, mint 10 percet	11-30 percet
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	15	8
		Expected Count	14,5	8,2
		% within Biztonságtudatosnak gondolja-e Önmagát?	5,9%	3,1%
		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	65,2%	61,5%
		% of Total	3,7%	2,0%
	Nem	Count	5	2
		Expected Count	4,2	2,4
		% within Biztonságtudatosnak gondolja-e Önmagát?	6,7%	2,7%

		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	21,7%	15,4%
		% of Total	1,2%	0,5%
	Nem tudom	Count	3	3

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?		
			Fél-egy órát	1-2 órát	3-4 órát
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	26	48	61
		Expected Count	25,2	51,1	60,5
		% within Biztonságtudatosnak gondolja-e Önmagát?	10,2%	18,8%	23,8%
		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	65,0%	59,3%	63,5%
		% of Total	6,4%	11,8%	15,0%
	Nem	Count	5	19	14
		Expected Count	7,4	15,0	17,7
		% within Biztonságtudatosnak gondolja-e Önmagát?	6,7%	25,3%	18,7%
		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	12,5%	23,5%	14,6%
		% of Total	1,2%	4,7%	3,4%
	Nem tudom	Count	9	14	21

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?		
			5-6 órát	6 óránál többet	
Biztonságtudatosnak gondolja-e Önmagát?	Igen	Count	38	60	256
		Expected Count	37,2	59,3	256,0

		% within Biztonságtudatosnak gondolja-e Önmagát?	14,8%	23,4%	100,0%
		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	64,4%	63,8%	63,1%
		% of Total	9,4%	14,8%	63,1%
	Nem	Count	8	22	75
		Expected Count	10,9	17,4	75,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	10,7%	29,3%	100,0%
		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	13,6%	23,4%	18,5%
		% of Total	2,0%	5,4%	18,5%
	Nem tudom	Count	13	12	75

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	
			Kevesebb, mint 10 percet	11-30 percet
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	4,2	2,4
		% within Biztonságtudatosnak gondolja-e Önmagát?	4,0%	4,0%
		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	13,0%	23,1%
		% of Total	0,7%	0,7%
Total		Count	23	13
		Expected Count	23,0	13,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	5,7%	3,2%

		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	100,0%	100,0%
		% of Total	5,7%	3,2%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?		
			Fél-egy órát	1-2 órát	3-4 órát
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	7,4	15,0	17,7
		% within Biztonságtudatosnak gondolja-e Önmagát?	12,0%	18,7%	28,0%
		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	22,5%	17,3%	21,9%
		% of Total	2,2%	3,4%	5,2%
Total		Count	40	81	96
		Expected Count	40,0	81,0	96,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	9,9%	20,0%	23,6%
		% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	100,0%	100,0%	100,0%
		% of Total	9,9%	20,0%	23,6%

Biztonságtudatosnak gondolja-e Önmagát? * Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt? Crosstabulation

			Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?		
			5-6 órát	6 óránál többet	
Biztonságtudatosnak gondolja-e Önmagát?	Nem tudom	Expected Count	10,9	17,4	75,0
		% within Biztonságtudatosnak gondolja-e Önmagát?	17,3%	16,0%	100,0%

	% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	22,0%	12,8%	18,5%
	% of Total	3,2%	3,0%	18,5%
Total	Count	59	94	406
	Expected Count	59,0	94,0	406,0
	% within Biztonságtudatosnak gondolja-e Önmagát?	14,5%	23,2%	100,0%
	% within Egy átlagos napon mennyi ideig használ aktívan okos mobil eszközt?	100,0%	100,0%	100,0%
	% of Total	14,5%	23,2%	100,0%

Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	8,710[a]	12	,727
Likelihood Ratio	8,923	12	,710
Linear-by-Linear Association	,142	1	,707
N of Valid Cases	406		

a. 4 cells (19,0%) have expected count less than 5. The minimum expected count is 2,40.

Symmetric Measures

		Value	Approximate Significance
Nominal by Nominal	Phi	,146	,727
	Cramer's V	,104	,727
	Contingency Coefficient	,145	,727
N of Valid Cases		406	

RÖVIDÍTÉSEK JEGYZÉKE

Rövidítés	Magyar megnevezés	Idegen nyelvű megnevezés
ACT	Szövetséges Transzformációs Parancsnokság	Allied Command Transformation
API	alkalmazásprogramozási interfész	Application Programming Interface
app	alkalmazás	application
C2C	egyének közötti vásárlás	consumer to consumer
CA		Cambridge Analytica
CaaS	Szolgáltatás szerű bűnözés	Crime as a Service
CCD CoE	Kooperatív Kibervédelmi Kiválósági Központ	Cooperative Cyber Defence Centre of Excellence
CDMA	Kibervédelmi Hatóság	Cyber Defence Management Authorityt
CDMB	Kibervédelmi Tanács	Cyber Defence Management Board
CERT	Számítástechnikai Sürgősségi Reagáló Egységek	Computer Emergency Response Team
CIA	bizalmasság-sértetlenség-rendelkezésre állá	Confidentiality- Integrity- Availability
CIMIC	civil-katonai együttműködés	Civil-Military Co-Operation
CIRT	Számítógép incidenskezelő csoport	Computer Incident Response Team
CNO	számítógép-hálózati műveletek	Computer Network Operations
CSE		Communications Security Establishment
CYBINT	kiber hírszerzés	Cyber Intelligence
DaU	napi átlagos felhasználó	Daily Active Users
DEA		Drug Enforcement Administration
DESI	Digitális Gazdaság és Társadalom Index	Digital Economy And Society Index
DIP	Digitális Immunerősítő Program	
DJP	Digitális Jólét Program	
DNINT	digitális hálózati hírszerzés,	Digital Network Intelligence

DoS	szolgáltatásmegtagadással járó támadás	Denial of Service
DPI	mély csomagvizsgálat	Deep Packet Inspection
DSD		Defense Signals Directorate
EIV	Elektronikus információbiztonsági vezető	
ENISA	Európai Unió Hálózat- és Információbiztonsági Ügynöksége	European Network and Information Security Agency
ENSZ	Egyesült Nemzetek Szövetsége	United Nations
ENSZ BT	Egyesült Nemzetek Szövetsége Biztonsági Tanácsa	United Nations Security Council
EW	elektronikai hadviselés	Electronic Warfare
FBI	Szövetségi Nyomozó Iroda	Federal Bureau of Investigation
FININT	pénzügyi hírszerzés	Financial Intelligence
GCHQ		Government Communications Headquarters
GCSB		Government Communications Security Bureau
GDPR	Általános Adatvédelmi Rendelet	General Data Protection Regulation
GG	Google Szemüveg	Google Glass
GovCERT-Hungary	Kormányzati Eseménykezelő Központ	
Hjt.	2012. évi CCV. törvény a honvédek jogállásáról	
Hszt.	2015. évi XLII. törvény a rendvédelmi feladatokat ellátó szervek hivatásos állományának szolgálati jogviszonyáról	
HVK	Honvéd Vezérkar	
HUMINT	emberi erővel folytatott információszerzés	Human Intelligence
IÁ	Iszlám Állam	Islamic State

Ibtv.	2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról	
IKT	infokommunikációs technológia	Information and Communications Technology
IMINT	képfelderítés	Image Intelligence
INFOSEC	információbiztonság	Information Security
Infotv.	2011. évi CXII. törvény az információs önrendelkezési jogról és információszabadságról	
IOCTA	Szervezett bűnözés internetes fenyegetettsége	Internet Organised Crime Threat Assessment
iOS	iPhone Operációs Rendszer	iPhone Operation System
IP	Internetprotokoll	Internet Protocol
ISAF	Nemzetközi Biztonsági Közreműködő Erő	International Security Assistance Force
ITU	Nemzetközi Távközlési Egyesület	International Telecommunications Union
KLE	kulcsfontosságú vezetőkkel kapcsolatos tevékenység	Key Leader Engagement
Lrtv.	2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről	
OIMSZ	online identitásmenedzselő szoftver	
OPSEC	műveleti biztonság	Operation Security
OS	Operációs Rendszer	Operation System
OSINT	nyílt forrású információszerzés	Open-Source Intelligence
MASINT	mérés- és jelmeghatározó hírszerzés	Measurement and Signature Intelligence
MaU	havi átlagos felhasználó	Monthly Active Users

MEDINT	orvosi hírszerzés	Medical Intelligence
MH	Magyar Honvédség	
MH HKNYP	MH Hadkiegészítő és Központi Nyilvántartó Parancsnokság	
MILDEC	megtévesztés	Military Deception
MTA	Magyar Tudományos Akadémia	
NAIH	Nemzeti Adatvédelmi és Információszabadság Hatóság	
NATO	Észak- Atlanti Szövetség	North Atlantic Treaty Organisation
NBSZ	Nemzetbiztonsági Szakszolgálat	
Nbtv.	1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról	
NCIRC TC	Számítógépes Incidenskezelő Képesség Technikai Központ	NATO Computer Incident Response Capability Technical Centre
NIS irányelv	Hálózati és információs rendszerek biztonságáról szóló irányelv	The Directive on Security of Network and Information Systems
NKE	Nemzeti Közszolgálati Egyetem	
NKI	Nemzeti Kibervédelmi Intézet	
NMHH	Nemzeti Média- és Hírközlő Hatóság	
NSA	Nemzetbiztonsági Ügynökség	National Security Agency
PC	személyi számítógép	Personal Computer
PET	privát szférát erősítő technológiák	Privacy Enhancing Technologies
PPP	megjelenés, viselkedés, arculat	Presence, Posture, Profile
PSYOPS	lélektani műveletek	Psychological Operations
Q	negyedév	quarter
SIGINT	elektronikai felderítés	Signals Intelligence
SOCMINT	közösségi médiában folytatott hírszerzés	Social Media Intelligence
SOPA	Online kalózkodás elleni törvény	Stop Online Piracy Act
SJR	SCImago Folyóirat Rangsor	Scimago Journal Rank

TAM	technológia elfogadás modell	Technology Acceptance Model
TECHINT	technikai hírszerzés	Technical Intelligence
VoIP	internetprotokoll feletti hangátvitel	Voice over IP
VPN	virtuális magánhálózat	Virtual Private Network