KÖZÖSSÉGI MÉDIA ÉS KÖZSZOLGÁLAT

Bányász Péter

NEMZETI KÖZSZOLGÁLATI EGYETEM
BUDAPEST

SZÉCHENYI 2020
MAGYARORSZÁG KORMÁNYA
Európai Unió
Európai Szociális Alap
BEFEKTETÉS A JÖVŐBE

KÖZÖSSÉGI MÉDIA ÉS KÖZSZOLGÁLAT

Szerző:
Bányász Péter

A kézirat lezárásának dátuma:
2018. augusztus 21.

Kiadó:
Nemzeti Közszolgálati Egyetem Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

A kiadvány a KÖFOP-2.1.2-VEKOP-15-2016-00001 azonosítószámú,
„A jó kormányzást megalapozó közszolgálat-fejlesztés” című projekt
keretében készült el és jelent meg.

TARTALOM

ELŐSZÓ

Napjainkban szinte közhelynek számít a kijelentés, hogy a közösségi média sok tekintetben átformálta életünket. Első ránézésére csupán a kapcsolattartási formákban hozott változást, azonban hatásai majd' mindegyik társadalmi alrendszerbe begyűrűztek.

A közösségi média mára nem csupán a szabadidőnk jelentős részét tölti ki, ott van velünk utazás közben, az iskolákban, a munkahelyeken. Ez a fajta elterjedtség azonban új típusú kihívásokat is magával hozott. 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 katasztrófaesemény során kríziskommunikációra használjuk. De ahogy minden éremnek két oldala van, úgy a pozitívumok mellett rengeteg kihívást, kockázatot, fenyegetést is jelenthetnek egyben, amik sok esetben kapcsolódnak a honvédelmi, rendvédelmi-, nemzetbiztonsági szolgálatok, az állami és önkormányzati szervezetek működéséhez, ahogy a politikai szereplők szempontjából is elsődleges a megfelelő használatuk. 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.

A közszolgálatot hivatásuknak választók különösen értékes célpontot jelentenek a bűnözőknek, idegen államok nemzetbiztonsági szolgálatainak. Ennek rendkívül egyszerű okai vannak: vagy hozzáférhetnek olyan információhoz, ami aranyat érhet a támadóknak, vagy ha nincs megfelelő jogosultságuk a megszerezni kívánt információkhoz, rajtuk keresztül hozzáférhetnek a védett rendszerekhez.

A hírszerzés-történelemben nem számít újdonságnak, hogy az egyes szolgálatok még fiatalon, egyetemi éveik idején szervezték be a célpontokat, folyamatosan egyengetve a későbbiekben a karrierjüket, hogy végül értékes pozícióba kerüljenek; hiszen sokkal nehezebb lehet valakit úgy behálózni, hogy több évtizedes rutinja alakult már ki, illetve a veszteni valója is sokkal nagyobb. Erre a legjobb példával a híres Cambridge-i Ötök szolgál, ami egy rendkívül sikeres szovjet kémhálózat volt Kim Philby vezetésével. Az elnevezés az 1930-as évekre nyúlik vissza, ekkor sikerült Alexander Mihajlovics Orlov ezredesnek Kim Philbyt és társait szovjet ügynöknek beszervezni a cambridge-i Trinity College tagjai köréből. Az ideológiai meggyőződés mellett azért szerepet játszott az is, hogy az „Ötök" közül ketten, Guy Burgess és Anthony Blunt, bizonyítottan homoszexuálisok voltak, Donald Duart Maclean pedig biszexuális volt. Cambridge szinte determinálta, hogy akik ott végeztek, a későbbiekben valamilyen fontos gazdasági vagy politikai pozícióba fognak kerülni, ahogy ez az „Ötök" esetében is beigazolódott. Philby a hírszerzésért felelős MI6 tisztjeként lépdelt fokozatosan előre, mígnem a CIA és az MI6 összekötő tisztje lett belőle, így a szovjetek hozzáférést szereztek az amerikaiak szigorúan titkos adataihoz is (például a kubai partraszállás részleteihez).

Az eset tanulságai a Nemzeti Közszolgálati Egyetemre hatványozottan érvényesek. Hallgatóink a diploma megszerzését követően jó eséllyel a honvédelem, a közigazgatás, rendvédelem, nemzetbiztonság területén fognak elhelyezkedni, akik az életpályamodellnek köszönhetően karriert építhetnek. Hazánk emellett az Európai Unió és az Észak-atlanti Szövetség tagja, így a beosztásuknak megfelelően e két Szervezet által kezelt adatokhoz is hozzáférhetnek. Ennélfogva különösen fontos, hogy hallgatóink megfelelő ismeretekkel rendelkezzenek a kibertér jelentette fenyegetésekről, hogy azok ellen védekezni tudjanak.

E tankönyv ebben kíván hasznos segítséget nyújtani a közösségi média oldaláról.

1. A KÖZÖSSÉGI MÉDIA FEJLŐDÉSE

1.1. A KÖZÖSSÉGI MÉDIA KIALAKULÁSA

Az egyik legizgalmasabb írás Keith Loellhez köthető, aki a Forbes magazinban játszott el annak a gondolatával, hogy tulajdonképpen a közösségi média kialakulása a 12. századi céhek vagy Sir Isaac Newton idejére datálható-e.[1] A szerző felvetése szerint a céhek az adott szakmán belül bár roppant zárt csoportot alkottak, de a céhekben 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[2] Newton vezetése alatt megháromszorozta taglétszámát, ami egyúttal egy rendkívül élénk tudományos közéletet is teremtett. Tudósok akár hónapokat is hajlandóak voltak utazni, hogy bekapcsolódjanak abba a Londonban zajló tudományos diskurzusba, amelynek során megvitatták, csiszolták, adott esetben módosították elméleteiket, hogy aztán továbbadják az így megszületett eredményeket. A céhek azonban összességében károsak voltak az innováció és verseny szempontjából, mégis ők tekinthetőek a „társadalmi tőke" megalkotóinak, hiszen megosztották egymás közt a szabályokat, az információkat, mindezzel erős iparági és politikai befolyást értek el. A Királyi Természettudományos Társaság később pedig folyamatosan a legjobb „contentet", tartalmat állította elő – olyan fórumokat szervezett, ahol az adott témák legelismertebb szakértőit lehetett elérni. Loell megállapítása szerint mind a céhek, mind a Királyi Természettudományos Társaság üzleti alapú közösségi médiaplatformok 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;
- biztosítani kell a vitákban részt vevőknek a társadalmi elismertségért folytatott versenyt.

Bár a két analógia csalóka, mindenesetre remekül szemlélteti, hogy a társadalmakban mindig is megvolt az erős közösségszervező igény, de az infokommunikációs technológiák elterjedésével, az idő- és térbeli korlátok leomlásával a kapcsolattartás lehetősége kiszélesedett.

---

[1] LOELL, Keith (2013): Did Sir Isaac Newton Invent Social Media? In: Forbes, 2013. április 18. URL: http://www.forbes.com/sites/gyro/2013/04/18/did-sir-isaac-newton-invent-social-media/ (Letöltés ideje: 2017. június 26.).

[2] A The Royal Society of London for Improving Natural Knowledge a legősibb angol tudományos társaság. A Társaság rövid időn belül meghatározóvá vált világszerte, amit a politikai és vallási kérdések vizsgálatától való szigorú elzárkózásának tudható be. A Társaságról bővebben lásd: https://royalsociety.org/.

1.2. A KÖZÖSSÉGI MÉDIA FOGALMA

A Loell által megfogalmazottakat azért is tartom helyesnek, mert alapot nyújtanak az általam elfogadásra javasolt közösségimédia-fogalomnak. A közösségi média meghatározására rengeteg kísérlet született az elmúlt évtizedben. Kezdetekben alapvetően a marketing tudományterületéről származó fogalmakkal találkoztunk..[3]

Az Oxford Dictionaries[4] a közösségi médiát weboldalak és alkalmazások összességeként írja le, amelynek során a felhasználók tartalmat készíthetnek és oszthatnak meg a közösségi hálózatokon. Ehhez a definícióhoz köthetők az Andreas Kaplan és Michael Haenlein által megfogalmazottak, miszerint 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"*.[5]

Elfogadva, mégis kiegészítve Kaplan és Haenlein meghatározását én közösségi média alatt olyan internetes oldalak és alkalmazások összességét értem, amelyben a felhasználók állítják elő a tartalmat, a szolgálatók csupán a keretet biztosítják. Ebből következik, hogy a közösségi média a felhasználói interakcióból alakul ki, azonban ez a tartalom állandóan változhat a többi felhasználó interakciója révén. Így a tartalom, a Loell gondolatkísérletében megfogalmazottakhoz hasonlóan, folyamatosan csiszolódhat a vita az új információk hatására. Látszólag nincs számottevő eltérés a Kaplan és 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 közötti interakcióra épülnek, másrészt integratív szerepet töltenek be a különböző közösségi eszközök között. Megítélésem szerint ezt a Google példája igazolja leginkább: a kezdetben keresőszolgáltatóként működő cég mára egy személyben integrálja a különböző közösségi eszközöket (blogszolgáltató, fénykép- és videómegosztó, közösségi hálózat, okostelefon-platform stb.).

1.3. A KÖZÖSSÉGI MÉDIA EVOLÚCIÓJA

Az integráció okát gazdasági szempontok magyarázzák, hiszen az online marketing piaca évről évre jelentős mértékben növekedik, amelyből a cégek a lehető megnagyobb részt szeretnék kihasítani. Mindez egy rendkívül kiélezett innovációs versenyhez vezet a vállalatok között. A 2002-ben megalapított magyar fejlesztésű IWIW tökéletesen példázza ezt: a kezdetben óriási sikernek örvendő közösségi hálózat globális szinten képtelen volt felvenni a versenyt a megmerevedett struktúrájából következően, így a Facebook magyarországi megjelenését követően eljelelentéktelenedett, majd hosszas agonizációt követően megszűnt. Mindezt úgy, hogy egy időben Magyarországon az IWIW szinte egyet jelentett az internettel, számos esetben az átlag felhasználók nem az internetet köttették be, hanem az IWIW-et.

---

3 Heidi Cohen, marketingszakértő gyűjtött össze 30 közösségi médiafogalmat, amelyről bővebben lásd: COHEN, Heidi (2011): 30 Social Media Definitions. In: HeidiCohen.com, 2011. május 9. URL: http://heidicohen.com/social-media-definition/ (Letöltés ideje: 2017. június 26.).

4 Definition of social media in English, In: Oxford Dictionaries. URL: http://www.oxforddictionaries.com/definition/english/social-media (Letöltés ideje: 2017. június 26.).

5 KAPLAN, Andreas – HAENLEIN, Michael (2010): Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, volume 53. issue 1.

Nem véletlen tehát, hogy a piacvezető oldalak mindent megtesznek annak érdekében, hogy a felhasználókat továbbra is megtartsák az oldalukon. Egy olyan környezetben, ahol egy jó ötlet könnyen átrendezheti a teljes piacot, nem egyszerű feladat elérni ezt. Éppen ezért igyekeznek felvásárolni a cégek már a kezdetek kezdetén azokat a startupcégeket, amelyek vetélytársaik lehetnek, és elcsábítják a felhasználókat. Nem egy esetben irreálisnak tűnő összegeket hajlandóak ezért fizetni: 2014-ben a Facebook 19 milliárd dollárért vásárolta meg a WhatsApp nevű üzenetküldő alkalmazást, holott 2012-ben, amikor az Instagram 1 milliárd dollárért kelt el, mindenki elképzelhetetlennek tartotta, hogy ennyit érhet egy alkalmazás.

> Természetesen ebből következik, hogy sok startup csak egy ötletet akar eladni a fejlesztési ciklus fázisában, remélve, hogy olyat találnak ki, amit egyből felvásárol egy óriás. Ily módon a startupok esetében is megfigyelhető egy olyan tendencia, ami mind üzletmodelljüket, mind fejlesztéseiket illetően igen csak irreálisnak mondhatóak. Szakértők szerint a közösségi hálózatok fejlesztését és a legújabb mobilalkalmazásokat fejlesztő startupcégek dinamikus növekedése és a befektetett milliárdok újabb dotcomlufihoz vezethetnek.

Amennyiben nem sikerül egy céget felvásárolni, úgy igyekeznek a szolgáltatást valami módon integrálni. A Facebook évekig próbálta felvásárolni a Snapchatet, azonban rendszeresen visszautasították. 2017-re így a Facebook a „Napom" funkcióval igyekszik integrálni a Snapchat népszerű szolgáltatásait.

A WhatsApp, Instagram, Snapchat nem véletlenül olyan értékes a Facebook számára. Az oldal régóta küzd azzal, hogy az Egyesült Államokban a fiatalok, különösen a tizenévesek tömegesen pártolnak el tőle. A Facebookot a fenti három oldalra cserélték, így nem maradt más hátra, mint a felvásárlás vagy a szolgáltatások másolása.

A felhasználók megtartásának egy másik fontos eszköze, hogy olyan tartalmat lásson a user, ami érdekli. A Facebookon egy átlag felhasználónak több száz, gyakran ezer közeli ismerőse van. Ha valamilyen módon nem szabályozzák, elkerülhetetlen, hogy ne fulladjunk a megosztott tartalomba. Mindenki számára vannak érdekes tartalmak, személyek, akiknek a megosztásaira elsősorban kíváncsiak vagyunk, ez azonban rendkívül speciális. Ha minden tartalom ömlesztve jelenne meg, akkor a számunkra értékes, érdekes megosztások minden bizonnyal elvesznének az érdektelen tartalmak tengerében.

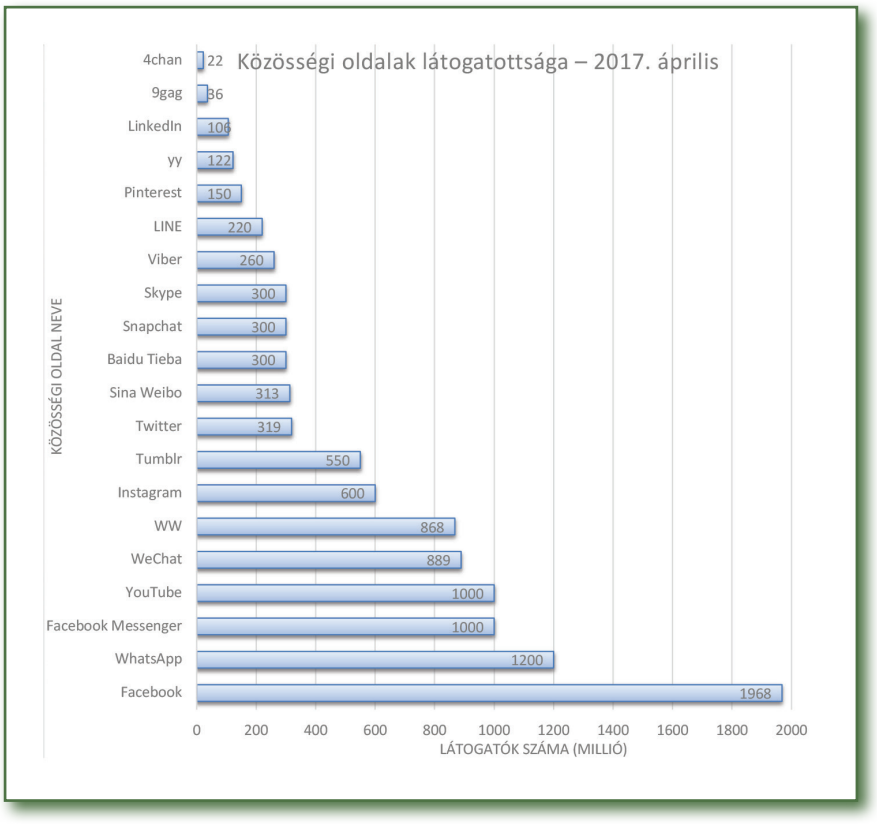
Annak érdekében, hogy a felhasználó számára a lehető legérdekesebb tartalmat jelenítsék meg, a nagy közösségi oldalak számos szempont alapján elemzik a felhasználókat. Maguknak az algoritmusoknak a pontos működése nem ismert, csupán részinformációkat ismerünk. A Facebook több mint 29 ezer szempont alapján vizsgálja a felhasználók viselkedését – ebből nagyjából hatszázra tehető azon indikátorok száma, amelyeket külső adatbrókerektől vásárolnak meg:

- az olyan egyértelmű dolgoktól kezdve, hogy kikkel beszélünk, kiknek kattintunk leggyakrabban a megosztásaira, milyen tartalmakat likeolunk, stb.;
- az olyan kevésbé evidens, ám érhető dolgokon keresztül, hogy hol tartózkodik általában az egerünk böngészés közben (a hirdetések elhelyezése okán fontos);
- az olyan nehezen magyarázható dolgokig bezárólag, hogy milyen tartalmat töröltünk ki, mielőtt elküldtük volna ismerőseinknek.

Ez utóbbit egy, a Facebook által végzett kutatásból tudjuk, amit hivatalosan az öncenzúra vizsgálatával indokolt a cég.[6] Nem nehéz belátni, ha ennyi adatot feldolgoznak rólunk, annak nem csak a marketing terén van értéke.

1.4. A KÖZÖSSÉGI MÉDIA TRENDJEI

A fejezet kezdetén szükséges rögzíteni, hogy várhatóan, amire a Tisztelt Olvasó a kezében tartja e könyvet, a bemutatott adatok nem lesznek a legfrissebbek. Ez azonban abban a tekintetben nem jelent problémát, hogy a közösségi média használatban megfigyelhető trendeket világosan jelzi, így következtetni lehet belőlük az adott oldalak népszerűségére. 2017 nyarán, e tankönyv írásának idején egyértelműen a Facebook tekinthető a legnépszerűbb közösségi oldalnak, ahogyan ez az 1. számú ábráról is leolvasható.[7] Az ábrán nem a napi elérések adatai (daily active user, DaU) szerepelnek, hanem a regisztráltak száma, kivéve a 9gag esetében, ott a Facebook-oldal követőinek a száma látható (36 millió). A Facebook népszerűsége okán érdemes az oldal DaU-ját is figyelembe venni, ami a 2017-es első negyedévi jelentés alapján 1,28 milliárd embert jelent.[8]



1. ábra: Közösségi oldalak látogatottsága 2017. áprilisában

Forrás: Statista.com, saját szerkesztés

[6] Das, Sauvik – Kramer, Adam (2013): Self-Censorship on Facebook, In: Facebook Research, URL: https://research.fb.com/wp-content/uploads/2016/11/self-censorship-on-facebook.pdf (Letöltés ideje: 2017. június 26.).

[7] Most famous social network sites worldwide as of April 2017, ranked by number of active users (in millions), In: Statista.com. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Letöltés ideje: 2017.június 26.).

[8] Facebook Reports First Quarter 2017 Results, In: Facebook Investor Relations, 2017. május 3. URL: https://investor.fb.com/investor-news/press-release-details/2017/Facebook-Reports-First-Quarter-2017-Results/default.aspx (Letöltés ideje: 2017.június 26.).

A We are social nevű online marketingre szakosodott reklámügynökség globális felméréseit alapul véve megállapíthatjuk, hogy 2018. januári adatok szerint az aktív internet felhasználók száma meghaladja a négymilliárd főt.[9] A közösségi médiaprofilok száma közel 3,2 milliárd főre tehető, ami 13%-kal magasabb, mint egy évvel korábban. Ebből a mobileszközről való elérés közel hárommilliárd felhasználói számot jelent, ez 14%-os éves növekedés (1. számú táblázat).

	Felhasználók száma (milliárd fő)	Penetráció aránya (%)	Éves növekedés aránya (millió fő)	Éves növekedés aránya (%)
Aktív internetfelhasználók	4,021	53	248	7
Aktív közösségi médiaprofilok	3,196	42	362	13
Egyéni mobilelőfizetők	5,135	68	218	4
Aktív mobilközösségi médiaprofilok	2,958	39	360	14

1. táblázat: Internet- és közösségi médiahasználat globális szinten, 2018. január

Forrás: We are social, saját szerkesztés

De mi a helyzet Magyarországgal? A 2018-as Digitális Gazdaság és Társadalom Index (DESI) mérése alapján hazánkban a közösségi médiahasználat 84%-ra tehető az internetezők körében.[10] Az Európai Unióban ezzel az első helyen szereplünk, az Uniós átlag csupán 65%. Ez mindenképpen figyelemreméltó eredmény úgy, hogy Magyarország egyéb területeken igen komoly lemaradásban van a DESI mérései alapján.

A We are social 2017-es Digitális Évkönyvét[11] alapul véve Magyarország vonatkozó adatai a 2. táblázatban szerepelnek.

Népesség szám (millió fő)	Internethasználók száma		Aktív közösségimédia-használók száma		Aktív mobilelőfizetések száma		Aktív közösségi médiahasználók mobilról	
	millió fő	penetrá-ció	millió fő	penetrá-ció	millió fő	penetrá-ció	millió fő	penetrá-ció
9,71	7,67	79 %	5,8	60 %	7,86	81 %	4,80	49 %

2. táblázat Magyarország internet- és közösségimédia-használata

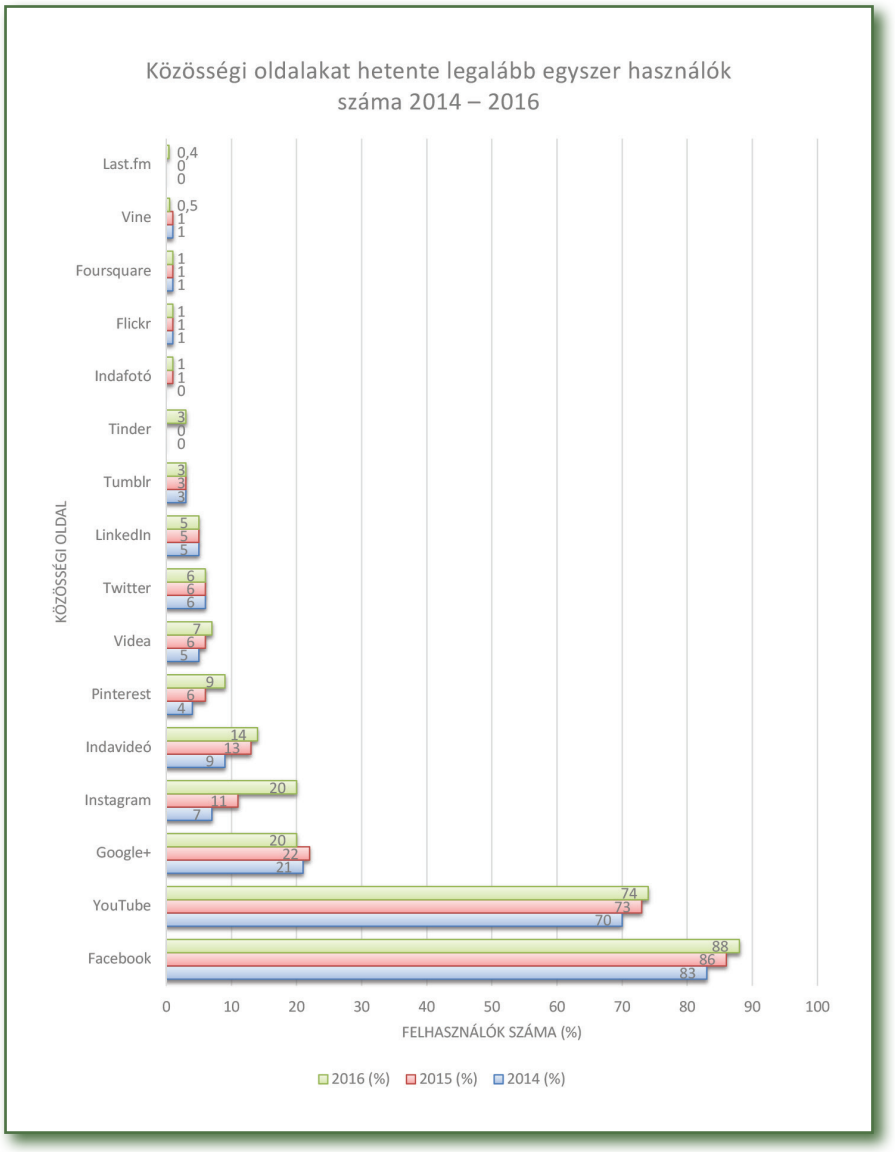
Forrás: We are social, saját szerkesztés

[9] Kemp, Simon: Global Digital Report 2018., We are social, 2015. január 21. URL: https://digitalreport.wearesocial.com/ (Letöltés ideje: 2018. augusztus 21.)

[10] Európa digitális fejlődéséről szóló jelentés (EDPR), 2018 – Országprofil Magyarországról. In: Európai Bizottság. URL: http://ec.europa.eu/information_society/newsroom/image/document/2018-20/hu-desi_2018-country-profile-lang_4AA43283-EC48-996F-09918493E34A691F_52334.pdf (Letöltés ideje: 2017. augusztus 21.)

[11] Kemp, Simon (2018): Digital in Eastern Europe. In: We are social, 2018. január 29., URL: https://www.slideshare.net/wearesocial/digital-in-2018-in-eastern-europe-part-2-east-86865266 (Letöltés ideje: 2018. augusztus 21.)

A Nemzeti Média- és Hírközlési Hatóság lakossági internethasználatra vonatkozó 2016-os felmérése alapján[12] az előző évhez hasonlóan a vonatkozó évben is 95% volt azon 16 évesnél idősebbek aránya, akik hetente legalább egy alkalommal meglátogattak valamilyen közösségi oldalt. A 2. ábrán látható, hogy hazánkban a Facebook- és a YouTube-használat mellett minden egyéb oldal látogatottsága rendkívül alacsonynak mondható. Jelentősnek tekinthető növekedést csupán az Instagram ért el, ami igazolja a Facebook felvásárlásának helyességét.



2. ábra: Közösségi oldalakat hetente legalább egyszer használók száma Magyarországon 2014–2016

Forrás: NMHH, saját szerkesztés

[12] NMHH: Lakossági internethasználat – Online piackutatás 2016., Ariosz Kft., NRC Kft. In: Nemzeti Média- és Hírközlési Hatóság. URL: http://nmhh.hu/dokumentum/187704/lakossagi_internethasznalat_2016.pdf (Letöltés ideje: 2017. június 26.).

Alapul véve az NMHH kutatását, a 3. számú ábrán látható, mik a közösségi oldal használatának okai. Ebből megállapítható, hogy a felhasználók jelentős többsége (78%-a) a barátokkal, családtagokkal való kapcsolattartásra használhatja. Érdekesség, de a globális trendeknek szintén megfelel, hogy a válaszadók közel fele (49%) elsődleges hírforrásként tekint a közösségi oldalakra. Ez a Facebook esetében egy tudatos stratégiaváltás eredménye is volt; gyakorlatilag rákényszerítették a mainstream híroldalakat, hogy a Facebook játékszabályait vegyék figyelembe a tartalommenedzsment szempontjából. Ennek, mint később látni fogjuk, több nem várt, igen súlyos következménye lett napjainkra.

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 híresség gel (pl. színésszel, zenekarral, politikussal)	5

3. táblázat: A közösségi médiahasználat okai százalékos megoszlás szerint

Forrás: NMHH, saját szerkesztés

1.5. A KÖZÖSSÉGI MÉDIA ALKOTÓI

A fogalmi meghatározást alapul véve a közösségi média alkotói tehát a különböző közösségi hálózatok, blogok, mikroblogok, videó- és fényképmegosztó oldalak, fórumok, illetve különböző okostelefonra optimalizált alkalmazások (továbbiakban appok), amelyek megfelelnek a tartalom előállítás-megosztás kritériumának.

Az 1. számú ábrán számos, talán ismeretlen közösségi oldallal is találkozott az olvasó, amelyek Észak-Amerikában vagy Nyugat-Európában kevésbé ismertek, azonban más területeken nagy népszerűségnek örvendenek (ilyen például a kínai Sina Weibo). Az ábrán nem csupán közösségi hálózatokat találhatunk, több csevegő alkalmazás helyet kapott (például WhatsApp, Facebook Messenger, Skype, Viber), de kép- és videómegosztó oldalakat, blogokat, fórumokat (például 4chan) is láthatunk.

Sokatmondó, hogy a Similar Web – internetes forgalmat figyelő honlap – top 10-es listája az alábbiak szerint alakult:[13] Google, Facebook, YouTube, Yahoo, VKontakte, Wikipedia, Twitter, Live, Google.com.br, Amazon. Az Amazont leszámítva mindegyik oldal beletartozik a közösségi média fogalmába. A Google-t a korábban kifejtett integratív tulajdonsága alapján sorolom ide. Érdekességként megemlíthető, hogy a 11. helyen a kínai Baidu nevű közösségi oldal szerepel.

Az alábbiakban áttekintjük a főbb, Magyarországon elterjedt közösségi oldalakat, amelyek a tankönyvben többször említésre kerülnek majd a későbbiekben.

Facebook

Az oldalt 2004-ben alapította Mark Zuckerberg a Harvard Egyetemen. Kezdetben csak a hallgatók számára volt elérhető a szolgáltatás, de a Facebook hamar népszerűvé vált a diákok körében, amit a fejlesztők előbb a többi egyetem hallgatói előtt is megnyitottak, majd továbblépve 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 népszerűségének növekedésével párhuzamosan folyamatosan új funkciókkal bővült (például videóchat), illetve számos egyéb szolgáltatást integrált magába (például Instagram, Paper). A Facebookot 2012-től a tőzsdén is jegyzik.

Instagram

Az eredetileg iOS-re készített Instagram egy képmegosztó szolgáltatás, amely az általa használt filterek, szűrők, effektek hatására rendkívül népszerűvé vált a fiatalok körében. A 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 vásárolta fel 2012-ben.

[13] Top Website Ranking. In: Similar Web. URL: https://www.similarweb.com/top-websites (Letöltés ideje: 2017.június 26.). Top Website Ranking. In: Similar Web. URL: https://www.similarweb.com/top-websites (Letöltés ideje: 2017.június 26.).

Twitter

A 2006-ban alapított Twitter egy közösségi hálózat és mikroblog-szolgáltatás, amelyen a felhasználók maximum 140 karakterben állíthatnak elő tartalmat (úgynevezett tweeteket). Az oldallal szemben indulása után bár sok kritikát fogalmaztak meg, azonban miután az oldal fejlesztői elérhetővé tették a Twitter alkalmazásprogramozási interfészét[14] (továbbiakban API), rengeteg olyan fejlesztés és mash-up[15] jelent meg, amelyek figyelembe vették a felhasználók igényeit. A Twitter mozgósításban betöltött szerepét a 2011-es „Arab tavasz" eseményei messzemenően igazolták. A tőzsdei bejegyezésre 2013-ban került sor.

Google

Amennyiben elfogadjuk az általam javasolt közösségimédia-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 közt matematikai analízisen alapuló kapcsolat áll fenn, amit felhasználva jobb keresési eredményeket lehet adni – ez az úgynevezett PageRank.[16] E tézis igazolására hozták létre a Google keresőrendszerének alapjait. Az egyszerű kezelhetőségnek, a releváns találati eredményeknek köszönhetően gyorsan népszerűvé vált. Napjainkra a Google több tucat különböző szolgáltatással, eszközzel bővítette profilját, mint például 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+), fordítóprogram (Translate), naptár (Calendar), csevegő (Hang Outs), 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

[14] 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.

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

[16] A szabadalmaztatott PageRank a fontosság számszerűsítése, egy olyan algoritmus, amely hiperlinkekkel összekötött dokumentumokhoz számokat rendel azoknak a hiperlinkhálózatban 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 (például úgynevezett „comment spamek" segítségével, amelyek linkek elhelyezését jelentik hozzászólásokban, vendégkönyvekben, vagy úgynevezett linkfarmok alkalmazásával, amelyek olyan weboldalak használatát jelentik, 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.

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.

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 (például 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.

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 mobileszközökről tekintik meg. A felhasználók percenként 300 órányi tartalmat töltenek fel, amely amatőr videókból és jogvédett tartalmakból (zenék, filmek) tevődik össze.

Wikipedia

A 2000-ben alapított Wikipédia egy többnyelvű, nyílt tartalmú, közösség által szerkesztett webalapú enciklopédia. Világszerte 39 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 wikirendszerű, a Wikipédiától független oldal létezik. A szabadon szerkeszthetőség nem egy esetben pontatlan információközléssel járhat, és több esetben derült ki, szándékos félrevezetéssel írtak meg egy-egy szócikket.[17]

[17] 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 moziadatbázisban, az IMDB-n is külön szócikket, illetve Facebook rajongói oldalt is készítettek. Bővebben lásd: Leleplezték a Wikipedia legnagyobb átverését. In: Index, 2013. május 5. URL: http://index.hu/tech/2013/05/01/lelepleztek_a_wikipedia_legnagyobb_atvereset/ (Letöltés ideje: 2017. június 26.).

Reddit

A 2006-ban indított Reddit egy közösségi hírmegosztó oldal, ahol a felhasználók úgynevezett alredditeket segítségével állíthatják elő a tartalmat, ami alapvetően híreket, cikkeket, képeket megosztásával, moderálásával keletkezik.[18] A felhasználók értékelhetik, kommentelhetik a tartalmat.

4chan

A 2003-ban létrehozott 4chan egy fórumszolgáltatás, ahol az alapvetően anonim felhasználók különböző tartalmakat osztottak meg egymással. Az oldal jelentősége a hacktivizmusban[19] jelentkezik; az Anonymous hackercsoport[20] az oldal felhasználóiból rekrutálódott.

Tinder

A Tinder egy 2012-ben létrehozott, tabletre, okostelefonra optimalizált társkereső alkalmazás. A felhasználók száma 2015 áprilisában 40 millióra tehető.[21] Úgy vélem, az alkalmazás alátámasztja, hogy egyes appokat a közösségi média alkotói közé soroljuk. A használatához Facebook-regisztráció szükséges, illetve a fejlesztők integrálták az Instagramot a szolgáltatásba. Miután a felhasználók párbaállnak, azt követően lehetőségük nyílik szöveges üzenetet váltani egymással, egy időben lehetőség volt fényképeket megosztani egy „Pillanatok"-nak nevezett üzenőfalon, ahol véleményezhették a párok által megosztott fényképeket.

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.

---

18 Ebből ered az oldal neve is, az angol „read" és „edit", azaz olvas és szerkeszt szavak összevonásából, illetve a „read it", azaz elolvasta.

19 A fogalomról bővebben: lásd 2.3. fejezet.

20 Az Anonymous hacktivista közösség decentralizált, egymáshoz lazán köthető csoportok globális hálózata. Kezdetben az internet cenzúrája ellen, az internet szabadságáért 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 WikiLeakset bojkottáló pénzügyi vállalatok, az iráni, egyiptomi, tunéziai kormányok, újabban az Al-Kaida és az Iszlám Állam. Berki Gábor (2013): A kibertéri konfliktusok változása. In: Hadmérnök, VIII/1. szám, pp. 173–185.

21 Tinder Information, Statistics, Facts and History. In: Dating Sites Reviews. URL: http://www.datingsitesreviews.com/staticpages/index.php?page=Tinder-Statistics-Facts-History#ref-ODS-Tinder-2015-5 (Letöltés ideje: 2015. július 10.).

Fontosabb fogalmak

Digitális gazdasági és társadalmi index, közösségi média, napi elérés, tartalomgyártás, web 2.0.

Áttekintő kérdések

1. Ön hogyan definiálná a közösségi média fogalmát?
2. Ön szerint minek van a legnagyobb hatása a közösségi oldalak fejlődésére?
3. Ön szerint mi lesz a következő lépcsőfok a közösségi média evolúciójában?
4. Megítélése szerint a közösségi média hatására a világunk kitágult vagy beszűkült?
5. Hasznosnak találja a személyre szabott reklámokat, mint a Facebook és a Google reklámjai?

2. KOCKÁZATOK, KIHÍVÁSOK, FENYEGETÉSEK A KIBERTÉRBEN

2.1. A BIZTONSÁGRÓL ÁLTALÁBAN

A biztonság szó a latin „securus" szóból (se = nélkül, cura = aggodalom, félelem) ered. Meghatározására számos kísérlet született, azonban leegyszerűsítve a fenyegetettség hiányát vagy a fenyegetés kivédésének képességét jelenti. A biztonság sajátos, fenyegetettség nélküli állapot, illetve kockázatmentes helyzet, amikor az elméleti veszélytényezők aktiválódása nem várható. Ebben a helyzetben nincs szükség különböző biztonsági intézkedések megtételére.[22] Másképpen megfogalmazva: a biztonság nem más, mint egy rendszer állapota. Egy olyan kedvező állapot, amelyben kellemetlen meglepetésnek, zavarnak, veszélynek, fenyegető hatásoknak nincs vagy alig van lehetősége, illetve amelyben ilyentől nem kell félni.[23]

A biztonságot szűkebb és tágabb dimenzióban értelmezhetjük. Szűkebb körébe tartozik:

- az egyéni biztonság, amely az egyén azon képessége, hogy megvédje magát a különféle káros behatásoktól (környezet, másik ember), biztosítsa fizikai létét;
- a kollektív biztonság az emberek csoportjának, kis közösségnek (család) biztonsági rendszerét foglalja magában;
- illetve a nemzeti biztonság, amely egy nemzet közössége által elfogadott értékek, érdekek védelme. A legnagyobb veszély ebben a dimenzióban más államok agressziója.

Tágabb dimenzióban a nemzetközi biztonságot értjük, amelynek középpontjában az áll, hogy az államok biztonsága összekapcsolható, együttműködés segítségével kölcsönösen erősíthető. Az együttműködéshez megfelelő szervezeti keretek szükségesek, amelyek lehetővé teszik az államok véleménycseréjét, valamint érdekeik harmonizálását a gazdaság, a külpolitika, a biztonságpolitika és a védelem területén.

A hidegháború idején a biztonságot alapvetően a katonai biztonság primátusa jellemezte, azonban a bipoláris világrend felbomlásával paradigmaváltás ment végbe a biztonsági tanulmányokban. Ennek hatására Barry Buzan és társai értelmezésében a biztonság fogalma kiszélesedett, munkásságuk nyomán megkülönböztetünk katonai, politikai, gazdasági, társadalmi és környezeti biztonságot.[24]

A fenyegetettség nélküli állapot azonban nem természetesen, nem önmagában valósul meg, így védelmi eszközök sorát kell alkalmaznunk, hogy létrejöjjön.

---

22 HAIG Zsolt (2015): Információ – társadalom – biztonság. NKE Szolgáltató Kft., Budapest.

23 MUNK Sándor (2007): Információbiztonság vs. informatikai biztonság. Hadmérnök, 2007/különszám. URL: http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html (Letöltés ideje: 2017. július 12.).

24 BUZAN, Barry – WÆVER, Ole – DE WILDE, Jaap (1997): A New Framework for Analysis, Lynne Rienner Publishers.

A Hadtudomány Lexikont segítségül hívva biztonságpolitikai kihívások, kockázatok és fenyegetések *„azok […] a veszélyt és fenyegetést magukban hordozó helyzetek és állapotok, amelyek általában negatívan befolyásolják az adott országban az átfogó biztonságot, annak egyes összetevőit, s gyengítik a belső és külső stabilitást."*[25]

Kölcsönözve Resperger István megfogalmazását: *„a biztonsági kockázatot az általános meghatározásból következően, a biztonsági dimenziók vonatkozásában értelmezhetjük. A fenyegetés a veszély konkrét, cselekvési szándékot is megjelenítő formája, amelynek célja a célország magatartásának befolyásolása a saját érdek érvényesítésére. Főként akkor beszélhetünk fenyegetésről, ha bizonyos érdekütközések kikényszerített vagy erőszakos úton történő megoldására van kilátás. A katonai fenyegetés megítélése esetén figyelembe kell vennünk az állami, politikai akarat meglétét, és értékelnünk kell ezek katonai vonatkozásait a képesség területén. Tehát szándék és katonai képességelemzést kell készítenünk környezetünkről, elemezve azokat a lehetséges veszélyeket, amelyek hazánkra hatással lehetnek."*[26]

A kihívások ennek megfelelően az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek legalacsonyabb megnyilvánulási szintjén, amelyek eredői általában hátrányosan befolyásolják a belső és külső stabilitást, és kihatással lehetnek egy adott régió hatalmi viszonyaira.

A kockázatok ezzel szemben az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek olyan megnyilvánulási szintjén, amikor a nemzeti érdekek sérülhetnek, ezáltal veszteségek keletkezhetnek.

A fenyegetések pedig az általánosan értelmezett biztonság egyes összetevőire ható olyan helyzetek és állapotok összessége a lehetséges veszélyek legmagasabb megnyilvánulási szintjét tekintve, amikor a nemzeti érdekek sérülhetnek, és közvetve hatással lehetnek a nemzeti értékek megőrzésére.

Az érdekek képviseletének módszerei és eszközei előnyben részesítik a kikényszerítést vagy az erőszakos úton történő megoldás lehetőségét. Amint az a fogalmi meghatározásokból kitűnik, Resperger a kihívásokat, kockázatokat és a fenyegetéseket a lehetséges veszélyek megnyilvánulási formáinak tekinti, amelyek általában hátrányosan befolyásolják a belső és külső stabilitást, és hatással lehetnek egy adott régió hatalmi viszonyaira. Ezek a fogalmak egymásra épülve egyre nagyobb feszültségi szint meglétét feltételezik, jellegükből következően csak dinamikus folyamatokként értelmezhetők.

2.2. A KIBERBIZTONSÁG ALAPJAI

Amikor kiberbiztonságról beszélünk, a laikusok többsége valamilyen műszaki aspektusra asszociál. Ez a szemlélet azonban elavultnak tekinthető, ahogy ezt az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény (Ibtv) is alátámasztja. Az Ibtv. megfogalmazása alapján a kiberbiztonság *„a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva*

[25] SZABÓ József – GABRIEL Győző – HORVÁTH Ferenc (szerk.) (1995): Hadtudományi Lexikon. Magyar Hadtudományi Társaság, Budapest.

[26] RESPERGER István (2002): Kockázatok, kihívások, fenyegetések a XXI. században. Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest.

a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhezés, működtetéséhez"[27] Mint látható, messze többről szól a kiberbiztonság, mint azokról a technikai, technológiai jellegű kérdésekről, hogy pl. milyen végponti védelmet állítottunk be az informatikai eszközünkön.

De hogyan is jutunk el ehhez a szélesen értelmezett fogalomhoz? Ennek megértéséhez vissza kell térnünk az alapokhoz, az adathoz és információhoz, a két védendő fogalomhoz.

Az Ibtv. alapján az adat *„az információ hordozója, a tények, fogalmak vagy utasítások formalizált ábrázolása, amely az emberek vagy automatikus eszközök számára közlésre, megjelenítésre vagy feldolgozásra alkalmas*."[28] Az információ pedig *„bizonyos tényekről, tárgyakról vagy jelenségekről hozzáférhető formában megadott megfigyelés, tapasztalat vagy ismeret, amely valakinek a tudását, ismeretkészletét, annak rendezettségét megváltoztatja, átalakítja, alapvetően befolyásolja, bizonytalanságát csökkenti vagy megszünteti"* [29]. Nagyon leegyszerűsítve az információ feldolgozott adatot jelent.

Az adat, információ tekintetében három további fogalmat szükséges tisztáznunk, amit a CIA-rövidítéssel szokás hivatkozni: ez a bizalmasság (C mint confidentiality), sértetlenség (I mint integrity), valamint rendelkezésre állás (A mint availability).

A bizalmasság elve alatt az elektronikus információs rendszer azon tulajdonságát értjük, *„ami szerint a benne tárolt adatot, információt csak az arra jogosultak és csak a jogosultságuk szintje szerint ismerhetik meg, használhatják fel, illetve rendelkezhetnek a felhasználásáról."*[30] A sértetlenség *„az adat tulajdonsága, amely arra vonatkozik, hogy az adat tartalma és tulajdonságai az elvárttal megegyeznek, ideértve a bizonyosságot abban, hogy az az elvárt forrásból származik (hitelesség) és a származás ellenőrizhetőségét, bizonyosságát"* [31]. A rendelkezésre állás *„annak biztosítása, hogy az elektronikus információs rendszerek az arra jogosult személy számára elérhetőek és az abban kezelt adatok felhasználhatóak legyenek."*[32]

A bizalmasság, sértetlenség, rendelkezésre állás – mint látható – a biztonság és a védelem fogalompár köré szerveződik.

Mit ért az Ibtv. a kockázat és fenyegetés alatt? A kockázat a fenyegetettség mértéke, amely egy fenyegetés bekövetkezése gyakoriságának (bekövetkezési valószínűségének) és az ezáltal okozott kár nagyságának a függvénye. A fenyegetés olyan lehetséges művelet vagy esemény, amely sértheti az elektronikus információs rendszer vagy az elektronikus információs rendszer elemei védettségét, biztonságát, továbbá olyan mulasztásos cselekmény, amely sértheti az elektronikus információs rendszer védettségét, biztonságát.[33]

Mielőtt rátérnénk a kiberfenyegetettségek ismertetésére, különbséget kell tennünk az informatikai biztonság és információbiztonság között, ugyanis a közbeszédben sokszor egymás szinonimájaként alkalmazzák – tévesen.

---

27 Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény. URL: http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158 (Letöltés ideje: 2017. július 6.)

28 uo.

29 uo.

30 uo.

31 uo.

32 uo.

33 uo.

Az informatikai biztonság az Ibtv. alapján egy informatikai rendszer olyan állapota, amelyben zárt, teljes körű, folytonos és a kockázatokkal arányos védelem valósul meg. Ez azt jelenti, hogy egy, az összes fenyegetést figyelembe vevő, a rendszer valamennyi elemére kiterjedő, az időben változó körülmények és viszonyok ellenére is megszakítás nélkül megvalósuló védelmi rendszer.[34] Célja az információ korábban ismertetett biztonsági tulajdonságainak biztosítása és folyamatos fenntartása. Ennek érdekében különféle hardveres és szoftveres biztonságtechnikai eszközöket alkalmaznak az illetéktelen hozzáférések és károkozás megelőzésére (például tűzfalak, vírusírtók, hozzáférés-szabályozás) továbbá biztonsági szabályzatokat, előírásokat (jelszóhasználat, biztonsági mentés) is létrehoznak.

Ezzel szemben az információbiztonság folyamat, amelynek során az információkat megvédjük a nem engedélyezett megzavarástól, hozzáféréstől, használattól, módosítástól, megsemmisítéstől, vagy kiszivárgástól. További jellemzője, hogy magában foglalja a politikai, társadalmi, gazdasági, katonai és környezeti biztonságot. Az információbiztonságnak négy szintjét különböztetjük meg:

- személyi biztonság, amely magában foglalja a támadás veszélyének felismerését és a kiemelten fontos személyek személyi védelmét, illetve a minősített információ megfelelő személyekhez való eljuttatását;
- fizikai biztonság, amely azokat a tényleges akadályokat (falak, sorompók, torlaszok, beléptető rendszerek) jelöli, amelyek megfosztják az illetékteleneket a kritikus információkhoz, dokumentumokhoz, eszközökhöz való hozzáféréstől;
- adminisztratív biztonság, amely azt jelenti, hogy az összes dokumentumot érzékenységének, minősítésének megfelelően kell megvédeni, tehát csak azok férhessenek hozzá ezekhez a dokumentumokhoz, akik erre jogosultak, és csak a jogosultságuk szintjén tehessék ezt meg;
- az elektronikus információbiztonság (lásd információbiztonság)

2.3. A KIBERFENYEGETETTSÉG TÍPUSAI

A szakirodalom a kiberfenyegetéseket négy csoport alapján kategorizálja:

- kiberbűnözés;
- kiberterrorizmus és hacktivizmus;
- kiberkémkedés;
- kiberhadviselés.[35]

Annak ellenére, hogy a közösségi médiahasználat mind a négy kategóriában jelentős szerepet tölt be, e fejezetben csupán magukat a fenyegetéstípusokat tekintjük át, a közösségi médiával való viszonyukat később tárgyaljuk. Tekintsük át tehát, mit is értünk alattuk.

[34] uo.

[35] KRASZNAY Csaba (2012): A polgárok védelme egy kiberkonfliktusban. Hadmérnök 2012/4. p. 143. URL: http://hadmernok.hu/2012_4_krasznay.pdf (Letöltés ideje: 2017. július 12.).

Kiberbűnözés

A kiberbűnözés célja az informatikai eszközök segítségével való anyagi haszonszerzés. Az Europol minden év tavaszán közreadja a Szervezett bűnözés internetes fenyegetését vizsgáló jelentését (továbbiakban IOCTA),[36] amely 12 területet foglal magába:

1. malware-ekkel[37] (például CryptoLocker, WannaCry, NonPetya stb.) való visszaélés.
2. gyerekek szexuális kizsákmányolása;[38]
3. fizetőeszközzel elkövetett csalás;
4. social engineering;
5. adatok megszerzése, hálózatok támadása;
6. létfontosságú rendszerelemek ellen elkövetett támadások;
7. különböző pénzügyi tevékenységek (criminal-to-criminal payments, payment for legitimate services, victim payments);
8. online kommunikáció;
9. a kibertér és a terrorizmus összefonódása;
10. Darknet;[39]
11. Internet of Things, Big Data, Clouds;
12. internetirányítás.[40]

[36] Europol The Internet Organised Crime Threat Assesment 2016., Europol, Hága. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (Letöltés ideje: 2017. július 12.).

[37] Az angol malware kifejezés az angol malicious software (rosszindulatú szoftver, káros szoftver, kártékony szoftver) összevonásából kialakított mozaikszó. Idetartoznak a vírusok, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit). Az informatikai eszközökre írt kártevő programok mennyisége folyamatosan növekszik, és időről időre új típusok terjednek el.

[38] Itt nem csupán a pedofil tartalmak terjesztésére kell gondolni, hanem a szexrabszolga-kereskedelemre offline és online (például stream) formában egyaránt. Amikor gyermekek szexuális kizsákmányolásáról beszélünk, tisztában kell lenni, hogy csecsemők sérelmére is követnek el ilyen bűncselekményeket. A Darkneten több olyan hálózatot lepleztek le, amelyek több százezer képet tartalmaztak, amik csecsemők megerőszakolását ábrázolták.

[39] A Darknet a Deepweb azon része, ahol magas szintű titkosítás mellett illegális eszközöket, szolgálatásokat lehet vásárolni, legyen szó fegyverről, kábítószerkereskedelemből, bérgyilkosságról, szexuális szolgáltatásokról stb. Annyira speciális szolgáltatást nyújtanak a szervezett bűnözők, hogy ha valaki például egy egykezű, thai, 8 éves fiú szexrabszolgát szeretne vásárolni, akinek zöld a haja, zöld a szeme, crackfüggő, akkor ennek megfelelően szállítják le. A magas szintű titkosítás miatt rendkívül nehéz felderíteni az itt elkövetett illegális cselekményeket, amelyek – a példából is látható – igen súlyos bűncselekményeket foglalnak magukba.

[40] Az internetirányítás fogalma azokat a globális megállapodásokat takarja, amelyek biztosítják az internet megfelelő működését és az internethez való hozzáférést. A legfontosabb kapcsolódó témák az internethez való hozzáférés, valamint az internet biztonsága

A 2016-os IOCTA-jelentés újdonsága az előző évekhez képest, hogy megjelent benne a terrorizmus és az internetirányítás. A terrorizmus itt való szereplése nem összekeverendő a kiberterrorizmussal; a jelentés az online kapcsolattartást (hangsúlyozva a közösségi média szerepét), az online fizetőeszközökhöz kapcsolódó kereskedelmet, a Darkneten a szolgálatások, eszközök beszerzését említi. A Darkneten az elmúlt években megjelent a „Crime as a Service", vagyis a szolgáltatásszerű bűnözés, ami összekapcsolta a szervezett bűnözői köröket a feketekalapos hackerekkel,[41] így szervezett bűnözők kibertámadáshoz használható eszközöket vagy konkrét kibertámadásokat is kínálnak online ügyfélszolgálattal igény szerint. A kínált szolgáltatás a barátunk, barátnőnk Facebook-fiókjának feltörésétől, az eszközükön való irányítás átvételétől kezdve egy kikötő informatikai rendszerébe történő behatolásán[42] át a kritikus infrastruktúrák elleni támadásig bezárólag számos területre kiterjed.

A kiberbűnözés elleni harc egyik legnagyobb korlátja, hogy a kibertérben nem értelmezhetőek a klasszikus határok. Hiába magyarországi felhasználó az áldozat, nem kizárt, hogy az elkövető egy orosz hacker, aki Argentínában lopja el például a bankkártyaadatokat, és azt TOR-hálózaton, nigériai elkövetők által üzemeltett oldalon keresztül indiai csalóknak adja el. Így tehát nemcsak a felderítés válik rendkívül nehézzé, de maga a felelősségre vonás is nagymértékben bonyolódik, hiszen a különböző országokban eltérő a kiberbűnözéssel kapcsolatos jogalkotás. Éppen ezért különösen fontos egy olyan nemzetközi megállapodás, ami a jogharmonizációt megkönnyíti. A 2001-ben Budapesten megkötött Cybercrime Egyezmény így jelentős lépésnek tekinthető, amely *„a számítástechnikai bűnözésről és az elektronikus bizonyítékokról szóló legfontosabb nemzetközi megállapodás marad, nemcsak a belföldi jogszabályok iránymutatásaként és a nemzetközi együttműködés alapjaként, hanem az együttműködési kapacitásépítés katalizátoraként*."[43] Bár az Európai Unió jogharmonizációs tekintetben élen jár, azonban fontos, hogy az említett Cybercrime Egyezményt minél szélesebb körben ratifikálják.

Kiberterrorizmus és hacktivizmus

A két fogalom bár eltér egymástól, mégis több azonosságot állapíthatunk meg esetükben, hiszen a kiberterroristák és a hacktivisták az informatikai bűncselekményekkel segítik az általuk vallott ideológiák minél szélesebb körben történő terjesztését. Mindkettő esetében kisebb, decentralizált csoportok működése a jellemző.

[41] Feketekalapos (black-hat) hackernek nevezzük azokat a hackereket, akik tudásukkal visszaélve jogosulatlanul számítógépbe, illetve számítógép-hálózatokba törnek be haszonszerzés vagy károkozás céljából. Black-hat hackerek csoportjába tartoznak azok az ipari kémek, akik technológiai fejlesztések után kutatva törnek be hálózatokba. Sok black-hat válik később white-hat hackerré, sőt nagyon nehezen képzelhető el, hogy valaki úgy dolgozzon white-hat hackerként, hogy előtte soha nem próbált betörni egy számítógépbe sem. Így a határ inkább etikus és etikátlan hackerre osztható.

[42] 2013-ban egy több éve zajló nyomozásról számolt be az Europol, ami az antwerpeni kikötőt érintette. Ennek során bűnözők feltörték a kikötő informatikai rendszerét, amelynek hatására egyrészt tudták, melyik konténer mit tartalmaz, másrészt feltörték a hitelesítést, amivel át tudták venni az általuk biztonságos helyre irányított értékes konténereket. Egy idő után kábítószer- és fegvercsempészetre is felhasználták az eljárást. Nem nehéz belátni, milyen egyéb lehetőségeket is tartogathat ez.

[43] SIMON Béla (2017): Bűnüldözés előtt álló digitális kihívások. Magyar Rendészet, XVII. évf. 5. szám.

A hacktivizmus számítógépes hálózatokon, általában az interneten, speciális eszközökkel folytatott proaktív politikai aktivizmus, legtöbbször a szólásszabadság, az emberi jogok és az információ szabadsága jegyében. Főbb eszközei lényegükben a hagyományos demonstrációk és polgári engedetlenség – egyelőre el nem ismert – digitális megfelelői, illetve a nem publikus információk megszerzése és kiszivárogtatása. A hacktivisták az írott jog szempontjait az etikai, illetve morális szempontoknak rendelik alá. Magát a kifejezést 1996-ban alkotta meg a legendás Cult of the Dead Cow hackercsoport egyik tagja.

Története az 1980-as évekig nyúlik vissza. A számítógépes hackelés fogalma és szubkultúrája ekkoriban született az MIT (Massachusetts Institute of Technology) berkeiben, az egyik első, nevezetessé vált hackercsoport, a texasi Cult of the Dead Cow (A Döglött Tehén Kultusza) pedig 1984-ben alakult. A ma hacktivizmus néven ismert jelenség első ismert példája szinte egyidős az internettel: hackerek 1989 októberében a WANK (Worms Against Nuclear Killers) nevű computerféreggel fertőztek meg egy hálózatot, amely megváltoztatta a fertőzött gépek kezdőképernyőjének ábráját.

A hacktivisták motivációja mögött gyakran a társadalmi egyenlőtlenségek megszüntetése áll, filozófiájuk szerint az információhoz való hozzáférés a legmagasabb rendű jog, felülírva sok esetben az államok nemzetbiztonsági érdekeit is. Az információ érdekcsoportok általi kisajátítása rendkívül komoly gazdasági és politikai erőt jelent a birtokosainak, amely a hacktivisták szerint kizárja a széles tömegeket a társadalmi egyenlőségből, gazdasági jólétből, ezért az információk nyilvánosságra hozatala egy jobb világot eredményez.

Ez az elgondolás állt Aaron Schwartz cselekedetei mögött is. Schwartzot a környezete informatikai csodagyereknek tartotta; 14 évesen részt vett az RSS-hírcsatorna kidolgozásában, a Reddit egyik társalapítója volt. 2011-ben a Massachusettsi Műszaki Egyetem alkalmazásában állt, és az Egyetem által előfizetett tudományos adatbázisból letöltött 4,8 millió tudományos publikációt, amit nyilvánosságra hozott, piaci értékét tekintve hozzávetőlegesen 50 ezer dollár értékben. Schwartzot, miután nyilvánosságra hozta a publikációkat, napokon belül letartóztatták; 35 éves letöltendő börtönbüntetés és egymillió dolláros pénzbüntetés várt rá. 2013-ban felmerült a vádalku lehetősége, ez azonban végül meghiúsult, aminek nyomán Schwartz 26 évesen önkezével vetett véget életének. Schwartz tragédiája természetesen óriási felháborodást váltott ki hacktivista körökben, illetve forradalmat indított el a tudományos publikációk ingyenes elérhetősége kapcsán.

A tudományos közéletben rendkívül fontos, hogy a kutatók a saját tudományterületük legfrissebb eredményeit ismerjék, felhasználják. Ehhez azonban hozzá kell férni többek között azokhoz a kutatási eredményekhez, amelyeket publikációk formájában tesznek közzé. A tudományos folyóiratok megjelentetése óriási üzleti lehetőséget jelent, ami ellen az elmúlt időszakban egyre többen emelik fel a hangjukat. 2017. január 1-étől több német egyetem, például a göttingeni egyetem hirdetett bojkottot[44] a szerintük kizsákmányoló kiadókkal szemben.[45] Az adatbázisokhoz való hozzáférés azonban meglehetősen drága, így sok felsőoktatási intézmény és több kutató nem

[44] Az Egyetem közleménye angol nyelven az alábbi linken olvasható angolul: https://www.sub.uni-goettingen.de/en/news/details/voraussichtlich-keine-volltexte-von-zeitschriften-des-elsevier-verlags-ab-dem-112017/ (Letöltés ideje: 2018. január 14.)

[45] A publikációs válság okairól, a kiadók és a kutatók ellentétéről rendkívül alapos és érdekfeszítő cikket a Budapest Science Meetup közölt „A tudomány publikációs válsága (és egy lehetséges kiút)" címen, ami az alábbi linken olvasható: https://sciencemeetup.444.hu/2016/04/10/a-tudomany-publikacios-valsaga-es-egy-lehetseges-kiut (Letöltés ideje: 2018. január 14.)

engedheti meg magának, hogy licenszet vásároljon. Ezzel azonban lemaradnak a tudományos versenyben. Márpedig a tudomány deklarált célja az emberiség szolgálata.

A hacktivisták vezérlőelvét Julian Assange, a WikiLeaks jelenlegi arca fogalmazta meg: *„Ne tegyetek kárt a rendszerekben, amelyekbe betörtök (ne is omlasszátok össze őket), ne változtassátok meg az azokban tárolt adatokat (eltekintve a nyomaitok eltüntetésére irányuló naplóátírásoktól) és osszátok meg az információkat."*[46]

A hacktivisták által vallott erkölcsi kódexet az alábbiak szerint foglalhatjuk össze:

- személyes adatok maximális védelme;
- a hatalomban nem lehet megbízni, decentralizáltság;
- információ szabadsága.

Eszközök és eljárások tekintetében pedig az alábbiakat alkalmazzák:

- digitális és valós életben való polgári engedetlenség, tüntetések;
- nem publikus információk megszerzése, nyilvánossá tétele;
- túlterheléses támadások, honlaprongálások.

Az egyik legismertebb hacktivista csoport az Anonymous, ami önmagát globális hacktivista közösségként definiálja. Lazán kötődő csoportok és egyének anarchikus, decentralizált hálózata. Kezdetben főleg az internet cenzúrája ellen, az információ szabadságáért szálltak síkra, de 2011 óta nyíltan és vállaltan a fennálló világrend, politikai és gazdasági rendszer átalakításáért küzdenek. A – tévhitekkel ellentétben – korántsem csupán hackerekből álló aktivista közösség tagjai, az úgynevezett anonok gyakran puszta eszmeként vagy „digitalizált globális agyként" is hivatkoznak rá. Az ikonikussá, az anonoktól kiindulva az új típusú rendszerkritikus mozgalmak egyik meghatározó jelképévé vált Guy Fawkes-maszkot is hasonló okból viselik, az egység szimbólumaként.[47] Erőszakmentes on- és offline ellenállást hirdettek, amivel kivívták a világ számos kormányának, kormányzati szervének, nagyvállalatának és egyházának haragját. A csoportot több országban kiberterrorista szervezetnek kiáltották ki. Saját megfogalmazásuk szerint azt teszik, ami etikus, akkor is, ha az nem feltétlenül legális. Az Anonymous-jelenség története 2003-ig nyúlik vissza és a 4chan-hez, az internet talán leghírhedtebb fórumához köthető, azon belül is az úgynevezett /b/ boardhoz, a random tartalmak felületéhez, ahol „bármi belefér". Az oldalon megengedett az anomim közzététel, a csoport neve is innen származik: a névtelenül megnyilvánuló felhasználók Anonymousként jelennek meg. Az igazi áttörést azonban az úgynevezett Project Chanology hozta meg 2008 elején. A csoport figyelmét az keltette föl, hogy a Szcientológia Egyház egy belső használatra készült, ám kiszivárgott és a neten vírusként terjedő videóját a szerzői jogra való hivatkozással igyekeztek eltüntetni. Mindezt cenzúraként értékelték, és mivel egyébként is bőven találtak kivetnivalót a szcientológusok ténykedésében, hamar támadásba lendültek, bevetve a rendelkezésre álló

[46] Amir Taaki: Nincs jövő múlt nélkül. Bitcoin Portál, 2011. december 29. URL: https://bitcoin.hu/nincs-jovo-mult-nelkul/ (Leöltés ideje: 2018. január 14.)

[47] Bár ironikus a globalizációkritika, amikor a jelképük szabadalma a globális filmcég, a Warner Bros tulajdonát képezi a V mint vérbosszú című film miatt.

eszközök széles skáláját. Ezt követően egyre aktívabban hirdettek háborút különböző szervezetek ellen (mexikói drogkartellek, Iszlám Állam, Izrael állam stb.), de az esetek nagy részében inkább a saját szerepük felnagyításában voltak hangosak, mintsem valódi eredmények elérésében.

Hacktivizmus kapcsán mindenképpen szót érdemel a WikiLeaks, ami egy nemzetközi nonprofit szervezet, amely kiszivárogtatott kormányzati és egyéb dokumentumokat publikál az Interneten, miközben forrásainak névtelenséget biztosít. Az egyik legjelentősebb, az oldalhoz köthető eset 700 ezer titkos és bizalmas amerikai kormányzati irat nyilvánosságra hozatala. A WikiLeaksen publikált titkos és bizalmas információk a „nyilvánosság versus nemzetbiztonsági érdek" dichotómiájában jelenlevő parázs vita mellett a másik legfontosabb kérdése a „Cui prodest", vagyis, ezeknek az információknak a napvilágra kerülése kinek az érdekét szolgálja leginkább. Talán az egyik legkényesebb terület ennek vizsgálata, ugyanis rengeteg összeesküvés-elmélet született ebben a témában.

A WikiLeaks alapítóinak saját bevallása szerint az oldalt disszidens kínai újságírók hozták létre a demokrácia és szólásszabadság védelme érdekében. Az oldal üzemeltetői úgy vélik, a tájékoztatás szabadsága, a tájékozódáshoz való jog minden más jog fölött áll, még ha nemzetbiztonsági érdeket is sért. A szerkesztők kezdetekben ázsiai és afrikai ügyekkel foglalkoztak, de a prioritás hamar az Amerikai Egyesült Államok kormánya által elkövetett jogsértésekre, visszaélésekre helyeződött át (guantanamói katonai támaszponton a fogvatartottakkal kapcsolatos bánásmódra vonatkozó titkos direktívák, 40 perces mozgóképfelvétel az amerikai csapatok egyik iraki rajtaütéséről, amelynek eredmények 12 halálos áldozat). A fentieken kívül közölték többek között:

- a Szcientológiai Egyházhoz kötődő bizalmas dokumentumokat;
- a szélsőjobbos Brit Nemzeti Párt tagnyilvántartását;
- 600 (részben bizalmas minősítésű) ENSZ-dokumentumot;
- közel 7000 olyan elemzést, amelyet az amerikai Kongresszus tudományos és kutatási hátttereként szolgáló Congressional Research Service készített;
- az amerikaiak afganisztáni jelenlétével és háborújával kapcsolatban 92 ezer dokumentumot, amelyek közül számos bizalmas és titkos minősítést kapott, de megtalálhatóak voltak köztük szigorúan titkosak is.

Az Amerikai Egyesült Államokat érintő ügyek dominanciája miatt többen is úgy vélik, hogy a WikiLeaks mögött eredetileg az USA stratégiai ellenfelei állnak, akik az emberi jogi, információ- és tájékoztatási szabadságot felhasználva kívánják gyengíteni az Egyesült Államokat, miközben a WikiLeaks arcát, Julien Assanget és társait idegen zászló alatt beszervezték. A 2016-os amerikai elnökválasztás idején ez az elmélet egyre több és erősebb igazolást nyert, de erről bővebben később.

Vizsgáljuk meg egy kicsit jobban a kiberterrorizmust is.

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."*[48]

[48] Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004. URL: http://www.fbi.gov/congress/congress04/lourdeau022404.htm (Letöltés ideje: 2017. július 18.).

Terroristák számos területen használják a kiberteret, amiben a magát Iszlám Államnak nevező terrorszervezet a tevékenységeivel igazi paradigmaváltást eredményezett. Nyolc különböző területet azonosíthatunk, amiben a terroristák sikeresen alkalmazhatják a kiberteret. Ezek az alábbiak:

- információgyűjtés;
- social engineering;
- kapcsolattartás;
- propaganda;
- új tagok toborzása;
- támogatók szerzése;
- lélektani műveletek (továbbiakban PSYOPS);
- kibertámadás.[49]

Az egyes területek részletes bemutatására a későbbiekben specifikusan a közösség médiára alkalmazva kerül sor. Itt egyedül azt fontos megemlíteni, hogy jelenleg, e tankönyv írásakor a terroristáknak nincs meg sem a technikai, sem a humán, sem az anyagi képessége, amivel egy komolyabb kibertámadást képesek lennének végrehajtani. Ahogy azonban a kiberbűnözésről szóló résznél már említésre került, a Darkneten számos olyan szolgáltatást árulnak, amivel, ha van elegendő pénzük a terroristáknak, komolyabb kibertámadást is végrehajthatnak.

Kiberkémkedés

A kiberkémkedés az államok, piaci szereplők által informatikai eszközökön történő hírszerző tevékenységet jelenti. Maga a hírszerzés egyidős az emberiséggel, és mindig élen járt a technológiai fejlődésben, így nem véletlen, hogy az informatikai eszközök jelentős szerepet töltenek be a hírszerzés világában. Mivel e tankönyv 5. fejezete a hírszerzésről szól, így bővebben ott bonyolódunk a kérdéskörbe.

Kiberhadviselés

A kiberhadviselés az államok közti konfliktusokban jelenik meg, amelynek segítségével a szembenálló felek számítógépeket és hálózatokat használnak fel katonai célok érdekében, például számítógép-hálózatok működésképtelenné tételére, akár a konvencionális hadviselés támogatására, akár önálló tevékenység folytatására. Kiberhadviselés során a hírszerzés eszközként jelenik meg, amelynek célja, hogy támogassa az adott katonai műveleteket.

A kiberhadviselés összetevőinek a számítógép-hálózati műveleteket, az elektronikai hadviselést és az elektronikai felderítést nevezzük.[50]

[49] Egy kibertámadás egy honlap tartalmának megváltoztatásától (deface) kezdve egy kritikus infrastruktúra ellen elkövetett támadásig sokféle lehet.

[50] HAIG et al. (2014): Elektronikai hadviselés (szerk. Németh András), Nemzeti Közszolgálati Egyetem, Budapest.

A számítógép-hálózati műveletek (Computer Network Operations) esetében három részterületet különböztetünk meg, amelyek a számítógép-hálózatok támadására, védelmére, illetve sebezhetőségeinek felderítésére vonatkoznak.

Az elektronikai hadviselés (Electronic Warfare) a Magyar Honvédség Összhaderőnemi Elektronikai Hadviselési Doktrínája alapján azon katonai tevékenység, amely az elektromágneses energiát felhasználva meghatározza, felderíti, csökkenti vagy megakadályozza a frekvenciaspektrum ellenség részéről történő használatát, és biztosítja annak a saját csapatok általi hatékony alkalmazását. Területei az elektronikai támogató tevékenység, az elektronikai ellentevékenység és az elektronikai védelem. Az elektronikai támogató tevékenység az elektronikai hadviselés azon része, amely magában foglalja – a fenyegetés azonnali jelzése érdekében – az elektromágneses kisugárzások felkutatására, elfogására és azonosítására, valamint a források helyének meghatározására irányuló tevékenységeket. Az elektronikai ellentevékenység az elektronikai hadviselés azon területe, amely magában foglalja az elektromágneses és irányított energiák kisugárzását abból a célból, hogy megakadályozza vagy csökkentse az elektromágneses spektrum ellenség által való hatékony használatát. Az elektronikai ellentevékenység egyik területe az elektronikai zavarás, amely az elektromágneses energia szándékos kisugárzását, visszasugárzását vagy visszaverését jelenti. Ennek célja, hogy megakadályozzuk az ellenség elektronikai eszközeinek vagy rendszereinek hatékony működését. Az elektronikai védelem az elektronikai hadviselés azon része, amely biztosítja az elektromágneses és egyéb spektrum saját részről történő hatékony használatát az ellenség elektronikai támogató és ellentevékenysége, valamint a saját csapatok nem szándékos elektromágneses interferenciái ellenére.[51]

Az elektronikai felderítés (Signals Intelligence – SIGINT) a hírszerzés egyik területének tekinthető, amelynek elsődleges célja különböző, alapvetően vezetékes vagy rádiós úton folytatott, titkosított vagy nem titkosított kommunikációhoz és jelekhez kapcsolódó felderítő, információgyűjtő tevékenység.[52] A SIGINT két alterületre bontható, COMINT-re (Communications Intelligence) és ELINT-re (Electronic Intelligence). Nagyon leegyszerűsítve a COMINT az ember és ember közötti, az ELINT a gép és gép közötti kommunikációra épülő hírszerzést jelenti.

[51] MH Összhaderőnemi Elektronikai Hadviselési Doktrína. MH DSZOFT Kód: 11222. HM HVK Felderítő Csoportfőnökség kiadványa, 2005.

[52] DOBÁK Imre (2014): Elektronikai eszközökkel végzett felderítés, In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest.

A kiberhadviselés eszközeinek az alábbiak tartoznak:

- nulladik napi sérülékenységek;[53]
- botnetek;[54]
- (célzott) malware-ek;[55]

[53] A nulladik napi támadás alatt olyan biztonsági fenyegetést értünk, amelyben a támadók egy szoftver még a fejlesztők által sem ismert sebezhetőségét használják ki. Mivel a hiba senki által nem ismert, így értelemszerűen nem készült biztonsági javítás. Zero-day exploitnak nevezik azt a tényleges kódot, amit a támadók használnak a sérülékenység kiaknázására, mielőtt a szoftver fejlesztője tudna arról. A kifejezés az exploit keletkezésének időpontjából adódik. Amikor a szoftverfejlesztő tudomást szerez egy biztonsági résről, megkezdődik a verseny a támadók és a fejlesztők között; a felelősségteljes fejlesztő igyekszik befoltozni a hibát, mielőtt nyilvánosságra kerül. A „nulladik napi" támadás az első vagy „nulladik" napon történik, amikor a fejlesztő már tud a hibáról, így még nem volt lehetősége arra, hogy a biztonsági javítást eljuttassa a szoftver felhasználóihoz. Számos esetben azonban hiába derül ki egy szoftverről, hogy biztonsági rést tartalmaz, amely súlyos következménnyel járhat a felhasználóra nézve, a kiadott frissítőcsomagokat nagyon kevesen telepítik; így hiába van megoldás a probléma befoltozására, a nem frissített alkalmazások ugyanolyan kockázatot jelentenek a felhasználó számára. Sok alkalmazás esetében van lehetőség bekapcsolni az automatikus frissítést, de több esetben előfordult már, hogy egy letöltött alkalmazás nem tartalmazott kártékony kódot, azonban a később letöltött frissítésbe rejtették el a támadók a fertőzött állományokat, és így fértek hozzá a rendszerhez. A nulladik napi sebezhetőségek rendkívüli nagy értékkel bírnak a támadóknak. Ezzel a típusú sebezhetőséggel változatos tevékenységeket végezhetnek, legyen szó például zsarolóvírusok terjesztéséről, számítógépek irányításának megszerzéséről vagy nukleáris erőművek tönkretételéről. Ez utóbbit kiválóan illusztrálja az iráni natanzi urándúsító esete, amelyben az azóta hírhedté vált kiberfegyver, a Stuxnet, egyes szakértők becslése alapján hat évre vetette vissza az iráni nukleáris programot. A Stuxnet négy nulladik napi sebezhetőséget használt ki, köztük a Windows operációs rendszerek korábbi sebezhetőségét, amely a számítógéphez csatlakoztatott külső adathordozókat automatikusan elindította. Ezt a fajta sebezhetőséget azóta a Microsoft befoltozta, és a Windows 7 óta a rendszer rákérdez, hogy mit szeretnénk tenni a csatlakoztatott adathordozóval; nem futtatja automatikusan. A 2017-ben a WikiLeaks által nyilvánosságra hozott „Vault 7"-iratok tanulsága szerint, ami az oldal állítása szerint a CIA kibertámadási képességéről rántja le a leplet, a szervezetnek közel 250 nulladik napi sérülékenységet ismert. Ezeket hol a CIA, hol a partnerszervezeti, pl. az NSA fedezte fel, nem kevés anyagi ráfordítással, hol pedig hackerektől vásárolták meg.

[54] Robothálózat vagy más néven zombihálózat alatt olyan fertőzött informatikai eszközök hálózatát értjük, amelyek fölött a támadók átvették az irányítást, és az eszköz erőforrásait saját céljaikra használják fel. Ezeket legtöbbször kéretlen levelek küldésére, bitcoinbányászatra használják, azonban ilyen bothálózatokat használnak rendszerek támadására is. A fertőzött eszközök tulajdonosai sok esetben nincsenek tisztában azzal, hogy a gépük egy bothálózat tagja, csupán annyit tapasztalnak, hogy az eszköz rendkívül lelassult. A Dolgok Internetének terjedése növelte a zombihálózatok számát, ugyanis rengeteg IoT-eszköz nem rendelkezik megfelelő informatikai védelemmel, amik fölött a támadók könnyűszerrel átvehetik az irányítást. 2016 októberében a fél internetet bénította meg egy olyan túlterheléses támadás, amiben több tízmillió eszközből álló botnethálózat irányított. A hálózat jelentős részét IoT-eszközök, így okoshűtők, webkamerák stb. alkották

[55] Káros szoftver, vagy más néven malware az angol malicious software összevonásából kialakított mozaikszó. Mint ilyen, a rosszindulatú számítógépes programok összefoglaló neve. Idetartoznak a vírusok, trójai falovak, férgek (worm), kémprogramok (spyware), agresszív reklámprogramok (adware), a rendszerben láthatatlanul megbúvó, egy támadónak emelt jogokat biztosító eszközök (rootkit). A vírus olyan rosszindulatú program, amely képes sokszorosítani és terjeszteni magát, az egyik gépről a másikra. Ugyanez a féregre is igaz, azzal a különbséggel, hogy a vírus általában „befúrja" magát egy futtatható fájlba, hogy teljesítse a célját. A trójai egy olyan malware-program, amely nem próbálja magát lemásolni, hanem inkább úgy tesz, mintha egy legális szoftver lenne, és a felhasználót veszi rá a telepítésre. A névét a görög

- DoS, DDoS;[56]
- APT-k;[57]
- social engineering;
- irányított energiájú fegyverek.[58]

A kiberhadviselés célpontjai a szembenálló fél információs rendszerei (katonai, nemzetbiztonsági, rendészeti és közigazgatási rendszerek, valamint a létfontosságú rendszerelemek. A 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló törvény (Lrtv) alapján *„létfontosságú*

mitológiából kapta, mivel ártalmatlan szoftvernek adja ki magát, de valójában rosszindulatú kódot rejt. A vírussal ellentétben nem akar más file-okat megfertőzni, helyette átadja az irányítást a támadónak. A féreg egy számítógépes vírushoz hasonló önsokszorosító számítógépes program. Míg azonban a vírusok más végrehajtható programokhoz vagy dokumentumokhoz kapcsolódnak hozzá, illetve válnak részeivé, addig a férgeknek nincs szükségük gazdaprogramra, önállóan fejtik ki működésüket. A kémprogramok segítségével a támadók megfigyelhetik az áldozat internetes tevékenységét, beleértve minden jellegű kommunikációjukat, átvehetik az irányítást a mikrofon, kamera fölött. Több esetben napvilágra került, hogy egyes laptopokba, telefonokba már a gyártósoron előre telepítették ezeket a kémprogramokat. Az adware működése során különféle reklámokat jelenít meg; általában trójai programként vagy kereskedelmi alkalmazások ingyenes változataiban települnek a felhasználó eszközére. Az adwarek egy része spywareként is funkcionálhat, hogy ily módon minél jobban megismerje a felhasználói szokásokat, preferenciákat, hogy célzott hirdetéseket jeleníthessen meg. A rootkit olyan szoftvereszközt jelent, amelynek telepítésével a támadók visszatérhetnek a fertőzött eszközre, ahol magas szintű felhasználói jogosultságot szerez. A rootkitet rendkívül nehéz kimutatni, mivel aktívan próbálja elrejteni magát a felhasználó, az operációs rendszer és az antivírus/anti-malware-programok elől. Ez a szoftver számos módon települhet a rendszerre, beleértve az operációs rendszer biztonsági réseinek kihasználását vagy adminisztrátori jogok szerzését a számítógépen

[56] Túlterheléses támadásnak két fajtáját különböztetjük meg, ezek a szolgáltatásmegtagadásos (Denial of Service vagy DoS) és az elosztott szolgtatásmegtagadásos (Distributed Denial of Service vagy DDoS) támadások. A támadás célja az informatikai szolgáltatás teljes vagy részleges megbénítása, helyes működési módjától való eltérítése. Egy meghatározott alkalmazás, operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokoll tulajdonságait (gyengéit) támadja meg. Célja, hogy az alkalmazás, vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógéprendszer vagy akár a számítógép-hálózat elérésében. A támadás eredményeképpen a rendszer nagyon lelassul, elérhetetlenné válik, esetleg össze is omolhat. A lényege, hogy lehetőség szerint megakadályozza a célgép elérését. A támadást botnethálózatok segítségével végzik.

[57] A célzott támadások kategóriájába soroljuk az úgynevezett APT-t (Advance Persistent Threat), ami fejlett folyamatos (információbiztonsági) fenyegetést jelent, olyan támadássorozat, amelynek célja nem a károkozás, hanem a folyamatosan fenntartott rejtett jelenlét és információszerzés.

[58] Irányított energiájú fegyver (Directed-Energy Weapon): olyan fegyver vagy rendszer, amelyik irányított energiát használ, hogy használhatatlanná tegye, megrongálja vagy megsemmisítse az ellenség felszerelését, létesítményeit és/vagy élőerejét. Ez alapján beszélhetünk kinetikus eszközökről, akusztikus eszközökről, rádiófrekvenciás eszközökről, lézereszközökről, részecskesugár-eszközökről. Az elektromágneses tartományt célszerűségi és az eszközeikben meglévő alapvető különbözőségi okokból már itt célszerű önálló csoportba sorolni. Akit érdekel e téma, bővebben lásd: Ványa László (2013): Irányított energiájú fegyverek, Nemzeti Közszolgálati Egyetem. URL: http://uni-nke.hu/downloads/konyvtar/kovasz/vanya_jegyzet.pdf (Letöltés ideje: 2017. július 19.).

rendszerelem: az 1–3. mellékletben meghatározott ágazatok valamelyikébe tartozó eszköz, létesítmény vagy rendszer olyan rendszereleme, amely elengedhetetlen a létfontosságú társadalmi feladatok ellátásához – így különösen az egészségügyhöz, a lakosság személy- és vagyonbiztonságához, a gazdasági és szociális közszolgáltatások biztosításához –, és amelynek kiesése e feladatok folyamatos ellátásának hiánya miatt jelentős következményekkel járna".[59]

A szakirodalom a történelem első kiberháborújának a 2007-es, Észtországot ért kibertámadást tekinti. Az eset előzménye, hogy az észt kormány eltávolított Tallinban egy második világháborús szovjet hősi emlékművet. Az országban élő nagyszámú orosz kisebbség körében tüntetés tört ki, Észtországot, egy NATO-tagállamot kibertámadás ért. A támadás során közel egy hónapig több mint 170 országból érkezett túlterheléses támadás az észt kormányzati és bankrendszer ellen. A NATO 5. cikkelye kimondja, hogy egy tagállamot ért támadás az egész szövetséget ért támadásnak tekintendő, ami kiváltja a kollektív védelem elvét. Bár Észtország a kezdetektől az orosz kormányzatot vádolta a támadással, nem lehetett hitelt érdemlően bizonyítani az orosz érintettséget, hiszen rengeteg országból érkezett a támadás. Ennélfogva a NATO is igyekezett az ügyet a katonai dimenzióból politikai dimenzióba terelni, mert ellenkező esetben katonai válaszcsapást kellett volna indítani. Ilyen irányú szándéka azonban nem volt, továbbá a Szövetséget is felkészületlenül érte az eset. Az eset nagy hatással volt a NATO-ra, ennek nyomán indult el az a stratégiai munka, amely létrehozta a NATO kiberbiztonságért felelős intézményrendszerét, illetve elindította a jogi gondolkodást is a témában. Jelenleg a nemzetközi jogban az egyik legérzékenyebb terület, hogy a kibertámadás kiváltja-e az önvédelemhez való jogot. Azt kijelenthetjük, inkább a politikai szándék hiányzik, mintsem a jogi háttér. Bár léteznek kísérletek arra, hogy a kibertámadást megpróbálják a genfi egyezményekkel összhangba hozni; ennek egyik legismertebb példája a Tallini Kézikönyv, amit a NATO megbízásából dolgoztak ki szakértők. Fontos azonban, hogy a Tallini Kézikönyv nem egy hivatalos NATO-dokumentum, és nem is jogszabály, egyelőre csak irányelvek gyűjteménye, amelyet egyébként a Cambridge University Press adott ki. 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 kombattánsként, azaz legitim célpontként határozza meg.[60]

Az Észtországot ért kibertámadás óta eltelt 11 év, azonban a normatív szabályozást illetően még mindig nem léptünk előre. Hogy ki követett el egy kibertámadást – amennyiben nem vállalja magára –, rendkívül nehéz bebizonyítani. A támadók könnyűszerrel képesek elrejteni a nyomokat, de olyan nyomokat is elhelyezhetnek, amellyel a felelősséget más országokra kenik. A nemzetközi jogban a realista értelmezés szerint az erősebb országok haté-

[59] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv (Letöltés ideje: 2017. július 19.)

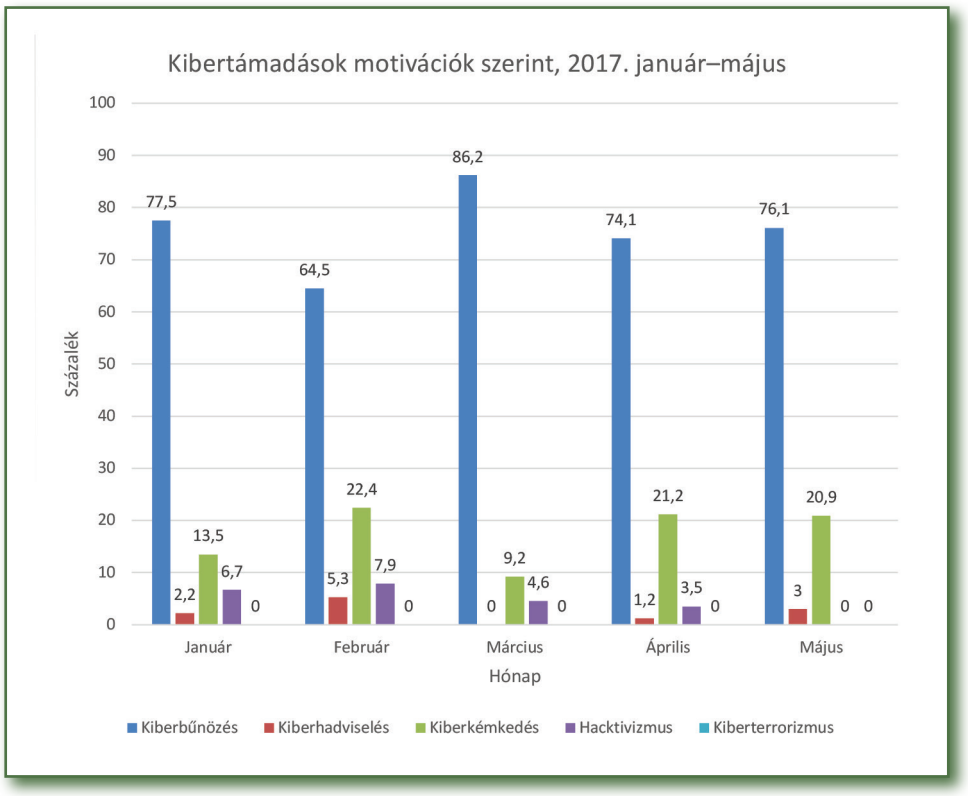
[60] BÁNYÁSZ Péter – ORBÓK Ákos (2013): A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. Hadtudomány Online, 2013/1. URL: http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf (Letöltés ideje: 2017. július 19.).

konyabban érvényesítik érdekeiket. Bár az ENSZ Alapokmánya szerint tilos háborút indítania az országoknak, csupán önvédelemből alkalmazhatnak fegyveres támadást, ellenkező esetben az ENSZ jóváhagyása szükséges hozzá. A második iraki háborút mégis az ENSZ Biztonsági Tanácsának felhatalmazása nélkül indította az USA, aminek nem lett semmilyen nemzetközi jogi következménye. A változást az fogja jelenteni a téma szempontjából, amikor egy ország úgy dönt, fegyveresen vesz elégtételt az őt ért kibertámadásért, ezt pedig a nemzetközi közösség hallgatólagosan nyugtázza. Az amerikai védelmi szakterminológiában különleges szerepe van az úgynevezett attribution fogalmának, mely azt jelenti, hogy megalapozott gyanú alapján nevesítik az elkövetéssel vádolt országot. 2017-ben két globális ransomware kampány is zajlott, májusban a WannaCry, júniusban a NotPetya, amelyek kapcsán több ország hivatalosan is Észak-Koreát a WannaCry, Oroszországot a Notpetya kapcsán nevesítette elkövetőként, így egyfajta elmozdulás figyelhető meg az említett területen.

2.4. A KIBERFENYEGETETTSÉG TRENDJEI

Ahogy korábban a közösségi média esetében, úgy a kiberfenyegetettségek kapcsán is nehéz egy tankönyv keretein belül trendekről beszélnünk, hiszen ezek hónapról hónapra változnak, így mire nyomtatásban vagy elektronikusan olvashatók lesznek, minden bizonnyal már elavultnak számítanak. Mégis szükséges azonban röviden szemléltetni a kibertámadások számának és megoszlásának arányait.

A legfrissebb adatok alapján 2017 első öt hónapjában magasan a kiberbűnözés állt a kibertámadások döntő többsége mellett (lásd 3. számú ábra).

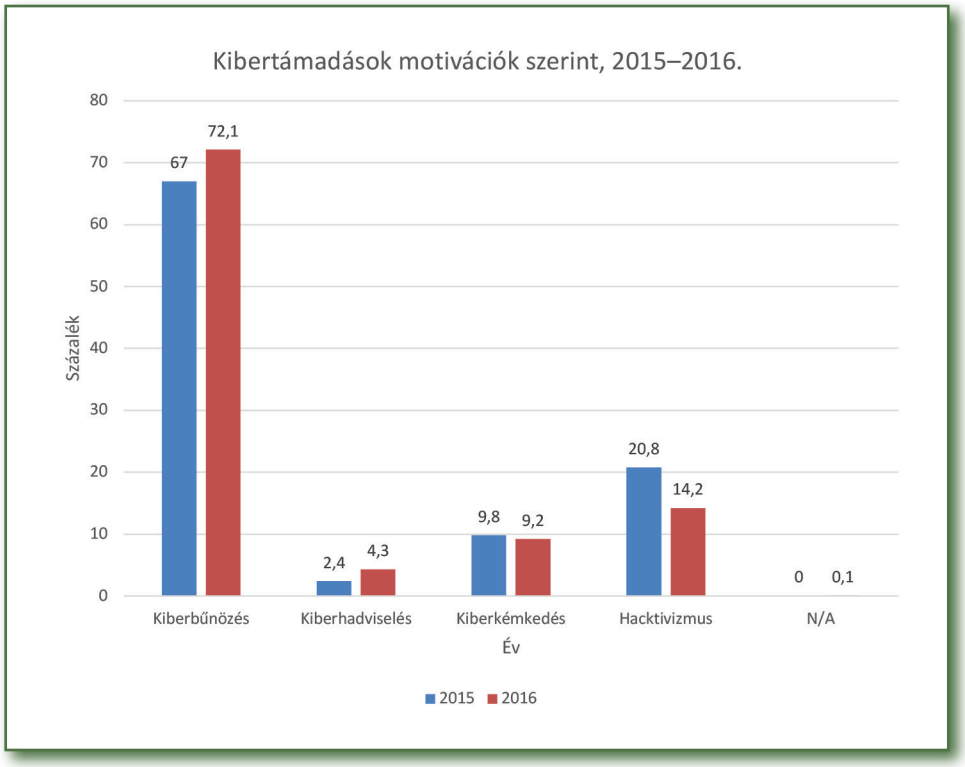


3. ábra: Kibertámadások motivációk szerint 2017. január–május

Forrás: http://www.hackmageddon.com, saját szerkesztés

A kiberbűnözés – februárt leszámítva – az összes támadástípus több mint kétharmadáért felelt; márciusban kimagasló értéket olvashatunk le, az összes támadás 86,2%-a e kategóriába sorolható. Ezt követi a kiberkémkedés, amely márciusban nem érte el a 10%-ot, de három hónapban így is a támadások több mint 20%-át tette ki. A kiberhadviseléssel összefüggő biztonsági incidensek viszonylag alacsony számon mozognak, a legnagyobb értéket februárban tapasztalhattuk. A hacktivizmus esetében is változatos eredményt kapunk.

Érdemes összevetni az adatokat a 2015–2016-ra vonatkozó értékekkel (4. számú ábra). Ebben látható, a kiberbűnözés folyamatosan növekvő tendenciát jelez, amely 2017-re hasonló arányú. A kiberkémkedés tekintetében az előző évekhez képest jelentős emelkedést figyelhetünk meg, míg a hacktivizmushoz köthető támadások száma csökkenést jelez.



4. ábra: Kibertámadások motivációk szerint 2015–2016.

Forrás: http://www.hackmageddon.com, saját szerkesztés

A kiberhadviseléssel kapcsolatos biztonsági események 2017 első felében hasonló tendenciát mutatnak, mint egy évvel korábban. Ami újdonságnak tekinthető, hogy 2016-ban az összes támadás 0,1%-ában nem ismert a motiváció.

Fontosabb fogalmak

Adat, adminisztratív biztonság, Anonymous, bizalmasság, biztonság, botnet, célzott támadás, Darknet, elektronikus információbiztonság, fenyegetettség, hacktivizmus, információ, információbiztonság, kártékony kód, kiberbiztonság, kiberbűnözés, kiberhadviselés, kiberkémkedés, kiberterrorizmus, kihívás, kockázat, rendelkezésre állás, sértetlenség, social engineering, számítógép-hálózati műveletek, személyi biztonság, túlterheléses támadás, WikiLeaks.

Áttekintő kérdések

1. Megítélése szerint egy kibertámadás kiváltja-e az önvédelemhez való jogot, amelynek során konvencionális eszközökkel támadhat vissza az állam?
2. Hogyan rangsorolná a kiberfenyegetettségeket az alapján, hogy mennyire érzi Önmagát fenyegetve?
3. Ön szerint a hacktivisták hősök vagy bűnözők?
4. Ön szerint ki(k) állnak a WikiLeaks mögött?

3. A MAGÁNSZFÉRA ÉS KIBERTÉR KAPCSOLATA

Az infokommunikációs technológiák, az internet és a közösségi média hatására a magánszféránk fokozatosan szűkül. Érdekes paradoxon ez, hiszen az internetre nagyon sokáig az anonimitás volt jellemző, azonban a közösségi hálózatok megjelenésével az anonimitás egyre inkább csökkenni kezdett, megnyitva az utat az olyan állami szabályozás felé – például Oroszország esetében –, amelyben teljesen száműznék az anonimitást a terrorizmus és a szervezett bűnözés elleni harc nevében.

Benjamin Franklintől származik a mondás, miszerint *„[a]zok, akik feladnák alapvető szabadságukat egy ideiglenes biztonságért, nem érdemelnek sem szabadságot, sem biztonságot."*

George Orwell az 1984 című regényében egy olyan disztópikus világot fest le, amelyben három totalitárius szuperállam, Óceánia, Keletázsia és Eurázsia áll háborúban egymással (a propaganda szerint mikor ezzel, mikor azzal), hatalmuk alapját az évtizedek óta zajló fegyveres konfliktus, valamint a totális megfigyelés biztosítja. A nap 24 órájában tartó folytonos megfigyelés egyik eszköze a telekép nevű készülék, amely minden középületben, minden párttag lakásának majdnem minden helyiségében kötelezően ott kell legyen. A telekép nem csupán televízióként funkcionál, van benne egy kamera, amelyen keresztül a párttagokat elvileg folyamatosan figyelik – az eszközt kikapcsolni természetesen szigorúan tilos.[61] A regényben a totális kontroll egy másik fontos eleme a kognitív dimenzió, amelynek legfontosabb eszköze az „újbeszél"; egy olyan nyelv kialakítása, amely rendkívül csökkentett szókinccsel és egyszerűsített nyelvtani szabályokkal bír. A cél az, hogy így önmagukat cenzúrázzák a Párt tagjai, és elkerüljék a „gondolatbűnt", hiszen ha nincsenek szavak, amelyek segítségével ki lehet fejezni érzéseket, pláne absztrakt kifejezéseket, mint például elnyomás, szabadság stb., akkor a gondolatuk sem alakul ki.

Elsőre az orwelli világ távolinak tűnhet, de ha belegondolunk abba, hogy majdnem mindannyiunk zsebében ott lapul egy eszköz, amin keresztül a nap minden percében megfigyelhetik életünk minden másodpercét, mi több gondolatainkat, legbelsőbb érzéseinket, amikről azt gondoljuk, csak egyetlen egy valakinek mondjuk el, akkor mégsem a megfoghatatlan jövőben járunk. Ennek a felismerésétől pedig nem jár messze az öncenzúra kialakulása, hiszen a legféltettebb gondolatainkat, amit csak egy embernek mondtunk, az egy adott körben kifejtett véleményünket, amit nem szántunk nagyobb nyilvánosság elé megismerhetik, visszaélhetnek vele. Ez ellen az egyetlen

---

[61] Orwell Állatfarm című regényéből származik egy másik, szállóigévé vált mondás – „Minden állat egyenlő, de egyes állatok egyenlőbbek a többieknél" –, amely az 1984-ben is érvényes. Az 1984-ben Óceánia társadalmát három részre oszthatjuk, a Belső Párt tagjai, akik a tényleges hatalmat gyakorolják, számos kiváltsággal rendelkeznek, mint például ők kikapcsolhatják a teleképet. A Külső Párt tagjai, akik viszonylag magas számban vannak, ők a társadalomi irányítás alapja, a közszolgák, kereskedők stb. Végül pedig a társadalom 85%-át kitevő proletárok, akik azonban semmilyen joggal nem rendelkeznek, mégis ők a legszabadabbak. Míg a Belső és Külső Párt tagjai számára tilos volt az erotika, a szerelem, addig a proletárok szabadan élhettek, őket nem figyelték meg semmilyen eszközzel, hiszen az irányításukhoz a legolcsóbb propagandaeszközök bőven elegendőnek bizonyultak, így apolitizálták őket.

védekezés, ha nem írjuk le, ha nem mondjuk ki a telefonunk, táblagépünk, számítógépünk, okostv-nk, és egyéb okos eszközeink közelében, amelyek mikrofont is tartalmaznak. Mindezek miatt különösen fontos a magánszféra védelme. Franklin gondolatai talán soha nem voltak ennyire aktuálisak, mint napjainkban.

3.1. JOGI HÁTTÉR, FŐBB FOGALMAK

Magánszféra

A magánszféra, amellett, hogy igény, egyben jog is, amelynek keretein belül az egyén meghatározhatja, hogy a vele kapcsolatos információkhoz kik férhetnek hozzá. Mindezek mellett egy ellenőrzési helyzet is, amelyben az egyén dönt a személyes információi és személyisége intim vonatkozásai felett. Ugyanakkor egy állapot, amelyben az egyénhez (gondolataihoz, testéhez, vele kapcsolatos információkhoz) való hozzáférés korlátozott.

A magánszféra érvényességi köre rendkívül nehezen határozható meg, ugyanis összefügg az információ és információvédelem, az elrejtőzés és a figyelem középpontjába való kerülésének kérdéseivel. Az információs szabadság ugyanakkor igény és jog a (tág értelemben vett) kormányzati dokumentumok nyilvánosságára, a hivatalos iratok titkosságának feloldására, a közélet működésének átláthatóságára. Az államok kormányzatai a közérdek védelmében látják el tevékenységüket. Esetükben az információ felhasználása kettősséget jelent. Egyrészt az információkat a köz érdekében használják fel, másrészt az információ a transzparencia forrása is, ami a kormányzatok esetleges túlkapásai ellen véd. Ahhoz, hogy egy kormányzat hatékonyan legyen képes ellátni funkcióját, megbízható információkra van szüksége, hiszen ezekből tud olyan döntéseket meghozni, ami a társadalom javát szolgálja. Éppen ezért a kormányzatok mindig is törekedtek arra, hogy minél szélesebb körből legyenek képesek információt gyűjteni, és igyekeztek kiterjeszteni a megfigyeléshez kapcsolódó képességüket – mind technikai-technológiai, mind szabályozási oldalról. Az információ hatalom, különösen annak kezében, aki kizárólagosan birtokolja azt. Az információhoz való hozzájutás az állampolgári jogok körébe tartozik, már csak azért is, mert a túlzott titkosság az önkény megalapozója, növeli a korrupciót, illetve rossz működési hatékonyságot eredményez.

A probléma abból ered, hogy a mindent körülvevő infokommunikációs technológiák használatából nagyszámú adat keletkezik.

Adat fajtái

Az adat objektív tények összessége. Olyan tény, mérési eredmény, amely egy szituációra vonatkozik egy adott időpontban.[62] Az adat tehát egy objektív mérési eredmény, egy rögzített ismeret, ami egy adott időpontban egy adott helyzetre jellemző, és vonatkozhat jelenségekre, fogalmakra, megfigyelésekre, tapasztalatokra stb. Ilyen adat, hogy valahol bankkártyával fizetünk, Facebookon közzéteszünk egy videót, a 4-es Metrón ülve rögzíti az arcunkat a járműre szerelt térfigyelő kamera, új telefont keresünk az interneten. De ha nem csinálunk semmit, ha alszunk, akkor is folyamatosan új adat keletkezik a telefonunk helymeghatározó funkciója által.

[62] DAVENPORT T.H. – PRUSAK, L. (2001): Tudásmenedzsment, Kossuth Kiadó.

A telefonunk e tekintetben különösen sok adatot állít elő. Jelenleg még csak szabadalmat nyújtott be a Facebook olyan technológiákra, mint például, hogy a telefonok kamerájának giroszkópjai egy adott helyen huzamosabb ideig merre irányulnak.[63] 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.

Ebből is látható, az adatok önmagukban nem értelmezhetőek, nem következik belőle még semmi. A minőségi ugrást az jelenti, amikor az adatokat értelmezzük. Ahogy Halassy Béla fogalmazta meg, az információ új ismeretté értelmezett adat.[64] Az információ keletkezésében a nehézséget az adatok nagy száma jelenti, ezt nevezzük big datának. Másképp fogalmazva, a Big Data a cégek, az intelligens hálózatok, a magánszektor és az egyéni felhasználók által világszerte és napi szinten előállított óriási adatmennyiséget jelenti. Strukturáltan és kielemezve ez a rengeteg információ nagy hasznot hozhat a cégek és ügyfelek számára.

Az adatokat típusuktól függően kategorizáljuk. A 2011. évi CXII. törvény az információs önrendelkezési jogról és információszabadságról[65] értelmező rendelkezései alapján

- 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 érdekképviseleti 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 formá-

[63] CHEN, Ben (2016): 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. URL: http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=%2820160114.PD.+AND+%28Facebook.AS.+OR+Facebook.AANM.%29%29&OS=PD/1/14/2016+and+%28AN/Facebook+or+AANM/Facebook%29&RS=%28PD/ (Letöltés ideje: 2018. január 16.)

[64] HALASSY Béla (1994): Az adatbázistervezés alapjai és titkai – Avagy az út az adattól az adatbázison át az információig. IDG Hungary, cop., Budapest.

[65] 2011. évi CXII. törvény az információs önrendelkezési jogról és információszabadságról. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (Letöltés ideje: 2017. november 11.)

ban 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.

Az adatok egy speciális aspektusát jelentik a minősített adatok. A 2009. évi CLV. törvény a minősített adat védelméről[66] 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.

Adatvédelem

Az adatok számától, jellegétől, érzékenységétől fogva nagyon nem mindegy, hogy kik, és milyen garanciális elvek mentén kezelik az adatainkat.

Magyarország Alaptörvénye az alábbiak szerint fogalmaz:

„(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."[67]

[66] 2009. évi CLV. törvény a minősített adat védelméről. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0900155.tv (Letöltés ideje: 2017. november 11.)

[67] Magyarország Alaptörvénye, Szabadság és Felelősség VI. cikk (1-3) bekezdés

Ebből következően a magánszféra védelme alkotmányos alapjognak tekinthető, azonban mégsem tartozik az abszolút alapjogok körébe, hiszen más alapjog védelme érdekében lehetőség nyílik a korlátozására – például a közbiztonság védelme jegyében.

Az Alaptörvény mellett a személyiségi jogok érvényesülésével a Polgári Törvénykönyv,[68] illetve a személyes adatainkkal kapcsolatos bűncselekményekkel a Büntető Törvénykönyv[69] foglalkozik.

Adatvédelemmel, információszabadsággal kapcsolatos normatív szabályozásról az Infotv. rendelkezik. Ez alapján az adatvédelem alatt személyes adatok jogszerű kezelését, az érintett személyek védelmét biztosító alapelvek, szabályok, eljárások, adatkezelési eszközök és módszerek összességét értjük. Fontos az érintett (más néven az adatalany) fogalma is, ami az Infotv. szerint bármely meghatározott személyes adat alapján azonosított vagy egyébként – közvetlenül vagy közvetve – azonosítható természetes személy. A személy különösen akkor tekinthető azonosíthatónak, ha őt – közvetlenül vagy közvetve – név, azonosító jel, illetőleg egy vagy több fizikai, fiziológiai, mentális, gazdasági, kulturális vagy szociális azonosságára jellemző tényező alapján azonosítani lehet.

Személyes adat kizárólag meghatározott célból, jog gyakorlása és kötelezettség teljesítése érdekében kezelhető- ezt nevezzük célhoz kötött adatkezelésnek. Az adatkezelésnek minden szakaszában meg kell felelnie az adatkezelés céljának, az adatok felvételének és kezelésének tisztességesnek és törvényesnek kell lennie. Csak olyan személyes adat kezelhető, amely az adatkezelés céljának megvalósulásához elengedhetetlen, a cél elérésére alkalmas. A személyes adat csak a cél megvalósulásához szükséges mértékben és ideig kezelhető. Az adatkezelés során biztosítani kell, hogy az adatok pontosak, teljesek és – ha az adatkezelés céljára tekintettel szükséges – naprakészek legyenek, valamint azt, hogy az érintettet csak az adatkezelés céljához szükséges ideig lehessen azonosítani.

Az adatbiztonság alatt az adatok jogosulatlan megszerzése, módosítása, továbbá megsemmisítése ellen megtett műszaki és szervezési megoldások összességét kell érteni. Mindkét esetben alapvető cél az adat jogellenes kezelésének vagy feldolgozásának megakadályozása, azaz az adatok megfelelő intézkedésekkel történő védelme a jogosulatlan hozzáférés, a megváltoztatás, a továbbítás, a nyilvánosságra hozatal, a törlés vagy a megsemmisítés ellen, valamint a sérülés elkerülése érdekében.

Ez azonban nem mindig valósul meg, hiszen számos körülmény játszhat közre, hogy valamilyen adatvédelmi incidens következzen be. Adatvédelmi incidens alatt a személyes adat jogellenes kezelését vagy feldolgozását, így különösen a jogosulatlan hozzáférés, megváltoztatás, továbbítás, nyilvánosságra hozatal, törlés vagy megsemmisítés, valamint a véletlen megsemmisülés és sérülés eseteit értjük.

A magyarországi gyakorlat az adatvédelmi incidensek szankcionálását illetően bár szigorúnak tekinthető, a 2018. május 25-étől hatályba lépő európai Általános Adatvédelmi Rendelet[70] (továbbiakban GDPR) komoly változásokat jelent, és nagy fokú szigorítás ment végbe.

---

[68] 2013. évi V. törvény a Polgári Törvénykönyvről. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300005.TV (Letöltés ideje: 2017. december 12.)

[69] 2012. évi C. törvény a Büntető Törvénykönyvről. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV (Letöltés ideje: 2017. december 11.)

[70] 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). URL: http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=HU (Letöltés ideje: 2017. december 12.)

Az Általános Adatvédelmi Rendelet megalkotásához az a felismerés vezetett, miszerint szükségessé vált egy olyan jogi alap, amely úgy biztosít az európai hagyományoknak megfelelően erős adatvédelmet, hogy közben jobban alkalmazkodik a mai információs technológiákhoz, képes kezelni a felhőszolgáltatásokat, a határokon átnyúló adatkezelést vagy éppen az EU-n kívülre irányuló adattovábbítást. Az európai adatvédelem hagyományosan szigorúbb, mint például az Amerikai Egyesül Államok ez irányú gyakorlata. Az Európában is oly népszerű közösségi oldalak, mint a Facebook, Youtube, Twitter stb. mind amerikai vállalatok, sokkal szabadabb adatvédelmi gyakorlattal, mint ami az Európai Unió területén érvényben van. Az Edward Snowden által nyilvánosságra hozott iratokból tudjuk, hogy az amerikai nemzetbiztonsági szolgálatok az ezen oldalakon regisztrált európai felhasználók adataihoz bírósági felhatalmazás nélkül szabadon hozzáférhettek, beleértve minden üzenetének a tartalmát is. Ez nem véletlenül töltötte el aggodalommal az európai döntéshozókat. Az új rendelet minden tagországra egységesen érvényes, és újdonság az is, hogy az EU-n kívüli országok cégeire is vonatkozik (így a közösségi oldalakra is), ha azok EU-s magánszemélyek vagy cégek adatait kezelik.

A GDPR alappillére, hogy az adatkezelő cégektől minél nagyobb fokú átláthatóságot és elszámoltathatóságot követel meg, nagyobb nyomatékot kap, hogy a teljes adatkezelési folyamatnak transzparensnek kell lennie. Megjelent a beépített adatvédelem elve, vagyis az adatbiztonságnak már az adatkezelési eljárások kidolgozásakor fontos szempontnak kell lennie, nem lehet puszta utógondolat.

Új kikötés, hogy a tájékoztatást egyszerű és közérthető formában, könnyen hozzáférhetően kell tálalni. Ennek része lesz valamilyen – még nem kidolgozott – egységes piktogramkészlet is, amellyel a szövegnél szembetűnőbben is jelezni kell majd a cégeknek az adatkezelési gyakorlatuk főbb jellemzőit. Az adatkezeléshez világos hozzájárulás szükséges, 16 éven aluli gyerekek esetében a szülőnek is jóvá kell hagyni. Minden felhasználónak jogában áll a személyes adatai töröltetéséhez, amennyiben az adott szolgáltatást nem kívánja a későbbiekben használni.

Szintén nóvum az adathordozhatóság szabályozása. A szolgáltatók kötelesek az általuk tárolt adatokat olyan formában átadni, hogy az mindenféle konvertálás nélkül másik szolgáltatóhoz lehessen átvinni. Hangsúlyosabbá vált a technológiasemlegesség jegyében a kompatibilitás és az átjárhatóság.

A rendelet tartalmazza az értesülés jogát adatvédelmi incidenseknél: ha hackertámadás vagy más, a felhasználót érintő biztonsági esemény következik be, ezekről a cégeknek ezentúl be kell majd számolniuk, illetve mindig értesíteniük kell 72 órán belül a Nemzeti Adatvédelmi és Információszabadság Hatóságot. Ennek elmulasztása súlyos pénzbüntetést von maga után. A rendelet meghatározza továbbá, hogy a cégeknek adatvédelmi felelőst kell kijelölniük. 2018. május 25-től az adatkezelőkre vagy adatfeldolgozókra vonatkozó rendelkezések megsértéséért maximálisan 10 millió Euró vagy a vállalkozás globális árbevétele 2%-ának megfelelő mértékű bírság szabható ki (a kettő közül a magasabb érvényes). Az adatkezelés (például hozzájárulás), az adatkezelt ügyfél jogainak, illetve a jóváhagyott adattovábbítási mechanizmusok alapelveinek megsértéséért maximálisan 20 millió Euró vagy a vállalkozás globális árbevétele 4%-ának megfelelő mértékű bírság szabható ki (a kettő közül a magasabb érvényes). Magyarországon korábban a legsúlyosabb büntetési tétel maximálisan 20 millió Ft volt.

3.2. A MEGFIGYELÉS LEHETŐSÉGEI A KIBERTÉRBEN

Mint az előző alfejezetben már volt szó róla, nem kell semmit tennünk ahhoz, hogy valamilyen adat keletkezzen velünk kapcsolatban. Ezeknek az adatoknak az értelmezése azonban rendkívül pontos és alapos megfigyelést tesz lehetővé. Jelenleg tiltott, még a nemzetbiztonsági szolgálatoknak is, hogy összekapcsoljanak bizonyos adatbázisokat, és egységesen kezeljék őket, azonban nem kétséges, hogy a nemzetbiztonsági szolgálatok és kormányok törekvése változásokat hoz majd.

Az alfejezetben a különböző megfigyeléssel kapcsolatos technikai eszközöket tekintjük át. Ezek nem mindegyike kötődik a közösségi médiához, de megítélésem szerint oly mértékben érintik, érinthetik mindannyiunkat, hogy fontos ismertetni azokat is.

Elektronikus megfigyelőrendszerek

A térfigyelő kamerákat a II. világháború alatt fejlesztették kettős céllal: egyrészt a rakétatámadások észlelésére, valamint a kockázatot jelentő ipari folyamatok távoli irányítására. Biztonsági technológiaként az Amerikai Egyesült Államokban kezdték ezeket árusítani az 1950-es években, és egy évtized kellett ahhoz, hogy a rendőrség is alkalmazásba vegye őket.

A térfigyelő kameráknak köszönhetően sikerült azonosítani több terrorcselekmény elkövetőjét, például a 2013-as bostoni maratonon történt robbantásos merénylet feltételezett elkövetőit, valamint a 2016-os budapesti körúti robbantót is a térfigyelő kamerák képei alapján azonosították.

Elektronikus megfigyelőrendszert alkalmazhatnak köztéren, munkahelyen, illetve magánlakásokban egyaránt. Kiépítésük, üzemeltetésük azonban komoly személyiségi jogi adatvédelmi és -kezelési kérdést vet fel. A jogi hátterét a korábban említett Alaptörvényi rendelkezés mellett a 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól,[71] a korábban is említett 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról, továbbá 2012. évi I. törvény a munka törvénykönyvéről[72] biztosítja. A Nemzeti Adatvédelmi és Információszabadság Hatóság segíti a vonatkozó törvények értelmezését, illetve ellenőrzi azok betartását.

Munkahelyi megfigyelés

2012-ig, a NAIH felállításáig az 1992. évi XXII. törvényben, az akkori Munka Törvénykönyvében kellett keresni a munkahelyi kamerarendszer alkalmazásának szabályait. Ezt azonban ki kellett egészíteni a személyes adatok védelméről és a közérdekű adatok nyilvánosságáról szóló 1992. évi LXIII. törvény (Avtv.) rendelkezéseivel, valamint az

[71] 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0500133.tv (Letöltés ideje: 2017. december 13.)

[72] 2012. évi I. törvény a munka törvénykönyvéről. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200001.TV (Letöltés ideje: 2017. december 13.)

adatvédelmi biztos ajánlásaival. Az azóta megújult Munka Törvénykönyve már pontosabban szabályozza a munkahelyi megfigyelés feltételeit.

A munkáltatónak joga van ellenőrizni a munkavállalót munkaidőben, munkaköri kötelességeinek ellátásával kapcsolatban. Fontos megjegyezni, hogy ez nem csupán kamerás megfigyelőrendszerrel végezhető, a munkahelyi e-mailjeire, internetezési tevékenységeire egyaránt érvényes. A kamerás megfigyelőrendszer használatához, valamint az ehhez kapcsolódó személyes adat kezeléséhez nem szükséges a munkavállaló beleegyezése. Ez azonban semmi esetre sem járhat az emberi méltóság vagy a személyiségi jogok megsértésével, továbbá a megfigyelés csupán a munkavégzéssel összefüggő tevékenységekre vonatkozik, tehát nem ellenőrizhető a munkavállaló magánélete, a munkavállaló magatartása, szokásainak megfigyelése, munkavégzésének intenzitása. Fő szabályként nem készülhet olyan felvétel, amelyen a dolgozó teljes alakja látszik, ez alól csupán akkor térhetnek el, ha a munkavégzés helyén a munkavállaló élete vagy testi épsége veszélyben van. A munkáltató adatvédelmi kötelezettsége során az arányosság[73] és elszámoltathatóság[74] elvében összhangban kell eljárnia.

Meg kell felelni továbbá különböző garanciális követelményeknek. Ez alapján kamerás megfigyelést alapvetően az élet, testi épség, személyes szabadság védelme, veszélyes anyagok őrzése, az üzleti, fizetési, bank- és értékpapírtitok védelme és vagyonvédelem céljából lehet alkalmazni. Figyelni kell arra, hogy a kamerák elhelyezése nem sértheti az emberi méltóságot, így bizonyos helyeken tilos alkalmazni (például orvosi rendelők, öltözők, zuhanyzók, illemhelyek stb.), kivéve abban az esetben, ha a munkavállaló jogszerűen nem tartózkodhat ott (például munkaidőn kívül). Tilos továbbá az egyes munkavállalókat folyamatosan megfigyelni a munkavégzés során.

A célhoz kötöttség elve alapján a kamerák látószögét oly módon kell beállítani, hogy kizárólag a megfigyelés céljában összhangban álló területre irányulhat. A felvételek tárolására három napot engedélyez a jogszabály,[75] ezt követően vissza nem állítható módon törölni köteles a munkáltató. Korlátozni szükséges továbbá a felvételekhez való hozzáférést. Tájékoztatási kötelezettség alapján ki kell térni:

- az adatkezelés jogalapjára;
- az egyes kamerák elhelyezése és a vonatkozásukban fennálló célra;
- a kamerák által megfigyelt területekre, tárgyakra;
- az adott kamerával közvetlen vagy rögzített megfigyelést végez-e a munkáltató;
- ki az elektronikus megfigyelőrendszert üzemeltető személy;
- a felvétel tárolásának helyére és időtartamára;
- melyek a felvételek tárolásával kapcsolatos adatbiztonsági intézkedések;
- kik jogosultak az adatok megismerésére, és a felvételeket milyen célból használhatja fel a munkáltató;
- munkavállalókat milyen jogok illetik meg az elektronikus megfigyelőrendszerrel összefüggésben, és milyen módon tudják gyakorolni a jogaikat;
- a munkavállalók információs önrendelkezési joguk megsértése esetén milyen jogérvényesítési eszközöket vehetnek igénybe.

[73] A megfigyelés során szerzett személyes adatok az adatkezelő jogszerű érdekének érvényesítéséhez szükségesek. Sérül az arányosság elve, ha az érintett érdekei ennél magasabb rendűek (alapvető szabadságjogok, magánélet tiszteletben tartásához való jog).

[74] Tudni kell bizonyítani a megfigyelés során szerzett adatok biztonságát, az adatkezelés megfelelőségét, valamint hogy a munkavállaló megfelelő tájékoztatásban részesült.

[75] Ezenfelül megfelelő indok szükséges.

A munkáltatónak bejelentési kötelezettsége van a kamerás megfigyelőrendszer használatáról a Nemzeti Adatvédelmi és Információszabadság Hatóság irányába, amennyiben a megfigyelt területen látogatók, ügyfelek tartózkodhatnak. Amennyiben csupán saját munkavállalók megfigyelését végzi, nem köteles bejelenteni.

Társasházi megfigyelés

A társasházakban kiépített kamerás megfigyelőrendszerre alapesetben vonatkoznak az általános elvek, azonban speciális szabályokkal egészülnek ki. Ilyen például, hogy a lakógyűlés kétharmadának a szavazata szükséges a rendszer kiépítéséhez. A megfigyelésnek és az adatkezelésnek szigorúan el kell válnia, a társasház lakóközössége mint jogi személy pusztán adatrögzítésre jogosult, a kezelést kizárólag szerződéses vagyonőr végezheti (ily módon a közösképviselő sem teheti), aki az illetékes hatósággal is tartja a kapcsolatot. A videórögzítőt zárt helyiségben kötelesek tartani, azokhoz az adatkezelőn kívül senki nem férhet hozzá, a felvételeket három napon belül meg kell semmisítani. A bizonyítékként felhasználandó felvételeket kizárólag lefoglalási jegyzőkönyv keretében a kezelő jogosult átadni a rendőrségnek, ügyészségnek. Azonban a lakóközösség tagjaként bárki megtagadhatja, hogy szerepeljen a felvételeken; ez esetben a kérvényező arcát ki kell takarni. A lakóházak esetén szintén él a tájékoztatási kötelezettség a megfigyelés tényéről.

Magánterületi megfigyelés

A magánterületi megfigyelés tekintetében a 2005. évi CXXXIII. Törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól minősül irányadónak. Fontos azonban, hogy magáncélú megfigyelés közterületen nem valósulhat meg, a magánépületekre telepített kamerák látószögébe kizárólag a saját birtokban levő ingatlan lehet, nem irányulhat nyilvános közterületre vagy ingatlanára. Amennyiben ez nem valósul meg teljes egészében, mert nincs mód másképp a kamerák kitakarására, úgy az üzemeltető köteles azokat a területeket kitakarni.[76] Magánterületen a tulajdonos szabadon dönthet megfigyelő rendszer üzemeltetéséről, a kép rögzítéséről, de ehhez hozzá kell járulnia az életvitelszerűen ott tartózkodóknak is. A tulajdonos a megfigyelés tényéről köteles tájékoztatni a szomszédokat; amennyiben pedig fennáll a lehetősége, hogy a kamera látószögébe kerülhetnek, akkor figyelmeztető táblával a járókelőket, továbbá fel kell hívni a területre belépő személyek figyelmét, hogy felvétel készülhet róluk, hogy ennek tudatában hozhassák meg a döntést, hogy belépnek-e, vagy sem a magánterületre. A magánterületeken végzett megfigyelésre is vonatkoznak az arányosság és célhoz kötöttség általános szabályai.

Közterületi megfigyelés

2009. szeptember 1-ig a rendőrség volt jogosult közterületi térfigyelő rendszer üzemeltetésére az 1994. évi XXXIV. törvény a Rendőrségről[77] alapján. Ezek a kamerák jellemzően forgalomfelügyeleti csomópontokban, nagy forgalmú utak kereszteződésében voltak telepítve, de ezek jól láthatóak kellett hogy legyenek.[78] Az új jogszabály a

[76] Videó-kaputelefon esetében, amennyiben az az utcára irányul, nem adhat felismerhető képet az egy méternél távolabb tartózkodókról.

[77] 1994. évi XXXIV. törvény a Rendőrségről. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99400034.TV (Letöltés ideje: 2017. december 13.)

[78] De megfigyelhető párhuzamosság is, amelyben a közterület-felügyelet üzemelteti a rendszert, az adatkezelést azonban a rendőrség látja el.

rendőrségen felül engedélyezte, hogy az önkormányzatok által működtetett közterület-felügyeletek is üzemeltethetnek köztéri térfigyelő rendszert, valamint végezhetnek ezzel kapcsolatos adatkezelést – természetesen ugyanolyan törvényi kötelezettséggel.

A közterületi megfigyelés esetében azonban problémát jelent, hogy nem tudunk kibújni a kamerák látószögéből, így pusztán ráutaló magatartással (elhaladunk előtte) fogadjuk el a megfigyelés tényét. Aggályos továbbá, hogy a gyakorlatban léteznek olyan kis lakosságszámú települések, ahol az önkormányzat egy helyiségből áll mindössze, és itt nincs mód elzártan üzemeltetni a megfigyelő rendszert, ami törvényi előírás lenne.

A felvételek tárolási idejére vonatkozó előírások

Vagyonvédelmi megfigyelés során általános esetben 3 munkanap, kiemelt esetekben, hatósági engedéllyel 30,[79] illetve 60[80] napot követően kell megsemmisíteni a felvételeket vissza nem állítható módon.[81]

A társasházi megfigyelések esetén a közös tulajdonban álló helyiségekben készült felvételeket 15 napig lehet megőrizni.

A közterület-felügyelet és a rendőrség által készített felvételek közül a (felügyeleti és a rendőrségi) intézkedésekről készült felvételeket 30 nap, a közbiztonsági és bűnmegelőzési kamerák felvételeit 8 nap elteltével köteles törölni az illetékes.

Közösségi közlekedési járművek belterében felszerelt kamerák felvételeit 16 napig lehet megőrizni, illetve közveszélyokozás és terrorcselekmény megelőzése érdekében ez lehet 30 nap is.

Jogsértések következményei

Az esetleges visszaéléseket a Nemzeti Adatvédelmi és Információszabadság Hatóság részére kell bejelenteni, amely a tapasztalt jogsértések szankcionálására is jogosult. Ez alapján elrendelheti a valóságnak nem megfelelő adatok helyesbítését, zárolását vagy törlését, illetve meg is tilthatja a személyes adatok jogellenes kezelését vagy feldolgozását. Súlyosabb esetben elrendelheti a kamerarendszer leszerelését. Amennyiben a felvételen szereplő személy betekintést kér a felvételbe, de az üzemeltető ezt jogellenesen megtagadja, a Hatóság elrendelheti az érintett tájékoztatását.

A Büntető törvénykönyv rendelkezik a személyes adattal való visszaéléssel. Ez alapján az adatok biztonságát szolgáló intézkedés elmulasztása, a jogosulatlan adatkezelés, valamint a tájékoztatási kötelezettség elmulasztása börtönbüntetéssel is szankcionálható. Minősített esetét jelenti, amennyiben hivatalos személyként vagy hivatalos eljárást színlelve valósul meg a személyes adattal való visszaélés, más tulajdonában álló területen történik az elektronikus megfigyelés, vagy üzletszerűen végzik a cselekményt.

---

[79] Amennyiben (1) emberi élet, testi épség, személyes szabadság védelme; (2) terrorcselekmény és közveszély okozás megelőzése; (3) jelentős értékű pénz, értékpapír, nemesfém biztonságos kezelése; (4) veszélyes anyagok őrzése.

[80] Pénzügyi szolgáltatást, jelzálog-hitelintézeti, befektetési szolgáltatási, tőzsdei tevékenységet, értékpapír-kezelést, biztosítási tevékenységet folytatók közönség számára nyilvános magánterületének védelme érdekében készült felvételek esetében.

[81] A határnapok a felvétel rögzítési idejétől számolandók, de nem érvényesek abban az esetben, ha a felvétel felhasználásra kerül. Felhasználás alatt bírósági vagy más hatósági eljárásban, bizonyítékként való felhasználást kell érteni

Intelligens térfigyelő kamerák

Az előzőekben ismertetett megfigyelések esetében módszertani problémát jelenthet, különösen közterületen, hogy túl sok kamerát üzemeltetnek, de nincs elegendő számú kezelőszemélyzet. Ennek kiküszöbölésére fejlesztették ki az intelligens térfigyelő kamerákat, ami a digitális kamerarendszereken zajló folyamatokat egy algoritmus segítségével értékelik, elemzik. Amennyiben valami szokatlan eseményt érzékel, riasztja a kezelőt, aki meghozza a szükséges döntést.

Az egyes rendszerek fejlettsége eltérő: vannak, amelyek csupán a rendszámok azonosítására képesek, de vannak, amelyek fejlett arcfelismerő szoftverrel vannak ellátva. Alkalmazástól függően az algoritmusnak képesnek kell lennie érzékelni a rendkívüli eseményeket, például egy őrizetlenül hagyott csomagot a kontextus függvényében, adott esetben üres térben, tömegben. A rendszereket folyamatosan fejlesztik; fontos elemét jelenti a gépi tanulás, aminek köszönhetően az esetleges változásokat is képes lesz észlelni – például a megfigyelt célszemély valamilyen változtatást eszközöl kinézetén. Ilyen intelligens kamerarendszerek kereskedelmi forgalomban kapható eszközök.

Közösségi média és elektronikus megfigyelés

Elsőre meglepőnek tűnhet, azonban a közösségi oldalak is működhetnek elektronikus megfigyelőrendszerként. Ennek oka az élő videóközvetítésekben keresendő, amelyet a nagyobb közösségi oldalak biztosítanak. Számos régi okostelefon van használaton kívül, amelyek egyébként tökéletesen alkalmasak kamerarendszer kiépítésére – nem egy alkalmazás épül erre az üzleti modellre, amelyek előfizetés függvényében akár mozgásérzékelő funkciót is használnak. Az okostelefonokba épített kamerák napjainkra igen komoly felbontással bírnak, így egy térfigyelőként használt okosmobileszköz komoly adatvédelmi aggályokat jelenthet.

Internetes megfigyelés mély csomagvizsgálattal

Az internet- és telefonszolgáltatók mindig is képesek voltak monitorozni a hálózatukon keresztül zajló adatforgalmat, kivel kommunikálunk, milyen weboldalakat látogatunk, azonban ezeket az adatokat többek között számlázáshoz, hálózatirányításhoz vagy marketingcélokra használták fel.

A mély csomagvizsgálatként defniált technológia segítségével azonban az interneten zajló kommunikáció teljes megfigyelése vált lehetővé a szolgáltatóknak, a nemzetbiztonsági szolgálatoknak egyaránt. A technológia segítségével monitorozni lehet, milyen weblapokat kerestünk fel, milyen videókat nézünk, milyen zenét hallgatunk, kivel mit beszélünk, akár e-mailben, akár valamilyen üzenetküldő alkalmazás segítségével. A mély csomagvizsgálatot végző alkalmazások megnyitják és átvizsgálják az üzeneteket, hogy kiszűrhessék közülük azokat, amelyek veszélyes tartalmakat hordoznak. Ez egyben azt is jelenti, hogy mindez automatizáltan történik, nem kell gyanúsítottnak lennünk valamilyen bűncselekményben. Ez azért fontos kitétel, hiszen valakinek a megfigyelése szigorúan bírósági vagy miniszeri felhatalmazás alapján valósulhat meg, jogszabály alapján.

Az információ, amit valakinek küldünk, egy igen bonyolult folyamaton keresztül érkezik meg, több számítógépen keresztül áthaladva. Ezek az eszközök az üzenetet – hogy könnyebben kézbesíthessék a hálózaton – feldarabolják több részre, ezeket nevezzük csomagoknak. Amikor ezek a csomagok megérkeznek a fogadó eszközre, újra összeállnak eggyé. Minden csomag több rétegből tevődik össze, amik különböző információkat tartalmaznak. Az internetszolgáltatóknak mindenképpen át kell vizsgálniuk bizonyos csomagokat, hiszen azok tartalmazzák példá-

ul, hogy az adott üzenetnek ki a címzettje. Ezek az információk azonban a felszínen vannak, ezért is nevezzük felszíni csomagvizsgálatnak. Mély csomagvizsgálat esetén az alkalmazás átvizsgálja a többi réteget is, vagyis az üzenet teljes tartalmát. Az algoritmusok mély csomagvizsgálat esetén bizonyos kulcsszavak alapján elemzik a tartalmakat, de hogy milyen tartalmak alapján történik a vizsgálat, azon múlik, ki futtatja, milyen szempontrendszert határoz meg. Ezek a beállított kulcsszavak kapcsolatban lehetnek konkrét bűncselekményekkel, vásárlási szokásokkal vagy rosszindulatú alkalmazásokkal. A mély csomagvizsgálatot eredetileg pont azért fejlesztették ki, hogy a segítségével ki lehessen szűrni a számítógépes kártékony kódokat. Mára azonban ez odáig fejlődött, hogy minden károsnak ítélt tartalom detektálható – később, mint látni fogjuk, ez meglehetősen aggályos kérdések felvetéséhez vezet.

A kezdetekben internetes cégek alkalmazták csupán a mély csomagvizsgálatot, de hamar felismerték a védelmi szférában is a jelentőségét, így a használata ott is elterjedt.

Európában, ahol hagyományosan szigorúbb az adatvédelem, legálisan csak korlátozott módon lehet alkalmazni; csupán hálózatbiztonsági szempontokból használhatják, hogy kiszűrjék a rosszindulatú alkalmazásokat. A gond az, hogy bár a technológia segítségével rengeteg káros tartalmat lehetne kiszűrni – gondoljunk csak a pedofil tartalmakra – az európai jogi szabályozás elavult, és még nem készült olyan, ami megfelelő módon képes lenne szabályozni a mély csomagvizsgálatot. Ezzel szemben az Amerikai Egyesül Államokban nincs erre vonatkozó normatív szabályozás, a cégek sokkal szabadabban élhetnek ezen eljárással. A gond ezzel az, hogy európaiként használunk olyan szolgáltatásokat, amelyeket amerikai cégek biztosítanak (például Gmail levelezőrendszer, Facebook), és az ezeken továbbított üzeneteink az Egyesült Államokban átesnek mély csomagvizsgálaton. Jelenleg nem kidolgozott, hogy milyen módon lehetne korlátozni a mély csomagvizsgálatot, mint ahogyan azt sem tudni, hogyan lehet észlelni. A szabályozás legnagyobb akadálya, hogy a technológia olyan gyorsan fejlődik, amivel a jogszabályalkotás nem képes felvenni a versenyt. Különösen a nemzetközi térben, hiszen az üzeneteink a világháló különböző pontjain haladnak végig, mielőtt megkapnánk őket, így olyan országok is érintettek lehetnek, amelyek az adatvédelmet illetően sokkal megengedőbbek, és az általuk elvégzett mély csomagvizsgálat során megfigyelteket nem tudni, hogy milyen módon használják fel az adott ország nemzetbiztonsági szolgálatai.

Mély csomagvizsgálatot motiváció alapján kereskedelmi, valamint közbiztonsági és nemzetbiztonsági céllal végeznek. Kereskedelmi céllal a hálózatbiztonsági felügyeletet, a digitális jogok védelmét, illetve a viselkedés alapú reklámokat említhetjük. Közbiztonsági és nemzetbiztonsági mély csomagvizsgálat bűncselekmények felderítésére, megelőzésére alkalmazható, valamint cenzúra is hatékonyan valósítható meg a technológia segítségével. Ahogyan fentebb, a kulcsszavak kapcsán már érintettem, a technológia alkalmazójától függ, milyen szempontrendszert határoz meg a szűrésre. A mély csomagvizsgálatot vélelmezhetően diktatórikus államok használják cenzúrára, ellenzéki vélemények elhallgattatására, ellenzékiek megfigyelésére. Ismereteink szerint többek között Kína, Irán, Líbia használja e célból a technológiát.

Okostelefonos helymeghatározás

A mobiltelefonokat, akárcsak a kamerás megfigyelő rendszert, a második világháború alatt fejlesztették ki. Ez az eszköz gyakorlatilag üzenetek küldésére és fogadására képes vezetéknélküli rádióvevő volt. A mikroprocesszorok fejlődésével az 1970–80-as években jelentek meg a „kézi" telefonok, de ezek még relatíve nehezek, téglaméretűek voltak, az akkumulátorok üzemideje pedig 20 perc volt. Az 1980-as években egyre több mobiltelefon-tornyot állítottak üzembe, ami jelentősen javította a helyi és nagy távolságú mobilkommunikációt.

A mobiltelefon-tornyok elengedhetetlenek a mobiltelefon működéséhez. A tornyok egy bizonyos földrajzi terület lefedéséért felelnek; a mobiltelefon használata nem lehetséges, ha nem kapcsolódik a legközelebbi mobiltelefon-toronyhoz. Ebből következően a torony rögzíti a kapcsolódó mobiltelefon helyét, amikor a felhasználó helyet változtat, és ha egy másik torony esik hozzá közelebb, a készülék automatikusan átkapcsolódik ahhoz a toronyhoz. Ez egyben azt is jelenti, hogy a mobilszolgáltató képes nyomon követni felhasználóinak mozgását csak abból, hogy a készüléke melyik mobiltoronyhoz kapcsolódik. Ezeket az adatokat a jelenleg érvényben levő európai uniós előírások alapján a szolgáltatók legalább 6, legfeljebb 24 hónapig tárolhatják.[82]

Az okosmobileszközök megjelenésével azonban két új módszer is kialakult, amellyel megfigyelhetővé válik a felhasználó helyzete: a globális helymeghatározó rendszer (GPS), illetve vezeték nélküli hálózatok segítségével ugyanúgy bemérhető a felhasználók tartózkodási helye.

A helymeghatározás az okosmobileszközök esetében számos népszerű alkalmazás kifejlesztését hozta el, hiszen maga a funkció rendkívül hasznos lehet. Nem csupán közelünkben levő helyeket találhatunk meg (mozi, pizzéria, söröző), hanem játékokat játszhatunk a segítségével (gondoljunk csak a kiterjesztett valóságot felhasználó Pokémon Góra), de veszélyhelyzet esetén is megkönnyíti a segélykérést. A gond ezzel nem más, mint hogy sokszor nem tudjuk, az alkalmazás készítői hogyan kezelik az adatainkat, hiszen nem egy esetben derült ki, hogy harmadik félnek adták el az ily módon begyűjtött információkat.[83] Igen aggasztó az is, hogy ezekből az adatokból kinyerhetőek a bizalmas, magántermészetű látogatások, amelyek adott esetben felhasználhatóak a személy ellen; így az egészségügyi intézmények, felekezeti hovatartozáshoz köthető intézmények, de ügyvédi irodák, sztriptíz- és, homoszexuális bárok, bizalmas találkozóra igénybe vett helyek ezekből az adatokból előállíthatóak. Elméletileg, ha a felhasználó kikapcsolja a helymeghatározást, akkor nem követhető nyomon, azonban egyrészt ez távolról aktiválható, másrészt az Androidos készülékek esetében vált ismertté, hogy kikapcsolás esetén ugyanúgy rögzítette a felhasználók helyzetét.[84]

A vezeték nélküli hálózatok – hasonló módon a mobiltornyokhoz – regisztrálják a kapcsolódó mobilkészülékeket, és visszakereshetőek az előzőleg csatlakozott hálózatok. Védelmet jelent az ilyen követés ellen, ha kikapcsoljuk a telefonon vezeték nélküli hálózathoz való csatlakozás funkcióját.[85]

Az okosmobileszközök helymeghatározását – a mély csomagvizsgálathoz hasonlóan – kereskedelmi, valamint közbiztonsági és nemzetbiztonsági céllal használják. Kereskedelmi célból többek között telefonos értékesítésre, célzott értékesítésre vagy akár várostervezésre. Közbiztonsági és nemzetbiztonsági célból többek között alkalmazzák eltűnt, sérült személyek felkutatására, bűnelkövetéssel gyanúsított személyek mozgásának nyomon követésére.[86]

---

82 Az Európai Unió Bírósága 2014-ben megsemmisítette a jogszabályt, de a tagállamok még nem építették be a vonatkozó normatív szabályozásukba ezt.

83 Adatokat eltulajdonító androidos zseblámpa-alkalmazás. In: GovCERT, 2013. december 6. URL: http://tech.cert-hungary.hu/tech-blog/131206/adatokat-eltulajdonito-androidos-zseblampa-alkalmazas (Letöltés ideje: 2017. december 14.)

84 COLLINS, Keith (2017): Google collects Android users' locations even when location services are disabled. In: Quartz, 2017. november 21. URL: https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/ (Letöltés ideje: 2017. december 17.)

85 Az iOS 11-es verziója hozta be azt az újdonságot, hogy a gyors elérésből nem lehet teljesen kikapcsolni a WIFI-t, ahhoz a Beállításokban kell kiválasztanunk ezt a tiltást. Ha a gyors elérést választjuk, akkor a készülék automatikusan bekapcsolja a WIFI-t, ha például korábban elmentett hálózatot érzékel.

86 De ugyanúgy családtagok követésére is használható.

Problémát jelent az is, hogy a geolokációs helymeghatározás során csoportok is azonosíthatóvá válhatnak, ami mondjuk egy tüntetés esetén az azon részt vevők beazonosítására is felhasználható. Ezt kivédendő, egyre több alkalmazást készítenek, ami a használójáról hamis geolokációs adatokat jelenít meg.

Okosmobileszközökre írt alkalmazások

Hogy mitől számít egy mobilkészülék okosnak, megoszlanak a definíciók, azonban a napjainkban használt okosmobilkészülékek esetében az alkalmazások megkerülhetetlenek. Ezek a helymeghatározás mellett rengeteg egyéb módot biztosítanak a felhasználók megfigyelésére.

Minden alkalmazás, legyen az ingyenes vagy fizetős, a használatáért cserébe különböző alkalmazásengedélyeket követel meg. Ezek az engedélyek sokfélék lehetnek, de alapesetben az alkalmazás funkciójához elengedhetetlen engedélyeket kérnek: egy zseblámpa-alkalmazás esetén a vakuhoz való hozzáférés adekvát; egy diktafonalkalmazás esetén a mikrofon vezérlését kéri, illetve azt, hogy hozzáférhessen az eszköz tárhelyéhez, és azon módosíthasson; egy üzenetküldő alkalmazás esetében feltétel, hogy az üzeneteinkhez férhessen hozzá, egy fényképalkalmazásnál pedig, hogy vezérelhesse a kamerát; stb.

A gond abból ered, hogy a felhasználók rendkívül óvatlanok az alkalmazások telepítésekor, és nem olvassák el, milyen engedélyeket adnak az alkalmazásnak. Egy alkalmazás ily módon kérhet olyan engedélyeket is, amelyek a használathoz nem szükségesek, ahogy a fentebb említett zseblámpa-alkalmazás esetén is volt. Az ily módon gyűjtött adatokat, amelyek gyakorlatilag mindent tartalmazhatnak, ami a mobilkészülékünkön szerepel, általában marketingcéllal értékesítik, de a célzott megfigyelés eszközei is lehetnek, hiszen egy kamera- és mikrofonvezérlést, az üzenetek tartalmához való hozzáférést engedélyező felhasználót az alkalmazás fejlesztői bármikor, akár valós időben lehallgathatnak, a kamera képét felhasználva megfigyelhetnek. Arról nem is beszélve, egyes alkalmazások egészségügyi adatokat is tárolnak rólunk,[87] amelyek védelme különösen fontos. Megadhatjuk, mire vagyunk allergiások, érzékenyek – az indok szerint, amik „fontosak lehetnek vészhelyzetben". Ez valóban fontos és hasznos. A gond az, ha az eszköz védelme nem megfelelő, a felhasználó olyan alkalmazásoknak is engedélyt ad, amik a készüléken tárolt adatokhoz is hozzáférhetnek, ezek pedig az adatokat is megszerezhetik. Ennek következménye lehet például az is, hogy ismerve valakinek az ételérzékenységét olyan étellel kínálják meg, amire allergiás, hogy ily módon okozzanak kárt neki.

Biometria

A biometrikus azonosítás története a 19. századra nyúlik vissza. Ekkorra az államok igazságügyi rendszereinek fejlődésekor felmerült az igény egy központosított, formalizált személyazonosító módszer kialakítására. Ennek egyik oka abban lelhető fel, hogy az igazságszolgáltatás jellemzően elnézőbb volt azokkal az elkövetőkkel szemben a

[87] Mi több, az iOS Egészség alkalmazásával egészségügyi dokumentumokat tárolhatunk a telefonunkon, s oszthatunk meg másokkal.

büntetési tételek meghatározásakor, akik először követtek el bűncselekményt, mint azokkal, akik visszaesőnek minősültek. Az elgondolás szerint ebben a központosított nyilvántartásban rögzítették volna az elkövetett bűncselekményeket, és az elkövetők valamilyen egyedi jellemzőjét. Franciaországban Alphonse Bertillon dolgozta ki a „Bertillonage"-nak nevezett eljárást, amely az egyének részletesen rögzített testi jellemzőit, például magasságukat, karjuk hosszát, külsejük leírását, valamint fényképeiket használta személyazonosításra. A továbblépés Francis Galton nevéhez fűződik, aki felismerte, hogy az emberek ujjlenyomata egyedi, és ez sokkal egyedibb azonosítást eredményez. A következő nagyobb ugrás az 1930-as évekre datálható; ekkor állt elő Frank Burch a retina mintázatait alapul vevő azonosítás ötletével, majd az 1960-as évektől kezdték el az arc-, valamint hangfelismerő technológiák kidolgozását.

Biometrikus jelzővel olyan rendszereket illetünk, amelyek személyek mérhető fizikai jellemzőit – az ujjlenyomatot, a DNS-t, a retina véredénystruktúráját, az arcvonásokat, esetleg a test szagát – használják, vagy egyedi viselkedési jellegzetességeket vizsgálnak, mint például a testtartás, a hang, esetleg a billentyűleütési szokások, abból a célból, hogy segítségével azonosítani, kategorizálni lehessen a személyeket. Több országban, köztük hazánkban is, rögzítik az állampolgárok valamilyen biometrikus azonosítóját az új típusú okmányokon.

A biometrikus azonosítás első lépése, hogy rögzítik az egyén valamely jellemzőjét, hogy egy biometrikus adatbázisban tárolják. Később az azonosítás ennek a rendszernek a segítségével történik, amikor a rögzített jellemzőket beolvassa az arra hivatott interfész.

Biometrikus azonosítást sokáig a rendvédelemben alkalmaztak bűncselekmények ismert vagy még ismeretlen elkövetőinek azonosítására, illetve annak megállapítására, hogy valaki jogosult-e belépni egy védett területre, például kormányhivatalokba, kutatólaborokba stb. A biometrikus azonosítást egyre gyakrabban alkalmazzák a határvédelem során. Az Európai Unióban például 10 ujjlenyomatot és egy digitális fotót rögzítenek azokról, akik EU-s vízumot kérvényeznek, amiket a VIS-adatbázisban (Visa Information System – Vízuminformációs Rendszer) tárolnak. Hasonló elven működik az EUROADAC-adatbázis, ami a 2003 óta érvényben levő dublini egyezményt hivatott segíteni azáltal, hogy az Európai Unió területére illegálisan érkezett menekültek biometrikus azonosításával megállapítsák, kik jogosultak az EU-n belül tartózkodni, kinek a kérelmét utasították el korábban, az EU mely tagállamában kérvényezte a tartózkodási engedélyt, stb.

A biometrikus azonosításnak katonai alkalmazása is elterjedt. Az Amerikai Egyesült Államok hordozható készüléket rendszeresített, amit elsősorban az iraki és afganisztáni hadszíntereken alkalmaztak a katonákkal kapcsolatba kerülő egyének azonosítására a szivárványhártya- mintázat vagy más biometrikus jellemző felhasználásával. Az ily módon gyanúsnak ítélt személyeket az „Engedélyezett Biometrikus Megfigyelési Listában" tárolták, és a rendszer azonnal jelezte a katonáknak. A legutóbbi információk szerint több mint 200 ezer személy adatait tartalmazta világszerte.

A rendvédelmi felhasználás mellett egyre jobban elterjedt a magánszférában is, hiszen a biometrikus azonosításon alapuló beléptetés biztonságosabb, mint például egy kártyás eljárás. Előnye, hogy a biometrikus jellemzőket nem lehet elhagyni, otthon felejteni, mint egy kulcsot vagy egy kártyát. Az azonosítás azonban itt is problémás lehet, ugyanis egy nem megfelelő rögzítés a későbbiekben megnehezíti az azonosítást, valamint ha kis mértékben is, de ezek a jellemzők az évek során megváltozhatnak.

A biometrikus azonosítást nem csak a biztonsági cégek alkalmazzák, egyre több okosmobileszköz ujjlenyomat-leolvasóval készül, de több gyártó az arcfelismerést igyekszik fejleszteni – eddig nem túl sok sikerrel, ahogyan az iPhoneX esetében is a várt áttörés elmaradt legutóbb.

Az arcfelismerés a gépi mélytanulás segítségével egyre hatékonyabb, ahogy a Facebook DeepFace nevű programja is példázza. Az algoritmus 97,25%-os pontossággal állapítja meg két képről, hogy ugyanaz a személy látható-e rajta.[88] A funkciót a felhasználók által feltöltött képek esetében használják, hogy automatikusan felismerje a képen látható személyeket, és segítse azok bejelölését. Ennek természetesen ismét van egy geolokációs helymeghatározáshoz hasonló aggálya, hiszen a fejlett arcfelismerő szoftverek képesek lehetnek tüntetésen részt vevők azonosítására is, ami a kormányzati berendezkedés függvényében igen komoly problémákat vethet fel. A képfelismerő szoftverek a rendvédelemben is igen hasznosak, erre igazán jó példa a Microsoft és a Darthmouth Egyetem közös szoftvere, a PhotoDNA. A program a bűnüldözés során elsősorban a kiskorúakat érintő szexuális abúzus felderítésében jelentős segítség. A technológiát beépítették saját képelemzőjükbe a nagyobb közösségi oldalak, így a Facebook és a Twitter is. Az algoritmus a képekből bizonyos matematikai modellek alapján egy, az ujjlenyomathoz hasonló egyedi azonosítót állít elő, aminek hatására képes azonosítani az adott képet. Ez önmagában véve nem lenne előrelépés, de a program ezt akkor is tudja, ha a képen bármilyen módosítást hajtottak végre: pédául átméretezték, Photoshoppal módosították, levágtak belőle, stb. A nyomozók a lefoglalt pedofiltartalmakat lefuttatják az alkalmazással, és ezt követően, ha az interneten valahol elérhetőek lesznek, a szűrő jelezi a találatot.[89]

A kereskedelmi felhasználásban a fentieken kívül megjelentek az olyan fejlesztések, elsősorban bankoknál, amely hang alapján azonosítja az ügyfeleket, hogy a jelszó bemondását követően intézhessenek tranzakciókat. Megjelentek olyan közterületen elhelyezett reklámfelületek is, amelyek a járókelőket nem és életkor alapján elemzik, hogy annak megfelelő hirdetést jelenítsenek meg. Egy másik iránya a fejlesztéseknek, hogy az azonosításon túl viselkedéselemzésben hasznosítják a biometrikus jellemzőket; számos fitneszalkalmazás használ légzés- és pulzusszámlálót, amelyek segítségével edzéstervvel, életvezetési tanácsadással látják el a felhasználókat.

A korábban tárgyalt intelligens térfigyelő rendszerek szoftverei is tartalmazhatnak biometrikus azonosításra szolgáló elemeket, ami új lehetőségeket biztosít a távfelügyeletben és megfigyelésben. A gépi tanulás ez esetben azt jelenti, hogy az ilyen rendszerek úgy is gyűjthetnek adatokat rólunk, hogy mi nem tudunk annak a tényéről.

Nem szabad elfeledkezni arról sem, hogy a korábban rögzített biometrikus adatokat valamilyen informatikai rendszerben tárolják, amihez kellő szakértelemmel nem elképzelhetetlen, hogy illetéktelenek hozzáférjenek, így meghamisíthatják ezeket az azonosítókat, ez pedig személyiséglopáshoz is vezethet, ami – ha a fenti bankok hangazonosítással kapcsolatos példájára gondolunk – akár komoly pénzügyi kockázatot is magában foglalhat. Jelenleg azonban még mindig könnyen át lehet verni bizonyos biometrikus azonosító rendszereket, mint például az arcfelismerő szoftvereket. Elég lehet smink, új frizura, borosta vagy – ahogyan a Samsung telefonok esetében – a felhasználó kinyomtatott fényképe. További probléma, hogy míg a biometrikus azonosítás drága és időigényes tevékenység volt, egyfajta védelmet jelentett a személyes adatainkat illetően. A tömegessé válás azonban egyrészt

[88] TAIGMAN, Yaniv (2014): DeepFace: Closing the Gap to Human-Level Performance in Face Verification. In: Facebook Research, 2014. június 24. URL: https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/ (Letöltés ideje: 2017. december 14.)

[89] Érdemes elolvasni a témában az Indexen megjelent teljes interjút. HANULA Zsolt (2016): Ezek nagyon okos fickók, de a végén úgyis elkapjuk őket In: Index, 2016. július 31. URL: https://index.hu/tech/2016/07/31/ezek_nagyon_okos_fickok_de_a_vegen_ugyis_elkapjuk_oket/ (Letöltés ideje: 2017. december 14.)

genetikai alapú diszkriminációhoz, illetve megfelelő biztosítékok hiányában a magánszféra jelentős szűküléséhez vezet, hiszen azáltal, hogy az okostelefonok, közösségi oldalak, intelligens térfigyelő rendszerek használják a technológiát, az anonim, ellenőrizhetetlen és szabad mozgásunk fokozatosan csökken. Arról sem szabad elfeledkezni, hogy korábban egy biometrikus adat rögzítéséhez az érintett egyén jóváhagyása szükséges volt,[90] az arcfelismerő szoftverek elterjedésével és alkalmazásával azonban erre nincs lehetőség, automatikusan, beleegyezésünk nélkül rögzítik arcunk jellemzőit. Mindez nagyban sérti az önkéntes belelegyezés jogát, valamint azt sem tudjuk pontosan, kik kezelik ezeket az adatokat, és mire használják fel. A Facebook DeepFace nevű algoritmusával, ami 97,25%-os pontossággal képes felismerni a felhasználókat a feltöltött képek alapján, rögtön más megítélés alá esik – véleményem szerint.

Pilóta nélküli légi járművek

A közvélemény a drónokat – tévesen – a pilóta nélküli repülőeszközökkel azonosítja, azonban ugyanúgy drón a pilóta nélküli eszköz, ami szárazföldön, vízen vagy a föld alatt közlekedik. A köznyelvben drónként használt eszköz hivatalos neve UAV, vagyis Unmanned Aerial Vehicle, azaz pilóta nélküli légi jármű.[91]

A pilóta nélküli légi járművek története az első világháború idejére nyúlik vissza. 1916-ban fejlesztette kis Archibald Low professzor, légügyi miniszter azokat a rádiós távirányítással irányított eszközöket, amelyeket a robbanóanyagokkal megrakott Zeppelin-léghajók elhárítására terveztek.

A pilóta nélküli légi járművek alkalmazási területei roppant széles körűek, kereskedelmi, rendészeti, katonai, nemzetbiztonsági szempontok alapján egyaránt jelentősek. A katonai felhasználás során alkalmazzák felderítésre, megfigyelésre, tüzérségi tűz helyesbítésére, célmegjelölésnek irányított fegyverek esetében, rádióelektronikai zavarásra, rádiótechnikai átjátszásra, célrepülőgépnek éleslövészetnél, zavarórepülésnek,[92] földi célok elleni csapásmérésre, illetve robotrepülőgépként is. Rendészeti aspektusból határvédelmi feladatok ellátására, rendezvények biztosítására, térfigyelő kamera kiváltására, tűzoltásra, tömegrendezvények megfigyelésére, tömegoszlatásra, természeti katasztrófák esetén személyek felkutatására, mentőtevékenységek ellátására, bűnügyi helyszínelésre, kábítószer-ültetvények felkutatására, rendőrségi üldözések támogatására alkalmazhatóak. Kereskedelmi forgalomban elláthatnak többek között térképészeti feladatokat, házhozszállítást végezhetnek, építkezéseknél alapanyagokat szállíthatnak, de ugyanúgy alkalmasak az időjárás megfigyelésére, sportesemények közvetítésére, mezőgazdasági földek permetezésére. Előnyük, hogy olyan helyeken is bevethetők, amelyeket embereknek veszélyes lenne megközelíteni: lavinák, földrengések, nukleáris balesetek helyszínein kiválóan alkalmasak mérési és egyéb feladatok ellátására.

[90] Kivéve persze a bűncselekmények elkövetői, gyanúsítottjai.

[91] Speciális fajtáját jelentik az úgynevezett Távolról Irányított (Légi) Járművek (RPV– Remotely Piloted (Aerial) Vehicle), illetve a harci robotok, vagyis olyan eszközök, amelyeket fegyverrel látnak el. Laikusok gyakran robotrepülőgépként hivatkoznak ezekre az eszközökre, ami azért téves, mert míg a robotrepülőgép maga a „fegyver", ami a bevetéskor megsemmisül, addig a pilóta nélküli légi járművek több alkalommal felhasználhatóak.

[92] Ez esetben például dezinformációs célt szolgál; vadászrepülőgépek jelenlétét kívánják elhitetni az adott műveleti területen.

A pilóta nélküli légi járművek kategorizálását több szempont szerint végezhetjük el: felhasználási terület, méret vagy meghajtórendszer alapján szokás megkülönböztetni őket.

A közterület megfigyelésére használt pilóta nélküli légi járművek előnye, hogy mozgékonyságuk okán sokkal nagyobb területet képesek ellenőrizni, a repülési magaslatok pedig új perspektívát jelentenek a rögzített kamerarendszerekkel szemben. Ebből következően képesek a gyanúsnak ítélt tárgyakat, személyeket jelezni, megjelölni, valamint a megjelölt személyeket követni. A repülési magasság függvényében mindezt rejtett formában is végezhetik, ellenben mondjuk a követést végző személyekkel. A közterület megfigyelésre alkalmazott pilóta nélküli légi járműveket így a bűnelkövetők is nehezebben veszik észre, aminek megvan az a pszichológiai hatása, hogy nem tudják biztosan, éppen megfigyelik-e az adott területet, vagy sem. Ez egyben az emberek biztonságérzetét is növelheti, hiszen annak a tudata, hogy egy esetlegesen bekövetkező rendkívüli eseményt egy felettünk tartózkodó pilóta nélküli légi jármű érzékel, azt az érzetet keltheti, hogy a riasztás hatására gyorsabban siethetnek a segítségünkre.

Másik oldalról viszont ez megteremti a lehetőségét annak, hogy még nagyobb mértékben gyűjtsenek rólunk adatokat, ami a korábban tárgyalt intelligens térfigyelő rendszerek és biometrikus azonosítás és viselkedéselemzés ötvözéséből igen komolyan szűkíti a magánszféránkat. A rögzített köztéri kamerákkal szemben a pilóta nélküli légi járművek olyan helyekről is képesek felvételt készíteni, amit a térfigyelő kamerák nem láthatnak be: falakon, kerítéseken túlról, a levegőből megnyílik a lehetőség, hogy olyan mértékben hatoljanak be a magánszféránkba, amire korábban nem volt lehetőség. Mindezt nem csak rendvédelmi szervek tehetik meg, hanem bárki, aki megvásárolt egy kamerával felszerelt pilóta nélküli légi járművet. Jelen szabályozás alapján ezeket az eszközöket nem kell regisztrálni, így nem tudjuk, hogy ki repteti például a kertünk fölé, és rögzíti az ott történteket, így feljelenteni sem tudjuk a privát szféránk vagy a személyes adataink megsértése miatt. A pilóta nélküli légi járművek esetében ugyanúgy létező kockázat, hogy az általuk tárolt adatokhoz illetéktelenek férnek hozzá, amennyiben feltörik azok informatikai rendszerét. Továbbá nem utolsó szempont, hogy sokkal kitettebbek a környezeti hatásoknak, és mivel nem vonatkoznak rájuk olyan szigorú biztonsági előírások, így meghibásodás esetén akár igen súlyos sérülést, közlekedési balesetet is okozhatnak, ha például nagy magasságból zuhannak rá egy alattuk tartózkodó személyre, járműre.

A fentiekből következően kiemelten fontos ezen eszközök normatív szabályozása, hiszen már pár tízezer forintért bárki vásárolhat magának ilyet. A jelenlegi nemzetközi szabályozás alapján minden nemzet saját hatáskörében dönthet a 150 kg felszállótömegű repített tárgyakról. Magyarországon 25 kg az a határ, ameddig a levegőbe küldhető bármi, és az adott esetben játéknak minősül. 2017 nyarára ígérték a hazai jogalkotók, hogy hatályba lép az úgynevezett „drónrendelet",[93] ami a pilóta nélküli légi járművek esetében töltené be a hiányzó szabályozási űrt. E tankönyv írásának idején (2017. év vége) a jogszabályt még mindig nem fogadta el az Országgyűlés, és nem lehet tudni, hogy ez mikor valósul meg. A rendelet négy kategóriába sorolja a pilóta nélküli légi járműveket. Ez alapján:

1. kategória: 250 gramm alatt nem kötik feltételhez a reptetést, ezek a drónok játéknak minősülnek majd;

2. kategória: 250 grammtól 2 kilogrammig egy online elérhető tanfolyam elvégzéséhez kötik a reptetést. Szintén ebbe a kategóriába tartoznak azok a pilóta nélküli légi járművek, amelyek repülési magassága meghaladja az 50 métert;

[93] A jogszabály elérhető: A Kormány …/2016. (… ...) Korm. rendelete az egyes légiközlekedéssel összefüggő kormányrendeletek módosításáról. URL: http://www.kormany.hu/download/8/db/e0000/RPAS__honlapra.pdf#!DocumentBrowse (Letöltés ideje, 2017. december 14.)

3. kategória: 2 és 25 kilogramm között már online nyilvántartásba kell venni a drónt, a pilótának vezetői engedélyt kell kiváltania, amihez képzésen kell részt vennie.
4. kategória: 25 kilogramm fölött, a jelentős közlekedésbiztonsági kockázat miatt, szakszolgálati engedély kell a reptetéshez, valamint üzemi és repülési naplót kell vezetni az eszköz légi alkalmassági vizsgálatához.

A jogszabály kötelező felelősségbiztosításról is rendelkezik, kategóriáktól függően 3–10 millió forintos összeghatárig védő felelősségbiztosítást tenne kötelezővé. A rendelet mellett egy mobilalkalmazás bevezetését is tervezik, amelynek használatával a tulajdonosok ellenőrizni tudják, hogy az adott terület fölött használhatják-e az eszközüket.

Fontosabb fogalmak

Adatbiztonság, adatvédelem, adatvédelmi felelős, adatvédelmi incidens, adatkezelés, Általános Adatvédelmi Rendelet, Big Data, biometria, bűnügyi személyes adat, elektronikus megfigyelő rendszer, értesülés joga, felszíni csomagvizsgálat, geolokációs helymeghatározás, gépi mélytanulás, információs szabadság, intelligens térfigyelő rendszer, közérdekből nyilvános adat, közérdekű adat, külföldi minősített adat, különleges adat, magánszféra, mély csomagvizsgálat, mesterséges intelligencia, minősített adat, nemzeti minősített adat, pilóta nélküli légi jármű, személyes adat, vezeték nélküli hálózat

Áttekintő kérdések

- Milyen eszközöket használ annak érdekében, hogy minimalizálja vagy akár teljesen megszüntesse annak a lehetőségét, hogy megfigyeljék internetes tevékenységét?
- Hasznosnak találja a személyre szabott reklámokat, mint a Facebook és a Google reklámjai?
- Véleménye szerint mennyire érzékeny az átlag felhasználó a közösségi oldalakon az adatvédelemre?
- A Facebook rengeteg szempont alapján elemezi az egyes felhasználókat, hogy a lehető legpontosabban jelenítse meg a felhasználóknak a személyre szabott reklámokat. Ön szerint ezeket az információkat csak marketingcélokkal használják fel?
- Véleménye szerint az internetes anonimitásnak mindenek felettinek kell lennie, mert ez a szabadság biztosítéka, vagy egy olyan jog, amit a bűnözők, a terroristák használnak ki, így a biztonságunk érdekében feláldozható?

4. A KÖZÖSSÉGI MÉDIA SZEREPE A HÍRSZERZÉSBEN, ELHÁRÍTÁSBAN

A közösségi média használata több tekintetben eredményezett paradigmaváltást Minden túlzás nélkül állítható, hogy nem csupán az interperszonális interakciók viszonyában hozott minőségi változást,[94] átalakította többek között a nyilvánosság szerepét, a magánszféra megítélését, értékét alapjaiban kérdőjelezte meg, de az információhoz való hozzáférés minőségében és mennyiségében is újat hozott. A nemzetbiztonsági szolgálatok egyből felismerték ezen oldalak nyújtotta lehetőségeket, és szinte a kezdetektől igyekeztek tevékenységük során felhasználni őket. Edward Snowdennek köszönhetően rengeteget tudtunk meg azokról a képességekről, amelyek a nemzetbiztonsági szolgálatok közösségi médiában való hírszerző tevékenységével kapcsolatosak. A hírszerzésen és elhárításon kívül természetesen egyéb műveleteket is végeznek a közösségi médiát felhasználva, elég csak a lélektani műveletek növekvő szerepére gondolni, ebben a fejezetben azonban csupán az információszerzésről lesz szó.

4.1. A NEMZETBIZTONSÁGRÓL ÁLTALÁBAN

A hírszerzést gyakran a második legősibb szakmaként szokták nevezni, holott vélhetően idősebb, mint a közvélekedés szerinti legősibb szakma (arról nem is beszélve, hogy gyakran veszik igénybe a „legősibb szakmát", hogy segítségével szerezzenek információkat). Nem véletlen, hiszen ahogy a magánszféra és kiberbiztonság címet viselő fejezetnél már volt szó róla, a kormányzatoknak, annak érdekében, hogy megfelelő módon elláthassák a funkciójukat, minél több információra van szükségük. Ez a megállapítás érvényes az emberi történelem minden időszakára, csupán a technikai-technológiai innováció hatására összetettebb tevékenységgé vált. Az őskortól kezdve az ember mindig is igyekezett megtudni, mik az ellenségei szándékai, egy hadjárat során milyen lépéseket tervez ellene, melyik a legideálisabb terep a harc megvívására, vagy érdemes-e egy adott területet meghódítani, és ott letelepedni.[95]

A történelem során a hírszerzésért felelős szolgálatok döntően a háttérben tevékenykedtek, munkájukról nem igazán szóltak még a nagy hadvezérek visszaemlékezései sem, holott nélkülük egészen biztosan nem értek volna el sikereket. Nem túlzás kijelenteni, sokszor az emberiség történelmét teljes egészében meghatározó volt a hírszerző szolgálatok sikere [96], vagy az elhárításért felelős szolgálatok kudarca [97], vagy a politikusoké, akik nem vették komolyan az információkat.[98]

---

[94] Hogy jót vagy rosszat, azt mindenki döntse el maga.

[95] Gondoljunk csak a magyar őstörténetre, amikor Árpád vezér követe egy darabka földet, füvet és vizet kért Szvatopluk fejedelemtől. Ezek minősége volt a döntő a honfoglaló magyaroknak, hogy a Kárpát-medencében telepedjenek le.

[96] Gondoljunk csak az Enigma feltörésére, ami a második világháború kimenetelében igen komoly hatással bírt.

[97] Számos példát lehetne sorolni, de az elmúlt évtizedekből talán a legnagyobb hatással az Amerikai Egyesült Államokat ért 2001, szeptember 11-ei terrortámadást lehet említeni.

[98] A 20. század egyik legjelentősebb hírszerzője dr. Richard Sorge, Sztálin „mesterkémje" volt, aki 1941 áprilisában jelezte többek között azt is,

A 21. századra a nemzetbiztonsági szolgálatok számos kihívás előtt állnak. Ezek közül a fontosabbak:[99]

- 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.

A felsorolásból, mint látható, igen komplex kihívások fenyegetik a társadalmakat, így érthető, hogy az ezekkel szembeni fellépés új típusú módszerek alkalmazásával jár együtt, és a kormányzatok a lehető legszélesebben akarják a nemzetbiztonsági szolgálatok jogosítványait kiterjeszteni, hogy elháríthassák, minimalizálhassák a fentiekből származó veszélyeket. A probléma abból ered, hogy a kiszélesített jogkörök milyen mértékben korlátozzák az állampolgárok magánszféráját. Amennyiben a szolgálatoknak jogukban áll tömegesen megfigyelni az egyéneket, róluk információt gyűjteni bírói vagy miniszteri felhatalmazás nélkül, a szigorú normatív szabályokat megkerülve, az igen komoly probléma. Nem véletlenül szükséges őrizni az őrzőket is, hiszen olyan túlhatalmat birtokolhatnak, ami legszélsőségesebb esetben egy totális rendszer kiépítéséhez vezethet.

A nemzetbiztonsági szolgálatok tevékenységének titkossága miatt a hírszerzés módját a jogszabályok nem konkretizálják. Ennek az is az oka, hogy a titkos információgyűjtésnek számos fajtáját különböztetjük meg, a technikai és technológiai innováció hatására rendre új eszközök és módszerek jelennek meg. Ebből következik tehát, hogy a jogszabályokban általában azokat a titkosszolgálati eszközöket és módszereket nevesítik, amelyeknek alkalmazása az alkotmányos alapjogok közvetlen sérelméhez vezethetnek, és az állampolgároknak a büntetőjog eszközeivel védett magánszférájába avatkoznak be. Ilyen esetben a titkos információgyűjtés során nem hajtanak végre bűncselekményt (például magánlakásba történő behatoláskor lehallgatókészülék elhelyezésével, vagy a célszemély informatikai rendszerébe történő behatolással), ugyanis törvényben meghatározott felhatalmazás (bírói vagy miniszteri engedély) alapján végzik tevékenységüket.

hogy Németország a Szovjetunió elleni invázióra készül 150 hadosztállyal. Május 20-án június 20-át jelölte meg a támadás időpontjának. Mint az közismert, a Barbarossa-hadművelet június 22-én vette kezdetét. Sztálin a visszaemlékezések szerint a kapott információt komolytalannak minősítette, hiszen Hitlerről nem tudta elképzelni, hogy megszegné a korábban között Molotov–Ribbentrop-paktumot.

[99] KIS-BENEDEK József (2013): A nemzetbiztonsági szolgálatok együttműködése. Hadtudomány, XXIII:(1–2) pp. 100–114.

4.2. A NEMZETBIZTONSÁGI SZOLGÁLATOKRÓL RÖVIDEN

A nemzetbiztonsági szolgálatokat az országok saját politikai kultúrájuknak, a szövetségi vagy koalíciós rendszerben vállalt kötelezettségeinek, illetve a nemzeti sajátosságoknak megfelelően hozzák létre. Általában két nagy csoport alapján szokás tagolni: ez alapján megkülönböztetünk polgári és katonai nemzetbiztonsági szolgálatokat, illetve hírszerzésért és felderítésért felelős szolgálatokat.

Az, hogy a különböző szervezetek melyik miniszter irányítása alá tartoznak, milyen széles jogkörrel ruházzák fel őket, illetve milyen struktúra alapján szervezik meg őket, sokszor politikai döntések, egyes politikai aktorok érdekérvényesítő képességének függvénye.

Magyarországon jelenleg – az 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról[100] alapján – polgári oldalról az elhárításért az Alkotmányvédelmi Hivatal, a felderítésért az Információs Hivatal felel. Szintén polgári szolgálat a Nemzetbiztonsági Szakszolgálat, de ez utóbbi kiszolgáló tevékenységet végez a megrendelőknek. Katonai oldalról a Katonai Nemzetbiztonsági Szolgálat látja el az elhárítás és felderítés tevékenységét a Katonai Felderítő Hivatal és Katonai Biztonsági Hivatal 2012-es integrációja óta.

A külügyminiszter irányítja az Információs Hivatalt, a belügyminiszter az Alkotmányvédelmi Hivatalt és a Nemzetbiztonsági Szakszolgálatokat, a honvédelmi miniszter pedig a Katonai Nemzetbiztonsági Szolgálatot. A nemzetbiztonsági szolgálatok működését, speciális feladatkörükből adódóan, a Magyar Országgyűlés a Honvédelmi és rendészeti bizottságon, illetve a Nemzetbiztonsági bizottságon keresztül kiemelten ellenőrzi. A szolgálatok demokratikus és alkotmányos működésének további garanciája, hogy a Nemzetbiztonsági bizottság elnöke mindig az aktuális parlamenti ellenzék soraiból kerül ki.

Az Információs Hivatal aktív szerepet játszik a nemzetközi és a hazánkat fenyegető terrorizmus, kábítószer-kereskedelem, illetve valutaspekuláció elleni harcban, de fontos szerepet tölt be Magyarország diplomáciai, külgazdasági és tudományos kapcsolataiban is. Az Alkotmányvédelmi Hivatal fő feladata, hogy felderítse és elhárítsa a hazánk területi egységét, függetlenségét, demokratikus berendezkedését, politikai és gazdasági érdekeit sértő cselekményeket. A Nemzetbiztonsági Szakszolgálat a magyar állam belső rendjének védelme érdekében szigorú jogszabályi keretek között nyílt és titkos információgyűjtést végez az erre felhatalmazott szervek kérésére. A Katonai Nemzetbiztonsági Szolgálat a hírszerző, elhárító, védelmi és ellenőrzési feladatok elvégzésével, a nyílt és a titkos információgyűjtés eszközrendszerével működési területén elősegíti Magyarország nemzetbiztonsági érdekeinek érvényesítését, ezáltal közreműködik az ország függetlenségének és törvényes rendjének védelmében.

Gyakran a Terrorelhárítási Központot is a nemzetbiztonsági szolgálatok köré sorolják, ez a besorolás azonban téves, mert bár bizonyos pontokban vonatkozik rá az Nbtv., a Terrorelhárítási Központ rendészeti szervezetnek minősül.

A titkos információgyűjtés végzése során megkülönböztetjük a külső engedélyhez kötött és külső engedélyt nem megkövetelő eljárásokat. Külső engedélyhez nem kötött információgyűjtés körébe tartozik többek között a felvilágosításkérés, a nemzetbiztonsági jelleg leplezésével történő információgyűjtés; titkos kapcsolat létesíté-

[100] 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV (Letöltés ideje: 2017. december 16.)

se magánszeméllyel; személy, objektum, útszakasz megfigyelése; fedőintézmény létrehozása. Külső engedélyhez kötött adatgyűjtésnek minősül a lakás titkos átvizsgálása, technikai eszközök elhelyezése, levél- és egyéb postai küldemények felbontása, telefonlehallgatás.

A nemzetbiztonsági szolgálatok hatékony működését nagyban befolyásolhatja, milyen modellt választottak a nemzetbiztonsági rendszer kialakítására. Általánosságban három modellt különböztetünk meg:[101]

- Konkuráló modell esetén minden szolgálat a maga információi alapján értékel és jelent; verseng a döntéshozók figyelméért, elismeréséért, támogatásáért. Erőssége: azonos témában minden vélemény megjelenik, lehetőséget kap a meghallgatásra; a vélemények (értékelésének, jelentések) ütköznek, egymással, értékük és deficitjük kiderül. Hátránya: drága a működtetése, minden szervezet rendelkezik értékelő központtal, sok az átfedés, a duplikáció; a döntéshozók helyzete nehéz, az információdömping miatt sokféle értékelés alapján kell dönteniük a legnagyobb valószínűséggel igaz információk alapján.
- Szektorra épülő modell esetében az egyes szolgálatok az alapfunkciónak megfelelő ágazati miniszter irányításával dolgoznak. Erőssége: egyértelmű a munkamegosztás, az információáramlás útja világos, keskeny és rövid, szigorú belső konspirációt biztosít; az érintett miniszternek nagy hatalmat biztosít. Hátránya: releváns információk – részben vagy teljesen – megrekedhetnek, nem jutnak el esetleg illetékes másik miniszterhez, így a döntéshozatalra nem minden esetben tud hatással lenni az adott szolgálat vagy információ.
- Kooperatív modell esetében az egyes szolgálatok saját jelentéseiket kommunikálják a kormánynak, de csak egy helyen történik értékelés; ez az egységes értékelő szolgálat vagy szervezet az összes rendelkezésre álló forrásból származó információt értékeli, az illetékes miniszteréknek továbbítja. Erőssége: a lehető legjobb felkészültségű értékelők egységes álláspont szerint tevékenykednek, az információkat a kormányzat tényleges igényei szerint értékelik, nem hajlanak el a parciális szervezeti érdekek felé. Hátránya: a véleménykülönbségek elsimulnak, nem tükrözik a sokszínűséget, az ellentmondásokat; a szolgálatokat közvetlen politikafüggővé teheti a naprakészségre és a hírigények kielégítésére való törekvés, esetlegesen a valóságos információ helyett a megrendelést teljesítik.

A nemzetbiztonsági szolgálatok belföldi együttműködése mellett fontos a nemzetközi együttműködés tartalma és kerete. Hazánk európai uniós és Észak-atlanti Szövetségbeli tagsága, valamint a nemzetbiztonsági szolgálatok előtt álló kihívások globális jellegéből fakadóan a nemzetközi együttműködéseknek különösen fontos szerep jut. Nemzetközi együttműködés tekintetében megkülönböztetjük a multilateriális és bilateriális együttműködéseket. Sem a NATO, sem az EU nem rendelkezik saját hírszerző szolgálattal, így az információk a tagállamok közötti információmegosztásból állnak elő. Különböző típusú információk megosztása azonban nem kapcsolódik hivatalos partnerszolgálati együttműködéshez. Tipikusan ilyen a készülő terrortámadások felderítése egy másik ország területén, amit minden esetben jelezni szoktak az információt megszerző nemzetek nemzetbiztonsági szolgálatai. Az együttműködések egyik fő motivációja, hogy eltérő képességekkel rendelkeznek az egyes államok nemzetbiztonsági szolgálatai a különböző információgyűjtéseket illetően. Az Amerikai Egyesül Államokat gyakran érte

[101] HÉJJA István (2014): Nemzetbiztonsági szervezeti modellek. In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest. pp. 57–72.

az a vád, hogy az emberi erővel végzett hírszerzési képességét leépítette a technológiai hírszerzése miatt, mert ebben látták a jövőt – mint később látni fogjuk, nem alaptalanul. Afganisztánban azonban azzal szembesültek, nem képesek a technológiai hírszerzéssel információt gyűjteni olyan személyektől, akik barlangokban bujkálnak; a kapcsolattartást kizárólag futárok útján végzik, mellőzve minden elektronikai eszközt. Vannak a világnak olyan övezetei, ahol különböző országok nemzetbiztonsági szolgálatai a történeti fejlődés okán jobb pozíciókban vannak, például Franciaország Afrika különböző országaiban, vagy Nagy-Britannia a Közel-Keleten. A partnerszolgálati együttműködés így lehetővé teszi, hogy például azokat az erősségeket, amelyek, mondjuk, az adott célterületen hiányoznak emberi erővel végzett hírszerzésnél, azt a partner nemzetbiztonsági szolgálat végezze el, cserébe más jellegű tevékenységet végez a partnerország szolgálata.

4.3. A HÍRSZERZÉS ÉS ELHÁRÍTÁS FELADATRENDSZERE

Hírszerzés

Izsa Jenő fogalmi meghatározása alapján *„a hírszerzés 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."*[102] 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.[103]

Izsa Jenő definíciójában az állam szerepel, azonban mára nem csak államok folytatnak hírszerző tevékenységet. Például nyílt forrású információgyűjtést gyakorlatilag bárki legálisan végezhet, de lényegében a piackutatás, közvéleménykutatás mind-mind hírszerzésnek minősül. Ahogyan korábban már volt szó róla, a titkos információgyűjtést szigorú jogszabályi előírások mentén lehet végezni, hiszen az eljárások sok esetben egyébként bűncselekményeknek minősülnek, de ez nem minden esetben tántorítja el, mondjuk, a piaci szereplőket az ipari kémkedéstől.

A hírszerzésnek alapvetően két fő funkciója határozható meg: az ország értékeinek és érdekeinek a védelme, valamint az ország érdekeinek érvényre juttatásának támogatása. Előbbi például idegen államok befolyásolási kísérleteinek, esetleges katonai tevékenységeinek felderítésére vonatkozik, utóbbi a döntéshozó állami vezetők döntéseinek elősegítését végzi. A hírszerzés alapvetően külföldön végzett tevékenység, a külföldi eredetű nyílt és titkos információk megszerzésére vonatkozik. A hírszerzés alapjának az információ tekinthető, amelynek megszerzése, értékelése-elemzése a fő tevékenysége a szolgálatoknak.

[102] IZSA Jenő (2009): A hírszerzés céljáról és rendszeréről. Hadtudomány, 2009/1–2.

[103] BÉRES János (2014): A hírszerzés feladatrendszere. In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete. 363 p. Nemzeti Közszolgálati Egyetem, Budapest. pp. 117–128.

A hírszerzés tevékenységi rendszere alapvetően három fő területre tagozódik:

- adat- és információszerzés;
- elemzés-értékelés;
- hírszerző műveletek végrehajtása.

Elhárítás

Az elhárítás Ádám László megfogalmazása alapján *„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."*[104] A fogalomból következik, hogy az elhárítás – ellentétben a hírszerzéssel – egyszerre belső és külső irányú. A hírszerzés és elhárítás egymásból következő feladatok; míg az egyik oldal az információ védelmét igyekszik biztosítani, addig az ellenérdekelt fél ennek az információnak a megszerzésre törekszik. Úgy is mondhatnánk, a kém, akinek a tevékenységét meg kell akadályozni, az ellenség hírszerzője.

Az elhárító munka fő irányai ez alapján tehát:

- *„behatolás a külföldi hírszerző és fedőszervezetekbe, rezidentúrákba, ügynöki állományba terveik, szándékaik, módszereik, hírigényük stb. felderítése érdekében,*
- *általános és speciális megelőzés, hatékony védelem a hírszerzés által támadott területeken,*
- *aktív felderítő-szűrő-kutató munka, megfelelő jelzőrendszerek létrehozása és működtetése a titkosszolgálati felderítésre érzékeny területeken, a leginkább veszélyeztetett titokhordozók védelme,*
- *információgyűjtés a külföldi hírszerző szervek és ügynökeik közötti összeköttetés konkrét eszközeinek és módszereinek felderítése, az ellenséges ügynökök felkutatása,*
- *aktív feldolgozó munka az ellenérdekű tevékenység, az előkészületben lévő bűncselekmény elkövetésének megelőzése, korlátozása, megszakítása, elhárítása, vagy a már megvalósult bűncselekmények felderítése, leleplezése céljából."*[105]

Az elhárító tevékenység alapja a megelőzés akkor igazán sikeres, ha úgy védjük a személyeket, intézményeket, hogy az ellenérdekelt nemzetbiztonsági szolgálatok el sem jutnak hozzá. Ez alapján olyan intézkedéseket hoznak meg, amelyek az objektumok zavartalan működését biztosítják, megakadályozzák illetéktelenek behatolását, megelőzik a rendkívüli eseményeket, valamint felderítik az ellenérdekelt nemzetbiztonsági szolgálatok tevékenységét.

[104] ÁDÁM László (2014): Az elhárítás feladatrendszere. In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete. 363 p. Nemzeti Közszolgálati Egyetem, Budapest. pp. 129–145.

[105] Uo.

E tankönyv előszavában már volt szó arról, hogy Egyetemünk hallgatói kiemelt célpontként jelentkeznek az idegen nemzetbiztonsági szolgálatoknál, de ezt nem lehet elégszer hangsúlyozni. A hírszerző szolgálatok kiemelt célpontjai általánosságban a politikai élet, kormányzati és más állami szervek; a gazdasági és tudományos intézetek; stratégiai, nemzetgazdasági szempontból fontos intézmények; fontos és bizalmas munkakört vagy választott pozíciót betöltő döntéshozók.

4.4. A FELDERÍTÉS TERÜLETEI

Napjainkban kilenc fő adat- és információgyűjtő módszert különböztetünk meg, amelyek különböző alterületekre bonthatóak. Ez a felosztás nem kőbe vésett, vannak szerzők, akik új típusú módszereket is használnak. Erre szolgál példaként a SOCMINT, azaz Social Media Intelligence, vagyis a közösségi médián keresztül folytatott hírszerzés. Megítélésem szerint ez azonban nem tekinthető önálló ágnak az információgyűjtésben. Nem vitás, a közösségi média több módszer esetében jelentős, azonban úgy vélem, értelmetlen külön kiemelni.

Emberi erőforrásokkal végzett hírszerzés, HUMINT (Human Intelligence)

Az emberi erőforrásokkal végzett hírszerzés a legősibb adat- és információgyűjtő módszer. [106] Megkülönböztetjük a nyílt, legális pozícióban (nem összekeverendő a nyílt forrású információgyűjtéssel, az OSINT-tal!) végzett hírszerzést, valamint az ügynöki, fedett hírszerzést.

Előbbit az 1961-ben megkötött diplomáciai kapcsolatokról szóló Bécsi Egyezmény hagy jóvá,[107] amely lehetővé teszi a diplomaták számára, hogy törvényi kerteken beül információt gyűjtsenek magáról a fogadó országról, és azt továbbítsák a saját ország kormányának. Idesorolható továbbá a katonai missziók hír- és információszerző támogatást hírszerző elemekkel biztosított hírszerző tevékenysége. Mindkettő esetében közös pont, hogy a hírszerzést végző személyek neve, beosztása, hovatartozása nyíltan felvállalt.

Ezzel szemben a fedett vagy ügynöki hírszerzés során mind a hovatartozás, tevékenység fedésével, titokban, konspirált körülmények között folytatja a hírszerző szervezet és annak ügynöki hálózata a munkát. Az ügynöki hálózat nagyobb része a célországba települ, de a küldő országban is működtetnek támogató kategóriákat. Ez a fajta hírszerzés minden országban illegálisnak minősül. Nagyon speciális fajtáját jelentik a fedett hírszerzőknek az úgynevezett alvóügynökök, akiket a célországban valamilyen legenda által telepítenek, és akár évtizedekig is dolgoznak legális keretek között, akár családot is alapítanak, hogy ezzel is erősítsék a legendát, majd csak ezt követően aktiválják őket.

[106] KIS-BENEDEK József (2014): Az emberi erőkkel folytatott információszerzés: HUMINT – Human Intelligence. In: DOBÁK Imre (szerk.) A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Budapest. pp. 153–163.

[107] 1965. évi 22. törvényerejű rendelet a diplomáciai kapcsolatokról Bécsben, 1961. április 18-án aláírt nemzetközi szerződés kihirdetéséről. URL: https://net.jogtar.hu/jr/gen/getdoc2.cgi?docid=96500022.TVR (Letöltés ideje: 2017. december 20.)

Az emberi erőforrással végzett hírszerzést mindig a célterületen folytatják. Az információforrást személyek, a dokumentumokat, információkat pedig személyeken keresztül szerzik meg. A HUMINT előnye, hogy olyan információkhoz is hozzáférhetnek általa, amelyet más módszerrel lehetetlen megszerezni – gondoljunk csak Oszama Bin Ladenre. Az előnyei közé sorolható továbbá a visszacsatolás, az információ pontosításának, kiegészítésének, megerősítésének lehetősége.

Rádióelektronikai felderítés, SIGINT (Signals Intelligence)

A rádióelektronikai felderítés többnyire a honi területről, passzív eszközökkel a célország által üzemeltett rádióelektronikai rendszerei ellen irányuló információgyűjtés, amelynek során a távközlési és elektromágneses hullámok felfedését, lehallgatását végzik. A rádióelektronikai felderítést két alkategóriára osztjuk, a kommunikációs felderítésére (COMINT, Communications Intelligence), valamint elektronikai felderítésére (ELINT, Electronic Intelligence).[108]

A COMINT a célország egy másik országnak vagy az országon belül szánt kommunikációját, írásos, illetve hanganyagok elfogását jelenti (nagyon leegyszerűsítve az ember és ember közti kommunikációt). Az ELINT a radarok felderítését végzi, de idetartozik a célország haditechnikai eszközei által (műholdak, repülőgépek, hajók, tengeralattjárók stb.) kibocsátott elektromágneses jelekből kinyerhető információk megszerzése – ez utóbbi a gépi rádióforgalmazással kapcsolatos hírszerzés (FISINT, Foreign Instrumentation Signal Intelligence) (nagyon leegyszerűsítve, a gép és gép közti kommunikáció). Az ELINT nem csak haditechnikai eszközök esetében érvényes hírszerző eljárás, a tv-k, monitorok által kibocsátott sugárzás felderítése és az azokból levonható információk gyűjtése is idesorolható. Az elektronikai hírszerzés egy másik ága a felderítő műholdak és pilóta nélküli repülőgépek adatcsatornáinak lehallgatása, vagy a távirányított eszközök (műholdak, rakéták, pilóta nélküli repülőgépek stb.) által automatikusan közvetített, repülési jellemzőikre vonatkozó információk megszerzése, amit telemetriai hírszerzésnek (TELINT, Telemetry Intelligence) nevez a szakirodalom.

Nyílt forrású információgyűjtés, OSINT (Open Source Intelligence)

A nyílt forrású információgyűjtés napjainkra egyre nagyobb szerepet játszik a hírszerzésben.[109] *„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.*"[110] A nyílt forrású információgyűjtést sokan tévesen az internettel, a közösségi médiával azonosítják, ez azonban tévedés, hiszen a hagyo-

[108] i. m. DOBÁK (2014).

[109] KENEDLI Tamás (2014): A nyílt forrású információszerzés, In: DOBÁK Imre (szerk.) A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest. pp. 169–178., 2014.

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

mányos (nyomtatott és elektronikus) média, szürke irodalom, szakértők és megfigyelők tapasztalatai, kereskedelmi műholdas felvételek, könyvtárak anyagai, tanulmányok, nyilvános konferenciák előadásai, de prospektusok, reklámanyagok mind-mind részét képezhették a nyílt forrású információgyűjtésnek. Természetesen az internet óriási mennyiségi változást hozott a nyílt forrásból fellelhető információk terén, ez azonban az OSINT hátrányát is jelenti, hiszen nehéz kiválogatni – pláne ma, a post truth, fake news korában –, hogy melyik információ releváns, valódi, mi az, amit szándékosan dezinformatív szándékkal állítottak elő.

A nyílt forrású információgyűjtés viszonylag kis költségek mellett is végezhető, és nagy mennyiségű információt lehet megszerezni. Ahogy Ferenczy Gábor doktori értekezésében megfogalmazza, *„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"*.[111]

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 jövőbeni 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.[112]

Kiberhírszerzés, CYBINT/DNINT (Cyber Intelligence/Digital Network Intelligence)

A kiberhírszerzés[113] az infokommunikációs technológiák, a Dolgok Internete (vagyis IoT, Internet of Things) egyre nagyobb körben való elterjedése okán növekvő szerepet tölt be a hírszerzésben. Célja a célország védett informatikai hálózatokon tárolt információinak megszerzése. A kiberhírszerzésnek alapvetően három alterületét különböztetjük meg:

- a nyílt számítógépes hálózatokban védett információk megszerzése;
- a zárt számítógépes hálózatokban védett információk megszerzése;
- a számítógépes hálózatok által kisugárzott jelekből folytatott adatszerzés.

[111] FERENCZY Gábor (2007): Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása: doktori (PhD) értekezés. ZMNE, Budapest. p. 17.

[112] MESTYÁN Márton – YASSERIVEL, Taha – KERTÉSZ János (2013): Early Prediction of Movie Box Office Success Based on Wikipedia Activity Big Data. PLOS One, 2013. augusztus 21. URL: http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0071226&type=printable (Letöltés ideje: 2017. december 20.)

[113] DOBÁK Imre – KOVÁCS Zoltán (2014): Új technológiák hatása a hírszerzésre, In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest. pp. 206–220.

Képfelderítés, IMINT (Image Intelligence)

A képfelderítés a műholdak, légifelvételek által gyűjtött információk megszerzésére vonatkozik, de gyakran összevonják a térinformatikai felderítéssel (GEOIN, Geospatial Intelligence). A képi felderítés a célország objektumaira, eszközeire, esetleges csapatmozgásaira irányul. A képi felderítés által szerzett képek értékeléséhez különösen magas szakértelmet igénylő elemzők szükségesek.

Mérés- és jelmeghatározó hírszerzés, MASINT (Measurement and Signature Intelligence)

A mérés- és jelmeghatározó hírszerzés a megcélzott eszközöket, tárgyakat és tevékenységeket az általuk kibocsátott, kisugárzott jelek alapján szenzorok segítségével azonosítja. A mérés- és jelmeghatározó hírszerzés szenzorai lehetnek vegyianyag-elemzők, sugárzásmérők (NUCINT, Nuclear Intelligence), elektrooptikai felvevők, kisugárzott energiamérők, hangrögzítők (ACOUSTINT, Acoustic Intelligence), rezgésmérők, rádiófrekvencia-mérők és anyagelemzők. Adott esetben a földrengéssel kapcsolatos adatok is fontos hírszerzési információkat jelentenek, ahogyan például az észak-koreai nukleáris program esetében becsülték, hogy hol tartanak az észak-koreai mérnökök a nukleáris fegyverkezési kísérletekben.

Egyedülálló technikai azonosító képessége alapján számos szakértő szerint a MASINT lesz a jövő legfontosabb technikai adatszerző ága.

Technikai hírszerzés, TECHINT (Technical Intelligence)

A technikai hírszerzés nem összekeverendő a rádióelektronikai felderítéssel, a képi felderítéssel vagy a mérés- és jelmeghatározó hírszerzéssel. Ez esetben a technikai jelző nem a technológia felhasználásával történő információgyűjtésre vonatkozik, hanem egy adott technológia megszerzésére. A cél, hogy egy adott technológiát kifejlesztő államtól valamilyen úton megszerzett technikai eszközt visszafejtsenek, és képesek legyenek ők is előállítani, megtörve így a technológiai fölényt. Ennek kapcsán elég az orosz atombomba előállítására gondolni.

A technikai hírszerzés egyik fajtája az úgynevezett reverse engineering, amikor egy adott eszköz működési elvét tervrajzok, kutatás és fejlesztési kísérletek nélkül, az eszköz tanulmányozásával reprodukálják.

A technikai hírszerzésben Magyarország a bipoláris világrend idején igen jelentős országnak számított.[114] A Coordinating Committee for Multilateral Export Controls, avagy közismert nevén a COCOM-lista egy csúcstechnológiás termékeket tartalmazó multilaterális kereskedelmi embargó volt, amely a korszak gazdasági hadviselésének volt egy rendkívül fontos eszköze. A társult országok vállalták, hogy a Kölcsönös Gazdasági Segítség Tanácsa (KGST) országaiba, valamint Kínába nem exportálnak a COCOM-listán szereplő technikai eszközökből, hogy hátrányba

[114] Nagy szerepe volt ebben a például a Híradástechnikai Ipari Kutató Intézetnek, ami 1975-ben az Intel 8080-as jelű mikroprocesszorát reprodukálta, vagy az 1986-ban gyanús körülmények között leégett Mikroelektronikai Vállalatnak.

hozzák a keleti blokkot a fegyverkezési versenyben.[115] A COCOM-lista kijátszására nagy hangsúlyt fektettek, élen járt ebben a KGB Nyolcadik Főigazgatóságán belül működő, úgynevezett X-osztály, valamint a keletnémet Stasi WT- (Wissenschaft und Technik, vagyis Tudomány és Technika) részlege. A magyar Állambiztonsági Szolgálatot esetében a III/I-es Csoportfőnökség 5-ös osztálya foglalkozott a tudományos és műszaki hírszerzéssel.

Pénzügyi hírszerzés, FININT (Financial Intelligence)

A pénzügyi tranzakciók (banki átutalások, be- és kifizetések, valuták átváltása stb.) felderítésére vonatkozó információgyűjtő eljárás. Fontos szerepe van a terrorizmus és szervezett bűnözés elleni felderítő tevékenységekben.

Orvosi hírszerzés, MEDINT (Medical Intelligence)

Az orvosi hírszerzés a célország elsősorban politikai, katonai vezetőinek egészségügyi adatainak felderítésére vonatkozik. Nem nehéz belátni, hogy milyen fontos szerepe van ezeknek, amikor az ellenséges nemzet döntéshozóinak döntését kell prognosztizálni, hiszen befolyásolhatja az egészségügyi állapota a döntés meghozatalában. Egy olyan szituációban, amilyen például a kubai rakétaválság volt, nem mellékes az az információ, hogy a döntéshozók hogyan képesek a stresszt kezelni, bírnak-e valamilyen szenvedélybetegséggel (alkoholizmus, drogfüggőség), amik befolyásolják a meghozandó döntést.

Fontos azonban leszögezni, nem célszerű az egyes információgyűjtő eljárások túlzott preferálása, a sikeres nemzetbiztosági feladatok ellátását az összadatforrású felderítés alkalmazásával lehet végezni.

4.5. EDWARD SNOWDEN

Edward Snowden megítélése rendkívül összetett. E könyv szerzője is ellentmondásosan viszonyul személyéhez, hiszen egyrészt az általa megtörtént szivárogtatás jelentős nemzetbiztonsági kockázatot jelentett; az amerikai Nemzetbiztonsági Ügynökség (NSA) és partnerszervezetei képességeinek feltárásával a világunk tagadhatatlanul kevésbé maradt biztonságos, mivel a komolyabb terrorista szervezetek, szervezett bűnözői körök, ellenérdekelt nemzetbiztonsági szolgálatok megismerték azokat a megfigyeléssel kapcsolatos eljárásokat, amelyeket az NSA tökélyre fejlesztett, így képesekké váltak védekezni ellene. Az érem másik oldala, hogy olyan tömeges megfigyelésről rántotta le a leplet, amely mindenkit érint, aki internetezik. Snowdennek köszönhetően értesültünk arról, hogy gyakorlatilag megszűnt a magánszféránk.

[115] i.m. DOBÁK – KOVÁCS (2014).

A nagy elől, az Echelon

Nem sokkal az információk nyilvánosságra hozatalát követően írtam egy tanulmányt „Kémkednek a kémek" címmel, amelyben feldolgoztam az eset tanulságait.[116] A cím Krasznay Csaba egy parafrázisára utalt, amellyel jellemezte az esetet követő általános meglepődést, amikor a sajtó munkatársai, az átlagemberek konstatálták, hogy „jéé, a hírszerzők végzik a munkájukat", csak éppen nem gondoltak bele ennek a gyakorlati részébe. Azért is volt meglepő számomra, hogy az esetet ily módon interpretálta a média, ugyanis egészen pontosan 25 évvel korábban, 1988. augusztusában publikálta Duncan Campbell a Somebody's Listening[117] (Valaki figyel) címet viselő írását egy olya témában, amit már évek óta pletykáltak: öt angolszász ország hírszerző szolgálata a világ telekommunikációs forgalmának majdnem teljes egészét lehallgatja, elemzi.

Az öt társult állam az Amerikai Egyesült Államok és a Brit Nemzetközösség országainak hírszerző szolgálatai, vagyis az USA Nemzetbiztonsági Ügynöksége, 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.[118]

Az együttműködés csíráit az 1943. május 13-án aláírt BRUSA-egyezményben[119] kell keresnünk, amely a két angolszász nagyhatalom, az USA és Nagy-Britannia hírszerző szervezeteinek az ellenséges országok kommunikációjának lehallgatására[120] vonatkozó megállapodása volt. A második világháború befejeztével azonban nem zárult le az együttműködés, a bipoláris világrend létrejöttét követően a BRUSA egyezmény az UKUSA-egyezményként élt tovább, a kor követelményeinek és kihívásainak megfeleltetve: az együttműködés fokozásával, amely nem csupán a szakemberek, logisztikai képességek, infrastruktúra fejlesztését jelentette, hanem a Brit Nemzetközösség többi országának csatlakozását is. A hidegháború alatt több állam is jelezte szándékát az együttműködésre (NSZK, Dél-Korea, Norvégia, Japán), de nem bővítették a kooperációt. Napjainkban a Snowden-botrány egyik legfontosabb tanulsága megítélésem szerint ebben keresendő, de erről bővebben a későbbiekben szólok.

Mire volt képes az 1980-as években az Echelon? Elméletileg a bolygón bármilyen műszaki eszközzel vagy módszerrel képes volt kommunikációt folytatni, illetve továbbítani rögzítésére, kódolt közlést megfejtésére, elemzé-

---

116 BÁNYÁSZ Péter (2014): Spies Act As A Spy: The Edward Snowden Case. In: SOPÓCI, Milan – PETRUFOVÁ, Mária – ŠKOLNÍK, Miroslav – FRIANOVÁ, Viera – NEKORANEC, Jaroslav – BELAN JIRÁSKOVÁ, Lubomír – KUSTROVÁ, Milota – MORONG, Stanislav (szerk.): Manažment - teória, výučba a prax 2014: zborník príspevkov z medzinárodnej vedecko-odbornej konferencie. Akadémia ozbrojených síl generála Milana Rastislava Štefánika, Liptovsky Mikulas. pp. 194–201.

117 CAMPBELL, Duncan (1988): Somebody's Listening. In: New Statesman, 1988. augusztus 12. URL: http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf (Letöltés ideje: 2017. december 20).

118 CAMPBELL, Duncan – HONIGSBAUM, Mark (1999): Britain and US spy on world. In: The Guardian, 1999. május 23. URL: http://www.duncan-campbell.org/menu/journalism/guardian/britain.pdf (Letöltés ideje: 2017. december 20.).

119 NSA: UKUSA Agreement Release 1940–1956, In: National Security Agency: Public Information, Declassification and Transparency. URL: http://www.nsa.gov/public_info/declass/ukusa.shtml (Letöltés ideje: 2017. december 20.).

120 Az együttműködés eredményei közé sorolhatjuk többek között a VENONA-projektet. Bővebben lásd: NSA: VENONA. In: National Security Agency: Public Information, Declassification and Transparency. URL: http://www.nsa.gov/public_info/declass/venona/ (Letöltés ideje: 2017. december 20.).

sére, értékelésére. Mivel elképesztő mennyiségű adatról van szó, ezért az elemzéshez valamilyen előre megadott jellemző szükséges, legyen szó akcentusról, időpontról, kulcsszóról (bomba, terrorizmus, Allah stb.), karakterkészletről, nyelvről stb.

A szinte korlátlan és automatikus megfigyelés az emberjogi és adatvédelmi aggályokon kívül egy nagyon fontos szempontra irányította rá a figyelmet. A nemzetbiztonság érdekében végzett megfigyeléseket a politikai döntéshozók számos esetben használták fel gazdasági hírszerzésre. Az Európai Parlament vizsgálata[121] alapján 1993 és 2000 között 25-30 ezermilliárd dollárnyi üzletet kötöttek (többek között műholdrendszerek, repülőtenderek, telekommunikációs és vegyipari fejlesztések, energiatermelés, szemétfeldolgozás stb.) az Echelon által megszerzett információkat felhasználva, versenyelőnyt biztosítva az eredeti partnerrel szemben. R. James Woolsey, a CIA egykori igazgatójának megfogalmazása alapján, az Egyesült Államok az ezúton megszerzett információkkal csupán esélyegyenlőséget teremtett, hiszen a francia kormány és francia hadiipari vállalatok megvesztegetéssel szorították ki konkurenseiket.[122]

A kiszivárogtatások kapcsán egy másik nagy elődöt is említeni szükséges, a WikiLeakset, ezt azonban a hacktivizmussal kapcsolatos részben bőven kifejtettem már.

Snowden

Edward Snowden 2013 nyarán történő színre lépése, mint láttuk, egyáltalán nem nevezhető előzmények nélkülinek. De ki is ő?

Edward Joseph Snowden 1983. június 21-én született az észak-karolinai Elizabeth Cityben. Családi hátterét illetően anyja a baltimore-i szövetségi bíróság számítógépes és adminisztrációs hálózatának vezetője, apja a Parti Őrség egykori tisztje. A középiskolát nem fejezte be, a középiskolai végzettségnek megfelelő General Educational Development (GED) oklevelét esti képzésen szerezte meg, közben számítógépes tanfolyamokat folytatott. 2004-ben jelentkezett önkéntesként a hadseregbe, ahol elkezdte a különleges erők kiképzéséi programját, de a képzést nem fejezte be, ugyanis egy baleset miatt leszerelték. Ezt követően biztonsági őrként dolgozott az NSA-nél, majd 2007-től a CIA alkalmazásába került informatikai területen. 2009-től tanácsadóként dolgozott a Dell és az amerikai hírszerzés árnyékbirodalmaként számon tartott Booz Allen[123] cégeknél. Elmondása szerint már 2008-ban a nyilvánosság elé akart lépni az NSA kémprogramjával, azonban hitt Barack Obama választási ígéreteiben a változás politikáját illetően, de később csalódott, hogy Obama folytatta elődje politikáját.[124]

---

[121] European Parliament: Temporary Committee On The Echelon Interception System Directorate-General For Committees And Delegationsbrussels Meeting, 2001. január 22–23. URL: http://www.duncancampbell.org/menu/surveillance/echelon/Contract_analysis.pdf (Letöltés ideje: 2017. december 20.).

[122] WOOLSEY, James R. (2000): Why We Spy on Our Allies. In: The Wall Street Journal, 2000. március 17. URL: http://online.wsj.com/article/SB953268243116572 69.html (Letöltés ideje: 2017. december 21.

[123] HANULA Zsolt – IVÁN András (2013): Az amerikai hírszerzés árnyékbirodalma, In: Index, 2013. 2013. június 25. URL: http://index.hu/kulfold/2013/06/25/az_amerikai_hirszerzes_arnyekbirodalma/ (Letöltés ideje: 2017. december 21.

[124] MACASKILL, Ewen (2013): Edward Snowden, NSA files source: ‚If they want to get you, in time they will'. In: The Guardian, 2013. június 10. URL: http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why (Letöltés ideje: 2017. december 21.)

Ez idő alatt tovább gyűjtötte a megfigyelésről szóló adatokat. A napvilágra került anyagok olyan dokumentumokat is tartalmaznak, amelyhez Snowdennek nem volt hozzáférése, de informatikusként meggyőzte kollégáit, hogy adják meg a belépéshez szükséges adataikat, ugyanis rendszergazdaként szüksége van rá. Az NSA hawaii regionális központjában dolgozó mintegy 20-25 kollégájától sikerült ily módon illetéktelenül adatokat lementenie.[125]

2013 decemberében Alan Rusbridger, a The Guardian főszerkesztője a Parlament belügyi bizottságának meghallgatásán azt vallotta, hogy a Snowden által átadott 58 ezer feljegyzés eddig 1%-át jelentették meg. A médiában az egyik legtöbbet feldolgozott program a PRISM nevet viselte, ami központi szerepet játszott az Oliver Stone által 2016-ban megjelent Snowden-filmben is.

A PRISM

A PRISM a SIGAD[126] US-984XN kódnevű titkos tömeges megfigyelésre képes elektronikus adatbányász rendszer, ami az 1978-as Foreign Intelligence Surveillance Act (továbbiakban FISA) 2008-as módosítása, és a 2001-es, de 2007-ben módosított Patriot Act rendelkezésein alapul. A megfigyelések jogszerűségének ellenőrzését, illetve a titkos adatgyűjtésre az engedélyt a FISC biztosítja. A PRISM nem egyenlő a kormányzati megfigyelő programmal, csupán a közel két tucat megfigyelő rendszer egyike. Ha figyelembe vesszük, hogy a nagy közösségi oldalak abban az időben csupán pár éve léteztek, alkalmazhatóság tekintetében rendkívül jó helyzetfelismerésről tanúskodik a szolgálatok részéről.[127]

A The Guardian által közzétett slide-ok alapján[128] az NSA 2007 óta fér hozzá a PRISM által a 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. A nagy techcégek először tagadták, hogy az NSA hozzáférne az adatbázisaikhoz, azonban a 2013 augusztusában nyilvánosságra kerültek alapján vált ismertté, hogy az NSA a Google-nek, a Microsoftnak, a Yahoonak és a Facebooknak is fizetett a lehallgatásokhoz szükséges infrastruktúra-fedezéséért cserébe.[129]

A FISA alapján bírósági felhatalmazás nyomán kötelezhetőek a cégek adatok kiszolgáltatására, az Edward Snowden által közzétett információk azonban azt bizonyítják, hogy az NSA számos esetben az amerikai törvényeket megszegve végezte az adatgyűjtést. A The Guardian által közölt XKeyscore-programhoz készített oktatóanyagból kiderült,[130] hogy bármilyen bírósági felhatalmazás nélkül, gyakorlatilag egy személyes adat felhasználásával (legyen szó telefonszámról, IP-címről) bármelyik állampolgárt alapos megfigyelés alá vonhatják. Az ügynökök a

[125] HVG: Snowden kollégái jelszavával ügyeskedve szivárogtatott. In: HVG, 2013. november 8. URL: http://hvg.hu/vilag/20131108_Snowden_kollegai_jelszavaval_ugyeskedve_s (Letöltés ideje: 2017. december 21.).

[126] SIGINT Activity Designator, vagyis rádióelektronikai felderítő tevékenységet meghatározó alfanumerikus azonosító.

[127] Egyes összeesküvés-elméletek szerint a nagy közösségi oldalak létrejötte mögött valójában a különböző titkosszolgálatok állnak.

[128] The Guardian: NSA Prism program slides. In: The Guardian, 2013. november 1. URL: http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (Letöltés ideje: 2017. december 21.)

[129] MACASKILL, Ewen (2013): NSA paid millions to cover Prism compliance costs for tech companies. In: The Guardian, 2013. augusztus 23. URL: http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid (Letöltés ideje: 2017. december 21.)

[130] GREENWALD, Glenn (2013): XKeyscore: NSA tool collects ‚nearly everything a user does on the internet'. In: The Guardian, 2013. július 31. URL: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (Letöltés ideje: 2017. december 21.)

program segítségével hozzáférhettek az összes e-mailhez, chatbeszélgetéshez, keresési előzményhez. Bár az amerikai jogszabályok tiltják amerikai állampolgárok engedély nélküli megfigyelését, az NSA egy jogi kiskapu segítségével megtalálta a módját az adatgyűjtésnek: amennyiben a megfigyelni szándékozott állampolgár kapcsolatba hozható egy megfigyelt külföldivel, úgy elvégezhető az adatgyűjtés. Belső vizsgálatok alapján azonban ismertté vált, hogy 2008 óta évente több ezer alkalommal sértették meg az adatvédelmi törvényeket, túllépve a megszabott hatáskörükön, illetve az ezúton megszerzett információkat megosztották a DEA-vel.[131] A megfigyelésből szerzett adatokat azonban nem csupán belföldi partnerekkel, hanem külföldiekkel is megosztotta az NSA. Egy 2009. márciusi megállapodás jegyzőkönyve szerint az NSA a még ki nem elemzett, nyers adatokat átadta az izraeli partnerszervének, az Israeli SIGINT National Unitnak (ISNU) is.[132]

Nem ez volt az egyetlen együttműködés az NSA és partnerszervezetek között. Az NSA például 100 millió fontot fizetett a GCHQ-nak, hogy segítse az internetforgalom megfigyelését.[133]

és a többiek…

Az Edward Snowden által kiszivárogtatott információk nem csupán az e-mail és közösségi média teljes megfigyelésének lehetőségéről szóltak, hanem többek között:

- titkosított beszélgetésekhez (Skype, Outlook, Hotmail stb.) való hozzáférésről;[134]
- pornónézési szokások elemzéséről;[135]
- online stratégiai játékokba történő beépülésről;[136]
- állami vezetők hivatali és magántelefonjainak lehallgatásáról;[137]
- a mobileszközök világszerte történő követéséről;[138]

---

131 GELLMAN, Barton (2013): NSA broke privacy rules thousands of times per year, audit finds. In: The Washington Post, 2013. augusztus 16. URL: 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 (Letöltés ideje: 2017. december 21.)

132 GREENWALD, Glenn – POITRAS, Laura – MACASKILL, Ewen (2013): NSA shares raw intelligence including Americans' data with Israel. In: The Guardian, 2013. szeptember 11. URL: http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents (Letöltés ideje: 2017. december 21.)

133 HOPKINS, Nick – BORGER, Julian (2013): Exclusive: NSA pays £100m in secret funding for GCHQ. In: The Guardian, 2013. augusztus 1. URL: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden (Letöltés ideje: 2017. december 21.)

134 GREENWALD, Glenn et al. (2013): Microsoft handed the NSA access to encrypted messages. In: The Guardian, 2013. július 12. URL: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (Letöltés ideje: 2017. december 21.)

135 HP: Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit ‚Radicalizers'. In: Huffington Post, 2013. november 26. URL: http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html?1385526024 (Letöltés ideje: 2017. december 21.)

136 BALL, James (2013): Xbox Live among game services targeted by US and UK spy agencies. In: The Guardian, 2013. december 9. URL: http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life?CMP=twt_gu (Letöltés ideje: 2017. december 21.)

137 SPIEGEL STAFF: Embassy Espionage: The NSA's Secret Spy Hub in Berlin. In: Spiegel Online, 2013. október 27. URL: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (Letöltés ideje: 2017. december 21.)

138 GELLMAN, Barton – SOLTANI, Ashkan (2013): NSA tracking cellphone locations worldwide, Snowden documents show. In: The Washington Post, 2013. december 4. URL: http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html?hpid=z1 (Letöltés ideje: 2017. december 21.)

- mobileszközök kamerairányításának távolról történő átvételéről;[139]
- postán rendelt informatikai eszközök szállítás közbeni „bepoloskázásáról", illetve az informatikai eszközök megfigyelését lehetővé tevő módszerekről;[140]
- politikai csúcstalálkozók (például G20) lehallgatásáról;[141]
- nemzetközi politikai szervezetek székházainak (például ENSZ- és EU-s intézmények) lehallgatásáról;[142] [143]
- a fentiekben említett titkosítások feltörésére vonatkozó műveletekről is.

A hálózati adatok figyelése bevett szokásnak számít, a titkosszolgálatok jelentős része él vele, azonban az Egyesül Államok helyzetelőnyt élvez e téren, ugyanis a világ internetforgalmának releváns része az amerikai hálózatokon is keresztülmegy, illetve az egyre elterjedtebb felhőszolgáltatásokban tárolt adatok többségét az amerikai szerverparkok rejtik. Vélhetően az optikai üvegszálak „bontása" magyarázza a projekt nevét is – „PRISM". Nem szabad elfelejteni, a csomópontokon áthaladó adatok teljes mennyiségét megszerzik, így elképesztő mennyiségű információ áll az NSA rendelkezésére, amit elemezni szükséges. Ennek technológiai hátteréről jelenleg nem rendelkezünk ismeretekkel. Bár az adatok egy része titkosított csatornán halad keresztül, az NSA és a GCHQ feltörte az internetes szolgáltatások titkosítására használt SSL-technológiát, így képessé vált a korábban biztonságosnak hitt e-mailekhez, de akár az egészségügyi adatokhoz, banki információkhoz hozzáférni. Ezt a titkosítást használják egyébként a nagy techcégek, mint a Google vagy a Facebook.

Az NSA évek óta szándékosan gyengítette a kriptológiai szabványokat. Fedőcégeken keresztül olyan titkosítási protokollokat igyekeztek elterjeszteni, melyekben beépített hátsó kapuk voltak, megkönnyítendő a feltörésüket.[144] Ez természetesen meglehetősen kontraproduktív, hiszen az elhelyezett kritikus sebezhetőségeket így más, esetlegesen ellenséges csoportok is felfedezhették. Ha nem sikerült feltörni egy titkosítást, az NSA megvesztegetést alkalmazott. Az egyik legnagyobb hírű informatikai biztonsággal foglalkozó cég RSA BSafe nevű termékébe 10 millió dollárért épített bele olyan algoritmust, amely hozzáférést biztosított az NSA számára.[145] Az eset érdekessége, hogy az RSA a 90-es években határozottan lépett fel, amikor a nemzetbiztonság egy kémkedést segítő chip beépítésére akarta kötelezni a kommunikációs eszközök gyártóit, ezáltal egyfajta ikon szerepét töltötte be.

---

139 LICA: Távolról is bekapcsolható az iPhone kamerája. In: Index, 2014. január 1. URL: http://index.hu/tech/2014/01/01/tavolrol_is_bekapcsolhato_az_iphone_kameraja/ (Letöltés ideje: 2017. december 21.)

140 SOTTEK, T.C. (2013): NSA reportedly intercepting laptops purchased online to install spy malware. In: The Verge, 2013. december 29. URL: http://www.theverge.com/2013/12/29/5253226/nsa-cia-fbi-laptop-usb-plant-spy (Letöltés ideje: 2017. december 21.)

141 GREENWALD, Glenn et al. (2013): New Snowden docs show U.S. spied during G20 in Toronto. In: CBC, 2013. november 27. URL: http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448 (Letöltés ideje: 2017. december 21.)

142 HVG: Obama leállíttatta az ENSZ-székház lehallgatását. In: HVG, 2013. október 30. URL: http://hvg.hu/vilag/20131030_ensz_lehallgatas_obama_leallit (Letöltés ideje: 2017. december 21.)

143 POITRAS, Laura et al. (2013): Attacks from America: NSA Spied on European Union Offices. In: Spiegel Online, 2013. június 29. URL: http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html (Letöltés ideje: 2017. december 21.)

144 Ball, James – Borger, Julian – Greenwald, Glenn (2013): Revealed: how US and UK spy agencies defeat internet privacy and security, In. The Guardian, 2013. szeptember 6. URL: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Letöltés ideje: 2017. december 21.)

145 MENN, Joseph (2013): Exclusive: Secret contract tied NSA and security industry pioneer. In: Reuters, 2013. december 20. URL: http://www.reuters.com/article/2013/12/21/us-usa-security-rsa-idUSBRE9BJ1C220131221 (Letöltés ideje: 2017. december 21.)

Az NSA a napvilágra került dokumentumok tanulsága szerint évek óta rendszeresen megfigyelte a nemzetközi pénzforgalmi adatokat, valamint banki és hitelkártya-tranzakciókat is. Egy prezentáció szerint a megfigyelés célpontjai európai, közel-keleti és afrikai Visa-ügyfelek, a megfigyelés célja pedig a vezető hitelkártya-társaságok „tranzakciós adatainak begyűjtése, tárolása és elemzése" voltak.[146] A Spiegel beszámolója szerint az NSA hozzáfért a több ezer bank nemzetközi fizetési forgalmát bonyolító brüsszeli SWIFT- (Society for Worldwide Interbank Financial Telecommunication) társaság adataihoz. A banki adatok után történő kémkedésre válaszul az EU Bizottsága jogsértésre hivatkozva kilátásba helyezte az Egyesül Államokkal szemben a SWIFT-egyezmény felfüggesztését.

Talán az egész megfigyelési ügy legnagyobb visszhangot kiváltó eseményének a szövetséges államok vezetőinek lehallgatása, megfigyelése tekinthető. A 2013 októberében megrendezésre kerülő EU-csúcs központi témájává vált az addigra botránnyá dagadt lehallgatási ügy, amely az európai vezetők mobiltelefonjainak megfigyeléséről szólt. Angela Merkel és François Hollande nyilatkozatokban ítélték el az Egyesül Államok ez irányú hírszerző tevékenységet, amelyek elsősorban a politikai kommunikáció szintjén értelmezendőek („Barátok között elfogadhatatlan a kémkedés"). A nyilatkozatok mögött azonban reálpolitikai megfontolások álltak, hiszen az EU egy új adatvédelmi szabályozás elfogadására készült, amelynek az egyik legjelentősebb újítása tiltaná, hogy a vállalatok az EU-állampolgárok adatait idegen titkosszolgálatoknak szolgáltassák ki,[147] illetve realizálta az amerikai infrastruktúrától független, önálló európai stratégiai digitális eszközök (például európai adatfelhő) létrehozásának szükségességét.

Arról sem szabad megfeledkezni, hogy Németország évtizedek óta szeretett volna részese lenni az UKUSA-egyezménynek. Megítélésem szerint az ország és (közvetetten) az egész EU lehallgatásokkal kapcsolatos politikai nyilatkozatai beilleszthetőek voltak a csatlakozás elnyeréséhez (lásd Snowden Európai Parlament által tervezett meghallgatását [148]). Amerikai részről szinte azonnal megindult egy diplomáciai offenzíva, amelynek célja az európai szövetségesek kiengesztelése volt.

Az NSA megfigyelési gyakorlata élénk vitát váltott ki világszerte. Az eljárás védői között visszatérő elemként jelentkezett, hogy a kiszivárogtatás nemzetbiztonsági érdeket sért, Nagy-Britanniában felmerült, hogy a The Guardian munkatársait terrorizmussal összefüggő bűncselekményekkel vádolhatják meg.[149] Mindeközben egy amerikai hivatalnok elszólásából kiderült, hogy David Mirandának, a Snowden-dokumentumokat kiszivárogtató Glenn Greenwald élettársának kilenc órán át tartó kihallgatása mögött azon újságírók fenyegetése állt, akik további

146 SPIEGEL ONLINE: Überwachung: NSA späht internationalen Zahlungsverkehr aus. In: Spiegel Online, 2013. szeptember 9. URL: http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaeht-internationalen-zahlungsverkehr-aus-a-922283.html (Letöltés ideje: 2017. december 21.)

147 EURológus: Dúl a háború az európai adatokért. In: Index, 2013. október 23. URL: http://index.hu/kulfold/eurologus/2013/10/23/folyik_a_haboru_az_adatokert/ (Letöltés ideje: 2017. december 21.)

148 EURológus: Megszavazta Snowden meghallgatását az EP. In: Index, 2013. december 13. URL: http://index.hu/kulfold/eurologus/2013/12/13/snowden_ep_meghallgatas/ (Letöltés ideje: 2017. december 21.)

149 David Cameron értékelte Snowdent és a vele együttműködő újságírókat, hogy „azok kezére játszanak, akik a családokat akarják felrobbantani". Bővebben lásd: LENOIR, Francois: UK's Cameron says Snowden and media spy leaks ‚helping enemies'. In: Reuters, 2013. október 25. URL: http://www.reuters.com/article/2013/10/25/us-usa-spying-cameron-idUSBRE99O0K520131025 (Letöltés ideje: 2017. december 21.)

dokumentumokat kívánnának nyilvánosságra hozni.[150] Mirandától a kihallgatás során több ezer dokumentumot foglaltak le. A GCHQ kötelezte (és személyesen felügyelte) a The Guardiant a székházában tárolt adathordozók megsemmisítésére, amelyeken a Snowdentől kapott dokumentumok szerepeltek.[151]

Időközben eltérő bírói ítéletek születtek az NSA adatgyűjtésének törvényességét illetően. Egy köztes szövetségi bírósági döntés alkotmányellenesnek nyilvánította az amerikai nemzetbiztonsági szolgálat mobiltelefonos adatgyűjtését, melynek esetében fennállt, hogy akár perek sorozatát is magával hozhatja.[152] Ezzel szemben döntött az alkotmány 4. kiegészítésére hivatkozva egy manhattani bíró, aki törvényesnek értékelte az NSA gyakorlatát.[153]

Barack Obama 2013 októberében bejelentette, hogy kezdeményezi az NSA külföldi működésének ellenőrzését, amelynek következtében a felkért tanácsadó testület egy 46 pontból álló, 300 oldalas jelentésében tette közzé javaslatait.[154] Többek között:

- az NSA képességeinek korlátozását, mert nagy tömegben rögzíteni tudja az amerikaiak telefonhívásait;
- az NSA ne tárolhassa saját létesítményeiben a megszerzett adatokat;
- az NSA-nak bírósági engedélyt kellene beszereznie ahhoz, hogy a megszerzett adatok között kutatást végezzen;
- a baráti országok vezetőivel szemben folytatott hírszerzés ellenőrzését, szabályainak kidolgozását;
- néhány kémprogram működésének megszüntetését.

Megítélésem szerint a megfigyelések kontrolljának tekintetében a normatív szabályozásnál nagyobb jelentőséggel bír a jóváhagyott költségvetés mértéke. Az amerikai nemzetbiztonsági szolgálatok 52,6 milliárd dollárból gazdálkodhatnak,[155] amelyből finanszírozhatják többek között például a titkosítások gyengítését vagy a megfigyelést szolgáló infrastruktúra biztosítását.[156] Bár 2001. szeptember 11-e óta az amerikai közvélemény a biztonság érdekében számos jogról lemondott, a kiszivárogtatás hatására a személyes adatok védelme egyre központibb kérdésnek

[150] MASNICK, Mike (2013): US Official Admits That UK Detention Of Glenn Greenwald's Partner Was ‚To Send A Message'. In: TechDirt, 2013. augusztus 20. URL: http://www.techdirt.com/articles/20130820/03160924251/us-official-admits-that-uk-detention-glenn-greenwalds-partner-was-to-send-message.shtml (Letöltés ideje: 2017. december 21.)

[151] BORGER, Julian (2013): NSA files: why the Guardian in London destroyed hard drives of leaked files. In: The Guardian, 2013. augusztus 20. URL: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london (Letöltés ideje: 2017. december 21.)

[152] BUMP, Philip (2013): Federal Judge: NSA's ‚Almost-Orwellian' Data Collection Likely Violates Constitution. In: The Wire, 2013. december 16. URL: http://www.thewire.com/politics/2013/12/federal-judge-nsas-almost-orwellian-phone-data-collection-likely-violates-constitution/356207/ (Letöltés ideje: 2017. december 21.)

[153] STEMPEL, Jonathan (2013): U.S. judge says NSA phone surveillance is lawful. In: Reuters, 2013. december 27. URL: http://news.yahoo.com/u-judge-says-nsa-phone-data-program-lawful-163733246.html (Letöltés ideje: 2017. december 21.)

[154] SCIUTTO, Jim – PEREZ, Evan (2013): Review: NSA snooping program should stay in place. In: CNN, 2013. december 18. URL: http://edition.cnn.com/2013/12/18/politics/nsa-report/ (Letöltés ideje: 2017. december 21.)

[155] GELLMAN, Barton – MILLER (2013), Greg: U.S. spy network's successes, failures and objectives detailed in 'black budget' summary. In: The Washington Post, 2013. augusztus 29. URL: http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (Letöltés ideje: 2017. december 21.)

[156] A költségvetésről bővebben lásd a The Washington Post által készített részletes infografikát: The Washington Post: Black Budget. In: The Washington Post. URL: http://www.washingtonpost.com/wp-srv/special/national/black-budget/ (Letöltés ideje: 2017. december 21.)

számít. Míg korábban a terrorizmusellenes attitűd uralkodott, ami egyet jelentett a titkosszolgálatok működésének feltétel nélküli támogatásával, felmérések szerint az amerikaiak növekvő hányada tartja túlzottnak az NSA meglevő jogkörét. Ennek a paradigmaváltásnak tudható be, hogy a képviselőházban egy olyan törvényről szavaztak, ami a védelmi minisztérium költségvetésének csökkentését vonná maga után. Igaz, maga a javaslat elbukott, de a Snowden-ügy kirobbanása előtt elképzelhetetlen lett volna, hogy ilyen törvénytervezetet nyújtsanak be.[157]

4.6. A KÖZÖSSÉGI MÉDIA SZEREPE A HÍRSZERZÉSBEN, ELHÁRÍTÁSBAN

A fejezetben hosszan értekeztem a hírszerzés módszereiről, illetve az Edward Snowden által nyilvánosságra hozott információkról. Mint látni fogjuk, a közösségi média meglehetősen sok szempontból használható hírszerzési céllal.

Rádióelektronikai felderítés és közösségi média

Az Edward Snowdennel kapcsolatos alfejezetben a PRISM kapcsán már bőven volt szó a közösségi média és SIGINT (azon belül a COMINT) kapcsolatáról, így ennél a résznél részleteiben nem tárgyalom. Amit fontos látni, a PRISM az amerikai Nemzetbiztonsági Ügynökség által fejlesztett megfigyelő program, ami gyakorlatilag valós időben képes megfigyelni a célszemélyt. Jelenleg nincs ismeretünk arra vonatkozóan, hogy mások használnak-e a PRISM-hez hasonló rendszereket. Nyilvánvalón az államok nemzetbiztonsági szolgálatai szeretnének olyan képességeket, amely által az NSA-hez hasonló megfigyelést tudnak végezni a saját és más országok állampolgáraival szemben, azonban a lehetőségeik korlátozottak az amerikai szolgálatokhoz képest. A nagy közösségi oldalak többsége amerikai tulajdonban áll, így az amerikai jogszabályok alapján a hatóságok hatékonyabban tudják az ilyen irányú akaratukat aggregálni. Minden bizonnyal hasonlóan történik mindez Oroszországban, az orosz állami tulajdonú VKontakte közösségi oldalon is, vagy a Kínában a kínai közösségi oldalakon. Arról sincs információnk, hogy a nem amerikai felhasználók esetében milyen megállapodást kötöttek a magas érdekérvényesítő képességgel bíró nemzetek. Uganda demokratikus kormányzata vélhetően kevésbé képes a Facebookot vagy a Google-t rávenni arra, hogy Uganda demokratikus népének tömeges megfigyelését segítse. Ezzel szemben Kína, hogy megengedje a Facebook kínai piacra történő lépését, cserébe olyan garanciákat vár el, amelyekbe a közösségi oldalak kénytelenek beleegyezni. Sajtóhírek szerint a Facebook például egy olyan tartalomblokkolásért felelős alkalmazást fejleszt Kínának, amelynek üzemeltetését egy harmadik félnek, egy kínai hatóságnak adná át.[158] Hogy ezenfelül egyéb megállapodáshoz kötötték-e a piacra lépést, nem tudni, mindenesetre a kínai állam igénye, hogy kontroll alatt tartsa a kínai internetezőket (gondoljunk csak a kínai „nagy tűzfalra", a VPN-ek betiltására, a cenzúrára), vitathatatlan tény. Kína gazdasági

[157] BUMP, Philip – OHLHEISER, Abby (2013): The Amash Amendment Fails, Barely. In: The Wire, 2013. július 24. URL: http://www.thewire.com/politics/2013/07/amash-amendment-fails-despite-democratic-support/67584/ (Letöltés ideje: 2017. december 21.)

[158] HORVÁTH Balázs (2016): A Facebook ördögi tervvel férkőzne be Kínába. In: 24 Tech, 2016. november 23. URL: https://24.hu/tech/2016/11/23/a-facebook-ordogi-tervvel-ferkozne-be-kinaba/ (Letöltés ideje: 2017. december 29.)

érdekérvényesítő ereje rendkívül nagy, a számára szimbolikus kérdésekben is (például Dalai Láma állami vezetők által történő fogadása) keresik a kegyeit az államok kormányzatai és a piaci szereplők. Természetesen Uganda kormányának is lehetősége van adatszolgáltatásra vonatkozó kérelmet benyújtania az állampolgáraival kapcsolatban, ezeket azonban a közösségi oldalak üzemeltetői minden esetben megvizsgálják, és ha jogosnak tartják, akkor kiadják a kért adatokat. 2017 első félévében például 78900 kormányzati adatbekérés érkezett a Facebookhoz, ebből Magyarországról 234 kérvényt nyújtottak be, 390 felhasználó adataival kapcsolatban.[159] [160] Ezeket az adatbekéréseket azonban nem szabad összekeverni a rádióelektronikai felderítéssel.

Azok az államok, amelyek nem tudják rákényszeríteni a szolgáltatókat, hogy számukra hozzáférést biztosítsanak az állampolgáraik adataihoz, megpróbálhatnak behatolni a rendszerbe, és ily módon megszerezni a kívánt adatokat. Az ilyen tevékenységeket általában a nemzetbiztonsági szolgálatok által támogatott hackercsoportok, szervezett bűnözői körök hajtják végre.

Nyílt forrású információgyűjtés és közösségi média

A közösségi média a nyílt forrású információgyűjtés aranybányája. Ennek főbb okai közé sorolhatjuk, hogy az átlag felhasználóknak nem kellően magas az adat- és információbiztonsági tudatosságuk, így életük rengeteg momentumát a nyilvánosság előtt élik. Minél hosszabb ideje, minél több közösségi oldalt használ valaki, annál pontosabb profilt lehet vele kapcsolatban meghatározni – már amennyiben nem korlátozza a láthatóságot.

Nyílt forrású információgyűjtést bárki végezhet, nem csupán a nemzetbiztosági szolgálatok. Maga a tevékenység, ha a művelője nem ismeri az eljárásokat, igen hosszadalmas folyamat is lehet, azonban léteznek olyan weboldalak, amelyek ezt rendkívüli módon felgyorsítják. Ennek egy kiváló eszköze az 5. ábrán látható oldal (www.uk-osint.net), amelynek Facebook-menüpontjában végezhetjük munkánkat. Az oldal használatához szükségünk van a célszemélyünk ID numberére, amit a tárgyalt oldalon tudunk megszerezni a több ID number generálásra hivatott oldal segítségével (6. számú ábra). Ehhez nem kell mást tennünk, csak a célszemély Facebook-profiljának linkjét bemásolnunk az oldalra, és pár másodperc alatt hozzáférünk a célszemély Facebook-profiljának ID numberéhez. Ha ezzel megvagyunk, csupán be kell illeszteni ezt a számsort a kívánt részhez, és az oldal azonnal listázza a témával kapcsolatos tartalmakat (7. számú ábra). Fontos megjegyezni, hogy az oldal csupán azokat az információkat fogja a rendelkezésünkre bocsátani, amelyek nyílt forrásból elérhetőek. Tehát semmi olyat nem fogunk találni, amiket a felhasználó nem oszt meg nyilvánosan, pláne nem listázza a személyes üzeneteit. Azonban kereshetünk minden olyan helyen, ami nyilvánosan elérhető: 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 például olyan helyre kommentelünk, ahol az ismerősünk nem tiltotta le a láthatóságot, meg fogjuk találni.

[159] Facebook Trancparency: Magyarországi adatbekérések 2017. január – 2017. június. In: Facebook, 2017. URL: https://transparency.facebook.com/country/Hungary/2017-H1/ (Letöltés ideje: 2017. december 29.)

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

5. ábra: Nyílt forrású információgyűjtés pár kattintással a Facebookról

Forrás: www.uk-osint.net

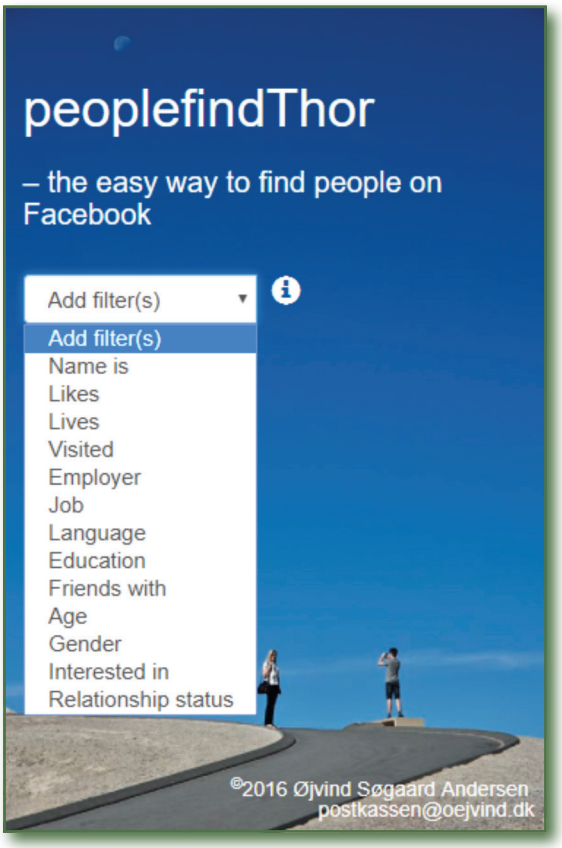
6. ábra: Hogyan szerezzük meg a célszemély Facebook ID Numberét

Forrás: http://findfacebookid.com/

7. ábra: Néhány példa, hogy milyen információkat szerezhetünk meg pár perc alatt

Forrás: https://inteltechniques.com/OSINT/facebook.html

Előfordulhat olyan is, hogy még nem ismerjük a célszemélyünket. Szerencsére (?) különböző variánsok alapján ugyanúgy végezhetünk keresést (lásd 8. számú ábra), ha bizonyos információkat tudunk csak róla: például hol lakik, hány éves, miket szeret, stb., így a megadott jellemzők alapján tudjuk kiválasztani a számunkra érdekes célszemélyeket, akiket később további vizsgálatok alá vethetünk. Természetesen itt is csak akkor kerül bele valaki a találati listába, ha ezeket az információkat nyilvánosan kereshetővé tette magáról.



8. ábra: Nyílt forrású keresés különböző variásnok alapján

Forrás: https://www.peoplefindthor.dk/

Úgy vélem, a nyílt forrású információgyűjtés egyfajta szürkezónáját jelenthetik az okosmobileszközökre készített alkalmazások, amelyek a használatáért cserébe bizonyos engedélyeket kérnek. Azért szürkezóna, mert bár engedélyt ad a használatért cserébe a felhasználó bizonyos adataihoz, ezek azonban vonatkozhatnak olyan adatokra is, amelyek semmi esetre sem minősülhetnek nyílt információnak. A geolokációs helymeghatározás, ismerőseink listája és profilképünk beletartozhat a nyílt adatok körébe abban az esetben, ha felhasználóként ezeket egyébként is nyílt információként kezeljük, azonban felmerül az a kérdés, hogy például az ismerősünk is nyíltan kezeli-e kapcsolati hálóját. A felsoroltakon kívül engedélyt adhatunk az üzeneteink tartalmához is, ez azonban megítélésem szerint semmilyen körülmények között nem nevezhető nyílt forrású információnak.

Korábban már volt szó arról, hogy a nyílt forrású információgyűjtés kiválóan használható trendelemzésre. Big Data-analízissel, a mesterséges intelligencia megjelenésével lehetséges a közösségi oldalakon folytatott kommunikáció, tartalommegosztás valós időben történő automatizált elemzése. Az amerikai Titkosszolgálat (Secret Service)[161] túllépve a közösségi médiafelületeken keletkező nagy mennyiségű tartalom szintetizálására és vizuális

[161] A Secret Service-t 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.

ábrázolására képes analitikus programon, egy olyan alkalmazás kifejlesztését tűzte ki céljául, amely többek között automatizálja a közösségi médiát monitorozó műveleteket, valamint felismeri a szarkazmust a megosztott tartalmakban.[162] Figyelembe véve, hogy egy átlagember mennyire képes felismerni a szarkazmust, különösen írott formában, az algoritmus kifejlesztése nagy előrelépés lenne mindenképpen a mesterséges intelligencia evolúciós folyamatában.

Emberi erőforrással végzett információgyűjtés és közösségi média

Az emberi erőforrással végzett információgyűjtésben a közösségi média csupán támogató funkcióval bír. Segítségével, akár nyílt forrásból, akár titkos információgyűjtést alkalmazva lehetőség nyílik a célszemélyekről olyan információkat gyűjteni, amelyek segítségével ki lehet építeni a kapcsolatot

Social engineering és közösségi média

A social engineering hírszerzéssel kapcsolatos fejezetben való szerepeltetése elsőre talán meglepőnek tűnhet, azonban számos olyan eljárást alkalmaznak a social engineerek, amelyeket a hírszerzésnél használnak.

A social engineering egy olyan támadásforma, amely során a támadó az emberi tényező kihasználható tulajdonságait[163] használja fel, hogy ily módon férjen hozzá megtévesztéssel, zsarolással a védett információkhoz, rendszerekhez.[164] Kevin D. Mitnick[165] 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."*[166]

[162] ZEZIMA, Katie (2014): The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work. In: Washington Post, 2014. június 3. URL: 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/ (Letöltés ideje: 2017. december 29.)

[163] Naivitás, hiszékenység, segítségnyújtás, kíváncsiság, biztonságtudatosság hiánya, figyelmetlenség, szexualitás stb.

[164] DEÁK Veronika (2017): Biztonságtudatosság az információs környezetben. Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, 2017/3. pp. 59–77.

[165] Kevin Mitnick magát sosem tartotta 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.

[166] MITNICK, Kevin D. – SIMON, William L.(2003): A legendás hacker – A megtévesztés művészete. Perfact-Pro, Budapest.

A social engineering támadásokat humán-[167] és IT-alapú[168] 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.[169]

Egy social engineering támadás négy fázisból épül fel:

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

A közösségi média információgyűjtésben betöltött szerepét már nem szükséges külön magyarázni. A támadók mindig azt a személyt fogják megkeresni, akin keresztül hozzáférhetnek a rendszerhez. Amennyiben az elsődlegesen kinézett személy mégsem válik be, akkor addig keresik a megfelelőt, amíg meg nem találják. A nyílt forrású információgyűjtés ez esetben is rendkívül hasznos. A már említett www.uk-osint.net nevű oldalon kezdve a műveletet először megtalálhatjuk a számunkra érdekes egyéneket. Minél nagyobb a szervezet, annál több potenciális jelöltet vizsgálhatunk utána egyénileg.

A nyílt forrású információgyűjtés mellett a 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;
- okosmobileszközökre írt alkalmazások használatával;
- adathalászoldalak felhasználásával;[170]
- rosszindulatú alkalmazások egyéb úton történő fertőzésével;[171]
- WIFI-hálózat feltörésével és lehallgatásával.

[167] DEÁK Veronika (2017): A social engineering humán alapú támadási technikái. In: Biztonságpolitika, 2017. április 10. URL: http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai (Letöltés ideje:)

[168] DEÁK Veronika: A számítógép alapú social engineer támadási technikák. In: Biztonságpolitika, 2017. április 28. URL: http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai (Letöltés ideje:)

[169] 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 beléptetőrendszer, a megfigyelőrendszer, 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.

[170] 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.

[171] Gondoljunk Emily Williams esetére, aki e-mail helyett mondjuk Facebook Messengeren küldi az elektronikus képeslapot.

A kapcsolat kiépítése a következő lépés, amely a megszerzett információk hatására nem okoz nehézséget. Tudhatjuk a célszemély preferenciáját, azt is, hová szokott járni, adott esetben milyen rendezvényen való részvételt igazolt vissza. Ezeket az információkat felhasználva a támadók sokszor minden gyanú nélkül rendezhetik meg a találkozót, amelynek során kiépítik a kapcsolatot. Ha a célszemély megosztásaiból ki lehet rajzolni, hogy milyen típusú nők/férfiak az esetei, mi a kedvenc zenekara, mi a kedvenc regénye, illetve hová jár gyakran, és milyen időpontban, nem nehéz úgy elrendezni a szituációt, hogy a célszemély maga vegye fel a kapcsolatot a támadóval, ha ő a célszemély kedvenc könyvével, egy kedvenc zenekarának a pólójával, olyan vizuális megjelenéssel ül be a törzshelyére.

A kapcsolatfelvételnek egy izgalmas kísérletét végezte két biztonsági kutató, Aamir Lakhani és Joseph Muniz, akik létrehozták egy fiatal, csinos, intelligens, a Massachusetts Institute of Technologyn végzett hölgy, Emily Williams Facebook- és LinkedIn-profiját, aki éppen munkát keresett, és kapcsolatépítésbe kezdett egy meg nem nevezett amerikai kormányügynökség tagjaival, akik valamilyen kiberbiztonságért felelős szervezetnél dolgoztak.[172] A nem létező Emilyt elég hamar hívták randevúra a beszélgetések során. Volt, aki laptopot ajándékozott neki, ezenfelül több állásajánlatot is kapott a szövetségi szervezetnél. Egy közelgő ünnep alkalmából Emily elektronikus képeslapot küldött a partnereinek, amiben egy kártékony kódot rejtettek el a kutatók. Az ügynökség több munkatársa, köztük az informatikai biztonságért felelős vezető is a munkahelyi számítógépén nyitotta meg az elektronikus képeslapot, így a támadók hozzáférhettek a rendszerhez, és bizalmas információkat tölthettek le.

A kapcsolat kiépítését követően természetesen tovább is végezhető az információgyűjtés, egészen addig, amíg nem sikerül olyan terhelő információt gyűjteni a célszemélyről, vagy nem sikerül olyan mértékű bizalmat kiépíteni, amelynek a hatására rávehető, hogy megtegye, amire a támadók kérik. Hogy mit kérnek a támadók, az a motivációjuktól függ, szimpla anyagi haszonszerzéstől kezdve hacktivista cselekedetre, terrorizmusban való segédkezésre, de akár kritikus infrastruktúra támadására is felhasználhatják a célszemélyt.

Fontosabb fogalmak

Big Five Eyes, BRUSA-egyezmény, COCOM-lista, Echelon, elektronikai felderítés, elhárítás, emberi erőforrásokkal végzett hírszerzés, FISA, gépi rádióforgalmazással kapcsolatos hírszerzés, képfelderítés, kiberhírszerzés, hírszerzés, kommunikációs felderítés, konspiráció, kriptográfia, külső engedélyhez kötött információgyűjtés, külső engedélyhez nem kötött információgyűjtés, mérés- és jelmeghatározó hírszerzés, nemzetbiztonsági modellek, NSA, nyílt forrású információgyűjtés, orvosi hírszerzés, pénzügyi hírszerzés, PRISM, rádióelektronikai felderítés, reverse engineering, Snowden-iratok, technikai hírszerzés, telemetriai hírszerzés, térinformatikai felderítés, titkos információgyűjtés, UKUSA-egyezmény, XKeyscore

Áttekintő kérdések

1. Megítélése szerint a titkosítási szabványok gyengítése fontos nemzetbiztonsági érdek, vagy egy olyan kétélű fegyver, amellyel saját magát is sokkal kitettebbé teszi a veszélyekkel szemben?
2. Milyen lehetőségek léteznek arra, hogy titkosítsuk az internetes kommunikációnkat?

[172] LAKHANI, Aamir – MUNIZ, Joseph (2013): Social Media Deception. In: RSA Cyber Security Summit Konferencia – Európa, 2013. október 29–31. URL: http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (Letöltés dátuma: 2018. január 11.)

3. Mennyire tartja megbízhatónak a titkosítást kínáló szolgáltatókat (például Snapchat, Facebook, Google, Signal, Telegram Messenger stb.)?
4. Ön szerint Edward Snowden hős vagy áruló?
5. Ön szerint a Snowden által nyilvánosságra hozott információk mennyire befolyásolják napjainkban az átlag internetező mindennapjait?
6. Megítélése szerint korlátozható-e a magánszféra a biztonság megteremtése érdekében?
7. Az okoseszközök elterjedése az Ön megítélése szerint mennyire segítenék elő egy orwelli állam fenntartását?
8. Megítélése szerint mi az a határ, amit egy demokratikus jogállam még megtehet az állampolgárai megfigyelése során?
9. Ön szerint hogyan lehet őrizni az őrzőket?

5. A KÖZÖSSÉGI MÉDIA KAPCSOLATA A HONVÉDELMI ÉS RENDVÉDELMI SZERVEKKEL

A közösségi médiának, ahogy az előző fejezetben láthattuk, igen komoly szerepe van a katonai és polgári nemzetbiztonsági szolgálatok tevékenységében, beleértve a bűnügyi felderítést is. Ebben a fejezetben a hírszerzésen túli egyéb feladatokat tekintjük át, amelyek a honvédelmi és rendvédelmi szervezetek jogszabályban előírt tevékenységét támogatják.

5.1. HONVÉDELEM

Az alfejezetben a közösségi média egy újszerű értelmezésére teszek kísérletet. Ahogyan már korábban megfogalmaztam, a közösségi médiát sokan, sokféleképpen interpretálják, de mindegyik definíció a szerző tudományterületéről vagy a használat általános mivoltából fakad.

A most következő megközelítés a közösségi média mint információs hadszíntér speciális tartományára vonatkozik.

A kibertér mint hadszíntér

Ahogyan a közösségi médiára, úgy a kibertér definíciójára is rengeteg kísérlet született műszaki és társadalomtudományi aspektusból egyaránt. Társadalomtudományi oldalról különösen izgalmas a kibertér térszerkezeti, társadalomföldrajzi megközelítése,[173] amely

- koncepcionális térfelfogás,[174]
- infrastrukturális térfelfogás,[175]
- oldaltérképek terei,
- sajátos „páva”-modellek terei és
- virtuális világok alapján differenciálja a kiberteret.[176]

[173] MÉSZÁROS Rezső (2001): A kibertér társadalomföldrajzi megközelítése. Magyar Tudomány, 2001/7., pp. 769–779.

[174] Gyakorlatilag az internetet magát értik alatta.

[175] E térfelfogás a fizikai dimenziót jelöli, beleértve a szervereket, gerinchálózatokat stb.

[176] JAKOBI Ákos (2002): A virtuális világ terei – Reflexiók Mészáros Rezső „A kibertér társadalomföldrajzi megközelítése” című tanulmányához. Magyar Tudomány, 2002/11. pp. 482 –491.

Magyarország Nemzeti Kiberbiztonsági Stratégiája a kiberteret az alábbiak alapján értelmezi: *„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"*.[177] A Magyar Honvédség Kibervédelmi Szakmai Koncepciójában az instrumentális térfelfogás jobban megjelenik, szemben a Nemzeti Kiberbiztonsági Stratégiában megfogalmazott, inkább társadalmi alrendszerekkel kapcsolatos megközelítésével: *„…az elektromágneses spektrum használatával meghatározható, dinamikusan változó tartomány, mely összekapcsolt hálózatok, eszközök és kiegészítő fizikai infrastruktúrák közötti adatok kezelésére szolgál"*.[178] A talán legkomplexebb megfogalmazás Haig Zsolttól származik: ez alapján *„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"*.[179]

Az Észak-atlanti Szövetség is egyre hangsúlyosabban kezelte a kibertér jelentette fenyegetettségeket, de ez a 2007-es Észtországot mint NATO-tagállamot ért kibertámadás után nem véletlen. Legelőször a 2010-es lisszaboni csúcson elfogadott stratégiai dokumentumban jelent meg hangsúlyosan a kibervédelem,[180] ami végül a 2016-os varsói NATO-csúcson teljesedett ki, ahol is a Szövetség a kiberteret ötödik hadszíntérként deklarálta, valamint a kibervédelmet a NATO kollektív feladatai közé emelték.[181]

A kibertérnek mint hadszíntérnek a megjelenése az információs eszközök elterjedésével és hadviselésben is betöltött szerepével magyarázható. Ennek következtében jelent meg az információs környezet fogalma, amely alatt mindazon egyének, szervezetek és rendszerek összességét értjük, akik és amelyek az információ gyűjtésével, feldolgozásával, szétosztásával foglalkoznak.[182] Ily módon a fizikai dimenzió kibővült egy földrajzi dimenzióval, mindez pedig az információs hadszíntér kialakulásával járt.[183] Az itt folytatott műveleteket nevezi a szakirodalom információs műveleteknek, amelyben az információs jelzőnekkettős jelentősége van: egyrészt vonatkozik az em-

177 1139/2013, (III. 21.) Korm. határozat Magyarország Nemzet Kiberbiztonsági stratégiájáról. In: Magyar Közlöny, 2013/47.

178 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról. In: Honvédelmi Közlöny, CXL évfolyam 10. szám, 2013.

179 i.m. HAIG (2015).

180 VARGA Gergely (2010): A NATO új, lisszaboni stratégiai koncepciója. Nemzet és Biztonság, 2010/10, pp. 79–86.

181 Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016 (online), 2016. július 9. URL: https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf (Letöltés ideje: 2018. január 23.)

182 Joint Publication 3–13, Information Operations, 27 November 2012 by United States Government US Army, p. I-1.m.

183 HAIG et al. (2014): Elektronikai hadviselés (szerk. Németh András), Nemzeti Közszolgálati Egyetem, Budapest.

lített tevékenységek folytatására, másrészt, hogy ezek nagyban támaszkodnak az infokommunikációs technológiákra. Az információs hadszíntér a valós és virtuális terekből, eszközökből, helyekből, rendszerekből tevődik össze, 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, annak hatékonyabb felhasználásáért versengenek. Az információs hadviselés célja az információs fölény, illetve ennek birtoklását követően a vezetési fölény megszerzése, a saját oldali vezetési folyamat számára az időcsökkentés, míg az ellenfél számára az időnövelés. *„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.”*[184]

Haig Zsolt és Várhegyi István az említett írásukban az információs műveleteket tevékenységi körük alapján az alábbiak szerint csoportosítják:

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

A NATO információs műveletekkel foglalkozó doktrínája a következő képességeket, eszközöket és eljárásokat határozta meg az információs célkitűzésekkel kapcsolatban:

- lélektani műveletek (PSYOPS);
- megjelenés, viselkedés, arculat (PPP);
- műveleti biztonság (OPSEC);
- információbiztonság (INFOSEC);
- megtévesztés (MILDEC);
- elektronikai hadviselés (EW);
- fizikai pusztítás;
- kulcsfontosságú vezetőkkel kapcsolatos tevékenység (KLE);

[184] HAIG Zsolt – VÁRHEGYI István (2005): Hadviselés az információs hadszíntéren. Zrínyi Kiadó, Budapest.

- számítógép-hálózati műveletek (CNO);
- civil-katonai együttműködés (CIMIC).[185]

Az információs hadviselés célja egyformán lehet támadó vagy védekező művelet. Támadó esetén a megvalósítandó cél, hogy a speciális érdekekre vagy speciális fenyegetésekre választ adva hatást gyakoroljanak a másik félre, ez békében, válságban vagy konfliktus idején egyaránt végezhető. A védelmi információs hadviselés célja pedig, hogy megvédje a saját információkat, illetve fenntartsa az információkhoz való hozzáférést, továbbá elősegítse az információs rendszerek hatékony használatát.[186]

A közösségi média mint az információs hadszíntér speciális tartománya

Az előző alfejezetben bemutattam, hogyan alakult ki az információs hadszíntér fogalma, most tekintsük át, mi alapján tekinthető a közösségi média ennek egy tartományának.

Ahhoz, hogy tartományról beszéljünk, meg kell határozni annak kereteit, valamint azokat a területeket, amelyek az információs műveletek esetében megjelennek.

A tartomány kerete értelemszerűen a felhasználókat jelenti, nem csupán a magánszemélyeket, ezenfelül gazdasági, piaci, politikai szerepelőket, valamint azokat a szervezeteket, amelyeket jogszabályi előírások alapján felhasználják a közösségi oldalakat.

A területeket az említett NATO-doktrína alapján határozhatjuk meg.

Lélektani műveletek

A lélektani műveletek (psychological operations, PSYOPS) olyan tevékenységet jelölnek, amelyek során az azt alkalmazó tudatos lélektani ráhatással kívánja célját elérni.[187] Lélektani műveleteket – noha korábban nem így nevezték – a hadviselés kezdetétől folytatnak,[188] a kifejezés pedig a 20. század második felében jelent meg. Ekkortól kezdve tudományos alapokon tervezték meg a különböző műveleteket.

Lélektani műveleteket nem csupán az ellenség ellen végeznek, ugyanúgy lehet célpontja szövetséges, semleges állam vagy annak saját lakossága. Korábban gyakran propagandaként hivatkoztak a lélektani műveletekre, azonban ez nem teljesen helytálló, hiszen a propaganda gyakran valamilyen ideológiai töltetet képvisel. A propagandát, eljárások tekintetében, három kategória alapján szokás megkülönböztetni:

185 AJP-3.10 Allied Joint Doctrine for Information Operation, 2009. URL: https://info.publicintelligence.net/NATO-IO.pdf (Letöltés ideje:...)

186 BÁNYÁSZ Péter: A közösségi média, mint az információs hadszíntér speciális tartománya. Hadmérnök, XII. Évfolyam „KÖFOP" szám – 2017. október.

187 PIX Gábor (2005): A lélektani műveletek jellemzőinek vizsgálata, Doktori (PhD) értekezés. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest.

188 Gondoljunk csak arra, amikor befestették magukat, állati csontokkal díszítették magukat, harci dobokat alkalmaztak, stb., hogy ijesztőbbnek tűnjenek, és ily módon jussanak előnyhöz harc közben.

- A fehér propaganda jellemzője, hogy ismert a közvetítője; gyakran valósághű, a hírforrása hiteles, így könnyű a terjedését megakadályozni, illetve cáfolni a valótlanságokat. Eszköztárának jellegzetes példányai a vicclapok, karikatúrák, amelyekkel az ellenséget teszik nevetségessé.
- A fekete propaganda a valóságtól eltérő hírközlést jelent, alkalmazói gyakran álcázzák önmagukat, megtévesztve a célközönséget, mintha az nem az ellenségtől származna, hanem a saját kormánytól.
- A 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. Idetartozhat például a hátországból származó álhírek terjesztése, amelyben a katonák családjainak pusztulásáról vagy éppen feleségeik, barátnőjük hűtlenségéről szólnak.

A NATO lélektani műveleti doktrínája[189] éppen azért, hogy a propaganda kifejezéshez társuló történelmi és ideológiai[190] képzettársításokat elkerülje, a célzott információközlés fogalmát használja. A célzott információközlésre számos eszköz áll rendelkezésre, de napjainkban az egyik legjelentősebb forrás a közösségi média. Az egyik legelterjedtebb módja az álhírek alkalmazása, amely napjainkra globális hatásúvá vált, a politikai-közéleti kérdésekben az egyik legnagyobb kockázatként nevesítve politikai szereplők részéről. Az álhírek jelentőségéről és szerepéről a közösségi médiával és a politikai alrendszerrel kapcsolatos fejezetben bővebben lesz szó.

Megjelenés, viselkedés, arculat

A megjelenés, viselkedés, arculat (Presence, Posture, Profile – PPP) kiemelten fontos minden szervezet számára, hiszen ezek az általuk képviselt célok, feladatok végrehajtása esetében is relevánsnak tekinthetők. A csapatok, de akár az egész szervezet megjelenése, viselkedése, cselekedetei üzenetértékűek, amelyek akár elrettentésre, akár a bizalom erősítésére is szolgálhatnak. Nem véletlen, hogy a NATO a bipoláris világrend felbomlását követően egy olyan együttműködő, barátságos, a hidegháborútól eltérő szervezet képét igyekezett magáról festeni, ami egyben a legitimációs válságáról is eltereli a figyelmet. Éppen ezért a NATO igen komoly közösségi médiajelenlétet valósít meg a különböző platformokon.

A megjelenés, viselkedés és arculat megfelelő tervezése jelentős lehet a szervezet pozitív percepciójának megteremtésében, ami a toborzásban, a lakosság körében való mélyebb beágyazódást, támogatást is erősíti. Ez utóbbi különösen fontos, ugyanis amennyiben a szervezetet komolytalannak gondolják, úgy az nem csak a rekrutációban érezteti negatív hatását, hanem a költségvetési források odaítélésében is.

A Magyar Honvédség közösségi médiában való jelenléte professzionálisnak tekinthető, és ezt a színvonalat évek óta tartja.

[189] AJP-3.7. NATO Military Policy on Psychological Operations, 2003. URL: https://info.publicintelligence.net/NATO-PSYOPS-Policy-2003.pdf (Letöltés ideje:...)

[190] A modern propaganda atyjának Joseph Göbbelst tartjuk, aki miatt a propaganda szó gyakran a nácizmussal fonódik össze.

Műveleti biztonság

A műveleti biztonság (Operations Security, 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.[191] A műveleti biztonság és a közösségi média összefüggését korán felismerték; az Egyesült Államok hadserege kézikönyvet is kiadott, amelyben a műveleti biztonság megteremtésének módjait határozták meg. Ebbe nem csupán az tartozik bele, hogyan használják a katonák a közösségi oldalakat, hogyan jelenjenek meg rajtuk, de az is, milyen információkat osszanak meg, és hogyan. Nem egy alkalommal fordult elő, hogy egy katonai akciót el kellett halasztani, ugyanis az abban részt vevő katona kiposztolta, hogy mikor és hová készül bevetésre, például egy ciszjordániai hadműveletre induló izraeli katona.[192] A geolokációs helymeghatározás is befolyásolja a műveleti biztonságot. Egy iraki katonai bázison történt meg, hogy új helikopterek érkeztek egy repülőegység számára, és az ott szolgálatot teljesítő katonák a róluk készült képeket feltöltötték 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.[193]

Információbiztonság

Az információbiztonság (Information Security, INFOSEC) bár része a műveleti biztonságnak, azonban sokkal szélesebb területet jelent. A hírszerzéssel kapcsolatos fejezetben részletesen volt szó arról, mennyi információt lehet gyűjteni a felhasználókról, így ennél a résznél nem ismételjük meg. Jogosan merülhet fel a kérdés, miért nem tiltják akkor a katonák számára a közösségi oldalak használatát, ha ilyen kockázatot jelent a műveleti és információbiztonságra egyaránt. Bár volt kísérlet a tiltásra, de a katonai vezetők belátták, hogy ez nem vezet eredményre. Ennek egyik legfontosabb oka, hogy igen fontos szerepe van a katonák családjukkal történő kapcsolattartásában, ez pedig a morál fenntartásának egyik legfontosabb eszköze. Amennyiben tiltani szeretnék, úgyis megtalálnák a módját, hogy kijátsszák, ezáltal pedig valószínűleg igen súlyos biztonsági kockázatokat is generálva.

Kulcsfontosságú vezetőkkel kapcsolatos tevékenységek

A kulcsfontosságú vezetőkkel kapcsolatos tevékenységek (Key Leaders Engagement – KLE) elsősorban az általuk kezelt infokommunikációs technológiák használatához, illetve azok védelméhez kapcsolódnak. Egy katonai művelet során[194] az ott szolgálatot teljesítő katonai vezetőknek elsődleges, hogy megfelelő kapcsolatot tartsanak fenn a

[191] MUHA et al. (2007): Az informatikai biztonság kézikönyve (szerk. Szenes Katalin). Verlag Dashöfer, Budapest.

[192] MTI: Izrael lefújt egy katonai akciót a Facebook miatt. In: Metropol, 2010. március 3. URL: http://www.metropol.hu/cikk/535056 (Letöltés ideje: 2018. január 13.)

[193] RODEWIG, Cheryl (2012): Geotagging poses security risks. In: Army.mil, 2012. március 7. URL: http://www.army.mil/article/75165/Geotagging_poses_security_risks/ (Letöltés ideje: 2018. január 13.)

[194] Napjainkban a katonai műveletek jellemzően békeműveleti tevékenységek körébe tartoznak. Háború indítására a nemzetközi jog csupán az Egyesült Nemzetek Szövetségének Biztonsági Tanácsa általi felhatalmazására van lehetőség, ennek ellenére mégis gyakoriak a katonai konfliktusok. Minden ilyen esetben a NATO az ENSZ Biztonsági Tanácsának felhatalmazása alapján vesz részt valamilyen béketámogató

műveleti területen élő kulcsfontosságú katonai, politikai, gazdasági vezetőkkel. Ennek érdekében különösen fontos, hogy elegendő információkkal rendelkezzenek az adott személyekről, hogy a bizalmat a lehető legmagasabb szintűre építhessék ki. A vezetőkről való információszerzésnek kiváló eszközei a közösségi oldalak, az okosmobileszközök, hiszen az említett személyek nem feltétlenül rendelkeznek magas információbiztonsági és adatvédelmi tudatossággal. Elég ez esetben Hillary Clintonra gondolni, aki külügyminiszterként a tiltás és protokollok ellenére saját mobileszközét is használta hivatalos levelezésre, amelyhez hackerek végül hozzáfértek. Az is kockázatot jelent, ha a vezetők az általuk birtokolt eszközöket másoknak is odaadják, például a kisgyerek rátelepít valamilyen alkalmazást, hiszen megnő az esélye, hogy az eszközökön tárolt érzékeny információk harmadik fél részére hozzáférhetőek legyenek. Éppen ezért a kulcsfontosságú vezetőkkel kapcsolatos tevékenységek két oldalról értelmezhetőek: míg egyrészt a saját vezetőink esetében ezen eszközök védelme, addig a másik oldalról a szemben álló felek kulcsfontosságú vezetők által használt közösségi eszközök feltérképezése információszerzés reményében elengedhetetlen.[195]

Számítógép-hálózati műveletek

A számítógép-hálózati műveletek (Computer Network Operations – CNO) kapcsán a közösségi média támogató szerepet játszik. A CNO-ról a második fejezetben volt szó, ezért itt csupán említés szintjén foglalkozunk a témával. A közösségi média elsősorban rosszindulatú alkalmazások terjesztésében játszik fontos szerepet, amely mind a hálózatokhoz, rendszerekhez való hozzáférésben jelentkezhet, mind az azokban tárolt információk megszerzését segítheti elő.

Civil-katonai együttműködés

A közösségi média a civil-katonai együttműködésben (Civil-Military Cooperation – CIMIC) különösen fontos eszköz. A civil környezet hatással bír a nem háborús katonai feladatok ellátásának sikerességére, hiszen nagyban befolyásolja, hogy a civil környezet mennyire barátságos vagy ellenséges az ott szolgálatot teljesítő idegen katonai erőkkel szemben. 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 támogassa az idegen katonai erők tevékenységét, CIMIC-csoportokat hoznak létre, amelyek feladata a lakosság, a kulcsfontosságú vezetők támogatásának elnyerése, de ha ez nem is érhető el, legalább a semleges viszony kialakítása. 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 hosszú távon segíthet kialakítani egy olyan civil környezetet, amely növeli a konfliktus békés lezárását, a nemzetközi erők kivonása után a béke fenntartását.

---

műveletben, amely vonatkozhat megelőző diplomáciára, béketeremtésre, békefenntartásra, békeépítésre, béke kikényszerítésre, válság diplomáciára. Bővebben lásd: RESPERGER István (2012): A „diadal" és egyéb módszerek alkalmazása a nemzeti válságkezelési feladatok megoldásánál. Hadtudományi Szemle, 5. évfolyam 1–2. szám. pp. 141–165. URL: http://archiv.uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2012/2012_1/2012_1_br_resperger_istvan_141_165.pdf (Letöltés ideje:...)

[195] KOVÁCS Zoltán (2014): Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára. Hadmérnök, IX/3. szám, pp. 182–190., 2014.

A közösségi média szerepe a létfontosságú rendszerelemek elleni támadásban

Figyelembe véve a közösségi média szerepét az információs műveletekben, nem nehéz belátni, hogy mekkora szerepe lehet a közösségi médiának egy komplex kibertámadás kivitelezésében, vagy akár egy létfontosságú rendszerelemet érintő támadás megvalósításában.[196] [197]

Egy ilyen támadás esetén a közösségi médiát első lépésként a hírszerzésre használhatják a támadók. A hírszerzést követően a számítógép-hálózati műveletek során olyan kártékony kódkampányokat hozhatnak létre, amelyek segítségével botnethálózatokat építhetnek fel. A botnethálózatoknak egyrészt a következő fázisban, a lélektani műveletek végzésében lesz szerepe, majd az azt követő konkrét támadás megvalósításában.

A támadók következő lépése a lélektani műveletek végzése lesz. Ez esetben először, az úgynevezett sejtetés időszakában, a támadók egy hozzájuk köthető blogon, híroldalon megjelentetnek egy olyan hírt, például a kibervédelem gyengeségéről vagy valamilyen kritikus infrastruktúra védelmének hiányosságáról, amely ezt követően virális tartalomként megjelenik a közösségi médiában (terjesztés fázisa), majd egyre többen osztják meg ezeket a híreket, nagymértékben támogatva a támadók által üzemeltetett álprofilokkal, botnethálózatok segítségével (megosztás fázisa) működő oldalt. Ezt követően (kiemelés fázisa) a közösségi oldalakról átkerülnek a hírek először a bulvársajtóba, majd a mainstream médiába, ahol az „eredeti hír" még nagyobb figyelmet kap.[198]

A támadás következő fázisa a látványos informatikai ostrom, amelyet a korábban felépített botnethálózat segítségével végezhetnek. Ezek a támadások egyrészt túlterheléses támadások formájában, másrészt a híroldalak, állami szervek híroldalainak és közösségi oldalainak úgynevezett „defacement"-támadásaiban valósulhatnak meg. Utóbbi esetében olyan tartalmakat publikálhatnak, például be nem következett terrortámadásokról szóló beszámolókról stb., amelyek növelik a pánik kialakulását. A közösségi oldalaknak nagy szerepe van a kríziskommunikációban (erről a következő fejezetben bővebben lesz szó), így ezeknek a csatornáknak a támadása és ezen keresztüli pánikkeltésre való felhasználása igen komoly fenyegetést jelent, ami valószínűsíthetően elég nagy károkat okozna.

5.2. RENDVÉDELEM

A rendvédelem esetében a bűnügyi felderítés az elsődleges alkalmazási területe a közösségi médiának (amelynek módszereiről korábban volt szó), ezenfelül kiemelt terepe lehet a különböző rendőrségi kampányok terjesztésének is. A közösségi oldalak rólunk gyűjtött információi nagyon pontos hirdetések megjelenítésére alkalmasak; számos jellemző (lakhely, korosztály, iskolai végzettség, preferancia stb.) alapján targetálhatunk kampányokat, így a különböző üzeneteket különböző célcsoportoknál eltérően jeleníthetjük meg, legyen szó a drogfogyasztásról, ittas vezetésről stb.

[196] KOVÁCS László – KRASZNAY Csaba (2010): A digital Mohács: a cyber attack scenario against Hungary. Nemzet És Biztonság: Biztonságpolitikai Szemle III:(Spec. Issue Winter). pp. 49–59.

[197] KOVÁCS László – KRASZNAY Csaba (2017): Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, In. Nemzet és Biztonság, 2017/1. pp. 3–16. URL: http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf (Letöltés ideje:)

[198] A kiemelés fázisát is erősíthetik természetesen a támadók saját erőforrásaik függvényében.

Ebben az alfejezetben azonban alapvetően azokat a területeket tekintjük át, amelyek a kiberbűnözés kapcsán érintettek, hiszen mint a kiberfenyegetettségek trendjeinél egyértelműen megállapíthattuk, a kiberbűnözés a legygyakoribb kibertámadás a motivációk szerint megoszlás alapján.

De mik azok a területek, ahol a kiberbűnözés összefonódik a közösségi médiával? Ennek megválaszolásához a második fejezetben már idézett Europol szervezett bűnözés internetes fenyegetettségét vizsgáló éves jelentését hívom segítségül. A jelentés 12 területet foglal magában, amelyek a kiberbűnözés során veszélyeztetettek. Ebből csupán két terület, a különböző pénzügyi tevékenységek, illetve az internetirányítás nem kapcsolódik semmilyen módon a közösségi médiával. A 10 érintett területet inkább áttekintésként vizsgáljuk, mert korábban különböző formákban már érintettük.

Malware-ekkel való visszaélés

A közösségi médiából a malware-ek kiirthatatlannak tűnnek. Kampányszerűen bukkannak fel, és gyakran nagymértékű fertőzést érnek el. Annak ellenére, hogy viszonylag könnyen kiszűrhetőek azok a jellegzetességek, amik arra utalnak, hogy kártékony kóddal fertőzött hivatkozással, videóval van dolgunk, mégis rendszeresen felbukkannak, sokszor ugyanazokat az áldozatokat megfertőzve, akiket korábban is. A közösségi oldalakon, különösen a Facebookon terjedő malware-eknek a főbb ismertetői az alábbiak:

- idegen nyelvű üzenetet kapunk olyan ismerősünktől, aki nem beszél azon a nyelven;
- hírességről vagy saját magunkról szóló erotikus tartalmat ígérő videó, hivatkozás;
- tömegesen jelölnek meg ismerőseink valamilyen megosztott tartalomnál;
- rövidített link, amely vagy a fentieket vagy egyéb szenzációt ígérte;[199]
- óriási kedvezményt ígérő tartalom (például márkás napszemüveg néhány dollárért stb.).

Az ily módon megfertőzött számítógép sokmindenre használható, ami a malware létrehozójának céljától függ. Ez alapján:

- zsarolóvírus kerülhet az eszközre, ami titkosítja a file-jainkat;
- hozzáférést engedélyezhet a rendszerünkhöz;
- kémprogramok kerülhetnek az eszközre;
- botnethálózat részévé válhat az eszközünk, és az erőforrásainkat a támadók saját céljaikra használhatják, például kriptovaluta bányászása, spamküldés vagy akár DoS támadásban való felhasználás.

Gyerekek szexuális kizsákmányolása

A pedofil tartalmak napjainkra egyre inkább a Darknetre helyeződnek át, amelynek fő oka a felderítés nehézségére vezethető vissza, azonban a közösségi oldalak igen nagy kockázatot jelentenek. A YouTube tele van olyan kísérletekkel, amelyek során a támadók fiatal fiúknak adták ki magukat, és közösségi oldalakon ismerkedtek fiatal lányokkal, akiket különböző dolgokra vettek rá: találkozzanak valahol kettesben, felveszik őket a furgonjukkal, és elmennek

[199] A rövidített URL nem minden esetben jelent kockázatot, de olyankor mindenképpen gyanús kell legyen, amikor olyan ismerősünk küldi, aki vélhetően nem tudja a módját, hogyan kell egy URL-t rövidíteni.

szórakozni, vagy amikor a lány szülei nincsenek otthon, átmennek hozzá.[200] Ezekbe a kísérletekbe a szülők is be voltak avatva, akik meg voltak győződve arról, a lányaik nem fognak igent mondani a megkeresésekre, hiszen elmondták nekik, milyen veszélyt is jelentenek az ismeretlenek. Nem nehéz belátni, ha a támadók célja a gyermekek szexuális abúzusa, milyen könnyen a bizalmukba tudnak férkőzni a közösségi oldalakon létrehozott álprofilok segítségével. Mint láthattuk, azokat is könnyű megtéveszteni, akiknek a szülei megpróbálták az ezzel kapcsolatos veszélyekre felhívni a figyelmet, és odafigyelnek. Azok pedig, akiket a szüleik elhanyagolnak, és emiatt különböző komplexusok vezérelnek, az elismerésért, illetve hogy szeressék őket, mindent képesek megtenni, óriási veszélyben vannak.

Nem szabad elfedni azt sem, hogy az okos mobil eszközökbe egyre jobb minőségű kamerák kerülnek, ami a Facebook Live, YouTube Live vagy egyéb streamingszolgáltatásokkal mindenféle technikai ismeret és komolyabb felszereltség nélkül jó minőségű audiovizuális tartalmakat lehet szolgáltatni. Nyilvánvalóan nem a Facebook vagy a YouTube lesz a pornográf streamingszolgáltatások felülete, de adott esetben ezeken az oldalakon közvetíthetnek olyan tartalmakat, amelyek a kiskorú megalázását mutatják, legyen szó fizikai vagy szexuális erőszakról.

Fizetőeszközzel elkövetett csalás

A fizetőeszközökkel elkövetett csalások alapvetően a bankkártyával összefüggő csalásokra (visszaélés, hamisítás stb.) vonatkoznak. Az e-kereskedelem elterjedésével azonban a visszaélések növekvő százaléka az egyéni vásárlók közötti (C2C) üzleti tevékenységekkel kapcsolatos.[201] Az e-kereskedelem növekvő sikere így természetesen az egyes közösségi oldalakon (például Facebook Marketplace) is lehetővé teszi az egyéni vásárlók közti üzleti tevékenységek folytatását.

Social engineering

A social engineeringről a negyedik fejezetben bővebben volt szó, így itt nem térünk ki rá.

Adatok megszerzése, hálózatok támadása

Adatok megszerzése alatt az adathalász-technikákat kell értenünk a közösségi média esetében. A közösségi oldalakon, különösen a Facebookon rengeteg olyan adathalász-alkalmazás található, amely egy pár perces szórakozást ígér (Mi az indián neved? Melyik amerikai elnök lennél? Mennyire ismered a keleti blokk autócsodáit? A kitöltők csupán 2%-a tudja a helyes megoldást…[202]), cserébe hozzáférést adunk az adatainkhoz. Az ilyen alkalmazásoknak az adataink kicsalása mellett egy másik aspektusát is fontos megemlíteni. Vannak alkalmazások, amelyek számtalan ilyen mini „játékot" üzemeltetnek (például a NameTest). Minél több ilyen kérdésre felelünk, egy idő után egyre pontosabb személyiségprofil rajzolható ki a felhasználóról, amit az alkalmazás készítői marketingcélokra továbbadnak – erről a következő fejezetben bővebben is lesz szó.

---

200 Érdemes megtekinteni például az alábbi videót: https://www.youtube.com/watch?v=6jMhMVEjEQg, vagy a YouTube keresőjébe a The Dangers Of Social Media (Girl Edition)! cím beírásával.

201 KRASZNAY Csaba – SIMON Béla (2017): Kiberbűncselekmények az online kereskedelemben. Hadmérnök, XII. Évfolyam „KÖFOP" szám – 2017. október.

202 Mindezek nyilvánvalóan rendkívül bonyolult kérdések, hiszen nagyszámban osztják meg az emberek, lásd az ember kihasználható tulajdonságait a social engineering esetében.

Az alkalmazások mellett, hasonlóan a kártékony kódokkal, időnként kampányszerűen terjednek olyan átverések, amelyek segítségével szintén kicsalják a gyanútlan felhasználók adatait (például ingyen repülőjegyek).

A hálózatok támadásra a malware-eknél írtak érvényesek.

Létfontosságú rendszerelemek ellen elkövetett támadások

A létfontosságú rendszerelemek elleni támadások a kiberhadviselés klasszikus célpontjai. Egy ilyen nagymértékű, komplex támadás azonban komoly tudást feltételez, ezért is az államok közti konfliktusokban jelenik még csak meg. Ez a fajta tudás azonban pénzre váltható, és a szolgáltatásszerű bűnözés megjelenésével megvan a kockázata, hogy akár terroristák is megvehetik azokat a hackereket a Darkneten, akik képesek egy ilyen célzott támadás végrehajtására.

A közösségi média a létfontosságú rendszerelemek támadásában az alábbi módokon használható fel:

- információgyűjtés;
- social engineering;
- malware-ekkel való visszaélés;
- lélektani műveletek.[203]

Online kommunikáció

Snowdennek köszönhetően tudjuk, milyen mértékben képesek megfigyelni a nemzetbiztonsági szolgálatok az internetes aktivitásunkat. Ennek ellenére mégis vannak olyan területek, amelyeket – legalábbis jelenlegi ismeretek alapján – nem tudnak megfigyelni, így titkosított kommunikációt folytathatunk általuk. Ilyen alkalmazás például a Signal, a Telegram Messenger, de ilyen titkosított beszélgetést ígér a Facebook és a Hangouts is. Utóbbiakról viszonylag korán kiderült, hogy ez csupán ígéret. Legyen szó bármelyik VoIP-alapú alkalmazásról, mindegyik esetében a bizalom kulcskérdés: elhisszük-e a fejlesztőknek, hogy valóban titkosítást biztosít.

Mindezek ellenére a konspirált kapcsolattartásra számos lehetőséget rejtenek a közösségi oldalak. Képekbe rejtett üzenetek kiszűrésére megvan a technikai háttér, de a különböző kódolt üzenetekre, amelyeket, mondjuk, YouTube-on hagynak egymásnak, és csak a feladó és fogadó ismeri a valódi tartalmat, már sokkal nehezebb.[204] Szintén nehéz a különböző online játékokban kiszűrni azokat, akik ezeket használják kapcsolattartásra. Nem véletlen, hogy az NSA külön osztályt tartott fenn azoknak az ügynököknek a koordinálására, akik különböző online játékokba épültek be. A 2015-ös párizsi terrortámadás esetében is felmerült, hogy a terroristák a PlayStation 4 segítségével tartották a kapcsolatot egymással.[205]

[203] Egyrészt a támadás előtt álhírekkel pánikot kelteni, a támadás során, közben pedig fokozni a pánikot.

[204] Persze így is sikerült már orosz alvóügynököket letartóztatni, akik ily módon tartották a kapcsolatot egymással.

[205] Azóta bebizonyosodott, hogy nem így történt ebben az esetben.

A kibertér és a terrorizmus összefonódása

A kibertér és terrorizmus összefonódására az Iszlám Állam tökéletes példával szolgál. Ez alapján az alábbi területeken használhatják a közösségi médiát, mint ahogy többségüket az elmúlt években használták is:

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

Szerencsére napjainkban még nincs meg a humán és technikai képességük a terroristáknak, hogy egy létfontosságú rendszerelem ellen kövessenek el kibertámadást, azonban a Darkneten kellő anyagi forrás meglétével megvásárolhatnak ilyen szolgáltatást.

Darknet

A Darknetről többször volt szó e tankönyv során. Több olyan területet is meghatároztunk korábban, amelyek a közösségi médiával kapcsolatba hozhatóak, például pedofil tartalmak, amelyeket közösségi oldalakon csaltak ki gyanútlan felhasználóktól, vagy szolgáltatások, amelyeket itt vásárolnak meg (közösségi profil feltörése, adathalász malware-ek stb.).

Bár nem a Darknethez mint az internetes illegális „kereskedő felületéhez kapcsolódik", de nem feledkezhetünk meg az anonimitás igényéről, ami nem feltétlenül illegális cselekmények elkövetésének szándékából következik. A TOR-böngésző kifejlesztése mögött az az igény fogalmazódott meg, hogy segítségével kapcsolatot tudjanak tartani azok az ellenzéki szereplők, akiknek egyébként nincs módjuk a politikai véleményük kifejezésére vagy politikai szerveződésre az elnyomó államhatalommal szemben. Ahogy Edward Snowdentől is tudjuk, olyan mértékben figyelnek meg tömegesen, akár valós időben a demokratikus államok is, amely a magánszféránk szinte teljes megsemmisülésével jár együtt. Így természetes, hogy az ember elkezdi keresni annak a lehetőségét, hogy megőrizze a magánszféráját. A TOR-böngésző vagy a kriptovaluták használatából még nem következik a bűnös szándék.

Internet of Things, Big Data, Clouds

Big Datáról már többször volt szó. Az általa kinyerhető információk rendkívül értékesek megfelelő kezekben. Nem véletlen, hogy a nyílt forrású információgyűjtés egyik iránya a Big Data trendelemzésre való felhasználása. A közösségi oldalakon az elmúlt évtizedben rengeteg adat keletkezett. A különböző adathalász-alkalmazások esetében már említettem azokat a kvízeket, amelyeket valójában profilozásra használnak, hogy azokat értékesítsék harmadik fél részére. A 2016-os BREXIT-népszavazás során a kilépéspártiak, valamint Donald Trump elnöki kampányában nagy segítségre volt egy Cambridge Analytica nevű Big Data-analízissel és lélektani műveletekkel foglalkozó cég, ami számos forrásból, többek között ilyen kvízekből gyűjtött adatokat a felhasználói szokásokról, s használta fel célzott politikai hirdetések megjelenítésére. Kihasználva a „Filter Bubble"-jelenséget, vagyis azt az állapotot, amikor egy felhasználó azokat a tartalmakat látja, amelyeket egy algoritmus a felhasználói szokásait elemezve úgy

értékel, hogy ezek a tartalmak érdekelhetik, a Cambride Analytica olyan célzott politikai hirdetéseket jelenített meg, amelyek a felhasználó esetében teljesen egyediek voltak. Amennyiben valaki abban hitt, hogy Hillary Clinton valójában gyíkember, és az elnökségén keresztül szeretnék a Szabadkőművesek chemtraillel, oltásokkal továbbra is megtéveszteni az embereket, hogy a föld nem lapos, akkor az a személy bizony ilyen konkrét politikai üzeneteket látott. A Cambridge Analytica mellett természetesen a Facebook, a Google is rendkívül pontos, egyénre szabott hirdetéseket forgalmaz, politikai kampányok esetében külön csomagokat létrehozva.

A felhők használata számos pozitív dologgal jár, de egyben rengeteg kockázatot is rejt. Felhőket sokszor úgy is használunk, hogy nem tudjuk az adott szolgáltatásról, hogy az felhőként is üzemel. A Facebookot, a Gmailt sokszor ilyen módon alkalmazzuk, hiszen képeket, file-okat tárolunk segítségével olyan szervereken, amelyek nem a mi birtokunkban vannak. A kérdés az, hogy az itt tárolt dokumentumoknak ki a tulajdonosa. Csak mi magunk? Vagy lemondunk a felhasználásukról? A Google esetében több botrány is övezte a felhőszolgáltatásukat. Az egyik a Google Drive elindításához kapcsolódott, amikor a felhasználási feltételekben az a kitétel szerepelt, hogy a felhasználó lemond a feltöltött file-okról, és a Google szabadon felhasználja céljaira. A botrány hatására ezt megváltoztatták, és arra hivatkoztak, hogy csupán elírás történt. Szintén a Google esetében keltett kisebb felzúdulást, hogy a feltöltött képeket reklámcélra felhasználhatták.

A felhők biztonsága kulcskérdés, számos esetben szivárogtak ki feltöltött erotikus fényképek, amelyek az érintett híresség miatt nagy hírverést okoztak. Nem mindegy tehát, milyen típusú és tartalmú fájlokat tárolunk a felhőben. Azáltal, hogy az üzleti szférában egyre elterjedtebbek a felhőszolgáltatások, kulcskérdés, ki és milyen módon fér hozzá a felhőkben tárolt adatainkhoz.

Fontosabb fogalmak

Big Data, célzott információközlés, civil-katonai együttműködés, Darknet, „defacement"-támadás, dezinformáció, elektronikai hadviselés, felhőszolgáltatás, fizetőeszközzel elkövetett csalás, gyermekek szexuális kizsákmányolása, hadszíntér, információs célpontok fizikai pusztítása, információbiztonság, információs fölény, információs környezet, információs műveletek, Internet of Things, kibertér, kriptovalulta, kulcsfontosságú vezetőkkel kapcsolatos tevékenység, lélektani műveletek, létfontosságú rendszerelemek, megjelenés, viselkedés, arculat, műveleti biztonság, propaganda, stratégiai kommunikáció, számítógép-hálózati műveletek, szolgáltatásszerű bűnözés, TOR, vezetési fölény.

Áttekintő kérdések

1. Ön szerint az államok nemzetbiztonsági szolgálatai céljaik megvalósítása érdekében felhasználják-e a kiberbűnözőket?
2. Hogyan értékeli a TOR-böngészőt?
3. Ön szerint milyen módon lehet megvédeni a fiatalkorúakat a kibertámadásoktól?
4. Ön szerint szükséges, hogy a katonák, rendőrök speciális szabályok mentén használják a közösségi oldalakat?
5. Ön tiltaná vagy engedélyezné, hogy a katonák, rendőrök használják a közösségi oldalakat?
6. Ön szerint a kibertér önálló hadszíntérnek minősül, vagy túlértékelik a hadviselésben betöltött szerepét?

6. A KÖZÖSSÉGI MÉDIA A KÖZSZOLGÁLATBAN

Ahogyan korábban már megfogalmazásra került, a közösségi média olyan, ahogyan használjuk. A második fejezet, amelyben alapvetően a fenyegetettségeket mutattuk be, azt a hamis illúziót keltheti, hogy alapvetően veszélyes a közösségi oldalak használata, de ez természetesen félrevezető. Rengeteg pozitív dologra alkalmazható, nemcsak a magánéletben, de a közszolgálatban is. E fejezetben a pozitív és negatív oldalát járjuk körbe.

6.1. A KÖZÖSSÉGI MÉDIA AZ ÖNKORMÁNYZATOK OLDALÁRÓL

Az infókommunikációs technológiák, az internet elterjedése jelentős mértékben hozzájárulnak a gazdaság fejlődéséhez.[206] Ez alatt nem csak a távmunkát, az e-kereskedelmet és az egyéb, világhálón keresztül lebonyolított tranzakciókat, illetve az internethez köthető gazdasági tevékenységeket kell érteni; az internet elterjedése, sőt, magának a kapcsolatnak a sebessége is jelentős hatással van a GDP növekedésére.[207] A széles sávú internetpenetráció növekedésével többek közt a távmunka és a rugalmas munkavégzés terjedése, illetve a szolgáltatások bővítése és hatékonyabbá tétele révén számottevően növelhető egy gazdaság termelékenysége. Ezt támasztja alá az is, hogy egyes felmérések szerint a széles sávú internetpenetráció 10 százalékpontos növekedése 1,1%-kal emeli a hazai összterméket, ezer új előfizetés pedig 80 új munkahelyet teremt.

Az infokommunikációs technológia jelentősége sosem volt ilyen nagy, mint most, hiszen távközlés és informatika nélkül ma már elképzelhetetlen az oktatás, az egészségügy, a közlekedés vagy a közigazgatás működtetése. Mindezek alapján úgy gondolom, kijelenthetjük, hogy az informatikailag elmaradott települések lemaradnak. Természetesen ezek az elmaradott, felzárkóztatásra szoruló térségek jellemzői, amelyek nem rendelkeznek megfelelő infrastruktúrával. A piaci, de különösen az állami szereplők akkor gondolkodnak helyesen, ha a javak egyenlőségének utópiája helyett a javakhoz való hozzáférés egyenlőségének megteremtésén fáradoznak. Az infokommunikációs technológiában rejlő lehetőségek kiválóan alkalmasak ennek megteremtésére.[208]

---

206 MCKINSEY & CO.: Online and upcoming: The Internet's impact on aspiring countries, 2012. január. URL: http://www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries pp. 81-91. (Letöltés ideje: 2017. augusztus 8.).

207 ERICSON PRESS RELEASE: New study quantifies the impact of broadband speed on GDP. In: Ericson, 2011. szeptember 27. URL: http://www.ericsson.com/news/1550083 (Letöltés ideje: 2017. augusztus 8.).

208 GARTNER PRESS RELEASE: Gartner Says Capitalism Going Social Will Require Organizations to Build Two-Way Relationships with the „99 Percent". In: Gartner Research, 2012. december 12. URL: http://www.gartner.com/newsroom/id/2260917 (Letöltés ideje: 2017. augusztus 8.)

Egy önkormányzat több céllal használhatja a közösségi médiát:

- a kommunikációt erősítésére;
- a településünk imázsának építésére;
- turisták vonzására;
- befektetőket szerzésére;
- a lakosok aktivizálására;
- kapcsolattartásra;
- fontos témák közéletbe való beépítésére;
- költséghatékony ügyfélszolgálatként;
- rendkívüli események kezelésére.

Mivel e tankönyv alapvetően a biztonság fogalma köré épül, így a felsoroltak közül bővebben a rendkívüli események kezelésével fogunk foglalkozni.

6.2. A KÖZÖSSÉGI MÉDIA ÉS A RENDKÍVÜLI ESEMÉNYEK

Először is, fontos tisztáznunk, mi a vészhelyzet: olyan természeti csapás vagy ember okozta hirtelen esemény által bekövetkezett rendellenes körülmény, amely nagy területekre is kiterjedhet, és emberéletet, testi épséget, anyagi javakat veszélyeztet. Ezzel szemben a veszélyhelyzet jogszabályban rögzített, minősített időszakot jelent, amely esetben a védekezés költségét állami forrásból biztosítják, s az általános közigazgatási rendszertől eltérő, akár szigorúbb jogszabályok léphetnek életbe.

Ha a magyarországi szabályozást vesszük alapul, akkor a katasztrófavédelem mind az Alaptörvényben, mind külön jogszabályban meghatározott joga és kötelezettsége az állampolgároknak. Ahogy Az Alaptörvény[209] XXXI. cikk (5). bekezdése fogalmaz: *„Magyarországi lakóhellyel rendelkező, nagykorú magyar állampolgárok számára honvédelmi és katasztrófavédelmi feladatok ellátása érdekében – sarkalatos törvényben meghatározottak szerint – polgári védelmi kötelezettség írható elő.”*, illetve (6). bekezdése szerint: *„Honvédelmi és katasztrófavédelmi feladatok ellátása érdekében – sarkalatos törvényben meghatározottak szerint – mindenki gazdasági és anyagi szolgáltatás teljesítésére kötelezhető.”*. Erre épül a 2011. évi CXXVIII törvény[210] 1. § (2) bekezdése is, amely kimondja: *„Minden állampolgárnak, illetve személynek joga van arra, hogy megismerje a környezetében lévő katasztrófaveszélyt, elsajátítsa az irányadó védekezési szabályokat, továbbá joga és kötelessége, hogy közreműködjön a katasztrófavédelemben”*.

A katasztrófák elleni védekezés azonban elképesztően komplex feladatok végrehajtását követeli meg, amelynek során az állami, civil résztvevőknek szorosan együtt kell működni. A jegyző és a polgármester védelmi igazga-

[209] Magyarország Alaptörvénye. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100425.ATV (Letöltés ideje: 2017. augusztus 8.).

[210] 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100128.TV (Letöltés ideje: 2017. augusztus 8.).

tással kapcsolatos feladatait a honvédelmi törvény[211] és kapcsolódó rendeletei határozzák meg. A katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról szóló 234/2011 (XI.10.) Korm. rendelet 76. §-a[212] alapján a katasztrófavédelmi felkészítés célja a közbiztonsági referensek felkészítése a polgármesterek katasztrófák elleni védekezési feladatainak segítése érdekében. A polgármesterek normál időszakban az illetékességi területén irányítják és szervezik a felkészülés és a védekezés feladatait, illetve a polgári védelmi feladatok végrehajtását[213]. Az árvizeket leszámítva, ha olyan káresemény következik be, amit helyi szinten képesek kezelni, akkor megalakul a Helyi Védelmi Bizottság, amelynek a polgármester az elnöke. Amennyiben több település érintett a káreseményben, úgy Megyei Védelmi Bizottság alakul.

A 2010-es árvíz és kolontári baleset hatására felülvizsgálatra került a települések polgári védelmi besorolása. Míg korábban inkább katonai szemlélet volt a besorolás alapja – például határ menti települések magasabb kategóriába kerültek –, most már a természeti adottságokat és katasztrófavédelmi (lakosságvédelmi) szempontokat veszik figyelembe (például veszélyes üzemek, nukleáris létesítmény, utak, csomópontok, árvízi öblözet, népsűrűség. A 2011. évi CXXVIII. törvény rendelkezése alapján az eddigi 4 helyett mára 3 kategória került meghatározásra. Tovább bonyolítja a védelmi igazgatás rendszerét a 2013. január 1-től bevezetett járási rendszer.

Rendkívüli esemény azonban nem csak ember vagy természet okozta katasztrófa lehet, egy terrorcselekmény is ebbe a kategóriába tartozik.

A közösségi média mint a rendkívüli események elleni védekezés eszköze nem újdonság, már 2011-ben is vizsgálták tudományos szempontból. Az Amerikai Tudósok Szövetsége[214] a „Social Media and Disasters: Current Uses, Future Options"[215] című kiadványában[216] azt vizsgálta, hogyan használható fel a közösségi média vészhelyzetekben. A jelentés négy területet határozott meg a felhasználást illetően:

- a kríziskommunikáció eszközét;
- a segélykérés eszközét;
- a felhasználói aktivitás monitorozásának eszközét, ami erősítheti a védekezés tudatosságát;
- a fényképek feltöltését a kárbecslés eszközeként.

211 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100113.TV (Letöltés ideje: 2017. augusztus 8.).

212 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról. URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1100234.kor (Letöltés ideje: 2017. augusztus 8.)

213 HORNYACSEK et al. (2010): Önkormányzati vezetők felkészítése a védelmi igazgatási feladatokra. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest.

214 The Federation of American Scientist. URL: http://www.fas.org/

215 Közösségi média és katasztrófák: felhasználható területek a jelenben és a jövőben (a szerző fordítása).

216 LINDSAY, Bruce R. (2011): Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Congressional Research Report. In: The Federation of American Scientist, 2011. szeptember 6. URL: http://www.fas.org/sgp/crs/homesec/R41987.pdf (Letöltés ideje: 2017. augusztus 15.)

A lista azonban hiányos, ugyanis a lakosságfelkészítés – megítélésem szerint – rendkívül fontos, amiben szintén komoly hatása van a közösségi médiának.

Onnantól, hogy a jogszabály a katasztrófák elleni védekezést kötelezettségként fogalmazza meg, és ahhoz, hogy ezt az állampolgárok hatékonyan el tudják látni, szükséges, hogy tisztában legyenek a védekezés elveivel, eljárásaival, eszközeivel. Ez egyben a lakosságfelkészítés kiinduló tétele. Ez azonban összetett feladatot jelent, hiszen a lakosságfelkészítésnek eltérőnek kell lennie, többek között korcsoport, lakóhely, érintettség szempontjából. Szintén eltérő stratégiákra van szükség az egyes speciális jellemzők okán: legyen szó árvízi érintettségről, atomerőmű környékéről, hegyvidékről. A lakosság felkészítésének kettős értelme van: egyrészt felkészíteni az állampolgárokat a rendkívüli események elleni védekezésre, kötelességeikre általános eljárásai, másrészt pedig a közelgő rendkívüli eseményre aktualizált felkészítésre (például egy közeledő hurrikán várhatóan hol fog átvonulni, hol találhatóak menedékhelyek, milyen óvintézkedéseket szükséges megtenni, stb).

Tekintsük át, hogyan használhatjuk a közösségi médiát a lakosságfelkészítés során. Fel kell, ismernünk, hogy a minél eredményesebb munkavégzés érdekében célszerű kombinálni a különböző eszközöket.

Először a videómegosztó oldalakat kell említeni, amelyek kiváló terepet biztosítanak a különböző oktatóvideóknak, specializáltan a különböző célcsoportok számára. Ahogy a statisztikákból látható volt, a YouTube tekinthető a legjelentősebb videómegosztó oldalnak, így megkerülhetetlen. A Facebook is igyekszik méltó konkurenssé válni, rengeteg energiát fektet abba, hogy ne csak a képmegosztás tekintetében legyen az egyik legjelentősebb piaci szereplő, hanem az oldalra feltöltött videók szempontjából is. Szintén hasznosak a blogok, ahol részletesebben, akár videókat beágyazva lehet végezni ezt a feladatot. A közösségi média egyik előnye a felhasználói interakció, így kialakulhat párbeszéd az olvasók között, amely a tapasztalatcsere során még hatékonyabbá teheti a munkát. Természetesen elengedhetetlen, hogy az oldal üzemeltetői is reagáljanak a felhasználók kérdéseire.

Egy bekövetkezett esemény során azonban talán még inkább felértékelődnek ezek az oldalak, hiszen a helyzetnek megfelelően lehet aktuális információkkal ellátni a lakosságot, ami egyúttal fontos szerepet játszanak a lakosság megnyugtatásában, illetve erősíti a bizalmat a rendkívüli események felszámolásáért felelős szervezetek irányában, aminek nagy lélektani jelentősége van. A YouTube-on és a Facebookon egyaránt lehetőség van élő videós közvetítés indítására, így nem szükséges a tájékoztatásra különböző technikai eszközöket vinni, csak megfelelő mobilinternet-hozzáférés szükséges.[217]

Szintén fontos a Twitter és Facebook az információk megosztásában. A hashtaggel ellátott bejegyzések segítenek egy csokorba gyűjteni az azonos tartalmú posztokat. 2012 októberében, amikor a Sandy hurrikán végigsöpört az amerikai kontinensen, az amerikai hatóságok példamutatóan használták a közösségi oldalakat. Twitteren több mint 20 millió tweetet küldek #sandy hashtaggel. Emellett a Vöröskereszt, a FEMA[218], a New York-i polgármesteri hivatal és a Maryland Emergency Management Agency számára ingyenessé tette az egyébként fizetős, kiemelt tweeteket[219], hogy a közérdekű információk minél szélesebb körhöz jussanak el.[220]

[217] Ezt természetesen nehezítheti a hálózat leterheltsége.

[218] Federal Emergency Management Agency.

[219] Hurricane Sandy: Resources on Twitter. In: Twitter blog, 2012. október 29. URL: http://blog.twitter.com/2012/10/hurricane-sandy-resources-on-twitter.html (Letöltés ideje: 2017. augusztus 15.).

[220] Ezenfelül arra bíztatta az érdekelt helyi szervezeteket, hogy csatlakozzanak a fenti kezdeményezéshez.

A kríziskommunikáció során szempontnak kell lennie, ha a lakosság több nyelven beszél, akkor a közzétett információk ennek megfelelően szintén többnyelvűek legyenek.

Fontos azonban látni, ha nagyszámú tartalom keletkezik, azok között könnyen elterjedhetnek hoaxok, álhírek, így elengedhetetlen, hogy a hivatalos kommunikáció validált legyen. A felkészítés során fel kell hívni a figyelmet arra is, hogy csak a megerősített, hivatalos szervek által hitelesített információkat tekintsék irányadónak. Egy álhír hatására kialakult pánik óriási károkat képes okozni.

A nem ellenőrzött információknak egy másik aspektusát jelenti, amikor például egy terrortámadást követően az elkövetők utáni hajszában (például 2012-ben a bostoni merényletet követően, vagy 2015-ben a Chalie Hebdo szerkesztősége ellen elkövetett merénylet során)[221] az állampolgárok megosztják a rendőri erők pozícióját, hol zajlik razzia, stb. Ezzel olyan információk birtokába juthatnak az elkövetők, amellyel nagyobb eséllyel lesznek képesek elkerülni a letartóztatást.

> Rendkívül izgalmas kérdés, hogy egy terrortámadás után szükséges-e, egyáltalán lehet-e cenzúrázni a médiát. A terrorszervezetek célja, hogy akcióikkal minél nagyobb nyilvánosságot érjenek el, ezzel növelve a szervezet ismertségét, erősítve propagandatevékenységüket. Így akarva-akaratlanul a média szenzációhajhász viselkedése sokszor a terrorszervezeteknek megteszti ezt a szívességet. Több esetben felmerült, hogy a nagy híroldalak csupán a terrortámadás megtörténtéről számolnak be, minden egyéb információt elhallgatnak (ki vállalt felelős, mi a célja, stb.), de a közösségi média korában kérdéses, mennyire érvényesíthető az öncenzúra. Bárki feltölthet képeket, videókat, amik a különböző közösségi oldalakon rendkívül gyorsan jutnak el nagy tömegekhez.

Az információmegosztás, tájékozódás mellett fontos szerepük lehet a közösségi oldalaknak a segítségkérésben is. A Sandy hurrikán idején a 911-es segélyhívóvonal annyira túlterhelt volt,[222] hogy időnként elérhetetlenné vált, így sokan Twitteren, Facebookon kértek segítséget. A Facebook a terrortámadások, katasztrófák esetében egy lokalizált szolgáltatást vezetett be Safety Check néven 2014-ben, aminek a lényege, hogy katasztrófa vagy terrortámadás sújtotta helyeken a Facebook-alkalmazás egy üzenetben megkérdezi a közelben tartózkodó felhasználókat, hogy jól vannak-e. Amennyiben a válasz igen, ezt megosztja a hírfolyamban, hogy ezzel is megnyugtassa az ismerősöket. Az alkalmazás először 2015-ben, a nepáli földrengés során volt aktív. Jelenleg azonban nem lehet ezen keresztül segítséget kérni, ha valaki nemleges választ adna meg.

Végezetül a kárfelszámolást kell megemlítenünk, ugyanis számos közösségi finanszírozású projektet lehet kezdeményezni, amely az adománygyűjtés mellett akár összeköthetni azokat az embereket, akik fizikailag segítenének a károk enyhítésében.

[221] E két esetről a későbbiekben bővebben is szó esik.

[222] Manhattanben egy átlagos napon 1000 hívás érkezik, ez idő alatt óránként 10000 hívást regisztráltak.

Fontosabb fogalmak

Dezinformáció, honvédelmi kötelezettség, infokommunikációs technológiák, katasztrófavédelem, katasztrófavédelmi felkészítés, kárfelszámolás, kríziskommunikáció, lakosságfelkészítés, rendkívüli esemény, segélykérés, védelmi bizottság, védelmi igazgatás, vészhelyzet.

Áttekintő kérdések

1. Ön szerint milyen célból érdemes használni elsősorban az önkormányzatoknak a közösségi médiát?
2. Ön szerint mennyire használható a közösségi média az állampolgárok politikai döntéshozatalába történő bevonásában?
3. Ön milyen oktatást tartana a közösségi médiát felhasználva a rendkívüli eseményekre való felkészítésben?
4. Ön szerint korlátozható a közösségi média rendkívüli események (például terrortámadás) idején?
5. Véleménye szerint napjainkban mi a legnagyobb kiberfenyegetettség, ami az állami rendszereket érintheti?
6. Véleménye szerint a közigazgatásban dolgozók, még ha nem is foglalkoznak minősített adatokkal, kitettebbek-e más országok nemzetbiztonsági szolgálatainak támadásaival szemben?

7. A KÖZÖSSÉGI MÉDIA ÉS A POLITIKAI ALRENDSZER

Carl von Clausewitztől származik a mondás, mely szerint *„a háború a politika folytatása más módszerekkel”*. A tankönyvben bőségesen foglalkoztunk olyan eljárásokkal, amelyek a kiberhadviselés körébe tartoznak, de mint azok esetében is láttuk, a kibertér katonai célú felhasználása a politikai döntéshozatal befolyására törekedett. E fejezetben néhány esettel illusztráljuk, hogyan is függ össze a közösségi média a politikai alrendszerrel.

2011 februárjában a bostoni Raw Story felfedezte az US Air Force „online identitásmenedzselő szoftverre” kiírt pályázatát.[223] A kiírás gyakorlatilag egy olyan botnethálózatra vonatkozott, amelyben közösségi oldalakra regisztrált álprofilokat lehetett irányítani, hogy az adott műveleti területen ezeket politikai döntéshozatal befolyásolására, szélsőséges esetben kormányváltásra is felhasználhassák. Értelemszerűen a szoftvernek képesnek kellett lennie arra, hogy az adott műveleti területre érvényes legendával ruházza fel az álprofilokat is, illetve virtuális magánhálózat segítségével a megfelelő helyre lokalizálja őket. Elvégre egy Közel-Keleten használni szándékozott botnethálózat esetében meglehetősen érdekes lenne, ha a profilok egyébként székely identitásúak lennének, valamint geolokációs helymeghatározás Coloradoba, az US Air Force Akadémiájához vezet.

Nem tudni, hogy korábban használtak-e effélét, mindenesetre a következő években több esetben láttak napvilágot több százezres álprofilt működtető botnethálózatok. Időközben az is ismertté vált, hogy hasonló botnethálózatokat alkalmaznak álhírek terjesztésére, hogy azáltal befolyásoljanak választási küzdelmeket. E fejezetben a lényeges eseteket tekintjük át, amelyek esetében a közösségi médiát a politika befolyásolására használták.

7.1. „ARAB TAVASZ”

Az „Arab tavasz” néven elhíresült eseménysor 2010. év végén vette kezdetét Tunéziában, amikor egy zöldségárus öngyilkosságot követett el; halála a munkanélküliség és a drágaság elleni tiltakozó mozgalmat indított el. A felkelés nyomására 2011. január 14-én a több mint 20 éve hatalmon lévő Zin el-Abidin ben Ali tunéziai elnök lemondott. A tunéziai események azonban továbbgyűrűztek a Közel-Kelet több országára is.

Egyiptomban 2011. január 25-én tüntetések kezdődtek az 1981 óta hatalmon lévő Hoszni Mubarak államfő rendszere ellen, amelyek több mint 800 halálos áldozattal járó zavargásokba torkolltak. Február 11-én a szűnni nem akaró tüntetések, megmozdulások hatására Mubarak elnök lemondott, és 2012-ben életfogytiglani börtön-

[223] Webster, Stephen C. (2011): Revealed: Air Force ordered software to manage army of fake virtual people. In: The Raw Story, 2011. február 18. URL: http://www.rawstory.com/rs/2011/02/18/revealed-air-force-ordered-software-to-manage-army-of-fake-virtual-people/ (Letöltés ideje: 2018. január 20.)

büntetésre ítélték. Mubarakot 2012-ben Mohamed Murszi, a Muzulmán Testvériségből alakult párt, a Szabadság és Igazságosság Pártja vezetője váltotta, aki 2014-ben végül lemondani kényszerült. A választásokon ezután Abdel-Fatták esz-Szíszi volt hadseregparancsnok, védelmi miniszter szerezte meg a legtöbb szavazatot, aki végül kormányt alakított, és 2016-ra sikerült stabilizálnia a hatalmát. A 2018-ban esedékes elnökválasztás demokratikussága kétségessé vált, ugyanis a Szíszi ellen induló elnökjelöltek az utolsó percben rejtélyes körülmények között visszaléptek.

Líbiában 2011 februárjában népfelkelés kezdődött az 1969 óta hatalmon lévő Moammer Kadhafi ezredes ellen. Kadhafit 2011. októberében megölték, ám halála óta sem sikerült stabilizálni az ország biztonsági és belpolitikai helyzetét.

Szíriában a 2007-ben újraválasztott Bassár el-Aszad elnök uralma ellen 2011. márciusában kezdődtek békés tüntetések, amelyek a véres megtorlások hatására polgárháborúba torkolltak. A polgárháború egy rendkívül összetett globális, regionális és lokális konfliktussá változott, törékeny szövetségi rendszerek tömkelegét kialakítva. 2018-ban a polgárháború továbbra is zajlik; e fejezet írásának idején[224] jelenleg Törökország a szíriai kurdok ellen indított katonai műveleteket.

Marokkóba is – bár politikailag viszonylag stabil ország volt szabadon választott parlamenttel és többpártrendszerrel – begyűrűztek az„Arab tavasz" eseményei. 2011 elején tüntetések robbantak ki, a tiltakozók jobban működő demokráciát és nagyobb társadalmi egyenlőséget követeltek. Végül alkotmányreform, előre hozott választások és a szegénység leküzdésére tett intézkedések ígéretével sikerült elejét venni, hogy fegyveres erőszak eszkalálódjon az országban.

A többnyire szunniták lakta Szaúd-Arábiában minimális volt a térségben kialakult események hatása, ezek többsége inkább az olajban gazdag, síiták lakta keleti tartományokra korlátozódott.

Jemenben 2011 novemberében felkelések robbantak ki, amelyek 2014-re polgárháborúvá szélesedtek, amely 2018-ra még mindig nem rendeződött teljes egészében.

Bahrein, Jordánia és Kuvait szintén felkelésekkel nézett szembe, de ezeken a területeken sikerült stabilizálni a tüntetéseket.

Miért érdekes ez esetünkben? A tüntetéseket eredetileg Tunéziában szervezték közösségi oldalakon keresztül. Ezeknek pedig a többi országban is jelentős szerepük volt. A kezdeti békés tüntetésekre a kormányzatok erőt mutatva reagáltak, ami a térségben nem meglepő. A brutális fellépés képei, az azokról készült videók azonban a tüntetők zsebében rejlő okostelefonoknak köszönhetően ellepték a közösségi oldalakat, amik hamar átkerültek a mainstream médiába, kiszélesítve az érintett lakosság körében a felháborodást, és növelve a tüntetők számát, valamint ráirányítva a nemzetközi közvélemény figyelmét a történésekre. A mobiltelefon és internet elterjedése előtt is szerveztek az emberek politikai mozgalmakat, tüntetéseket, de a közösségi média új dimenziót nyitott meg, aminek oka az országok demográfiai adataiból kimutathatók, hiszen a régió egyik legerősebb feszültségforrását a nagyszámú fiatalokból eredeztetik. Ezek a fiatalok pedig már készségszinten használják az internetet. [225]

[224] 2018. év eleje.

[225] Ahogy Selján Péter tanulmányából kitűnik: *„Tunéziában, ahol az átlag életkor 30 év, a 10 milliós lakosságnak közel 23%-a 14 éven aluli. Egyiptomban, ahol az átlag életkor 24 év, az ország 83 milliós lakosságának 33 százaléka fiatalabb 14 évesnél. A mobiltelefonok mindkét ország-*

A nemzetközi közvélemény figyelme és az ezzel kapcsolatos felháborodás több ország életében hozott változásokat. Egyiptomban például az amerikai kormányzat által támogatott Mubarak végül az amerikaiak közrejátszásának hatására mondott le, de Líbiában is Franciaország hatékony közreműködése vezetett Kadhafi bukásához.

Játsszunk el a gondolattal, ha az US Air Force által kiírt „online identitásmenedzselő szoftver" létezett volna az „Arab tavasz" előtt, és egy ország saját érdekeinek megfelelően alkalmazta volna, hogy a térségben politikai változások menjenek végbe, milyen forgatókönyvet lehetne megállapítani.

A botnethálózat megléte esetén az első lépés, hogy megvárjuk, míg tüntetések törnek ki, vagy szükség estén megteremtik a feltételeit egy olyan eseménynek, amire válaszul el lehet indítani a műveletet. A történelem bebizonyította, hogy az egyes hírszerző szervezetek nagyon kreatívak tudnak lenni, ha „black ops"-ról van szó.[226]

Hogyan működik egy ilyen tiltakozás megszervezése? Először is kell valaki, aki létrehoz egy csoportot/rajongói oldalt/eseményt az adott témában. Esetünkben, mondjuk, egy tüntetést a korrupció ellen, vagy politikai szabadságjogok biztosítása érdekében. Ezt követően minél több emberhez kell eljuttatni az értesítést. Minél többen jelezték vissza a támogatást, annál nagyobb súlyt jelenthet. Nemcsak hogy fel lehet mutatni ezt a bizonyos támogatottságot, hanem további konspirációs tevékenységgel szélesebb publicitást lehet az adott agendának biztosítani. A botnethálózatok, a közösség oldalak működései a fizetett hirdetésekkel, az egyénre szabott targetálási lehetőségek, a „Filter Bubble"-jelenség hatására nagy arányban lehet terjeszteni ezeket az eseményeket, híreket anélkül, hogy a valójában mögötte álló szervezet dekonspirálódna. Több állam működtet úgynevezett „trollhadseregeket", amelyek feladata, hogy az adott tematika mentén meghatározott számú kommentet, bejegyzést hozzon létre különböző profilok segítségével – erről az Oroszországról szóló részben bővebben lesz szó.

Az elektronikus és a hagyományos média is előszeretettel hivatkozik a közösségi eszközökre, sokszor abból véve át a tudósításokhoz képeket, videókat vagy akár kommenteket, tweeteket. Ennek egyik legfőbb oka, hogy a közösségi oldalakon a kommunikáció „real time", azaz azonnali időben folyik. Ezzel a képességgel az elektronikus híroldalak még csak-csak versenyezhetnek, de a hagyományos médiának esélye sincs. Ami a közösségi média erejét növeli, az a nagyszámú résztvevő, aki az események átélésekor elvben azonnal tudósíthat[227]. Ha azonban rendel-

ban elterjedtek, Tunéziában minden 100 emberre jut 93 mobiltelefon előfizetés, míg Egyiptomban 100 emberből 67 rendelkezik mobiltelefonnal. Mindezek mellett ráadásul a kormány cenzúrázta a médiát, ami arra késztette az embereket, hogy az Interneten keresztül próbáljanak meg tájékozódnia az eseményekről. Az Internethasználat szintén jelentős mindkét országban: Tunéziában a lakosság 25 százaléka, Egyiptomban pedig 10 százaléka használta már az Internetet. Az Internethasználóknak ráadásul több mint a fele 34 évesnél fiatalabb." Bővebben lásd: Selján Péter: A közösségi média szerepe a 21. században, avagy az „arab tavasz" és a közösségi oldalak. In: Biztonságpolitika.hu, 2011. december 9. URL: http://old.biztonsagpolitika.hu/index.php?&id=16&aid=1137&title=a-kozossegi-media-szerepe-a-21-szazadban-avagy-az-arab-tavasz-es-a-kozossegi-oldalak&load=ZVD6ci0SpPs (Letöltés ideje: 2018. január 27.)

226 A „black operation", azaz fekete művelet alatt olyan eseményeket értünk, amelyek túllépnek a törvényesen végrehajtható műveletek keretén. Például, amikor az amerikai ATF (Bureau of Alcohol, Tobacco and Firearms, azaz az Alkohol- és Dohánytermékek, illetve Lőfegyverek Forgalmával Foglalkozó Iroda, szövetségi rendőri szerv) a mexikói fegyvercsempész-útvonalak feltérképezése érdekében különböző csatornákon keresztül automata fegyvereket juttatott a drogkartellek kezébe. Egy ilyen műveletről az esetek nagy részében természetesen csak akkor értesülünk, ha kudarcba fulladnak, és botrány kerekedik belőle, mint ahogy a példaként említett esetben is történt.

227 Ahogy meg is tette ezt egy pakisztáni lakos, aki nem tudván a valós okot, de Twitteren élőben közvetítette Oszama Bin Laden elfogására tett

kezünk egy nagyszámú mesterséges felhasználó tömeggel, nem szükséges a véletlenre bíznunk a támogatottság nagyságának bemutatását. Természetesen egy ilyen esetben a támogatottság nem az adott ország médiáján keresztül jelenik meg elsősorban, hiszen a diktatórikus államberendezkedések esetében a média erős állami kontroll alatt áll; a művelet célja a globális közvélemény figyelmének felhívása és befolyásolása.

A Közel-Keleten végbement változások feltehetően nem ilyenfajta módon szerveződtek meg, vagy ha volt is külső behatás, a műveleti tervezők vélhetően nem számoltak ekkora „spill over"-hatással,[228] hiszen az események alapjaiban változtatták meg a nagyhatalmak érdekszféráját, valamint a globális biztonságot, amit összességében esetükben is a biztonság csökkenéséhez vezetett. Azonban fontos látni, és a következő alfejezetek is alátámasztják, a politikai döntések befolyásolására számos eszköz áll rendelkezésre, amellyel az egyes államok és nemzetbiztonsági szolgálataik aktívan élnek.

7.2. OROSZORSZÁGBÓL SZERETETTEL

Oroszországot rendszeresen éri az a vád, hogy a kiberteret, azon belül a közösségi médiát aktívan alkalmazza idegen államok belpolitikai döntéshozatalának befolyásolására. A legnagyobb visszhangot a 2016-os amerikai elnökválasztásban feltételezhető szerepe váltotta ki. Mindez nem előzmények nélküli.

Az orosz kormányzat a 2000-es évek közepén kezdett gyümölcsöző kapcsolatokat kialakítani az európai szélsőjobboldali pártokkal, alapvetően hármas cél megvalósítása érdekében:

- az Európai Unió, annak tagállamai és azok transzatlanti kapcsolatainak destabilizálása;
- az orosz kormány és pozíciójának destabilizálása;
- információszerzés és dezinformálás. [229]

Ezek a pártok több esetben támogatták Oroszországot a számára geopolitikailag fontos területeken.[230] Azonban nem csak az egykori szovjet érdekszférába tartozó szélsőjobboldali pártokra jellemző az oroszorientáltság, a francia Nemzeti Frontot 2015-ben az a vád érte, hogy 9 millió eurós bankkölcsönnel vásárolták meg a párt támogatását, hogy legitimáljak Oroszország krími beavatkozását.[231] 2016-ban az amerikai kongresszus megbízta James Clappert, a Nemzeti Hírszerzés Igazgatóját, [232] vizsgálja ki, nyújtott-e Oroszország titkos pénzügyi támogatást európai pártok-

kísérletet.

228 A „spill over"-hatás lényege, hogy egy alrendszerben történt változás idővel más alrendszerekre is hatással van, „átcsordul" a következménye. Például a gazdasági integráció idővel a politikai integrációt is magával vonja.

229 Juhász Attila et al. (2015): „Eurázsiai vagyok"- A magyar szélsőjobboldal kapcsolata a Kremllel, In: Political Capital, 2015. március. URL: http://www.politicalcapital.hu/wp-content/uploads/PC_SDI_Boll_tanulmany_EurazsiaiVagyok.pdf (Letöltés ideje: 2018. január 23.).

230 Például a 2008-as orosz–grúz konfliktus megítéléséről vagy orosz gázvezetéktervekről. Bővebben lásd: Oroszbarátok a jobbszélen. Gondola, 2009. december 1. URL: http://gondola.hu/cikkek/68518 (Letöltés ideje: 2018. január 21.)

231 Chazan, David (2015): Russia ‚bought' Marine Le Pen's support over Crimea. In: The Telegraph, 2015. április 4. URL: http://www.telegraph.co.uk/news/worldnews/europe/france/11515835/Russia-bought-Marine-Le-Pens-support-over-Crimea.html (Letöltés ideje: 2018. január.23.)

232 Foster, Peter (2016): Russia accused of clandestine funding of European parties as US conducts major review of Vladimir Putin's strategy. In: The Telegraph, 2016. január 16. URL: http://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html (Letöl-

nak, hogy felhasználva az EU-ban tapasztalható széthúzást, rajtuk keresztül gyengítse a NATO-t, megakadályozza az amerikai rakétavédelmi programot, illetve a Krím-félsziget annektálását követően bevezetett gazdasági szankciókat visszavonják. [233] Ennek megfelelően a szélsőjobboldali honlapokon, közösségi oldalakon gyakori volt az Oroszországgal kapcsolatos pozitív hírek, vélemények megjelenése, amiben Vlagyimir Putyin elnök a hanyatló, dekadens nyugat egyetlen védelmezőjeként tűnt fel, szemben a korrupt, globális érdekeket kiszolgáló NATO-val, EU-val.

E tekintetben az áttörést a 2013. év végi ukrajnai konfliktus jelentette, amely jelentősen felerősítette az orosz lélektani műveleteket, amelyek során a közösségi média volt az egyik fő csatorna. Az orosz–ukrán háborút a hibrid hadviseléssel szokták jellemezni. 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 folytatathat »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."*[234] Ebben a hadviselési módban a közösségi média megkerülhetetlen, hiszen az álhírekkel kapcsolatos lélektani műveletek igen hatásosak az állami hivatalos narratívákkal szembeni bizalmatlanság fokozására, dezintegrációra.

Ami az „Arab tavasz" esetében lehetséges forgatókönyvként szerepelt, nevezetesen, hogyan lehet egy közösségi médiában megjelenő tartalomnak globális figyelmet biztosítani, 2014-ben Magyarország megtapasztalta. A Hídfő.net nevű, a Magyar Nemzeti Arcvonalhoz köthető szinte ismeretlen internetes portálon megjelent egy hír, amely szerint Magyarország T-72-es harckocsikat szállít Ukrajnának, megszegve az európai uniós fegyverexport-tilalmat. Később kiderült, hogy az adott hír az orosz nemzetbiztonsági szolgálatok közreműködésével jelent meg. A Hídfő.net olvasottsága nem volt jelentős, ennek ellenére valahogy „véletlenül" az orosz Külügyminisztérium is olvasta, amely hivatalosan is tiltakozott a magyar kormánynál. Természetesen a diplomáciai jegyzék hamar nemzetközi figyelmet kapott, és a globális közvélemény ezzel foglalkozott.

Először Oroszország esetében vált ismertté, de később például Kína esetében is napvilágot látott, hogy nagyszámú „trollhadsereget" tart fent a lélektani műveleteinek végzésére.[235] Nagy-Britannia például dandárszintű egységet hozott létre 77-es dandár néven.[236] Az 1500 főt számláló egység deklarált célja a közösségi médián folytatott lélektani műveletek végzése.

Egykori tagok beszámolói alapján ezek a műveletek szigorúan szabályozott keretek között működnek.[237]

TÉS IDEJE: 2018. JANUÁR 23.)

233 A cikk a magyarországi Jobbikot, a francia Nemzeti Frontot, a görög Arany Hajnalt, illetve az olasz Északi Ligát nevesíti.

234 HOFFMAN, FRANK G. (2007): CONFLICT IN THE 21ST CENTURY: THE RISE OF HYBRID WARS. POTOMAC INSTITUTE FOR POLICY STUDIES, VIRGINIA. P. 8.

235 Ne legyen illúziónk, az Egyesült Államok és más nyugati országok is élnek ezzel az eszközzel.

236 Macaskill, Ewan (2015): British army creates team of Facebook warriors. In: The Guardian, 2015. január 31. URL: http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade (Letöltés ideje: 2018. január 24.)

237 Walker, Shaun (2015): Salutin' Putin: inside a Russian troll house. In: The Guardian, 2015. április 2. URL: http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house (Letöltés ideje: 2018. január 24.)

A Szentpéterváron található Internet Research Agency nevű online kutatással foglalkozó cégnél ezen beszámolók szerint váltott műszakban,[238] hármas csoportokban[239] eltérő bérkategóriába[240] sorolva dolgoznak, becslések szerint ezren, hogy nyugatellenes, Kreml-barát híreket osszanak meg hazai és külföldi portálokon.[241] A témákat az adott nap elején jelölik ki, és meghatározott számú kommentet[242] kell meghatározott számú profillal elhelyezni. Ezeket nagyban meghatározzák az aktuális kül- és belpolitikai történések.[243]

Egy, az amerikai nemzetbiztonsági szolgálatok által nyilvánosságra hozott jelentés több szereplőt nevesít, akik aktív közreműködői az orosz lélektani műveleteknek. Edward M. Roche látványosan foglalta össze ezeket az aktorokat, akik között hírszerző szolgálatokat, hackereket, illetve a propagandáért felelős szervezeteket egyaránt találunk (lásd 9. számú ábra). Ez alapján három részre oszthatjuk a szereplőket: a pirossal jelölt, propagandában érintetteket, idesorolva 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, ideértve többek között a WikiLeakset vagy a katonai hírszerzést; sötétebb kékkel jelölve a hírszerző szolgálatokat. Az ábrán sárgával látható az egyes szereplők hatása a közösségi oldalakon, illetve a hírodalakon.

238 Helyiségenként hozzávetőlegesen 20 fő dolgozott 3 szerkesztő alá sorolva.

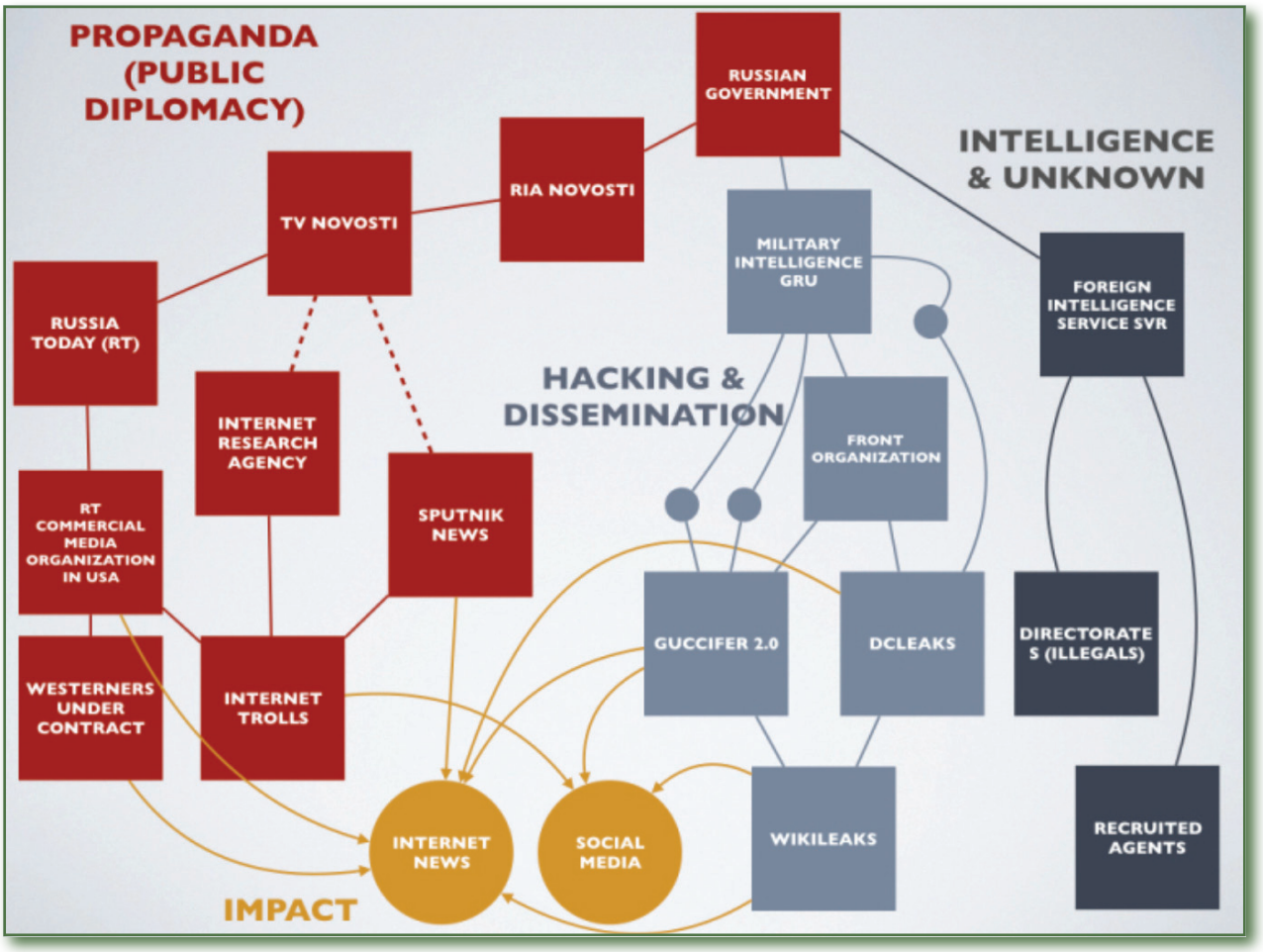
239 Ebből volt egy témafelvető, akihez később csatlakoztak a többiek, vitát generálva, megerősítve a hírt, stb.

240 2015-ben ez 45 ezer rubelnek (219 ezer forintnak) megfelelő havi bérezést, angol nyelvű kommentek esetében 65 ezer rubelt (316 ezer forint) jelentett.

241 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.

242 12 órás műszakban 135 kommentet.

243 Gondoljunk csak a Törökország által 2015 novemberében lelőtt orosz vadászgép esetére, vagy a szilveszteri kölni zaklatások után az orosz média által hangoztatott 13 éves orosz kislány tömeges megerőszakolására.



9. ábra: Az orosz lélektani műveletek szereplői

Forrás: cyberarmscontrolblog[244]

Vádak szerint az orosz lélektani műveletek igen komoly hatást gyakoroltak az európai migrációs válság kezelésére, a 2016-os angliai népszavazás, valamint amerikai elnökválasztás során (az utóbbi két eseményről a következő alfejezetben lesz szó).

[244] Roche, Edward M. (2017): Comments on "Assessing Russian Activities and Intentions in Recent US Elections". In: Cyberarmscontrolblog, 2017. január 8. URL: https://cyberarmscontrolblog.com/2017/01/08/comments-on-assessing-russian-activities-and-intentions-in-recent-us-elections/ (Letöltés ideje: 2018. január 24.)

7.3. BREXIT ÉS TRUMP

A kiberbűnözés és Big Data kapcsán már volt szó a Cambride Analytica nevű cégről, amelynek jelentős szerepet tulajdonítanak e két esemény politikai kampányában. Természetesen összességében vizsgálva ezek csak egy-egy részét adták a végső eseményeknek, így hibás következtetés teljes egészében ezzel indokolni a történteket. Már csak azért is, mert ezek hatására olyan politikai és szolgáltatói döntések születtek, amelyek igen komoly hatást fognak gyakorolni a jövőnkre.

Nagy-Britannia és az Európai Unió viszonya mindig is különleges volt. Eleve már az EU-ba történő belépés sem ment egyszerűen, de a pár évtizedes tagság is a különutasság jegyében telt. A terjedelmi korlátok nem teszik lehetővé, hogy a BREXIT körülményeivel foglalkozzunk, csupán arra szükséges felhívni a figyelmet ezzel kapcsolatban, hogy a vádak szerint a kilépéspártiak győzelme mellett Oroszország érintettsége is jelentős volt. Theresa May brit miniszterelnök 2017 novemberében vádolta meg Oroszországot, hogy aktív lélektani műveleteket folytattak a kilépéspártiak mellett a közösségi médiában alkalmazott álhírekkel, illetve anyagi támogatásban is részesítették őket. Több kutatás mutatta ki, hogy a választást megelőző napokban orosz Twitter-fiókok különböző információkkal és álhírekkel igyekeztek társadalmi feszültségeket kelteni, alapvetően a bevándorlásellenességet felhasználva. A korábban említett brit 77-es dandárnak mindenesetre van még mit tennie a képességfejlesztés kapcsán. Ettől eltekintve látni kell, sokkal nehezebb dolguk van azoknak, akiknek védekezniük kell az ilyen irányú műveletekkel szemben, mint azoknak, akiknek végre kell azokat hajtania. Azt is fontos tisztázni, ha volt is erős befolyásolási szándék idegen államok részéről, nem tudjuk annak eredményességét, nincsenek objektív mérési adataink arról, hány esetben ez vezetett el ahhoz a döntéshez, hogy a kilépés mellett voksoljon a britek többsége.

Hangsúlyozottan igaz ez a megállapítás az amerikai elnökválasztási kampányra is. Meglehetősen szokatlan, hogy egy ország nemzetbiztonsági szolgálatai konkrétan, a nyilvánosság előtt nevesítenek egy másik országot az őket ért kibertámadás felelőseiként. A Belbiztonsági Minisztérium az FBI-jal közös, JAR-16-20296A jelzésű elemzésében már a címében is jelzi, hogy kiket tartanak felelősnek. 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."*[245]

Donald Trump elnöki kampányának sikere természetesen számos esemény összjátékának eredménye, beleértve a demokrata elnökjelölti verseny eredményét, a gazdaság polarizációját és számos egyéb társadalmi problémát, de több, a kibertérben végbement művelet is közrejátszott. A Kovács–Krasznay szerzőpáros egy rendkívül alapos kronológiai gyűjtést ad az eseményekkel kapcsolatban, ebből itt csupán néhányat szükséges kiemelni:

[245] Kovács László – Krasznay Csaba (2017): „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. Stratégiai Védelmi Kutatóközpont – Elemzések, 2017/9. pp. 1–11.

- 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.
- 2017. januárjában bár azt a tájékoztatást adják a nemzetbiztonsági szolgálatok, hogy az elektronikus választási rendszert nem sikerült kompromittálni az oroszoknak, azonban júniusban kiderült, hogy történtek kísérletek a választások közvetlen befolyásolására. Informatikai támadás ért legalább egy olyan céget, amely az elnökválasztás lebonyolításában használatos hardvereket és szoftvereket gyárt. A cégtől lopott adatokkal aztán 122 helyi választási tisztviselőt vettek célba adathalász e-mailekkel. A jelentések mindezekért az orosz katonai hírszerzést, a GRU-t nevezték meg felelősként, csakúgy, mint a DNK-t ért informatikai támadások elkövetőiként. A támadás célja az volt, hogy egy trójai alkalmazást juttassanak be a választási rendszerbe, átvéve az irányítást felette. Azt azonban nem tudni, hogy sikerrel jártak-e, és ily módon befolyásolták-e a választás kimenetelét.

Az elnökválasztási küzdelem során lezajlott célzott informatikai támadás részleteiről az idézett tanulmány részletes leírást ad, mi csupán a közösségi médiával kapcsolatos részekre szorítkozunk.

Egyik fontos eleme az eseményeknek a WikiLeaks szivárogtatásai voltak. Egy magát Guccifer 2.0-nak nevező személy vállalta magára Hillary Clinton e-mailjeinek feltörését és az így megszerzett információk átadását a WikiLeaksnek, de több jel utal arra, hogy Guccifer 2.0 valójában a Fancy Bear[246] által kreált legenda volt. Assange folyamatosan tagadta, hogy az iratokat az oroszoktól kapta volna, azonban nagyon sok jel utalt arra, hogy ez nem fedi a valóságot. A WikiLeaksen megjelent információknak volt egy érdekes hatása is: kezdetben a Facebook blokkolta a Hillary Clinton e-mailjeivel kapcsolatos megosztásokat, amik a WikiLeaksre mutattak. A Facebook természetesen tagadta, hogy ez szándékos lett volna; technikai hibával magyarázták a történteket, de ez megalapozott azoknak a vádaknak, amelyek szerint Hillary Clinton elnökjelöltségét támogatja az oldal.

A Facebook egykori dolgozói például azzal vádolták meg az oldalt, amit a kezdeti tagadás után végül a Facebook is elismert, hogy az Egyesült Államokban népszerű, úgynevezett „Trending topics"-ot valójában nem egy algoritmus állítja össze az alapján, hogy milyen tartalmakat osztanak meg a felhasználók a legnagyobb számban, hanem emberek, akik viszont szándékosan háttérbe szorították a jobboldali konzervatív tartalmakat, és a kevésbé olvasott liberális baloldali híreket sorolták ide, hogy ezzel segítsék a nagyobb olvasottságot.

Végül ezek a súlyos vádak vezettek el oda, hogy a Facebook nem mert beavatkozni az elnökválasztási kampány alatt egyre nagyobb számban terjedő álhírek megakadályozásában, ugyanis ezek 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 kö-

[246] A Fancy Bear hackercsoportot a már említett GRU-hoz kötik, ami nem összekeverendő a Cozy Bear nevű hackercsoporttal, utóbbiak ugyanis az orosz Szövetségi Biztonsági Szolgálathoz (FSZB), a KGB jogutódjához tartoznak. A Fancy Bear tehát katonai, a Cozy Bear pedig polgári kötődésű.

zel háromezer hirdetés megjelentetésére. A hirdetések nem csupán politikai tartamúak voltak. Akárcsak a BREXIT esetében, a bevándorlóellenességre építő álhírek, tartalmak jelentek meg, valamint 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. Ezenfelül 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 36 ezer automatikusan tweetelő álprofilt azonosított (emlékezzünk vissza az US Air Force pályázatára az online identitásmenedzselő szoftverére), amelyek összesen 1,4 millió bejegyzést tettek közzé a kampány során. A Google is érintett volt ez ügyben, a YouTube-ra pedig 1108 darab vonatkozó videót töltöttek fel, 43 órát kitevő tartalommal. Ezek terjesztését bizonyíthatóan 4700 dollárnyi hirdetéssel indították be.

A fizetett hirdetések mellett a Facebook egyébként más módon is profitált a kampány során. Kifejezetten olyan csomagot állítottak elő kampányszakembereknek, amelyek során azonosíthatókká váltak a politikailag legaktívabb felhasználók, ily módon pedig jobban irányíthatóvá váltak a célzott politikai reklámok. Ennek a jelentősége abban áll, hogy a felhasználók sokkal nagyobb bizalmat fektetnek az ismerőseik által megosztott tartalmakba, mint amiket hirdetésként látnak. Így tehát a pártok úgy hirdethetnek, hogy a felhasználók nem észlelik, hogy valójában politikai reklámot látnak – azt nem a megrendelő párttal azonosítják, hanem az ismerősükkel, aki megosztotta a hírfolyamában. A Facebook mint kampánycsatorna azért is kifejezetten előnyös a pártoknak, mert míg a tévés politikai hirdetések szigorúan szabályozottak, addig a közösségi médiában ezek a szabályok nem érvényesek. Így tehát nehéz megállapítani a hirdetések forrását, nehéz megmondani azt is, hogy egyáltalán mi minősül hirdetésnek, és mi nem.

A Facebooknak egyébként a fentieken felül óriási szerepe van a politikai döntéshozatal befolyásolásában. A 2010 novemberében esedékes amerikai választások alatt végeztek egy olyan kísérletet, amelynek során elhelyeztek egy Szavaztam gombot, melynek a megnyomásával a felhasználók jelezhették, hogy már voltak szavazni, és így a profilképüknél megjelent ez az információ.[247] Ezzel azt vizsgálták, kialakul-e valamilyen közösségi nyomás arra vonatkozóan, hogy akik még nem éltek a választójogukkal, azok elmenjenek szavazni. A mérések alapján, akiknek a hírfolyamában megjelent ez a jelzés, 0,39%-al nagyobb arányban mentek el szavazni, ami bár nem tűnik nagy számnak, összességében 340 ezer plusz szavazót jelentett. 2000-ben csupán 537 szavazaton múlt George W. Bush győzelme a floridai eredmények hatására. E kísérlet természetesen nem célzott manipuláció volt, nem avatkoztak bele irányítottan a választás menetébe, azonban nem nehéz belátni, hogy a Facebooknak megvan erre a lehetősége. Ismeri a felhasználók politikai preferenciáját, befolyásolni tudja, milyen tartalmak jelenjenek meg előtte, sőt, akár a felhasználók érzelmeit is képes befolyásolni. 2012-ben a Facebook egy pszichológiai kísérletet végzett[248] a

[247] Zittrain, Jonathan (2014): Facebook Could Decide an Election Without Anyone Ever Finding Out – The scary future of digital gerrymandering—and how to prevent it. In: New Republic, 2014. június 1. URL: https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering (Letöltés ideje: 2018. január 25.)

[248] A felhasználási feltételek alapján ehhez joga van.

felhasználók tudta nélkül, mintegy 700 ezer személyt bevonva. Két csoportra osztották a vizsgálandó alanyokat: az egyikben csak pozitív, a másikban csak negatív tartalmakat jelenítettek meg. Az eredmény azt mutatta, hogy azok, akik pozitív tartalmakat láttak, hajlamosak voltak pozitív tartalmakat megosztani, míg akik negatívat láttak, azok negatív tartalmakat osztottak meg.[249]

Ezen adatok felhasználásával az említett közösségi oldal képes lehet mozgósítani a felhasználókat a választáson való részvételre, akár még oly módon is, hogy kire szavazzanak. Ezt nevezik digitális gerrymanderingnek, ami a körzethatár-átrajzolás virtuális változata.

Donald Trump győzelmét követően rengeteg támadás érte a Facebookot, amiért nem tett meg mindent az álhírek visszaszorítása érdekében, ezért óriási nyomás nehezedett a vállalatra, hogy valamit lépjen ez ügyben. Persze korábban is voltak kísérletek ezzel kapcsolatban, de nem igazán voltak hatékonyak. 2015-től a felhasználók jelenthetik az álhíreket, ami kétélű fegyver, hiszen ezáltal az ellenőrzött híreket is jelenthetik. 2016-ban a kattintásvadász tartalmakat igyekeztek háttérbe szorítani egy mesterséges intelligenciával támogatott algoritmus segítségével, illetve 2016 év végén csatlakoztak a Twitterrel közösen egy, a Google által támogatott kezdeményezéshez, amelynek a célja az álhírek kiszűrése a közösségi médiából.

A kampány során nem csupán politikai céllal terjesztettek álhíreket egyes oldalak. Nem egy esetben anyagi haszonszerzés motiválta ezek üzemeltetőit, hiszen a minél nagyobb számban megosztott tartalmak növelték a weblapok hirdetési bevételeit. Egy montenegrói kisvárosban, Velesben például legalább 140 Trump-párti álhíroldalt üzemeltettek. 2017. év végén ezért mind a Facebook, mind a Google az ilyen oldalakkal szemben is harcot hirdetett azáltal, hogy az álhírterjesztő oldalként azonosított weblapoknál tiltja a hirdetési rendszer integrálását.

További kísérletként vezették be, amely jelöli a megosztott híreknél, hogy azok valószínűleg álhírek. Ezt úgy kívánták megoldani, hogy a jelentett, gyanús tartalmakat tényellenőrzésnek vetették volna alá, és amennyiben ennek az eredménye az, hogy a hír hamis, akkor ez megjelenik az oldalon. Ennek a kockázata egyrészt, hogy nehéz meghatározni a vélemény és a hír közti különbséget, hiszen a véleménynek nem kell tényszerűnek, elfogulatlannak lennie. Másrészt, ha valaki ideológiai indíttatásból hisz egy álhírnek, előfordulhat, hogy az álhírként jelölt tartalmat úgy ítéli meg, hogy az az ellentétes véleményt vallók hadjárata, amivel el akarják hallgattatni az igazságot, és ezért álhírnek hazudják.

Az álhírek elleni harcban az egyik legjelentősebb lépést Németország tette 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[250] 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 20 német jogszabály alapján nyílik mód egy bejegyzés jelentésére, beleértve az önkényuralmi jelképek tiltásáról szóló jogszabályt, az alkotmányos rend felforgatásának kísérletét

[249] Adam et al. (2014): Experimental evidence of massive-scale emotional contagion through social networks. In: PNAS, 2014., vol. 111., no. 29. URL: http://www.pnas.org/content/pnas/111/24/8788.full.pdf (Letöltés ideje:...)

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

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 nagyszámban 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" kirovásán 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 Reklámtörvény elnevezéssel, ami a közösségi média, elsősorban a Facebook politikai felelősségével foglalkozik. A jogszabály előírná, hogy:

- 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;
- 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 harc 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 nemcsak 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 nemcsak 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 nagymértékben beavatkozhat más, szuverén nemzetek életébe. Visszautalva a német szabályozásra, a közösségi oldalak egyre kevésbé lesznek érdekeltek abban, hogy a felhasználók anonim módon legyenek jelen, ez pedig az internet nagy fokú szabályozását, állami ellenőrzésének lehetőségét vetíti elő.

7.4. ISZLÁM ÁLLAM

Fontos látnunk, a „politikacsinálás" nem csak állami szereplők részéről adott. Civil szervezetek, de akár politikai elemzők ugyanúgy lehetnek a politikai tér alakítói. Hatványozottan igaz ez a terrorizmusra is, hiszen a terroristák akcióikkal politikai hatást akarnak kiváltani, legyen szó a fogyasztói társadalom kritikájáról, egy elnyomásként percepcionált élethelyzet elleni küzdelemről. Az Iszlám Állam nevű terrorista szervezet ebben a tekintetben is újat hozott, hiszen önálló államot, kalifátust alapított, amelyben teljes egészében gyakorolta az állami funkciókat.

Az Iszlám Állam az Al-Kaida egyik szárnya volt, azonban túlzott erőszakossága okán kitették onnan. Ennek ellenére néhány év alatt elérte, hogy ismertebbé, jelentősebbé váljon, mint az anyaszervezet. Ehhez persze egy évtized politikai kudarcai is szükségesek voltak, mint például a NATO és szövetségesei intervenciója 2001-ben, Szaddam Husszein iraki elnök és Moammer Kadhafi líbiai elnök megbuktatása, illetve a szíriai polgárháború kezelése.. Túlzás nélkül állítható, hogy az Iszlám Állam több tekintetben volt paradigmaváltó, többek között a közösségi média, az internet professzionális használatával.

A terrorizmus egyik „éltetője" a propaganda, amelynek segítségével felhívja a figyelmet a szervezet által képviselt célokra, éppen ezért az akciójukat úgy választják ki, hogy azzal a lehető legnagyobb médiafigyelmet váltsák ki. A közösségi média, mint láttuk, a propaganda közvetítésében kiemelt csatorna. A propaganda célja ez esetben kettős. Nem csupán a minél nagyobb hírérték segítségével növelni a szervezet elismertségét, de egyúttal az új tagok, pénzügyi támogatókat is könnyebben toboroznak maguknak, ami a működés elengedhetetlen része.

Az Iszlám Állam propagandájának első állomása maga a névválasztás volt; 2003-as megalakulásától kezdve 2014-ig, a Kalifátus kikiáltásáig.[251]

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 médiában terjesztette hashtagekkel, rengeteg felületen.

Margitics József tanulmányában kiválóan összefoglalja ezeket a felületeket:[252]

- Dzsihád Média Platform weblap, amin a regisztrált felhasználók oszthatják meg a híreket, és kommentelhetik azokat. 2015-ben a regisztrált 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 (angol, francia, német). Korán-értelmezésekkel kapcsolatos topikok, propagandafotók és -videók mellett családi, egészségügyi témákban is születtek írások.

[251] 2003-ban Iraki Al-Kaida néven alakult meg, 2011-ben, amikor a szomszédos Szíriában kitört a polgárháború, ott is megjelent, majd 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 szemben, ami alapvetően a Nyugat elleni harcot tekinti szervező elemnek. Az Iraki és Levantei Al-Kaida az iszlám Kalifátus megvalósítását tekinti fő céljának. Persze az Al-Kaida ideológiájában is megjelent a kétezres évek elején a globális Kalifátus gondolata, amit egy 20 éves terv végeredményeként terveztek megvalósítani, de a 2010-es évek elején ezt az Iszlám Állam képviselte. Az erőszakosság mellett tulajdonképpen ez az ideológiai különbség vezetett a szakadáshoz, és végül 2013-ban az Iraki és Levantei Iszlám Állam (ISIS) nevet vették fel az ismert 2014-es névváltozásig.

[252] Margitics József (2017): Az ISIS által használt internetes propaganda eszközök áttekintése, In: Veres Eszter – Pliska Virág – Nagy Bianka – Fülöp Eszter – Dobák Imre (szerk.): Nemzetbiztonsági Szakkollégium Kiadványkötete, Budapest.

- Iszlám Állam Archívum weblap, amin az Iszlám Államhoz köthető beszámolók, fényképek, videók szerepelnek, beleértve harcosok üzeneteit, amit toborzásra, propagandára használtak.
- A Facebookon számos oldalt és csoportot üzemeltettek. Az oldalakhoz sorolható többek között az Iszlám Állam friss hírei, Mudzsahed hírek, Abu-Bakr Baghdadi stb.; a csoportokhoz: Az „Iszlám Erő Csoport" Hálózata, Az Umma Dzsihád a csúcsra kerül, Az Iszlám Állam médiasejtje stb.
- A 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.
- A YouTube-on is számos csatornát üzemeltettek, amelyek a kiképzésektől a mindennapi élet bemutatásán át a fogvatartottak üzenetéig bezárólag sok mindenre kiterjedtek. Emellett, hogy megszólítsák a fiatalokat, olyan tartalmakat is nagyszámban 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 csupán kapcsolattartásra használtak, mint például a Telegram Messengert, hanem propaganda terjesztésére is. Amikor 2014 augusztusától az említett James Foley kivégzése hatására nagyszámban 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 általuk használt közösségi oldalakon híreket tegyenek közzé. Ezáltal lényegében szinte kiírthatatlanná téve az Iszlám Államot a közösségi oldalakról.
- Blogok, köztük az Iszlám Kalifátus, Iszlám Állam a fentiekhez hasonlóan híreket, propagandaüzeneteket közvetített.

Amögött, hogy az Iszlám Állam ilyen professzionálisan jelent meg a közösségi médiában, feltehetően egy szír–amerikai állampolgár, Ahmad Abousamra állt, aki az Egyesült Államokban szerzett informatikus végzettséget, és telekommunikációs cégeknél dolgozott.

Mindezek mellett nagy gondot fordítottak a tagok képzésére is. Kézikönyveket adtak ki a megfelelő közösségimédia-használattal kapcsolatban, amelyben információbiztonsági szempontokra is felhívták a figyelmet a propaganda és a konspiratív kommunikáció eljárásai mellett.[253] A kiadvány érdekessége, hogy eredetileg egy kuvaiti biztonsági cég, a Cyberkov állította össze, elsősorban újságíróknak és politikai aktivistáknak, akik a gázai övezetben dolgoztak, de az Iszlám Állam a saját szervezetének megfelelően adaptálta, és átírta a kézikönyvben foglaltakat.

Az Iszlám Állam napjainkra szerencsére rengeteget veszített befolyásából, azonban az megállapítható, hogy az út, amire rálépett a propaganda ilyen magas szintű alkamazásával, 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 második fejezetben a kiberterrorizmussal kapcsolatos résznél már megfogalmaztuk.

[253] A kiadványt lásd: Several cybersecurity to protect your account in the social networking. URL: http://www.wired.com/wp-content/uploads/2015/11/ISIS-OPSEC-Guide.pdf (Letöltés ideje: 2018. január 30.)

Fontosabb fogalmak

Arab tavasz, attribution, álhírek, black ops, BREXIT, botnethálózat, Filter Bubble, célzott támadás, Cozy Bear, dezinformáció, dezintegráció, digitális gerrymandering, dzsihádizmus, Fancy Bear, GRU, Guccifer 2.0, hibrid hadviselés, Iszlám Állam, online identitásmenedzselő szoftver, trollhadsereg, VPN, WikiLeaks

Áttekintő kérdések

1. Véleménye szerint egyértelműen bizonyítható Oroszország érintettsége a kibertámadásban?
2. Mennyire tart attól, hogy egy idegen állam nemzetbiztonsági szolgálata beavatkozik a magyarországi választásokba?
3. Megítélése szerint, ha bebizonyosodik, hogy egy idegen állam beavatkozott egy másik állam választási eljárásába a kibertérben elkövetett támadásokkal, milyen választ adhat erre a megtámadott ország?
4. Oroszországot rendszerint éri az a vád európai politikusok részéről, hogy botnetek segítségével álhíreket terjeszt, feltöri a politikusok privát levelezéseit, és nyilvánosságra hozza azokat, ezzel befolyásolva az európai választásokat. Megítélése szerint miért állhat ez Oroszország érdekében?
5. Ön szerint szükséges államilag szabályozni a közösségi oldalakat?
6. Megítélése szerint a németországi jogi szabályozás megengedő vagy túlzottan szigorú?
7. Ön szerint hogyan lehet harcolni az álhírek ellen?
8. Ön szerint hol kezdődik az egyén felelőssége az álhírekkel kapcsolatban?
9. Ön szerint milyen módon lehet felkészíteni az embereket az álhírek felismerésére?

JOGSZABÁLYTÁR

1. 1139/2013, (III. 21.) Korm. határozat Magyarország Nemzet Kiberbiztonsági stratégiájáról. In: Magyar Közlöny, 2013/47.
2. 1965. évi 22. törvényerejű rendelet a diplomáciai kapcsolatokról Bécsben, 1961. április 18-án aláírt nemzetközi szerződés kihirdetéséről, URL: https://net.jogtar.hu/jr/gen/getdoc2.cgi?docid=96500022.TVR (Letöltés ideje: 2017. december 20.)
3. 1994. évi XXXIV. törvény a Rendőrségről, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99400034.TV (Letöltés ideje: 2017. december 13.)
4. 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=99500125.TV (Letöltés ideje: 2017. december 16.)
5. 2005. évi CXXXIII. törvény a személy- és vagyonvédelmi, valamint a magánnyomozói tevékenység szabályairól, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0500133.tv (Letöltés ideje: 2017. december 13.)
6. 2009. évi CLV. törvény a minősített adat védelméről, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a0900155.tv (Letöltés ideje: 2017. november 11.)
7. 2011. évi CXII. törvény az információs önrendelkezési jogról és információszabadságról, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100112.TV (Letöltés ideje: 2017. november 11.)
8. 2011. évi CXIII. törvény a honvédelemről és a Magyar Honvédségről, valamint a különleges jogrendben bevezethető intézkedésekről, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100113.TV (Letöltés ideje: 2017. augusztus 8.).
9. 2011. évi CXXVIII. törvény a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100128.TV (Letöltés ideje: 2017. augusztus 8.).
10. 2012. évi I. törvény a munka törvénykönyvéről, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200001.TV (Letöltés ideje: 2017. december 13.)
11. 2012. évi C. törvény a Büntető Törvénykönyvről, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1200100.TV (Letöltés ideje: 2017. december 11.)
12. 2013. évi V. törvény a Polgári Törvénykönyvről, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1300005.TV (Letöltés ideje: 2017. december 12.)
13. 234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1100234.kor (Letöltés ideje: 2017. augusztus 8.).
14. 60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról. In: Honvédelmi Közlöny, CXL évfolyam 10. szám, 2013.
15. A Kormány …/2016. (… ...) Korm. rendelete az egyes légiközlekedéssel összefüggő kormányrendeletek módosításáról, URL: http://www.kormany.hu/download/8/db/e0000/RPAS__honlapra.pdf#!DocumentBrowse (Letöltés ideje, 2017. december 14.)

16. A létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló 2012. évi CLXVI. törvény, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=a1200166.tv (Letöltés ideje: 2017. július 19.).
17. Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény, URL: http://njt.hu/cgi_bin/njt_doc.cgi?docid=160206.323158 (Letöltés ideje: 2017. július 6.)
18. 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), URL: http://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32016R0679&from=HU (Letöltés ideje: 2017. december 12.)
19. Magyarország Alaptörvénye, URL: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A1100425.ATV (Letöltés ideje: 2017. augusztus 8.)

IRODALOMJEGYZÉK

Adam et al.: Experimental evidence of massive-scale emotional contagion through social networks, In: PNAS, 2014., vol. 111., no. 29. URL: http://www.pnas.org/content/pnas/111/24/8788.full.pdf (Letöltés ideje:...)

Adatokat eltulajdonító androidos zseblámpa alkalmazás, In: GovCERT, 2013. december 6. URL: http://tech.cert-hungary.hu/tech-blog/131206/adatokat-eltulajdonito-androidos-zseblampa-alkalmazas (Letöltés ideje: 2017. december 14.)

AJP-3.10 Allied Joint Doctrine for Information Operation, 2009. URL: https://info.publicintelligence.net/NATO-IO.pdf (Letöltés ideje:...)

AJP-3.7. NATO Military Policy on Psychological Operations, 2003. URL: https://info.publicintelligence.net/NATO-PSYOPS-Policy-2003.pdf (Letöltés ideje:...)

Ádám László: Az elhárítás feladatrendszere. In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete. 363 p. Nemzeti Közszolgálati Egyetem, Budapest, pp. 129–145., 2014.

Ball, James: Xbox Live among game services targeted by US and UK spy agencies, In: The Guardian, 2013. december 9. URL: http://www.theguardian.com/world/2013/dec/09/nsa-spies-online-games-world-warcraft-second-life?CMP=twt_gu (Letöltés ideje: 2017. december 21.)

Ball, James – Borger, Julian – Greenwald, Glenn (2013): Revealed: how US and UK spy agencies defeat internet privacy and security. In: The Guardian, 2013. szeptember 6. URL: http://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security (Letöltés ideje: 2017. december 21.)

Bányász Péter: A közösségi média, mint az információs hadszíntér speciális tartománya. Hadmérnök, XII. Évfolyam „KÖFOP" szám – 2017. október.

Bányász Péter (2014): Spies Act As A Spy: The Edward Snowden Case. In: Sopóci, Milan – Petrufová, Mária – Školník, Miroslav – Frianová, Viera – Nekoranec, Jaroslav – Belan Jirásková, Lubomír – Kustrová, Milota – Morong, Stanislav (szerk.): Manažment - teória, výučba a prax 2014: zborník príspevkov z medzinárodnej vedecko-odbornej konferencie. 380 p. Akadémia ozbrojených síl generála Milana Rastislava Štefánika, Liptovsky Mikulas. pp. 194–201.

Bányász Péter – Orbók Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében. Hadtudomány Online, 2013/1. URL: http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf (Letöltés ideje: 2017. július 19.).

Berki Gábor (2013): A kibertéri konfliktusok változása. Hadmérnök, VIII/1. szám. pp. 173–185.

Béres János (2014): A hírszerzés feladatrendszere. In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete. 363 p. Nemzeti Közszolgálati Egyetem, Budapest, pp. 117 –128.

Borger, Julian (2013): NSA files: why the Guardian in London destroyed hard drives of leaked files. In: The Guardian, 2013. augusztus 20. URL: http://www.theguardian.com/world/2013/aug/20/nsa-snowden-files-drives-destroyed-london (Letöltés ideje: 2017. december 21.)

Bump, Philip (2013): Federal Judge: NSA's ‚Almost-Orwellian' Data Collection Likely Violates Constitution. In: The Wire, 2013. december 16. URL: http://www.thewire.com/politics/2013/12/federal-judge-nsas-almost-orwellian-phone-data-collection-likely-violates-constitution/356207/ (Letöltés ideje: 2017. december 21.)

Bump, Philip – Ohlheiser, Abby (2013): The Amash Amendment Fails, Barely. In: The Wire, 2013. július 24. URL: http://www.thewire.com/politics/2013/07/amash-amendment-fails-despite-democratic-support/67584/ (Letöltés ideje: 2017. december 21.)

Buzan, Barry – Wæver, Ole – De Wilde, Jaap (1997): A New Framework for Analysis, Lynne Rienner Publishers.

Campbell, Duncan (1988): Somebody's Listening. In: New Statesman, 1988. augusztus 12. URL: http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf (Letöltés ideje: 2017. december 20).

Campbell, Duncan – Honigsbaum, Mark (1999): Britain and US spy on world. In: The Guardian, 1999. május 23. URL: http://www.duncancampbell.org/menu/journalism/guardian/britain.pdf (Letöltés ideje: 2017. december 20.)

Chazan, David (2015): Russia ‚bought' Marine Le Pen's support over Crimea, In: The Telegraph, 2015. április 4. URL: http://www.telegraph.co.uk/news/worldnews/europe/france/11515835/Russia-bought-Marine-Le-Pens-support-over-Crimea.html (Letöltés ideje: 2018. január. 23.)

Chen, Ben (2016): 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. URL: http://appft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.html&r=1&p=1&f=G&l=50&d=PG01&S1=%2820160114.PD.+AND+%28Facebook.AS.+OR+Facebook.AANM.%29%29&OS=PD/1/14/2016+and+%28AN/Facebook+or+AANM/Facebook%29&RS=%28PD/ (Letöltés ideje: 2018. január 16.)

Cohen, Heidi (2011): 30 Social Media Definitions. In: HeidiCohen.com, 2011. május 9. URL: http://heidicohen.com/social-media-definition/ (Letöltés ideje: 2017. június 26.).

Collins, Keith (2017): Google collects Android users' locations even when location services are disabled. In: Quartz, 2017. november 21. URL: https://qz.com/1131515/google-collects-android-users-locations-even-when-location-services-are-disabled/ (Letöltés ideje: 2017. december 17.)

Das, Sauvik – Kramer, Adam (2013): Self-Censorship on Facebook. In: Facebook Research. URL: https://research.fb.com/wp-content/uploads/2016/11/self-censorship-on-facebook.pdf (Letöltés ideje: 2017. június 26.).

Davenport T.H. – Prusak, L. (2001): Tudásmenedzsment. Kossuth Kiadó, Budapest.

Deák Veronika (2017): A social engineering humán alapú támadási technikái. In: Biztonságpolitika, 2017. április 10. URL: http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-social-engineering-human-alapu-tamadasi-technikai (Letöltés ideje:...)

Deák Veronika (2017): A számítógép alapú social engineer támadási technikák. In: Biztonságpolitika, 2017. április 28. URL: http://biztonsagpolitika.hu/publikaciok-2017/deak-veronika-a-szamitogep-alapu-social-engineering-tamadasi-technikai (Letöltés ideje:...)

Deák Veronika (2017): Biztonságtudatosság az információs környezetben. In: Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, 2017/3. pp. 59 –77.

Definition of social media in English, In: Oxford Dictionaries. URL: http://www.oxforddictionaries.com/definition/english/social-media (Letöltés ideje: 2017. június 26.).

Dobák Imre (2014): Elektronikai eszközökkel végzett felderítés. In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Budapest. pp. 163 –168.

Dobák Imre – Kovács Zoltán (2014): Új technológiák hatása a hírszerzésre. In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Budapest, pp. 206 –220.

ERICSON PRESS RELEASE: New study quantifies the impact of broadband speed on GDP. In: Ericson, 2011. szeptember 27. URL: http://www.ericsson.com/news/1550083 (Letöltés ideje: 2017. augusztus 8.).

EUROLÓGUS: Dúl a háború az európai adatokért. In: Index, 2013. október 23. URL: http://index.hu/kulfold/eurologus/2013/10/23/folyik_a_haboru_az_adatokert/ (Letöltés ideje: 2017. december 21.)

EUROLÓGUS: Megszavazta Snowden meghallgatását az EP. In: Index, 2013. december 13. URL: http://index.hu/kulfold/eurologus/2013/12/13/snowden_ep_meghallgatas/ (Letöltés ideje: 2017. december 21.)

European Parliament: Temporary Committee On The Echelon Interception System Directorate-General For Committees And Delegationsbrussels Meeting, 2001. január 22–23. URL: http://www.duncancampbell.org/menu/surveillance/echelon/Contract_analysis.pdf (Letöltés ideje: 2017. december 20.).

Európa digitális fejlődéséről szóló jelentés (EDPR), 2018 – Országprofil Magyarországról. In: Európai Bizottság. URL: http://ec.europa.eu/information_society/newsroom/image/document/2018-20/hu-desi_2018-country-profile-lang_4AA43283-EC48-996F-09918493E34A691F_52334.pdf (Letöltés ideje: 2017. augusztus 21.)

Europol The Internet Organised Crime Threat Assesment 2016. Europol, Hága, 2016. URL: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016 (Letöltés ideje: 2018. január 15).

Facebook Reports First Quarter 2017 Results. In: Facebook Investor Relations, 2017. május 3. URL: https://investor.fb.com/investor-news/press-release-details/2017/Facebook-Reports-First-Quarter-2017-Results/default.aspx (Letöltés ideje: 2017.június 26.)

Facebook Trancparency: Magyarországi adatbekérések 2017. január – 2017. június. In: Facebook, 2017. URL: https://transparency.facebook.com/country/Hungary/2017-H1/ (Letöltés ideje: 2017. december 29.)

Ferenczy Gábor (2007): Internet alapú nyílt információszerzés elvi rendszertechnikai megvalósítása: doktori (PhD) értekezés. ZMNE, Budapest.

Foster, Peter (2016): Russia accused of clandestine funding of European parties as US conducts major review of Vladimir Putin's strategy. In: The Telegraph, 2016. január 16. URL: http://www.telegraph.co.uk/news/worldnews/europe/russia/12103602/America-to-investigate-Russian-meddling-in-EU.html (Letöltés ideje: 2018. január 23.)

GARTNER PRESS RELEASE: Gartner Says Capitalism Going Social Will Require Organizations to Build Two-Way Relationships with the „99 Percent". In: Gartner Research, 2012. december 12. URL: http://www.gartner.com/newsroom/id/2260917 (Letöltés ideje: 2017. augusztus 8.)

Gellman, Barton (2013): NSA broke privacy rules thousands of times per year, audit finds. In: The Washington Post, 2013. augusztus 16. URL: 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 (Letöltés ideje: 2017. december 21.)

Gellman, Barton – Miller, Greg (2013): U.S. spy network's successes, failures and objectives detailed in 'black budget' summary. In: The Washington Post, 2013. augusztus 29. URL: http://www.washingtonpost.com/world/national-security/black-budget-summary-details-us-spy-networks-successes-failures-and-objectives/2013/08/29/7e57bb78-10ab-11e3-8cdd-bcdc09410972_story.html (Letöltés ideje: 2017. december 21.)

Gellman, Barton – Soltani, Ashkan (2013): NSA tracking cellphone locations worldwide, Snowden documents show. In: The Washington Post, 2013. december 4. URL: http://www.washingtonpost.com/world/national-security/nsa-tracking-cellphone-locations-worldwide-snowden-documents-show/2013/12/04/5492873a-5cf2-11e3-bc56-c6ca94801fac_story.html?hpid=z1 (Letöltés ideje: 2017. december 21.)

Greenwald, Glenn et al. (2013): Microsoft handed the NSA access to encrypted messages. In. The Guardian, 2013. július 12. URL: http://www.theguardian.com/world/2013/jul/11/microsoft-nsa-collaboration-user-data (Letöltés ideje: 2017. december 21.)

Greenwald, Glenn – Poitras, Laura – Macaskill, Ewen (2013): NSA shares raw intelligence including Americans' data with Israel. In: The Guardian, 2013. szeptember 11. URL: http://www.theguardian.com/world/2013/sep/11/nsa-americans-personal-data-israel-documents (Letöltés ideje: 2017. december 21.)

Greenwald, Glenn et al. (2013): New Snowden docs show U.S. spied during G20 in Toronto. In: CBC, 2013. november 27. URL: http://www.cbc.ca/news/politics/new-snowden-docs-show-u-s-spied-during-g20-in-toronto-1.2442448 (Letöltés ideje: 2017. december 21.)

Greenwald, Glenn (2013): XKeyscore: NSA tool collects ‚nearly everything a user does on the internet'. In: The Guardian, 2013. július 31. URL: http://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data (Letöltés ideje: 2017. december 21.)

Gyaraki Réka (2017): A nyomozóhatóság és a katasztrófavédelem feladata a kiberbűncselekmények vonatkozásában. Szakmai Szemle, XV. évf. 4. sz. pp. 113–127.

Gyaraki Réka – Simon Béla (2017): Biztonsági események rendészeti szempontból – a kiberbűncselekmények kezelése. Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2017, Nemzeti Közszolgálati Egyetem, Budapest.

Szabó József – Gabriel Győző – Horváth Ferenc (szerk.) (1995):Hadtudományi Lexikon. Magyar Hadtudományi Társaság, Budapest.

Haig Zsolt (2015): Információ – társadalom – biztonság. NKE Szolgáltató Kft., Budapest.

Haig Zsolt – Várhegyi István (2005): Hadviselés az információs hadszíntéren, Zrínyi Kiadó, Budapest.

Haig et al. (2014): Elektronikai hadviselés (szerk. Németh András), Nemzeti Közszolgálati Egyetem, Budapest, 2014.

Halassy Béla (1994): Az adatbázis tervezés alapjai és titkai – Avagy az út az adattól az adatbázison át az információig. IDG Hungary, cop., Budapest.

Hanula Zsolt (2016): Ezek nagyon okos fickók, de a végén úgyis elkapjuk őket. In: Index, 2016. július 31. URL: https://index.hu/tech/2016/07/31/ezek_nagyon_okos_fickok_de_a_vegen_ugyis_elkapjuk_oket/ (Letöltés ideje: 2017. december 14.)

Hanula Zsolt – Iván András (2013): Az amerikai hírszerzés árnyékbirodalma. In: Index, 2013. 2013. június 25. URL: http://index.hu/kulfold/2013/06/25/az_amerikai_hirszerzes_arnyekbirodalma/ (Letöltés ideje: 2017. december 21.

Héjja István (2014): Nemzetbiztonsági szervezeti modellek. In: A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest. pp. 57–72.

Hoffman, Frank G. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for policy studies, Virginia. p. 8.

Hopkins, Nick – Borger, Julian (2013): Exclusive: NSA pays £100m in secret funding for GCHQ. In: The Guardian, 2013. augusztus 1. URL: http://www.theguardian.com/uk-news/2013/aug/01/nsa-paid-gchq-spying-edward-snowden (Letöltés ideje: 2017. december 21.)

Hornyacsek et al. (2010): Önkormányzati vezetők felkészítése a védelmi igazgatási feladatokra. Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest.

Horváth Balázs: A Facebook ördögi tervvel férkőzne be Kínába. In: 24 Tech, 2016. november 23. URL: https://24.hu/tech/2016/11/23/a-facebook-ordogi-tervvel-ferkozne-be-kinaba/ (Letöltés ideje: 2017. december 29.)

HP: Top-Secret Document Reveals NSA Spied On Porn Habits As Part Of Plan To Discredit‚Radicalizers'. In: Huffington Post, 2013. november 26. URL: http://www.huffingtonpost.com/2013/11/26/nsa-porn-muslims_n_4346128.html?1385526024 (Letöltés ideje: 2017. december 21.)

Hurricane Sandy: Resources on Twitter. In: Twitter blog, 2012. október 29. URL: http://blog.twitter.com/2012/10/hurricane-sandy-resources-on-twitter.html (Letöltés ideje: 2017. augusztus 15.).

HVG: Obama leállíttatta az ENSZ-székház lehallgatását. In: HVG, 2013. október 30. URL: http://hvg.hu/vilag/20131030_ensz_lehallgatas_obama_leallit (Letöltés ideje: 2017. december 21.)

HVG: Snowden kollégái jelszavával ügyeskedve szivárogtatott. In: HVG, 2013. november 8. URL: http://hvg.hu/vilag/20131108_Snowden_kollegai_jelszavaval_ugyeskedve_s (Letöltés ideje: 2017. december 21.).

Izsa Jenő (2009): A hírszerzés céljáról és rendszeréről. Hadtudomány, 2009/1–2.

Jakobi Ákos (2002): A virtuális világ terei – Reflexiók Mészáros Rezső „A kibertér társadalomföldrajzi megközelítése" című tanulmányához, In: Magyar Tudomány, 2002/11. pp. 482–1491.

Joint Publication 3–13, Information Operations, 27 November 2012 by United States Government US Army, p. I-1.m.

Juhász Attila et al. (2015): „Eurázsiai vagyok" – A magyar szélsőjobboldal kapcsolata a Kremllel. In: Political Capital, 2015. március. URL: http://www.politicalcapital.hu/wp-content/uploads/PC_SDI_Boll_tanulmany_Eurazsiai-Vagyok.pdf (Letöltés ideje: 2018. január 23.)

Kaplan, Andreas – Haenlein, Michael (2010): Users of the world, unite! The challenges and opportunities of Social Media. Business Horizons, volume 53 issue 1. pp. 59–68.

Kemp, Simon (2018): Digital in Eastern Europe. In: We are social, 2018. január 29. URL: https://www.slideshare.net/wearesocial/digital-in-2018-in-eastern-europe-part-2-east-86865266 (Letöltés ideje: 2018. augusztus 21.)

Kemp, Simon: Global Digital Report 2018. In: We are social, 2015. január 21. URL: https://digitalreport.wearesocial.com/ (Letöltés ideje: 2018. augusztus 21.)

Kenedli, Tamás (2014): A nyílt forrású információszerzés. In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete, Nemzeti Közszolgálati Egyetem, Budapest, pp. 169–178.

Kis-Benedek József (2013): A nemzetbiztonsági szolgálatok együttműködése. Hadtudomány, XXIII:(1–2) pp. 100–114.

Kis-Benedek József (2014): Az emberi erőkkel folytatott információszerzés: HUMINT – Human Intelligence. In: Dobák Imre (szerk.): A nemzetbiztonság általános elmélete. Nemzeti Közszolgálati Egyetem, Budapest. pp. 153–163.

Kiss Tibor (2014): Gyűlölet-bűncselekmények és szélsőséges csoportok az információs társadalomban. In: Prazsák Gergő (szerk.): Nemzeti szempont. Apeiron Kiadó, Budapest. pp. 71–92.

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

Kiss Tibor – Parti Katalin (2016): Informatikai bűnözés. In: Borbíró Andrea – Gönczöl Katalin – Kerezsi Klára – Lévay Miklós (szerk.): Kriminológia. 1031 p. Wolters Kluwer, Budapest. pp. 491–517.

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

Kovács László – Krasznay Csaba (2017): Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. In: Nemzet és Biztonság, 2017/1. pp. 3–16., 2017. URL: http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf (Letöltés ideje:...)

Kovács László – Krasznay Csaba (2017): „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. In: Stratégiai Védelmi Kutatóközpont – Elemzések, 2017/9. pp. 1–11.

Kovács László – Sipos Mariann (2010): A Stuxnet és ami mögötte van: Tények és a cyberháború hajnala. Hadmérnök, V. évf., 4. szám, pp. 163–172.

Kovács Zoltán (2014): Hordozható infokommunikációs eszközök használatához kapcsolódó biztonságtudatossági képzési tematika védett vezetők számára. In: Hadmérnök, IX/3. szám. pp. 182–190., 2014.

Krasznay Csaba (2012): A polgárok védelme egy kiberkonfliktusban. Hadmérnök, VII. évf. 4. szám. pp. 142–151.

Krasznay Csaba – Simon Béla (2017): Kiberbűncselekmények az online kereskedelemben. Hadmérnök, XII. Évfolyam „KÖFOP" szám – 2017. október.

Krasznay Csaba – Varga-Perke Bálint (2013): Ifjúságvédelem a hacker szubkultúrában. In: Bíró A. Zoltán – Gergely Orsolya (szerk.): Ártalmas vagy hasznos internet? A média hatása a gyermekekre és fiatalokra. Státus Kiadó, Csíkszereda. pp. 179 –202.

Lakhani, Aamir – Muniz, Joseph (2013): Social Media Deception. In: RSA Cyber Security Summit Konferencia – Európa, 2013. október 29–31. URL: http://itcafe.hu/dl/cnt/2013-11/102992/hum-w01-social-media-deception.pdf (Letöltés ideje: 2018. január 11.)

Leleplezték a Wikipedia legnagyobb átverését. In: Index, 2013. május 5. URL: http://index.hu/tech/2013/05/01/lelepleztek_a_wikipedia_legnagyobb_atvereset/ (Letöltés ideje: 2017. június 26.).

Lévay, Gábor (2006): OSINT (Open Source Intelligence) – Nyílt információs hírszerzés. Egyetemi jegyzet, ZMNE, Budapest.

LICA: Távolról is bekapcsolható az iPhone kamerája. In: Index, 2014. január 1. URL: http://index.hu/tech/2014/01/01/tavolrol_is_bekapcsolhato_az_iphone_kameraja/ (Letöltés ideje: 2017. december 21.)

Lindsay, Bruce R. (2011): Social Media and Disasters: Current Uses, Future Options, and Policy Considerations, Congressional Research Report. In: The Federation of American Scientist, 2011. szeptember 6. URL: http://www.fas.org/sgp/crs/homesec/R41987.pdf (Letöltés ideje: 2017. augusztus 15.).

Loell, Keith (2013): Did Sir Isaac Newton Invent Social Media? In: Forbes, 2013. április 18. URL: http://www.forbes.com/sites/gyro/2013/04/18/did-sir-isaac-newton-invent-social-media/ (Letöltés ideje: 2017. június 26.).

Macaskill, Ewan (2015): British army creates team of Facebook warriors. In: The Guardian, 2015. január 31. URL: http://www.theguardian.com/uk-news/2015/jan/31/british-army-facebook-warriors-77th-brigade (Letöltés ideje: 2018. január 24.)

Macaskill, Ewen (2013): Edward Snowden, NSA files source: ‚If they want to get you, in time they will'. In: The Guardian 2013. június 10. URL: http://www.theguardian.com/world/2013/jun/09/nsa-whistleblower-edward-snowden-why (Letöltés ideje: 2017. december 21.)

Macaskill, Ewen (2013): NSA paid millions to cover Prism compliance costs for tech companies. In: The Guardian, 2013. augusztus 23. URL: http://www.theguardian.com/world/2013/aug/23/nsa-prism-costs-tech-companies-paid (Letöltés ideje: 2017. december 21.)

Margitics József (2017): Az ISIS által használt internetes propaganda eszközök áttekintése, In: Veres Eszter – Pliska Virág – Nagy Bianka – Fülöp Eszter – Dobák Imre (szerk.): Nemzetbiztonsági Szakkollégium Kiadványkötete, Budapest

Masnick, Mike (2013): US Official Admits That UK Detention Of Glenn Greenwald's Partner Was ‚To Send A Message'. In: TechDirt, 2013. augusztus 20. URL: http://www.techdirt.com/articles/20130820/03160924251/us-official-admits-that-uk-detention-glenn-greenwalds-partner-was-to-send-message.shtml (Letöltés ideje: 2017. december 21.)

MCKINSEY & CO.: Online and upcoming: The Internet's impact on aspiring countries, 2012. január. URL: http://www.mckinsey.com/client_service/high_tech/latest_thinking/impact_of_the_internet_on_aspiring_countries pp. 81-91. (Letöltés ideje: 2017. augusztus 8.)

Menn, Joseph (2013): Exclusive: Secret contract tied NSA and security industry pioneer. In: Reuters, 2013. december 20. URL: http://www.reuters.com/article/2013/12/21/us-usa-security-rsa-idUSBRE9BJ1C220131221 (Letöltés ideje: 2017. december 21.)

Mestyán Márton – Yassarivel, Taha – Kertész János (2013): Early Prediction of Movie Box Office Success Based on Wikipedia Activity Big Data. In: PLOS One, 2013. augusztus 21. URL: http://journals.plos.org/plosone/article/file?id=10.1371/journal.pone.0071226&type=printable (Letöltés ideje: 2017. december 20.)

Mészáros Rezső (2001): A kibertér társadalomföldrajzi megközelítése. In: Magyar Tudomány, 2001/7. pp. 769–779.

MH Összhaderőnemi Elektronikai Hadviselési Doktrína. MH DSZOFT Kód: 11222. HM HVK Felderítő Csoportfőnökség kiadványa, 2005.

Most famous social network sites worldwide as of April 2017, ranked by number of active users (in millions). In: Statista.com. URL: https://www.statista.com/statistics/272014/global-social-networks-ranked-by-number-of-users/ (Letöltés ideje: 2017.június 26.)

Mitnick, Kevin D. (2003): A legendás hacker – A megtévesztés művészete. Perfact-Pro, Budapest.

MTI: Izrael lefújt egy katonai akciót a Facebook miatt. In: Metropol, 2010. március 3. URL: http://www.metropol.hu/cikk/535056 (Letöltés ideje: 2018. január 13.)

Muha et al. (2007): Az informatikai biztonság kézikönyve (szerk. Szenes Katalin), Verlag Dashöfer, Budapest.

Munk Sándor (2007): Információbiztonság vs. informatikai biztonság. Hadmérnök, 2007/különszám. URL: http://hadmernok.hu/kulonszamok/robothadviseles7/munk_rw7.html (Letöltés ideje: 2017. július 12.).

NMHH: Lakossági internethasználat – Online piackutatás 2016., Ariosz Kft., NRC Kft. In: Nemzeti Média- és Hírközlési Hatóság. URL: http://nmhh.hu/dokumentum/187704/lakossagi_internethasznalat_2016.pdf (Letöltés ideje: 2017. június 26.).

NSA: UKUSA Agreement Release 1940–1956. In: National Security Agency: Public Information, Declassification and Transparency. URL: http://www.nsa.gov/public_info/declass/ukusa.shtml (Letöltés ideje: 2017. december 20.).

NSA: VENONA. In: National Security Agency: Public Information, Declassification and Transparency. URL: http://www.nsa.gov/public_info/declass/venona/ (Letöltés ideje: 2017. december 20.)

Oroszbarátok a jobbszélen. In: Gondola, 2009. december 1. URL: http://gondola.hu/cikkek/68518 (Letöltés ideje: 2018. január 21.)

Pix Gábor (2005): A lélektani műveletek jellemzőinek vizsgálata. Doktori (PhD) értekezés, Zrínyi Miklós Nemzetvédelmi Egyetem, Budapest.

Poitras, Laura et al. (2013): Attacks from America: NSA Spied on European Union Offices. In: Spiegel Online, 2013. június 29. URL: http://www.spiegel.de/international/europe/nsa-spied-on-european-union-offices-a-908590.html (Letöltés ideje: 2017. december 21.)

Resperger István (2012): A „diadal" és egyéb módszerek alkalmazása a nemzeti válságkezelési feladatok megoldásánál. In: Hadtudományi Szemle, 5. évf. 1–2. szám. pp. 141–165. URL: http://archiv.uni-nke.hu/downloads/kutatas/folyoiratok/hadtudomanyi_szemle/szamok/2012/2012_1/2012_1_br_resperger_istvan_141_165.pdf (Letöltés ideje:...)

Resperger István (2002): Kockázatok, kihívások, fenyegetések a XXI. században. Az Országos Kiemelt Kutatási Tanulmányok pályázata, Budapest.

Roche, Edward M. (2017): Comments on "Assessing Russian Activities and Intentions in Recent US Elections". In: Cyberarmscontrolblog, 2017. január 8. URL: https://cyberarmscontrolblog.com/2017/01/08/comments-on-assessing-russian-activities-and-intentions-in-recent-us-elections/ (Letöltés ideje: 2018. január 24.)

Rodewig, Cheryl (2012): Geotagging poses security risks. In: Army.mil, 2012. március 7. URL: http://www.army.mil/article/75165/Geotagging_poses_security_risks/ (Letöltés ideje: 2018. január 13.)

Sciutto, Jim – Perez, Evan (2013): Review: NSA snooping program should stay in place. In: CNN, 2013. december 18. URL: http://edition.cnn.com/2013/12/18/politics/nsa-report/ (Letöltés ideje: 2017. december 21.)

Selján Péter (2011): A közösségi média szerepe a 21. században, avagy az „arab tavasz" és a közösségi oldalak. In: Biztonságpolitika.hu, 2011. december 9. URL: http://old.biztonsagpolitika.hu/index.php?&id=16&aid=1137&title=a-kozossegi-media-szerepe-a-21-szazadban-avagy-az-arab-tavasz-es-a-kozossegi-oldalak&load=ZVD6ci0SpPs (Letöltés ideje: 2018. január 27.)

Simon Béla (2017): Bűnüldözés előtt álló digitális kihívások. Magyar Rendészet, XVII. évf. 5. szám.

Sottek, T.C. (2013): NSA reportedly intercepting laptops purchased online to install spy malware. In: The Verge, 2013. december 29. URL: http://www.theverge.com/2013/12/29/5253226/nsa-cia-fbi-laptop-usb-plant-spy (Letöltés ideje: 2017. december 21.)

SPIEGEL ONLINE: Embassy Espionage: The NSA's Secret Spy Hub in Berlin. In: Spiegel Online, 2013. október 27. URL: http://www.spiegel.de/international/germany/cover-story-how-nsa-spied-on-merkel-cell-phone-from-berlin-embassy-a-930205.html (Letöltés ideje: 2017. december 21.)

SPIEGEL ONLINE: Überwachung: NSA späht internationalen Zahlungsverkehr aus. In: Spiegel Online, 2013. szeptember 9. URL: http://www.spiegel.de/netzwelt/netzpolitik/nsa-spaeht-internationalen-zahlungsverkehr-aus-a-922283.html (Letöltés ideje: 2017. december 21.)

Stempel, Jonathan (2013): U.S. judge says NSA phone surveillance is lawful. In: Reuters, 2013. december 27. URL: http://news.yahoo.com/u-judge-says-nsa-phone-data-program-lawful-163733246.html (Letöltés ideje: 2017. december 21.)

Szabó András (2017): A felhasználók digitális lábnyomának, anonimitásának vizsgálata technikai szempontból I. rész – Személyi számítógépek. Hadmérnök, XII. Évfolyam „KÖFOP" szám – 2017. október. pp. 163–180.

Szádeczky Tamás (2012): The role of technology. Auditing and certification in the field of data security. In: Gergely László Szőke (ed.): Privacy in the Workplace. Data Protection Law and Self-regulation in Germany and Hungary. HVG-ORAC, Budapest. pp. 311–337. ISBN 9789632581972

Szádeczky Tamás (2016): Risk Management of New Technologies. Academic and Applied Research in Military and Public Management Science, 15:(3) pp. 279–290. 2016.

Taaki, Amir (2011): Nincs jövő múlt nélkül, In: Bitcoin Portál, 2011. december 29. URL: https://bitcoin.hu/nincs-jovo-mult-nelkul/ (Leöltés dátuma: 2018. január 14.)

Taigman, Yaniv (2014): DeepFace: Closing the Gap to Human-Level Performance in Face Verification. In: Facebook Research, 2014. június 24. URL: https://research.fb.com/publications/deepface-closing-the-gap-to-human-level-performance-in-face-verification/ (Letöltés ideje: 2017. december 14.)

Testimony of Keith Lourdeau, Deputy Assistant Director, Cyber Division, FBI Before the Senate Judiciary Subcommittee on Terrorism, Technology, and Homeland Security February 24, 2004. URL: http://www.fbi.gov/congress/congress04/lourdeau022404.htm (Letöltés ideje: 2017. július 18.).

The Guardian: NSA Prism program slides. In: The Guardian, 2013. november 1. URL: http://www.theguardian.com/world/interactive/2013/nov/01/prism-slides-nsa-document (Letöltés ideje: 2017. december 21.)

The Washington Post: Black Budget. In: The Washington Post, http://www.washingtonpost.com/wp-srv/special/national/black-budget/ (Letöltés dátuma: 2017. december 21.)

Top Website Ranking In: Similar Web. URL: https://www.similarweb.com/top-websites (Letöltés ideje: 2017.június 26.).

Varga Gergely (2010): A NATO új, lisszaboni stratégiai koncepciója. Nemzet és Biztonság, 2010/10. pp. 79–86.

Ványa László (2013): Irányított energiájú fegyverek. Nemzeti Közszolgálati Egyetem, Budapest. URL: http://uni-nke.hu/downloads/konyvtar/kovasz/vanya_jegyzet.pdf (Letöltés dátuma: 2017. július 19.)

Walker, Shaun (2015): Salutin' Putin: inside a Russian troll house. In: The Guardian, 2015. április 2. URL: http://www.theguardian.com/world/2015/apr/02/putin-kremlin-inside-russian-troll-house (Letöltés ideje: 2018. január 24.)

Warsaw Summit Communiqué, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016 (online), 2016. július 9. URL: https://ccdcoe.org/sites/default/files/documents/NATO-160709-WarsawSummitCommunique.pdf (Letöltés ideje: 2018. január 30.)

Webster, Stephen C. (2011): Revealed: Air Force ordered software to manage army of fake virtual people. In: The Raw Story, 2011. február 18. URL: http://www.rawstory.com/rs/2011/02/18/revealed-air-force-ordered-software-to-manage-army-of-fake-virtual-people/ (Letöltés ideje: 2018. január 20.)

Woolsey, James R. (2000): Why We Spy on Our Allies. In: The Wall Street Journal, 2000. március 17. URL: http://online.wsj.com/article/SB95326824311657269.html (Letöltés ideje: 2017. december 20.).

Zezima, Katie (2014): The Secret Service wants software that detects social media sarcasm. Yeah, sure it will work. In: Washington Post, 2014. június 3. URL: 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/ (Letöltés ideje: 2017. december 29.)

Zittrain, Jonathan (2014): Facebook Could Decide an Election Without Anyone Ever Finding Out – The scary future of digital gerrymandering—and how to prevent it. In: New Republic. URL: https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering (Letöltés ideje: 2018. január 25.)

A Nemzeti Közszolgálati Egyetem kiadványa

Kiadó:
Nemzeti Közszolgálati Egyetem
Közigazgatási Továbbképzési Intézet
www.uni-nke.hu

Felelős kiadó:
Prof. Dr. Kis Norbert rektorhelyettes
Címe: 1083 Budapest, Üllői út 82.

Kiadói szerkesztő:
Kelemen Dóra

Tördelőszerkesztő:
Mikes Vivien

ISBN 978-963-498-202-9 (elektronikus)