SZAKKOLLÉGIUMI TANULMÁNYKÖTET

2

NEMZETBIZTONSÁGI SZAKKOLLÉGIUM

NEMZETI KÖZSZOLGÁLATI EGYETEM
NEMZETBIZTONSÁGI SZAKKOLLÉGIUM

TANULMÁNYKÖTET
2.

Budapest, 2019

SZERKESZTŐK:

Kiss-Szemán Johanna
Barcza-Tóth Tímea
Dobák Imre

SZERZŐK:

Fodor Dóra
Kovács Márk Károly
Lőrincz Virág
Tóth Tamás
Krausz József
Bietry Kevin

A TANULMÁNYKÖTETBEN MEGJELENT ÍRÁSOKAT LEKTORÁLTÁK:

Dr. Forgács Balázs
Prof. Dr. Resperger István
Dr. Dobák Imre
Hegedűs Tamás
Dr. Hegedűs Ernő
Dr. Bács Zoltán György

A Nemzeti Közszolgálati Egyetem Nemzetbiztonsági Szakkollégiumának kiadása
https://nbi.uni-nke.hu/szakkollegium/kapcsolat
https://www.facebook.com/NemzetbiztonsagiSzakkollegium/

Előszó

„Tiszteld a múltat, hogy érthesd a jelent, és munkálkodhass a jövőn." - ahogyan Széchenyi István mondja. A hagyományok tiszteletével, a napjainkban zajló konfliktusok, események megértésével adódhat lehetőségünk arra, hogy az elkövetkezendő időkben, a jövőben, eredményesen munkálkodhassunk. A Szakkollégium a jövőért tenni akaró, képzett szakemberek oktatását, motiválását hivatott szorgalmazni.

A Nemzetbiztonsági Szakkollégium 2013-as megalakulása óta, immáron második alkalommal publikálja tanulmánykötetét, amelyben a tagok által elkészített kutatások, elemzések, értékelések jelennek meg. A Szakkollégium célja, hogy az egyetemi képzés mellett az érdeklődő hallgatóknak biztosítson lehetőséget arra, hogy nemzetbiztonsági témakörben bővíthessék ismereteiket, szakmai tudásukat gyarapítsák, majd az érdemi munkájuknak publikációs felületet teremtsen. Az alábbi tanulmánykötet, és a konferenciákon, versenyeken, pályázatokon szakkollégisták által elért további sikerek is bizonyítékai annak, hogy a tehetséggondozás eredményes.

A jelen tanulmánykötetben megjelenő írások, a szakkollégium tagjai által feldolgozott témák, amelyek a napjainkban zajló konfliktusok eseményeit elemzik vagy dolgozzák fel, érintve a kiberbiztonság, a terrorizmus, a radikalizmus, a nemzetközi szerződések és a modern hadviselés témakörét.

Kiss-Szemán Johanna

TARTALOMJEGYZÉK

LŐRINCZ VIRÁG: A XXI. SZÁZADI INFORMÁCIÓS ÉS KIBERHADVISELÉS KOCKÁZATAI

Bevezetés

A tanulmány célja a XXI. század információs társadalmában az internet és egyéb kommunikációs formák mögött megjelenő kockázatokra történő figyelemfelhívás. A hagyományos értelemben vett fegyverek nélküli hadviselésnek többnyire a számítógépes rendszereken, számítógépes hálózatokon keresztül, a kibertérben végzett támadások jelentik az egyik leghatékonyabb és legnépszerűbb módját, mégpedig a technológiáját tekintve relatív olcsósága, egyszerűsége és az elkövetőket védő anonimitása miatt. Jelen tanulmány konkrét példákon keresztül fogalmaz meg gondolatokat a XXI. századi információs tér biztonsági kihívásaihoz.

Az információs háború

"Az információ hatalom" - ez tekinthető talán az információs háború egyik kulcsának, amelynek megértéséhez elsőként az információs társadalom körülírására térek ki. Az információs társadalmat az internet és a különböző kommunikációs eszközök XXI. századra történő robbanásszerű elterjedése, a digitalizáció térhódítása, a technológiai fejlődés és az információ, mint olyan, elsődlegessé válása jellemzi. Ennek megfelelően egyre fontosabbá válik az információk megszerzése, feldolgozása, kezelése és a tanulmány szempontjából leginkább releváns elemként, az információk védelme. Ezzel párhuzamosan a katonai tevékenységekre és a hadseregek műveleteire is nagy hatással volt az információtechnológia, a technika fejlődésével az információ kulcsszerepet kapott. A XX. századi háborúk és forradalmak után kérdésként merülhet fel, hogy a XXI. század vajon a kiberháborúk és információs forradalmak kora?[1]

Az kétségkívül leszögezhető, hogy az információs háború a XXI. század meghatározó jelensége, noha az információs műveletek egyes területei már korábban is megjelentek a katonai műveletekben, illetve a gazdasági, politikai életben is. Gondolhatunk itt az elektronikai eszközök zavarására, a felderítésre és megtévesztésre, vagy a lélektani hadviselésre. A XX. század háborús eseményei során ezek a módszerek jelentős fejlődésen mentek keresztül és folyamatosan tökéletesedtek a korabeli technológiai fejlettségnek megfelelően.

Az információs hadviselés fő jellemzői:

- információk gyűjtése
- a gyűjtött információk hitelességének ellenőrzése
- tömegek dezinformálása az ellenség megtévesztése érdekében
- az ellenség birtokában lévő információk megsemmisítése, megmásítása

[1] DANNREUTHER Roland: Nemzetközi biztonság (Budapest, Antall József Tudásközpont, 2016), pp. 308- 315.

- az ellenség információgyűjtő tevékenységének akadályozása. [2]

Az információs hadviselést különböző szempontok alapján lehet típusokba sorolni. Ezek közül kiemelem Martin C. Libicki nevéhez köthető megközelítést, amely az alkalmazott eszközök szerint végzi a csoportosítást. Így megkülönböztethető a vezetés és irányítás hatáskörében történő hadviselés, melynek célja az irányító és az irányított közötti információáramlás akadályozása, továbbá az adatszerzésre irányuló hadviselés, melynek ékes példája az ECHELON[3], amely globális szintű kommunikáció ellenőrzésére hivatott, az elektronikus hadviselés, mely az ellenség elektronikai eszközeiben okoz kárt, a pszichológiai, mely célzott üzenetet hordozva kívánja hallgatói vagy nézői érzelmeit befolyásolni, valamint a hacker, a gazdasági és a kiberhadviselés. Ezek természetesen szervesen összefüggnek, nem különíthetők el teljesen egymástól.

Az információs hadviselést résztvevői, szereplői, illetve azok hatóköre szerint is osztályozhatjuk. Ez az értelmezés Winn Schwartau Information Warfare (1996) című könyvében jelent meg. Ez alapján az alábbi három csoport szerint osztályozhatók a résztvevők:

- személyes információs hadviselés,
- vállalati információs hadviselés és
- kormányzati információs hadviselés.

A személyes információs hadviselés során a támadás célja egy adott ember, akinek személyes adatai sérülhetnek vagy megsemmisülhetnek (például személyiséglopás esetén). A vállalati szintű információs hadviselésre az ipari kémkedés jó példa, amely során a versengő vállalatok vagy cégek intéznek támadást egymással szemben. A legmagasabb, kormányzati szintű információs hadviselésre pedig a 2007-ben Észtország ellen elkövetett kibertámadás hozható fel példaként. Ennek során összehangolt túlterheléses támadások terhelték az észt kritikus infrastruktúrákat és kormányzati oldalakat. [4]

Összefoglalva tehát megállapítható, hogy az információs hadviselés az információ, és ezáltal a hatalom birtoklásáért információs eszközökkel, valamint kognitív támadások útján, az információs térben folytatott konfliktusok összessége[5]. A kibertér alkalmazása

[2] REISMAN, Michael W. – ANTONIOU, Chris T.: The laws of war: a comprehensive collection of primary documents on international laws governing armed conflict (New York, 1994) című könyve alapján

[3] Az ECHELON műholdas lehallgató rendszer, amely a legkülönbözőbb kommunikációs eszközök (telefon, fax, Internet...) lehallgatására alkalmas. Öt ország (USA, Kanada, Ausztrália, Nagy-Britannia és Új-Zéland) együttműködésével épült ki az egész emberiség kommunikációs hálózatának forgalmát figyelő, szigorúan titkos műholdak, földi megfigyelő bázisok, kémhajók és tengeralattjárók integrált rendszere. (GYURÁK Gábor: A kriptográfia és a hírszerzés hadtudományi gyökerei, Hadtudományi szemle 2014. VII. évfolyam 3. szám)

[4] BÁNYÁSZ Péter – ORBÓK Ákos: A NATO kibervédelmi politikája és kritikus infrastruktúra védelme a közösségi média tükrében http://mhtt.eu/hadtudomany/2013/2013_elektronikus/2013_e_Banyasz_Peter_Orbok_Akos.pdf (Letöltés ideje: 2019.02.18.)

[5] FEKETE Csanád: Konfliktusok az információs térben, Az információs hadviselés fejlődése és aktuális kérdései, Katonai Nemzetbiztonsági Szolgálat tudományos-szakmai folyóirata, XVI. évfolyam 2. szám p.70-71.

mellett napjainkban egyre jelentősebb szerepet kap a tömegmédia is (pl.: hírlapok, TV, rádió, közösségi média). Ezek jelentősége abban rejlik, hogy a hihetetlen sebességgel terjedő hírek mellett, a szabad véleményformálás lehetősége is megjelenik. Az álhírek, dezinformálás különösen veszélyes a közösségi oldalak által lehetővé tett közösségi önszerveződés tekintetében.

Az információs hadviselés összetettsége - a kiberhadviselés

Az információs hadviselés összetett jelenség, azonban az információs tér a XXI. századra egyre inkább a számítógép-rendszerekre és hálózatokra korlátozódik, hiszen valamennyi politikai, katonai rendszer rá van szorulva a modern technológia vívmányaira. Ezáltal minden személy vagy rendszer, amely ennek az információs térnek a része, célponttá válhat. A kibertérben számos kártékony program szolgál eszközül a különböző támadások végrehajtására. Ezek lehetnek kártékony szoftverek, melyek információkat gyűjtenek, átalakítanak, megsemmisítenek vagy akár tönkre is teszik az ellenséges rendszert.

A következőkben ismertetett két példa esetében nem az információk megszerzése, feldolgozása, továbbítása vagy hamis információk terjesztése volt kizárólag a cél, hanem mindezek eszközéül szolgáltak egy nagyobb volumenű károkozásnak.

1982-ben felrobbant egy szibériai szovjet gázvezeték. A robbanás nem véletlen esemény volt, hanem a Szovjetunió elleni gazdasági hadviselés része. Az ügy hátterében az állt, hogy a gázvezetékek felügyeleti szoftvere egy trójai vírussal volt "kibővítve", melyet a CIA által megbízott programozók írtak. Ez olyan hibákat hozott létre a szivattyúk és szelepek szabályozásában, amely robbanáshoz vezetett. A valaha volt legnagyobb nem nukleáris robbanás következett be, amelyet a világűrből is látni lehetett. Az időpontot és a résztvevő két államot tekintve a hidegháború utolsó szakaszáról van szó, amikor a technológia fejlődésével a kibertér nem hadszíntér volt, hanem harci technika. [6]

2010-ben a Stuxnet által új mérföldkőhöz érkezett a számítógépes vírusok, "férgek" kora.[7] Ez az új féreg kifejezetten az ipari folyamatirányító rendszerek ellen lett kifejlesztve, tehát a kritikus infrastruktúrára nézve jelentett fenyegetést. Működésének lényege az volt, hogy olyan nagy sebességű motorok frekvencia átalakítóira bukkanva aktivizálódott, melyek csak az iráni urándúsítókban voltak fellelhetők. A Stuxnet megfertőzte tehát az iráni Natanz nukleáris létesítményének rendszerét, hozzávetőlegesen két év hátrányba kényszerítette az iráni atomprogramot. A támadásért senki nem vállalta a felelősséget, de nagy valószínűséggel az USA és Izrael áll a háttérben, hiszen ez a két állam a legérdekeltebb az iráni atomprogramot akadályozó vírus kitervelésében és megvalósításában.[8]

Az említett két eset csupán példaként szolgál a számítógépes-hálózatok sebezhetőségére. A támadások kivédésére számos módszer és eljárás létezik, ezek célja a saját hálózat védelmének megszervezése a jogosulatlan behatolókkal szemben. A

[6] BERKI Gábor: A kibertéri konfliktusok változásai, Hadmérnök, VIII. évfolyam 1. szám – 2013. március
[7] DANNREUTHER i.m.
[8] Ezek a gondolatok Ralph Langner hamburgi vírusszakértő következtetéseire épülnek

védelemnek beszélhetünk passzív és aktív módszereiről is. A passzív eszközök közé tartoznak például a tűzfalak, a vírusirtók, a hozzáférés-szabályozás és a behatolásdetektálás és -megelőzés. Az aktív módszerek eszközei a megelőző támadások, az ellentámadások és az aktív megtévesztés.[9]

A tömegmédia

Az információs hadszíntér egészére tekintve a kibertér csupán az egyik terület, de nem az egyetlen. A tömegmédia napi szinten történő használata során mi is ráébredhetünk arra, hogy mekkora kockázata lehet annak, ha nem áll rendelkezésre a szükséges információ, vagy ami napjainkban még nagyobb problémát jelent, ha nem valós információkkal próbálják befolyásolni az embereket. A tömegmédia által az információt befogadók manipulálásáról lehet szó anélkül, hogy a megtévesztett tisztában lenne azzal, hogy áldozattá válik. Eredményképpen a célpont tudat alatt akár saját érdeke ellen, de mindenképpen az információs háborút vívók érdekében cselekszik. A tömegmédiára helyezve a hangsúlyt, az információs hadviselés legfőbb elemei a propaganda általi manipuláció, az álhírek terjesztése, esetleg igaz hírek beállítása hamisnak, TV közvetítés vagy rádióadás, internet blokkolása, online social media megbénítása stb. Ezekkel az eszközökkel elérhető az információs fölény megszerzése az ellenféllel szemben.

A tömegmédia befolyásoló erejére helyezve a hangsúlyt, Herbert Kelman szociálpszichológus az alábbi három formáját fogalmazta meg a társadalmi befolyásolásnak:

- megfelelés,
- azonosulás, valamint
- internalizáció.

Ebben az értelmezésben a megfelelés azt jelenti, hogy a személy amellett ért egyet a befolyásolóval, hogy közben megtartja a saját véleményét. Ha a befolyásoló információ megszűnik, a személy visszatér saját hozzáállásához, tehát ez a módszer csupán rövid távon vált ki hatást. Az azonosulás ennél egy fokkal többet ér el, hiszen célja, hogy hosszútávon befolyásoljon. Az egyén azért teszi magáévá a befolyásoló véleményét, mert hozzá hasonlóvá akar válni. Az internalizáció során a befolyásolás olyan szintjéről beszélhetünk, amikor a befolyásolt személy teljes mértékben elfogadja, és ellenőrzés nélkül követi mások nézeteit és értékeit.

Összefoglalva tehát, az információs térben megszerzett információs fölény nem csupán a technikai képességekre korlátozódik, hanem jelentős mértékben támaszkodik a befolyásolóképességre is. Az utóbbi egyre nagyobb szerephez jut az internetes hírportálok és közösségi média használata által.

[9] HAIG Zsolt: Információs műveletek a kibertérben (Budapest, Dialóg Campus Kiadó, 2018)

A WikiLeaks ügy

A WikiLeaks nevű weboldalt 2006-ban hozta létre az ausztrál származású Julian Assange. Az ő szavaival élve a cél egy jobb, titkok nélküli világ megteremtése volt, ez vezérelte a közel negyedmillió amerikai titkos katonai dokumentum és diplomaták közt váltott üzenet kiszivárogtatásakor. Azt hirdette, hogy ezáltal a sajtószabadságot segíti és a cenzúrázatlan igazságot deríti fel. 2007-ben a guantanamói[10] foglyokról, illetve a börtönszigetről kerültek nyilvánosságra titkos adatok. 2008-ban nyilvánosságra hozta a Brit Nemzeti Párt tagjainak listáját személyes adataikkal együtt. Az információkat titkos források továbbították a WikiLeaks-nek, amely teljes anonimitást biztosított cserébe.[11]

Az egyik legnagyobb port kavaró dokumentum kiszivárogtatására 2010-ben került sor. Egy videót tettek közzé, amelyben az amerikai hadsereg katonai helikopteréből tüzet nyitottak két Reuters[12] újságíróra és iraki civilekre is 2007-ben az iraki háború során. Szintén 2010-ben 92 000 dokumentum vált mindenki számára elérhetővé az afganisztáni háború (2004-2009) titkos katonai aktái közül. Ennek következtében szólította föl először Barack Obama többek közt Nagy-Britanniát, Németországot és Ausztráliát, hogy tegyenek büntetőjogi intézkedéseket Julian Assangedzsal szemben. A több százezer oldalnyi titkos katonai és külügyminisztériumi adat ellopásával Bradley (ma már: Chelsea) Manning amerikai közlegényt gyanúsították. A 2010-ben nyilvánosságra hozott titkos dokumentumok publikálásához a WikiLeaks-nek a nagy világlapok segítségére is szüksége volt. Ezek közé tartozott a *The Guardian*, a *The New York Times* és a *Der Spiegel*. A nagy presztízsű lapok és a WikiLeaks álláspontja abban tért el jelentősen, hogy előbbiek ragaszkodtak az adatok megszerkesztéséhez, hiszen a hadi jelentések informátorokat leplezhettek le, az életüket veszélyeztetve ezzel, míg Assange csonkítatlan publikációt akart.[13]

Kezdetben a WikiLeaks számos pénzügyi támogatást is szerzett, 2010-ben azonban Julian Assange bankszámláját befagyasztották és az utalásokat kezelő Mastercard és Visa is blokkolta a szervezet számára érkező összegekhez való hozzáférést, illegális tevékenységre hivatkozva.[14]

Ezután megkezdődött az érintett pénzintézetekkel szemben is a kiberhadviselés. A WikiLeaks-szel szimpatizáló hackercsoport, az Anonymus csoport tagjai DoS (Denial of Service – szolgáltatásmegtagadás) támadásokkal terhelték a pénzintézetek internetes rendszereit. Ezenkívül más eszközöket is igénybe vettek. Ingyenesen elérhető

[10] Az amerikai kormány a 2001. szeptember 11-i egyesült államokbeli terrortámadások után hozta létre a börtöntábort Kuba szigetén (amerikai fennhatóság alatt álló haditengerészeti támaszpont), ahol a terrorcselekménynel vádolt személyeket bírói ítélet nélkül tartották fogva és embertelen bánásmódban részesítették, forrás: https://mandiner.hu/cikk/20160223_elkeszult_a_terv_a_guantanamoi_borton_bezarasara (Letöltés ideje: 2019.02.12.)

[11] ANTIKAINEN, Anita: Diplomatic Transparency: A Wikileaks Case Study (Tallinn, 2015)

[12] londoni székhelyű világhírügynökség

[13] ANTIKAINEN i. m.

[14] KOVÁCS László: Kiberháború? Internetes támadások a Wikileaks ellen és mellett, Nemzet és biztonság biztonságpolitikai szemle, 2011/1 szám

faxszolgáltatásokon keresztül számos faxszámra küldték szét a kiszivárogtatott dokumentumokat London számos pontján.[15]

2010-ben magyar vonatkozású diplomáciai táviratok is kiszivárogtak. Ezek többek között a 2008-as grúz-dél-oszét háborúval, illetve a magyar nukleáris energiával álltak kapcsolatban.[16]

2012-ben végül Svédország majd az USA is kérték a londoni ecuadori nagykövetségről Julian Assange kiadását, a férfi azonban menedéket kapott a követségen. 2017-ben már az ecuadori állampolgárságot is megszerezte és Svédország ejtette vele szemben a korábban emelt vádat szexuális zaklatásért.[17]

A weboldalon közzétett információk egyértelműen felkeltették az emberek figyelmét, telefonos alkalmazást is létrehoztak, melyen elérhetőek voltak az oldal legfrissebb hírei. Ezt az AppleStore néhány napon belül eltávolította, arra hivatkozva, hogy az alkalmazás szabályellenes.[18]

Összefoglalva a WikiLeaks ügyet kétségtelen, hogy a demokráciának a véleménynyilvánítás és a sajtószabadság elengedhetetlen kelléke, de ez nem összekeverhető az államtitkok, diplomáciai levelezések válogatás nélküli megosztására az interneten. Az *évszázad kiszivárogtatásának* is nevezett akció, illetve mind a mellette és az ellene irányuló támadások azt jelzik, hogy minden olyan ország, amely fejlett informatikai hálózattal és médiaplatformokkal rendelkezik, ki van téve ezeknek a veszélyeknek. A kérdés tehát, amelyet a WikiLeaks, és a körülötte kibontakozó botrány felvet, hogy meddig szabad elmenni a sajtószabadság és véleménynyilvánítás terén, és hol kell meghúzni a határt az államtitkok védelme érdekében?

Dezinformálás - az amerikai (2016) és a francia választások (2017)

A dezinformálás lényege valamilyen cél érdekében manipulatív tartalmak közzététele. Sokféle szempontból lehet az ilyen jellegű tevékenységeket csoportosítani. Ezek közül Jacek Borechi rendszerezését emelem ki. Szerinte az első csoportba az olvasók megtévesztését célzó hamisított dokumentumok, a hivatalos vagy illegális úton megszerzett és tartalmuk megváltoztatása után publikált adatok tartoznak. Másik csoportba sorolja a "társadalmi manipulációra" épülő eszközöket, melyek célja, hogy egyes érdekcsoportoknak követőket szerezzen trollok, botok vagy propaganda által. A harmadik csoportba pedig az előbb felsorolt kettő elegye tartozik.

Egy tipikus dezinformációs kampány modelljét három fázisra osztva lehet ideálisan ábrázolni:

[15] BERKI Gábor i. m.
[16] Wikileaks-ügy: Magyar dokumentumok egy orosz lapban, forrás: https://honvedelem.hu/cikk/ikileaks-ugy_magyar_dokumentumok_egy_orosz_lapban (Letöltés ideje: 2019.02.18.)
[17] https://edition.cnn.com/2013/01/18/world/julian-assange-fast-facts/index.html (Letöltés ideje: 2019.02.19.)
[18] https://techcrunch.com/2010/12/20/apple-removes-wikileaks-app-from-app-store/?guccounter=1&guce_referrer_us=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_cs=bRIA7GNBmPLjykdM3rBQ5w (Letöltés ideje: 2019.02.19.)

1. A dezinformáló fél érdekeit szolgáló hivatalos, illetve a félhivatalos médiák vagy hackerek "kiszivárogtatott" információkat tesznek közzé. Ez mindenképpen úgy történik, hogy az emberek figyelmét megragadja.
2. Az ilyen módon megjelent álhíreket ún. trollok és automata kommentíró botok[19] rendszeresen terjesztik, esetlegesen félelem keltő hozzászólásokat is megosztanak a hírekkel kapcsolatban.
3. A gyorsan terjedő információkat ezután átveszik a különböző hírforrások, blogok, a dezinformációs tevékenységet valamilyen okból támogató média és a "hasznos idióták".

Az információs hadviselés nagysága abban rejlik, ha valaki az interneten, a közösségi oldalakon, különböző hírportálokon keresztül a politikát is befolyásolni tudja. Erre nagyszerű példa a 2016-os amerikai elnökválasztás.

Az elnökválasztás eseményeit nagyban befolyásolták az internetes támadások, melyek sok esetben azonban nem bizonyíthatók.[20] Az információs műveletek során elemzéseket és e-maileket loptak el Donald Trumpról, levelezéseket szivárogtattak ki Hilary Clintonról és bizalmasáról, John Podestaról és a Demokrata Nemzeti Bizottság rendszerébe betörve a vezetők személyes adatait hozták nyilvánosságra. Noha a gyanúsított hacker csoportok orosz kormány pártiak, Putyin tagadott, Trump szerint a kínaiak is lehettek. A kiszivárgott információk mindenesetre Trump pozícióját erősítették Clintonnal szemben. A titkos információk közül sokat a hacktivista WikiLeaks oldalán oszottak meg, a helyzet milyenségét tekintve Julian Assange (WikiLeaks alapítója) is szót kapott, aki tagadta, hogy orosz kormányzati forrásokból kapták volna a DNC (Democratic National Comittee) adatait.[21] A DNC tagjairól szóló adatok ellopása feltehetőleg egy nagyon egyszerű adatlopási modell alapján történt meg.

Ennek első lépése az ún. *spearphising,* amely célzott üzenetet jelent e-mailben, vagy a keresetthez hasonló tartalmú oldalra történő átirányítás által, mindössze az emberi hiszékenységre alapozva. Második lépésben a kártékony program (malware) a megnyitott üzenetben vagy oldalon általában csatolt fájlként jelenik meg, jellemzően Word vagy PDF formátumban. Végezetül a program megnyitása által megtörténik a fertőzés, mely hozzáférést biztosít a keresett adatokhoz.[22]

Milyen szerepe volt ebben a WikiLeaks-nek?

Majdnem biztossággal állítható tehát, hogy Moszkva szivárogtatott a WikiLeaksen keresztül, mégpedig annak megbízhatósága és a világ szemében való hitelessége miatt. A

[19] Automatikus, felügyelet nélküli működésre tervezett program (robot). A botok általában felügyeleti vagy adatgyűjtő funkciókat látnak el, forrás: https://pcforum.hu/szotar/?term=bot&tm=miaz (Letöltés ideje: 2019.02.12.)
[20] KOVÁCS László - KRASZNAY Csaba: "Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során, SVKK Elemzések 2017/9.
[21] Political Capital és Friedrich-Ebert-Stiftung: Az orosz választási dezinformáció elleni stratégiák kommunikációs lehetőségei Magyarországon (Budapest, 2017)
[22] KOVÁCS - KRASZNAY i. m.

weboldal alapítója, Julian Assange rendszeres szereplője az orosz forrásból finanszírozott RT (Russia Today) TV adónak, mely szintén példája az ausztrál férfi és Moszkva feltehetőleg jó kapcsolatának.

Mindez tehát tökéletes példa arra, hogyan lehet közvetve, pl. álhírkampánnyal ekkora volumenű eseményt befolyásolni.

Ehhez hasonló eset a 2017-es francia választások során zajlott információs hadviselés. Két nappal a választás előtt Emmanuel Macron e-mailjei kerültek ki az internetre adatlopás eredményeként. Emellett Oroszország különböző álhíreket terjesztett a volt szocialista párti miniszterről, és minden erejével a szélsőjobboldali Marine Le Pent támogatta. Az orosz beavatkozási kísérlet azonban itt már kevésbé ért célba, melynek oka lehetett a bevetett ügynökök alacsonyabb szintű nyelvtudása, vagy még valószínűbb, hogy a Macron-stáb jobban fel volt készülve ilyen jellegű támadásra. Közel harmincezer hamis Facebook fiókot töröltek le és hamis e-mail címekkel és oldalakkal tévesztették meg a hackereket. Másrészt a francia sajtó a választás előtti kampánycsendben nem igazán foglalkozott a kiszivárogtatott anyagokkal.[23]

A szintén 2017-ben zajlott német választások már azt bizonyították, hogy az (orosz) információs támadások kellő felkészültséggel kivédhetők. Angela Merkel a parlamentben is fellépett az álhírekkel szemben, ráadásul olyan jogszabályt léptettek hatályba, amely komoly pénzbüntetés terhe mellett kötelezi a médiaplatformokat a hamis hírek eltávolítására.

A felhozott példák az elmúlt évek legnagyobb port kavaró eseményei voltak az információs hadviselés terén, és nem lehet nem észrevenni Oroszország aktív részvételét a történtekben. Az orosz információs befolyás főként a balti államokban veszélyes, hiszen a nagyszámú orosz nyelven beszélő kisebbség szinte hazai terepet jelent. Emellett Oroszország érdekeit a nemzetközi médiában a nyugati típusú, technológiailag színvonalas Sputnik és a már említett RT képviseli.[24] Főként a volt szovjet tagállamok vagy más baráti országokat látnak el oroszbarát médiaanyagokkal. Ezáltal a kelet-közép-európai államok a legsebezhetőbb láncszemek. A 2015-ben alapított NATO rigai Stratégiai Kommunikációs Kiválósági Központjának éppen ezért egyik fő kutatási területe az orosz dezinformáció.

Összefoglalva, számos módon lehet dezinformálni egy adott embercsoportot, nincsen egységes forma, a befogadók igényei szerint testreszabhatók, ebből fakad kiemelt veszélyessége. Az információs háborúval szembeni védekezés, propaganda elleni technológiai, intézményes fellépés lehetőségei közé tartozik a közösségi médiaplatformok együttműködése. Ennek egyik példája, hogy a Facebook, Youtube, Microsoft, Twitter közt létezik egy megállapodás, ún. "hamis hír szűrő", melynek értelmében megvizsgálják, és megfelelő alternatívákat dolgoznak ki a gyűlöletbeszéd miatt megjelölt bejegyzésekre. Továbbá a Google is kapcsolatban áll a különböző

[23] https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/(Letöltés ideje: 2019.02.21.)
[24] KOVÁCS - KRASZNAY i. m.

tényellenőrző cégekkel. Azonban nem tünteti el az álhírt, hanem alternatív, cáfoló híreket hoz fel mellette.[25]

Következtetések

A tanulmány célja, hogy rávilágítson az elmúlt évtizedek néhány legnagyobb port kavaró eseményén keresztül az információs hadviselés kiterjedtségére, összetettségére és magában hordozott veszélyeire. A múltban és jelenben felhasznált eszközök a technológiai fejlődéssel párhuzamosan a jövőben folyamatosan javulni fognak, és feltehetőleg számos új lehetőség is rendelkezésre fog állni. Jelenleg a kibertérben zajló hackertámadások, és a közösségi platformokon megfigyelhető dezinformáció-áradat tekinthető véleményem szerint a leghatékonyabb módnak, de mit hoz vajon a jövő? Az egyre kifinomultabb és „okosabb" technológiai vívmányok dinamikus fejlődése várhatóan jóval nagyobb károkat lesz képes okozni. A kibertérben felgyűlő adatok mennyisége folyamatosan nő, ennek megfelelően növekvő tudatosságra és biztonsági intézkedésekre van szükség a megvédésük érdekében.

[25] Political Capital és Friedrich-Ebert-Stiftung: i. m.

Felhasznált irodalom

1. BERKI Gábor: A kibertéri konfliktusok változásai, Hadmérnök, VIII. évfolyam 1. szám – 2013. március
2. DANNREUTHER Roland: Nemzetközi biztonság (Budapest, Antall József Tudásközpont, 2016), pp. 308- 315.
3. DAMJANOVIĆ, Dragan Z.: Types of information warfare and examples of malicious programs of information warfare, forrás: https://scindeks-clanci.ceon.rs/data/pdf/0042-8469/2017/0042-84691704044D.pdf (Letöltés ideje: 2019.02.04.)
4. HAIG Zsolt: Információs műveletek a kibertérben (Budapest, Dialóg Campus Kiadó, 2018)
5. http://hu.iranyitok.wikia.com/wiki/Információs-háború (Letöltés ideje: 2019.02.04.)
6. http://www.politicalcapital.hu/hireink.php?article_read=1&article_id=2328 (Letöltés ideje: 2019.02.04.)
7. https://alapblog.hu/az-informacios-hadviseles-szerepe-az-orosz-strategiaban/ (Letöltés ideje: 2019.02.04.)
8. https://edition.cnn.com/2013/01/18/world/julian-assange-fast-facts/index.html (Letöltés ideje: 2019.02.04.)
9. https://honvedelem.hu/cikk/ikileaks-ugy_magyar_dokumentumok_egy_orosz_lapban (Letöltés ideje: 2019.02.04.)
10. https://kiberhaboru.hu (Letöltés ideje: 2019.02.04.)
11. https://www.wired.com/2017/05/nsa-director-confirms-russia-hacked-french-election-infrastructure/ (Letöltés ideje: 2019.02.04.)
12. KOVÁCS László - KRASZNAY Csaba: "Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során, SVKK Elemzések 2017/9.
13. KOVÁCS László: Kiberháború? Internetes támadások a Wikileaks ellen és mellett, Nemzet és biztonság biztonságpolitikai szemle, 2011/1 szám
14. LIBICKI, Martin C.: What is information warfare? (National Defense University, Institute for National Strategic Studies, 1995)
15. Political Capital és Friedrich-Ebert-Stiftung Budapest: Az orosz választási dezinformáció elleni stratégiák kommunikációs lehetőségei Magyarországon (Budapest, 2017)