Stratégiai Védelmi Kutatóközpont
ELEMZÉSEK 2017/9.

2017. március 30.

Kovács László – Krasznay Csaba:[1] „Mert övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során

Vezetői összefoglaló

- Az amerikai közvélemény többsége szerint az orosz kormányzat közvetve, információs műveletekkel és kiberkémkedéssel befolyásolni próbálta az elnökválasztás eredményét. Egyetértés van abban is, hogy az orosz információs műveletek kevéssé befolyásolták a választók akaratát.
- Ha valaki részben vagy egészben befolyásolni tudja az interneten, a közösségi média felületein a híreket, a médiaeseményeket és tevékenységeket, az egy olyan nagy volumenű eseményre is hatással tud lenni, mint az amerikai elnökválasztás.
- Már napjainkban is, de a közeljövőben még inkább számolni kell az ilyen tevékenységgel. Az internet globális volta, a közösségi médiumok felhasználóinak tömegei magától értetődő módon nyújtják az eszközt a befolyásoláshoz, a gazdasági vagy politikai viszonyok alakításához. Ez már nemcsak informatikai biztonsági megoldásokat igényel, hanem nemzetbiztonsági válaszokat is, akár stratégiai irányváltásokkal.

A 2016-os amerikai elnökválasztásban, illetve az azt megelőző kampány során minden eddiginél nagyobb szerepet kapott az a törekvés, hogy külföldi államok különböző – elsősorban informatikai támadásokkal és médiaeszközökkel – befolyásolják a választások eredményét. A média különösen sokat foglalkozott a kérdéssel mind az az Egyesült Államokban, mind Európában. Ugyanakkor tényeken alapuló, bizonyítékokkal alátámasztott, az elnökválasztást érdemben befolyásoló tényezőkről keveset hallhattunk. Jelen írás azokat az informatikai támadásokat és különböző médiaműveleteket igyekszik kronológiai sorrendbe állítani és elemezni, amelyek hatással lehettek az elnökválasztásra.

Hackerek az amerikai választásokban

A 2016-os amerikai elnökválasztás eseményeiben komoly szerepet játszottak az internetes támadások. Ezek a hackerek által elkövetett internetes akciók azonban számos esetben nem vagy csak részben bizonyíthatók. Ugyanakkor az akciók volumene mindenképpen átlépte azt a küszöböt, amikor érdemes megvizsgálni azt, hogy az internetes támadások hogyan és milyen mértékben tudnak befolyásolni egy olyan eseményt, amely elviekben a világ egyik legjobban szervezett és legjobban felügyelt választásához kapcsolódik. Mindenekelőtt azért, mert az elnökválasztási kampány során napvilágot látott internetes támadásokról szóló hírek kronológiájának ismeretében pontosabb áttekintést kaphatunk arról, hogy milyen módon és sorrendben hathattak az egyes kiberműveletek a szavazás végeredményére. Az alábbiakban ismertetett kronológia a CNN gyűjtésére támaszkodik.[2]

- 2016. június 14.: A *The Washington Post* elsőként számol be arról, hogy feltételezhetően az orosz kormányzathoz közel álló hackerek betörtek a Demokrata Nemzeti Bizottság (Democratic National Committee – DNC) számítógépes rendszereibe, és onnan Donald Trumpról készült elemzéseket, valamint egymás között váltott e-maileket és chatszövegeket loptak el. Az orosz fél tagadta a vádakat, és a hivatalos amerikai források sem erősítették meg egyértelműen az orosz kormányzati kapcsolatot.

[1] Prof. Dr. Kovács László (kovacs.laszlo@uni-nke.hu), a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Karának egyetemi tanára; Dr. Krasznay Csaba krasznay.csaba@uni-nke.hu, a Nemzeti Közszolgálati Egyetem Államtudományi és Közigazgatási Karának egyetemi adjunktusa.
[2] 2016 Presidential Campaign Hacking Fast Facts, [online], 2017. 03. 20. Forrás: cnn.com [2017. 03. 29].

- 2016. június 15.: A DNC által megbízott kiberbiztonsági cég saját honlapján jelenti be, hogy vizsgálatai szerint a támadásokat a „Cozy Bear" és a „Fancy Bear" néven ismert orosz hackercsoportok hajtották végre. Ezen csoportokat már korábban az orosz kormányzathoz közel állónak tartották. A vádakra reagálva feltűnik egy magát „Guccifer 2.0"-nak nevező hacker, aki magára vállalja a támadást, egyben jelzi, hogy az ellopott adatokat továbbította a Wikileaks kiszivárogtató oldalnak. Donald Trump is megjelenik a saját elméletével, miszerint a demokraták önbetörést hajtottak végre, ezzel próbálva elterelni a figyelmet Hillary Clinton kiszivárgott levelezéséről.
- 2016. július 22.: A Demokrata Nemzeti Konvenció előtt pár nappal a Wikileaks közel 20 000 e-mailt hoz nyilvánosságra, melyek a DNC szerveréről származnak. Ebből kiderül, hogy a DNC vezetője, Debbie Wasserman Schultz Clinton mellett kampányol, ezzel hátrányba hozva a másik jelöltet, Bernie Sanderst.
- 2016. július 25.: Az FBI bejelenti, hogy nyomozást indít a DNC szervereinek feltörésével kapcsolatban. Névtelen kormányzati források ekkor már egyértelműen utalnak a támadás orosz kormányzati hátterére.
- 2016. augusztus 12.: Nyilvánosságra kerül bizonyos DNC-vezetők, így Nancy Pelosi telefonszáma és privát e-mail címe. A demokrata vezetők ezután folyamatosan offenzív üzeneteket kapnak ezeken a csatornákon.
- 2016. szeptember 1.: Vlagyimir Putyin a *Bloomberg*nek adott interjúja során kijelenti, hogy személy szerint sem neki, sem az orosz kormánynak nincs kapcsolata a hackerekkel. Egyben jelzi, hogy a tettesek kiléténél sokkal fontosabb a kiszivárgott információ, melyek nagyon fontosak az amerikai választók számára.
- 2016. szeptember 22.: Dianne Feinstein és Adam Schiff demokrata szenátorok közös nyilatkozatot adnak ki, melyben kijelentik, hogy a titkosszolgálati információk alapján a támadás mögött orosz titkosszolgálati szervezetek állnak, és felszólítják Putyint a befolyásoló tevékenységek beszüntetésére.
- 2016. szeptember 26.: Az elnöki vita során Trump megkérdőjelezi azt, hogy oroszok állnak a DNC-támadás mögött. Véleménye szerint a kínaiak vagy bárki más is lehetett az elkövető.
- 2016. október–november: A Wikileaks további 58 000 üzenetet közöl, melyek John Podestának, Clinton kampányvezetőjének feltört e-mail fiókjából származnak.
- 2016. október 7.: A Belbiztonsági Minisztérium (Department of Homeland Security – DHS) és a választás biztonságáért felelős Nemzeti Hírszerzési Igazgató (Director of National Intelligence – DNI) közös nyilatkozatban nevesíti az orosz kormányt a támadás elkövetésével összefüggésben.
- 2016. november 29.: Demokrata szenátorok egy csoportja levélben kéri Barack Obama elnököt arra, hogy hozza nyilvánosságra az orosz kormányzat amerikai választásokkal kapcsolatos szándékairól összegyűjtött információkat.
- 2016. december 9.: A *The Washington Post* cikke szerint a CIA biztos abban, hogy az orosz kormányzat szándéka Trump erősítése Clintonnal szemben. Trump nevetségesnek tartja és visszautasítja ezt a véleményt. Obama elnök 2008-ig visszamenően elrendeli a politikai eseményekkel kapcsolatos kiberbiztonsági tevékenységek kivizsgálását. Az orosz külügyminiszter szóvivője kifejezi kétkedését a vizsgálattal kapcsolatban, és azt kéri az amerikai féltől, hogy osszák meg velük az információkat.
- 2016. december 11.: A CNN forrásai szerint az amerikai hírszerző ügynökségek egyetértenek abban, hogy Oroszországnak nagy szerepe van a hackertámadásokban, de a CIA és az FBI nem ért egyet a motivációt illetően. Míg a CIA értékelése szerint a támadások célja Clinton lejáratása és ezzel Trump segítése, az FBI nem talált bizonyítékot arra, hogy a cél a republikánus jelölt megválasztásának elősegítése lenne. Ekkor derül ki az is, hogy a támadók a Republikánus Nemzeti Bizottságtól is sikerrel szereztek adatokat.
- 2016. december 13.: A *The New York Times* nyilvánosságra hozza azt, hogy a DNC annak ellenére nem reagált a támadásokra időben, hogy az első jelzéseket már 2015 szeptemberében megkapták. A beszámoló szerint adathalász e-mailek és kommunikációs hibák vezettek a sikeres támadáshoz, valamint azt is megemlítik, hogy Guccifer 2.0 és a DCLeaks portál is Oroszországhoz kapcsolódik. Egy másik cikk szerint Guccifer 2.0 olyan körzetekben ajánlotta fel elsősorban az általa megszerzett dokumentumokat, ahol a demokrata jelöltek eséllyel indulhattak az elnökválasztási kampányban.

- 2016. december 29.: Obama elnök rendeletben hoz szankciókat Oroszország ellen. Ebben hat orosz magánszemélyt nevesítenek a támadásban való részvétellel kapcsolatban. Emellett 35 orosz diplomatát utasítanak ki, akiknek 72 órájuk van elhagyni az Amerikai Egyesült Államokat.
- 2017. január 3.: Julian Assange, a Wikileaks vezetője egy interjúban tagadja, hogy orosz kormányzati források adták ki nekik a DNC-től kiszivárgott leveleket.
- 2017. január 3–4.: Trump több Twitter-üzenetben kérdőjelezi meg az amerikai hírszerző szervek véleményét az orosz befolyással kapcsolatban. Idézi Assangenak azt a véleményét, miszerint egy hacker, s nem az orosz állam áll a támadások mögött.
- 2017. január 5–6.: A titkosszolgálatok külön-külön Obamát és Trumpot is tájékoztatják a kiberbiztonsággal kapcsolatos eseményeket illetően. Eszerint a választásokat közvetlenül nem befolyásolták, azaz a választásnál használt szavazógépek és számítógépek nem kompromittálódtak, de az oroszok más módokon, például álhírkampánnyal mégis törekedtek a szavazók befolyásolására.
- 2017. január 6–7.: Trump elismeri, hogy orosz kapcsolatok lehetnek a DNC megtámadásában, de jelzi, hogy a kibertámadások nem befolyásolták a választás eredményét.
- 2017. február 9.: A *The Washington Post* arról számol be, hogy Trump nemzetbiztonsági tanácsadója – Michael Flynn – beszélt a szankciókról az orosz nagykövettel, Szergej Kiszljakkal. Januárban az alelnök – Mike Pence – és a Trump-adminisztráció tisztviselői ennek az ellenkezőjét nyilatkozták.
- 2017. február 13.: Lemond Michael Flynn. A lemondási levelében elismeri, hogy nem teljes körűen tájékoztatta a megválasztás előtt álló alelnököt az orosz diplomatával folytatott beszélgetéseit illetően.
- 2017. február 17.: A Szenátus Hírszerzési Bizottságának (Senate Intelligence Committee) tagjai zárt ajtók mögötti beszélgetést folytatottak az FBI igazgatójával, James Comeyval. Az egyik jelenlévő, CNN-nek tett nyilatkozata szerint a találkozó témája az Orosz Föderáció volt és vizsgálatot fognak indítani az orosz befolyásolás ügyében.
- 2017. március 10.: A *The Washington Times*nak adott interjújában Roger Stone, Trump eseti tanácsadója azt nyilatkozta, hogy a kampány alatt ugyan a Twitterén keresztül kapcsolatban állt Guccifer 2.0-val, de teljesen „ártalmatlan" kapcsolatban. A következő nap a *The New York Times*ban megjelent interjúban pedig azt nyilatkozta, hogy Guccifer 2.0-val a DNC-támadás után lépett kapcsolatba, ezzel azt bizonyítva, hogy a Trump-kampánynak nem volt köze a DNC feltöréséhez.
- 2017. március 20.: Az FBI igazgatója kongresszusi meghallgatásán megerősítette, hogy az FBI jelenleg vizsgálja a Trump-kampánysták tagjai és az Oroszországi Föderáció közötti lehetséges kapcsolatokat.

Cikkünk írásának időpontjában az amerikai közvélemény véleménye szerint az orosz kormányzat közvetve, információs műveletekkel[3] és az ehhez információt szolgáltató kiberkémkedéssel próbálta befolyásolni az amerikai elnökválasztás eredményét. Ennek okát Putyin Hillary Clintonnal szembeni ellenségességében jelölik meg, nem pedig Donald Trump segítésében. Egyetértés van abban is, hogy a gyaníthatóan orosz információs műveletek kevéssé befolyásolták a választók akaratát. Az eset azonban minden korábbinál erősebben mutat rá a kibertér fenyegetéseire, aminek nemcsak az USA, de szinte minden ország kitett, és amelyekre még a legfelkészültebb kibervédelemmel rendelkező államnak sem sikerült érdemi választ adnia.

Érdemes tehát áttekinteni, milyen kibertámadási módszerek jelentek meg az elnökválasztási kampány során és azok lehettek-e valóban orosz eredetűek, vagy valahol máshol kell a támadások forrását keresni. A támadási

[3] Információs műveletek kifejezéssel írják le – alapvetően a nemzetközi média szóhasználatára támaszkodva – a főleg az orosz kibertéri és médiaműveleteket. Ugyanakkor az információs műveletek az eredeti NATO-terminológia szerint olyan katonai tevékenységek összessége, amelyekben koordináltan jelennek meg a műveleti biztonság, a katonai megtévesztés, a pszichológiai műveletek, az elektronikai hadviselés, valamint a számítógép-hálózati műveletek során végzett különböző feladatok. Ennek megfelelően nem célszerű azonosítani az információs műveleteket a megtévesztésre és befolyásolásra irányuló, alapvetően politikai és nem elsősorban katonai célokkal rendelkező tevékenységekkel. Mivel azonban jelen írás célja bepillantást nyerni a befolyásolás politikai játszmáiba, mi is információs műveletek összefoglaló névvel illetjük ezeket a tevékenységeket.

stratégia három jól elkülöníthető módszert vonultatott fel. Először a támadók az úgynevezett célzott támadások (Advanced Persistent Threat – APT) útján jutottak hozzá a DNC levelezéséhez, majd ezeket a hacktivista Wikileaks útján hozták nyilvánosságra. Mindeközben a közösségi médiában terjesztett álhírekkel próbálták felerősíteni az egyébként mérvadó sajtó által is táplált botrányt.

Célzott támadások high profile célpontok ellen, az emberi faktor

Az első lépésről, azaz a célzott támadás kivitelezéséről áll talán rendelkezésre a legtöbb információ, köszönhetően annak, hogy a DHS és az FBI a JAR-16-20296A jelzéssel ellátott közös elemzésében számos műszaki információt tett közzé.[4] Ennek már a címében egyértelműen jelzik, kit tartanak felelősnek, a jelentés ugyanis a Grizzly Steppe – Orosz kártékony kiberműveletek címet viseli. 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.[5]

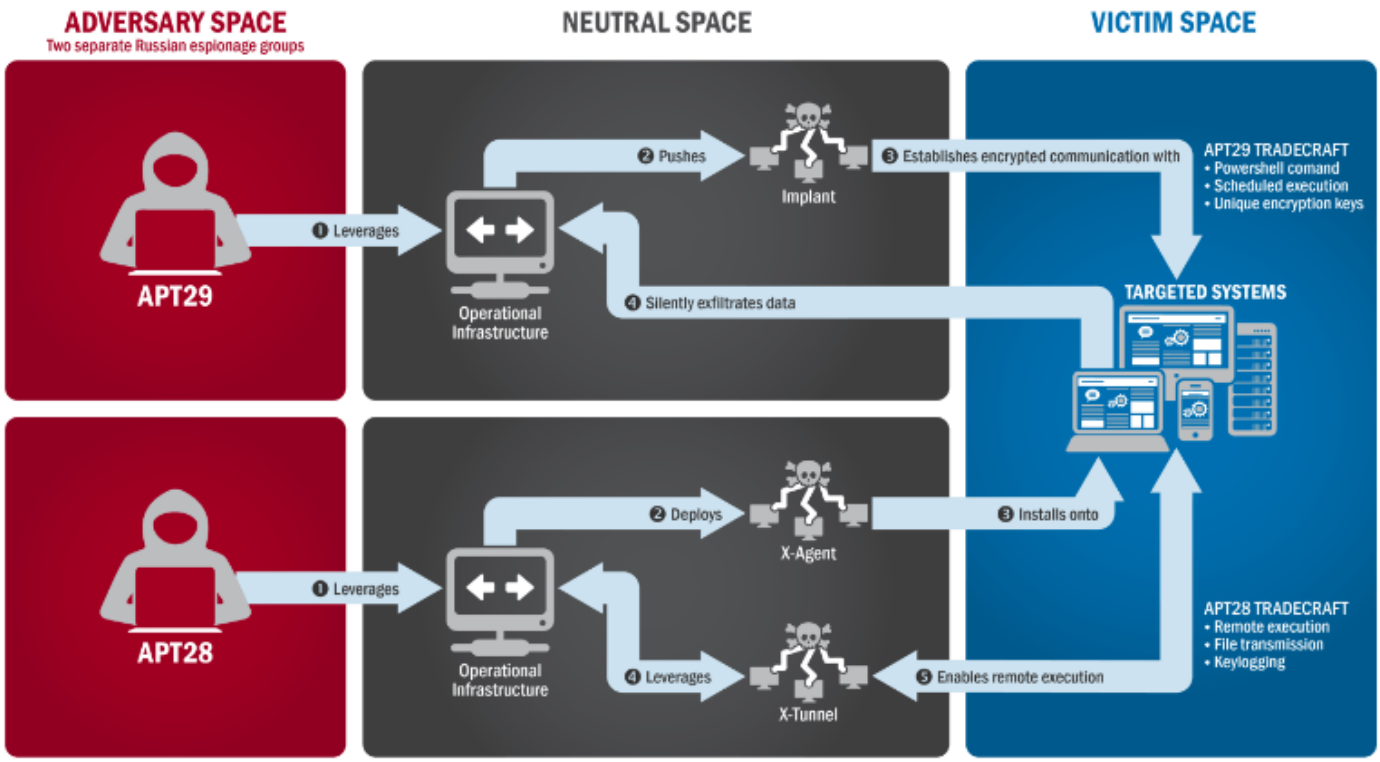
A kibertámadás a hírszerző szervezetek álláspontja szerint szélesebb körű volt annál, mint amivel a sajtó foglalkozott. A célzott adatszerző támadások célpontjai között kormányzati intézmények, kritikus infrastruktúrák, think tank-ek, egyetemek, politikai szervezetek és vállalatok is érintettek voltak. Egyes esetekben az orosz titkosszolgálatok meghamisított identitás mögé rejtőztek. Itt a jelentés feltehetően Guccifer 2.0 szerepére utal. A végrehajtásban egyértelműen két csoportot, az elsőként megjelenő APT 29-et, más néven Cozy Bear-t, illetve a másodikként belépő APT 28-at, azaz a Fancy Bear-t nevesítik. Mindkét csapat a feltételezések szerint valamelyik orosz titkosszolgálathoz kapcsolódi,k és a különböző kormányzati célpontok elleni támadásaik hosszú évekre visszavezethetők.

A Cozy Bear-t[6] az orosz titkosszolgálatok közül vagy a Szövetségi Biztonsági Szolgálathoz (Federalnaja Szluzsba Bezopasznosztyi Rosszijszkoj Federacii – FSZB) vagy az Külső Hírszerző Szolgálathoz (Szluzsba Vnyesnyej Razvedki – SZVR) kapcsolják, tehát feltehetően polgári kötődésük van. Jellemzően hosszabb időt, akár éveket hagynak egy-egy adatlopási kampányra. Ezt azt jelenti, hogy a leginkább rejtve maradnak, lassú ütemben „szívják le" az információt. Első feltűnésük 2008-ra datálódik, ekkor kötötték őket a miniDuke kártékony kódhoz, mely diplomáciai szervezeteket támadott, többek között magyar külképviseleteket is. Felderítésében óriási szerepe volt a Budapesti Műszaki és Gazdaságtudományi Egyetemen működő Crysys Labornak.

A Fancy Bear[7] csoportot ezzel szemben elsősorban az orosz fegyveres erők vezérkarának Felderítő Főcsoportfőnökségéhez (Glavnoje Razvedivatyelnoje Upravlenyije – GRU), azaz az orosz katonai titkosszolgálathoz kapcsolják. Ezt a kapcsolatot erősíti az is, hogy a csoportnak tulajdonított támadások nagyobb része katonai célpontok, illetve katonai célok támogatásával kapcsolatos. Többek között az ukrán légtérben lelőtt Malaysian Airlines-repülőgép tragédiájának kivizsgálásával foglalkozó holland nyomozócsoport, az ukrán hadsereg tüzérsége vagy éppen a NATO tartozott a célpontok közé. De az APT 28-nak tulajdonítják a Nemzetközi Antidopping Ügynökség, azaz a WADA elleni támadást is. A csoport első feltűnése 2007-re datálódik, technikájuk gyorsabb eredmények elérésére koncentrál, mint amit a Cozy Bear-nél lehet látni.[8]

[4] Grizzly Steppe – Russian Malicious Cyber Activity, [online], 2016. 12. 29. Forrás: us-cert.gov [2017. 03. 20].
[5] JAR-16-20296. AGRIZZLY STEPPE – Russian Malicious Cyber Activity. US Department of Homeland Security and Federal Bureau of Investigation [online] 2016. 12. 16. Forrás: us-cert.gov [2017. 03. 04].
[6] Cozy Bear, [online]. Forrás: wikipedia.org [2017. 03. 20].
[7] Fancy Bear, [online]. Forrás: wikipedia.org [2017. 03. 20].
[8] JAR-16-20296. AGRIZZLY STEPPE – Russian Malicious Cyber Activity, i. m.

A titkosszolgálati jelentés az 1. ábrán látható szemléltető sémát osztotta meg a két csoport által használt stratégiáról.



1. ábra: Az APT 28 és az APT 29 csoportok által használt taktikák (forrás: JAR-16-20296A)

Eszerint a támadás kivitelezése a következőképpen nézett ki:

1. 2015 nyarán az APT29 csoport úgynevezett *spearphising* kampányba kezdett. A spearphising lényege az, hogy viszonylag kisszámú, de stratégiailag fontos személy számára küldenek üzenetet, általában e-mail-ben, ritkábban közösségi hálózaton vagy chat-alkalmazáson keresztül. Az üzenet célzott, ami azt jelenti, hogy tartalma valamilyen valós élethelyzetre, eseményre, tevékenységre utal, ami miatt a célpont azt hiszi, hogy az üzenet valós. Nagyon gyakori például, hogy a HR osztály kap olyan e-mailt, amelyet egy valós álláshirdetésre utalva küldenek el. A Cozy Bear ebben az esetben több mint 1000 – köztük kormányzati – személyt célzott meg.
2. Az e-mail üzenetben mindig van egy csatolmány (általában Microsoft Word dokumentum vagy PDF fájl). A spearphising célja az, hogy az áldozat ezt a csatolmányt megnyissa. Amennyiben az üzenet jól van megfogalmazva, azaz a fenti példa alapján a HR osztály munkatársa elhiszi, hogy a csatolmányban küldött PDF fájl egy önéletrajz, akkor a célpontok többsége biztosan meg fogja nyitni a fájlt. Ez az úgynevezett *social engineering,* azaz emberi ráhatással történő támadás. A hackelések túlnyomó többsége napjainkban a szervezet védelmének „feltöréséhez" az emberi faktort, azaz a hiszékenységet használja fel. Ez ellen gyakorlatilag lehetetlen védekezni: minden szervezetnél lesz legalább egy olyan ember, akin keresztül a támadást végre lehet hajtani. Ez történt a DNC esetében is.
3. A csatolt fájlok valamilyen beágyazott aktív kódot tartalmaznak, ami azt jelenti, hogy megnyitásukkor a felhasználó tudta nélkül végrehajtódik valamilyen olyan kártékony program *(malware),* mely elkezd egy külső szerverrel kommunikálni, így gyakorlatilag a számítógépen egy hátsó kaput *(backdoor)* nyitnak, melyen keresztül a támadó bármikor hozzáférhet az ily módon kompromittált géphez. A felhasználó jellemzően

a kód lefutása előtt kap egy figyelmeztető ablakot, mely engedélyt kér az aktív kód futtatására, de a felhasználók többsége ezen az ablakon gondolkodás nélkül az OK gombra kattint.

4. A fertőzés után a gépen futó kártékony kód kommunikálni kezd egy interneten futó szerverrel, onnan kap „parancsot" arra, hogy milyen tevékenységet végezzen a megfertőzött gépen. Az első feladat az úgynevezett perzisztálás, ami azt jelenti, hogy a kártékony kód minden esetben induljon el, amikor a számítógépet bekapcsolják, és kezdjen el kommunikálni a parancsokat adó szerverrel. Második lépésként a feladat a „kitörés" a számítógépről, azaz annak a hálózatnak a felderítése, ahol a gép fut, a hálózat többi számítógépén található sebezhetőségek megtalálása, majd a kártékony kódok elterjesztése más gépeken is. A végső cél olyan rendszeradminisztrátori hozzáférések megszerzése, amelyekkel a teljes hálózat összes erőforrásához hozzá lehet férni. Ezt nevezik privilégium kiterjesztésnek *(privilege escalation),* amit számos módon végre lehet hajtani. Az APT 29 a hálózatok lelkét jelentő szolgáltatáshoz, a felhasználók jelszavait és jogosultságait kezelő rendszerhez fért hozzá, így gond nélkül tudták a DNC levelezőszerverének teljes forgalmát is monitorozni, majd a kiépített csatornán keresztül ezeket a leveleket apránként kiküldeni.
5. Az APT28 2016 tavaszán tűnt fel a színen. Támadásuk sokkal célzottabb volt, csak bizonyos VIP-személyeket támadtak, ugyancsak spearphising technikával. Itt azonban nem a csatolmányok megnyitása volt a cél, hanem az, hogy olyan weboldalakra vezessék az áldozatot, amelyek megtévesztően hasonlítanak az általuk használt és ismert belső szolgáltatások weboldalaira. Ezeken a weboldalakon azután felkérték őket, hogy változtassák meg a jelszavaikat. Ez a klasszikus adathalász, azaz *phishing* támadás, melynek során a mit sem sejtő áldozat megadja a felhasználónevét és jelenlegi jelszavát, majd beír egy új jelszót. Ezzel a támadónak rendelkezésre áll a valós szolgáltatáshoz tartozó felhasználónév és jelszó, ezekkel be tud lépni a védett rendszerbe és meg tudja változtatni a jelszót arra, amit az áldozat megadott. Így a továbbiakban nemcsak az áldozatnak vannak meg a szükséges hozzáférési jogosultságok, hanem a támadónak is. Az egyik ilyen áldozat lehetett John Podesta. A bejövő e-mailek utalhattak arra, hogy az áldozat faxot kapott, meghívót az Európai Parlamenttől, jelszóváltoztatásra a Microsoft Outlook Web Access levelezőszolgáltatásban, vagy éppen kiberbiztonsági veszélyre figyelmeztettek.

Bár Trump és Assange is kijelentette, hogy „Podesta e-mailjeit egy 14 éves gyerek is fel tudta volna törni",[9] a titkosszolgálati jelentés ezt jelentősen árnyalja. Néhány érv amellett, hogy nagy erőforrásokkal rendelkező, profi szervezet áll a támadás mögött, méghozzá azok a csoportok, amelyeket a jelentés nevesít:

- A megtalált kártékony kódok jelentős hasonlóságot mutatnak a korábban használt kódokkal. Gyakori kritikaként fogalmazódik meg, hogy e kódok egy részének forrása elérhető az interneten, így bárki átírhatta azokat. Ugyanakkor valószínűtlen, hogy ez történt. A kártékony kód egy jól megtervezett fejlesztési folyamat eredménye, kellően bonyolult ahhoz, hogy az íróin kívül bárki érdemben fejleszteni tudja.
- A kód terjesztéséhez használt spearphisinghez tudni kell, hogy kiket célozzanak. Ehhez műveleti tervezésre van szükség, ki kell jelölni az elérendő célt, fel kell deríteni a potenciális gyenge pontokat. Titkosszolgálati elemzés nélkül nehezen elképzelhető, hogy a támadó be tudja azonosítani a széles közönség számára egyébként láthatatlan, de mégis fontos háttérembereket és szervezeteket. Szintén ismerni kell azokat a belső élethelyzeteket, amikre hivatkozva a kártékony kódokat tartalmazó leveleket megfogalmazzák. Ez is elemzőmunkát, esetleg lehallgatást feltételez.
- A fertőzött gépek és a parancsokat adó szerverek közötti kommunikációt álcázni kell. Ehhez nem elég a titkosítás, a parancsadó szervert is folyamatosan változtatni kell, azaz nagyméretű infrastruktúra kell, hogy rendelkezésre álljon. Az infrastruktúra jellemzően korábban feltört számítógépekből áll össze, melyek a világ bármely részén lehetnek. Mivel ennyi gépet nehéz feltörni és uralom alatt tartani, a célzott támadások során nem sűrűn szokták az infrastruktúrát megváltoztatni. Ha tehát egy olyan gép tűnik fel, amit egy korábbi támadásban már használtak, joggal feltételezhető, hogy ugyanaz a csoport áll a támadás mögött. A konkrét

[9] Gareth DAVIES, Thomas BURROWS: Assange says a 14-year-old could have hacked Democratic emails as he reveals John Podesta's password was 'password', [online], 2017. 01. 04. Forrás: dailymail.co.uk [2017. március 29.].

esetben vannak jelek arra, hogy már korábban is használt szerverek kerültek bevonásra, dacára annak, hogy ezeket az anonimitást elősegítő TOR, azaz anonimitást biztosító hálózaton keresztül megpróbálták elrejteni.

A Wikileaks és a szivárogtatók szerepe

Egy, a választási kampány során született közkeletű vicc így fogalmazta meg a szivárogtató oldal szerepét: „Mi a különbség a Wikipedia és a Wikileaks között? A Wikipediát bárki szerkesztheti, a Wikileakset csak az FSZB." Ez is rámutat arra az ellentmondásos viszonyra, ami az amerikai kormányzat és a Wikileaks között feszül. Julian Assange jelenleg Ecuador londoni nagykövetségén él menekültként, hiszen az Egyesült Államok a kiadatását kéri. Ennek okai többek között, hogy a Wikileaksen jelentek meg milliószámra a Bradley (azóta Chelsea) Manning által ellopott amerikai diplomáciai üzenetek, melyet Cablegate néven ismerhetünk. Mindemelett az ügy hátterében főleg az Edward Snowden, a Wikileaks és az orosz kormány közötti bizonytalan kapcsolat áll. Assange egyébként gyakori vendége az RT (korábban Russia Today) hírcsatornának, ami nem erősíti az USA bizalmát iránta. A két félnek tehát bőven van törlesztenivalója egymással szemben.

A szivárogtatást[10] a Guccifer 2.0 néven jelentkező hacker vállalta magára. Ez egyben utalás Gucciferre, arra a román hackerre, aki először 2013-ban tűnt fel a médiában azzal, hogy román és amerikai politikai személyiségek levelezését törte fel. Guccifert, azaz az Arad közelében élő, a hírek szerint magyar nemzetiségű Marcel Lazăr Lehelt végül 2014-ben elfogták. A nyomozás során kiderült, hogy tettét magányosan hajtotta végre. Bár 2016-ban bevallotta Hillary Clinton levelezésének feltörését, erre nem találtak bizonyítékot. Guccifer 2.0 saját állítása szerint egy, a nagy elődje nyomdokaiba lépő, szintén román hacker, azonban a Motherboard magazinnak adott interjúja során nem volt képes a hirtelen románra váltó riporter kérdéseit megérteni és arra románul felelni.[11] A feltételezések szerint Guccifer 2.0 a Fancy Bear csoport által kreált alteregó.[12]

Assange határozottan tagadja, hogy a kiszivárogtatott anyagok orosz állami forrásból származnak, viszont – szemben Manninggel vagy Snowdennel – nyoma sincsen annak, hogy lenne egy magányos elkövető a háttérben. Valószínűtlen, hogy egy ilyen horderejű ügyben anonim tudna maradni egy olyan személy vagy csoport, akinek nincsen meg a megfelelő titkosszolgálati támogatása. Az USA-ból kitiltott 6 orosz személy nevesítése pedig azt jelzi, hogy még titkosszolgálati védettséggel rendelkező személyek esetén is ki lehet deríteni az online név mögött lévő valódi személyt.

Az NSA, az FBI és a CIA 2017. január 6-án hozta nyilvánosságra azt az összefoglaló jelentését (Intelligence Community Assessment – ICA),[13] melyben a titkosítás alól feloldott információkat mutatja be, megvilágítva az amerikai hírszerző közösség álláspontját az orosz műveletekkel kapcsolatban. A jelentés célja az, hogy bemutassa az „attribution", azaz Oroszország nevesítésének hátterét. Ebben külön kitérnek a Wikileaks szerepére. Eszerint a Wikileakset azért választotta Moszkva, mert a korábbi szivárogtatások miatt megbízható, hiteles forrásnak tekinthetők a világ szemében. Putyin pedig a nyilvánosság előtt is fontosnak tartotta azt, hogy az amerikai választók „megismerjék az igazságot" a demokratákról. A Wikileaks és Moszkva között a kapcsolatot az RT, orosz forrásból működő tévéadó, konkrétan ennek főszerkesztője jelenti. Assange rendszeresen megjelenhet az RT adásaiban és kifejtheti véleményét.

[10] 2016 Democratic National Committee email leak, [online]. Forrás: wikipedia.org [2017. 03. 20].
[11] Lorenzo FRANCESCHI-BICCHIERAI: We Spoke to DNC Hacker 'Guccifer 2.0', [online], 2016. 06. 21. Forrás: motherboard.vice.com [2017. március 29.].
[12] Hacker 'Guccifer' extradited from Romania, appears in U.S. court, [online], 2016. 04. 01. Forrás: reuters.com [2017. 03. 04.]; Catherine HERRIDGE, Pamela K. BROWNE: 'Guccifer' casts doubt on Obama administration's Russia hacking claims, [online], 2017. 01. 04. Forrás: foxnews.com [2017. március 29.]; Mike WENDLING: Conversations with a hacker: What Guccifer 2.0 told me, BBC trending, [online], 2017. 01. 14. Forrás: bbc.com [2017. 03. 04.].
[13] Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, [online]. Forrás: dni.gov [2017. 03. 20].

Meglepő lenne tehát, ha Assange nem tudná, honnan származnak a kiszivárogtatott e-mailek. Természetesen elképzelhető, hogy félrevezetik, hiszen ő a világ egyik leginkább megfigyelt embere, a brit adófizetőknek például már több millió fontjába került az évek óta tartó 24 órás megfigyelés, tehát nem feltétlenül van rálátása a nagyobb összefüggésekre. A folyamatos bezártság sem biztos, hogy jót tesz a józan ítélőképességnek, így lehet, hogy Assange már könnyebben megvezethető, mint néhány évvel ezelőtt. Az viszont biztos, hogy egy darabig még nem fogunk tisztán látni ebben az ügyben.[14]

Információs műveletek a közösségi médiában

A világ médiamunkásai és újságírói sorban csodálkoznak rá arra, hogy egyes nagyhatalmak előszeretettel használják ki a közösségi médiumokat álhírek vagy félreértelmezhető magyarázatok terjesztésére. Az információs műveletek használata azonban nem új jelenség, maximum annak a korszellemhez igazított formája jelenthet újdonságot. De nem annak, akik olvasták az Oroszországi Föderáció Katonai Doktrínájának vonatkozó részeit.[15]

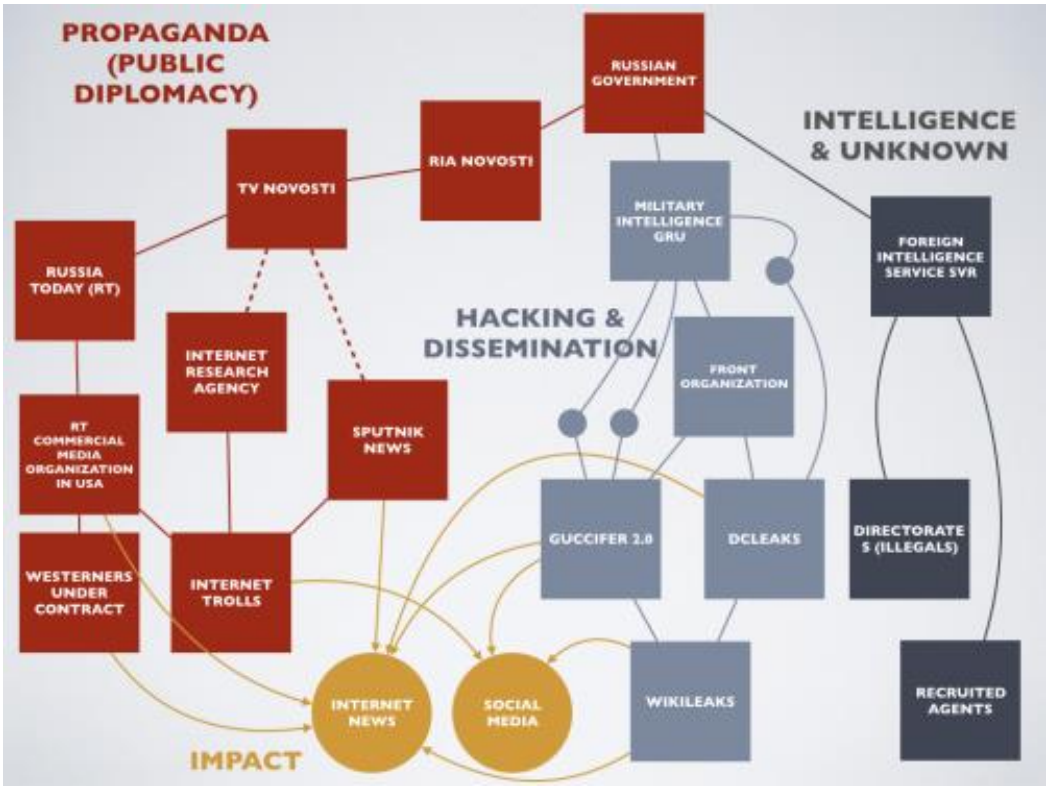
Ennek 12. m) pontja világosan megfogalmazza, hogy az Oroszországi Föderáció külső fenyegetésként értelmezi azon információs és kommunikációs technológiák alkalmazását katonai és politikai célok elérése érdekében, melyek szembe mennek a nemzetközi joggal és az orosz szuverenitást, politikai függetlenséget, területi integritást veszélyeztetik, valamint fenyegetést jelentenek a nemzetközi békére, biztonságra, valamint a globális és regionális stabilitásra. Ez a meglehetősen kiterjesztő definíció alapvetően meghatározza azt, hogy Oroszország a kibertérben széles körű ellenműveleteket indíthat.

A 21. v) pont szerint olyan védelmi környezetet kell létrehozni, mely lehetővé teszi az információs és kommunikációs technológiák jelentette kockázatok csökkentését a katonai és politikai célok ellenében. A 22. pont értelmében az Oroszországi Föderáció megfontolhatja a fegyveres erők, valamint más szervezetek és testületek alkalmazását olyan esetekben, amikor vele vagy szövetségeseivel szemben agressziót követnek el. Érdemes még megemlíteni a 32. i) pontot, mely szerint a fegyveres erők békeidejű feladatai közé tartozik olyan duális felhasználású infrastruktúra-elemek kiválasztása, melyek segíthetik a hadsereget védelmi feladataik ellátásában, valamint a 35. j) pontot, mely előírja az információbiztonság fejlesztését a fegyveres erőknél és más szervezeteknél. Emellett figyelmet érdemel a 38. d) pont, mely előírja a más, fegyveres erőkön kívüli szervezetekkel való kooperációt is.

Mindezek és a doktrína egyéb pontjai is magyarázatot adhatnak arra, hogy miért merül fel Oroszország neve elsőként az álhírterjesztők listáján. Amennyiben az orosz politikai vezetés stratégiai fenyegetésként, Oroszország politikai stabilitását veszélyeztető tényezőként ítélte meg a demokrata elnökjelölt múltbeli és vélhetően jövőbeni tevékenységét is, a doktrína szellemisége értelmében a katonai és a hozzá kapcsolódó civil védelmi rendszer megtehette azokat az ellenintézkedéseket a kibertérben, melyek segíthettek ennek a kockázatnak a csökkentésében.[16]

Edward M. Roche kiberhadviseléssel foglalkozó blogján kiválóan foglalta össze azokat a szereplőket, akiknek valamilyen szerepe lehetett a vélt vagy valós stratégiai fenyegetés elhárításában.[17] A 2. ábra mutatja be a szereplőket.

[14] Intelligence Community Assessment: Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, National Intelligence Council [online], 2017. 01. 07. Forrás: senate.gov [2017. 03. 04.].
[15] Военная доктрина Российской Федерации, [online], 2014. 12. 30. Forrás: rg.ru [2017. 03. 20.].
[16] Uo.
[17] Edward M. Roche: Comments on "Assessing Russian Activities and Intentions in Recent US Elections", [online]. Forrás: 2017. 01. 08. cyberarmscontrolblog.com [2017. 03. 20.].



2. ábra: Az ICA-jelentésben említett szereplők
(forrás: Edward M. Roche, Cyberarms Control Blog)

A három fontos tényező közül kettőnek, a hackereknek és a hírszerzőknek a szerepét fentebb már összefoglaltuk, érdemes röviden a propagandával foglalkozók tevékenységét is bemutatni. Ezek egyrészt ismert, bejegyzett szereplők, olyan médiumok és fizetett vagy „hívő" szakértők, akiknek az aktivitása világosan követhető, másrészt az internet névtelen szereplői, a fizetett trollok, akiknek feladata a közösségi médiában a hírek és az azokhoz kapcsolódó narratíva befolyásolása.[18]

A már idézett ICA mellékletében részletes elemzés található az RT szerepéről és fontosságáról. Az orosz gyökerű tévéadó már a 2012-es választás előtt is kritikusan állt az Egyesült Államokhoz, folyamatosan kerültek adásba olyan anyagok, amelyek megkérdőjelezték a szavazás demokratikus folyamatát. Hangsúlyosan számoltak be az Occupy Wall Street protesztmozgalomról, amely alapvetően az amerikai kapitalista államberendezkedés ellenében jött létre. A 2016-os választásoknak tehát kellő „rutinnal" vágtak bele. Ahogy azt az ICA összefoglalja, minden lehetséges területen az USA kormányzatával szemben foglaltak állást, legyen szó akár a rendőri brutalitásról, a valutaszabályokról, az USA adósságáról vagy a drónhasználatról. Amikor szóba kerül, hogy ez a hozzáállás ellentétes az USA nemzeti érdekeivel, Margarita Simonyan, az RT főszerkesztője minden esetben a szólásszabadságra hivatkozik. A jelentés foglalkozik az RT Kremlbe való beágyazottságával is, mely szerint Alekszej Gromov, az elnöki adminisztráció helyettes vezetője, korábbi elnöki szóvivő az elsődleges kapcsolattartó. Őt egyébként 2014-ben kitiltották az USA-ból a Krím-félsziget megszállásával kapcsolatos szankciók keretében.[19]

Az RT fontosságát a közösségi média elérésében kell keresni. A Youtube-on napi 1 millió elérése van, 550 millió ember láthatja világszerte, csak az USA-ban 85 millió néző kapcsolhat az adásaira. 450 ezer ember iratkozott fel a Youtube csatornájára, amely több, mint a BBC vagy a CNN elérése. Közel 1 millió felhasználó like-

[18] Uo.
[19] Intelligence Community Assessment: Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution, i. m.

olja a Facebookon. Lehet tehát mondani, hogy a nyugati világban sokan vannak olyanok, akik találkoznak az RT-vel és fogyasztják az általa előállított tartalmat.

Az internetes trollok feladata felerősíteni egyes narratívákat, eközben pedig kikezdeni, gyengíteni a narratíva ellen ható gondolatokat és felhasználókat. A trollkodás egyidős az internettel, azonban tudatos politikai felhasználása csak néhány évre tekint vissza. Valószínűleg a világon minden jelentős politikai párt rendelkezik olyan szimpatizánsokkal vagy fizetett alkalmazottakkal, akik a központi pártútmutató alapján próbálják befolyásolni a közösségi párbeszédet. Oroszország esetében a szentpétervári Internet Research Agency-t nevesítik olyan központként, amelynek feladata a Kreml iránymutatása alapján beavatkozni a Facebookon és a Twitteren kialakuló hírfolyamba.

Összefoglalás, következtetések

A 2016-es amerikai elnökválasztás, illetve az azt megelőző kampány során tapasztalt egyre inkább hangsúlyosabbá váló informatikai támadások, e-mail fiókok feltörése, a megszerzett levelek célzott nyilvánosságra hozása, vagy a közösségi médiumokban tömegével megjelenő álhírek világosan rávilágítanak arra a tényre, amely jelen írás címében kimondva-kimondatlanul megfogalmazódik. A politikai viszonyok formálására a média, esetünkben az internet és a segítségével igénybe vett közösségi médiumok hatalmas lehetőséget rejtenek magukban.

Mert övék a hatalom címmel 1979-ben jelent meg David Halberstam Pulitzer-díjas amerikai újságíró kétkötetes műve[20] az amerikai tömeghírközlés történetéről F. D. Roosevelt elnökségétől Nixon távozásáig. Halberstam azonban nemcsak a média egyre növekvő hatalmát mutatta be, hanem azt a politikai változást is, amely részben ennek a médiatörténelemnek a során, annak hatására következett be. Azokat a médiabirodalmakat mutatja be a könyv, amelyek komoly hatással voltak a politikai viszonyokra, és végső soron az ország sorsára.

Ennek analógiáján az internet, az ott lévő közösségimédia-felületek számos hasonlóságot mutatnak. Abban az esetben, ha valaki részben vagy egészben irányítani tudja az ott folyó híreket, médiaeseményeket, illetve tevékenységeket, akkor az nagy befolyással rendelkezik, és akár egy olyan nagy volumenű eseményre is hatással tud lenni, mint az amerikai elnökválasztás.

A bemutatott és elemzett amerikai hírszerzési jelentések világosan rámutatnak, hogy Oroszországnak komoly érdeke és lehetősége is volt különböző internetes támadásokkal, valamint közösségi médiumokban álhírekkel befolyást gyakorolni emberek tömegére világszerte.

Mindezek alapján megállapíthatjuk, hogy már napjainkban is, de a közeljövőben még inkább számolni kell az ilyen és ehhez hasonló tevékenységekkel. Az internet globális volta, a közösségi médiumok felhasználóinak eddig sosem látott tömegei magától értetődő módon nyújtják az eszközt a befolyásoláshoz, a gazdasági vagy politikai viszonyok alakításához.

Ahogy a 20. században a nyomtatott sajtó, a rádió vagy a televízió egyre nagyobb tömegeket ért el, úgy ez ma a 21. században az internet esetében hatványozottan igaz.

A biztonság mind technikai, mind humán értelmezése kulcsfontosságúvá válik. Az orosz katonai doktrína világosan rávilágít arra a tényre, hogy egyre inkább olyan horderejűvé válik ez a kérdés, amely már nemcsak egyszerű informatikai biztonsági megoldásokat igényel, hanem nemzetbiztonsági válaszokat is, akár stratégiai irányváltásokkal.

[20] A magyar kiadás 1988-ban jelent meg az Európa Könyvkiadó gondozásában, Félix Pál fordításában.

Az „SVKK Elemzések” 2003 óta a kutatóközpont munkatársainak tematikus szakpolitikai elemzéseit megjelentető időszakos kiadvány, melyben a szerzők független kutatói álláspontjukat közlik.

Az NKE Stratégiai Védelmi Kutatóközpont független szakpolitikai kutatóintézet, a kiadványaiban megjelenő elemzések, álláspontok, vélemények nem feltétlenül tükrözik a szerkesztőség vagy a kiadó véleményét. Az elemzésben foglalt információk, adatok, megállapítások tájékoztatás céljából készültek.

Kiadó: NKE Stratégiai Védelmi Kutatóközpont

Szerkesztés és tördelés:
Bazsó Márton, Csiki Tamás

A kiadó elérhetősége:

1581 Budapest, Pf. 15.

Tel: 00 36 1 432-90-92

E-mail: svkk@uni-nke.hu

2012– : NKE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4862)

2011–2012: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)
2007–2011: ZMNE Stratégiai Védelmi Kutatóintézet Elemzések (ISSN 2063-4854)
2003–2007: ZMNE Stratégiai Védelmi Kutatóközpont Elemzések (ISSN 2063-4854)