DR. HÓDOS LÁSZLÓ

GONDOLATOK MAGYARORSZÁG NEMZETI BIZTONSÁGI STRATÉGIÁJÁBAN AZONOSÍTOTT, EGYES KIEMELT BIZTONSÁGI KOCKÁZATOK NEMZETBIZTONSÁGI ASPEKTUSAIRÓL

1. Bevezető

Magyarország Kormánya, kiemelten a Honvédelmi Minisztérium munkatársai munkájának köszönhetően elfogadta Magyarország Nemzeti Biztonsági Stratégiáját (a továbbiakban: NBS). Ez a korábbi, 2012-ben elfogadott előző, azonos elnevezésű stratégiai dokumentumot helyezi hatályon kívül. A tanulmány célja, hogy az NBS VII. fejezetében megjelenített Kiemelt biztonsági kockázatokkal összefüggésben a hazánkat érő kihívások, kockázatok és fenyegetések nemzetbiztonsági aspektusait vizsgálja. Az előbbiek közül jelen publikációban kiemelten a c), d) és o) pontban rögzítettekkel foglalkozom, mivel a nemzet biztonsága szempontjából egyformán jelentős biztonsági kockázatok közül véleményem szerint ezek rendelkeznek leginkább aktualitással, a tudományos és a védelmi szektor figyelme napjainkban ezekre fókuszál legjobban.

2. Az NBS kiemelt biztonsági kockázatokként azonosított, a tanulmány szempontrendszere alapján fókuszba állított fenyegetésekről[1]

A 2012-ben kiadott Nemzeti Biztonsági Stratégia elfogadását követően számos, egész Európát, és benne természetesen Magyarországot is cselekvésre kényszerítő esemény történt. Talán ezek közül leglátványosabb a tömeges migráció megjelenése volt 2015-ben. Ennek során hazánk transzport útvonallá változott, emiatt a kormányzat azonnali és határozott lépéseket tett, melynek során az Ideiglenes Biztonsági Határzár is kialakításra került.
A tanulmány fókuszába az NBS c), d) és o) pontja szerinti, alábbi három fenyegetések közötti esetleges összefüggést, valamint az egymásra gyakorolt hatást helyeztem:
„c) ***összehangolt és széleskörű diplomáciai, információs és titkosszolgálati műveletek, pénzügyi-gazdasági nyomásgyakorlással, pénzügyi spekulációs támadásokkal vagy katonai fenyegetéssel párosulva (hibrid) Magyarország destabilizálása****, kormányzati cselekvőképességének, politikai stabilitásának és társadalmi egységének gyengítése, továbbá nemzetközi érdekérvényesítő képességének korlátozása céljából;*
d) ***jelentős károkat okozó kibertámadások*** *a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen;*

[1] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról VII. fejezet

*o) a **lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség** magyarországi megjelenése és gyors terjedése."*

3. Hibrid típusú fenyegetések azonosítása és a hazai válaszlehetőségek

Az NBS VII. fejezet c) pontjában megjelenített jellemzőkkel bíró, új típusú fenyegetettség megjelenése, vagy inkább alkalmazása a nemzetközi színtéren egyre erőteljesebb és kiterjedtebb. Az alkalmazó e tevékenységsorozat közben a modern technológiák által nyújtott kifinomult lehetőségeket használja fel, és a gazdaságra, médiára, a kibertérre és a szociális érintkezés különböző formáira is kiterjeszti műveleteit. Az egyes elemek (támadó intézkedések) külön-külön vagy egymást erősítő hatású alkalmazása – a hagyományosnak tekinthető támadási formák használata nélkül is – már alkalmas lehet a befolyásolásra, a zavarkeltésre, egyes államok belső rendjének megbontására, a társadalom hangulatának formálására. Az új típusú fenyegetettség fokozott szintjére tekintettel Magyarország kiemelt feladatként tekint a hibrid fenyegetések elleni fellépésre, illetve azok kezelésére.

A hibrid kihívások nemzetbiztonsági szempontból történő azonosításának egyik meghatározó eleme, hogy a detektálhatóan ellenérdekelt szolgálathoz tartozó „hivatásos" vagy az állami szereplő kötelező jelenlétének keresését, felderítését mellőzhetjük, sőt érdemes is tágabb látókörrel keresnünk az intézkedés szereplőit, valamint forrását. Nem elengedhetetlenül szükséges a tevékenység irányítójára „foglalkozásszerű összeesküvőként" tekinteni. Miként az NBS V. fejezete Magyarország biztonsági helyzetének elemzése során rámutat, „*az állami és nem állami szereplők által szponzorált politikai, gazdasági és társadalmi folyamatok befolyásolására irányuló stratégiák száma, változatossága és hatásfoka növekszik. A befolyásolás egyik eszköze lehet a nemzetközi közvélemény szervezett és módszeres Magyarország ellen hangolása. Az információs műveletek hatékonyságát növeli, hogy az álhírek, dezinformációk terjedését a közösségi média rendkívül gyorssá teszi. A nyílt befolyásolás politikai és gazdasági nyomásgyakorlásban is megjelenhet, amely során az ellenérdekelt nemzetközi szereplők korlátozni próbálhatják hazánk cselekvőképességét."* Ez sokkal súlyosabb veszélyt jelent, a nem csak állami szereplőkkel szembeni küzdelemben tehát komolyabb erőforrás-ráfordítást igényel, mint korábban gondolhattuk. A nyílt politikai befolyásolás eszköze lehet egy olyan cikk megjelentetése, mely „véletlenül" tíz percen belül, tökéletes fordításban legalább három különböző nyelven jelenik meg a világ különböző pontjain, és Magyarország mozgásterének jelentős korlátozását eredményezi.

Az Európai Unió új, 2019–2024 közötti időszakra vonatkozó stratégiai menetrendje a társadalom hibrid fenyegetések, rosszindulatú informatikai tevékenységek és dezinformáció elleni védelmének fontosságát emeli ki, továbbá hangsúlyozza, hogy az ilyen veszélyek kezelése átfogó megközelítést igényel, több kooperációval, koordinációval, erőforrással és komolyabb technológiai eszközpark bevetésével. Ez a feladatkör azért kimondottan bonyolult, mert a tevékenység leginkább a nemzetállamok elszigetelése, hiteltelenítése útján valósul meg, vagyis – akár az EU akár a NATO esetében – a tagállamok egymás iránti bizalmának

csökkentése a cél[2]. Ennek ellensúlyozására válik rendkívül fontossá az ellenséges hírszerzési tevékenységgel szembeni ellenálló képesség erősítése.

A tagállamok egymás közötti, illetve a tagállamok és más érintett nemzetközi szervezetek közötti koordináció, különösen a NATO-val, támogatná az EU-ban végzett ellenséges tevékenységekkel szembeni kémelhárítás összehangolását[3]. Ehhez társul továbbá, hogy a hibrid hadviselés, mint nem katonai, illetve katonai tevékenység jelentős költségvonzattal jár. Így Magyarország esetében „*kiemelt jelentősége van annak a szempontnak, hogy a „korlátozott erőforrásokkal" rendelkező államok esetében a nemzetbiztonsági struktúrák hatékony működtetése, a koordinációs, irányítási, a technikai és az emberi erőforrásokra épülő információgyűjtő, az elemző-értékelő, vagy akár a különböző szakértői területek összehangolt munkája*"[4] ténylegesen összeadódjon és így kerüljön felhasználásra akár a fenyegetések felderítése és elhárítása, akár Magyarország nemzetbiztonsági érdekeinek, céljainak érvényesítésekor.

A bűnüldözés hagyományos értelemben vett elsődleges feladatával ellentétben a nemzetbiztonsági funkció – érdemben – információgyűjtést, előzetes felderítést és elhárítást, továbbá – általában – megelőző jellegű tevékenységet hajt végre mind a környezet, mind a fenyegetések vonatkozásában. Ezzel a biztonság megőrzése (fenyegetés elhárítása) mellett tágabb értelemben is erősíti és előmozdítja a nemzeti érdekek érvényesítését (ide értve akár az ún. befolyásolást is), tehát rendeltetésében, feladatát tekintve, és ebből adódóan eszközrendszerében és hatásköreiben is eltér a védelmi szféra többi ágazatától. A deklarált munkamegosztás mellett az NBS VIII. fejezetének 126. pontjában megjelenítettek szerint: „*Az azonosított kihívások megelőzése, kezelése és elhárítása elsődlegesen nemzeti felelősség, amely a Kormány feladata, együttműködésben a társadalommal. A biztonság elsődleges alapja a szilárd társadalmi, gazdasági és pénzügyi szerkezet, valamint nemzeti szinten a megelőző és védelmi intézkedések fenntartható és rugalmas rendszere, ezen belül pedig a haderő, valamint a rendvédelmi szervek (a rendőrség, a büntetés-végrehajtás, a nemzetbiztonsági szolgálatok, a katasztrófavédelem és rendvédelmi feladatai tekintetében az állami adó- és vámhatóság) célirányos fejlesztése."* Vagyis az állami szervek, kiemelten a rendvédelmi szervek és az egyedüli nemzetbiztonsági szolgálat, amely nem rendvédelmi szerv is egyben, a Katonai Nemzetbiztonsági Szolgálat feladata a társadalommal közösen a biztonság garantálása. Az eltérő feladatrendszerből adódik, hogy hibrid kihívásokkal összefüggésben más eszközrendszer áll a Honvédség, a Rendőrség és egy nemzetbiztonsági szolgálat rendelkezésére.

---

2 Az Európai Parlamentnek és a Tanácsnak A hibrid fenyegetésekkel szembeni fellépés közös keretéről szóló közös közleménye (https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52016JC0018) (Letöltés ideje: 2019. 10. 26.)

3 A reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítése, Európai Bizottság, 2018. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018JC0016&from=GA (Letöltés ideje: 2019. 10. 26.)

4 DOBÁK Imre: Nemzetbiztonsági szolgálatok – Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe; Hadtudomány, 2015/4. p. 114.

Ezt a védelmi igazgatási szempontból is jelentős elkülönülést nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény indokolása is az alábbiak szerint rögzíti:

„Az államok nemzetbiztonsági érdekeik védelme és más nemzetek szándékainak megismerése érdekében igénybe veszik a nemzetbiztonsági szolgálatok sajátos, más szervezetek által nem helyettesíthető lehetőségeit. Az alapvetően titkos és rá jellemző[5] *eszközöket felhasználó nemzetbiztonsági tevékenység megfelelő jogi szabályozást igényel annak érdekében, hogy semmilyen körülmények között ne jelenthessen veszélyforrást a demokratikus jogrendre, ezen belül az állampolgári jogokat csak akkor és olyan mértékben korlátozhassa, amennyiben az az ország nemzetbiztonságának megóvása, szuverenitásának érvényesítése céljából szükségszerű és indokolt."*[6]

Magyarország Alaptörvénye határozza meg azt, hogy a nemzetbiztonsági szolgálatokat a Kormány irányítja, a szervezetükre, működésükre vonatkozó részletes szabályokat, a titkosszolgálati eszközök és módszerek alkalmazásának szabályait, valamint a nemzetbiztonsági tevékenységgel összefüggő szabályokat sarkalatos törvény[7] határozza meg.

A kialakított struktúrában a nemzetbiztonsági szektormodellek[8] alapján történő áttekintés eredményeként a magyarországi szolgálatokkal összefüggésben megállapítható, hogy még mindig érvényesül az egymással konkuráló szolgálatok közötti korlátozott együttműködés. Ennek következtében detektálható esetleges hátrányok[9] egy koordinatív funkcióval rendelkező kormányzati igazgatási szerv útján volnának ellensúlyozhatók, míg a vetélkedő jelleg erősségei hatékonyabban kihasználhatóvá válhatnak a megfelelő elemzést, értékelést felhasználó gyakorlati működéssel.

A koordináció és a különböző ágazatok közötti együttműködés szükségességét az NBS IV. fejezetében, hazánk alapvető adottságainak felsorolása során a jogalkotó kiemeli, miszerint „*a Hibrid támadással szembeni ellenálló képességünket növeli a nemzet egysége, demokráciánk szilárdsága, a közös nyelv, a felgyorsított döntéshozatali képesség, valamint a honvédelmi és rendvédelmi erők szoros együttműködése egymással és a releváns polgári infrastruktúrával. Az új biztonsági kihívások miatt azonban folyamatosan szükséges fejleszteni az információs és*

---

5 Figyelmet érdemlő körülmény, hogy előbbiek rögzítésének évében, 1994-ben a leginkább a nemzetbiztonsági szolgálatok eszközrendszerében elhelyezkedő képességek, ismeretek és alkalmazások jelenleg széles körben kerülnek felhasználásra a nem állami, ún. magán hírszerzési tevékenységet végző (különösen a jelentős ipari, gazdasági) szereplők által is, így ma már nem beszélhetünk kizárólag állami felhasználókról ezen eszközök tekintetében.

6 A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény általános indokolása alapján

7 Lásd Magyarország Alaptörvényének a 46. cikk (4) és (6) bekezdéseit. A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény az a sarkalatos törvény, amelyre az Alaptörvény utal.

8 Dr. HÉJJA István: Nemzetbiztonsági szervezeti modellek; In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete. NKE Nemzetbiztonsági Intézet, Budapest, 2014. pp. 57-72.

9 Uo. p. 63.

kiberhadviselés elleni védekezés rendszerét".[10] Mivel az érintett országgal szembeni hibrid hadviselés eredményessége az ott lévő, elhárító feladatokat ellátó szervek – egymással – konkuráló működése mellett jelentősen megnövekszik, ezért nem lehet elégszer hangsúlyozni, hogy a fenyegetés kivédése csak sokkal szorosabb együttműködés mellett lehetséges. Ennek kialakításakor, figyelemmel az előbbiekre, nem szabad megfeledkeznünk arról sem, hogy *„…A globális biztonsági környezetben zajló változások következtében felértékelődik a hírszerzés es az elhárítás szerepe. A műveleti területre jellemző összetett kihívások, valamint a gyakran változó biztonsági helyzet szintén megnöveli a pontos és időbeni információk és értékelések iránti igényt."*[11]

4. Fenyegetés a kibertérből és az arra adható válaszok

Az információs műveletek és a bizalom aláásása során kiemelt jelentősége van a kibertérből érkező fenyegetések elhárításának. A kölcsönös bizalom megrendülését előidéző szakmai hibák, a kibertámadások súlyos következményeit egy nagyon tanulságos történet segít jobban megvizsgálni. Ez az NBS VII. fejezetének d) pontjában szereplő kiemelt biztonsági kockázat egy véletlenszerűen kiragadott – detektált és dokumentált – esete, amely az Amerikai Egyesült Államok legutóbbi elnökválasztását is beárnyékolta, és az egész világ elektronikai információbiztonsággal foglalkozó szakembereit cselekvésre ösztönözte. A védelem erősítése iránti igényt a politikai vezetés is támogatta, ennek hazánkban is számos megnyilvánulási formáját tapasztaltuk az elmúlt években. A példa szerinti történet azonban nem Magyarországról szól, hiszen mindig igaznak fogadható el az a kijelentés, hogy jobb mások kárán tapasztalatot szerezni, mint az, ha magunk szenvednénk meg érte.

Az Amerikai Egyesült Államok 2020-ban újra elnököt választ. A tanulmány írásának idején a COVID-19 ellenes küzdelem közepette, elsődlegesen Kína felé fordulnak ugyan a gyanakvó amerikai választópolgári tekintetek (kiemelten a republikánusok által emlegetett választási panelek miatt), azonban a demokraták nyilván nem fognak megfeledkezni az állandó és súlyos orosz veszélyről sem a választási kampány során, különösen, ha megint elveszítik az elnökválasztást. A tanulmány témája szempontjából vizsgálva fókuszba állított kiberhadviseléssel összefüggésben érdemes megjegyezni egy, a Holland Királyság katonai és a polgári nemzetbiztonsági szolgálatai közös munkásságának köszönhetően felderített, ugyanakkor előző amerikai elnökválasztást beárnyékoló COZY BEAR incidenst. Elsődlegesen a polgári nemzetbiztonsági szolgálat, vagyis az Általános Hírszerző és Biztonsági Szolgálat (Algemene Inlichtingen- en Veiligheidsdienst – AIVD) sikeréről van szó, melynek köszönhetően maga Hollandia is célkeresztbe került végül, és emiatt kellett elővigyázatosságból kézzel számolni minden szavazatot a 2017 márciusában tartott választáson.

---

[10] NBS IV. fejezet 31. pontja

[11] SZENTGÁLI Gergely: Csendben szolgálni, 1. rész: A magyar nemzetbiztonsági szektor helyzete és átalakítása 2010 es 2014 között, Hadtudomány, 2015/1-2. p. 52.

4.1. Az incidens az AIVD szemszögéből

Az érdemben 2014 nyara óta működő Közös SIGINT és Kiber Egység (Joint Sigint Cyber Unit[12] – JSCU) az AIVD és a Holland Katonai Hírszerző és Biztonsági Szolgálat (Militaire Inlichtingen- en Veiligheidsdienst – MIVD), közös egysége, amely más feladatai mellett a hírszerzés kiberműveletek révén történő fókuszálására koncentrál. Ugyanezen a nyáron az egység tippeket kapott egy orosz hackercsoportról, amely egy moszkvai egyetemi komplexumban működik. A JSCU lobogója alatt működő AIVD-csoportnak sikerült behatolnia az orosz belső számítógépes hálózatba. Az AIVD nemcsak a számítógépes hálózathoz szerzett hozzáférést, hanem a folyosón lévő biztonsági kamera felvételeihez is. A felvételeken látható személyekkel kapcsolatos információkat megosztották az amerikai hírszerző szolgálatokkal. Hollandiában[13] stratégiai szinten a kibervédelmi feladatok végrehajtását az Igazságügyi és Biztonsági Minisztérium alárendeltségébe tartozó Nemzeti Kiberbiztonsági Központ (Nationaal Cyber Security Centrum – NCSC) koordinálja. A katonai kibertámadások elhárításáért a Kibervédelmi Parancsnokság (Defensief Cyber Command – DCC) szakmai alárendeltségében lévő Számítógépes Eseménykezelő Védelmi Csoport (Defensief Computer Emergency Response Team) felelős. A kiberhírszerzési (CYBINT) feladatok végrehajtása a MIVD feladata. Ebbe az intézményi rendbe illeszkedik a szolgálatok közös egysége a JSCU.
Hazánk kibervédelmi képességeinek fejlesztése is elsődlegesen két pilléren nyugszik, amely a redundancia miatt helyes megoldásnak tartható. A katonai pillért a Katonai Nemzetbiztonsági Szolgálat, míg a polgári pillért a Nemzetbiztonsági Szakszolgálat biztosítja.

2014 őszén az oroszok hozzáféréshez jutottak a Fehér Ház nem minősített számítógépes hálózatához. Ez lehetővé tette számukra bizalmas feljegyzések és nem nyilvános információk megismerését Obama elnök utazásairól, és sikeresen ellopták e-mailjeinek – legalább – egy részét. Ezeket a kibermanővereket is felfedte a holland hírszerző szolgálat, és értesítette az amerikaiakat.

2014 novemberében a hollandok detektálták, hogy az orosz hackerek (újra) sikeresen behatoltak a State Department számítógépes hálózatába. Miután a holland hírszerző vezetők erre felhívták a figyelmet, az amerikaiak az orosz támadást 24 órán belül sikerrel elhárították. A digitális összecsapást évekkel később egy aspen-i vitafórumon az NSA igazgatóhelyettese kemény kézitusaként aposztrofálta. Hírszerzési forrásokra támaszkodva a Washington Post azt írta, hogy egy nyugati szövetségese segítséget nyújtott a támadás elhárítása érdekében, azonban további részleteket nem jelenítettek meg.

2015 nyarán a holland hírszerző szolgálat volt az első, aki figyelmeztette amerikai kollégáit a Cozy Bear által a Demokrata Nemzeti Bizottság (az Amerikai

---

[12] A közös SIGINT egység létrehozásáról szóló dokumentum (Parlamenti levél) https://web.archive.org/web/20141108103250/http://www.defensie.nl/binaries/defensie/documenten/kamerstukken/2014/07/03/kamerbrief-en-convenant-jscu/kamerbrief+en+convenant+gecombineerd.pdf (Letöltés ideje 2020. 04. 26.)

[13] A feladatok megosztásáról részleteiben lásd: AIVD annual report 2018 https://english.aivd.nl/publications/annual-report/2019/05/14/aivd-annual-report-2018 (Letöltés ideje: 2020. 04. 26.)

Egyesült Államok Demokrata Pártjának igazgatási szempontból legfontosabb szervezete – röviden a DNC) elleni egy, az orosz kormányhoz kötődő hackercsoport által végrehajtott kibertámadásra. A legtöbb nyugati hírszerző szolgálat feltételezi, hogy a csoportot az (orosz) SVR külföldi hírszerző szolgálat irányítja. A nyugati hírszerző szolgálatok és a kiberbiztonsági társaságok évek óta vadásznak a csoportra, amely szerte a világon, beleértve Hollandiát is, kormányzati ügynökségeket és vállalkozásokat támadott meg.

A Hollandia által a DNC-t, a Fehér Házat és más állami hivatalokat ért támadásról megosztott információk Robert Muellernek, az FBI által az amerikai választásokba való esetleges orosz beavatkozást kivizsgáló különleges ügyésznek az íróasztalára kerültek. A New York Times pedig az év decemberében bejelentette, hogy többek között Ausztráliából, az Egyesült Királyságból és Hollandiából származó információk alapján végezte a vizsgálatot az FBI.

4.2. A Cozy és a Fancy Bear csoportokról[14]

Az előbbieket végrehajtó orosz hackereket a hírszerző szolgálatok és a kiberbiztonsági társaságok a The Dukes és az APT29 néven ismerik, ám leginkább Cozy Bear néven említik őket. Az orosz hackerek egy másik csoportja a Fancy Bear (más néven APT28-cal) is felelős (a Cozy Bear mellett) a DNC elleni támadásokért. Ugyanis a Cozy Bear 2015 nyarán, míg a Fancy Bear 2016 áprilisában „kereste fel" a demokraták washingtoni szervereit. A hollandok 2016-ben is tetten érték a támadókat és ismét figyelmeztették az Egyesült Államok hatóságait.

The New York Times beszámolt róla, hogy a DNC már hónapok óta nem vette komolyan az FBI figyelmeztetéseit. Végül a Crowdstrike kiberbiztonsági vállalat vizsgálta ki az eseményeket a Demokrata Párt megbízása alapján, melynek során arra a következtetésre jutott, hogy a Cozy Bear és a Fancy Bear együttesen felelősek a támadásokért[15]. Az amerikai hírszerző szolgálatok szerint az oroszok végül továbbították a Fancy Bear által megszerzett e-maileket a Wikileaks-nek, amely ezeket egyből közzé is tette. A publikált levélváltások óriási botrányt eredményeztek az amerikai választási kampányban, ennek hullámai Hazánkban is érezhetők voltak (a magyar külpolitika orosz, illetve amerikai orientációjára utaló cikkek jelentek meg). Az incidens műszaki és technikai körülményeiről az ESET szoftverfejlesztő és forgalmazó cég készített elemzést, mely a biztonsági réseket és a felhasználói hibák sorát jeleníti meg[16].

4.3. Az eset tanulságai, a levonható következtetések

A rendelkezésre álló adatok (átadott információk) alapján az AIVD hackerek már nem férnek hozzá a Cozy Bear adataihoz. A sajtóértesülések szerint az amerikai hírszerzési munkatársak, politikai szereplők, akik 2017-ben egy nyugati szövetséges

---

[14] Bear on bear; https://www.economist.com/united-states/2016/09/22/bear-on-bear (Letöltés ideje: 2020. 04. 26.)

[15] Who is Cozy Bear; https://www.crowdstrike.com/blog/who-is-cozy-bear/ (Letöltés ideje: 2020. 04. 26.)

[16] ESET Operation Ghost Dukes; https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf (Letöltés ideje: 2020. 04. 26.)

segítségét dicsérték a levelezésükben, vélhetően az alkalmazott eszközök és módszerek dekonspirálódását okozhatták. A nyilvánosságra kerülés a holland szakmai és politikai elitet is mélyen megrázta, nagyfokú csalódottságát eredményezte. Egy televíziós műsorban nyugdíjba vonulása előtt, 2018 nyarán az AIVD igazgatója, Rob Bertholee kijelentette, hogy különös óvatossággal kell eljárni a műveleti információk megosztásakor az Egyesült Államokkal, most, amikor Donald Trump elnök[17]. Úgy fest, hogy érdemes ezt észben tartania a szakmai és politikai közösségeknek. Gróf Széchenyi István szavaival élve *„Józan ész soha sem áldoz fel pillanati vagy igen kis időre terjedő haszonért, habár ma nyulhat is hozzá, jövendő nagyobb `s tartósb hasznot; de inkább az ideigóráiglani rövid nyomást a várható hosszabb kellem miatt békével türi”.*

5. Az NBS VII. fejezet a c), d) és o) pontban rögzített kiemelt biztonsági kockázatok közötti kapcsolatról

A hibrid és kiberhadviselés közötti kapcsolat összefüggései jól láthatók. Hogyan kapcsolódik előbbi kettőhöz *„a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenése és gyors terjedése?”*[18] Lehetséges-e előzőek káros hatásainak szándékos, gondatlan vagy vétlen növelése a járvány miatt elrendelt veszélyhelyzet idején? Elegendő a kormányzati tájékoztatást követnünk ahhoz, hogy felismerjük, a kibertérben elindított dezinformáció, mint az országos nyilvánosságot kapott „Budapestet hamarosan le fogják zárni” tartalmú hamis híresztelés miféle politikai, gazdasági, társadalmi károkat képes okozni. A Készenléti Rendőrség Nemzeti Nyomozóiroda és a Nemzetbiztonsági Szakszolgálat gyors, határozott intézkedéseinek köszönhetően a Budapest lezárásáról szóló, de más álhírek terjesztőit is azonosították és velük szemben büntetőeljárás indult. A bármely okból kialakult sebezhetőség kiváló lehetőség az online csalások elkövetői számára is, akik szintén a kibertérben követik el a bűncselekményeket. A sebezhetőség a járvány miatti bizonytalanság eredményeként alakul ki. Ennek legjobb ellenszere a magyar kormány által is alkalmazott széles körű tájékoztatás. Interneten, televízióban, nyomtatott és elektronikus sajtóban közöl folyamatosan adatokat a kormányzat, megerősíti a társadalomban, hogy a helyén van az államapparátus, pánikra nincs ok. A dezinformáció terjesztése, a bizalom aláásásának kiváló eszköze ellen csak így lehet felvenni a harcot. Azok a biztonsági kockázatok, amelyeket sajátos szempontok szerint kiemeltem, pontosan a társadalom kötőszövetét rombolják le. Az államapparátus vagy a helyi szintű vezetők munkájába vetett bizalmat, de akár a kormányzati vagy nem kormányzati munkahelyek légkörét is teljesen tönkre tudják tenni azok a megnyilvánulások, melyeket jobb esetben csak sajtóhírekből ismertünk meg az elmúlt hónapokban.

---

[17] Did the Trump admin alert Russia that foreign intel were watching their hacking program? https://www.dailykos.com/stories/2018/1/26/1736337/-Did-Trump-or-his-loyalists-reveal-foreign-intel-on-hacking-program-to-the-Russians (Letöltés ideje: 2020. 04. 26.)

[18] Az NBS VII. fejezet o) pontjában leírtak szerint

Az álhírek terjesztésének egyik legveszélyesebb területe a jogalkotás tevékenységének támadása hazai és nemzetközi színtéren. Az úgynevezett lawfare[19], amely elsősorban a jogi eszközök alkalmazását jelenti a hibrid hadviselés során, megítélésem szerint értelmezhető úgy, hogy ide sorolandó a jogalkotás legfelsőbb szintje által alkotott jogforrások folyamatos, az esetek többségében alaptalan támadása is, mivel a célja a jogalkotó hiteltelenítése, a belé vetett közbizalom megingatása. A jog uralmának helyességébe vetett társadalmi bizalom gyengítése alkalmas az állam destabilizálására, mozgásterének csökkentésére.

Az NBS-ben szereplő, a tanulmány fókuszába helyezett kihívások elleni küzdelem során kulcsszerepe van a proaktív jogalkotásnak[20] és a megfelelő alkotmányos kontroll melletti jogalkalmazásnak.

Összegzés, következtetések

Megállapíthatjuk, hogy a kibertérből érkező álhírek a járvány elleni védekezést alapvetően nehezítik meg és ezzel számos emberéletet és jelentős anyagi javakat sodornak veszélybe. A közösségi oldalak igyekeznek ezeket kiszűrni, sajnos azonban hazánkban (is) több olyan esettel (álhírrel) találkozhattunk, amely a legnépszerűbb videómegosztó honlapról, vagy valamelyik közösségi oldalról indult útnak, és okozott jelentős hátrányt.

Nem szabad megfeledkezni a jogintézmények alapjogkorlátozó voltáról, miközben vizsgáljuk a jogalkotási lehetőségeket még az ország életében extrémitásnak tekinthető különleges jogrend alkalmazásának idején sem. A szükségesség és arányosság követelményeinek ekkor is meg kell felelnie a döntéseknek, intézkedéseknek.

A kibertérben jelenlévő, pontosabban onnan érkező, azt felhasználó dezinformációs művelet a járvány idején (de minden más, különleges jogrend kihirdetését megalapozó helyzetben) jelentősebb eredménnyel jár (hátránnyal fenyeget). Emiatt komolyabb dologi és személyi erőforrásokat igénylő feladatokat képez a nemzetbiztonsági elhárításért és rendvédelemért felelős szervek számára is, így erre a (veszélyek elhárítására történő) folyamatos felkészülés, illetve a (jövőbeli, konkrét) feladatok tervezése során a nemzetbiztonsági szolgálatoknak és más állami szerveknek fokozottan figyelniük kell.

---

[19] A kifejezés használatáról bővebben lásd: Colonel Charles J. Dunlap: Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts; http://people.duke.edu/~pfeaver/dunlap.pdf (Letöltés ideje: 2019.10.31.)

[20] Fontos megjegyezni, hogy emiatt elengedhetetlen a különleges jogrend alkalmazása során a rendeletek útján történő irányítás.

Felhasznált irodalom:

- BÉRES János (szerk.): Külföldi nemzetbiztonsági szolgálatok; Zrínyi Kiadó, Budapest, 2018. ISBN: 9789631295481, pp. 66-79.
- DOBÁK Imre: Nemzetbiztonsági szolgálatok – Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe; Hadtudomány, 2015/4. pp. 113-130.
- FARKAS Ádám: A védelmi kötelezettségtől a fegyveres védelem rendszeréig; Katonai Jogi és Hadijogi Szemle, 2018/1. pp. 7-22.
- FINSZTER Géza: A rendészeti stratégia és az alkotmányozás; Kriminológiai Közlemények, 2010. pp. 155-165.
- HÉJJA István: Nemzetbiztonsági szervezeti modellek; In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete. NKE Nemzetbiztonsági Intézet, Budapest, 2014. ISBN: 978-615-5305-49-8, pp. 57-72.
- HÓDOS László: Gondolatok a gerilla-hadviselés elleni küzdelem egyes összefüggéseinek tudományos vizsgálatáról; Szakmai Szemle 2019/3. pp. 67-80.
- KENEDLI Tamás: Magyarország külpolitikájának stratégiai kérdései és a belőle következő nemzetbiztonsági feladatok. In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete. NKE Nemzetbiztonsági Intézet, Budapest, 2014. ISBN: 978-615-5305-49-8, pp. 95-99.
- KENEDLI Tamás: Magyarország nemzeti biztonsági stratégiája és a belőle származtatható nemzetbiztonsági feladatok. In: DOBÁK Imre (szerk.): A nemzetbiztonság általános elmélete, NKE Nemzetbiztonsági Intézet, Budapest, 2014. ISBN: 978-615-5305-49-8, pp. 73-94.
- KOVÁCS Krisztián: A befolyásolás szerepe a modern hadviselésben. Felsőfokú Nemzetbiztonsági Tanfolyam, Nemzeti Közszolgálati Egyetem, Budapest, 2018.
- PORKOLÁB Imre: Aszimetrikus hadviselés: az ortodox és a gerilla hadikultúra összecsapásai című előadása; Hadtudomány 2005/4. pp. 188-193.
- SZABÓ Károly: A katonai kémelhárítás feladatrendszerének új vonásai Európa és Magyarország megváltozott biztonsági környezetében; Felderítő Szemle 2018/2. pp. 179-189.
- SZENTGÁLI Gergely: Csendben szolgálni: 1. rész: A magyar nemzetbiztonsági szektor helyzete és átalakítása 2010 es 2014 között; Hadtudomány, 2015/1-2. p. 54.

Felhasznált jogszabályok:

- Magyarország 2011. április 25-én kihirdetett Alaptörvénye
- 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról
- 94/2018. (V.22.) Korm. rendelet a Kormány tagjainak feladat- és hatásköréről
- 1144/2010. (VII. 7.) Korm. határozat a Kormány ügyrendjéről szóló

- 1035/2012 (II.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 1063/2020. (IV.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
- 23/2020. (IV. 24.) HM utasítás a honvédelmi szervezetek 2020. évi kiemelt feladatainak, valamint a 2021-2022. évi fő célkitűzéseinek meghatározásáról

Internetes források:

- A közös SIGINT egység létrehozásáról szóló dokumentum (Parlamenti levél) https://web.archive.org/web/20141108103250/http://www.defensie.nl/binaries/defensie/documenten/kamerstukken/2014/07/03/kamerbrief-en-convenant-jscu/kamerbrief+en+convenant+gecombineerd.pdf (Letöltés ideje 2020. 04. 26.)
- AIVD annual report 2018; https://english.aivd.nl/publications/annual-report/2019/05/14/aivd-annual-report-2018 (Letöltés ideje: 2020. 04. 26.)
- Az Európai Parlamentnek és a Tanácsnak A hibrid fenyegetésekkel szembeni fellépés közös keretéről szóló közös közleménye; https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52016JC0018 (Letöltés ideje: 2019. 10. 26.)
- Bear on bear; https://www.economist.com/united-states/2016/09/22/bear-on-bear (Letöltés ideje: 2020. 04. 26.)
- Colonel Charles J. Dunlap: Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts; http://people.duke.edu/~pfeaver/dunlap.pdf (Letöltés ideje: 2019. 10. 31.)
- Did the Trump admin alert Russia that foreign intel were watching their hacking program? https://www.dailykos.com/stories/2018/1/26/1736337/-Did-Trump-or-his-loyalists-reveal-foreign-intel-on-hacking-program-to-the-Russians (Letöltés ideje: 2020. 04. 26.)
- ESET Operation Ghost Dukes; https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf (Letöltés ideje: 2020. 04. 26.)
- Who is Cozy Bear; https://www.crowdstrike.com/blog/who-is-cozy-bear/ (Letöltés ideje: 2020. 04. 26.)