TANULMÁNY KÖTET 2020 2021

NBSZK

NEMZETBIZTONSÁGI SZAKKOLLÉGIUM

Biztonság, védelem, nemzetbiztonsági tudatosság

Szerzők

Csizmadia Martin

Hankó Viktória

Kalmár Vanessza

Krausz József

Lőrincz Virág

Szőke Ágoston

Tóth József Lukács

Tóth Tímea

Szakmai lektor

Dr. Bányász Péter

Dr. Berényi László

Dr. Magyar Sándor

Dr László Gábor

Dr. Regényi Kund Miklós

Dr. Tóth András

Dr. Zalai-Göbölös Noémi

Drusza Tamás

A kézirat lezárásának időpontja: 2021. június 30.

Szerkesztő: Hankó Viktória és Baranyi Ágnes

Tördelő-szerkesztő: Schlemmer Attila

Tartalom

Előszó

Tisztelt Olvasó Közönség!

A Nemzetbiztonsági Szakkollégium életében a 2013-as megalakulása óta rengeteg változás ment végbe, de ezek nem akadályozták meg abban, hogy mindig a legmagasabb minőséget képviselje, legyen szó akár tudományos előadásokról vagy elemzésekről. Jelenlegi tanulmánykötetünk is ezt a hagyományt követi: hallgatóink a Nemzeti Közszolgálati Egyetem kutatói és oktatói mentorálása mellett mutatják be legújabb kutatásukat, elméleteiket, gyakorlati tapasztalataikat. Az itt olvasható művek a szakkollégistáink által tartott konferenciaelőadások, versenyek, pályázatok, önálló kutatások végtermékei, amelyek ismét bizonyítékai annak, hogy a szakkollégiumi tehetséggondozásra a Nemzeti Közszolgálati Egyetem kiemelt figyelmet fordít, és eredményekben gazdag a tagok élete.

A nemzetbiztonság határai is kitolódnak, átalakulnak, folyamatosan változnak - amik milyenségét és ismérveit a kutatóknak is egyre gyorsabban kell lejegyezniük, elemezniük, szintetizálniuk. Az interdiszciplinaritás, valamint a szakkollégium széles kutatási köre megjelent már az első két tanulmánykötetben, de a mostaniban különösen érvényes: rendkívül sok helyen összefonódnak a biztonságpolitika, a jog, a politológia, a nemzetközi kapcsolatok, a hadtudomány, a műszaki tudományok tanai.

Egyértelmű és megkerülhetetlen priorizált kutatási terület a digitalizáció és a nemzetbiztonság kapcsolata lett. Foglalkoztunk már a minősített adatok informatikai védelmén át, a távirányítású fegyverek elterjedésén keresztül a terroristák internetes propagandájáig szinte mindennel, ahol a digitalizáció kulcsszerepet játszik. Nincs ez most sem másképp, sőt, a tanulmánykötetben található kutatások már mindegyike szorosan kapcsolódik ehhez a témakörhöz. Központi témáink a digitális kor okozta veszélyek és az ezek ellen való védekezés, nem csupán állami, hanem állampolgári szinten is. Szerencsésnek mondhatjuk magunkat, hogy nem olyan korszakában élünk történelmünknek, amikor a legtöbb konfliktust a csatatereken vagy lövészárkokban vívják, ám az információs társadalom generálta hálózati összekapcsolódások révén az ártó hatások is könnyebben elérnek minden szintre. A hibrid hadviselés érzékelteti hatását mindennapjainkban: állami és nem állami, katonai és nem katonai szereplők vívják ádáz küzdelmüket, anélkül, hogy háborús szintre eszkalálnák az összeütközéseket. Ennek fő terepe a kommunikációs tér, ahol manapság szinte mindenki elérhető valamilyen formában, legyen szó akár a televízióról, internetről, mobiltelefonokról. Nem csak a nemzetközi jog alapvető szereplői, azaz az államok vívják meg csatáikat legtöbbször fedetten a virtuális térben, hanem bekapcsolódnak nem kormányzati szervezetek, terroristák, bűnözők stb.

Az ő célpontjaik már nem csak a kiemelt intézmények vagy személyek: gyakorlatilag senki sincs biztonságban ármánykodásuktól, ezért rendkívül fontos, hogy a biztonságtudatosságot a lehető legszélesebb körben biztosítsuk és felhívjuk a figyelmet az új típusú veszélyekre, kihívásokra. Ilyenforma utat jár be az aktuális tanulmánykötet, hiszen a mindenki számára lényeges biztonságos jelszókezelés és jelszóválasztástól kezdve a közösségi média álhírein és az internetes fenyegetéseken át, Észtország információs rendszerének megbénításáig széles kört lefed a tanulmányok sora. Mint ebből a pár példából is érzékelhető, a fenyegetések bárkit, bármit és bárhol elérnek. Így a fenti József Attila idézet – habár meglepőnek is hangozhat – még aktuálisabb lett, mint korábban, attól függetlenül, hogy hazánk egyik legnagyobb költője valószínűleg nem pontosan a mostani zűrzavaros, sok kérdést felvető biztonsági környezet leírására szánta.

Sáfrán József

Csizmadia Martin

Bankkártyás csalások, biztonságos kártyahasználat

Napjainkban a készpénzes vásárlásokat egyre inkább felváltják a bankkártyával történő fizetési módok. Az újítás leginkább a fiatalabb korosztályok körében népszerű. Az MNB 2018-as jelentése szerint a 18-22 éves korosztály közel 50 százaléka intézné pénzügyeit kizárólag vagy nagyobb részt okostelefonja segítségével és ez az arány hasonló a 23-30 éves korosztály körében is. A legtöbb ügyfél a kényelem és a gyorsaság miatt választja a kártyás fizetést, amelyre egyre több helyen van lehetőség, így valóban nagyban megkönnyíti az életünket. Az új innovációk terjedése, azonban felvethet fogyasztóvédelmi és adatvédelmi aggályokat is. Az újítások nem megfelelő ismerete nem kellően megalapozott fogyasztói döntéseket eredményezhet. A tranzakciók és utalások átfutási ideje rendkívül lerövidült, így tartózkodni kell az impulzív döntéshozataltól.

Nem csak mi keverhetjük magunkat bajba a virtuális fizetések világában. Számos bűnöző próbál óvatlan emberektől adatokat, illetve pénzt szerezni, ezzel súlyos károkat okozva mind a pénzintézeteknek, mind pedig a bankszámlák tulajdonosainak. Az alábbiakban áttekintem a leggyakoribb módszereket, melyeket a csalók használnak aszerint, hogy a csalás „offline" vagy „online" módon történik-e.

Elsőként vegyük számba az általam „offline" csalásokként említett módszereket, melyek lényege, hogy a bankkártya adatait közvetlenül vagy valamilyen materiális eszközzel szerzik meg a csalók.

1. **Bankkártya és PIN kód ellopása a tulajdonos figyelmének elterelésével:**

Ennél a módszernél elengedhetetlen, hogy több elkövető legyen és azok összedolgozzanak. Általában egyikük igyekszik valamivel elterelni az áldozat figyelmét, míg társa ellopja annak mobiltelefonját és pénztárcáját. Mikor az áldozatban tudatosul, hogy meglopták le akarja majd tiltatni bankkártyáját. Ekkor érkezik a harmadik elkövető, aki „segíteni" próbál az áldozatnak és felajánlja, hogy az ő telefonjáról beszéljen az áldozat a bankjával. A vonal végén viszont ugyanúgy csalók jelentkeznek, akik arra kérik az áldozatot, hogy a telefon billentyűinek segítségével adja meg PIN kódját. A csalók rögzítik a folyamatot, így már nem csak a bankkártya, de a hozzá tartozó PIN kód is a birtokukban van, mellyel könnyedén megkárosítják a gyanútlan áldozatot.

Elkerülés: Az első és legfontosabb megjegyeznünk, hogy bankunk soha nem fogja elkérni a számlához tartozó PIN kódunkat. Ők általában valamilyen más adat (név, lakcím stb.) alapján azonosítanak be bennünket, így ha valaki a PIN kódunkat kéri, legyen azonnal gyanús a helyzet. További megoldás még a bankkártya hátoldalán lévő segélykérő telefonszám feljegyzése így probléma esetén mi magunk tudjuk tárcsázni a bank ügyfélszolgálatát. Minden esetben hasznos lehet SMS szolgáltatás igénylése (kivéve, ha telefonunk is ellopták), mellyel nyomon tudjuk követni a tranzakciókat és értesülünk minden kártyahasználatról.

2. **Csalások ATM-eknél:**

Az ATM-es kézpénzfelvételeknél is érdemes vigyázni, ugyanis számos módszer van, mellyel megszerezhetik PIN kódunkat, a kártyánk adatait vagy akár a kártyánkat is. Gyakori eset, hogy az ATM kártyanyílására egy kis olvasót szerelnek, amely az eredeti nyílással teljesen megegyezik, így észrevétlenül lopják el a kártya adatait.
Ehhez a módszerhez tartozik még egy kis kamera elhelyezése is, amellyel a PIN kód beütését rögzítik. Gyakran az ATM-re helyezett matrica alá rejtik a kamerát, vagy valamilyen az ATM mellett lévő tárgyra (reklámtartó, virágcserép, állvány stb.), ezért előírás szerint ilyenek nem is lehetnek az ATM-ek környékén. A csalók azonban olykor megrepesztik az ATM burkolatát, hogy oda rejtsék a kamerát, illetve attól sem riadnak vissza, hogy egy második billentyűzetet helyezzenek az ATM-re.

Hazánkban a legtöbb ATM-et bankok üzemeltetik, viszont az Egyesült Államokban lehetőség van ATM vételére és üzemeltetésére, akár magánszemélynek is, így ott a csalók ezt is kihasználják és jó néhány módosított ATM-mel lopják el az állampolgárok kártyaadatait. Elkerülés: Igyekezzünk mindig ugyanabból az ATM- ből kézpénzt felvenni (lehetőség szerint egy bankfiókban találhatóról), illetve kézpénzfelvétel előtt vizsgáljuk meg az ATM-et. Nem veszünk- e észre valami gyanúsat, mozgassuk meg a kártyakiadót és a billentyűzetet.

3. **Üzletekben, éttermekben történő csalások:**

Gyakori módszernek számít a bevásárló központok pénztárainál lévő PIN padek kicserélése. Ez a bűnözőknek pillanatokba telik, viszont a bolt dolgozói akár hónapokon keresztül sem veszik észre a csalást. A másik kedvelt módszer még üzletek esetében, hogy egyszerűen csak körbefotózzák a kártyát, hozzájutva így minden adathoz, ami az internetes vásárlásokhoz szükséges. Vendéglátó egységekben is könnyedén áldozatok lehetünk. Kártyánkat akár a pincérek is lemásolhatják. Fizetéskor, miután átadtuk a kártyánkat, a pincér leejti, majd a bokáján lévő olvasóval lemásolja a kártyát. A másik esetben pedig úgy tesz, mintha a kasszához vinné, majd mégis a mobil leolvasót hozza ki. Mire visszakapjuk a kártyát, már lemásolták. A PIN kódot és a kártya képét minikamerával rögzítik.

Elkerülés: Soha ne adjuk ki a kezünkből a bankkártyánkat, ne tegyük a pénztár pultjára sem, és igyekezzünk a PIN kódunkat a másik kezünkkel takarva beütni.

4. **Telefonos csalások**

Az utolsó és egyben napjainkban legritkább módszer, mikor egyszerűen csak felhívnak telefonon és egy bank alkalmazottjának tűnő személy elhiteti velünk, hogy most vásároltak, valamilyen nagyobb összegért a kártyánkkal. Ahhoz pedig, hogy törölhessék a tranzakciót szükségük van a kártyánk adataira. Amint ezeket megadtuk, már el is lopták a kártyánk adatait, melyekkel ezután szabadon rendelkezhetnek.

Elkerülés

Az első és legfontosabb, hogy a bank sosem kéri el a kártya adatait, ezért azt senkinek ne adjuk meg. Erre az óvatosságra figyelmeztessük családtagjainkat is, főként az időseket.

Most pedig feltárok néhány online módszert, amivel megkárosíthatnak bennünket. Az előzőektől eltérően most először csak a problémákról fogok írni, majd az elkerülés érdekében alkalmazható módszereket a végén foglalom össze.

5. **Kártékony programok**

Gyakori eset, hogy csalók emailben küldenek különböző linkeket felhasználóknak, akik azt megnyitva akaratlanul is adathalász vírusokat (trójai programok) telepítenek a gépükre, melyek megpróbálják leállítani a vírusvédelmet és a tűzfalat. Amennyiben ez sikerült, megszerzik a banki adatokat.

6. **Rosszindulatú oldalak**

Manapság egyre népszerűbb az internetes vásárlás. Az ilyen honlapokon a vásárlásokhoz, azonban minden banki adatot meg kell adnunk, ami komoly kockázattal jár. Számos ilyen weboldal csalók által üzemeltetett, akik miután begépeltük a banki adatokat, lementik és felhasználják azokat.

7. Megtévesztő weboldalak

Talán az egyik legnehezebben felismerhető csalásról van szó az ál weboldalak esetében. Ilyenkor a csalók egy emailt küldenek a bank nevében valamilyen problémára hivatkozva és egy linket, mellyel elérjük a „bank" oldalát. A link azonban csak egy a saját netbankunkhoz kísértetiesen hasonlító oldalra kalauzol minket, ahol látszólag ugyanazon a felületen kell belépnünk, mint mindig. A csalók ezen a felületen megszerzik adatainkat miután begépeltük azokat, majd átirányítanak a valódi netbankunkba, így észre sem vesszük mi történt.

A lehetséges módszerek feltárása után vegyük számba, hogy miként tudunk védekezni és biztonságosan kezelni online pénzügyeinket. Segítségképpen egy listába szedek minden olyan fontosabb tanácsot melyet tudni érdemes:

Kerüld a nyílt wifi hálózatokat!

Nagyon kényelmes, mindenki számára elérhető és még ingyen is van, de a mindenkibe a rosszindulatú hackerek is beletartoznak, akik ellophatják adataidat. Használj inkább mobilnetet vagy VPN-t

1. Csak https:// előtagú honlapokat látogass!
   Ezek olyan weboldalak, amik megfelelően titkosítják a felhasználók adatait. A legtöbb hazai és külföldi bank weboldala is ezt a biztonsági tanúsítványt használja.
2. Kapcsold be a kétlépcsős azonosítást!
   Nem csak bankolásnál, de például az emailjeid megvédése céljából is hasznos lehet. Általában egy másik email címet vagy telefonszámot kérnek, melyen értesíthetnek, ha illetéktelenek akarnak belépni a nevedben.
3. Vigyázz a megtévesztő emailekkel!
   Jegyezd meg, hogy a bankod se emailben, se telefonon nem kéri el a belépéshez szükséges adataidat. Ha ilyet tapasztalsz, hívd bankod ügyfélszolgálatát. Fontos, hogy sose küldött linkről lépj be bankod honlapjára, hanem gépeld be azt böngésződ keresősávjába.
4. Mindig erős jelszavakat adj meg!
   Jelszavaid lehetőség szerint tartalmazzanak kis- és nagybetűket, valamint számokat is és ne legyenek köthetőek hozzád, így elkerülheted fiókjaid feltörését.
5. Használj vírusírtót!
   Sok ingyenes vírusírtót lehet találni, de évente megérheti azt a néhány ezer forintot eszközeink védelme. A legtöbb vírusírtó már emailjeinket is nézi, tűzfal funkciója is van, illetve netbankolásnál is segít.
6. Rendszeresen frissítsd eszközeid!
   Olykor unalmasnak és feleslegesnek tűnhet az operációs rendszerek vagy különböző programok frissítései, de ezek amellett, hogy jobb teljesítményt nyújtanak, számos biztonsági fejlesztést is tartalmaznak.
7. Használd bankod mobilalkalmazását és kapcsold ki a bluetooth-t
   Kevesen tudják, hogy a bankunk által kínált mobilalkalmazások sok esetben biztonságosabbak, mint a böngészőben intézett netbankolás. Ezen kívül fontos, hogy készülékeinken csak szükség esetén használjuk a bluetooth-t, mert ezen keresztül a legtöbb eszköz könnyen feltörhető.

Remélem sikerül, ezzel a kis ismertetővel biztonságosabbá tenni a pénzügyeket. Mindenkinek ajánlom figyelmébe a leírtakat.

Felhasznált Irodalom

„A bankkártyás csalásokról”. Elérés 2020. március 5. https://www.mnb.hu/fogyasztovedelem/bankkartyak/biztonsag/a-bankkartyas-csalasokrol.

„A bankkártyás csalásokról”. Elérés 2020. március 5. https://www.mnb.hu/fogyasztovedelem/bankkartyak/biztonsag/a-bankkartyas-csalasokrol.

MNB: Pénzügyi fogyasztóvédelmi jelentés 2018. Elérés 2020. március 5. https://www.mnb.hu/letoltes/fogysztovedelmi-jelentes-2018-hun.pdf.

Kiszámoló - egy blog a pénzügyekről. „Így fosztják ki a bankszámládat”, 2012. április 20. https://kiszamolo.hu/igy-fosztjak-ki-a-bankszamladat/.

Kiszámoló - egy blog a pénzügyekről. „Így lopják el a bankkártyád adatait az ATM-nél”, 2016. július 5. https://kiszamolo.hu/igy-lopjak-el-a-bankkartyad-adatait-az-atm-nel/.

„Internetes csalások”. Elérés 2020. március 6. https://www.mnb.hu/fogyasztovedelem/bankszamlak/elektronikus-banki-szolgaltatasok/internetes-csalasok.

Kiszamolo. „ATM karácsonyra”. *Kiszámoló - egy blog a pénzügyekről* (blog), 2018. december 26. https://kiszamolo.hu/atm-karacsonyra/.

Bankkártyás csalások – II. rész. ATM, POS terminál, étterem-sehol nem vagy biztonságban”.*Kiszámoló - egy blog a pénzügyekről* (blog), 2012. április 20. https://kiszamolo.hu/bankkartyas-csalasok-ii-resz-2/.

„Online bankolás biztonságosan – 10 tuti tipp | Wifipedia”. Elérés 2020. március 6. https://wifipedia.hu/10-tuti-tipp-a-biztonsagos-online-bankolasert.

Profit7. „Bankkártyás csalások – trükkök, megoldások”. profit7.hu, 2018. július 16. https://profit7.hu/ado-penzugy/bankkartyas-csalasok-trukkok-megoldasok.

Hankó Viktória

A koronavírussal kapcsolatos álhírek alakulása hazai és nemzetközi szinten 2020 tavaszán

1. Bevezetés

2020 a változások éve, ugyanis március 11-én a Egészségügyi Világszervezet (WHO) világjárvánnyá nyilvánította a koronavírust, Magyarországon pedig március 16-án kihirdetésre került a veszélyhelyzet – így a megszokottól eltérően szükséges volt az oktatást, valamint a munkák bizonyos részét otthonról megszervezni. A helyzet következménye többek között az is, hogy megnőtt az internetforgalom, hiszen a home office, illetve a digitális oktatás sikerességéhez a világháló igénybevétele elengedhetetlen. A kötelező tevékenységek elvégzése mellett azonban a felhasználók időt szakítanak a pihenésre, feltöltődésre is, így a különböző közösségi oldalak látogatottsága is megnövekedett az elmúlt időszakban. A munka és kikapcsolódás mellett az emberek nyilvánvalóan az aktuális hírekre is kíváncsiak, mind belföldön, mind külföldön egyaránt. Ez kitűnő alkalmat nyújt az álhírek megalkotóinak, terjesztőinek, hogy egy esetleges hiú reményt – megtalálták a vírus ellenszerét szalagcím például –, pánikkeltést – különböző koneók által – okozzanak a tevékenységükkel.

A tanulmányban felvezetésre kerülnek a témához tartozó alapfogalmak, bemutatásra kerül az általam használt szoftverhez kapcsolódó módszertan, a kutatás eredményei, s végül, de nem utolsó sorban egy nemzetközi kitekintést is eszközölök az összegzés előtt.

Elsőként szükséges definiálni magát a vírust, a jellemzőit, majd pedig az álhír fogalmát. A WHO tájékoztatása szerint az új koronavírus betegség – *COVID-19* – egy újonnan felfedezett fertőző betegség. Azok, akik enyhe vagy közepes légúti megbetegedést tapasztalnak speciális kezelés nélkül felépülnek. Azonban az idősebb emberek, valamint akik mögöttes egészségügyi problémával küzdenek nehezebben, súlyosabb tüneteket mutatva gyógyulhatnak ki a betegségből. A vírus elsősorban cseppfertőzéssel terjed. Jelenleg nincs specifikus oltás vagy kezelés a koronavírus orvosolására. Megelőzésként, vagy a terjedés lassítása érdekében annyit tehetünk, hogy gyakran mosunk kezet – akár alkoholos kézfertőtlenítővel, akár szappanos vízzel –, valamint kerüljük az arc érintését.

Emellett indokolt említést tenni az *egészségügyi információk*, hírek megjelenéséről a közösségi média felületén. A hétköznapi felhasználó általánosságban véve úgy aktív felhasználója az adott felületnek, hogy megosztják a történéseiket, tapasztalataikat főként az ismerőseikkel. A különböző médiaplatformok azonban lehetőséget nyújtanak különböző csoportok létrehozására is, ennek egyik példája az *egészségügyi tartalmakkal kapcsolatban szerveződő csoportok*. Ebben az egyének megoszthatják szövegesen, de akár képpel vagy videóval csatolva is a saját problémáikat, amire érkezhetnek a különböző tanácsok, javaslatok akár egy átlag polgártól, akár egy egészségügyben dolgozó személytől is. Ezáltal a közösségi média egyfajta lehetőséget kínál az egészségügyi szektor számára a szolgáltatások reklámozására, esetleges javítására . A pozitív eshetőségek mellett viszont ott vannak a negatív esetek is, melyek félrevezethetik a felhasználókat – egy világjárvány idején különösen fontos odafigyelni, hogy az adott tanács, hír, amit olvasunk mennyi valóságtartalommal is rendelkezik. Egy ilyen időszakban az átlagos hamis hírek, megosztások mellett megnőhet ezen tartalmak száma. Az egészségügyi felvezetés után áttérnék a tanulmány másik alapkövét adó fogalom tisztázására is, ami nem más, mint az álhír.

Az *álhír*, avagy hoax fogalmára különböző definíciókat találhatunk, amit a mögöttes szándék, a motiváció különféle formájának vagy intenzitásának vizsgálatával alkottak meg a kutatók. *Robert Nares* brit lelkész, filológus a

hoax szót csalásként határozta meg, ezzel szemben *Jan Harold Brunvand* szerint ezt a kifejezést csak abban az esetben lehetne használni, ha tudatos félrevezetésre irányuló kísérlet valószínűsíthető. *Lynda Walsh* (a Nevadai Egyetem professzora) álláspontja szerint néhány hoax anyagi természetű, így a „sikeres hoax elkövetők" gyakran pénzbeli nyereséghez vagy hírnévhez jutnak kitalációikat felhasználva, ennek értelmében a hoax és a csalás között nem feltétlenül tisztázott a különbség. *Alex Boese*, a Museum of Hoaxes honlap megalkotója úgy nyilatkozik, hogy a hoaxok közötti egyetlen különbség a nyilvánosság reakciójában rejlik. A *Magyar értelmező szótárban* az álhír definíciójaként azt találjuk, hogy az egy megtévesztő, valótlan hír. *Fenyvesi Judit* értelmezésében pedig az álhír olyan szándékosan előállított, hamis, de legalábbis problematikus információt tartalmazó, hitelesnek tűnő hír, amely virális jelleget ölt, függetlenül a forrás eredeti céljától, mely lehet humor vagy akár csalás is . Ezek egyik megjelenési formája az úgynevezett „DeepFake"-technológia gépi mélytanulás segítségével létrehozott tartalom. Ez lehetővé teszi olyan – akár valós időben közvetített audiovizuális – tartalmak közvetítését, amelyekben valakinek az arcát, illetve hangját rámontírozzák egy másik személyre. Az álhírek nagyobb része, melyek a közösségi médiában terjednek különböző sémák felismerésével könnyen azonosítható. Azonban egy ilyen esetben még a rutinos, az álhíreket nagy hatékonysággal felismerő illetőnek is nehéz dolga akad.

2. Módszertan

A közösségi média-analízis (social media analysis), amit gyakran *social listening*-nek is hívnak egyre népszerűbbé vált, hiszen a közösségi oldalak nagy hatással vannak az emberek életére, ugyanis azt várják el a polgároktól, hogy a közösségépítés és az interakció révén minél aktívabbak legyen az internetes felületeken, mint tartalom-készítők.

A tanulmány során a *SentiOne* szoftvert használtam, amely egy social listening szoftver. A program Európa teljes területén elérhető, lényege, hogy webes *szöveganalitikán* alapul és kulcskeresés alapján figyeli, indexálja, valamint elemzi a jelenlegi valamint a korábbi – akár 3,5 évre visszamenőleg – szöveges tartalmakat (amik önmagukban vagy akár kontextusban tartalmazzák a felhasználó által már előre megadott, illetve a platformra felvitt kulcskifejezések bármelyikét), melyeket az internetes fórumokon, blogokon, weboldalakon és közösségi média csatornákon tettek közzé. A kapcsolódó tartalmakat – kvantitatív kutatás céljából és ezt megkönnyítendő – különböző fókuszpontok és paraméterek alapján állítja össze a program, és ezeket interaktív grafikonokon szemlélteti. Ezen túl a kutatás elősegítését szolgáló módszertani és technológiai felépítés biztosítja a felhasználó számára az összes releváns indexált tartalmat, posztot, kommentet és cikket is, és ezek elemzését is – akár egyenként, akár pedig kategorizálva ("SentiOne"). Ennek lefuttatása után kirajzolódik számunkra egy *érzelmi skála*. Az érzelmi elemzés alapját John R. Crawford és Julie D. Henry munkássága képezi. Az ő nevükhöz fűződik a PANAS – *Positive and Negative Affect Schedule* (Pozitív és Negatív Érzelmi Térkép), amely a pozitív és negatív érzelmi állapotok gyakoriságát és intenzitását vizsgáló modell. A magas NA pontok a kellemetlen kötöttségeket jelentik, az alacsonyak viszont a tapasztalat hiányára utalnak. Ezzel szemben a magas PA a lelkesedést, éberséget jelent, az alacsony értékek pedig a letargiát és a szomorúságot jelzik.

3. Magyarországi helyzet

A *Political Capital* szerkesztői január 11. és február 11. közötti időszakban vizsgálta a SentiOne szoftverrel a koronavírussal kapcsolatos tartalmakat. A kutatás során kiválasztottak bizonyos Facebook-oldalakat (például: Minden Egyben Blog), amik a hozzájuk tartozó weboldalról linkeltek tartalmat a közösségimédia-profilukra. A vizsgálatban olyan *keresőszavakat* határoztak meg, mint „koronavírus", „Vuhan", „Wuhan", „vírus", illetve „karantén". A vírust azért volt szükséges külön is megemlíteni, mert egyes dezinformációs portálok előszeretettel hivatkoztak „*Vuhan-vírusként*" a járványra. A nem releváns cikkek eltávolításra kerültek. Az eredmény

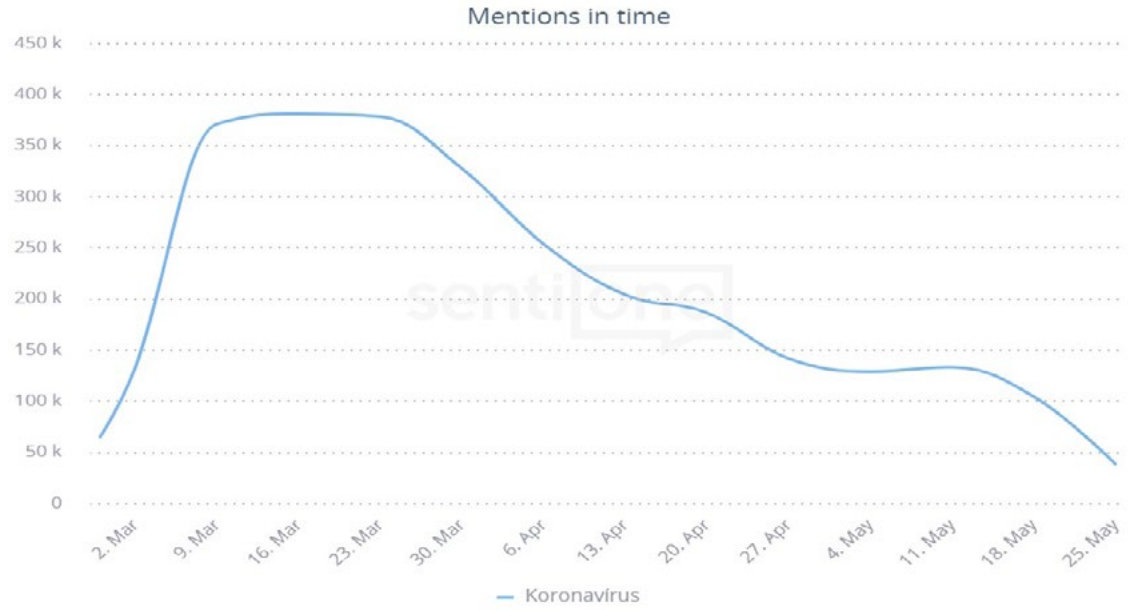
a magyar médiateret négy csoportra osztotta: „népirtás-elméletek”, „biológiai fegyver” elméletek, „világvége”-elméletek, valamint a vírus „ellenszerét” taglaló cikkek.

Kutatásom során a *Urbanlegends* oldal kategorizálását vettem alapul, amely hat hírkategóriába osztja a dezinformációs portálokat: kitalált hírek, kattintásvadász cikkek, politikailag elfogult tartalmak, áltudományos cikkek, konteós cikkek, és szatirikus anyagok . Ezek közül az áltudományos cikkek csoportján belül keresgéltem, és a Facebook platformján is megjelenő oldalak közül választottam ki a *Titok terminál*, valamint a *Mindenegyben Blog* hírmegosztókat. Ezek mellett a Political Capital által vizsgált egyik oldal – *A világ titkai* – tevékenységét is megfigyeltem. Ez a három oldal rendelkezik a legtöbb követővel, így célszerűnek láttam az ő tevékenységüket feltérképezni, hiszen ezen oldalak posztjai jutnak el ezáltal a legtöbb magyar felhasználóhoz.

Keresőszóként csupán a „*koronavírus*”-t használtam a vizsgált időszakban, ami *február 28*. és *május 27*. között volt meghatározva, illetve beállításra került, hogy csak *magyar* nyelvű találatok jelenjenek meg.

4. Eredmények

A meghatározott időszakban összességében 2.813.601 bejegyzés született a közösségi média különböző felületein, ebből *2.768.910* csak a Facebookon, ezek változását az alábbiakban látható 1. ábra szemlélteti. Jól látható, hogy az idő múlásával csökkent a bejegyzések száma. A megosztott tartalmak közül kiemelkedő az a 24.hu által megosztott cikk, mely március 29-én látott napvilágot. A bejegyzés a felhalmozott élelmiszerek kidobálásáról szól, és kimutatható a felhasználók felháborodása – ezt a 3487 „*dühös*” reakció támasztja alá.



1. ábra Koronavírussal kapcsolatos bejegyzések számának alakulása a vizsgált időszakban
(Forrás: saját szerkesztés a SentiOne adatbázisa alapján)

A továbbiakban a három kiemelt oldal tevékenységének vizsgálata kerül bemutatásra, ezek közül elsőként az oldalak jellemzőinek ábrázolása:

1. táblázat Kiemelt oldalak legfőbb adatai (forrás: saját szerkesztés)

Oldal neve	Követők száma	Kulcsszavas bejegyzések száma
Mindenegyben Blog	684.929 fő	294
A világ titkai	106.902 fő	110
Titok terminál	51.933 fő	86

A Mindenegyben Blog lenépszerűbb bejegyzése 404 megosztást és 831 hozzászólást tudhat magáénak. A bejegyzés egy felgyógyult beteg örömhírét tartalmazza. A világ titkai portálon egy kísérleti vakcináról szóló poszt a legnépszerűbb *5166* megosztással, és mindössze *32* hozzászólással. A Titok terminál oldalán pedig a média viselkedés vitató lett a legfelkapottabb, amely *1728* megosztást és *45* kommentet tudhat magáénak. A bejegyzésekre összesen *20.326* megosztás, valamint *5.832* hozzászólás érkezett. Vannak olyan tartalmak is, melyek többször jelentek meg, egyik esetben figyelmen kívül hagyva, a későbbiekben pedig óriási figyelmet elnyerve.

A bejegyzések áttekintése során a Political Capital csoportosítása ebben az időszakban is tökéletesen kirajzolódik, azonban kiegészülnek a *vírus végét előrejelző cikkekkel*. Bizonyos tartalmak készítői megírták, hogy a szakértők kimondták pontosan a vírus megszűnésének dátumát, de van amelyik azt taglalja, hogy egy észak-olasz városban már ki is iktatták a betegséget. A vizsgált időszakban legnagyobb számban az *ellenszert*, vagy különböző megoldásokat kínáló bejegyzések láthatóak. Ezen cikkek szerint napokon belül kész lehet az ellenszer, vagy már egy magyar labor elő is állította. Emellett megjelennek olyanok is, melyekben brit tudósok nyilatkoznak olyan kezelésről, amely remények szerint csökkentheti a hatásokat a súlyosabb fertőzötteknél. Jelen vannak továbbá a *vírus szándékos elterjesztését* taglaló cikkek, amit főként Amerikához kötik, azonban van olyan írás is, amely Angela Merkelre utal, aki 2019 novemberében látogatta meg Kínát. További két kategória a korábban említettek mellett a *biológiai fegyverként* említő – konkrétan biológiai világháborúként hivatkoznak rá –, valamint a *világvége elméleteket* – mely szerint a vuhani hatóságok meghamisították a betegekre vonatkozó adatok számát – tartalmazó cikkek.

Az érzelmi megoszlás vizsgálata során a következő eredmények rajzolódtak ki:

2. ábra A bejegyzések érzelmi megoszlása a vizsgált portálokon (Forrás: saját szerkesztés a SentiOne adatai alapján)

Jól látható, hogy A világ titkai és a Titok terminál esetében *azonosak* az érzelmek megoszlásai, míg a Mindenegyben Blog esetében bizonyos *eltérést* tapasztalhatunk. Legnagyobb arányban *közömbösséget* vált ki az emberekből a tartalom, azonban a negatív érzelmek aránya nagyobb, mint a pozitívoké. Az utóbbi két tartalommegosztó esetében csupán 1-1 bejegyzésnél volt kimutatható a pozitivitás.

5. Következtetések

Érdekes következtetések vonhatók le a korábban feltárt eredményekből. Nyilvánvalóvá válik az 1. ábrán látható diagramból, hogy az idő múlásával a megadott kulcsszót tartalmazó tartalmak száma folyamatosan csökken. Ennek valószínűsíthető oka a járvány enyhülése. Az eredményekből kiderül továbbá, hogy a koronavírussal kapcsolatosan megosztott tartalmak tekintetében az álhíreket megosztó oldalak kis részt tesznek ki. Azonban a bejegyzések megosztásának, valamint a hozzászólások száma ahhoz képest igen magas. Így az a következtetés vonható le, hogy hiába a viszonylag kevés bejegyzés a megosztások magas számának következtében több százezer állampolgárhoz eljuthattak/eljuthatnak ezek a hamis információt terjesztő írások.

Az álhírekkel kapcsolatos csoportosítás egyezése a korábbi időszakkal azt mutatja, hogy a készítők ugyanolyan jellegű tartalmakat gyártanak, egy bejegyzést akár többször is megosztva. Kiderül az is, hogyha egy poszt nem a kívánt népszerűséget éri el – azaz figyelmen kívül hagyják a felhasználók – akkor a későbbiekben újra megosztásra kerül az oldal által. Megfigyelhető emellett az is, hogy az általam vizsgált időszakban inkább az ellenszerrel, különböző gyógymódokkal, tünetek kezelésével kapcsolatos kattintásvadász cikkek alkotják a legnépesebb részt a közétett írásokon belül, valamint ezek vonzzák a legtöbb ember figyelmét is. Ez arra enged következtetni, hogy az embereket inkább a betegség kezelése, gyógyítása, mintsem annak eredete foglalkoztatja. Emellett az új kategória – ami a járvány végét jósolja előre – megjelenése azt a jelentéstartalmat hordozza magában, hogy a polgárok egyre inkább vissza szeretnének térni az életük eredeti rendjéhez, úgy, mint a kirándulások, idősebb szerettek meglátogatása, vagy éppenséggel a különböző rendezvények látogatása.

Az érzelmek megoszlását figyelembe véve jól kirajzolódik a közömbösség, valamint még ha kisebb mértékben is, de a negatív érzések meghaladják a pozitívokat. Ezek alapján az emberekből nem váltanak ki szélsőséges érzelmeket az adott tartalmak. Az érdeklődés hiányát kifejező érzelmek nagy száma utalhat arra, hogy a felhasználók hitelesebb forrásokból tájékozódnak – erre kitűnő példa a Kormány által létrehozott, naprakész információkat nyújtó koronavírussal kapcsolatos weboldal. Ezen túlmenően, ha a két szélső értéket nézzük – a negatív érzések többségét – azt mondhatjuk, hogy inkább rossz érzést, ellenszenvet keltenek a bejegyzések. Az, hogy a Mindenegyben Blog bejegyzései esetében 15%-os az arány, míg a másik két portál tekintetében csak 7-7% abból következik, hogy a blog nagyobb követőbázissal rendelkezik, illetve több tartalmat is osztott meg a vizsgált időszakban, így jobban kirajzolódtak az érzelmek megoszlásai.

A valótlan híreket megosztó oldalak nem fognak teljes mértékben eltűnni a közösségi média felületéről, de talán csökkenhet a látogatottságuk, tartalmaik megosztásának a száma különböző felhívásokkal. Erre kitűnő példa az a 2020. márciusában megjelent bejegyzés, melyet az *Európai Parlament* tett közzé honlapján a koronavírussal kapcsolatos álhírek terjedéséről. A cikk a példák mellett kitér arra is, hogy mit tesz az Európai Unió (továbbiakban: EU) ezen hírek terjedése ellen – *külön uniós honlap* lett létrehozva a koronavírussal kapcsolatos információkat tartalmazó híreknek. Emellett olvashatunk még a terjesztés okairól is, s említést tesznek az *EU félretájékoztatással foglalkozó blogjáról* is, ahol további információkat kaphatunk az álhírekről (angol nyelven). A bejegyzésben szó esik továbbá a félretájékoztató hírek felismeréséről, valamint arról az eshetőségről is, ha a baráti körünkben oszt meg valaki valótlan történetet [1].

1 „Félretájékoztatás és álhírek: vírusszerűen terjednek a COVID-19 járvány idején | Hírek | Európai Parlament”, 2020. március 30., https://www.europarl.europa.eu/news/hu/headlines/society/20200326STO75917/felretajekoztatas-es-alhirek-virusszeruen-terjednek-a-covid-19-jarvany-idejen.

6. Nemzetközi kitekintés

Nemzetközi színtéren is megjelentek olyan cikkek, melyek a koronavírussal kapcsolatos álhíreket taglalják. Túlnyomórészt a valótlan tartalmakat megosztó írások bemutatása van jelen, illetve bizonyos értekezések az adott ország állampolgárinak hír megosztási hajlandóságait, hírek valódiságának vizsgálatát taglalja. Ezek közül emelném ki az alábbi két tanulmányt.

A Kínával szomszédos Japán földrajzi helyzetéből adódóan több álhír elszenvedője is volt az elmúlt időszakban – erről *Kazuki Shimizu* ír egy cikkében. Írásában kiemeli azt a január 29-én megjelent cikket, amely egy német oldalra hivatkozta hozta le a hírt, miszerint *elmarad a 2020-as Tokiói Olimpia*[2] . Kitért arra is, hogy az álhírek az okai annak a xenofóbiának is, amely egy január 24-én keletkezett cikk miatt alakult ki, miszerint kínai utasok Wuhan tartományból átcsúsztak a Kanasi Nemzetközi Repülőtér ellenőrzésén. Bár a reptér vezetősége tagadta ezt a tényt, Japánban megjelent a kínai polgárok diszkriminációja. Ennek eredményeként terjedt el a Twitteren a *#ChineseDon'tComeToJapan* trend, mely a Kínából érkező embereket piszkosnak, érzéketlennek, sőt egyesek bioterroristának minősítik [3]. Ez már egy ártalmasabb szintje az álhírek terjedésének, hiszen egy egész nemzet diszkriminációját okozta egyetlen valótlan tényeket terjesztő tartalom.

Egy amerikai tanulmány alapja az a két részből álló kísérlet, melynek első fázisát 2020. március 12-én végezték 853 résztvevővel, a második fázist pedig 2020. március 13-15. között 856 fő részvételével. Az első fázis estében a kitöltés megkezdése előtt két kérdésre kellett megadnia a választ a résztvevőnek. Az első kérdés úgy szól, hogy „*Mennyire aggódik a COVID-19 (új koronavírus) miatt?*" – amelyre egy 0-tól 100-ig terjedő skálán tudták bejelölni válaszukat, ahol a 0 az egyáltalán nem aggódik, a 100 pedig a rendkívül aggódik értéket jelölte. A második által pedig arra voltak kíváncsiak, hogy „*Milyen gyakran ellenőrzik a COVID-19-el kapcsolatos híreket?* – ebben az esetben egy 1-től 5-ig terjedő skálán lehetett megadni a választ, ahol az 1 a soha választ, míg az 5 a nagyon gyakran-t jelentette. Ezután következett a *hírértékelési* feladat, amelynek keretében 15 igaz és 15 hamis cím került megalkotásra, és azok valódiságát kellet a résztvevőknek megítélni, majd arra válaszolni, hogy megosztanák-e online[4] - mindkét esetben igen vagy nem lehetőséget lehetett megadni. Mindezek után a résztvevőknek 6-elemű kognitív reflexiós tesztet kellett elvégezni, továbbá egy általános tudományos felmérőt is, valamint a készítők azt is feltérképzeték, hogy az adott személyek mennyire hajlamosak felkeresni az orvost akár egy kisebb probléma esetén is – egy orvosi maximalizáló-minimalizáló skála felállításával –, és végül a politikai ideológiát célzó kérdéseket eszközöltek demográfiai és fiskális témakörök érintésével. A válaszadások közé beszúrtak a tanulmány készítői három kérdést, amelyek a *figyelem ellenőrzésére* szolgáltak.

A második fázis során hasonlóan alakult a teszt felépítése. Az érdemi rész előtt azonban nem koronavírussal kapcsolatos kérdéseket tettek fel a készítők, hanem a résztvevő *pontosságát felmérő* szalagcímet kellett értékelniük – aminek szintén nem volt köze a COVID-19-hez. A hír megosztására vonatkozó részben ugyanazokat a valós, illetve hamis címeket kapták meg, mint amik az első tanulmányban szerepeltek annyi eltéréssel, hogy nem igen vagy nem válasz megadásával kellett dönteniük, hanem egy 1-től 6-ig terjedő *skálán* kellett besorolniuk a hitelességüket. Végül, ebben az esetben is jelen voltak a figyelem ellenőrzésére szolgáló random kérdések.

2 Szerzői megjegyzés: az már más kérdés, hogy a későbbiekben a Nemzetközi Olimpiai Bizottság márciusban bejelentette, hogy valóban nem kerülnek megrendezésre idén az ötkarikás játékok. Forrás: 2020 Olympics - Next Summer Olympic Games | Tokyo 2020 [WWW Document], n.d. . International Olympic Committee. URL https://www.olympic.org/tokyo-2020 (accessed 5.27.20).

3 Kazuki Shimizu, „2019-NCoV, Fake News, and Racism", *The Lancet* 395, sz. 10225 (2020. február 29.): 685–86, https://doi.org/10.1016/S0140-6736(20)30357-3.

4 Szerzői megjegyzés: az alkalmazott valós és hamis hírek címsorát a következő oldalon lehet megtekinteni: https://osf.io/7d3xh/, ezen belül a COVID-19 New Content fület kell lenyitni.

Az *eredmények* a következők: a tanulmány első időszakában résztvevők hajlandóak voltak hamis híreket megosztani a koronavírusról még akkor is, ha képesek beazonosítani azok valótlanságát, amennyiben közvetlenül kérdezik meg tőlük. Ezen kívül kimutatható az is, hogy azok az egyének, akik alacsonyabb tudományos ismeretekkel rendelkeznek rosszabb helyzetben vannak az álhírek megítélésével kapcsolatban – mind a besorolás, mind pedig a megosztási arányokat tekintve. A második tanulmány résztvevői esetében másképp alakultak az eredmények. Az elején beiktatott pontosságot vizsgáló feladat, valamint a második részben a skála alkalmazása az eldöntendő kérdések helyett az egyének sokkal jobb eredményt értek el. Ez a kis beavatkozás elegendő volt arra, hogy több, mint kétszer annyian kiszűrték a valódi és a nem valódi címeket [5].

7. Összegzés

Mint az a fentiekből kiderül a 2020-as év különböző kihívások elé állított minket, ezek közé tartozik maga a koronavírus világjárvány, illetve az ezzel kapcsolatban megjelenő álhírek, mind hazai, mind pedig nemzetközi szinten. Hazai szinten kimutatható, hogy az idő múlásával csökken azon bejegyzések száma a közösségi médiában, amely a koronavírus keresőszót tartalmazza. Emellett a koronavírussal kapcsolatos álhírek, melyek a Facebook felületén megjelenő, álhíreket készítő oldalak által megosztott tartalmak a korábbi négy kategória – „népirtás-elméletek", „biológiai fegyver" elméletek, „világvége"-elméletek, valamint a vírus „ellenszerét" taglaló cikkek – most már kibővültek egy új elemmel – vírus végét előrejelző cikkek. Ezek a hírek viszont a felhasználókból az esetek 90%-ban közömbösséget váltanak ki, nagyon kevés esetben tapasztalhatunk pozitív vagy negatív irányba való elmozdulást. Azokban a bizonyos kivételes esetekben pedig a negatív reakciók vannak nagyobb arányban. Segítségünkre van a hiteles tájékozódáshoz a Kormány koronavírussal foglalkozó honlapja mellett az Európai Parlament által létrehozott weblap is, amely a hírek mellett tanácsokat is fogalmaz meg a valótlan hírek felismerésével kapcsolatban.

Nemzetközi szinten főként a valótlan tartalmakat megosztó írások bemutatását megfogalmazó írásokkal találkozhatunk. Emellett jelent vannak még az adott ország állampolgárinak hír megosztási hajlandóságait, hírek valódiságának vizsgálatát elemző tanulmányok is. A kiemelt két cikkből az első esetében a megjelent álhírek margójára írható egy rasszista trend megjelenése. Utóbbi értekezés pedig az amerikai állampolgárok hírmegosztási szokásait vizsgálva megmutatja, hogy amennyiben pontosabban vizsgálják a címeket, többen megállapítják a valós és valótlan írásokat.

5 Gordon Pennycook és mtsai., „Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy Nudge Intervention", preprint (PsyArXiv, 2020. március 17.), https://doi.org/10.31234/osf.io/uhbk9.preprint (PsyArXiv, 2020. m\\uc0\\u225{}rcius 17.

Felhasznált irodalom

Auer Ádám, és Joó Tamás, szerk. *Hálózatok a közszolgálatban*. Budapest: Ludovika Egyetemi Kiadó, 2019.

„Burjánzanak az álhírek a koronavírus nyomában", 2020. https://politicalcapital.hu/hirek.php?article_id=2502.

Crawford, John R., és Julie D. Henry. „The Positive and Negative Affect Schedule (PANAS): Construct Validity, Measurement Properties and Normative Data in a Large Non-Clinical Sample". *British Journal of Clinical Psychology* 43, sz. 3 (2004): 245–65. https://doi.org/10.1348/0144665031752934.

„Félretájékoztatás és álhírek: vírusszerűen terjednek a COVID-19 járvány idején | Hírek | Európai Parlament", 2020. március 30. https://www.europarl.europa.eu/news/hu/headlines/society/20200326STO75917/felretajekoztatas-es-alhirek-virusszeruen-terjednek-a-covid-19-jarvany-idejen.

Fenyvesi Judit. „Határok átlépése koncepciózus hoaxokkal". *JEL-KÉP* 4 (2015). https://doi.org/10.20520/Jel-Kep.2015.4.63.

Lemon, Narelle. „Collaborating and co-curating knowledge: Participatory engagement on Twitter between galleries, libraries, archives and museums (GLAM) and education audiences". *Australasian Journal of Popular Culture* 7, sz. 1 (2018. március 1.): 93–106. https://doi.org/10.1386/ajpc.7.1.93_1.

Marinov Iván. „Megtévesztő magyar híroldalak listája 2020", 2020. január 13. https://www.urbanlegends.hu/2020/01/megteveszto-magyar-hiroldalak-listaja-2020/.

Pennycook, Gordon, Jonathon McPhetres, Yunhao Zhang, és David Gertler Rand. „Fighting COVID-19 Misinformation on Social Media: Experimental Evidence for a Scalable Accuracy Nudge Intervention". Preprint. PsyArXiv, 2020. március 17. https://doi.org/10.31234/osf.io/uhbk9.

„SentiOne". Elérés 2020. május 27. https://sentione.com/hu/tudasbazis.

Shimizu, Kazuki. „2019-NCoV, Fake News, and Racism". *The Lancet* 395, sz. 10225 (2020. február 29.): 685–86. https://doi.org/10.1016/S0140-6736(20)30357-3.

Viviani, Marco, és Gabriella Pasi. „Credibility in social media: opinions, news, and health information - A survey". *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, 2017. június 4., e1209. https://doi.org/10.1002/widm.1209.

World Health Organization. „Coronavirus", 2020. https://www.who.int/westernpacific/health-topics/coronavirus.

Kalmár Vanessza

Esettanulmány az aszimmetrikus háború természetének bemutatására az első és a második orosz-csecsen háború mentén

1. Bevezetés

Jelen tanulmány fő hangsúlya a hadtudomány egy vitatott részével, az aszimmetrikus konfliktusok természetével foglalkozik. Vizsgálja a terrorizmus, valamint a gerilla hadviselés közötti különbségeket, hasonlóságokat, illetve ezek ötvözését a harcok során. Ennek aktualitását mutatja, hogy a nemzetközi és a hazai szakirodalomban is egyre nagyobb teret nyertek az utóbbi időben az aszimmetrikus konfliktusok. A tanulmány kísérletet tesz ennek a dinamikájának bemutatására az első és a második orosz-csecsen háború elemzésével. Oroszországi Föderáció számára stratégiailag és gazdaságilag is kulcsfontosságú helyen fekszik Csecsenföld. Az elszakadását sem Föderáció, sem a nemzetközi közösség nem támogatta. A konfliktus szeparatista mozgalomból egy kiterjedt észak-kaukázusi terrorista mozgalommá nőtte ki magát.

1.1 Fogalmi keretek

Mi a terrorizmus?

A terrorizmus definiálására való vállalkozás azzal a problémával kezdődik, hogy nincs egységesen és nemzetközileg elfogadott fogalom. A dolgot viszont megkönnyíti, hogy rengeteg nemzetközi szervezet megfogalmazta már, hogy számukra mit is jelent a terrorizmus[1]. A tanulmánynak nem célja ezeket felsorolni, összehasonlítani és egy átfogó definíciót létrehozni, viszont a téma értelmezésének megkönnyítése érdekében jó, ha először megnézzük (a teljesség igénye nélkül) milyen összetevői, fogalmi elkülönítései vannak a terrorizmusnak. Ehhez segítségül hívom a Global Terrorism Database (továbbiakban: GTD) 2019 októberi kódkönyvében leírtakat.

A GTD úgy határozta meg, hogy a terrorcselekmény fenyegetés vagy tényleges felhasználása az illegális erőnek és az erőszaknak egy nem állami szereplő által politikai, gazdasági, vallási vagy társadalmi cél elérésére a félelem, a kényszerítés vagy a megfélemlítés útján. Fontolóra veszi a GTD, hogy az az adatbázisába kerüljön egy esemény, ha az három tulajdonságnak megfelel: (1) az eseménynek szándékosnak kell lennie; (2) erőszakot vagy közvetlenül erőszakkal való fenyegetést kell magában foglalnia; (3) az elkövetőinek szubnacionális szereplőknek kell lenniük. Ezen túlmenően még a következő három kritériumból legalább kettőnek fenn kell állnia ahhoz, hogy egy esemény bekerüljön a GTD-be.

1. kritérium: a cselekvésnek politikai, gazdasági, vallási vagy társadalmi cél elérésére kell irányulnia. A gazdasági célok szempontjából szisztematikus gazdasági változásokra kell törekednie.
2. kritérium: bizonyítéknak kell lenni, arra, hogy az erőszak, a megfélemlítés, vagy más üzenet közvetítését nagyobb közönségnek akarják továbbítani, mint a közvetlen áldozatok (akik általában civilek).
3. kritérium: a fellépésnek a törvényes hadviselési tevékenységek keretein kívül kell lennie (vagyis a cselekménynek a nemzetközi humanitárius jog által megengedett paramétereken kívül kell állnia, amennyiben nem kombattánsokat céloz meg). [2]

A Stockholm Nemzetközi Békekutató Intézet 23. számú jelentésében. Ez az Oxford University Press által kiadott egyetemi tankönyvet takarja „Terrorism in asymmetrical conflict. Ideological and Structural Aspects”

1 Éberhardt (2019) 40.
2 Codebook: Inclusion Criteria and Variables. 10-11.

címmel. A következőket találhatjuk a terrorizmus behatárolásához, amit az alábbi komplex táblázat (1. táblázat) segítségével teszek áttekinthetővé.

1. táblázat Tipológia Forrás: Ekaterina (2008) 5-11. (A táblázat a szerző szerkesztése a forrás szövege alapján)

Tipológia	Kategóriák	Kritériumok	Megjegyzés
Területi kiterjedtség szerint	1. Helyi, 2. Regionális, 3. Globális szint	-	-
Domináns motivációk szerint	1. Forradalmi anarchisták (baloldali, jobboldali szélsőségesek); 2. Nacionalisták (nemzeti felszabadító mozgalmak etno-szeparatista szervezetek) 3. Vallási terrorizmus (ideológiáját vallási követelmények uralják).	Nem mindig tükrözi pontosan a terrorista csoportok motivációinak és ideológiáinak komplex jellegét. Mindig politikai vetülettel rendelkeznek.	Probléma: a) kevés csoport rendelkezik „tiszta” motivációval, b) a domináns cél egyértelműsége és a célok összeolvadása idővel
Funkcionalitás	1. Klasszikus (békeidőben pl.: kommunisták és más baloldali terroristák 1970-es 1980-as évek Nyugat-Európájában) 2. Konfliktusokkal összefüggő (pl.: csecsen, kasmír, palesztin, tamil) 3. Szuperterrorizmus (globális cél pl.: Iszlám Állam[3])	a) a csoport végső céljainak szintje (globális vagy lokalizált) b) kapcsolódnak a terrorista tevékenységek egy tágabb fegyveres konfrontációhoz	-

Aszimmetrikus fegyveres konfliktusok, aszimmetrikus hadviselés

Hasonlóan a terrorizmushoz, itt sem fogunk találni élesen lehatárolt definíciókat, olyanokat, amelyeket mindenki egységesen elfogadna. Fontos látni, hogy az aszimmetrikus konfliktus nem csupán katonai kifejezés, mint az aszimmetrikus hadviselés, de mindkettő az új típusú fenyegetések és kihívások közé tartoznak, amelyek egyre változatosabbak, ezért a velük való foglalkozás és a vizsgálatuk megkerülhetetlen.[4] A második világháború óta eltelt időt tekintve közel 160 fegyveres konfliktus zajlott a világon és ezek több mint háromnegyede sorolható az aszimmetrikus konfliktusok kategóriájába.[5]

Mivel nincs meghatározott definíciónk, így az a kérdés, ha felsoroljuk az aszimmetrikus háborúval kapcsolatos tulajdonságokat, mennyi és melyik tulajdonságoknak elegendő érvényesülni közülük ahhoz, hogy egy konfliktust ide soroljunk. A Berglund – Souleimanov 2020-as tanulmányából kiindulva megkülönböztethetünk három aszimmetriát a konfliktusokban: [6]

(1) a felek eltérő jogi státuszokkal rendelkeznek (állami szereplők és a nem állami szereplők)
(2) különböző képességekkel rendelkeznek (az erősebb fél fejlett fegyverzettel, technológiai, gazdasági, demográfiai és egyéb strukturális erőforrásokkal felszerelve küzd egy gyenge szereplővel, akik nem férnek hozzá ilyen erőforrásokhoz)
(3) különböző stratégiákat alkalmaznak (az egyik szereplő [az erősebb] közvetlen stratégiákat, míg a másik szereplő közvetett stratégiákat alkalmaz).

3 Resperger (2018) 74.
4 Stepanova (2008) 15.
5 Porkoláb (2016) 16-17.
6 Berglund – Souleimanov (2020) 87.

Az, hogy ezek alapján meghatározzuk mennyi és melyik tulajdonságoknak elegendő érvényesülni nem kétoldalú „minden vagy semmi” elven rendeződik, hanem inkább fokozatokat lehet ebből leszűrni (2. táblázat), amelyeket a szürke színek szemléltetnek a táblázatban. Minél szürkébb a sor, annál biztosabban beszélhetünk aszimmetrikus konfliktusról.[7]

2. táblázat: Forrás: BERGLUND, Christofer – SOULEIMANOV, Emil Aslan (2020): What is (not) asymmetric conflict? From conceptual stretching to conceptual structuring. Dynamics of Asymmetric Conflict, 2020/1. 94. A szerző szerkesztése.

Jogi státusz	Képességek	Stratégiák	Aszimmetria foka
Igen	Nem	Nem	**Periférikus**
Nem	Igen	Nem	
Nem	Nem	Igen	
Igen	Igen	Nem	**Általános**
Nem	Igen	Igen	
Igen	Nem	Igen	
Igen	Igen	Igen	**Klasszikus**

Az aszimmetrikus hadviselés egy katonai fogalom, a hadviselés egy formája. Egységes fogalmat itt is nehéz találni, de van egy tanulmánykötet, ami az első olyan munka magyar nyelven, amely átfogóan foglalkozik az aszimmetrikus hadviseléssel. Ebből az aszimmetrikus hadviselés fogalmát kiolvashatjuk: „Pontosan körvonalazott politikai célok érdekében folytatott, gyakran több szervezet ideológiai, vallási, etnikai közösségén alapuló katonai, és nem katonai műveleteket, eljárásokat és módszereket alkalmazó közvetlen és közvetett hatásokra építő és egymás hatásait felerősítő, a biztonság különböző dimenziónak területét veszélyeztető harcmodor, főként harcászati eljárás, melyek együttes hatásával kényszeríthetjük akaratunkat az ellenségre.”[8] A műveletekben az állam (vagy államok) ellen a nem állami szereplők harcolnak. A szereplők erőinek, eszközeinek az aránya eltér egymástól, tehát van egy gyengébb és egy erősebb fél. Stratégiai cél az ellenség kifárasztása, akaratunk rákényszerítése, az ellenség akaratának a megtörése, kivéreztetése. Ezekre a fő módszerek a gerilla, a felkelő és a terrorista módszerek.[9] A gyengébb fél nyilvánvaló minimális követelménye, hogy ne veszítsen, ha fenntartják a háborús helyzetet. Mindezek mellett kisebb anyagi befektetést igényelnek a konfliktusok a gyengébb féltől. Ennek elérése érdekében a felkelőknek nemcsak verhetetlennek kell lenniük, de annak is kell tűnniük az erősebb fél társadalma részére, így az hosszú távon a politikai akaratának feladásához vezethet.[10] A halott-sebesültek arányát tekintve 1:6-14. A hadviselések közül a legmagasabban ebben jelenik meg, míg a hagyományosnál 1:3; a hibridnél 1:2,5-5 ez az érték.[11] Az aszimmetriát leglátványosabban az irreguláris hadviselés különböző formái (elsősorban a gerillaháború és a terrorizmus) kapcsán érhetjük tetten.[12]

7 Berglund – Souleimanov (2020) 92-94.
8 Resperger – Kis – Somkúti (2013) 25.
9 Resperger (2018) 80.
10 Bakos (2015) 100-101.
11 Resperger (2018) 80.
12 Gazdag – Remek (2018) 112.

Terrorizmus és a gerillaharc, mint az aszimmetrikus konfliktusok egyik taktikája

Aszimmetrikus fegyveres konfliktusok során a terrorizmust szisztematikus taktikaként alkalmazzák a harcosok (például csecsen, kasmír, palesztin, tamil harcoló csoportok). A politikai céljai ezeknek a harcosoknak lehetnek például a hatalom megragadása egy államban, új állam létrehozása vagy harc az idegen megszállás ellen. Általában nem terjed túl a helyi vagy regionális határokon. A konfliktusokkal összefüggő terrorizmust olyan csoportok gyakorolják, amelyek némi helyi támogatást is élveznek. Hajlamosak többféle erőszakos cselekedetet alkalmazni egyszerre. Például gyakran kombinálják a terrorizmust gerilla taktikával a reguláris hadsereg ellen.[13]

A másik szisztematikus taktika a gerillaharc. Ennek keretében viszonylag kis alakulatok harcolnak szétszórtan, akik kerülik a közvetlen összecsapást, és hosszan elnyúló, sok kisebb támadást levezénylő háborúra rendezkednek be. Az aszimmetrikus háborúk legelterjedtebb taktikája. A terrorizmushoz hasonlóan a gerillaharcok is elhúzódó küzdelmet feltételez, de a gerilla-hadviselés elsősorban a fizikai összecsapásra épít, míg a terrorizmusnál a lélektani elemek állnak a középpontban. A terrorizmus nem tesz különbséget harcolók és nem harcolók között, illetve a háborús övezetek határait sem tiszteli.[14]

Összegezve az eddigieket, tehát a terrorizmus az erőszak szándékos felhasználása vagy azzal való fenyegetés egy nem-állami szereplő által a politikai célok elérése érdekében. A terrorizmus nem maga a politikai cél, hanem a politikai cél elérésének sajátos taktikája. A civilek, mint az erőszak közvetlen célpontja jelennek meg a terrorizmus útjában, viszont nem ők a terroristák üzenetének szándékos végső címzettjei, hanem az állam vagy azok csoportja. Ez egy taktika, amit az erős fél ellen fegyverként használ a gyenge fél, amely nem csak fizikailag és műszakilag gyengébb, hanem egy aszimmetrikus konfrontációban alacsonyabb státusszal is rendelkezik. A taktika funkciója, hogy a gyenge fél kompenzálja a gyengeségeit a katonai dimenzióban. [15] Végül szem előtt kell tartani, hogy nem minden aszimmetrikus fenyegetés okoz fegyveres konfliktust és nem is feltétlenül kapcsolódik ahhoz. Az aszimmetrikus konfrontációkban a felkelés vagy a gerillaharc továbbra is a leggyakoribb a többi aszimmetrikus taktika közül.[16]

2. Esettanulmányok

Az előzőekben átnézett elméletet ültessük át a gyakorlatba. Ehhez kiválasztottam az orosz-csecsen háborúkat, mert itt – a 2. táblázat alapján – a klasszikus aszimmetriáról van szó. A harcok során a csecsen milíciák egyaránt használták a gerilla és a terror akciókat, mint taktikákat az ellenség kifárasztására és akaratuk megtörésére. Mindenféleképpen meg kell említenem, hogy a csecsenföldi konfliktusról olvasva a szakirodalmat a kérdés rendkívül bonyolult és ellentmondásos az elemzők körében is.[17]

2.1 Orosz-csecsen helyzet

Az első háború 1994-1996

Az Etno-szeparatizmus térnyerése

Csecsenföld földrajzi fekvése és a történelme az, amelyek a puskaporos hangulatot kialakította. A konfliktus közvetlen előzménye, hogy a Szovjetunió széthullásával 1991 októberében kiáltották ki a Csecsen Köztársaság

13 Stepanova (2008) 10.
14 Répási (2011) 36-37.; Stepanova (2008) 10.
15 Stepanova (2008) 11-14.
16 Stepanova (2008) 14-23.
17 Chechnya: Russia's Experience of Asymmetrical Warfare.http://www.southasiaanalysis.org/paper619

függetlenségét élén Dzsohar Dudajevvel, de ezt egyetlen állam sem ismerte el. Az új állam gazdasági helyzete romokban volt, amit fegyvercsempészettel, szervezett bűnözéssel és főleg a Csecsenföldön áthaladó orosz érdekeltségű kőolajvezeték lecsapolásával akarták helyre billenteni. Ez azért volt hatalmas probléma az oroszoknak, mert az itt áthaladó vezetékeknek kulcsfontosságú szerepe volt, hogy megakadályozza az Oroszországot elkerülő gáz- és kőolajvezeték projektek megvalósulását. Az új csecsen politikai elit többséget a bűnözés világából érkezők, köztük nagy számban a külföldről hazatérő „csecsen maffia" tagjai, vagy az általuk támogatott személyek tették ki, akik saját hadsereggel kívántak rendelkezni. Ezáltal a szervezett bűnözői csoportoknak közvetlen és napi befolyása volt a közigazgatásra. A társadalom kezdeti örömét a függetlenedésről gyorsan felváltotta a válság miatti elégedetlenség és a frusztráció, amit a politikusok oroszellenes retorikával próbáltak meg kezelni. Ez elsősorban a radikális nacionalistáknak és a radikális iszlámistáknak kedvezett és nem Dudajevnek. [18] Ennek a táptalaja azok az iszlám vallású csecsenek voltak, akik a lakosság zömét, kb. 600 ezer főt teszik ki.[19] Rajtuk kívül 300 ezer orosz élt itt, akikért Moszkva a csecsen oroszbarát ellenzéket pénzügyileg is támogatta, hogy bebizonyítsák az Oroszországi Föderációhoz tartozva jobb élni, mint Dudajev államában. Ezt erősítette, hogy 1993. decembert követően módosult az oroszok politikai álláspontja a csecsenekkel kapcsolatban. Ennek a lényege, hogy a háttérből kellett támogatni a csecsen kormányzat ellenzékét, vagy akár katonai beavatkozás árán is meg kell dönteni a csecsen hatalmat. Az előbbi törekvés megbukott. Az ellenzéknek nem sikerült felülkerekedni a Dudajev mellett kiálló erőkön, ami cáfolni látszott a Dudajev-rezsim gyengeségét. Ennek eredménye, hogy Moszkvában döntés született az első csecsen háború megindításáról. [20]

A háború

Az orosz erők - a Védelmi Minisztérium, a Belügyminisztérium, a határőrség, a vasúti fegyveres erők és az FSZB erőiből összeállított egyesített harccsoport - kb. 24 ezer katonával, 80 harckocsival, 208 szárazföldi harcjárművel, 90 helikopterrel kezdte meg a cselekményeket. Velük szemben a Dudajev-vezetésnek meglehetősen korlátozottak voltak a lehetőségei, képességei. A csecsen erők három fajta nagyobb formációból álltak: a reguláris hadseregből, a különböző különleges egységekből, illetve gárdákból (kb. 12-15 ezer fő), valamint a katonai és háborús tapasztalatokkal nem rendelkező önkéntes és önvédelmi egységekből (kb. 30-40 ezer fő). A reguláris hadsereg 40 harckocsival, 50 szárazföldi harcjárművel, 100 löveggel és aknavetővel, 600 különböző páncéltörő eszközzel rendelkezett.[21]

Az első szakaszban (1994. december 11. – 1995. január 31.) az orosz előrenyomulás lassú volt, mert hátráltató tényezőként hatott az oroszok számára, hogy a haderejük nem volt felkészülve és felkészítve lázadásellenes, városi harc jellegű hadműveletekre. A küzdelmek centruma a csecsen főváros, Groznij volt, ahol a városi gerillaharc sajátos módszereit eszközeit alkalmazták a csecsenek. Az orosz erők csak jelentős veszteségek után tudták elfoglalni Groznijt, mert nem törődtek a hátukban visszamaradt gerillacsoportokkal, minden erővel a város központjának és az elnöki palotának elfoglalására törekedtek. Ezalatt a csecsenek támadták a vezetési pontokat, tartalékokat és az utánpótlást szállító gépjárműoszlopokat. [22]

A második szakaszban (1995. február 1. – 1995. június 14.) az oroszok katonai célja a teljes csecsenföldi uralom megszerzése lett volna, de ez csak részben sikerült áprilisra megszerezni. A déli területek települései bombázásával próbálkoztak, de Hamzat Gelajev – a csecsenek parancsnoka – az orosz hadifoglyok kivégzésével kikényszerítette ennek leállítását. Ez sikertelen volt a csecsen részről, amely még erőszakosabb válaszokat fogalmazott meg a katonai vezetőkben. Így a harmadik szakaszban (1995. június 14. – december 14.)

18 Kecskés (2012) 24-27.
19 Kőszegvári (2009) 67.
20 Kecskés (2012) 27-30.
21 Kecskés (2012) 32-33.
22 Kőszegvári (2009) 67.; Kecskés (2012) 34.

1995. június 14-én Samil Baszajev parancsnok a százfős csecsen fegyveres élén elfoglalta a Csecsenföld határaitól 150 kilométerre, bugyonnovszki[23] kórházat. 1200 embert, köztük kórházi dolgozókat és betegeket ejtett túszul. Politikai célja ezzel a csecsenföldi harcok leállítása, a szövetségi csapatok kivonása és közvetlen, elnöki vagy miniszterelnöki szintű orosz-csecsen tárgyalások követelése. Az orosz központi hatalom tehetetlennek bizonyult. A terrorelhárító egység kiszabadítási kísérletei véres kudarcba fulladtak, amellyel több mint száz túsz megölése következett be. A csecsenek ígéretet kaptak követeléseik teljesítésére, miután június 18-án az oroszok felfüggesztették a harcot, 19-én megkezdődtek a tárgyalások. Baszavej június 20-án elengedte a megmaradt túszait.[24]

A negyedik szakaszban (1995. december 14. – 1996. április 22.) választások megtartására 1995. december 14-17. között tettek kísérletet, amelynek az lett a vége, hogy az ellenzék 95%-kal nyert. Ezt törvénysértőnek és meghamisítottnak minősítették Dudajevék, de még az orosz emberi jogi biztos is. A választások időszakát a csecsen katonai vezetés saját pozícióinak kiszélesítésére használta fel. 1996. január 9-én Salman Radujev csecsen harcos vezetésével a bugyonnovszkihoz hasonló akciót kíséreltek meg végrehajtani a dagesztáni Kizljárban. 250 fegyveresével elfoglalta a helyi kórházat 3 ezer embert túszul ejtve. Követelései között az orosz fegyveres erőknek a dél-kaukázusi térségből való kivonása, a decemberi választások eredményeinek megsemmisítése, Dudejevvel való közvetlen tárgyalások megkezdése és csapata szabad elvonulásának biztosítása szerepelt. Annak ellenére, hogy Radujev végül megelégedett a szabad elvonulás biztosításával az akció január 17-én tragédiával végződött. 160 tússzal megkezdett visszavonulását Pervomajszkoje településnél az orosz fegyveres erők támadása szakította meg, melynek eredményeként 128 civil túsz, valamint 78 katona és rendőr halt meg. Borisz Nyikolajevics Jelcin – az akkori orosz elnök – március végén már a harcok befejezését tervezte a közvélemény és a közelgő választás miatt, de Dudajev 1996. április 22-én rakétatámadásban meghalt. [25]

Az ötödik szakaszban (1996. április 24. – augusztus 31.) az oroszok reménykedtek, hogy az első csecsen elnök halála komoly politikai destabilizációt okoz a szeparatista mozgalmon belül. Viszont fennállt a veszély, hogy a háború lezárásánál a helyi parancsnokokkal, hadurakkal egyenként kell megegyezni. Július és augusztus folyamán Aszlan Maszhadov[26] és Baszajev felújította a harcokat, így augusztus 31-én a háború befejezéséről szóló haszavjurti egyezményt Maszhadov írta alá. Az Oroszországi Föderáció és Csecsen Köztársaság közötti viszonyt a nemzetközi normáknak megfelelően kell rendezni 2001. december 31-ig. A csecsen vezetés ezt úgy értelmezte, hogy Moszkva elismerte Csecsenföld állami szuverenitását. [27]

A konfliktus elemzése

Az Oroszországi Föderáció jogi státusza megkérdőjelezhetetlen szemben Csecsenföldével.[28] Csecsenföld új államiságát a nemzetközi közösség egyik tagja sem ismerte el, főleg nem az oroszok, akik az 1993-as orosz alkotmány alapján a csecsen függetlenedést Oroszország területi egységét sértő tevékenységként aposztrofáltak. Azonban az orosz és a nemzetközi média nagy része, illetve legtöbb elemző megkérdőjelezték a hadsereg bevetésének jogszerűségét.[29]

Az orosz és a csecsen erőviszonyokat összehasonlítva, az orosz katonák szervezett alakulatokból, egységekből származtak, amíg az új állam erői nagy részét szakmai tapasztalatok nélküli, nem professzionális, hanem

23 Sztavropoli határterületen belül található.
24 Kecskés (2012) 34-35.
25 Kecskés (2012) 35.
26 Az első háború után ő lett Csecsenföld elnőke
27 Kecskés (2012) 36-37.
28 Chechnya: Russia's Experience of Asymmetrical Warfare.http://www.southasiaanalysis.org/paper619
29 Kecskés (2012) 31.

önkéntes kombattánsok alkották. Ezutóbbiak között voltak azok a mélyen vallásos és fanatikus fiatalokból álló öngyilkos egységeknek, akik képesek voltak az ellenséggel való halálig tartó küzdelmet választani a háborúk során.[30] Előnyükre válhatott, hogy a lakosság jelentős része rendelkezett otthon fegyverekkel, mert ezt a csecsen férfiak a jólét szimbólumának tekintették. Így elmondható, hogy a csecsenek sokkal jobban voltak motiváltak a harcokban és a területet is sokkal jobban ismerték, ezáltal a helyi lakosság segítségére tudtak támaszkodni, ami a szállás és az ellátásban is megnyilvánult. A helyiek nem feltétlenül támogatták a lázadókat. A helyi lakosság azért volt hajlandó segíteni a lázadóknak, mert féltek tőlük és nem azért, mert barátságosabbak voltak velük szemben. [31]

Az oroszok magas veszteségét[32] és a háború elhúzódását egyértelműen a föderációs erők felkészületlenségével magyarázzák az elemzők. Az orosz katonák képzetlenek voltak, sokan közülük nem is tudták szakszerűen használni fegyvereiket és eszközeiket, amelyek nem voltak korszerűek. A helyzetét rosszul mérte fel a katonai vezetés: túlságosan optimistán és elbizakodottan ítélte meg. Probléma, hogy a kontingens olyan egységekből állt, amelyek korábban nem gyakorolták az együttműködést. Lebecsülte a csecsen harcosokat, akik a helyismerettel, de a szakmai tudás hiánya miatt a gerilla- és városi harcra tudtak hagyatkozni. Ezért a terepviszonyokat is jobban ki tudták kihasználni. Arról nem is beszélve, hogy ekkor a gazdasági válság miatt a hadsereg finanszírozása zuhant, a korrupció pedig belülről emésztette a katonaság morálját. A rossz körülmények ellenére az orosz hadsereg továbbra is jó volt a hagyományos katonai tényezők – a nehéz fegyverzet és a hadsereg – szempontjából, azonban ez ebben a konfliktusban nem játszott döntő szerepet, mert a hagyományostól eltérő aszimmetrikus hadviselésre jellemző harcokra kellett volna berendezkedniük.[33]

A szemben álló felek közötti aszimmetriáról az eszközök is árulkodnak, hiszen a csecsenek légierővel egyáltalán nem rendelkeztek és a nehéz fegyverzetük száma is kevesebb volt az oroszokénál. A legierő fölényt az oroszok nem tudták meghatározó előnnyé kovácsolni. Ennek az oka, hogy a csecsen erők kis csapatokban nagy térben szétszóródva helyezkedtek el, főleg városi terepen. Ez nagy kockázatot hozott létre arra, hogy nagyszámú polgári veszteséggel járjanak a bombázások. Hatékonynak bizonyult viszont az ellenséges erődítmények és a hegyvidéki táborok elpusztítása szempontjából.[34]

A terrorakciókat tekintve mindkettő Csecsenföldön kívül történt, ami arra enged következtetést, hogy a határokat az oroszok egyáltalán nem ellenőrizték jól, a csecsen erőket az oroszok nem tartották bekerítve. A terrorakciókat rendszerint kicsi, 10 főnél kevesebb csoport szokta elvégezni, itt viszont a csecsen parancsnokok sokkal több, kb. egy századnyi erővel tették meg ezeket a cselekményeket.[35]A bugyonnovszki és a kizljari események nemcsak ráébresztették az orosz társadalmat, hogy a csecsenföldi konfliktus az ország más területeire

is átterjedhet, de komoly belpolitikai válságot is eredményeztek az elnökválasztásra készülő Oroszországban. A csecsenek a bugyinnovszki akcióval sikeresen rá tudták erőltetni a másik félre az akaratukat, hiszen Viktor Csernomirgyin orosz miniszterelnök megalázó tárgyalásokra kényszerült Baszajevvel. [36] Viszont a megkötött tűzszünetet mindkét oldalról megszegték ezután, tehát a háborúnak nem lett vége. A későbbi, kizljári akció

30 Kecskés (2012) 33.
31 Chechnya: Russia's Experience of Asymmetrical Warfare.http://www.southasiaanalysis.org/paper619
32 Pontos, egységesen elfogadott adat nem áll rendelkezésre. Az számok irodalmanként változnak, azonban a magas veszteségeket senki nem kérdőjelezte meg. (Chechnya: Russia's Experience of Asymmetrical Warfare. http://www.southasiaanalysis.org/paper619; Kecskés (2012) 37.)
33 Chechnya: Russia's Experience of Asymmetrical Warfare. http://www.southasiaanalysis.org/paper619; Kecskés (2012) 37-38.
34 Chechnya: Russia's Experience of Asymmetrical Warfare. http://www.southasiaanalysis.org/paper619
35 Gazdag-Remek 2018. 174. táblázat
36 Rácz (2011) 23-24.

már nem ért el ekkora sikert. Mindkettőről megállapítható, hogy az oroszok hibája elsősorban az, hogy a biztonsági szervek egyáltalán nem értettek a terrorakciókkal egybekötött túszejtés kezelésére.[37]Ezért rengeteg ártatlan civil esett áldozatul. A csecsenföldi civil halottak számára is különböző adatokat találunk. Anatolij Kulikov belügyminiszter 20 ezerre, Lebegy tábornok 80-100 ezerre becsülte a halottakat és 250 ezerre a sebesülteket Az orosz történészek szerint 30-35 ezren haltak csak meg és közel 400 ezer embernek kellett elhagynia lakhelyét. [38].

A második háború 1999-2000

Az Etno-szeparatizmus iszlám radikalizálódása

A haszavjurti egyezmény nem hozott javulást Csecsenföld területén.[39] A megállapodás értelmében a köztársaságból kivonultak a szövetségi erők, így az lényegében kikerült Moszkva irányítása alól. A sokak által remélt békés felvirágzás helyett azonban a szervezett bűnözés és anarchia korszaka következett Csecsenföldön.[40] A mérsékelt politikusoknak nem sikerült stabilizálni a köztársaságot, igaz valójában Moszkva sem segítette ezt. Az 1997-es választásokon az oroszok által támogatott Aszlan Maszhadovot választották meg elnöknek. Ő a riválisBaszajevet, a helyi parancsnokokat is bevonta a kormányzásba, abban bízva, hogy a hatalom megosztásával sikerül mérsékelnie a csecsen hadurak és klánok radikalizmusát. Ugyanis a munkanélküli, sokszor egész családjukat elvesztett csecsen fiatalok körében rohamosan terjedt az iszlám szélsőséges, vahhabita irányzata. Áramlottak az országba különféle szélsőséges nézeteket hirdető fegyveresek, elsősorban Szaúd-Arábiából, és tálibok Afganisztánból. A szélsőséges iszlám térnyerését aktívan támogatta Maszhadov két legnagyobb politikai riválisa. Az első háborúban még etno-szepatratista, radikális nacionalista, nemzeti felszabadítási mozgalomként lehetett őket számontartani, amelyek kezdetben nem voltak kapcsolatban a vallási szélsőségességgel, de a második háború előtt iszlamizálódtak. [41] 1997 tavaszától rendszeressé és tömegessé váltak a váltságdíjért végrehajtott emberrablások, amelyeknek orosz politikai és belügyi vezetők és külföldiek is áldozatul estek. Maszhadov 1999 januárjában Csecsenföldön kénytelen volt engedélyezni az iszlám törvénykezés bevezetését és bejelentette, hogy a köztársaságot iszlám állammá alakítják át. [42]

A háború

A háború első fele 1999. augusztus 4. Dagesztánban kezdődött, ahol Baszajev és Ibn-al-Hatták[43] parancsnoksága alatt az Iszlám Nemzetközi Brigád milícia bevonult Dagesztánba, hogy támogassa az iszlamista dagesztáni szeparatista mozgalmat. A bevonulás után Hattab és Baszajev 1999. augusztus 10-én ki is kiáltották

a Dagesztáni Iszlám Államot. Az orosz fegyveres erők már műveleteknek ebben a szakaszában is bombáztak csecsenföldi célpontokat, szisztematikusan készülve a katonai akciókra. A híres lakóházrobbantások is részben ehhez az összecsapáshoz kapcsolódnak. Az első támadás ugyanis éppen Dagesztánban történt: Bujnakszkban robbantottak fel szeptember 5-én egy katonacsaládok által lakott panelházat. Ezt követték aztán a nemzetközileg is hírhedtté vált moszkvai és volgodonszki akciók, amelyek összesen több mint háromszáz ember halálát okozták. Egyértelmű bizonyíték máig nincs arra, hogy kik tették ezeket a robbantásokat. Vlagyimir Putyin miniszterelnök viszont a Dagesztán elleni csecsen támadásra és a házrobbantásokra hivatkozva megindította

37 Kecskés (2012) 36.
38 Hodgson (2003) 67.
39 Северный Кавказ: Сложности интеграции (I), этничность и конфликт Доклад International Crisis Group №220 (Европа), 19 октября 2012 года. https://www.kavkaz-uzel.eu/articles/215385/ (Letöltve: 2020.05.31.)
40 Rácz (2011) 24.
41 Stepanova (2008) 118-119.
42 Kecskés (2012) 41.
43 Harmadik „mudzsahedin emír", a harcok iszlamista ágának egyik legjelentősebb vezetője.

a második csecsen háborút azzal a céllal, hogy Csecsenföldet integrálják az Oroszországi Föderációba. 1999. szeptember 30-án az orosz csapatok beléptek Csecsenföldre az úgynevezett „terrorizmusellenes művelet" végrehajtására. A védelmi minisztérium több mint 60 ezer, a belügyi tárca pedig mintegy 30 ezer katonát vezényelt a térségbe. Velük szemben a csecsenek maximum 50 ezer harcossal szálltak szembe az oroszokkal. 1999 decembertől a műveletek Groznij ostromáról és elfoglalásáról szóltak, amelyek közel másfél hónapon keresztül zajlottak és 2000. február 6-án jelentették be a város teljes felszabadítását. A második csecsen háború katonai szakasza 2000 tavaszán, Groznij elfoglalásával lényegében véget ért. Eredményeként 2000. június 8-án Putyin elnök bejelentette, hogy személyes irányítása alá veszi a köztársaságot és Ahmed Kadirovot nevezte ki csecsen adminisztráció vezetőjének, aki így a Csecsen Köztársaság első elnöke lett. Ez után az „antiterrorista műveletek" azonban hivatalosan még 2009-ig folytatódtak, amelyre a tanulmányom keretei nem terjednek ki, ezekre a műveletekre számos más irodalomból olvashatunk.[44]

A konfliktus elemzése

A városi gerillaharcban kiderült, hogy az oroszok még mindig nem készültek fel a felkelők ezen harcmodorának kezelésére. Ugyanis az orosz reguláris erők harctéri fölényét a csecsenek az első háborúhoz hasonlóan gerilla-hadviseléssel próbálták ellensúlyozni. A gerillacsoportok csak lényegtelen veszteségeket szenvedtek el. A nagyrészben helyi lakósokból alakult gerillaerők jól ismerték a város szerkezetét és megfelelő menekülési útvonalakat használtak az orosz csapások elkerüléséhez. Az első háborúhoz képest az a különbség, hogy a Csecsenföld és Dagesztán területén végrehajtott kisebb-nagyobb rajtaütések, robbantásos merényletek mellett immár az Észak-Kaukázuson túli területek polgári lakossága is a csecsen radikálisok célpontjává vált. Ez olyan szempontból fontos különbség, hogy a gerilla-hadviselés, vagy gerilla-hadikultúra a polgári lakosság elleni erőszakot általában elveti. [45]

A második háború sokkal brutálisabbnak bizonyult, mint az első, a harcosok gyakran terrorista módszereket alkalmaztak, és az oroszok erre válogatás nélküli erőszakkal válaszoltak. A hadsereg, bár jobban felkészült, mint az első háborúban, de technikailag és módszertani szempontból még mindig meg nem reformált és a régi taktikákat alkalmazva, nagyszabású konfliktusra tervezett fegyverekkel harcolt. Különbség még az elsőhöz képest, hogy az orosz légierőnek jóval nagyobb és meghatározóbb szerepe lett a második konfliktusban. Mintegy 1300 bevetést hajtottak végre tüzérséggel kiegészítve a harcosok kis csoportjainak felszámolására, ami időnként egész környékek és települések megsemmisítéséhez vezetett sok civil áldozatot követelve.[46]

A gerilla és a felkelés elleni harcokon kívül azonban tény, hogy az oroszok sok hibából levonták a következtetést. Az akció előkészítése, a műveletek irányítása és a harci taktika egyes elemei (speciális erők és mesterlövészek jobb kihasználása) vonatkozóan az erők vezetése megtanulta az első háború kudarcának leckéit, ezért ezek a másodikban már sokkal jobban mentek, ami hozzájárult is az orosz győzelemhez. [47]

A háborúban az elsőhöz képest nagyobb csoportos terrorakció, túszejtés és túszok megölése, nem történt, azonban fontos tudni, hogy a kétes szeptember elejei lakóházrobbantásokért a Kreml és az orosz sajtó túlnyomó többsége a csecseneket tette felelőssé. Ennek az lett az eredménye, hogy az orosz lakosság körében nőtt a csecsenekkel való háború elfogadása. 1995 októberében a megkérdezetteknek mind össze 20%-a támogatta

44 Kecskés (2012) 42-45.; Северный Кавказ: Сложности интеграции (I), этничность и конфликт Доклад International Crisis Group №220 (Европа), 19 октября 2012 года. https://www.kavkaz-uzel.eu/articles/215385/ (Letöltve: 2020.05.31.)
45 Kecskés (2012) 44-45.; Kőszegvári (2009) 67-68.
46 Rácz (2011) 24-25.; Северный Кавказ: Сложности интеграции (I), этничность и конфликт Доклад International Crisis Group №220 (Европа), 19 октября 2012 года. https://www.kavkaz-uzel.eu/articles/215385/ (Letöltve: 2020.05.31.)
47 Kecskés (2012) 51.

a csecsen kérdés háború útján történő megoldását és 65% ellenezte, addig 1999 októberében a támogatók aránya 53%, az ellenzőké 21% lett. Azok aránya, akik a csecsen fegyveresek végleges megtöréséig vezetett háborút tartották a legjobb megoldásnak, 1995 októberében csupán 3%-ot tett ki, 1999 októberében viszont 63%-ot.[48]

A fentebb említett sorozatos emberi jogsértések miatt a második csecsen háborút folyamatosan figyelemmel kísérte a nemzetközi média és különféle jogvédő csoportok, bár tevékenységük csekély gyakorlati hatással volt az orosz műveletekre. A Csecsenföldön történtekre irányuló erős nemzetközi figyelem nyilvánvalóan kellemetlen volt az orosz kormánynak. [49]

3. Összegzés

A csecsen nép függetlenedési kísérlete az Oroszországi Föderációtól tipikus példája az aszimmetrikus konfliktusoknak. A háború eseményeit tanulmányozva láthatjuk, hogy egy aszimmetrikus háborúnak a hadviselő felek taktikái stratégiái igencsak eltérhetnek egymástól. Az oroszok ekkor még a hagyományos nagy háborúk megvívására voltak berendezkedve, nem vették észre, hogy más módszereket kíván az aszimmetrikus háború megvívása. Az, hogy a felek közül ki kerül ki győztesen, már nem annak a függvénye, hogy ki rendelkezik az erőfölénnyel, hanem hogy ki tud tovább talpon maradni. A gyengébb fél sikerét jelentheti, ha kompenzálja a gyengeségeit, fenntartja a háborút és különböző erőszakos taktikákkal megpróbál felülkerekedni az erősebb féllel szemben. A terrorista taktikák közül láthattunk olyat is a csecsen háborúknál, amelyikkel a lélektani hatásokkal együtt el tudták érni a politikai célját az erősebb féllel szemben, azonban ezek a taktikák a társadalom körében igen negatívan hatnak a harcosok megítélését illetően. A harcosok rengeteg ártatlan civilt öltek meg, amelynek semmilyen ideológia vagy vallási legitimációját nem lehet elfogadni. Az orosz-csecsen konfliktusok vizsgálata rávilágít, hogy a felkelők és a terroristák elleni harcnak egyedi a kezelése. Oroszországról a tanulmányban vizsgált alkalmak mindegyikénél elmondható, hogy egyáltalán nem kezelte a helyén ezeket az akciókat. A térség erőteljes iszlamizációja stratégai probléma, amely az oroszoknak a mai napig fejtörést okozhat.

Felhasznált irodalom

Bakos Csaba Attila (2015): Clausewitz „újratöltve”. *Hadtudomány*, 2015/1-2. 99-104.

Berglund, Christofer – Souleimanov, Emil Aslan (2020): What is (not) asymmetric conflict? From conceptual stretching to conceptual structuring. *Dynamics of Asymmetric Conflict*, 2020/1. 87-98.

Éberhardt Gábor (2019): Migráció és terrorizmus. *Hadtudományi Szemle* 2019/3. 37-59.

Gazdag Ferenc – Remek Éva (2018): *A biztonsági tanulmányok alapjai.* Budapest, Dialóg Campus Kiadó.

Gerencsér Árpád (2016): *A Kaukázus térség biztonságföldrajzi értékelése.* Doktori értekezés, Budapest, Nemzeti Közszolgálati Egyetem

Hodgson, Quentin (2003): Is the Russian bear learning? an operational and tactical analysis of the second Chechen war, 1999–2002. *Journal of Strategic Studies*, 2003/2. 64–90.

Porkoláb Imre (2016): A különleges műveleti erők szerepe az aszimmetrikus kihívásokból adódó katonai feladatok tükrében, különös tekintettel a nemzetközi terrorizmus elleni küzdelemre. – 2008. *Nemzetbiztonsági Szemle*, 2016/2. 16-19.

48 Kecskés (2012) 46-47.

49 Rácz (2011) 28.

Kecskés Tímea (2012): *Az orosz-csecsen szembenállás története. A terrorista módszerek és eszközök szerepe az orosz-csecsen konfliktusban.* Doktori értekezés, Nemzeti Közszolgálati Egyetem

Kőszegvári Tibor (2009): Gerilla-hadviselés a városokban. *Hadtudomány*, 2009/1-2. 63-71.

Rácz András (2011): Háború két és fél fronton: Oroszország a terrorizmus elleni küzdelemben. *Nemzet és Biztonság,* 2011/szeptember. 22-31.

Resperger István (2018): II. A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések In: Resperger István (2018): *Nemzetbiztonsági tanulmányok.* Budapest, Dialóg Campus Kiadó, 29-84.

Resperger István (2017): Az aszimmetrikus hadviselésre adható válaszok. *Honvédségi Szemle*,2017/1. 24-43.

Resperger István – Kis Álmos Péter – Somkúti Bálint (2013): *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest, Zrínyi Kiadó.

Répási Krisztián (2011): A gerillaharc és a terrorizmus szerepe a felkelésekben. *Nemzet és Biztonság* 2011/ május 34-41.

Stepanova, Ekaterina (2008): *Terrorism in asymmetrical conflict. Ideological and Structural Aspects.* Oxford, Oxford University Press

Global Terrorism Index 2019. http://visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf (Letöltve: 2020.05.30.)

Codebook: Inclusion Criteria and Variables. https://www.start.umd.edu/gtd/downloads/Codebook.pdf (Letöltve: 2020.05.30.)

Chechnya: Russia's Experience of Asymmetrical Warfare. http://www.southasiaanalysis.org/paper619 (Letöltve: 2020.06.04.)

Источник информации. https://histrf.ru/biblioteka/b/vtoraia-chiechienskaia-voina (Letöltve: 2020.06.03.)

Северный Кавказ: Сложности интеграции (I), этничность и конфликт Доклад International Crisis Group №220 (Европа), 19 октября 2012 года. https://www.kavkaz-uzel.eu/articles/215385/ (Letöltve: 2020.05.31.)

Krausz József

Biztonságos jelszókezelés és jelszóválasztás

1. Bevezetés

Valószínűleg a mai modern információs társadalomban már mindannyian fent vagyunk valamilyen internetes platformon, ahol különböző személyes adatainkat tároljuk és amiket jelszóval védünk. Kezdve itt a közösségi média oldalaktól – Facebook, Instagram, Twitter – egészen a netbank oldalakig. Kijelenthető, hogy a társadalmunk minden korosztálya már rutinosan használja az internetes felületeket, tehát a kibertér életünk szerves részévé vállt.

2. A jelszóhasználat a mindennapokban

A következő kérdések már talán meg sem fogalmazódnak a felhasználókban:

Megfelelő jelszót választottam magamnak?
Megfelelően védi a választott jelszó az adataimat?
Mennyi ideig tartana feltörni a jelszavamat?
Mit kellene tennem annak érdekében, hogy ezeket megakadályozhassam?

Az elkövetkező tanulmányban a következő kérdésekre keressük a válaszokat. A cél az, hogy a tanulmány végére mindenki egy átfogóbb képet kapjon az adatainak védelméről és ezek után jobban figyelhessen a jelszavai megválasztására.

2.1. Az általánosan elkövetett hibák

Tartja a mondás: az okos ember saját hibáiból tanul a bölcs ember máséból. Ezért legyünk bölcs emberek és vizsgáljuk meg mások hibáit, azáltal, hogy végig vesszük az általánosan előforduló hibákat a jelszóválasztásnál:

1. Fizikailag könnyű hozzáférni
2. Túl gyakori
3. Könnyű kitalálni
4. Személyes név vagy adat
5. Csak betűk
6. Túl rövid
7. Túl régi
8. Mindig ugyanaz
9. Mindenkinek elmondjuk

Fizikailag könnyű hozzáféri: ezen azt kell érteni, hogy az adott személy nem tudja megjegyezni a jelszavát (ami természetes emberi tulajdonság), azonban nem egy biztonságos helyre írja föl, hanem egy papírcetlire, amit esetleg a billentyűzet alá rejt csak el, tehát könnyen megtudják mások szerezni.

Túl gyakori: túl gyakoriknak mondhatók azok a jelszavak, amelyek tipikus szóösszetételekből állnak és akár egy szótárt felütve is ki lehet találni

Könnyű kitalálni: ide tartoznak az egyszerű jelszavak, mint például az 1234, jelszó stb.

Személyes név vagy adat: gyakran előfordul hiba, hogy saját nevüket, szerelmük nevét, évfordulót, születésnapot adnak meg a felhasználók jelszónak.

Csak betűk: az, amikor a jelszóban csak betűk vannak, holott a szakemberek kérik, hogy a billentyűzet minden karakterét, használjuk fel (Sándor, 2011.), mert ezáltal nehezebb a feltörés. Használjunk számokat, kis és nagybetűt stb.

Túl rövid: minél rövidebb egy jelszó annál hamarabb fellehet törni, minél hosszabb annál tovább tart a feltörése nem véletlen mondják, hogy minimum 12 karaktert adjunk meg és ezért van, hogy az oldalak már kényszerítik a felhasználót egy minimum karakterszámra.

Túl régi: ez alatt azt kell érteni, hogy nem változtatjuk meg a jelszavainkat. Azonban érdemes lenne minimum 90 naponként megváltoztatni jelszavunkat.

Mindig ugyanaz: minden felületre ugyanazt a jelszót adjuk meg, így növelve a feltörés esélyeit, mert ha egy helyen kitalálták a jelszavunkat így a többi hely sem marad már védett.

Mindenkinek elmondjuk: egyszerűen azt jelenti, hogy elmondjuk minden ismerősünknek jelszavunkat, mert jóhiszeműek vagyunk és azt hisszük ő nem árthat nekünk.[12]

1. ábra Forrás: https://www.gravoc.com/wp-content/uploads/2017/04/Password-hacker-methods-Password-Cracking-Tools.png

2.2 A ránk leselkedő veszélyek

Most, hogy megtudtuk milyen hibákat védhetünk tudjuk meg milyen veszélyeket rejthet magában az, ha feltörik a jelszavainkat. Önmagában nem ijesztő az, ha elolvassuk az általános hibákat és közben magunkra ismerünk, mert csak legyintünk velünk úgysem történhet meg, hogy feltörik profilunkat. Azonban, ha megismerjük a veszélyeket ez adhat olyan motiváló erőt, hogy az emberek odafigyeljenek mégis a jelszavaikra.

A mai világban a legkülönbözőbb féle oldalakon vagyunk fönt a közösségi oldalaktól kezdve egészen a webáruház oldalakig. Ezeken a felületeken egészen a saját nevünkben küldözgetett álüzenetektől kezdve bankkártyánk lenullázásáig terjedhet a minket érintő veszélyek tárháza.

Nézzük meg, ha egy facebook profilt törnek fel mik történhetnek. Itt megtehetik azt a tettesek, hogy nevünkben elkezdenek ismerőseinknek írogatni kellemetlen helyzetbe hozni minket vagy olyan tartalmakat osztani meg, ami szintén nekünk okozhat kellemetlenséget. Így aztán barátainkat is ellenünk fordíthatják vagy akár

1 (Bjork, 2019.)
2 (Abagnale, 2019.)

egyetemünkön munkahelyünkön is kellemetlen helyzetbe hozhatnak minket, amíg el nem magyarázzuk, hogy feltörték a profilunkat. Persze megtehetjük azt, hogy töröljük magunkat vagy megváltoztatjuk a jelszavunkat, azonban, logikusan az első lépésük az lesz, hogy megváltoztatják jelszavunkat, hogy minket kizárjanak saját profilunkból és így akár még zsarolhassanak is minket. Ez igaz lehet bármelyik közösségi oldalunkra.

Következő körben, ami még igazán fontos az az interneten való vásárlás kérdése. Nagyon sokszor intézzük pénzügyi dolgainkat már a kibertérben és ezért fontos, hogy vigyázzunk, pénzünkre. Ebből következik, ha nem megfelelő jelszót választunk vagy nem biztonságos oldalakon megadjuk bankszámla adatainkat könnyen azt vehetjük észre, hogy pénzünket levonják kártyánkról. Persze ilyenkor az első lépés a kártyánk letiltása, azonban így is kellemetlenségbe fogunk keveredni és nem biztos, hogy minden pénzünket visszakapjuk.

Most, hogy végig vettük a lehetséges hibákat és lehetséges következményeket nézzük meg, hogyan védekezhetünk hatékonyan a rossz szándékú emberek ellen.

```python
import socket
import struct
import sys

HOST = '192.168.1.1'
PORT = 32764

def send_message(s, message, payload='') :
    header = struct.pack('<III', 0x53634D4D, message, len(payload))
    s.send(header+payload)
    sig, ret_val, ret_len = struct.unpack('<III', s.recv(0xC))
    assert(sig == 0x53634D4D)
    if ret_val != 0 :
        return ret_val, "ERROR"
    ret_str = ""
    while len(ret_str) < ret_len :
        ret_str += s.recv(ret_len-len(ret_str))
    return ret_val, ret_str

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
s.connect((HOST, PORT))
send_message(s, 3, "wlan_mgr_enable=1")
print send_message(s, 2, "http_password")[1]
```

2. ábra Forrás: https://1.bp.blogspot.com/-neKKGAGU3EU/UsedXhUjT7I/AAAAAAAAZaw/BXSKG_0QX9s/s728/Hacking+Wireless+DSL+routers+via+Admin+Panel+Password+Reset+vulnerability.jpg

2.3 Megoldás a problémára

Ahogy említettem vegyük akkor sorra miket is kell csinálnunk ahhoz, hogy fiókjaink védettebbek legyenek. Természetesen fontos kiemelni, hogy tökéletes védelem nincs azonban a feltörés esélyét lehet csökkenteni.

Ahogy az előzőkben megbeszéltük a jelszavunk ne legyen rövid, mivel minél hosszabb annál nehezebb feltörni. A Nemzeti Média és Hírközlési Hatóság 2017-es adatai szerint ezért jelszavunk hosszát minimum 12 karakterben válasszuk meg (természetesen, ha hosszabbat írunk az nem baj) és minden elemét használjuk fel a billentyűzetnek. Tehát legyen benne kisbetű, nagybetű, szám és speciális karakter, ezáltal is csökkentve a feltörés esélyét.[3][4]

Szintén megemlítettem, hogy ne használjuk egy helyre ugyanazt a jelszót is mivel egyrészt egy gyengébben védett oldalról könnyen megszerezhetővé válik, másrészt hiába van egy erős jelszavunk, ha mindenhova

3 (Hatóság, 2017)
4 (Intézet, 2018)

ugyanazt adjuk meg feltörése sokkal könnyebbé válik, mivel elég csak egy oldalról megszerezni. Ezért mindig adjunk meg többféle jelszót, mivel ezzel is csökkentjük a feltörés esélyét.[5]

Továbbá ne elégedjünk meg azzal se, ha mindenhol más jelszavunk van és már 10 éve hozzá se nyúltunk, mivel így a feltörőknek 10 éve volt arra, hogy kitalálják jelszavainkat. Jelszavainkat periodikusan változtatnunk kell. A Microsoft javaslata szerint 30-90 naponta cseréljük jelszavunkat, így sokkal kevesebb esélyt adunk a hackereknek.[6]

Korábban említettem, hogy figyeljünk az oldalak biztonságára védettségére. Mindannyian ismerjük, hogy az oldalak címében benne van a http vagy https ez azt jelenti hypertext transfer protocol (hiperszöveg átirányítási protokoll). A kettő közötti különbség az, hogy a http nem a https viszont alkalmaz titkosítást az információk továbbításában, tehát védettebb, (az s egyébként a secure-t jelöli nevében). Fontos kiemelni ezt mivel egy http oldalon könnyebben megszerezhetik adatainkat, mint egy https-en ezért kifejezetten figyeljünk, hova milyen adatot adunk meg.[7]

Szintén javasolják a jelszavaknál, hogy alkalmazzunk kétlépcsős azonosítást. A kétlépcsős azonosítás alatt azt értjük, hogy amikor bejelentkezünk nemcsak a jelszavunkat kell megadnunk, hanem a telefonunkra küldött biztonsági kódot is. Ezáltal megnehezítve a hackerek feladatát, hogy még egy védelmi vonallal látjuk el fiókunkat. A Google oldalán több is megtalálható erről a módszerről.[8]

Néhány példát arra vonatkozóan milyen jelszavakat is alkalmazhatunk. A Szer3temAzAlmát! például egy jó megoldás, hiszen minden karakter megtalálható benne könnyen megjegyezhető, de mégsem egyértelmű, más platformra pedig módosíthatjuk Szer3temAGmailt!-re is.

Másik lehetőség például a mothertyukja vagy 5mother1Tyukja9. Szintén könnyen megjegyezhető és kevésbé kikövetkeztethető ráadásként egyszerre két nyelven van írva.

De itt van egy másik lehetőség is a JjbdUnnvuőŐÉú78/=/11. Ez már egy nehezen megjegyezhető jelszó, azonban nehezen megfejthető. Ezért is javasolják egyes helyeken a LastPass jelszómenedzser alkalmazását, hogy megtudjuk jegyezni jelszavainkat.[9] [10]

Azonban én nem gondolom, hogy jó ötlet egy programba összeírni jelszavainkat, mert azt is feltörhetik másrészt kitudja a cég kinek adja ki adatainkat titokban.

5 (Intézet, 2018)
6 (Webshark, 2018.)
7 (Vukadinovic, 2018.)
8 (Google, dátum nélk.)
9 (Hatóság, 2017)
10 (Pass, dátum nélk.)

3. ábra Forrás: https://www.moneycrashers.com/wp-content/uploads/2019/03/create-password-prevent-hacking-phishing-1068x713.jpg

2.4. A legfontosabb szabályok egyben

Végezetül röviden összefoglalva az előzőekben megállapított lényeges tételmondatok a következő:

- Hosszú jelszavakat adjunk meg
- A billentyűzet minden karakterét alkalmazzuk
- Ne adjuk meg ugyanazt a jelszót több helyre
- Cserélgessük bizonyos időközönként jelszavainkat.
- Ne adjuk meg másoknak a jelszavunkat
- Ne legyen könnyen kitalálható ránk jellemző jelszó
- Figyeljünk az oldalak védettségére
- Használjuk kettős azonosítást
- Ha muszáj használjunk jelszó menedzsert

3. Összegzés

Tehát megállapítható az, hogy ahhoz, hogy megfelelően működhessünk az online közegben szükségünk van arra, hogy ismerjük a törvényeit. Az interneten rengeteg elérhető forrás van arra vonatkozóan, hogy hogyan is kell egy fiókot biztonságosan felépíteni. Példaként elég már, ha csak a Google fiók ajánlásait is megnézzük. A biztonsági rendszerek egyre inkább finomodtak megnehezítve a hackerek dolgát, azonban sajnos kijelenthető, hogy sosem lesz 100%-ig védett profil. Végül az is megállapítható, hogy sajnálatos módon sok ember csak akkor figyel már oda a biztonságra, ha már a fiókjában megtörtént a baj. Ez általában annak a mentalitásnak köszönhető, hogy ez velem úgysem történhet meg és még ott van az emberi lustaság is. Végezetül kijelenthető, hogy ha azt akarjuk, hogy fiókjaink védettek legyenek, akkor nekünk kell cselekedni.

Felhasznált irodalom

Abagnale, F. (2019.. szeptember 24.). *CNBC: 'These 9 biggest password mistakes will get you in trouble,' warns fraud expert and ex-con artist*. Forrás: https://www.cnbc.com/2019/09/24/dont-make-these-9-biggest-password-mistakes-warns-fraud-expert-and-ex-con-artist.html

Attila, S. (2011.. június VI. Évfolyam 2. szám). *Hadmérnök: AZ Y GENERÁCIÓ ÉS AZ INFORMÁCIÓBIZTONSÁG*. Forrás: http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1376/2011_2_schuller.pdf?sequence=1&isAllowed=y

Bjork, D. (2019.. január 10.). *The Software Pro: Smart Security: Top 10 Password Mistakes*. Forrás: https://thesoftwarepro.com/password-mistakes/

Foltýn, T. (2019.. december 16.). *We live security: The worst passwords of 2019*. Forrás: https://www.welivesecurity.com/2019/12/16/worst-passwords-2019-did-yours-make-list/

Google. (dátum nélk.). *Google: Fokozott védelem Google Fiókja számára*. Forrás: https://www.google.com/landing/2step/?hl=hu#tab=how-it-works

Hatóság, N. M. (2017. november 15). *Milyen a biztonságos jelszó 2017-ben*. Forrás: http://nmhh.hu/cikk/191035/Milyen_a_biztonsagos_jelszo_2017ben

Intézet, N. K. (2018). *Jelszóhasználat*. Forrás: https://nki.gov.hu/it-biztonsag/tartalom/eszkoztar/jelszohasznalat/

Magyarország, G. D. (2017.. május 9.). *Ilyen a biztonságos jelszó*. Forrás: https://virusirto.hu/blogbejegyzesek/2017/05/09/ilyen-a-biztonsagos-jelszo/

Pass, L. (dátum nélk.). *Last Pass: Effortless security from anywhere*. Forrás: https://www.lastpass.com/

Sándor, F. R.-M. (2011.. szeptemner VI. Évfolyam 3. szám). *Hadmérnök: INFORMATIKAI BIZTONSÁGI ÚTMUTATÓK, KONTROLLOK*. Forrás: http://hadmernok.hu/2011_3_fleiner_munk.pdf

Vukadinovic, D. (2018.. május 22.). *Global Sign: What's the difference between HTTP and HTTPS?* Forrás: https://www.globalsign.com/en/blog/the-difference-between-http-and-https

Webshark. (2018.. október 18.). *Biztonság a neten: Jelszavak használata, hibák és tanácsok*. Forrás: https://webshark.hu/hirek/netes-biztonsag/

Lőrincz Virág

Az új típusú terrorizmus elleni küzdelem Izraelben[1]

1. Bevezetés

Az Izraeli Állam 1948. május 14-én kiáltotta ki függetlenségét az ENSZ Közgyűlés 181. [1947] számú határozata alapján. A határozat a Földközi-tenger és a Jordán folyó közötti Brit Mandátum területén egy zsidó (Izraeli Állam) és egy arab állam (Palesztin Állam) létrejöttéről rendelkezett, az ott élő palesztinok azonban elutasították a kétállami megoldást. A kibontakozó területi és etnikai konfliktusok eszközrendszerében megjelent a terrorizmus, amely változó intenzitással a mai napig meghatározó a térségben.

A hidegháború után béketárgyalások kezdődtek a térségben Izrael és az arab országok között, 1991-től tíz éven keresztül annak a látszatát keltve, hogy a területi vitákat Izrael és a palesztin oldalt hivatalosan képviselő Palesztin Felszabadítási Szervezet (PFSZ) rendezni tudja és sikerülhet átfogó békét kötni a környező arab államokkal is. A feszültségek 2000-ben ismét felszínre törtek, kirobbant a második intifáda (palesztin népfelkelés) és a palesztin-izraeli szembenállás nyíltan fellángolt. Az Egyesült Államokban 2001. szeptember 11-én bekövetkezett terrortámadás globális szinten is felhívta a figyelmet az új típusú terrorizmus megjelenésére, mely a 21. század egyik legnagyobb biztonsági kihívásává vált.

A téma aktualitását az adja, hogy a kétezres évek elején számos európai országot ért váratlanul és felkészületlenül sok áldozatot követő terrortámadás, és ez felhívta a figyelmet az új fenyegetés jelentőségére. A figyelem Izraelre irányult, amely a Közel-Kelet egyetlen demokráciájaként már létrejötte óta küzd a terroristákkal a határain belül, a határain, illetve a határain kívül is. Ebből következik, hogy a terrorizmus elleni küzdelem terén több évtizedes tapasztalattal rendelkező ország módszerei, eszközrendszere és stratégiája példaként szolgálhat más, hasonló kihívásokkal szembenéző – elsősorban demokratikus – államoknak is.

2. Országismertető

Izrael a 20. század közepén sajátos körülmények között jött létre. A század elejétől meghatározó a palesztin arabok és a zsidók közötti konfliktus, mely a Palesztina területéből kiváló zsidó állam megalakulásából eredeztethető. 1947-ben Nagy-Britannia, amely az első világháború utolsó éveitől a mandátumi területet felügyelte, döntött a területről való kivonulásáról. Ezt és a mandátumi terület felosztását az ENSZ Közgyűlés 181. (1947) számú határozata rögzítette, mely az egykori Palesztina területét három részre osztotta: Izraelre, Ciszjordániára és a Gázai-övezetre, melyek közül a két utóbbi terület alkotta volna a Palesztin Államot.[2]

A mai napig tartó konfliktus fő oka, hogy az Egyiptom, Jordánia, Szíria, Libanon és a Földközi-tenger által határolt területet mind a palesztinok, mind pedig az izraeliek őshazájuknak tekintik, erre hivatkozva ragaszkodnának saját nemzetállami elképzelésükhöz az említett területen. Az ENSZ határozat által javasolt kétállami megoldás arab (palesztin) részről elutasításra került és Izrael-ellenes retorikát eredményezett, mely gyakran arab támadásokban, terrorcselekményekben nyilvánult meg.

2.1. Vitatott státuszú területek

A térségben a 20. század eleje óta változó intenzitással zajló palesztin-izraeli konfliktus során a fő kiváltó ok területi vitákra vezethető vissza. A politikai, katonai és gazdasági síkon is megjelenő konfliktus mára globá-

1 Az Innovációs És Technológiai Minisztérium ÚNKP-20-1-I-NKE-151 kódszámú Új Nemzeti Kiválóság Programjának szakmai támogatásával készült.

2 Kis-Benedek József: *A palesztin-izraeli konfliktus*. Felderítő Szemle, I. évf. 2002/1., 61–85., 62.

lissá vált és a nemzetközi közösség tagjai közül is sokan közvetve vagy közvetlenül résztvevőivé váltak.[3] A területi viták kialakulásának oka abból eredeztethető, hogy Izrael létrejötte és a 20. században a szuverenitása megtartásáért vívott háborúk során több olyan területet is megszállt és a mai napig fennhatósága alatt tart, amelyet a nemzetközi közösség nem minden tagja ismer el az Izraeli Állam részeként.

Az izraeli megítélés és a nemzetközi közösség által elfogadott álláspont meg nem egyezésének eredményeként több vitatott státuszú stratégiai fontosságú és a terrorizmus helyszínéül szolgáló terület van a térségben, melyek a következők: Golán-fennsík, Gázai-övezet és Ciszjordánia.

A Golán-fennsík Izrael, Szíria és Libanon határán fekszik. Izrael 1967-ben foglalta el Szíriától, a jelenleg 1800 km^2-es területnek kétharmada áll izraeli megszállás alatt. Stratégiai szempontból kiemelt jelentőségű, mert a magaslatról könnyen belátható Libanon és Szíria is, a terepviszonyok pedig megnehezítik a Szíria felől érkező esetleges támadásokat.[4] Izrael 1981-ben egyoldalúan kiterjesztette a Golán-fennsíkra a törvénykezését is. A terület Izrael általi annektálását 2019 márciusában az Egyesült Államok elismerte, azonban ezt a döntést az ENSZ és az Európai Unió tagállamai is elutasították.[5]

A Gázai–övezet 360 km^2-es terület, délről Egyiptom, keletről a Földközi-tenger, többi oldaláról pedig Izrael határolja. A főleg palesztinok által lakott területet 1967-ben vonta saját fennhatósága alá Izrael. A független Palesztina létrehozását támogató szervezetek (például Hamász, Iszlám Dzsihád) és az izraeli megszálló erők között 1987 óta fegyveres konfliktusok zajlanak, az 1993-ban megkötött Oslói Megállapodás biztosította az autonóm palesztin kormányzást a terület fölött.[6] A Gázai-övezetet uraló radikális iszlamista Hamász és Izrael között 2019. novemberében lépett életbe a tűzszünet.[7]

Ciszjordánia 5650 km^2-en terül el a Jordán folyó nyugati oldalán. A Gázai-övezettel együtt az 1967-es hatnapos háborúban szállta meg Izrael. A palesztin nacionalista törekvések elnyomására a döntően palesztin lakosság kitelepítése és a zsidó telepesek betelepítése zajlik. Az Oslói Megállapodás a palesztin-zsidó békefolyamat részeként létrehozta a Palesztin Hatóságot (Palestinian Authority, PA), mely a mai napig Ciszjordánia döntő részének irányításáért felel. Az izraeli kormány telepespolitikája révén próbálja a területen a befolyását növelni, illetve a Jordán-völgy annektálását előkészíteni. Ezáltal a ciszjordániai területeken az izraeli kormány különböző kedvezményekben részesíti az odatelepülő zsidó lakosságot, mely így egyre nagyobb számban lesz jelen a térségben az ott élő palesztinok mellett.[8]

A fent ismertetett területeken kívül Izrael fővárosának egyértelmű meghatározása is akadályokba ütközik és Jeruzsálem vitatott jogi státuszának kérdését veti fel. Jeruzsálem városát az ENSZ 181. [1947] sz. határozata az ENSZ Gyámsági Tanács alá kívánta helyezni. Az 1948-49-es első arab-izraeli háború során azonban Izrael elfoglalta Jeruzsálem nyugati részét, míg a keleti része később Jordániához került.Az 1967-es hatnapos háború után Izrael elfoglalta Kelet-Jeruzsálemet és azóta Jeruzsálem de facto az izraeli kormány székhelye, azonban a nemzetközi közösség legtöbb tagja nem ismeri el Jeruzsálem fővárosi státuszát. Ezt jelzi, hogy a külföldi

3 Szabó Regina: *A palesztin – izraeli konfliktus története és a béke lehetősége a Szentföldön.* Nemzetbiztonsági Szemle, VII. évf. 2019/1., 66–84., 67.

4 Giora Eiland: *Defensible Borders on the Golan Heights*. 2009. http://www.jcpa.org/text/DefensibleBorders-GolanHeights.pdf (Letöltés időpontja: 2020. 05. 23.)

5 *Security Council Members Regret Decision by United States to Recognize Israel's Sovereignity over Occupied Syrian Golan*. 2019. https://www.un.org/press/en/2019/sc13753.doc.htm (Letöltés időpontja: 2020. 05. 23.).

6 *A Gázai övezet története*. 2012. https://web.archive.org/web/20121120052902/http://www.tortenelemklub.com/xxszazad/1990-utan/938-a-gazai-oevezet-toertenete (Letöltés időpontja: 2020. 05. 23.)

7 *Izrael-Gázai övezet: életbe lépett a tűzszünet*. 2019. https://hu.euronews.com/2019/11/14/izrael-gazai-ovezet-eletbe-lepett-a-tuzszunet (Letöltés időpontja: 2020. 05. 23.)

8 Szabó (2019) i.m. (3. lj.) 66–82.

diplomáciai képviseletek döntő többsége Tel-Avivban, az 1967 előtti, és a nemzetközi közösség döntő többsége által fővárosnak elismert városban található.[9] Vannak ez alól kivételek: a Trump-adminisztráció 2017-ben elsőként ismerte el Jeruzsálemet Izrael fővárosának és ennek jeleként az amerikai nagykövetséget Tel Avivból Jeruzsálembe költöztette.[10]

2.2. Geopolitikai és geostratégiai jellemzők

Az Izraeli Állam területe megközelítőleg 22 000 km^2, északon Libanon, északkeleten Szíria, keleten Jordánia, délnyugaton Egyiptom, nyugaton pedig a Földközi-tenger határolja. Népessége körülbelül 8,6 millió fő, etnikai megoszlását tekintve 74%-a zsidó, 21%-a arab és 5%-a egyéb etnikumhoz tartozó. Vallását tekintve hasonlók az arányok, 74% zsidó, 18% muszlim, ezen kívül számos keresztény, illetve drúz és egyéb vallás van jelen. Hivatalos nyelve a héber, továbbá különleges státuszt élvez az arab nyelv.[11]

Izrael nemzetközi környezetben betöltött szerepét alapvetően határozza meg geopolitikai helyzete, azaz földrajzi elhelyezkedése, természeti ásványkincsei, népessége és kulturális jellemzői. Kis ország révén nincsenek stratégiai mélységei, ezért kulcsfontosságú, hogy az előző alfejezetben ismertetett vitatott státuszú területeket ellenőrizni tudja, és ezáltal biztosítsa a határai védelmét.[12]

Zbigniew Brzezinski lengyel származású politológus *A nagy sakktábla* című művéből két fogalmat kell értelmezni Izrael esetében. Az első az aktív geostratégiai játékos, mely arra utal, hogy az adott állam „kellő erővel és nemzeti akarattal rendelkezik ahhoz, hogy hatalmát és befolyását határain túl felhasználja az éppen adott geopolitikai helyzet – Amerika érdekeit is befolyásoló mértékű – megváltoztatására. Az ilyen államnak megvan a képessége és/vagy hajlandósága a geopolitikai rugalmasságra.” [13] Izrael aktív geostratégiai játékos szerepe a terrorizmus elleni küzdelemben, a terroristák kiiktatásában és az ilyen irányú fellépések megalapozásául szolgáló hírszerző tevékenységben nyilvánul meg elsősorban. Továbbá egyre aktívabb diplomáciai tevékenysége eredményeként 2020 augusztusában szorosabb együttműködésről szóló megállapodást hozott létre az Egyesült Arab Emirátussal. Ez a térség arab államaival való ellenséges kapcsolat enyhülésében jelentős előrelépés, mert precedenst teremthet és hozzájárulhat a környező országok elutasító magatartásának változásához, illetve háttérbe szorítja a palesztin állami törekvéseket és Izrael államiságát hangsúlyozza.

A másik fogalom a geopolitikai pillér, mely azon országokra vonatkozik, amelyek „fontossága nem hatalmukból vagy becsvágyukból fakad, hanem stratégiai elhelyezkedésükből, illetve abból, hogy esetlegesen kiszolgáltatott helyzetük hogyan hat a geostratégiai játékosok viselkedésére.”[14] Izrael puszta léte is jelentős politikai és kulturális következményekkel jár a környező arab államokra nézve, mert a zsidó állam elismerésének kérdése megosztja a nemzetközi közösség tagjait. Izrael különleges helyzete abból fakad, hogy a Közel-Kelet egyetlen demokráciájaként az Egyesült Államok egyik legfontosabb szövetségese a térségben, és ez a szoros kapcsolat minimálisra csökkenti az arabok számára Izrael megsemmisítésének lehetőségét. Gazdasági erejét elsősorban a földgázforrásai jelentik, mely által az elmúlt két évtized során fontos exportőrré vált. Továbbá a térség egyedüli atomhatalma, amely komoly elrettentő erőt jelent az arab államok felé. [15]

9 Schweitzer András: *Jeruzsálem nemzetközi státusa – politikai dokumentumok és értelmezések.* Külügyi Szemle, II. évf. 2003/1., 62–79.

10 *Trump says US recognises Jerusalem: The speech in full*. 2017. https://www.bbc.com/news/world-middle-east-42264868 (Letöltés időpontja: 2020. 10. 07.)

11 The World Factbook: *Israel.* 2021. https://www.cia.gov/the-world-factbook/countries/israel/ (Letöltés időpontja: 2021. 02. 22.)

12 Tim Marshall: *A földrajz fogságában.* Budapest, Park, 2019. 203.

13 Zbigniew Brzezinski: *A nagy sakktábla*. Budapest, Antall József Tudásközpont, 2017. 57.

14 Uo.

15 *Israel Could Be Key to 2020 Middle East Geopolitics*. 2020. https://besacenter.org/perspectives-papers/israel-2020-geopolitics/ (Letöltés időpontja: 2020. 10. 23.)

3. Izrael terrorfenyegetettsége a 21. században

2001. szeptember 11-e a terrorizmus elleni küzdelem fontos mérföldkőjévé vált. Az Egyesült Államokban az amerikai polgárháború óta nem történt katasztrófa, amely ilyen súlyos veszteséget okozott volna. A támadás előtérbe helyezte a terrorizmus elleni küzdelmet.[16]

Az új évezred elején bekövetkezett katasztrófa következményeként a demokratikus országok kiemelt figyelmet szenteltek a terrorizmus elleni stratégiák megújítására, mely során kihívást jelentett a hatékony fellépés és az emberi jogok érvényesülése közötti egyensúly megteremtése. A tapasztalatok és bevált módszerek megosztása gyakori a demokratikus államok között, a terrorizmussal szembeni küzdelem esetében Izrael került a középpontba. Az országot gyakran éri kritika az emberi jogok megsértése és az áldozatul eső palesztin lakosság miatt, de kétségtelen, hogy rendelkezik példaértékű módszerekkel azon demokráciák számára, amelyek a terrorizmus egyre fenyegetőbb kihívásával néznek szembe.

A Global Terrorism Index (GTI) alapján Izraelben az elkövetett terrortámadások száma csökkenő tendenciát mutat, 2013-ban a 32. terrorizmus által legfenyegetettebb ország volt[17], 2018-ra azonban már a 40. helyen szerepelt a 163 államot vizsgáló listán.[18] A másik reprezentatív mutató a Global Peace Index (GPI), amely ugyanebben a 163 országban a béke szintjét méri a belső konfliktusok, szociális biztonság és militarizáció alapján. A listán Izrael a

145. helyen állt 2019-ben. A GPI mérésénél vizsgált három szegmens közül a militarizáció –mely a katonai képességek, fegyverek, aktív szolgálatot teljesítők, nukleáris fegyver birtoklása, védelmi költségvetés stb. alapján épül fel – terén kapható pontok Izrael esetében voltak a legmagasabbak, vagyis Izrael volt a legmilitarizáltabb 2019-ben (az országok közül a 163.).[19]

3.1. Új típusú terrorizmus

Az új típusú terrorizmus fogalmának megjelenése a szeptember 11-i támadáshoz köthető. A korábbi évtizedek alatt az ilyen jellegű aszimmetrikus támadások esetében a merényletet általában előre jelezték, rögzítették a követeléseket és a célokat. Ezzel szemben az új típusú terrorizmus sokkal kiszámíthatatlanabb.[20] Jellemzője, hogy céljai nem megvalósíthatók, a támadási opciók korlátlanok, hagyományos és nem hagyományos fegyverek is megjelennek, nagy területre kiterjed a hatása, transznacionális jellegű, általában nincs a támadások előtt figyelmeztetés, továbbá bevett módszerré váltak az öngyilkos merényletek.[21] A célpontok tekintetében az új típusú terrorizmus során az állami intézmények, szervek, személyek helyett a civilek, ártatlan állampolgárok is gyakran áldozatul esnek. Az okok korábban főként politikai jellegűek voltak, ma már az etnikai, vallási feszültségek a gyakoribbak. A terrorista szervezetek felépítését tekintve a centralizált struktúrát az egyszemélyes, cella alapú rendszer váltotta fel. Ezzel együtt az alkalmazott módszerek is megváltoztak, a korábbi túszejtések, emberrablások, robbantások mellett a terrorcselekmények eszközrendszere sokkal szélesebb skálán mozog, mint korábban.[22]

16 Resperger István: *Az iszlám világ és hatása a biztonságra*. Budapest, Egyetemi, 2003. 50-51.

17 Institute for Economics and Peace: *GTI*. 2014. https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%20Report%202014.pdf (Letöltés időpontja: 2020. 10. 28.)

18 Institute for Economics and Peace: *GTI*. 2019. http://visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf (Letöltés időpontja: 2020. 10. 28.)

19 Institute for Economics and Peace: *Global Peace Index*. 2020. https://visionofhumanity.org/wp-content/uploads/2020/10/GPI_2020_web.pdf (Letöltés időpontja: 2020. 11. 12.)

20 Fregan Beatrix – Hronyecz Erika: *Új trendek a terrorizmusban? Rövid európai kitekintés*. Hadmérnök, IX. évf. 2014/4., 156–163., 158.

21 Tálas Péter: *A nemzetközi terrorizmus és a szervezett bűnözés hatása a nemzetközi biztonságra és Magyarország biztonságára.* 2007. https://kisebbsegkutato.tk.mta.hu/uploads/files/archive/904.pdf (Letöltés időpontja: 2020. 10. 25.)

22 Fregan – Hronyecz (2014.) i.m. (20. lj.) 159.

Izrael esetében a 21. században megjelenő új típusú terrorizmus két fontos körülményhez köthető. Egyrészt a szeptember 11-i terrortámadás után az Egyesült Államok közel-keleti politikájában a terrorizmus elleni harc terén élesebbé vált a térség országainak differenciált támogatása, a másik fontos körülmény pedig a második palesztin intifáda kirobbanása.[23] Utóbbi tapasztalatait a következő alfejezetben részletesebben ismertetem, kitérve arra, hogy a terrorcselekmények megakadályozása érdekében pontosan milyen eszközökkel és módszerekkel lépett fel Izrael.

3.2. A második palesztin intifáda

A második palesztin intifáda, vagy más néven al-Aksza intifáda a 21. század legnagyobb terrorhullámát hozta Izraelben, 2000-2007 között megközelítőleg 5800 ember vesztette életét a támadások során.[24]

2000. szeptember 28-án tört ki a második palesztin intifáda, amely népfelkelésből vált alacsony intenzitású fegyveres konfliktussá. Az Izrael elleni palesztin felkelés visszavetette az 1990-es években beindult békefolyamatokat Izrael és a Palesztin Hatóság között és a terror új hullámát indította meg.[25] A kudarcba fulladt békefolyamatból fakadó feszültség utolsó lökését egy izraeli politikai vezető, később miniszterelnök, Ariel Saron provokatív látogatása adta meg a palesztinok (valamint a zsidók) szent helyének is tekintett jeruzsálemi Templom-hegyen. A másnap megkezdődő palesztin demonstrációkra – elsősorban a Gázai-övezetben és Ciszjordániában – az izraeli rendvédelmi erők rendkívül hevesen reagáltak, mely eredménye négy palesztin halott és közel kétszáz sebesült volt. A kezdeti izraeli intézkedések intenzitásából fakadt, hogy az intifáda első három hónapjában palesztin részről fegyveresek elenyésző számban vettek részt, az áldozatok száma mégis a palesztinoknál volt sokkal jelentősebb.[26]

A második intifáda során a terrorizmus terén megmutatkoztak új eszközök és módszerek. A konfliktus alatt a palesztin részről alkalmazott eszközök a következők voltak: tömegdemonstrációk, melyek során kődobálás, kézigránátok dobálása, Molotov-koktélok, autógumik felgyújtása zajlott, a gerilla hadviselés, mint például út menti bombák a közlekedés akadályozására elsősorban a zsidó telepesek és a katonai objektumok felé vezető utakon, illetve a „stratégiai" terrorizmus, azaz a katonák elrablása, gépkocsi robbantások, késeléses merényletek, öngyilkos merényletek.[27] A palesztin öngyilkos merényletek csupán 1%-át tették ki a terrortámadásoknak,

mégis az okozott károk 44%-áért voltak felelősségre vonhatók. Ilyen merényleteket a második intifáda előtt is követtek el többek között a Hamász és a Palesztin Iszlám Dzsihád terrorista szervezetek részéről, de csak 2000 után váltak a leggyakrabban bevett és leghatékonyabb eszközükké.[28]

Az izraeli hadsereg válaszcsapásainak lehetőségeit korlátozta, hogy a harcok döntően civilek által lakott területeken folytak. Ebből az okból kifolyólag az IDF próbálta elkerülni az összetűzéseket a palesztin területeken, a hangsúly inkább a terrorista vezetők kiiktatásán volt. A komoly katonai szervezést és hírszerző tevékenységet igénylő akciók során a beazonosított személyeket a levegőből pilótanélküli légijármű (Unmanned Air Vehicle, UAV)[29] által

23 Kis-Benedek József: *A palesztin intifáda biztonságpolitikai és katonai összefüggései.* Felderítő Szemle, V. évf. 2006/2., 41–72. 46.

24 *Israeli-Palestinian Fatalities Since 2000 – Key Trends.* 2007. https://unispal.un.org/DPA/DPR/unispal.nsf/0/BE07C80CDA4579468525734800500272 (Letöltés időpontja: 2020. 10. 28.)

25 Kis-Benedek (2002) i.m, (2.lj.) 64–70.

26 Nagy Levente Balázs: *A második intifáda kitörése és első másfél éve.* 2002. http://www.europeer.hu/tanulmany/nagy_masodikintifada2002.pdf (Letöltés időpontja: 2020. 10. 27.)

27 Kis-Benedek (2002) i.m. (2. lj.) 78.

28 *Fear Management in Counter-Terorrism – A Study of Framing Approaches during the Second Intifada.* 2016. https://www.researchgate.net/publication/305730807_Fear_Management_in_Counter-Terrorism_-_A_Study_of_Framing_Approaches_during_the_Second_Intifada (Letöltés időpontja: 2020. 10. 26.)

29 Békési Bertold et alii: *Pilóta nélküli repülés profiknak és amatőröknek.* Nemzeti Közszolgálati Egyetem, Budapest, 2013, 11.

semmisítették meg.[30] Az IDF válaszcsapásainak eszközei közé tartozott továbbá a terroristagyanús személyek tömeges letartóztatása, a fegyverek használata a civil lakossággal szemben, a palesztin civilek élő pajzsként használata (épületek felderítésére, akadályok eltávolítására, izraeli katonák fedezésére), az ún. házrombolás (house demolition*)*, amely által több tucat házat dózerolt le a hadsereg néha előzetes figyelmeztetés nélkül (2001-2005 között 669 épületet romboltak le ilyen célból[31]), az orvosi ellátáshoz való hozzáférés akadályozása, továbbá Izrael biztonsági kerítést hozott létre bizonyos szakaszokon a Gázai-övezet és Ciszjordánia körül, melyeken csak a kijelölt ellenőrző pontokon lehetett áthaladni.[32]

Összességében az a következtetés vonható le, hogy a második palesztin intifáda az elsőhöz képest jóval szervezettebb, és felülről irányított volt, míg az 1987-es sokkal inkább volt népfelkelésnek tekinthető, továbbá megjelent néhány új módszer mindkét oldalon, de az izraeli terrorizmus elleni harcban nem következett be érdemi változás, tapasztalatait döntően az 1960-70-es évek konfliktusaiból szerezte. A hatékony terrorizmus elleni harc alapját a katonai műveletek, védelmi intézkedések és a hírszerzés magas színvonala és összehangolt alkalmazása jelentette és jelenti ma is.[33] A felsoroltakon kívül a második palesztin intifáda következményeként az izraeli társadalom biztonságpercepciója is átalakult, ami szintén meghatározó abban, hogyan és milyen intenzitással tud fellépni az izraeli kormány és ezáltal a hadsereg a terrorizmussal szemben. Az egyén és az állam biztonsága (nemzetbiztonság) közötti határ az elmúlt évtizedek történései és fenyegetési hatására összemosódott, kölcsönösen feltételezik egymást, ezért Izrael biztonságának kérdése központi szerepet tölt be a társadalmi kérdésekkel, kihívásokkal foglalkozó diskurzusokban.[34]

Fontos megállapítás továbbá, hogy az izraeli terrorizmus elleni fellépés sikere taktikai szinten nyilvánult meg, egyfajta paradox helyzetet teremtve: az állam célja az állampolgárok biztonságának szavatolása, ugyanakkor a heves katonai fellépések a palesztin terroristákkal szemben, a területfoglalások és a Palesztin Állam támogatásának hiánya éppen a terrorizmus táptalaját jelentik. Politikai szinten tehát az ismertetett módszerek nem, vagy csak kisebb mértékben mondhatók sikeresnek.[35]

3.3. Izraelt fenyegető terrorszervezetek

Izraelnek létrejötte óta több terrorszervezettel kellett már felvennie küzdelmet, melyek döntően palesztin csoportok, de a közel-keleti elhelyezkedésből adódóan a nem palesztin radikális iszlamista szervezetek is fenyegetést jelenthetnek. A továbbiakban a Global Terrorism Database alapján a 21. században Izraelben, illetve a Gázai-övezetben és Ciszjordániában aktív terrorista csoportokat ismertetem, melyek a következők:

Hamász[36]

A Hamász a Gázai övezetben és Ciszjordániában jött létre az első palesztin intifádát követően (1987-1991). Politikai ideológiája az egyiptomi Muzulmán Testvériség Mozgalmán alapszik, célja a palesztin területek felszabadítása és a zsidók kiűzése Izraelből a dzsihád, azaz a szent háború nevében. A béketörekvéseket elveti, kizárja a kompromisszum megkötését Izraellel és nem ismeri el annak jogállamiságát. Továbbá vitatja a Palesztin Felszabadítási Szervezet kizárólagos jogát a palesztin képviseletre vonatkozóan, ezért létrejötte óta a PFSZ, illetve

30 Kis-Benedek (2002) i.m. (2. lj.) 82.
31 Daniel Byman: *Curious Vistory: Explaining Israel's Suppression of the Second Intifada, Terrorism and Political Violence*. 2012., 24:5, 836.
32 Eyal Raz – Yael Stein: *Operation Defensive Shield.* 2002. https://www.btselem.org/download/200207_defensive_shield_eng.pdf (Letöltés időpontja: 2020. 11. 04.)
33 Byman (2012) i.m. (31. lj.) 826.
34 Paragi Beáta: *Biztonsági percepciók Izraelben*. Nemzet és Biztonság, 2009/7., 61.
35 Byman (2012) i.m. (31. lj.) 827.
36 A szó az arab Harakat al-Muqawama al-Islamiyya akronímája, magyar jelentése Iszlám Ellenállási Mozgalom.

annak legerősebb pártja, a Fatah alternatívája kíván lenni. Létrejöttekor elsősorban a rászorulók segítőjeként jelent meg, ma is végez szociális tevékenységet, többek között iskolák és kórházak fenntartása által. 2006-ban a palesztin választások után kormányt alakíthatott, majd egy évvel később a Fatahot kiszorítva, de facto átvette az irányítást a Gázai-övezet fölött.[37]

A Hamászhoz köthető a második palesztin intifáda legtöbb halálos áldozatot követelő terrorcselekménye, amikor 2002-ben egy öngyilkos merénylő egy szállodában 30 izraeli életét vette el és 140-et sebesített meg.[38] A Hamász katonai szárnya az ún. Kasszem Brigádok, amely a GTI szerint az IDF 2005-ös gázai kivonulását követően 2018-ig megközelítőleg 250 terrortámadást kivitelezett elsősorban fegyveres támadások, robbantások és öngyilkos merényletek által.[39] Sajátos módszere a Hamásznak az alagút-rendszer, amely a Gázai-övezet nagy részét lefedi, a járatokat katonai célra használják, többek között fegyverek csempészésére és raktározására.[40] Izrael déli területein ma sincsen béke a terrorszervezettel, az elmúlt néhány hónapban is több rakétatámadás történt a Gázai-övezet és Izrael határán.[41]

Palesztin Iszlám Dzsihád (Palestinian Islamic Jihad, PIJ)

A Palesztin Iszlám Dzsihád egyiptomi alapítású (1979), a Muszlim Testvériség Mozgalomból vált ki, a Hamasz után a második legnagyobb terrorszervezet a Gázai-övezetben, de előbbivel ellentétben nincs jelen politikai téren és szociális, társadalmi szerepet sem vállal. A Gázai-övezeten kívül a szervezethez köthető terrorista sejtek Libanonban és Szíriában is jelen vannak. A PIJ célja a zsidók kiűzése és egy iszlám állam létrehozása Izrael területén. A szervezet fő támogatója Irán és Szíria, továbbá a Hamasszal közösen egyre több merényletet követ el. Katonai ereje az Egyesült Államok becslése szerint ezer fő körül van, saját bevallása szerint nyolcezer harcképes katonával rendelkezik.[42] A második intifáda végétől 2018-ig közel kétszáz terrortámadásért vállalt felelősséget a Gázai-övezetben, Ciszjordániában és az ezekkel határos izraeli területeken.[43]

Al-Aksza Mártírjainak Brigádja (Al-Aqsa Martyrs' Brigade, AAMB)

Az al-Aksza Mártírjainak Brigádja a második intifáda kitörése után jött létre, mint a Fatah radikális katonai szárnya. Nem iszlamista mozgalom, ezért a támadások motivációja nem a globális dzsihádból eredeztethető, hanem a palesztin nacionalizmusból, célja a Palesztin Állam létrehozása. A szervezet decentralizált jellege miatt nehéz pontosan meghatározni a méretét, de becslések szerint ezer fő körül lehet a létszáma. 2002-től (az al-Aksza intifáda második felétől) célpontjaik már nem csak az izraeli fegyveres erők voltak, hanem a Gázai-övezet és Ciszjordánia civil lakossága is. A kézifegyveres és robbanóeszközök mellett bevetté váltak az öngyilkos merényletek, az ellenőrzőpontok megtámadása és az izraeli területek rakétával való támadása a palesztin fennhatóságú területekről.[44]

---

37 *Hamasz*. http://www.grotius.hu/publ/displ.asp?id=EGNMSM (Letöltés időpontja: 2020. 10. 29.).

38 Byman (2012) i.m. (31. lj.) 830.

39 *Global Terrorism Database.* http://apps.start.umd.edu/gtd/search/Results.aspx?expanded=yes&casualties_type=b&casualties_max=&start_yearonly=2005&end_yearonly=2018&dtp2=all&success=yes&perpetrator=399&ob=GTDID&od=desc&page=1&count=100#results-table (Letöltés időpontja: 2020. 11. 10.)

40 *Hamas' Military Wing.* https://www.idf.il/en/minisites/hamas/hamas/hamas-military-wing/ (Letöltés időpontja: 2020. 10. 29.).

41 *Israel and Hamas said to reach agreement for 6-month ceasefire.* 2020. https://www.timesofisrael.com/israel-and-hamas-said-to-reach-agreement-for-6-month-ceasefire/ (Letöltés időpontja: 2020. 10. 29.)

42 *Palestinian Islamic Jihad.* https://www.counterextremism.com/threat/palestinian-islamic-jihad (Letöltés időpontja: 2020. 10. 29.)

43 *Global Terrorism Database.* http://apps.start.umd.edu/gtd/search/Results.aspx?page=2&casualties_type=b&casualties_max=&start_yearonly=2005&end_yearonly=2018&dtp2=all&perpetrator=30214&count=100&expanded=no&charttype=line&chart=overtime&ob=GTDID&od=desc#results-table (Letöltés időpontja: 2020. 10. 29.)

44 *Al-Aqsa Martyrs' Brigade.* 2015. https://mackenzieinstitute.com/terrorism-profile-al-aqsa-martyrs-brigade-aamb/ (Letöltés időpontja: 2020. 10. 29.)

Hezbollah

A Hezbollah (Isten Pártja) nem palesztin, hanem radikális iszlám szervezet. A siíta politikai párt és katonai szervezet Libanonban jött létre erős iráni befolyás alatt 1982-ben, kezdetben csak katonai szárnyból állt és eredeti céljai között Izrael elpusztítása, a nyugati befolyás megszüntetése, Libanon síita államma alakítása és a saját, illetve Irán ellenségeivel való leszámolás szerepelt. Továbbá az Aszad-rezsim mellett áll Szíriában és támogatja az egységes palesztin állam létrehozásának elképzelését.[45]

Az 1990-es évek óta a libanoni parlamentben politikai pártként van jelen, ezért megosztott a terrorista szervezetté való nyilvánítása a nemzetközi közösség részéről, noha katonai szárnya bombázásokért, merényletekért, emberrablásokért felelős. Széleskörű társadalmi elfogadottsága szociális tevékenységei köthető, mint az oktatás, egészségügy támogatása főként, továbbá rendelkezik saját hírügynökséggel és rendőrséggel is.[46] Az Izrael-ellenes tevékenysége alapvető elemei a fegyver-és embercsempészet, illetve a palesztin terrorista csoportok pénzelése. Aktívan együttműködik más terrorista szervezetekkel, mint a PIJ és a Hamász.[47]

Az IDF és a Hezbollah fegyveres összecsapásainak minimalizásáért és a béke megőrzéséért 1978-tól az ENSZ békefenntartó missziója (UNIFIL)[48] jelen van az izraeli-libanoni határon, de ennek ellenére rendszeresek a rakéta-és dróntámadások.[49]

A felsorolt terrorszervezetek jelentik a legnagyobb fenyegetést, de rajtuk kívül más csoportok is jelen vannak és ritkábban ugyan, de követnek el támadásokat, mint például az Iszlám Állam, amely 2014-ig volt komoly fenyegetésként számon tartva Izrael esetében.[50] Az Egyesült Államok által terrorszervezetnek nyilvánított csoportokon kívül érdemesnek tartom megemlíteni a Palesztin Hatóság tevékenységét. A 2000-es évek elején a PA biztonsági szolgálatai hivatalosan támogatták a második intifáda elleni küzdelmet, a valóságban azonban az elnök, Jasszer Arafat széndákosan nem lépett fel hatékonyan a felkelőkkel vagy terrorista cselekményeket elkövetőkkel szemben. Ez keményebb izraeli fellépést vonzott maga után, a meggyengített biztonsági szolgálatok azonban teret engedtek a radikális Hamasz megerősödésének a Gázai-övezetben.[51]

Kiegészítő gondolatként elmondható, hogy Izraelben jelenleg viszonylagos béke van. A vitatott területek határain rendszeresen zajlanak ugyan főként rakétatámadások, de a második palesztin intifádához hasonló tömegterrorizmus nem tapasztalható. Az alacsony intenzitással folyó katonai műveletek mellett az figyelhető meg, hogy Izrael területi vitái – és ezáltal a palesztin terrorszervezetekkel való kapcsolatai – a nemzetközi jog, politika és propaganda dimenziója felé tolódnak el, ezt támasztják alá az Egyesült Államok határozott állásfoglalásai is. A palesztin sérelmi kultúra nem változott, csak a stratégia és az eszközök. Terrorizmus szempontjából a jelenlegi viszonylagos béke a palesztinokkal akkor kerülhet veszélybe, ha a Palesztin Hatóság Fatah pártja vagy a Hamász destabilizálódik és elveszíti a kontrollt a fegyveres erők fölött.

45 *Hezbollah.* 2019. https://cisac.fsi.stanford.edu/mappingmilitants/profiles/hezbollah#text_block_18070 (Letöltés időpontja: 2020. 10. 31.)
46 *About Hezbollah*. https://hezbollah.org/about-hezbollah (Letöltés időpontja: 2020. 10. 31.)
47 Tomolya János*: A „34 napos" izraeli-libanoni háború.* Hadtudomány, XVII. évf. 2007/1., 1–23.
48 United Nations Interim Force in Lebanon.
49 *UN Peacekeepers investigating flareup on Israel-Lebanon border.* 2020. https://www.timesofisrael.com/un-peacekeepers-investigating-flareup-on-israel-lebanon-border/ (Letöltés időpontja: 2020. 10. 31.)
50 *A critical analysis of Israel's counter-terrorism strategy*. 2016. https://foreignpolicynews.org/2016/08/08/a-critical-analysis-of-israels-counter-terorrism-strategy/ (Letöltés időpontja: 2020. 11. 11.)
51 Byman (2012) i.m. (31. lj.) 829.

4. A terrorizmus elleni küzdelem

A terrorizmus elleni küzdelem alapját az offenzív és a defenzív műveletek megfelelő kombinációja jelenti. Izrael esetében az offenzív módszerek a terroristák vezetőinek letartóztatását és kiiktatását jelentik (megfelelő hírszerző tevékenységre alapozva), míg a defenzív intézkedések többek között a felderítést és az olyan fizikai akadályokat foglalják magukban, mint az ellenőrzőpontok és biztonsági kerítések Izrael és a vitatott területek határain.[52] Az offenzív és defenzív elemek mellett a harmadik lényeges terület a következménykezelés, amely a terroristatámadásokat követően kialakult katasztrófa-vagy szükséghelyzet helyreállítását jelenti.

Az izraeli hadsereg célzott támadásai a terrorista sejtek vezetőivel szemben gyakran járnak ártatlanok halálával is, ezért a nemzetközi közösség részéről éles kritikákhoz vezet. A nemzetközi vélemény formálásában – Izrael javára – nagy szerepet játszott a 2004-es madridi, a 2005-ös londoni, a 2015-ös párizsi, a 2016-os brüsszeli és a 2017-es londoni terrortámadás, melyek következményeként az Európai Unió tagállamai is más szemmel kezdték nézni a terrorizmus által jelentett veszélyt és az ellene való harc komplex kihívásait.[53]

4.1. Izrael fegyveres ereje

Az Izraeli Védelmi Erők (továbbiakban: IDF) 1948-ban az Izraeli Állam megalapításával együtt jött létre. Fő feladata az ország szuverenitásának és területi integritásának védelme, fennállása óta hat háborúban védte meg a hazáját, ezáltal a világ egyik legharcedzettebb haderejének mondható. A történelem során az izraeli hadsereg jellemzően számbeli hátrányban volt, ezért a hangsúlyt a fegyverrendszerek modernizálására, fejlesztésére helyezték.[54] A Világbank adatai szerint Izrael védelmi kiadásai 2019-ben a GDP 5,2%-át tették ki, amely az elmúlt tíz év legalacsonyabb értéke. A legmagasabb arány 2008-ban volt, amikor ugyanez az érték a GDP 6,4%-ával egyezett meg.[55]

Az izraeli aktív hadsereg létszáma 169,500 fő. Három haderőnem alkotja a hadsereget, a szárazföldi haderő, a légierő és a haditengerészet. Továbbá a terrorizmus elleni harc terén kiemelkedő fontosságú a különleges erők bevetése is. [56]

Az IDF korlátozott erőkivetítési képességgel rendelkezik, célja a területi integritás védelme és a szomszédos államokban történő rövidtávú beavatkozások. Izrael a küszöbországok közé tartozik, amelyek „nyíltan vagy titokban, akár nemzetközi kötelezettségeik megszegésével is nukleáris fegyverek megszerzésére, birtoklására törekedtek vagy törekszenek.”[57] Ezen belül Izrael el nem ismert atomhatalomnak számít, mert ugyan nem deklarálta nukleárisfegyver-előállítási képességét, de az információk alapján képes annak előállítására, sőt a SIPRI[58] jelentése szerint 2019-ben 90 db nukleáris robbanófejjel rendelkezett.[59]

Az IDF képességei elsősorban az Izraelen és a szomszéd arab országokon belüli műveletekre koncentrálódnak. Az országot érő fenyegetés aszimmetrikus jellege miatt az elmúlt évek során a légvédelmi képességek és precíziós fegyverek modernizációja zajlott. A védelmi képességek terén Izrael több területen is a világszínvo-

52 Avi Dicter – Daniel L. Byman: *Israel's Lessons for Fighting Terrorists and Their Implications for the United States*. 2016. https://www.brookings.edu/wp-content/uploads/2016/06/byman20060324.pdf (Letöltés időpontja: 2020. 11. 11.)
53 Uo.
54 *Izraeli Védelmi Erők.* https://embassies.gov.il/budapest/AboutIsrael/State/Pages/Izraeli-Védelmi-Erők.aspx (Letöltés időpontja: 2020. 11. 03.)
55 *Israel – Military Expenditure*. https://tradingeconomics.com/israel/military-expenditure-percent-of-gdp-wb-data.html (Letöltés időpontja: 2020. 11. 03.)
56 The International Institute for Strategic Studies: *The Military Balance 2020*, Routledge, 2020, 355.
57 Gazdag Ferenc – Remek Éva: *A biztonsági tanulmányok alapjai.* Budapest, Dialóg Campus, 2018. 195.
58 Stockholm International Peace Research Institute.
59 SIPRI: *World nuclear forces*. 2020. https://www.sipri.org/yearbook/2020/10 (Letöltés időpontja: 2020. 11. 03.)

nalú képességekkel rendelkezik, mint a páncélozott járművek, pilóta nélküli járművek, precíziós fegyverek és a kiberbiztonság.[60] A fentiek alapján elmondható, hogy az izraeli hadsereg jelentős elrettentő képességgel rendelkezik az atomfegyver birtoklása, a komoly támadóerővel bíró légierő, hadműveleti rakéták, rakéta-elhárító rendszerek, a haditengerészet korszerű felszerelése, elsősorban tengeralattjárók, a hatékony felderítés és az Egyesült Államokkal való stratégiai partnerség révén.[61]

Az IDF számos eszközt fordít az emberek védelmére. Az izraeli Raphael hadiipari vállalat a harcjárművek védelmére kifejlesztette a Trophy aktív védelmi rendszert (Active Protection System, APS), melynek elsődleges feladata az ellenséges páncéltörő rakéták semlegesítése.[62] Ugyanennek a cégnek a kis lőtávolságú rakéták, aknagránátok és tüzérségi lövedékek elleni védelemre kifejlesztett rakétavédelmi fegyverrendszere a „Vaskupola" (Iron Dome). Elsősorban a Hamász és más gázai-övezeti fegyveres csoportok, illetve a Hezbollah támadásainak kivédésére szolgál.[63] Az improvizált robbanóeszközök (Improvised Explosive Device, IED) azokat a „házilagos készítésű" robbanóeszközöket jelentik, amelyek egyszerűen, akár internetes útmutató alapján is, olcsón előállíthatók, de harcászati szinten az alkalmazásuk sok áldozattal jár, továbbá a Raphael kifejlesztett olyan védelmi rendszereket is, amelyek az IED fenyegetésre jelentenek megoldást. [64]

A terrorizmus elleni harc másik fontos elemeként a megelőzés feladatát ellátó biztonsági szolgálatokat mutatom be. Az Izraeli Állam kikiáltását követően két évvel megalakult a mai izraeli titkosszolgálati rendszer három fő pillére. A katonai felderítésért az IDF-en belül az *Aman* felel, a belbiztonsági tevékenységért a *Shin Bet*, a külföldi hírszerzésért pedig a *Moszad*.[65] Az 1990-es évek alatt kezdődött meg a titkosszolgálatok reformja, melynek eredményeként a szervek területi alapon határolódtak el egymástól nem pedig felelősségi körök alapján, ami elősegítette a hatékony, precíz titkosszolgálati munkát a szervek versengése helyett. A felsoroltak közül a terrorelhárítás elsősorban a Moszad és a Shin Bet feladatait közé tartozik. Előbbi a hírszerzés és külföldi műveletek által végez terrorelhárítási tevékenységet, utóbbi pedig ennél szélesebb értelemben felel a terrorhálózatok elleni harcért, a terrorgyanús elemek kihallgatásáért, a kémelhárításért, illetve a terrorelhárítási hírszerzésért a Gázai-övezetben és Ciszjordániában. A szolgálatok együttműködését a „need to share" klasszikus információszerzési elv helyett a „must to share" elvének alkalmazása biztosítja.[66] A hatékony hírszerzési közösség működéséhez hozzájárul az is, hogy nem a titkosszolgálatok nem csak egymással működnek teljes mértékben együtt, hanem többek között az Izraeli Határrendőrség terrorizmus elleni különleges egységeivel, mint a YAMAM[67] és a YAMAS[68].

Az izraeli hírszerzés módszerei közt a HUMINT (Human Intelligence, emberi erővel folytatott felderítés) és SIGINT (Signals Intelligence, rádióelektronikai felderítés) adatszerzés jelenik meg elsődlegesen, utóbbi sikeres alkalmazása abból is fakad, hogy Izrael innovációs nagyhatalomként a kiberbiztonság és technológiai fejlesztések terén élen jár.[69]

---

60 The International Institute for Strategic Studies: *The Military Balance 2020*, Routledge, 2020, 355.
61 Kis-Benedek József: *A Közel-Kelet katonai sajátosságai*. Külügyi Szemle, XII. évf. 2013/1., 79–99. 81.
62 *Trophy Active Protection System for AFVs.* https://www.rafael.co.il/worlds/land/trophy-aps/ (Letöltés időpontja: 2020. 11. 08.)
63 Kiss Álmos Péter: *Az izraeli integrált rakétavédelmi rendszer.* Honvédségi Szemle, 141. évf. 2013/5., 31–46. 40.
64 Kovács Zoltán: *Az improvizált robbanóeszközök főbb típusai*. Műszaki Katonai Közlöny, XXII. évf. 2012/2., 37–52. 35.
65 Rémai Dániel: *Az izraeli nemzetbiztonsági rendszer fejlődésének története*. Nemzetbiztonsági Szemle. VII. évf. 2019/4., 3–19. 5.
66 Uo. 12.
67 A YAMAM a héber Yehida Meyuchedet le'Milchama akronímája, magyarra fordítva izraeli terrorellenes csoportot jelent.
68 A YAMAS a héber Yehida Mishtartit Mistaravim akronímája, magyarra fordítva terrorellenes fedett egységet jelent.
69 *Mossad, realities and myths of Israel's national intelligence service.* 2018. https://www.nimmonsconsulting.com/mossad-mythology-reality/ (Letöltés időpontja: 2020. 11. 03.)

Az új típusú terrorizmus megfékezésére az izraeli hadsereg a hírszerzésre támaszkodva, több terrorellenes műveletet is végrehajtott. A 21. század négy legjelentősebb hadműveletе, amelyek tapasztalataira épülve az ország terrorizmus elleni stratégiája fejlődni tudott:

- Operation Defensive Shield („Védőpajzs" hadművelet) - 2002
- Operation Cast Lead („Öntött ólom" hadművelet) - 2008
- Operation Pillar of Defence („Felhőoszlop" hadművelet) - 2012
- Operation Protective Edge („Erős szikla" hadművelet) - 2014[70]

4.2. Terrorizmus elleni stratégiai irányelvek

A stratégia általános értelemben a társadalmi lét fenntartható fejlődésének és hatékony funkcionális működése érdekében alkalmazott eljárások és elvek összessége.[71] Ebből következik, hogy a terrorizmus elleni stratégia az ilyen jellegű támadások megakadályozásának és az elkövetők kiiktatásának módszereit, eszközeit és ezek alkalmazásának elveit foglalja magába. Az alfejezetben a terrorizmus elleni harc mint cél irányelveit mutatom be.

Az Izraeli Állam történelme során a terrorizmus hagyományosan meghatározta a lakosság életét, hatással volt a politikára és az ország gazdaságára is. Ezért fontos megvizsgálni, hogy stratégiai szinten milyen irányvonalakat szabott meg Izrael, hogy az ilyen típusú fenyegetést kezelni tudja. Az új típusú terrorizmus elleni küzdelmet és a hatékony stratégia kialakítását megnehezítette, hogy a második intifádát követően a terrorszervezetek éles elhatárolása egymástól gyakran lehetetlen volt, a konkrét ellenségkép meghatározása akadályokba ütközött. Az izraeli hadsereg terrorizmus elleni műveletei mentén ugyanakkor kirajzolódtak a stratégiai irányvonalak.

Benjamin Netanjahu, Izrael jelenlegi miniszterelnöke tíz pontban fogalmazta meg a terrorizmus elleni küzdelem elemeit. A katonai szektor mellett kiemelte a gazdasági, pénzügyi, jogi és társadalmi területeket is. Ezeket kifejtve a terroristák legyőzése nem csak katonai eszközökkel lehetséges, hanem további módszer a gazdasági szankciók, blokádok alkalmazása, pénzügyi számlák befagyasztása akár a terroristákat pénzzel vagy fegyverrel támogató országokkal szemben. Jogi aspektusból megközelítve a terroristagyanús személyek körözése, letartóztatása, illetve az elítéltek életfogytiglani büntetése vezet eredményre. Társadalmi szempontból az információmegosztáson több hangsúlynak kell lennie nemzetközi szinten is, továbbá az embereket tudatosságra és ellenállásra kell nevelni a terrorfenyegetett területeken.[72]

A 2000-es évek elején az izraeli terrorizmus elleni harc megoldását az akkori miniszterelnök, Ehud Barak a palesztinokkal való békés rendezés útján tartotta megvalósíthatónak. A tárgyalások kudarca, a második palesztin intifáda kitörése és az új izraeli miniszterelnök hivatalba lépése ezzel szemben 2001-től fordulatot hozott, és a terroristákkal való agresszív fellépés került előtérbe.[73]

Izrael terrorizmus elleni stratégiáját tágabb értelemben véve meghatározza a nemzeti biztonsági stratégia, melynek a 2006-2016-ig terjedő időszakban a következők váltak az irányelveivé: a megelőzés, elrettentés, defenzív és offenzív műveletek kombinációja, melyek alkalmazásánál különbséget kell tenni a létfenyegetés, és más jellegű fenyegetések, továbbá a valós és vélt fenyegetések között. Nagy hangsúly van a katonai erő fejlesztésén és a stra-

70 Israel Defense Forces: *Counterterrorism.* https://www.jewishvirtuallibrary.org/israeli-counter-terrorism (Letöltés ideje: 2020. 11. 03.)

71 Szendy István: *Hadügy és hadviselés*. Budapest, Dialóg Campus, 2017. 173.

72 Benjamin Netanyahu: *Fighting Terorrism. How Democracies Can Defeat the International Terrorist Network.* New York, Straus and Giroux, 2001. 178–196.

73 *The consequences of Israel's counter terrorism policy.* 2008. https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/439/Pia%20Jansen%20PhD%20thesis.pdf?sequence=6&isAllowed=y (Letöltés időpontja: 2020. 11. 08.)

tégiai kapcsolat fenntartásán az Egyesült Államokkal továbbá a közel-keleti régió államaival. Az erő alkalmazása a célok érdekében csak a szükséges és arányos mértékben történhet meg, továbbá a társadalom biztonságpercepcióját figyelembe kell venni és a biztonságtudatosságot ki kell alakítani az emberekben.[74]

Az IDF volt vezérkari főnöke, Gadi Eisenkot nevéhez köthető a 2007-ben kidolgozott Dahiya (jelentése: elutasítás) doktrína, amely többek között tartalmazta a polgári infrastrukturális elemek megsemmisítését, amennyiben azokat az ellenség használni tudja, akár aránytalan erő alkalmazás által is.[75] Ezzel megsértette a humanitárius jog egyik alapelvét, az arányosság elvét, amely szerint „tilos az olyan támadás indítása, amelyben az esetleges polgári áldozatok, vagy a polgári létesítményekben okozott kár aránytalan lenne az elérni kívánt konkrét és közvetlen katonai előnyhöz képest."[76] Ezen kívül más alapelvek is megsértésre kerültek, mint a megkülönböztetés elve, melynek értelmében a polgári lakosság és létesítmények nem lehetnek támadás célpontjai, továbbá az elővigyázatosság elve, mely alapján a támadás eszközét és módját úgy kellene megválasztani, hogy elkerüljék a polgári lakosságban és javakban okozott károkat.[77]

A 2010-es évek közepére az átfogó terrorizmus elleni stratégiát meghatározta a terrorista szervezetek infrastruktúrájának rombolása és gyengítése, a támadások által okozott kár csökkentése a defenzív jellegű műveletek által és a terrorizmus gyökereinek meggyengítése olyan módon, hogy a terroristák és az őket támogató országok motivációit minimálisra csökkentik.[78] Az új típusú terrorizmus jelentette fenyegetés során Izrael többször hajtott végre katonai műveleteket, melyek során alkalmazta a tömeges megtorlás módszerét, konkrétan 2008-ban, 2012-ben és 2014-ben.[79]

2015-ben új stratégiai dokumentum született szintén Eisenkot nevéhez köthetően *Deterring Terror – How Israel Confronts the Next Generation of Threats* címmel. A dokumentum elsődleges fenyegetésként a Gázai-övezetben megerősödő terrorizmust, a ciszjordániai palesztin erőszakot és a libanoni határnál a Hezbollah terrortevékenységét emelte ki. 2017-ben a Netanjahu miniszterelnök által kezdeményezett új nemzeti biztonsági stratégia az ezen fenyegetések elleni harchoz a következő irányvonalakat rendelte hozzá: az ellenségeivel szembeni relatív előny megőrzése, a nemzetközi kapcsolatok fejlesztése, továbbá a biztonság katonai, gazdasági, politikai és társadalmi dimenziója közötti átfedés. A Netanjahu-féle stratégia a szárazföldi képességek, a légierő és a hírszerzés fejlesztését irányozta elő a modern technológiák integrálásával, ezáltal nem a „holnap", hanem a „holnapután" kihívásaira felkészülve.[80]

2019-ben a következő sarokkövet Aviv Kohavi vezérkari főnök által meghirdetett Tenufa (jelentése: lendület) terv jelentette, melynek célja, hogy az IDF hatékonyabban és felkészültebben tudjon reagálni a fenyegetésekre, köztük a terrorizmusra is. Ennek eszközei közé tartozik az előzetes szcenáriók kidolgozása és az ezekhez szükséges védelmi képességek fejlesztése, a célpontok listájának folyamatos frissítése, a fegyverek modernizálása kiemelt tekintettel az informatikai rendszerekre és a hírszerzés fejlesztése.[81]

---

74 Dan Meridor – Ron Eldadi: *Israel's National Security Dotrine: The Report of the Committee in the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later.* 2019. https://www.inss.org.il/wp-content/uploads/2019/02/Memo187_11.pdf (Letöltés időpontja: 2020. 11. 06.)

75 Rémai Dániel*: Biztonsági kihívások hálójában, avagy az Izraeli Védelmi Erők esete az aszimmetrikus hadviseléssel.* Honvédségi Szemle. 148. évf. 2020/6., 16–31. 25.

76 *Humanitárius jog a gyakorlatban.* http://juris.oldportal.u-szeged.hu/download.php?docID=38511 (Letöltés időpontja: 2020. 11. 08.)

77 Uo.

78 Meridor –Eldadi (2019) i.m. (73. lj.)

79 Mark Vinson: *An Israeli Approach to Deterring Terrorism.* 2008. https://cco.ndu.edu/Portals/96/Documents/prism/prism_5-3/An_Israeli_Approach_to_Deterring_Terrorism.pdf (Letöltés időpontja: 2020. 11. 05.)

80 Rémai (2020) i.m. (74. lj.) 26.

81 *IDF appoints general to lead new Iran Command as threat escalates.* 2020. https://www.jpost.com/israel-news/idf-appoints-general-to-head-up-new-iran-command-as-threat-escalates-617507 (Letöltés időpontja: 2020. 11. 06.)

Az IDF által meghatározott terrorfenyegetést 2020-ban a Hamász, a Hezbollah, a palesztin „magányos farkas" terroristák és Irán jelentik. Utóbbi egyrészt a nukleáris fegyverkezés és hagyományosan Izrael ellenes külpolitikája, másrészt pedig a Hezbollah iszlám militáns szervezet támogatása miatt jelent fenyegetést.

A terrorizmus katonai értelmezésén túl megjelent a kibertér is, mint a támadások és a megfélemlítés további lehetséges dimenziója. A kiberterrorizmus elleni felkészültség kiemelt érdeke Izraelnek, lévén fejlett technológiával rendelkező, digitalizálódó ország. A „Facebook intifáda" kifejezés a palesztin terrorista csoportok – elsősorban a Hamász – által végzett olyan jellegű tevékenység, amely a közösségi média felületek használatán keresztül buzdít támadások elkövetésére, videókat oszt meg a terrorcselekményekről és azok kivitelezéséhez tanácsokkal is szolgál.[82] A kiberterrorizmus jelenségére reagálva Izrael 2016-ban új terrorizmus elleni törvényt vezetett be, amely az online térben végzett buzdító, támogató, toborzó tevékenységek széles skáláját is terrorcselekménynek minősíti.[83]

A 21. század során az emberi jogok megsértése és a kisebbségek felé tanúsított érzékenység nemzetközi szinten egyre nagyobb hangsúlyt kap, ezért Izrael a katonai válaszcsapásokat rugalmasan kezelve és minimálisra csökkentve hajtja végre. A palesztin és az izraeli stratégia is megváltozott, a katonai műveletek helyett egyre inkább nemzetközi jogi és gazdasági dimenzióba helyezve a palesztin-izraeli konfliktust, amely a terrorizmus egyik kiváltó oka Izraelben. A palesztin államiság kérdésének kezelése helyett az új stratégia a kívülről befelé haladó békekötés, mely elsősorban az arab országokkal való békés folyamatok megindulását szorgalmazza.

5. Következtetések

A publikáció elkészítése során az motivált, hogy az izraeli esettanulmányon keresztül a terrorizmus elleni küzdelem olyan mintáját elemezzem, amely más terrorfenyegetett országokban is alkalmazható lehet. Az ország létrejöttének sajátos körülményeiből, illetve *geopolitikai és geostratégiai jellemzőiből fakadóan* azt a megállapítást lehet tenni, hogy a terrorizmus hátterében álló motivációk is egyediek. Geopolitikai adottságai miatt körkörös a fenyegetés a szomszéd országok, a terrorista csoportok és a militáns iszlám részéről. Az ország folyamatos és hosszú ideje mély összetett (elsősorban politikai és gazdasági) válságokban levő országok környezetében létezik, ebből adódóan a terrorfenyegetettséget a mély gazdasági szakadék Izrael és az arab országok között csak erősíti. A különböző terrorista szervezetekben és militáns iszlám csoportokban közös motívum, hogy legtöbb esetben az Izraeli Állam megsemmisítése és el nem ismerése az elkövetett terrorcselekmények fő kiváltó oka.

A fent említettek alapján megállapítható, hogy Izrael esetében az egyik legfontosabb a terrorizmus elleni stratégia, amely nem egy konkrét dokumentum, hanem az ország történelme során megfogalmazott több stratégiai irányelv, nemzetbiztonsági és katonai doktrína együttese. Ezáltal a terrorizmus elleni stratégia megfelelően rugalmas, az adott fenyegetéshez rendeli a megfelelő védelmet, továbbá átfogó módon értelmezi a fenyegetéseket és minden kor terror eszközére adekvát választ biztosít. *Az élet, a lakosság védelme kiemelt prioritás,* az egy főre eső védelmi kiadás 2019-ben megközelítőleg 2257 dollár volt.[84] A rugalmas és megfelelő védelem biztosításának eszközei a rakétafenyegetéssel szemben a Vaskupola (Iron Dome) légvédelmi rendszer, a kibertér és elsősorban a közösségi médiafelületek esetében a különböző információs műveletek (INFOOPS), a terrorszervezetek infrastruktúrájának gyengítésére a célzott csapások, az állandó felderítés és hírszerzés, az UAV-ok alkalmazása és a pszichológiai műveletek (PSYOPS). Ezeken kívül globális szinten az aktív külpolitikai és diplomáciai tevékenység is hozzájárul a terrorizmus elleni küzdelemhez.

82 *The Facebook Intifada.* 2015. https://nationalpost.com/opinion/robert-fulford-the-facebook-intifada (Letöltés időpontja: 2020. 11. 07.)

83 *Israel's New Counter-Terrorism Law and Terrorism in Cyberspace.* 2016. https://www.cfr.org/blog/israels-new-counter-terrorism-law-and-terrorism-cyberspace (Letöltés időpontja: 2020. 11. 07.)

84 The International Institute for Strategic Studies*: The Military Balance 2020*, Routledge, 2020, 354.

A 2000-ben kirobbanó második palesztin intifáda eszközök és módszerek terén is hozott újdonságokat, az izraeli reakció azonban elsősorban a társadalmi biztonságpercepció átalakulását jelentette. A katonai műveletek ekkor még főként az 1960-70-es évek konfliktusai során szerezett tapasztalatokra épültek.

Az ezutáni időszakban azonban a terroristák által használt új eszközök, a nekik támogatást nyújtó államok magatartása és a nemzetközi közösség kritikusabb szemlélete miatt azonban az Izraeli Állam is új módszereket alkalmazott. *A hangsúly a nagyszabású katonai műveletek helyett egyre inkább a nemzetközi kapcsolatok, a jogi és a gazdasági dimenzió felé tolódott.* Ezen kívül a terrorcselekmények megelőzéséért a hírszerzés és az információmegosztás egyre nagyobb szerepet kapott, csakúgy, mint a modern hadiipari eszközök beszerzése és gyártása, amelyhez Izrael – lévén innovációs és technológiai nagyhatalom – jó adottságokkal rendelkezik.

A publikációban megvizsgált módszerek és stratégiai irányelvek alapján összegzem, hogy melyek azok a területek, amelyeken a terrorizmus által fenyegetett demokráciák tanulhatnak az izraeli példából.

Katonai szempontból az IDF által alkalmazott bevált taktikák közé *a megelőző csapások, az infrastruktúra meggyengítése, a vezető személyek elleni célzott támadások,* a határok fokozott ellenőrzése és a fejlett technológiák használata tartozik. A hadsereget támogató különleges egységek az Aman, YAMAM, Sayeret Matkal stb. A határok ellenőrzése mellett *a repülőterek és a légi közlekedés* kiemelt a biztonsági intézkedések tekintetében, mert köztudottan kedvelt célpontot jelentenek. Mind a határellenőrzés, mind a repülőterek fokozott biztonsági felügyelete és ellenőrzése követendő példa, hiszen a határokon átkelő terroristákra és repülőtéri terrortámadásra is volt már példa a közelmúltban Nyugat-Európában. Izraeli szakértők szerint Európában – éppen a határok viszonylag könnyű átjárhatósága miatt – nem országonként, hanem egy közösségként kellene szervezni és összehangolni a hírszerző tevékenységet.

Izrael esetében nagy hangsúly van a hírszerző és elemző tevékenységen. A Moszad és a Shin Bet, illetve a terrorizmus legyőzésére szakosodott speciális egységek prioritásként kezelik ezt a feladatot. Összehangolt tevékenységük és együttműködésük a terrortámadások meglőzése terén példaértékű. A katonai és gazdasági dimenzió határán említendő az ország technológiai fejlettsége és innovációs potenciálja, amely lehetővé teszi a „minőség a mennyiség felett" elv alkalmazását, ezáltal az ország modern hadiipari védelmi eszközökkel való felszerelhetőségét.

Társadalmi szempontból meghatározó, hogy *a biztonságpercepció átalakulásával az emberek hozzászoktak a folyamatos fenyegetettséghez, együttműködés jellemzi őket* a fegyveres erőkkel, melyet az is elősegít, hogy az izraeli állampolgároknak meghatározott ideig kötelező katonai szolgálatot kell teljesíteniük. A társadalom tudatos szembesítése a terrorizmus veszélyével azért is egyre fontosabb, mert a különböző közösségi média felületek használatával egyre könnyebb radikalizálódni, mely a „magányos farkas" elkövetők számának növekedéséhez vezethet.

Netanjahu a jövőre nézve négy pillért fogalmazott meg, amelyek által a terrorizmus legyőzhető. Első pillér *a katonai erő, amely az elrettentésből, valamint a defenzív és offenzív képességekből ered, a második pillér a gazdasági erő, amely a privát szektor bevonását és a globális gazdasági kapcsolatok erősítését jelenti, a harmadik pillér a politikai erő, mely a nemzetközi szövetségekben nyilvánul meg, illetve a negyedik szociális pillér, melynek központjában a társadalom tudatossága és ellenálló képessége áll. A sikeres küzdelem érdekében a négy pillér egyidejű alkalmazása szükséges.*[85]

85 *From Ben-Gurion to Netanyahu: The Evolution of Israel's National Security Strategy.* 2019. https://www.fdd.org/analysis/2019/05/13/from-ben-gurion-to-netanyahu-the-evolution-of-israels-national-security-strategy/ (Letöltés időpontja: 2020. 11. 11.)

6. Befejezés

A globális terrorizmus napjaink egyik legnagyobb biztonsági fenyegetéseként tartható számon, amely a 21. század során az eszközök, módszerek, célok és a szervezeti felépítés tekintetében olyan változásokon ment keresztül, amelyek következményeként már a terrorizmus új típusáról beszélhetünk. A tanulmány az izraeli példán keresztül mutatta be az új típusú terrorizmus elleni küzdelem lehetséges módját, amelynek bizonyos elemei más terrorfenyegetett országok esetében is alkalmazhatók lehetnek. Az izraeli terrorizmus elleni küzdelem legfőbb elemeiként a tanulmány kitekintett az ország fegyveres erejére, valamint a stratégiai szinten megfogalmazott legfőbb irányelvekre. A 21. század során Európa több országát is érte váratlanul és felkészületlenül sok áldozatot követelő terrortámadás, ezért a jövőre vonatkozóan javaslom a kutatás kiterjesztését Izrael és az Európai Unió terrorizmus elleni küzdelem terén való együttműködésének vizsgálatára.

Felhasznált irodalom

Békési Bertold et alii: *Pilóta nélküli repülés profiknak és amatőröknek.* Budapest, Nemzeti Közszolgálati Egyetem, 2013.

Brzezinski, Zbigniew: *A nagy sakktábla.* Budapest, Antall József Tudásközpont, 2017.

Byman, Daniel: *Curious Vistory: Explaining Israel's Suppression of the Second Intifada.* Terrorism and Political Violence, XXII. évf. 2012/5., 825–852.

Fregan Beatrix – Hronyecz Erika: *Új trendek a terrorizmusban? Rövid európai kitekintés.* Hadmérnök, IX. évf. 2014/4., 156–163.

Gazdag Ferenc – Remek Éva: *A biztonsági tanulmányok alapjai.* Budapest, Dialóg Campus, 2018.

Kis-Benedek József: *A Közel-Kelet katonai sajátosságai*. Külügyi Szemle, XII. évf. 2013/1., 79–99.

Kis-Benedek József: *A palesztin intifáda biztonságpolitikai és katonai összefüggései.* Felderítő Szemle, V. évf. 2006/2., 41–72.

Kis-Benedek József: *A palesztin-izraeli konfliktus*. Felderítő Szemle, I. évf. 2002/1., 61–85.

Kiss Álmos Péter: *Az izraeli integrált rakétavédelmi rendszer.* Honvédségi Szemle, 141. évf. 2013/5., 31–46.

Kovács Zoltán: *Az improvizált robbanóeszközök főbb típusai.* Műszaki Katonai Közlöny, XXII. évf. 2012/2., 37–52.

Marshall, Tim: *A földrajz fogságában.* Budapest, Park, 2019.

Netanyahu, Benjamin: *Fighting Terorrism. How Democracies Can Defeat the International Terrorist Network*. New York, Straus and Giroux, 2001.

Paragi Beáta*: Biztonsági percepciók Izraelben*. Nemzet és Biztonság, 2009/7., 61–78.

Rémai Dániel: *Az izraeli nemzetbiztonsági rendszer fejlődésének története*. Nemzetbiztonsági Szemle, 7. évf. 2019/ 4., 3–19.

Rémai Dániel: *Biztonsági kihívások hálójában, avagy az Izraeli Védelmi Erők esete az aszimmetrikus hadviseléssel.* Honvédségi Szemle, 148. évf. 2020/6., 16–31.

Resperger István: *Az iszlám világ és hatása a biztonságra.* Budapest, Egyetemi, 2003.

Schweitzer András: *Jeruzsálem nemzetközi státusa – politikai dokumentumok és értelmezések.* Külügyi Szemle, II. évf. 2003/1. 62–79.

Szabó Regina: *A palesztin – izraeli konfliktus története és a béke lehetősége a Szentföldön.* Nemzetbiztonsági Szemle, VII. évf. 2019/1., 66–84.

Szendy István: *Hadügy és hadviselés.* Budapest, Dialóg Campus, 2017.

The International Institute for Strategic Studies: *The Military Balance 2020*, Routledge, 2020.

Tomolya János: *A „34 napos" izraeli-libanoni háború.* Hadtudomány, XVII. évf. 2007/1., 1–23.

Internetes források

A critical analysis of Israel's counter-terrorism strategy. 2016. https://foreignpolicynews.org/2016/08/08/a-critical-analysis-of-israels-counter-terorrism-strategy/

A Gázai övezet története. 2012. https://web.archive.org/web/20121120052902/http://www.tortenelemklub.com/xxszazad/1990-utan/938-a-gazai-oevezet-toertenete

About Hezbollah. https://hezbollah.org/about-hezbollah

Al-Aqsa Martyrs' Brigade. https://mackenzieinstitute.com/terrorism-profile-al-aqsa-martyrs-brigade-aamb/

Dicter, Avi – Byman, Daniel L.: *Israel's Lessons for Fighting Terrorists and Their Implications fot the United States.* 2016. https://www.brookings.edu/wp-content/uploads/2016/06/byman20060324.pdf

Eiland, Giora: *Defensible Borders ont he Golan Heights.* 2009. http://www.jcpa.org/text/DefensibleBorders-GolanHeights.pdf

From Ben-Gurion to Netanyahu: The Evolution of Israel's National Security Strategy. 2019. https://www.fdd.org/analysis/2019/05/13/from-ben-gurion-to-netanyahu-the-evolution-of-israels-national-security-strategy/

Hamas' Military Wing. https://www.idf.il/en/minisites/hamas/hamas/hamas-military-wing/

Hezbollah. https://cisac.fsi.stanford.edu/mappingmilitants/profiles/hezbollah#text_block_18070

Humanitárius jog a gyakorlatban. http://juris.oldportal.u-szeged.hu/download.php?docID=38511

IDF appoints general to lead new Iran Command as threat escalates. https://www.jpost.com/israel-news/idf-appoints-general-to-head-up-new-iran-command-as-threat-escalates-617507

Institute for Economics and Peace: *Global Terrorism Index 2014.* https://reliefweb.int/sites/reliefweb.int/files/resources/Global%20Terrorism%20Index%20Report%202014.pdf

Institute for Economics and Peace: *Global Terrorism Index 2019.* http://visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf

Israel–Military Expenditure. https://tradingeconomics.com/israel/military-expenditure-percent-of-gdp-wb-data.html

Israel and Hamas said to reach agreement for 6-month ceasefire. https://www.timesofisrael.com/israel-and-hamas-said-to-reach-agreement-for-6-month-ceasefire/

Israel's New Counter-Terrorism Law and Terrorism in Cyberspace. https://www.cfr.org/blog/israels-new-counter-terrorism-law-and-terrorism-cyberspace

Israeli-Palestinian Fatalities Since 2000 – Key Trends. https://unispal.un.org/DPA/DPR/unispal.nsf/0/BE07C80CDA4579468525734800500272

Izrael-Gázai övezet: életbe lépett a tűzszünet. 2019. https://hu.euronews.com/2019/11/14/izrael-gazai-ovezet-eletbe-lepett-a-tuzszunet

Izraeli Védelmi Erők. https://embassies.gov.il/budapest/AboutIsrael/State/Pages/Izraeli-Védelmi-Erők.aspx

Meridor, Dan – Eldadi, Ron*: Israel's National Security Dotrine: The Report of the Committee in the Formulation of the National Security Doctrine (Meridor Committee), Ten Years Later.* 2019. https://www.inss.org.il/wp-content/uploads/2019/02/Memo187_11.pdf

Mossad, realities and myths of Israel's national intelligence service. https://www.nimmonsconsulting.com/mossad-mythology-reality/

Nagy Levente Balázs: *A második intifáda kitörése és első másfél éve.* 2002. http://www.europeer.hu/tanulmany/nagy_masodikintifada2002.pdf

Palestinian Islamic Jihad. https://www.counterextremism.com/threat/palestinian-islamic-jihad

Raz, Eyal – Stein, Yael: *Operation Defensive Shield.* 2002. https://www.btselem.org/download/200207_defensive_shield_eng.pdf

Tálas Péter: *A nemzetközi terrorizmus és a szervezett bűnözés hatása a nemzetközi biztonságra és Magyarország biztonságára.* https://kisebbsegkutato.tk.mta.hu/uploads/files/archive/904.pdf

The consequences of Israel's counter terrorism policy. https://research-repository.st-andrews.ac.uk/bitstream/handle/10023/439/Pia%20Jansen%20PhD%20thesis.pdf?sequence=6&isAllowed=y

The Facebook Intifada. https://nationalpost.com/opinion/robert-fulford-the-facebook-intifada

The World Factbook: *Israel*. https://www.cia.gov/the-world-factbook/countries/israel/

Trophy Active Protection System for AFVs. https://www.rafael.co.il/worlds/land/trophy-aps/

Trump says US recognises Jerusalem: The speech in full. https://www.bbc.com/news/world-middle-east-42264868

UN Peacekeepers investigating flareup on Israel-Lebanon border. https://www.timesofisrael.com/un-peacekeepers-investigating-flareup-on-israel-lebanon-border/

Vinson, Mark: *An Israeli Approach to Deterring Terrorism.* https://cco.ndu.edu/Portals/96/Documents/prism/prism_5-3/An_Israeli_Approach_to_Deterring_Terrorism.pdf

Szőke Ágoston

Az informatikai szektor – Észtország esete

1. Bevezetés

A szektoriális biztonságfelfogás egyik új és gyorsan fejlődő szektora az informatikai szektor. Magyarország 2020-as Nemzeti Biztonsági Stratégiája szerint *„az információs technológia rohamos fejlődéséből és terjedéséből kifolyólag az állam és a társadalom működése egyre inkább a digitalizációra épül.”*[1] A digitalizációban Észtország élen jár. Ezt támasztja alá az, hogy az ország az uniós Digitális Gazdaság és Társadalom Index rangsorban 2019-ben a nyolcadik helyet foglalta el,[2] illetve 2007-ben elsőként alkalmazott online szavazást parlamenti választáskor.[3] A digitalizációnak azonban biztonsági vonatkozásai is vannak. Erre mutattak rá például az Észtország elleni 2007-es kibertámadások. A kiberbiztonság kérdéskörét Észtország nemzetközi szinten is napirenden tartja. 2020 májusában például Észtország töltötte be az ENSZ Biztonsági Tanács elnökségét, és ekkor az ország célkitűzései között szerepelt a kiberfenyegetések napirendre vétele a Tanácsban.[4]

Észtország digitalizációjáról és az ezzel kapcsolatos biztonsági kihívásokról szóló szakirodalom meglehetősen szerteágazó, és az ilyen jellegű kutatások sokszor csak egy konkrét eseményre (pl. a 2007-es kibertámadásra) vagy egy jól körülhatárolható témára (pl. az i-szavazásra) koncentrálnak. Ezen tanulmány kiindulópontját Lene Hansen és Helen Nissenbaum cikke[5] jelenti. A cikkben a kiberbiztonság önálló szektorként jelenik meg, és az így létrejött elméleti keret esettanulmány formájában az Észtország elleni 2007-es kibertámadásokon keresztül kerül bemutatásra. A 2007-es eseményeket feldolgozó szakirodalomból kiemelendő Eneken Tikk és munkatársai elemzése.[6] Észtország digitalizációjáról komparatív elemzés formájában átfogó képet ad Maarit Ströbele és munkatársai tanulmánya.[7] A balti országokban élő oroszajkú lakosok közösségi média használatáról végzetek részletes kutatást Dmitri Teperik és munkatársai.[8] Az Észtország digitalizációját vizsgáló kutatások a biztonsági aspektust többnyire nem érintik. Azok a kutatások, amik a digitalizáció biztonsági vonatkozásait vizsgálják általában egy konkrét eseményt, vagy témát vizsgálnak. Ez a tanulmány az észt digitalizáció biztonsági aspektusát átfogóan kívánja vizsgálni.

A tanulmány célja az informatikai szektor vizsgálata Észtország esetében. Ennek eléréséhez két kutatási kérdést fogalmaztam meg:

1 1163/2020. (IV.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. 70. pont.

2 *Digital Economy and Society Index (DESI) 2019 - Country Report – Estonia.* European Commission, 2019. 3. Elérhető: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59894 (A letöltés dátuma: 2021. 03. 06.)

3 *How did Estonia become a leader in technology?* The Economist, 2013. Elérhető: https://www.economist.com/the-economist-explains/2013/07/30/how-did-estonia-become-a-leader-in-technology (A letöltés dátuma: 2021. 03. 06.)

4 *Estonia's presidency in UN Security Council.* Elérhető: https://un.mfa.ee/estonias-presidency-in-un-security-council/ (A letöltés dátuma: 2021. 03. 06.)

5 Lene Hansen – Helen Nissenbaum: Digital Disaster, Cyber Security, and the Copenhagen School, *International Studies Quarterly*, 53. (2009), 4. 1155-1175. DOI: https://doi.org/10.1111/j.1468-2478.2009.00572.x

6 Eneken Tikk – Kadri Kaska – Liis Vihul: *Interantional cyber incidents – Legal considerations*. Tallinn, NATO CCD COE, 2010. Elérhető: https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf (A letöltés dátuma: 2021. 03. 06.)

7 Maarit Ströbele – Nele Leosk – Alexander H. Trechsel: *Two Countries / Two Decades / Two Outcomes – A brief comparison of e-government solutions in Estonia and Switzerland.* Zurich, xUpery, 2017. Elérhető: https://xupery.com/wp-content/uploads/2017/08/A-brief-comparison-of-e-government-solutions-in-Estonia-and-Switzerland.pdf (A letöltés dátuma: 2021. 03. 06.)

8 Dmitri Teperik et alii: *Virtual Russian World in the Baltics*. Elérhető: https://www.stratcomcoe.org/virtual-russian-world-baltics (A letöltés dátuma: 2021. 03. 06.)

a. Az észt állami szolgáltatások[9] nagy mértékű digitalizáltsága milyen speciális biztonsági kihívásokat jelent?
b. Az oroszajkú lakosság jelenléte Észtországban hogyan befolyásolja az informatikai szektort?

A tanulmány az elméleti háttér felvázolása mellett a kutatási kérdések mentén két fő részre tagolódik. Az első rész röviden bemutatja e-Észtország jellemzőit és biztonsági kihívásait. A második rész az informatikai és a társadalmi szektor kapcsolódási pontjait tárja fel. Itt kerülnek bemutatásra az Észtország elleni 2007-es kibertámadások eseményei és a közösségi médiában végbemenő befolyásolási kísérletek. Az eredmények szekunder források és hírek elemzésén alapulnak.

2. Elméleti megfontolások

Az informatikai szektor eredetileg nem szerepelt a szektoriális biztonságfelfogást megalapozó *Biztonság* című könyvben, melyben a kiberbiztonságot olyan területként tüntették fel, mint ami ellenpéldája a sikeres biztonságiasításnak, mivel a hekkerek akciói nem vezetnének kaszkádeffektushoz.[10] A könyv 1998-as kiadása óta a kiberbiztonság értékelése megváltozott. Erre reflektált Hansen[11] és Nissenbaum, amikor a biztonságiasítás keretrendszerét felhasználva a kiberbiztonságot, mint egy elkülönült szektort határozták meg.[12] Úgy gondolták, hogy a számítógépes rendszereken végrehajtott támadások vezethetnek kaszkádeffektushoz, azaz a támadások nemcsak a hálózat, hanem azon túl más referens tárgyak (pl. társadalom, gazdaság) számára is járhatnak következményekkel.[13] Terminológiai szempontból megjegyzendő, hogy amíg Hansen és Nissenbaum a kiberbiztonsági szektor, addig Gazdag Ferenc és Remek Éva könyvükben[14] az informatikai szektor kifejezést használják. A kiberbiztonság[15] fogalma mást takar, mint az informatika fogalma (igaz, van köztük kapcsolat), így valószínűleg találóbb lenne kiberbiztonsági szektorról beszélni. Ennek a tanulmánynak azonban nem az a célja, hogy ezt a kérdést tisztázza, így az informatikai szektor megnevezés kerül használatra.

A Barry Buzan-féle biztonságfelfogás diszkurzív megközelítést alkalmaz,[16] így egy konstruktivista elméletről van szó, ami a biztonságiasítást egy interszubjektív és társadalmilag konstruált jelenségként határozza meg.[17] A diszkurzushoz kötöttség ellenére a biztonságiasítás nemcsak ad hoc, hanem intézményesített is lehet folyamatos, vagy visszatérő fenyegetések esetén.[18] A szektoroknak megvan a maguk grammatikája. Hansenék az informatikai szektor esetében a hiperbiztonságiasítást, a mindennapos biztonsági gyakorlatot és a technifikációt jelölték meg, mint sajátos nyelvhasználatot.[19] Ezek a grammatikák segítenek majd leírni bizonyos folyamatokat.

9 Az e-estonia.com oldalon a (digital) state service kifejezést használják. Ezt fordítottam állami (e-) szolgáltatásra. Alapvetően itt e-szolgáltatásokról és az azokat kiszolgáló infrastruktúráról van szó. Az állami jelzőt azért is tettem hozzá, mert az e-szolgáltatások általában állami keretben (ld. eID), kormányzati programok hatására jöttek létre és működnek. A terminológiai bizonytalanság miatt a tanulmányban leggyakrabban egyszerűen az e-szolgáltatások kifejezést használom.
10 Barry Buzan – Ole Wæver – Jaap de Wilde: *Security – A New Framework For Analysis*. London, Lynne Rienner Publishers, 1998. 25.
11 Hansen neve megjelenik a *Biztonság* létrejöttét segítők nevei között. Forrás: Buzan–Wæver–Wilde (1998) i. m. (11. lj.) viii.
12 Hansen–Nissenbaum (2009) i. m. (6. lj.) 1155.
13 Uo. 1163.
14 Gazdag Ferenc – Remek Éva: *A biztonsági tanulmányok alapjai*. Budapest, Dialóg Campus, 2018. 24.
15 A kiberbiztonság fogalmához ld. Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018. 18.
16 Hansen–Nissenbaum (2009) i. m. (6. lj.) 1156.
17 Buzan–Wæver–Wilde (1998) i. m. (11. lj.) 31.
18 Uo. 27.
19 Hansen–Nissenbaum (2009) i. m. (6. lj.) 1163-1166. – A fogalmak a későbbiekben kerülnek meghatározásra.

3. E-Észtország kialakulása, alapjai és biztonsági kihívásai

Az első kutatási kérdés arra keresi a választ, hogy az észt állami szolgáltatások nagy mértékű digitalizáltsága milyen speciális biztonsági kihívásokat jelent. Ennek körüljárásához első lépésként e-Észtország[20] kialakulásának és működésének a vizsgálata szükséges. Az e-Észtország kifejezéssel Észtország fejlett e-társadalommá válását fejezik ki.[21] Egyúttal a kifejezés a digitalizált Észtország „brandjét" is jelöli. Látható, hogy az e-Észtország kifejezés mögöttes tartalmát nehéz pontosan körülhatárolni. Azonban szerintem maga a kifejezés a tanulmányban hasznosítható. E-Észtország alatt a tanulmányban elsősorban a különböző észt állami e-szolgáltatások rendszerét és az ezt kiszolgáló infrastruktúrát fogom érteni.

Az 1991-es Szovjetuniótól való függetlenedést követően a „Tigrisugrás"[22] program jelentette az első komolyabb lépést a digitalizáció felé. Az 1996-ban elindított, kormányzati támogatásból megvalósuló program az iskolák internethez való csatlakoztatását és a technológia oktatásba való bevonását tűzte ki célul.[23] Az e-Észtország alappilléreit jelentő X-út[24] és az elektronikus személyazonosság[25] létrehozására a 2000-es évek elején került sor.

3.1 E-Észtország alapjait jelentő technológiák és a rájuk épülő szolgáltatások

Az X-út e-Észtország egyik alappillére. Az X-út biztonságos internetalapú adatcserét tesz lehetővé az állam informatikai rendszerei között.[26] A rendszert a nemzeti adatbázisok standardizálásának szükségessége és az erőforrások szűkössége hívta életre. Az X-utat 2001 végén állították üzembe és azóta egyszer sem állt le. A rajta lévő szolgáltatásokat magánvállalatok és egyének is elérhetik. A rendszer előnye, hogy naprakész adatokat képes szolgáltatni elektronikus úton, így például az online adóbevallásnál nincs szükség külön űrlapok kitöltésére, mert a releváns adatokat a rendszer képes a népességnyilvántartási rendszerből lekérdezni.[27] 2021. február 1-jén 598 vállalat, illetve 164 közszférában működő intézmény használta az X-utat, amin ekkor 2918 szolgáltatás volt elérhető. 2020-ban közel 1,6 milliárd lekérdezés történt a rendszerben.[28]

Az X-út mellett e-Észtország másik alappillére az elektronikus személyazonosság (eID). Az eID olyan adatkollekció, ami egy személyt az elektronikus környezetben összekapcsol a fizikai személyazonosságával. Ezt az adatkollekciót, amiből az eID létrejön többféle eszköz hordozhatja: személyazonosító igazolvány, tartózkodási kártya, diplomata személyazonosító igazolvány, Mobil-ID, Digi-ID és a Smart ID (részletesen ld. 1. táblázat).[29]

---

20 Angolul e-Estonia. A kifejezés nemzetközi „brandként" való használatát jól mutatja, hogy külön hivatalos honlapot hoztak létre ezzel a névvel az e-estonia.com címen.

21 Sandra Roosna – Raul Rikk: *e-ESTONIA – e-Governance in Practice*. 2016. 6. Elérhető: https://ega.ee/wp-content/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf (A letöltés dátuma: 2021. 03. 06.)

22 Tiger Leap.

23 Ströbele–Leosk–Trechsel (2017) i. m. (8. lj.) 6–8.

24 Az X-út észt és angol elnevezése az X-tee. A tee magyarul utat jelent. Korábban angolul X-Roadnak nevezték, de 2018 óta ez magára a technológiára utal, és az észt rendszert már angolul is X-teenek nevezik Forrás: *Data Exchange Layer X-tee.* 2020. Elérhető: https://www.ria.ee/en/state-information-system/x-tee.html (A letöltés dátuma: 2021. 03. 06.)

25 Az angol megnevezése Electronic Identity. A kifejezés bevett rövidítése az eID. Ld. *The 2020 yearbook of the Information System Authority.* Information System Authority. 8. Elérhető: https://www.ria.ee/sites/default/files/content-editors/ria_aastaraamat_2020_48lk_eng.pdf (A letöltés dátuma: 2021. 03. 06.)

26 *X-Road factsheet.* Elérhető: https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/x-road-factsheet-2014.pdf (A letöltés dátuma: 2021. 03. 06.)

27 Ströbele–Leosk–Trechsel (2017) i. m. (8. lj.) 8–9.

28 *X-tee factsheet.* Elérhető: https://www.x-tee.ee/factsheets/EE/#eng (A letöltés dátuma: 2021. 03. 06.)

29 *Electronic Identity eID.* Elérhető: https://www.ria.ee/en/state-information-system/electronic-identity-eid.html (A letöltés dátuma: 2021. 03. 06.)

1. táblázat: Az eID-t hordozó eszközök különböző típusai, forrás: a szerző szerkesztése

Angol elnevezés (bevezetés éve)[30]	**Lehetséges magyar elnevezés**[31]	**Tulajdonságok**	**Aktív hordozók száma (2020)**[32]
ID-card (2002)[33]	Személyazonosító igazolvány	Kötelező személyazonosító dokumentum. Észt állampolgároknak, illetve az Észtországban lakó uniós állampolgároknak adják ki.[34]	~1,3 millió kártya – ebből 930 ezret használnak elektronikusan.
Residence (permit) card (n.a.)	Tartózkodási kártya	Kötelező személyazonosító dokumentum helyi használatra. Azok a külföldiek kapják, akik nem uniós állampolgárok, de tartózkodási (lakhatási) engedéllyel vagy joggal vannak Észtországban.[35]	Pontos adat nem állt rendelkezésre, de a fő eID hordozókhoz képest (személyazonosító igazolvány, Mobil-ID, Smart-ID) kis részesedéssel bírnak.
Digi-ID (n.a.)	Digitális személyazonosító kártya	Az állam által kiadott digitális dokumentum. Használata az online térre korlátozódik. Személyek vizuális azonosítása nem lehetséges vele (sem fotó, sem biztonsági elemek nincsenek rajta). Egyébként megegyezik a személyazonosító igazolvánnyal, az online környezetben egyenrangúak. Kiváltásához személyazonosító igazolványra vagy tartózkodási kártyára van szükség.[36]	
Diplomatic (digital) ID (2017)[37]	(Digitális) diplomata személyazonosító igazolvány	Lehetővé teszi a tulajdonos elektronikus és (a Digi-ID-val ellentétben) fizikai azonosítását. Hozzáférést biztosít az e-szolgáltatásokhoz.[38] Észtországban lévő diplomáciai, konzuli képviseletek tagjai, vagy az ott dolgozók kaphatják.[39]	
E-Resident's digital ID (2014)[40]	E-lakos digitális személyazonosító kártyája	Az e-lakos programban részt vevő, nem Észtországban lakó külföldiek digitális személyazonosító kártyája. Használata az online térre korlátozódik. Gyakorlatilag egy Digi-ID, de a kiváltás alapfeltételei miatt érdemes külön kezelni.[41]	66 ezer
Mobile-ID (2007)[42]	Mobil-ID	Elektronikus személyazonosítási dokumentum, amit elektronikus azonosításra és digitális aláírásra lehet használni mobiltelefonon keresztül. Használatához speciális SIM kártyára, igényléséhez személyazonosító igazolványra van szükség.[43]	234 ezer
Smart-ID (2017)[44]	Smart-ID	Elektronikus azonosítási szolgáltatás. Használatához a Smart-ID mobilapplikációra van szükség, valamint rendelkezni kell személyi azonosító számmal. A többi megoldástól eltérően ezt az azonosítási megoldást egy magáncég, az SK ID Solutions AS nyújtja.[45]	501 ezer

30 Roosna–Rikk (2016) i. m. (22. lj.) 48–50;

31 A kártyáknak nem találtam hivatalos magyar fordítását. A szövegben frekventáltan a személyazonosító igazolvány (az észt dokumentum megfeleltethető a magyarnak), a Mobil-ID (angolhoz nagyon hasonló a magyar fordítás) és a Digi-ID fordulnak elő. A Digi-ID-hoz nincs hasonló magyar dokumentum, így a fordítása félrevezető lehet, ezért maradtam az angol elnevezésnél. A Smart-ID-t nem fordítottam le, mert ez észtül is Smart-ID. A többi kártya nem kap hangsúlyos szerepet a szövegben, ezért fordításuk csak tájékoztató jellegű.

32 The 2020 yearbook… i. m. (26. lj.) 5, 9.

33 Roosna–Rikk (2016) i. m. (22. lj.) 48. Az eID funkcionalitással bíró változat bevezetésének ideje.

34 *ID-card – Intro*duction. Elérhető: https://www.id.ee/en/rubriik/introduction/ (A letöltés dátuma: 2021. 03. 07.)

35 Residence per*mit card for an adult*. Elérhető: https://www.politsei.ee/en/instructions/residence-permit-card-for-an-adult (A letöltés dátuma: 2021. 03. 07.)

36 *Digital ID.* Elérhető: https://www.politsei.ee/en/instructions/digital-id (A letöltés dátuma: 2021. 03. 07.); Roosna–Rikk (2016) i. m. (22. lj.) 48.

37 *Estonian eID scheme: diplomatic identity card.* Police and Border Guard Board, 2018. 4. Elérhető: https://ec.europa.eu/cefdigital/wiki/download/attachments/62885749/EE%20eID%20LoA%20mapping%20-%20diplomatic%20identity%20card.pdf?-version=1&modificationDate=1531759815709&api=v2 (A letöltés dátuma: 2021. 03. 07.)

38 Ali Vahtla*: Employees of foreign embassies to be issued digital IDs.* 2017. Elérhető: https://news.err.ee/588887/employees-of-foreign-embassies-to-be-issued-digital-ids (A letöltés dátuma: 2021. 03. 07.)

39 Estonian eID scheme… (2018) i. m. (38. lj.) 4.

40 Roosna–Rikk (2016) i. m. (22. lj.) 7.

41 *E-Resident's digital ID.* Elérhető: https://www.politsei.ee/en/instructions/e-resident-s-digital-id (A letöltés dátuma: 2021. 03. 07.)

42 Roosna–Rikk (2016) i. m. (22. lj.)50.

43 *Means of eID.* Elérhető: https://www.ria.ee/en/state-information-system/electronic-identity-eid/means-eid.html (A letöltés dátuma: 2021. 03. 07.); Roosna–Rikk (2016) i. m. (22. lj.) 50.

44 *The 2020 ye*arbook… i. m. (26. lj.) 10.

45 *About Smart-ID.* Elérhető: https://www.smart-id.com/about-smart-id/ (A letöltés dátuma: 2021. 03. 07.)

Az eID felfogható egy átfogó rendszerként, ami lehetővé teszi az elektronikus azonosítást, az elektronikus hitelesítést és a digitális aláírást. A digitális azonosításhoz és a digitális aláíráshoz rendelkezni kell csippel ellátott eID hordozóval. Az első eID funkcionalitással ellátott személyazonosító igazolványok 2002-ben jelentek meg és 2006-ra cserélték le a korábbi személyazonosító igazolványokat. Elektronikus használatuk azonban csak a 2010-es évek elejétől kezdett el növekedni. Ez részben valószínűleg annak a hatására történt, hogy a nagyobb bankok ekkor kezdték el ügyfeleiket a saját authentikációs megoldásaiktól az eID felé terelni.

2020-ban közel 1,3 millió aktív személyazonosító igazolvány, 501 ezer Smart-ID és 234 ezer Mobil-ID volt használatban. A személyazonosító igazolvánnyal rendelkezők közel kétharada rendszeresen használja azt elektronikusan, például digitális aláírásra. A személyazonoító igazolvány és a Mobil-ID segítségével 2015-ben 66 millió digitális aláírásra került sor. Ez az adat egy 1,3 milliós lakosságú országban figyelemre méltó. Az eID nélkül számos állami szolgáltatás nehezen érhető el, ami elősegíti a használatát. Az eID tehát mára központi szerepet tölt be az online azonosításban.

Az X-útra és az eID-ra számos szolgáltatás épül. Ilyen például az e-adóbevallás, az e-iskola, az e-kabinet, az e-egészség, az e-bankolás, az e-adó és az i-szavazás. Ezek egy része már a kormányzat által kiadott eID funkcionalitással bíró személyazonosító igazolványok megjelenése előtt is elérhető volt. Ez összefügg azzal, hogy a privátszféra, és ezen belül is a nagyobb bankok élen jártak az online ügyintézésben. Az internetes bankolás Kitsing szerint jobban hozzájárult az állami e-szolgáltatások elterjedéséhez, mint az eID funkcionalitással bíró személyazonosító igazolványok. Az e-adóbevallás 2000-ben indult el (tehát az eID funkcionalitással bíró személyazonosító igazolványok kiadása előtt), és kezdetben a felületet online banki azonosításon keresztül lehetett elérni. A bankokon keresztül elérhető szolgáltatásokhoz képest az állami e-szolgáltatásokat valószínűleg kisebb gyakorisággal használják, de ez nem feltétlen jelenti azt, hogy megbízhatóságuk kevésbé volna fontos. Állami e-szolgáltatásként említhető a 2008-ban indított e-egészség szolgáltatás, melynek segítségével egy integrált rendszerben vannak a lakosok egészségügyi adatai (diagnózisok, gyógyszerek stb.), és ezeket az eID segítségével az állampolgárok is elérhetik. A 2005-ben bevezetett i-szavazás lehetővé teszi az állampolgároknak, hogy az eID segítségével online adják le a voksukat. Az e-egészség és az i-szavazás jellegük miatt talán jó példák arra, hogy miért fontos az e-szolgáltatások biztonsága. Az e-egészség érzékeny adatokat kezel, az i-szavazás pedig a demokratikus folyamatokban játszik mára kiemelkedő szerepet.

Az elmúlt években jött létre Észtország első adatnagykövetsége , ami alapesetben nem tartozik e-Észtország alappillérei közé, de különleges helyzetben fontos szerepet tölthet be. 2013-ban az „Adatnagykövetség Kezdeményezés" célul tűzte ki a digitális folytonosság biztosítását. Ennek három eleme volt: adatközpontok létrehozása Észtországban; nem érzékeny adatbázisok nemzetközi felhőszolgáltatókba történő feltöltése; érzékeny adatok adatnagykövetségekbe történő biztonsági másolása. Az adatnagykövetségek létrehozását valószínűleg az motiválta, hogy Észtországot érő kibertámadások, vagy Észtország területi épségének sérülése esetén is tovább tudjon működni az állam. Az első adatnagykövetség létrehozásáról szóló kétoldalú megállapodást Észtország Luxembourggal írta alá 2017. június 20-án. A megállapodás sajátos, nemzetközi jogilag új helyzetet teremt, de az adatnagykövetség sok tekintetben a diplomáciai kapcsolatokról szóló 1961. évi bécsi szerződésben meghatározottakhoz hasonló privilégiumokkal és immunitással bír. Észtország így megfelelő módon képes ellenőrzést gyakorolni az adatnagykövetség felett. Az ellenőrzés nem megfelelő foka miatt nem egy magán felhőszolgáltató mellett döntöttek, bár a Microsoft szolgáltatását tesztelték korábban. Egyelőre tíz stratégiai adatbázis került kiválasztásra (ebből az első négyet 2019 júniusában küldték át), melyek egy részét valós időben, más részüket pedig rendszeresen fogják menteni az adatnagykövetségbe.

3.2 E-Észtország biztonsági kihívásai

A digitalizáció már önmagában is számos biztonsági kihívást vet fel, így e-Észtország esetében a „rendszerből adódó" (többnyire speciális) kihívások egy része kerül bemutatásra. Az egyik ilyen, kevésbé speciális kihívást jelenti a rendszer elérhetetlenné válása. Erre példa a 2007-es kibertámadás, ami később kerül részletezésre. Kihívást jelenthet továbbá, ha a rendszer alappilléreiben, így az X-útban és az eID-ban nehezen kezelhető sérülékenységet fedeznek fel. A különböző e-szolgáltatások kapcsán több kihívás is felmerülhet, itt az i-szavazás kerül csak említésre.

Az X-út és az eID e-Észtország alappillérei, így biztonságuk kiemelten fontos. Az X-út egy 2017-es elemzés szerint 2001 óta egyszer sem volt elérhetetlen. Egy, a Tallinni Műszaki Egyetemen írt szakdolgozat nem talált konkrét sérülékenységet a rendszerben, ugyanakkor rámutatott arra, hogy a hálózat kis mértékben automatizált, így az azt működtető emberek social engineering technikával történő befolyásolása reális veszély lehet. Az eID esetében volt már példa komolyabb potenciális sérülékenység feltárására. A sérülékenységről a Riigi Infosüsteemi Ametet (RIA-t) 2017. augusztus 31-én értesítette egy kutató a cseh Masaryk Egyetemről. A ROCA-ként elnevezett sérülékenység az Infineon által gyártott csipek RSA kulcspár generálását érintette. Ilyen csipeket használt több észt eID hordozó kártya (a személyazonosító igazolvány és a Digi-ID), így a sérülékenységből adódóan elméletileg az elvártnál kisebb számítási kapacitással is lehetővé vált egy eID kártya RSA privát kulcsának kiszámítása az RSA nyilvános kulcs ismeretében. Ez lehetővé tette volna a kártya birtoklása nélkül a kártyatulajdonos nevében például dokumentumok aláírását vagy az online hitelesítést. A sérülékenység a kiadott kártyák kétharmadát, azaz 750 ezer eID funkcionalitással bíró, 2014 őszét követően kiadott kártyát érintett, így egy széleskörű, az állampolgárok nagy részét érintő problémáról volt szó.

A probléma kezelését – miniszterelnöki szintű egyeztetéseket követően – a RIA koordinálta. Egy másik kriptográfiai megoldást került kiválasztásra. Az új kártyák 2017. október végétől ezzel a megoldással kerültek kiadásra, a sérülékenységgel érintett kártyáknál viszont a kártyatulajdonosoknak vagy személyesen a hatóságnál, vagy távolról, például az otthoni számítógéppel frissíteni kellett a kártya szoftverét. Erre azért is volt szükség, mert a sérülékeny kártyákon a tanúsítványokat 2017. november 3-án felfüggesztették, így csak frissítést követően váltak újra használhatóvá. 2018. március 31-ig közel 500 ezer kártyát frissítettek, ebből 354 ezret távolról. Az e-szolgáltatások használatában nem volt tapasztalható visszaesés. A probléma sikeres kezeléséhez az érintett állampolgárok együttműködésére is szükség volt. Hansenék szerint az informatikai szektorra jellemző egyik grammatikának, a mindennapos biztonsági gyakorlatnak pont az a célja, hogy az egyén partner legyen a hálózat biztonságának megóvásában. Az észt kormány transzparensen igyekezett kezelni a kérdést, már 2017. szeptember 5-én felhívták a közvélemény figyelmét a sérülékenységre. Más országban is okozott problémát a sérülékenység. Szlovákiában 60 ezer, Spanyolországban 17 millió kártyát vontak vissza 2017 őszén, igaz ezekben az országokban a kártyákat kevésbé használták. Az állampolgárok együttműködésén túl fontos volt a kártyák melletti alternatív megoldások, azaz a Mobil-ID és a Smart-ID megléte (ezeket nem érintette a sérülékenység). A Mobil-ID-t és a Smart-ID-t a sérülékenység felfedezésekor kevesen használták (pl. a Mobil-ID-t 100 ezren), így ezekkel nem lehetett volna teljesen kiváltani a kártyákat.

Az észt válságkezelés végeredményét tekintve sikeres volt. A válságból több tanulság is levonható: a válság megoldásához szükséges kompetenciák jórésze a magánszektorban található, ezért fontos a köz- és magánszektor partnersége; nyitott és rugalmas architektúrákra van szükség (ld. kártyák távoli frissítésének lehetősége), mivel a globális vállalatok egy nagymértékű sérülékenység esetén saját üzleti kockázatértékelésüket

tartják szem előtt (az érintett állam csak egy a sok ügyfél között); a jelenlegi válságkezelési eljárások a hatás bekövetkezését követő reagálásra fókuszálnak, ezért olyan eljárásokat is ki kell dolgozni, amik a hatás bekövetkezését igyekszenek elkerülni (elméleti kockázatra reagálnak). A probléma azonban rámutatott arra, hogy komoly biztonsági kihívást jelenthet az, ha az e-Észtország egyik alappillérét jelentő eID egyes hordozóiban sérülékenység kerül feltárásra, főleg, ha ezen hordozókat sokan használják, és kevés alternatívájuk van.

Az e-ID-ra épülve Észtországban az interneten keresztüli szavazás is lehetséges. Először a 2005-ös helyi önkormányzati választásokon lehetett így szavazni. Akkor a szavazatok közel 2%-a lett online leadva. Ez az arány azóta folyamatosan nőtt. A 2011-es parlamenti választáson a választók 24,3%-a, a 2019-esen pedig már 43,8%-a adta le az internet keresztül a voksát. Az i-szavazás tehát mára központi szerepet tölt be az észt választási eljárásban. A szavazatok internetes leadása személyazonosító igazolvány, vagy Mobil-ID használatával lehetséges a papír alapú szavazás napját megelőzően. Az online leadott szavazatok több lépcsőben, központilag kerülnek feldolgozásra. A szavazatok számlálása egy, az internetre nem csatlakozó szerveren történik.

Az i-szavazás biztonsága a választási eljárásban játszott központi szerepe miatt egy fontos kérdés. Az ezzel foglalkozó elemzések főként technológiai és eljárásbeli sérülékenységekre mutattak rá. A technológiai sérülékenységek közé sorolhatóak a választók által a szavazat leadására használt eszközök biztonsági problémái, vagy a szervereken használt kódban található sérülékenységek. Az i-szavazás során alkalmazott eljárások alapvető fontosságúak annak biztonsága szempontjából (az eljárásokra egyelőre jobban alapoznak, mint a technológiai biztonsági megoldásokra, a jövőben azonban egyre nagyobb szerepet kaphat a technológia). Két elemzés is rámutatott arra, hogy egyrészt az eljárások egy része kis mértékben formalizált (illetve ha az is, akkor egyes problémák megoldása az eljárásrendtől eltérően, ad hoc módon történik), másrészt a szavazatok feldolgozására alkalmazott eszközök konfigurálásakor, illetve a dolgozók személyes eszközeinek a választási eljárásban történő használatát illetően is adódhatnak hiányosságok. Egy, a technológiai és eljárásbeli sérülékenységeket figyelembe vevő 2014-es kutatás arra jutott, hogy ezen sérülékenységek potenciálisan veszélyeztetik a választások integritását. A kutatók azt javasolták, hogy Észtország ne használja tovább az i-szavazást. A észt Nemzeti Választási Bizottság vitatta a kutatás megállapításait, jelezve, hogy a jelzett támadási módokkal számoltak, és hogy ezen támadások hatékony kivitelezése nem lehetséges. Megfigyelők szerint az eddigi választások szabadok és tiszták voltak, illetve nem volt tapasztalható beavatkozás. Az i-szavazás biztonságának további alakulása figyelemmel kísérendő terület, főleg úgy, hogy Hollandiában 2017-ben még a szavazatok elektronikus úton történő számlálását is elhagyták a választás biztonságának biztosítása érdekében.

A jövőben több olyan kihívás jelenhet meg, ami e-Észtország biztonságos működésére alapvető hatással lehet. Ilyen kihívások lehetnek a kvantumszámítógépek és az 5G megjelenése. A kvantumszámítógépek olyan számításokat is el fognak tudni végezni, amiket a hagyományos számítógépek jelenleg nem tudnak, így képesek lehetnek bizonyos titkosítások feltörésére. Ezen a véleményen van Dominique Unruh tartui professzor, aki szerint *„minden széles körben használt nyilvános kulcsú infrastruktúra (és ebbe beletartozik például az észt személyazonosító igazolvány) sebezhetőek a kvantumszámítással szemben”* Unruh kriptográfiával foglalkozik, és abban az irányban folytat kutatásokat, hogy Észtország hogyan tudna erre a kihívásra választ találni. A professzor megszólalása egyébként jó példa a technifikációra, az informatikai szektor egyik speciális grammatikájára. A technifikáció arra utal, hogy a számítógépes rendszerek működéséhez nagyon magas szintű szakmai tudásra van szükség, ami legitimációt biztosít az ezzel a tudással rendelkező szakértőknek ahhoz, hogy egy-egy problémát biztonságiasítsanak.

Észtországban alapvető kérdésként jelenik meg az 5G biztonságának az ügye. A Gazdasági és Kommunikációs Minisztérium a RIA-nak az egyik kiadványában közölt írásában meglehetősen határozottan írt erről az ügyről:

„Az egyik cégre […] *– a Huaweire – a világ számos táján nem mint egy független tech óriásra tekintenek, hanem mint egy szervezetre, amit a kínai kormány ellenőriz. Észtország kulcsfontosságú szövetségese, az USA, a Huaweit »a kínai hírszerzés trójai falovaként nevezte meg«. Számos nyugati hírszerző szolgálat, beleértve Észtországét is, osztja ezeket az aggodalmakat."*

Észtország tett olyan lépéseket, amik arra utalnak, hogy lehetséges, hogy korlátozni fogja a Huawei részvételét az 5G hálózatokban. 2019. november elején például Észtország (jogi kötőerővel valószínűleg nem bíró) közös nyilatkozatot adott ki az USA-val arról, hogy a hálózatokat kiépítő cégeknek megbízhatónak kell lenniük. Emellett Észtországban 2020. május 12-én fogadták el az új Elektronikai Kommunikációs Törvényt annak érdekében, hogy biztosítsák a jövő hálózataiba bekerülő távközlési eszközök biztonsági vizsgálatát. A törvény részletes implementálása a kormány hatáskörébe van utalva, a vizsgálatot végző hatóságok között pedig szerepelnek a hírszerző szolgálatok. Sem a közös nyilatkozat, sem a törvény nem említi a Huaweit (ez mutatja, hogy az észt kormány óvatosan közelíti meg a problémát). A törvény azonban „lex-Huaweiként" híresült el, mivel valószínűleg a törvényi feltételeit teremtette meg a Huawei korlátozásának. Ez nehéz helyzetbe hozza a Huaweit is használó Elisa mobilszolgáltatót, melynek vezetője szerint a Huawei megbízható és diszkreditálása az USA-Kína kereskedelmi háború része. A Huawei 5G hálózatokban való korlátozása túlmutat az informatikai szektoron, mivel nemcsak a technológia biztonsági kihívásairól, hanem Észtország USA-hoz és Kínához fűződő viszonyáról is szól.

3.3 E-Észtország biztonsági kihívásainak értékelése

E-Észtország alappilléreinek az X-út és az eID számítanak. Ezekre számos állami e-szolgáltatás épül. Az első kutatási kérdés arra vonatkozott, hogy az észt állami szolgáltatások nagymértékű digitalizáltsága milyen speciális biztonsági kihívásokat jelent. A tanulmány ezen részében több biztonsági kihívás is azonosításra került. Ilyen kihívás volt az eID-hoz használt csipekben fellelt sérülékenység, illetve az i-szavazás esetében egyes technológiai és eljárásbeli sérülékenységek. A jövőben biztonsági kihívásokat jelenthet majd az 5G és a kvantumszámítás megjelenése. Ezek a digitalizációból fakadó biztonsági kihívások véleményem szerint azért számíthatnak speciálisnak, mert (az eID elterjedtsége miatt) a lakosság széles körét érintik, érzékeny adatokról van szó (pl. e-egészségügy) és egyes megoldások, így az itt részletezésre került i-szavazás a demokratikus folyamatokban mára alapvető szerepet töltenek be.

4. Az informatikai és a társadalmi szektor közötti kapcsolatok Észtország esetében

Az informatikai szektor és a társadalmi szektor között kapcsolódási pontok figyelhetőek meg Észtország esetében. Ezek mögött a jelentős számú oroszajkú lakosság, illetve Oroszország jelenléte húzódik meg. A 2010-es évek elején Észtországban az 1,3 milliós lakosság 30%-a volt oroszajkú. A kihívást az jelenti, hogy az észtek és az oroszajkú kisebbség a mindennapi életük és értékrendjük tekintetében relatíve elkülönülten léteznek, és a történelmet (főleg a második világháborút) illetően nem osztják ugyanazt a kollektív emlékezetet. Ez vezetett részben a 2007-es ún. „Bronz Éjszakához", melynek van informatikai szektort is érintő vetülete. Az elkülönülésre épül és hozzá is járul az, hogy a két közösség nagyrészt különálló információs univerzumokban létezik, melynek legújabb terepe a közösségi média.

4.1 A 2007-es események bemutatása

A „Bronz Éjszakához" köthető eseményeket közvetlenül az váltotta ki, hogy az észt kormány 2007-ben úgy döntött, hogy a Bronz Katona szobrot és az alatta található, valószínűleg szovjet katonák maradványait Tallinn központjából egy katonai temetőbe helyezi át. A szobrot 1947-ben állították a szovjetek a második világháborús győzelem emlékéül. A szobor békés megemlékezések színhelye volt, egészen a 2000-es évek közepéig, amikor radikálisabb tüntetők is megjelentek. 2007. április 26-án kezdték meg a szobor eltávolítását, ami estére zavargásokhoz vezetett. Az éjszaka folyamán életét vesztette egy ember és körülbelül 150 fő sérült meg, míg a rendőrség közel ezer embert tartóztatott le. Április 27-én folytatódtak a kisebb összetűzések a rendőrök és a tüntetők között. Ezeket a rendőrség egy napon belül végül felszámolta. Az események ezzel nem értek véget, mivel Észtországot közel 22 napig kibertámadások érték. A kibertámadásokat két nagyobb hullámra lehet bontani. Az első hullám április 29-ig tartott és inkább érzelmi válaszadásnak lehet nevezni, mint szervezett akciónak. Az alkalmazott technikák egyszerűek voltak, a hozzájuk szükséges lépéseket orosz internetes fórumokon is fel lehetett lelni. A második hullám április 30-án kezdődött, és szofisztikáltabb, valamint jobban koordinált volt. A kibertámadások technikája alapvetően elosztott túlterheléses (DDoS) támadás volt.

A kibertámadások politikailag motiváltak voltak, viszont a támadások kiindulási helye, főképp a második szakaszban nem egyértelmű. Az biztos, hogy a támadások külföldről érkeztek, de a nehézséget jól mutatja, hogy mintegy 178 különböző ország számítógépei voltak érintettek a támadásban. Az orosz hatóságok tagadtak bárminemű részvételt a támadásokban, és máig nincsen konkrét bizonyíték a részvételükre. Ugyanakkor az is igaz, hogy az orosz kormány nem szólalt fel a támadások ellen. Kovács László szerint a támadások indítékai és összehangoltsága alapján valószínűsíthető, hogy Oroszország volt a támadások hátterében, de szerinte ezt nem lehet egyértelműen kijelenteni. A célpontok között voltak internetszolgáltatók, kormányzati és politikai intézmények (parlament, minisztériumok, politikai pártok), bankok és online újságok. Hatásukat tekintve a támadások nem voltak pusztítóak, de az e-megoldások elterjedtsége miatt fennakadásokat okoztak a helyi gazdaságban, illetve a lakosság hozzáférését csökkentették az állami szolgáltatásokhoz. Az okozott kárnál talán fontosabb, hogy a támadások *„felfedték Észtország sérülékenységeit, és demonstrálták a kibertámadásokban rejlő azon lehetőséget, hogy* [a kibertámadások] *ennél jóval tartósabb kárt okozzanak, ha van erre szándék*." Az észt kormány hiperbiztonságiasította a kibertámadásokat, például úgy, hogy a hálózatot ért támadásokat az ország politikai szuverenitását veszélyeztető műveletekként kommunikálta. Később Észtország a NATO segítségével intézmények létrehozásával is megerősítette ezt a biztonságiasítást, például a tallinni NATO Kooperatív Kibervédelmi Kiválósági Központ létrehozásával. Szintén az intézményesítésre példa az önkéntességen alapuló Észt Védelmi Ligán belül található Kibervédelmi Egység.

4.2 Az orosz befolyásolás példái a közösségi médiában

Az észt és az oroszajkú közösségek elkülönülése a közösségi médiában is jelen van. Egy kutatás a balti államok oroszajkú lakosainak online közösségi média használatát vizsgálta. A 2013-2017-es időszakot figyelembe vevő kutatás készítésekor Észtországban közel 600 ezer Facebook, 330 ezer VKontakte (VK) és 250 ezer Odnoklassniki (OK) felhasználó volt. A VK-t és az OK-t javarészt oroszajkúak használják. A kutatás különböző makrotémákat (pl. Szovjetunió, második világháború, Oroszország, Ukrajna) tartalmazó ideológia posztok előállítását és terjesztését vizsgálta. Az ideológiai posztok száma 2014 elején indult növekedésnek mindhárom platformon. Előállításukban a felhasználók kis, de annál aktívabb csoportja vett részt, akik valószínűleg céltudatosan állítottak elő ideológiai tartalmakat különböző témákban, amiből a kutatók arra következtettek, hogy nem ideológiai, hanem anyagi okok motiválhatták őket. Jellemző volt az is, hogy az egyes makrotémákról szóló diskurzusok megnövekedése kapcsolatban állt valós eseményekkel. A második világháború

1. ábra: Az ideológiai posztok (piros vonal) dinamikája az összes poszthoz képest (kék vonal) a VK-n a Baltikumban. Az ideológiai posztoknál a májusi csúcsokat érdemes figyelni.

Forrás: Teperik et alii i. m. 19. – Felhasználás a NATO StratCom COE engedélyével, a feliratokat a szerző fordította.

makrotéma körüli diskurzus például a VK-n minden év május 9-e körül felerősödött. A kutatás tehát tentatívan bizonyítja, hogy valamilyen mértékű befolyásolás tapasztalható az oroszajkúak által használt közösségimédia-felületeken Észtországban.

A közösségi médián keresztüli befolyásolási kísérletekről kaphatunk még egyfajta képet az észt Propastop blog tevékenységéből. Az önkéntesek által működtetett blog (aminek egyébként számos tagja az Észt Védelmi Liga tagja is) az Észtországot érintő (főként orosz) propagandatevékenységet igyekszik felfedni. A Propastopon például adtak hírt egy VK-n terjedő álhírről. A 2018. december 16-án megjelent orosz nyelvű posztban található képeken egy, az ENSZ migrációs politikája ellen tüntető aktivistát gyűr le egy járókelő, akin észt zászlós kabát van. A fotókon szereplő emberek arca nem látható, illetve más, aznap készült fotókon nem volt hó, amiből a Propastop arra következtetett, hogy álhírről volt szó. A Propastop bemutatott egy orosznyelvű YouTube csatornát is, ami egyszerű, automatizált technikával készült, de nagy mennyiségű (napi 4-5, összesen kb. 1800) videót tett közzé, melyek témái főképp Európához, a balti országokhoz és Ukrajnához kapcsolódtak. Ezek között a Propastop több tucat olyan videót talált, amik Észtországot negatív színben tüntették fel. Végül érdemes még megemlíteni egy kis orosz internetes újság által, néhány nappal 2020. május 9-e előtt megjelentetett álhírt, ami szerint az észtországi Kék Domboknál a XX. SS Gránátos Hadosztály emlékművét felrobbantották. Az álhír szerint az észt parlament kijelentette, hogy az FSZB-t és az Orosz Védelmi Minisztériumot okolja a történtekért, és hogy a robbantás a „Bronz Éjszaka" 13., a szovjet megszállás 75. évfordulójára esett. A Propastop megjegyezte, hogy a hír május 9-én orosz nyelvű Facebook csoportokban kezdett el megjelenni, mintegy tízezer reakciót kapott és közel ezren osztották meg. Ez egy példa lehet az előző bekezdésben említett jelenségre, miszerint május elején az ideológiai posztok aránya megnövekedhet az oroszajkúak által használt közösségimédia-felületeken. Az itt bemutatott Propastop bejegyzések alapján azonban csak korlátozott mértékben lehet következtetéseket levonni, tekintve, hogy ezen példák kontextusáról, és arról, hogy mennyire tekinthetőek általános jelenségnek, keveset lehet tudni. A Propastop tevékenysége annyit talán mutat, hogy az észtországi közösségi médiában valóban lehet találkozni orosz nyelvű álhírekkel.

4.3 A szektorok közötti kapcsolatok értékelése Észtország esetében

Észtország jelentős nagyságú oroszajkú lakossággal rendelkezik, ezért volt indokolt a társadalmi és az informatikai szektor közötti kapcsolatok vizsgálata. A második kutatási kérdés arra vonatkozott, hogy ezen oroszajkú lakosság jelenléte hogyan befolyásolja az informatikai szektort. A 2007-es események kapcsán az látható, hogy a társadalmi szektorban meglévő nyelvi, kulturális feszültségek nem maradtak meg ennek a szektornak a szintjén, hanem kibertámadásokon keresztül tovább gyűrűztek az informatikai szektorba, hatásukat (kormányzati, banki szolgáltatások részleges leállása) részben ott fejtették ki. A balti államok oroszajkú lakosainak közösségi média használatát vizsgáló kutatás és a közösségi médián keresztüli befolyásolásra példaként hozott Propastop blogbejegyzések azt mutatják, hogy napjaink Észtországában a társadalmi és az informatikai szektor szorosan összekapcsolódhat.

5. Összefoglalás

Az informatikai szektor vizsgálata Észtországban példaértékű, mivel az ország digitálisan fejlettnek tekinthető. A tanulmány célja az volt, hogy az informatikai szektort vizsgálja Észtország esetében, különös tekintettel az e-Észtországhoz kapcsolódó speciális biztonsági kihívásokra. Részletezésre kerültek az eID-hoz kapcsolódó egyik csipben talált 2017-es sérülékenység és az i-szavazással kapcsolatos biztonsági kihívások. Ezek a kihívások speciálisnak tekinthetőek, mivel egyrészt az eID elterjedtsége miatt a lakosság nagy részét érintik, érzékeny adatok is veszélybe kerülhetnek, illetve az i-szavazás esetében a demokratikus folyamatokban való meghatározó szerepről van szó. A jövőben a kvantumszámítás és az 5G megjelenése jelenthetnek speciális biztonsági kihívásokat. Az észtországi oroszajkú kisebbségre vonatkozó kutatási kérdés kapcsán a társadalmi és az informatikai szektor közötti kapcsolatok kerültek vizsgálatra. A 2007-es „Bronz Éjszaka” eseményei és az azt követő kibertámadások elemzéséből arra lehet következtetni, hogy a társadalmi szektorban jelentkező problémák az informatikai szektorba tovább gyűrűztek. A közösségi médián keresztüli befolyásolást vizsgálva pedig az látható, hogy ott a társadalmi és az informatikai szektor szorosan összekapcsolódik.

A szekunder forrásokon alapuló elemzés átfogó képet ad az informatikai szektorról Észtország esetében, ám nem képes minden releváns biztonsági kihívást, illetve az informatikai és a társadalmi szektor közötti kapcsolatot teljes egészében feltárni. A teljesebb kép érdekében szükséges primer adatgyűjtést is lefolytatni interjúk segítségével, illetve az e-Észtországgal kapcsolatos biztonsági kihívásokat más szemszögből is megvizsgálni. További kutatásra adhat okot az is, hogy a szektoriális biztonságértelmezésben az informatikai szektor helye és jellemzői elméleti szempontból nem kellően megalapozottak. Az elméleti újragondolás azért is megfontolandó, mert horizontálisan az informatikai szektor egyre több más szektorhoz is kapcsolódik (ld. társadalmi szektorral való kapcsolat), illetve a szektor egyes biztonsági kihívásai (pl. 5G) vertikálisan egyre magasabb, akár stratégiai szinten is jelentkezhetnek.

A tanulmány értékét, hasznosságát abban látom, hogy átfogó képet ad az észt állami e-szolgáltatások rendszeréről, ehhez kapcsolódóan rámutat speciális biztonsági kihívásokra és feltár összefüggéseket az informatikai és a társadalmi szektor között. Az észt rendszer vizsgálata azért lehet különösen hasznos, mert szinte a teljes lakosság rendelkezik eID funkcionalitással bíró személyazonosító igazolvánnyal és számottevő részük használja is az e-szolgáltatásokat. Emiatt a biztonsági kihívások nem szigetszerű rendszereket, hanem az egész társadalmat kiszolgáló rendszert érintenek. Ez a gyakorlatban működő rendszer más országok számára fontos tanulságokkal szolgálhat, amik közül kiemelném az alternatív megoldások fontosságát (ld. eID funkcionalitással bíró kártyákban talált sérülékenység), a magánszektor erősítését és az együttműködés fokozását, a jövőbeni kihívásokra való tudatos felkészülést (ld. kvantumszámítógépek), illetve a lakosság számítástechnikai

tudásának fejlesztését. Az informatikai és a társadalmi szektor között talált összefüggések segíthetik annak megértését, hogy a társadalmi folyamatok kibertérben való megjelenése milyen speciális kihívásokat jelent. A tanulmány eredményeinek értékelésénél figyelembe kell venni, hogy Észtország a kisebb lakosságú országok közé tartozik. Az elemzés így is rámutatott kritikus kérdésekre, amiket érdemes lehet tovább, vagy más országok esetében is vizsgálni.

Felhasznált irodalom

1163/2020. (IV.21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.

2007 cyber attacks on Estonia. In *Hybrid threats*. NATO StratCom COE. Elérhető: https://www.stratcomcoe.org/download/file/fid/80212 (A letöltés dátuma: 2021.03.06.)

Aasmae, Kalev: *Estonia's ID card crisis: How e-state's poster child got into and out of trouble*. 2017. Elérhető: https://www.zdnet.com/article/estonias-id-card-scrisis-how-e-states-poster-child-got-into-and-out-of-trouble/ (A letöltés dátuma: 2021. 03. 06.)

About Smart-ID. Elérhető: https://www.smart-id.com/about-smart-id/ (A letöltés dátuma: 2021. 03. 07.)

Annual Cyber Security Assessment 2018. Information System Authority, 2018. Elérhető: https://www.ria.ee/sites/default/files/content-editors/kuberturve/ria-csa-2018.pdf (A letöltés dátuma: 2021. 03. 06.)

Annual Cyber Security Assessment 2019. Information System Authority, 2019. Elérhető: https://www.ria.ee/sites/default/files/content-editors/kuberturve/ktt_aastaraport_eng_web.pdf (A letöltés dátuma: 2021. 03. 06.)

Attention! Provocative fake news is circulating in Narva. 2018. Elérhető: https://www.propastop.org/eng/2018/12/20/attention-provocative-fake-news-is-circulating-in-narva/ (A letöltés dátuma: 2021. 03. 06.)

Busvine, Douglas – Rinka, Andreas: *Huawei denies German report it colluded with Chinese intelligence.* 2020. Elérhető: https://www.reuters.com/article/us-germany-usa-huawei-idUSKBN1ZS197 (A letöltés dátuma: 2021. 03. 06.)

Buzan, Barry – Wæver, Ole – de Wilde, Jaap: *Security – A New Framework For Analysis*. London, Lynne Rienner Publishers, 1998.

Chan, Sewell: *Fearful of Hacking, Dutch Will Count Ballots by Hand*. 2017. Elérhető: https://www.nytimes.com/2017/02/01/world/europe/netherlands-hacking-concerns-hand-count-ballots.html (A letöltés dátuma: 2021. 03. 06.)

Clarka, Dylan – Martens, Tarvi: E-voting in Estonia. In Feng Hao – Peter Ryan (szerk.): *Real-world electronic voting*. Boca Raton, CRC Press, 2017. 129–141.

Cyber Security In Estonia 2020. Information System Authority, 2020. Elérhetőség: https://www.ria.ee/sites/default/files/content-editors/RIA/cyber_security_in_estonia_2020_0.pdf (A letöltés dátuma: 2021. 03. 06.)

Sharkov, Damien : *Victory Day: Why Is the May 9 Commemoration So Important to Russia?* 2017. Elérhető: https://www.newsweek.com/what-may-ninth-and-why-it-so-important-russia-605639 (A letöltés dátuma: 2021. 03. 06.)

Data Embassy – Factsheet. Elérhető: https://e-estonia.com/wp-content/uploads/2020mar-facts-a4-data-embassy.pdf (A letöltés dátuma: 2021. 03. 06.)

Data Exchange Layer X-tee. 2020. Elérhető: https://www.ria.ee/en/state-information-system/x-tee.html (A letöltés dátuma: 2021. 03. 06.)

Digital Economy and Society Index (DESI) 2019 - Country Report – Estonia. European Commission, 2019. Elérhető: https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=59894 (A letöltés dátuma: 2021. 03. 06.)

Digital ID. Elérhető: https://www.politsei.ee/en/instructions/digital-id (A letöltés dátuma: 2021. 03. 07.)

Electronic Identity eID. Elérhető: https://www.ria.ee/en/state-information-system/electronic-identity-eid.html (A letöltés dátuma: 2021. 03. 06.)

E-Resident's digital ID. Elérhető: https://www.politsei.ee/en/instructions/e-resident-s-digital-id (A letöltés dátuma: 2021. 03. 07.)

Estonia's presidency in UN Security Council. Elérhető: https://un.mfa.ee/estonias-presidency-in-un-security-council/ (A letöltés dátuma: 2021. 03. 06.)

Estonian eID scheme: diplomatic identity card. Police and Border Guard Board, 2018. Elérhető: https://ec.europa.eu/cefdigital/wiki/download/attachments/62885749/EE%20eID%20LoA%20mapping%20-%20diplomatic%20identity%20card.pdf?version=1&modificationDate=1531759815709&api=v2 (A letöltés dátuma: 2021. 03. 07.)

Gazdag Ferenc – Remek Éva: *A biztonsági tanulmányok alapjai*. Budapest, Dialóg Campus, 2018.

Hansen, Lene – Nissenbaum, Helen: Digital Disaster, Cyber Security, and the Copenhagen School, *International Studies Quarterly*, 53. (2009), 4. 1155-1175. DOI: https://doi.org/10.1111/j.1468-2478.2009.00572.x

How did Estonia become a leader in technology? The Economist, 2013. Elérhető: https://www.economist.com/the-economist-explains/2013/07/30/how-did-estonia-become-a-leader-in-technology (A letöltés dátuma: 2021. 03. 06.)

ID-card – Introduction. Elérhető: https://www.id.ee/en/rubriik/introduction/ (A letöltés dátuma: 2021. 03. 07.)

Information System Authority – State information system. Elérhető: https://www.ria.ee/en.html (A letöltés dátuma: 2021. 03. 06.)

Juurvee, Ivo – Mattiisen, Mariita: *The Bronze Soldier Crisis of 2007: Revisiting an Early Case of Hybrid Conflict.* International Centre for Defence and Security, 2020. Elérhető: https://icds.ee/wp-content/uploads/2020/08/ICDS_Report_The_Bronze_Soldier_Crises_of_2007_Juurvee_Mattiisen_August_2020.pdf (A letöltés dátuma: 2021. 03. 07.)

Kaiser, Robert: Reassembling the event: Estonia's 'Bronze Night', *Environment and Planning D: Society and Space*, 30. (2012), 6. 1046–1063.

Kitsing, Meelis: *Internet Banking as a Platform for E-Government.* 2017. Elérhető: https://www.riigikogu.ee/wpcms/wp-content/uploads/2018/08/IE-2017-Internet-banking-platform-final.pdf (A letöltés dátuma: 2021. 03. 06.)

Kovács László: *A kibertér védelme.* Budapest, Dialóg Campus, 2018.

Kund, Oliver: *Estonia to pick side in 5G dispute.* 2019. Elérhető: https://news.postimees.ee/6813047/estonia-to-pick-side-in-5g-dispute (A letöltés dátuma: 2021. 03. 06.)

Lips, Silvia et alii: Key Factors in Coping with Large-Scale Security Vulnerabilities in the eID Field. In Andrea Kő – Francesconi, Enrico (szerk.): *Electronic Government and the Information Systems Perspective*. Cham, Springer, 2018. 60–80. DOI: https://doi.org/10.1007/978-3-319-98349-3_5

Lobjakas, Ahto: *5G: Estonia Picks National Security over Technology.* 2020. Elérhető: https://www.aspen.review/article/2020/5g-estonia-picks-national-security-technology/ (A letöltés dátuma: 2021. 03. 06.)

McGuinnes, Damien: *How a cyber attack transformed Estonia*. 2017. Elérhető: https://www.bbc.com/news/39655415 (A letöltés dátuma: 2021. 03. 06.)

Kaldur, Kristjan et alii*: Integration Monitoring of the Estonian Society 2017 – Media use and information fields.* Institute of Baltic Studies and Praxis Center for Policy Studies, 2017. Elérhető: https://www.kul.ee/sites/kulminn/files/6_meedia_eng.pdf (A letöltés dátuma: 2021. 03. 06.)

Means of eID. Elérhető: https://www.ria.ee/en/state-information-system/electronic-identity-eid/means-eid.html (A letöltés dátuma: 2021. 03. 07.)

Molnár Mihály: Az Észt Belügyi Biztonsági Szolgálatot kihívásai. *Honvédelmi Szemle*, 10. (2017), 3. 244-264.

Müller, Roman: *Analysis of the estonian X-tee network based on centralized log data*, Szakdolgozat. Tallinn, Tallinn University of Technology, 2019. Elérhető: https://digikogu.taltech.ee/en/Download/4ddcf4a7-922e-4112-87cd-8f3809b6be24 (A letöltés dátuma: 2021. 03. 06.)

Nurse, Jason R. C. et alii: An Assessment of the Security and Transparency Procedural Components of the Estonian Internet Voting System. In Tryfonas, Theo (szerk.): *Human Aspects of Information Security, Privacy and Trust.* Cham, Springer, 2017. 366–383. DOI: https://doi.org/10.1007/978-3-319-58460-7_26

Ottis, Rain: *Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective*. 2008. Elérhető: https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf (A letöltés dátuma: 2021. 03. 06.)

Pääbo, Heiko: War of Memories: Explaining "Memorials War" in Estonia. *Baltic Security & Defence Review*, 10. (2008), 1. 5–28.

Pecen, Mark: *Quantum Safe Cryptography and Security.* ETSI, 2015. Elérhető: https://www.etsi.org/images/files/ETSIWhitePapers/QuantumSafeWhitepaper.pdf (A letöltés dátuma: 2021. 03. 06.)

Pernik, Piret – Tuohy, Emmet: *Cyber Space in Estonia: Greater Security, Greater Challenges.* Tallinn, International Centre for Defence Studies, 2013. Elérhető: https://icds.ee/wp-content/uploads/2013/Piret%20Pernik%20-%20Cyber%20Space%20in%20Estonia.pdf (A letöltés dátuma: 2021. 03. 06.)

Perrigo, Billy: *What the U.S. Can Learn About Electronic Voting From This Tiny Eastern European Nation.* 2019. Elérhető: https://time.com/5541876/estonia-elections-electronic-voting/ (A letöltés dátuma: 2021. 03. 06.)

Radin, Andrew: *Hybrid Warfare in the Baltics – Threats and Potential Responses.* Santa Monica, Calif., RAND, 2017. Elérhető: https://www.rand.org/content/dam/rand/pubs/research_reports/RR1500/RR1577/RAND_RR1577.pdf (A letöltés dátuma: 2021. 03. 06.)

Residence permit card for an adult. Elérhető: https://www.politsei.ee/en/instructions/residence-permit-card-for-an-adult (A letöltés dátuma: 2021. 03. 07.)

Riigikogu elections 2019 – Voting results in detail. 2019. Elérhető: https://rk2019.valimised.ee/en/voting-result/voting-result-main.html (A letöltés dátuma: 2021. 03. 06.)

Robinson, Nick – Martin, Keith: Distributed denial of government: the Estonian Data Embassy Initiative. *Network Security*, (2017), 9. 13–16. DOI: https://doi.org/10.1016/S1353-4858(17)30114-9

Robot videos spread anti-Estonian propaganda in Youtube. 2019. Elérhető: https://www.propastop.org/eng/2019/04/30/robot-videos-spread-anti-estonian-propaganda-in-youtube/ (A letöltés dátuma: 2021. 03. 06.)

Roosna, Sandra – Rikk, Raul: *e-ESTONIA – e-Governance in Practice*. 2016. Elérhető: https://ega.ee/wp-content/uploads/2016/06/e-Estonia-e-Governance-in-Practice.pdf (A letöltés dátuma: 2021. 03. 06.)

Sierzputowski, Bartłomiej: The data embassy under public international law. *International & Comparative Law Quarterly*, 68. (2019), 1. 225–242. DOI: https://doi.org/10.1017/S0020589318000428

Spreading fake news: Was a monument in the Blue Mountains to a SS Division blown up? 2020. Elérhető: https://www.propastop.org/eng/2020/05/15/spreading-fake-news-was-a-monument-in-the-blue-mountains-to-a-ss-division-blown-up/ (A letöltés dátuma: 2021. 03. 06.)

Springall, Drew et alii: Security Analysis of the Estonian Internet Voting System In. *CCS'14 Proceedings of the 21st ACM Conference on Computer and Communications Security.* New York, The Association for Computing Machinery, 2014. 703–715. DOI: https://doi.org/10.1145/2660267.2660315

Ströbele, Maarit – Leosk, Nele – Trechsel, Alexander H.: *Two Countries / Two Decades / Two Outcomes – A brief comparison of e-government solutions in Estonia and Switzerland.* Zurich, xUpery, 2017. Elérhető: https://xupery.com/wp-content/uploads/2017/08/A-brief-comparison-of-e-government-solutions-in-Estonia-and-Switzerland.pdf (A letöltés dátuma: 2021. 03. 06.)

Talmazan, Yuliya: *Data security meets diplomacy: Why Estonia is storing its data in Luxembourg.* 2019. Elérhető: https://www.nbcnews.com/news/world/data-security-meets-diplomacy-why-estonia-storing-its-data-luxembourg-n1018171 (A letöltés dátuma: 2021. 03. 06.)

Teperik, Dmitri et alii: *Virtual Russian World in the Baltics*. Elérhető: https://www.stratcomcoe.org/virtual-russian-world-baltics (A letöltés dátuma: 2021. 03. 06.)

The 2020 yearbook of the Information System Authority. Information System Authority. Elérhető: https://www.ria.ee/sites/default/files/content-editors/ria_aastaraamat_2020_48lk_eng.pdf (A letöltés dátuma: 2021. 03. 06.)

Tikk, Eneken – Kaska, Kadri – Vihul, Liis: *Interantional cyber incidents – Legal considerations*. Tallinn, NATO CCD COE, 2010. Elérhető: https://ccdcoe.org/uploads/2018/10/legalconsiderations_0.pdf (A letöltés dátuma: 2021. 03. 06.)

Torn, Tanel: *Security analysis of Estonian i-voting system using attack tree methodologies.* Tallinn, Tallinn University of Technology, 2014. Elérhető: https://digikogu.taltech.ee/en/Download/f1c0ad93-b6a3-401f-8734-15a3324cb33c (A letöltés dátuma: 2021. 03. 06.)

United States–Estonia Joint Declaration on 5G Security. 2019. Elérhető: https://ee.usembassy.gov/joint-declaration-on-5g/ (A letöltés dátuma: 2021. 03. 06.)

Vahtla, Ali*: Employees of foreign embassies to be issued digital IDs.* 2017. Elérhető: https://news.err.ee/588887/employees-of-foreign-embassies-to-be-issued-digital-ids (A letöltés dátuma: 2021. 03. 07.)

Vahtla, Aili: *ICDS director: 5G memorandum a matter of security for Estonia.* 2019. Elérhető: https://news.err.ee/997106/icds-director-5g-memorandum-a-matter-of-security-for-estonia (A letöltés dátuma: 2021. 03. 06.)

Vinkel, Priit – Kimmer, Robert: The How and Why to Internet Voting an Attempt to Explain E-Stonia In Kimmer, Robert et alii (szerk.): *Electronic Voting.* Cham, Springer, 2017. 178–191. DOI: https://doi.org/10.1007/978-3-319-52240-1_11

Virki, Tarmo: *Estonia passes ‚Huawei law' for telecom security reviews.* 2020. Elérhető: https://www.reuters.com/article/us-estonia-telecoms-law-idUSKBN22O22I (A letöltés dátuma: 2021. 03. 07.)

What is Propastop? 2017. Elérhető: https://www.propastop.org/eng/2017/03/06/what-is-propastop/ (A letöltés dátuma: 2021. 03. 06.)

X-Road factsheet. Elérhető: https://www.ria.ee/sites/default/files/content-editors/publikatsioonid/x-road-factsheet-2014.pdf (A letöltés dátuma: 2021. 03. 06.)

X-tee factsheet. Elérhető: https://www.x-tee.ee/factsheets/EE/#eng (A letöltés dátuma: 2021. 03. 06.)

Tóth József Lukács

Kiberbűnözés és adathalászat, aktuális internetes fenyegetettségek

1. Bevezetés

A publikáció elsődleges célja, hogy szembesítse az egyetemi polgárokat és fiatalokat az internet világában rejtőzködő fenyegetésekkel. Másodlagos célja, hogy tisztázza a legalapvetőbb fogalmakat, amelyek a kiberbűnözés, adathalászat és aktuális internetes fenyegetések témában elengedhetetlenek. A publikációt inkább figyelemfelhívásként, mintsem tudományos értekezésként kívántam elkészíteni.

Napjainkban egyre inkább elterjedtek az internet veszélyeivel kapcsolatos felhívások, informatív előadások, publikációk. Ennek ellenére rengeteg ember van, aki úgy gondolja, hogy egyszerűen felesleges és értelmetlen a profi antivírus szoftverek, vagy egyéb biztonsági eszközök beszerzése. Hackerek, etikus hackerek, zsarolóvírusok, malware, DDoS, Deep-web, Dark-web, mind olyan kifejezés és fogalom, amellyel már sokan találkoztunk. De vajon mi, egyetemi polgárok, felfogjuk-e azt, hogy ezek pontosan mit is takarnak?

2. Alapvető fogalomtisztázás

2.1 A kiberbűnözés

A kiberfenyegetéseket a szakirodalom négy csoportba sorolja[1]. Ezek a következők: kiberbűnözés, hacktivizmus és kiberterrorizmus, kiberkémkedés, kiberhadviselés. A kiberbűnözés tulajdonképpen egy gyűjtőfogalom, melynek lényege a számítógép és számítógépes rendszerek felhasználásával, más számítógépekre és hálózatokra irányuló támadások, bűncselekmények összefoglaló definíciója. A támadások célja legtöbbször valamilyen anyagi vagy érzelmi kár okozása.

2.2 Adathalászat (Phishing)

Az adathalász-támadások során az áldozat egy olyan tartalmú e-mailt kap, amelyben kérik, hogy töltsön ki egy online kérdőívet és így érzékeny személyes adatokhoz jutnak a csalók. Az online kérdőívet egy hamisított weboldalon helyezik el. Mivel elektronikus levélből irányítják az áldozatot a weblapra, az adathalászat nem valamilyen szoftverhiányosságot használ ki, hanem azt, hogy a felhasználó nem tud világosan különbséget tenni a valódi és a hamis weboldalak között[2].

3. Internetes fenyegetettség napjainkban

Manapság egyre többet hallhatunk a kiberbűnözésről és az egyéb olyan fenyegetésekről, amelyek az átlagembert célozzák. A kiberbűnözés mára olyan fejlett, profi és megdöbbentően szofisztikált módszereket alkalmaz, amely komoly problémát okoz a hatóságoknak. De pontosan mit is takar a kiberbűnözés? Nos, vírusok terjesztésétől kezdve, személyes adatok megszerzésén és dollármilliók ellopásáig, nagyjából minden olyan illegális tevékenység, amelyet valamilyen számítógépes rendszeren keresztül követnek el. De, vajon milyen mértékben terjedtek el a hasonló bűncselekmények? Talán statisztikai adatok ismertetésével tudnám ezt a legkönnyebben szemléltetni. A különböző szervezetek és cégek 88%-a vált phishing támadás célpontjává[3]. De a legmegdöbbentőbb statisztikai adat a kibertámadások által okozott kár amerikai dollárban meghatározott értéke, mely 2021-re eléri a közel 6 billió Dollárt[4].

1 Krasznay Csaba: A polgárok védelme egy kiberkonfliktusban, In. Hadmérnök, 2012, VII:(4) pp. 142–151.
2 Koltay Tibor, Jávorszky Ferenc: A web 2.0 legfontosabb biztonsági fenyegetései In TMT 56. évf. 2009. 11–12.
3 2020 State of the Phish: An in-depth look at user awareness, vulnerability and resilience, 12.
4 Steve Morgan: Cybercrime To Cost the World 10,5 Trillion Annually by 2025, megtekintve:2021.08.18, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Célpontok a nyilvános és nem nyilvános állami és civil weboldalak, szerverek, a vállalkozások nem publikus információi, amelyek a vetélytársak hasznára szolgálhat, kiskorúak, valamint szinte mindannyiunk személyes információi.

3.1 Az egyén, mint tényező

Az említett támadások ellen nagymértékben megóvhatnánk magunkat, ugyanakkor azok, akik még nem estek áldozatul, általában úgy gondolják, hogy őket úgy sem érheti semmilyen kár. Le kell szögeznem, hogy az a visszaélésekkel és fenyegetésekkel kapcsolatos hozzáállás, hogy: *„Én úgy se esek áldozatul”,* sajnosan nagyon gyakori és egyben naiv megállapítás. A valóság sajnos teljesen mást mutat.

Egyszerű megelőző műveletekkel nagyon sokat tehetünk személyes adataink biztonsága érdekében.

Ezek a következők:

- Használjunk minden weboldalon más, összetett jelszavakat, amelyeket fontos, hogy ne a számítógépen elmentve raktározzunk el. Ez azért fontos, mert a zsaroló E-mailek száma megsokszorozódott a Yahho, LinkedIn és Dropbox feltörése után, amikor is milliók felhasználóneveit és jelszavait dobták piacra. Az üzenetekben általában szerepeltek a különböző belépéshez használt azonosítók. Ezzel sokszor azt akarták bebizonyítani, hogy átvették az irányítást a rendszer fölött, még akkor is, ha ez nem történt meg és csak az azonosítókat szerezték meg, így kényszerítve az illetőt arra, hogy fizessen;
- Semmiféleképen ne nyissuk meg a gyanúsnak látszó E-maileket, mivel a malware-ek 94%-a ily módon fertőzi meg az eszközöket.[5] (A későbbiekben bemutatok egy globális támadást, amely szintén E-mailen keresztül indult el.);
- Kerüljük a nyílt vezeték nélküli internetkapcsolatokat;
- Készítsünk biztonsági mentést az eszközeinkről;
- Ne nyissunk meg gyanúsnak tűnő weboldalakat;
- Soha ne adjuk meg a jelszavunkat telefonon, vagy üzenet formájában;
- Ne vásároljunk olcsó, nem elterjedt márkától származó készülékeket.

Ha őszintén belegondolunk, hányan frissítettük már a routereinken futó szoftvereket? Meggyőződésem, hogy nem sokan. Megdöbbentene-e bárkit is az, ha azt mondanám, hogy a telefonunkon, csak a bekapcsolt Wi-Fi alapján meg lehet határozni bárki helyzetét? Igen, meg lehet, akár visszamenőleg is. Sőt, az okostelefonokkal készített fényképek nagy százaléka tartalmaz egy beágyazott GPS koordinátát. Ha valaki feltölt egy képet egy online platformra, egy hozzáértő könnyedséggel megszerezheti a GPS koordináták segítségével a tartózkodási helyünket. Ez azért érdekes, mert legtöbbször nem szívesen adjuk meg a tartózkodási helyünket, ugyanakkor bármi féle hezitálás nélkül megadjuk ily módon, nagyjából 15 méteres eltéréssel.

4. A Deep web és a Dark web

Mindennapi internet használat közben, amikor egyszerűen csak teendőinek intézzük, az internet számunkra elérhető, úgymond felszínével érintkezünk. Ugyanakkor a felszín alatt találhatóak azok az oldalak, amiket egy sima keresőmotorral, mint a Google vagy Yahho, nem érünk el. Ezt nevezzük deep webnek. Az internet azon részét, amelyet mi dark webnek hívunk, különleges keresőkkel lehet elérni. Ezeken a klienseken keresztül olyan weboldalak nyílnak meg előttünk, amelyeken szinte minden egyébként illegális termék és szolgáltatás elérhető. Hogy mi a legnagyobb előnye a dark webnek? Az anonimitás.

5 Josh Fruhlinger: Top cybersecurity facts, figures and statistics, megtekintve:2021.08.18, https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Természetesen, viták folynak arról, hogy tényleg teljesen lekövethetetlen-e ez az eljárás, de az biztos, hogy sokkal nagyobb biztonságot garantál, mint egy rendes internet böngésző. Egy normális kereső használata közben az IP-cím alapján a felhasználó bármikor lekövethető, kivéve, ha egy speciális böngészőt használ. Ezek ráadásul könnyen el is érhetőek. Kihasználva az anonimitást, a kiberbűnözők hatalmas bevételre tehetnek itt szert. Erre tökéletes példa a fekete piacok elterjedése, amelyek közül sokat le is állítottak a közelmúltban. Ugyanakkor sok hasonló oldal van még a mai napig, amelyeket még nem sikerült leállítani. Egy időben elterjedt az a közhiedelem, hogy az FBI feltörte a legismertebb dark web klienst, ennek következtében a dark webet használók száma 50%-kal lecsökkent. Sajnos, mint fekete piaci oldalból, webkliensből is sok elérhető a felhasználók számára.

A korábban említett felületeket a felhasználók nem csak az illegális áruk eladására és vételére használják. Rengetek propaganda terjeng itt, biztonságosabb információcsatornaként szolgál. A dark weben igyekeznek a különböző országok hatóságai is megállítani, lokalizálni, felfedni a különböző illegális tevékenységeket folytató egyéneket, legyen szó feketepiaci kereskedelmi csatornákról vagy radikális szervezetekről.

Talán elsőre meglepőnek tűnhet, de olyan hatalmas médiaóriások is, mint a New York Times vagy a Guardian. Az itt üzemeltetett weboldalak célja, hogy az identitásukat nem felfedni szándékozók dokumentumokat és információkat közölhetnek. Ugyanakkor jogosan merül fel bennünk a kérdés, hogy vajon miért nem kapcsolják le? Nos egyrészt azért, mert az állami szféra is használja, másrészt pedig azért, mert az embereknek anonim és „biztonságos" internet használatot biztosít. Így hát a dilemma adott.

5. Számítógépes vírusok és egyéb kártevők

Manapság már szinte mindenki megtapasztalta, hogy milyen az, amikor egy vírus megfertőzi a számítógépünket. A különböző vírusok általában *E-mailen keresztül*, *az internetről letöltött fájlok vagy külső adattárolókon* keresztül fertőzik meg a rendszerünket. Elég gyakori, hogy egy víruskereső program a támadások nagy részét meg tudja akadályozni, így mindenkinek ajánlott használni egyet! Ugyanakkor előfordul az is, hogy az antivírus programunk nem tudja felvenni a versenyt az adott vírussal. Ezek a programok előfordulhat, hogy pénzt követelnek azért, hogy az illető hozzáférjen a számítógépes adataihoz, vagy azért, hogy a számítógépen található szenzitív tartalmakat ne tegye közzé. A hasonló kártevő programok ellen, főleg a profi vírusok ellen, általában a megfelelő védekezés a legtöbb, amit tenni tudunk.

Csupán azért, hogy megértsük, milyen károkat képes okozni egy vírus, az elmúlt évek számos esetei közül kiragadtam egyet, amely nem más, mint a *„Conficker"* malware. Sokak szerint ez volt a legkárosabb mind közül, mivel becslések szerint közel 9 milliárd dolláros kárt okozott és közel 15 millió rendszert fertőzött meg. Az eset 2008-ban történt. A malware megfertőzte az Egyesült Királyság rendőrségeit, de még a Brit Haderőt is. Továbbá befolyásolt különböző műveleteket is. Többnyire Windows rendszereket támadott meg, a baj viszont az volt, hogy szinte mindegyik antivírust és frissítést megkerülte, így sok ideig nem tudták leállítani. Azért volt képes ilyen sok eszközt megfertőzni ez a malware, mert amennyiben egy eszközt megfertőzött, az összes többi azonos hálózaton lévő eszközt is elérte, valamint sokszorozta önmagát. Ezért fontos, hogy ha lehet, kerüljük az ismeretlen és nyilvános hálózatokat. Szerencsére nem okozott nagy károkat, feltehetően azért, mert hatalmas, nemzetközi hírnevet szerzett magának, így a készítői nem mertek komolyabb támadásokat indítani.[6]

Sajnos a kibertérben elkövetett bűncselekmények elég széles skálán mozognak. A kiberbiztonság mára egy olyan kritikus aspektussá nőte ki magát, amely semmi féle képen nem elhanyagolható. Cégek dollármilliókat

6 Conflicker and its legacy: An overview of the conflicker worm, megtekintve:2021.08.18 https://medium.com/@donovan.adams/what-is-this-confiker-y-you-speak-of-an-overview-of-the-conficker-worm-eb4997928107

költenek azért, hogy relatív biztonságban tudhassák magukat. A Microsoft cég, ami egy érdekes példa, mert egyszerre gyárt szoftvert és hardvert is, nagyjából egymilliárd dollárt költött csak kiberbiztonságra. Ez azt jelenti, hogy ahhoz, hogy egy eszközt vagy egy hálózatot valaki feltörjön, már nem elég egy egyszerű kód vagy program. A fekete piacon egy olyan program, amely képes kompromittálni egy Android rendszert, megközelítőleg 2,5 millió dollárba egy IOS rendszert 1,5 millió dollárba kerül.[7] Ebből következtethetünk arra, hogy egy multinacionális cég vagy kormányzati szerv feltörése se olcsó. Ugyanakkor, ha ezt összehasonlítjuk azzal, hogy egy átlagos ember mennyit költ a saját biztonságára az online térben, az összeg nagyjából egyenlő a nullával. Nem meglepően, legtöbbször ezért támadják a rosszindulatú hackerek az egyént, nem pedig a cégeket és különböző szerveket. Ez azért fontos, mert a humán erőforrás a cégek egyik alappillére. Egy személyes támadás ára a fekete piacon jelentősen kevesebb, nagyjából két-három számjegyes összeg, amerikai dollárban. Természetesen a hackerek rajtunk keresztül azokat a cégeket fogják támadni, amelyek alig költenek a kiberbiztonságra. Így hát nem meglepő az, hogy a támadások közel 70%-a kis- és közepes méretű vállalkozásokat céloz meg.

Csak hogy ismertessek egy megtörtént esetet, már 2013-ban már az interneten is reklámoztak különböző kártevő szolgáltatásokat, amelyek frappáns hirdetések kíséretében jelentek meg. Tulajdonképpen, amennyiben valakinek vetélytársa akadt például az üzleti szférában, nyugodtan rendelhetett egy szolgáltatást, ami egy *„DDoS"* (Szolgáltatásmegtagadással járó támadás) segítségével megszünteti a konkurenciát. *Distributed Denial of Service*, azaz *DDoS*-támadásnak azt nevezzük, amikor a támadó nagy mennyiségű forgalommal áraszt el egy hálózatot vagy szervert azzal a céllal, hogy annak működését ellehetetlenítse. Az ilyen támadásokat leginkább arra használják, hogy bizonyos weboldalakat vagy alkalmazásokat napokra, vagy akár még tovább is működésképtelenné tegyenek.[8] Ezt a szolgáltatást ráadásul nem egy nehezen hozzáférhető felületen reklámozták, hanem a YouTube-on.

1. ábra USB biztonsági kulcs

6. Fordítsunk pénzt a saját biztonságunkra is

Jogosan merül fel a kérdés, hogy vajon mit tehetünk azon kívül, amiket már korábban felsoroltam. Sokak szerint egy új korszakhoz érkezik a kiberbiztonság, mivel a különböző biztonsági eszközök egyre jobban elterjednek a piac kínálati oldalán, azaz egyre olcsóbbak és elérhetőbbek lesznek. Az első hasznos befektetés, amivel megvédhetjük a jelszavainkat egy kulcs. Ez a kulcs pontosan ugyan olyan funkciót tölt be, mint gondolnánk. Összességében annyi a különbség, hogy ezt a kulcsot egy USB nyíláson keresztül hozzá lehet csatlakoztatni az adott eszközhöz, így egy két lépcsős megerősítést alkalmazva szinte teljes mértékben meg lehet akadályozni a személyes adatokkal való visszaélést. Létezik ennek egy másik változata is, amely egy kódgenerátoron keresztül valósítja meg ugyanezt, ami szintén javasolt, ugyanakkor a fizikailag használt kulcs sokszor biztonságosabb. Egy másik hasznos szintén online beszerezhető termék, amelyet most név szerint nem nevezek meg, egy olyan eszköz, amelyet, ha a hálózatra csatlakoztatunk, csaliként lehet alkalmazni. Különböző országok közszférájában már rég óta alkalmazzák, de már elérhető a közönséges vásárlók számára is. Ez az eszköz egy könnyen feltörhető, sérülékeny rendszerként fog megjelenni, még ha nem is egy rendes számítógépes rendszer. Egy háztartásban számtalan számítógép, okos eszközök találhatóak és mind sebezhetőek. Mára annyi különböző felületen regisztráltunk, hogy nem változtatjuk meg a jelszavunkat minden esetben. Amennyiben egy olyan támadás érne minket, amely megpró-

7 Martin Casado: Cybersecurity and You, megtekintve 2021.08.18, https://a16z.com/2020/02/20/the-new-attack-surface-is-your-life/

8 Mi az a DDoS-támadás és hogyan védekezzünk ellene 2021, megtekitve: 2021.08.18 https://hu.safetydetectives.com/blog/mi-az-a-ddos-tamadas-es-hogyan-vedekezhetunk-ellene/#what

bálná megszerezni az azonosítóinkat, egy a korábban említett eszköz, csaliként szolgálhat, ezzel is megvédve a rendes eszközeinket. [9]

Természetesen, amennyiben eleget teszünk ezeknek, nem jelenti azt, hogy 100%-os biztonságban tudhatjuk magunkat. Ugyanakkor lecsökkentettük annak az esélyét, hogy áldozatok legyünk. Mint említettem, muszáj elhagynunk az *„Én úgy se esek áldozatul”* hozzáállást, mert mint már korábban ismertettem, számtalan eset történik nap mint nap.

7. Összegzés

Mindezek kapcsán talán a legfontosabb, amit tehetünk, a megelőzés. Tehát azzal, hogy telepítünk egy hiteles antivírus szoftvert, a különböző weboldalakon más-más, komplikált jelszavakat alkalmazunk, kétlépcsős hitelesítési eljárást alkalmazunk, valamint fordítunk pénzt, időt és energiát saját adataink biztonsága érdekében. Ne felejtsük el, hogy ne nyissunk meg gyanúsnak tűnő E-maileket, lehetőleg kerüljük a nyilvános internet hálózatokat.

Felhasznált irodalom

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

Koltay Tibor, Jávorszky Ferenc: A web 2.0 legfontosabb biztonsági fenyegetései In TMT 56. évf. 2009. 11–12.

2020 State of the Phish: An in-depth look at user awareness, vulnerability and resilience, 12.

Steve Morgan: Cybercrime To Cost the World 10,5 Trillion Annually by 2025, megtekintve:2021.08.18, https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

Josh Fruhlinger: Top cybersecurity facts, figures and statistics, megtekintve:2021.08.18, https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html

Conflicker and its legacy: An overview of the conflicker worm, megtekintve:2021.08.18 https://medium.com/@donovan.adams/what-is-this-confiker-y-you-speak-of-an-overview-of-the-conficker-worm-eb4997928107

Martin Casado: Cybersecurity and You, megtekintve 2021.08.18, https://a16z.com/2020/02/20/the-new-attack-surface-is-your-life/

Mi az a DDoS-támadás és hogyan védekezzünk ellene 2021, megtekintve: 2021.08.18 https://hu.safetydetectives.com/blog/mi-az-a-ddos-tamadas-es-hogyan-vedekezhetunk-ellene/#what

Joel de la Garza: 16 Steps to Securing Your Data (and Life), megtekintve: 2021.08.18, ,https://a16z.com/2019/11/12/16-steps-secure-you/

9 Joel de la Garza: 16 Steps to Securing Your Data (and Life), megtekintve: 2021.08.18, https://a16z.com/2019/11/12/16-steps-secure-you/

Tóth Tímea

Külföldi utazás során jelentkező kockázatok

1. Bevezetés:

A külföldre történő kiutazások mindig nagy örömet és izgalmat jelentenek legyen szó családi nyaralásról, tanulmányútról, külföldi konferencián való részvételről, Erasmus pályázatról esetleg munkavállalás céljából történő kiutazásról. Az ismert jogszabályok, ügyéntézés menete országonként más és más, emiatt, ha nem szeretnénk bonyodalmakba kerülni, legjobb ha körültekintően tájékozódunk és alaposan végig gondoljuk mire kell figyelnünk külföldi tartózkodásunk alatt, valamint milyen ismereteket kell szereznünk előtte. Ezekben szeretnék segíteni ebben a fejezetben.

A kockázatok a sebezhetőség és a veszély együttes megjelenéséből következnek. A veszély az az összetevő, melyre nincs ráhatásunk, nem tudunk tenni annak bekövetkezése ellen. Nagyon sokféle veszély érhet bennünket legyen az természeti katasztrófa, világméretű vírus, közúti baleset, támadás. Ezekre nem lehet felkészülni és nem is gondolunk rá a nap minden percében. A rendkívüli helyzetek nem jelezhetők előre, de vennek események, melyekre bizonyos mértékig felkészülhetünk. Ezért az országokat három fokozatú biztonsági kategóriába sorolták be, melyekről részletesebben a következő fejezetben írok.

A sebezhetőség a másik összetevő. Ez az az oldal, ami kivédhető, melyre fel tudunk készülni alapos körültekintéssel. A sebezhetőség kivédhetősége a felkészülésben rejlik. Egy külföldi országba való utazásunk előtt az általam összefoglalt gondolatok mentén felkészülhetünk, ez nagyban hozzájárulhat a biztonságos külföldi tartózkodásunkhoz.

2. Tervezés, utazás előtti teendők

Amikor eltervezésre kerül a külföldi utazás, első feladatunk a tájékozódás. A konzuli szolgálat honlapján minden fontos információ fel van tüntetve országonként. A következő linken elérhető oldalon (https://konzuliszolgalat.kormany.hu) tájékozódhatunk az adott ország biztonsági besorolásáról[1], éghajlatáról, gazdasági fejlettségéről, endémiás viszonyairól, helyi közlekedési szabályokról, szociális és politikai helyzetéről, a kiutazáshoz szükséges okmányokról, internetes és telefonszolgáltatók működéséről. Indulás előtt regisztrálhatunk konzuli védelemre. Ez nem más, mint egy egyszerű adatbejelentő, melyben megadjuk külföldi tartózkodásunk pontos helyét, utazásunk kezdetét és hazaérkezünk napját, így nyilvántartásba kerülünk. Egy esetleges vészhelyzet esetén segítségünkre lesz az állam, gondoskodik a hazajutásunkról, de mindenképpen pontos adattal rendelkezik arról, hogy külföldön tartózkodunk. Erről a következő linken kapunk bővebb információt: https://konzuliszolgalat.kormany.hu/az-allampolgarok-konzuli-vedelme

A következő oldalon van lehetőség regisztrálni a konzuli védelemre: https://konzinfougyseged.mfa.gov.hu/#!/login

1 Az országok biztonsági kategóriáinak meghatározását a Konzuli Szolgálat honlapján találjuk meg. A három fokozat közül a zöld, III. kategória, mely a legenyhébb besorolást kapja. Az e kategóriába tartozó országok közbiztonsági helyzete, szabályrendszere, közbiztonsága hasonló Magyarországéhoz. A II. kategóriát sárga színnel jelölik. Ebbe a biztonsági besorolásba tartoznak a fokozott biztonsági kockázatot rejtő országok, melyet meghatároz a járványveszély, háborús fenyegetettség, terrorista támadások veszélye, vagy más rendkívüli körülmény fennállásának lehetősége. Az I., piros színnel jelölt besorolás az utazásra nem javasolt országok kategóriája. Ez a legszigorúbb figyelmeztetés, mely az adott országban jelen lévő válsághelyzet, vegyveres összetűzések, háborús cselekmények, zavargások, természeti katasztrófák veszélyére hívja fel a figyelmet.

3. Az utazás tervezése

3.1 Utazási okmányok, vízum

Néhány országba elegendő a személyi igazolvány, máshova útlevél szükséges, bizonyos országokba vízumot is ki kell váltani. Természetesen az utazás célja is meghatározó lehet ez esetben, hiszen munkavállalás vagy tanulmányi célból történő kiutazás esetén nem elegendő a személyazonosító igazolvány, útlevéllel is rendelkezni kell bankszámla nyitáshoz. Erről időben tájékozódjunk, hiszen a vízum átfutási ideje heteket is igénybe vehet. Bizonyos országokba való utazás feltétele, hogy az útlevél a belépés idejétől számítva 6 hónapig érvényes legyen. Fontos továbbá, hogy a repülőjegynél megadott okmányunkat vigyük magunkkal. Néhány példa a fenti esetekre:

Személyazonosító igazolvány elegendő az utazáshoz:

- Az Európai Unió tagállamai: Ausztria, Belgium, Bulgária, Ciprus, Csehország, Dánia, Egyesült Királyság, Észtország, Finnország, Franciaország, Görögország, Hollandia, Horvátország, Írország, Lengyelország, Lettország, Litvánia, Luxemburg, Málta, Németország, Olaszország, Portugália, Románia, Spanyolország, Svédország, Szlovákia, Szlovénia.
- Az Európai Gazdasági Térség tagjaként személyi igazolvánnyal látogatható: Izland, Lichtenstein, Norvégia.
- További szerződés, megegyezés alapján: Andorra, Albánia, Koszovó, Bosznia-Hercegovina, Macedónia, Montenegró, Moldova - kivétel Dnyeszter-melléki Moldáv Köztársaság -, San Marino, Monaco, Svájc, Szerbia, Vatikán.

Kötelező az útlevél Fehéroroszországba, Ukrajnába, Törökországba és Oroszországba sőt, utóbbi a vízumot is megköveteli. Törökországban turisztikai céllal, 180 nap alatt 90 napot meg nem haladó tartózkodás vízum nélkül is lehetséges. Ugyancsak vízum- és útlevélköteles, népszerű célpont Kína, Mongólia, Thaiföld, Kuba, Jemen, Vietnám és az Egyesült Államok.

3.2 Repülőjegy, buszjegy, vonatjegy

A mai technikai eszközök lehetővé teszik, hogy menetjegyünket, repülőjegyünket QR-kód beolvasásával is érvényesíthetjük okoseszközeink segítségével. Ez nagyon kényelmes megoldás, de gondolnunk kell a kellemetlen kockázatokra is. Amennyiben netán lemerül telefonunk, nem árt, ha a biztonság kedvéért kinyomtatjuk a jegyeket, és azokat is magunkkal visszük.

3.3 Biztosítás, gyógyszerek

Utazásunk előtt mindig kössünk utasbiztosítást. Bármilyen esetleges baleset vagy megbetegedés esetén az ellátás vagy kezelés szükséges lehet, ami biztosítás ellenében visszatéríthető. Fontos meggyőződni róla, hogy a biztosítás kiterjed minden olyan tervezett tevékenységből eredő kockázatra, melyet végezni szeretnénk- legyen az búvárkodás vagy extrém vízi sport például. A biztosítás bizonylatát sem árt kinyomtatni és magunkkal vinni. Érdemes Európai Egészségbiztosítási Kártyát kiváltani, mert megkönnyíti az adminisztrációt. *„A magyar egészségügyi szolgáltatásra jogosult személyek, akik Magyarországon, vagy az Európai Unió más tagállamában rendelkeznek állandó lakóhellyel egy másik tagállamban a magyar egészségbiztosítás terhére vehetnek igénybe – orvosilag szükséges – egészségügyi szolgáltatásokat. Ezen ellátásokra való jogosultság az Európai Egészségbiztosítási Kártyával (a továbbiakban: Kártya) igazolható."*[2] A kártyát a következő linken

2 http://www.oep.hu/felso_menu/lakossagnak/ellatas_kulfoldon/az_europai_egeszsegbiztositasi_kartya/eu_kartya.html

lehet igényelni: http://neak.gov.hu/nyomtatvanytar/temp_sc_521884.html. Ezen kívül utazásunk előtt győződjünk meg róla, hogy ha vannak állandó gyógyszerek, melyeket használunk, legyen elegendő a külföldön tartózkodásunk idejére, valamint nem árt egy gyógyszeres csomagot magunkkal vinni a legszükségesebbekkel (fájdalomcsillapító, torokfertőtlenítő, széntabletta, ragtapasz, fertőtlenítő).

3.4 Gépjármű biztosítása

Amennyiben saját gépjárművel tervezzük az utazást, fontos előtte tájékozódjunk a megfelelő biztosításról. Bármilyen esetlegek baleset, koccanás esetén elengedhetetlen, hogy megfelelő biztosítása legyen. Indulás előtt ellenőrizzük a zöld kártya (a kötelező biztosítást igazolja) és a forgalmi engedély, egészségügyi alkalmasság érvényességét is. Sok országban előfordulhat, hogy a vezetési stílus eltér az általunk megszokottól, kellő óvatossággal, figyelemmel vezessünk külföldön. Külön kiemelném a balkáni és az arab országokat, ahol a KRESZ szabályai helyett a duda és az egyéni érdekek dominálnak. Itt jegyezném meg hogy a KRESZ szabályai is eltérőek lehetnek a hazaitól. Vannak országok, ahol az általunk megszokottól eltérően bal oldali közlekedés használatos. Arról, hogy mely országban miben térnek el az autóvezetés szabályai, a következő linken lehet tájékozódni: http://ec.europa.eu/transport/road_safety/going_abroad/index_hu.htm.

Az Európai Unió országaink kívül történő vezetéshez nemzetközi jogosítvány kiváltása szükséges. Ezt a következő linket tudjuk elintézni: https://magyarorszag.hu/szuf_fooldal#ugyleiras,7bd608a7-42ca-4c0c-8b15-29cf-3d0ec728,nemzetkozi_vezetoi_engedellyel_kapcsolatos_ugyinditas_-_tajekoztatas.

3.5 Szállásfoglalás

Kizárólag ellenőrizhető, felhasználók által értékelt, hivatalos oldalakon foglaljunk szállást. Ez sok kellemetlen helyzetet kiküszöböl. Amennyiben nem hotelt választunk, fontos, hogy utazás előtt több levelet váltsunk a szállásadóval, egyeztessük a pontos címet, ha előleget utalunk, vagy kifizetjük a teljes összeget, nyomtassuk ki a bizonylatot is.

3.6 Telefonszolgáltató, internet

Utazás előtt tájékozódjunk, hogy a célországban milyen szolgáltatási tarifák vonatkoznak a telefon és internethasználatra. Európai Uniós országokon kívül vásárolhatunk napijegyet, megy fix összegért korlátlan telefon és internethasználatot foglal magában. Ez nem minden országban elérhető. A mobilszolgáltatók oldalán fel van tűntetve, hogy mely országokban érvényes. Ha nem vásárolunk ilyet és Eu országon kívül tartózkodunk, fontos kikapcsolni a telefon beállításaiban a mobilinternet és az adatroaming szolgáltatást. A free wifi használatával is óvatosan bánjunk, de ezt az okostelefonok, okoseszközök veszélyei és fenyegetettségei, valamint a kiberbűnözés és adathalászat fejezet részletesen tárgyalja. Kizárólag megbízható hálózathoz csatlakoztassuk telefonunkat, laptopunkat.

4. További tájékozódás, felkészülés az utazásunk célországával kapcsolatban

A konzuli szolgálat oldalán a sárga és piros színnel jelzett I-es és II-es biztonsági besorolású országokba kizárólag egyéni felelősségvállalás mellett lehet kiutazni. Amennyiben ilyen helyre kívánunk látogatni, fontos, hogy legyünk tisztában csökkent biztonságunkkal és ennek tudatában kísérővel mozogjunk az országban, minden szabályt és előírást betartva. Ezen országok listája itt található: https://konzuliszolgalat.kormany.hu/utazasra-nem-javasolt-tersegek

Amennyiben tájékozódtunk az adott ország éghajlatáról, az adott évszak időjárásáról, vigyünk magunkkal az időjárásnak megfelelő ruhát.

Az endémiás[3] viszonyok, kötelező védőoltásokról való tájékozódás rendkívül fontos. Amennyiben a célországban olyan védőoltás beadását javasolják, mellyen nem rendelkezünk, a háziorvos felkeresése és a védőoltások beadatása igen fontos tényező. A speciális védőoltásokról tájékoztatást kaphatunk a Nemzeti Oltóközpont felkeresésével, ahol meg is kaphatjuk a szükséges vakcinát. Előfordulhat, hogy nem vagyunk védettek az adott betegséggel szemben, annak pedig súlyos következményei lehetnek.

Itt jegyezném meg, hogy az ételekkel is hasonló a helyzet. Ne együnk mosatlan gyümölcsöt és zöldséget, esetleg egzotikus, kétes higiéniás körülmények között készült ételeket, mert akár az életünkbe is kerülhet. Csak megbízható helyen, tiszta kézzel fogyasszunk el bármit is. Nem éri meg a kockázatot egy facebook-poszt arról, hogy például Mexikóban megesszük a pirított sáskát vagy Kínában a piacon egy nyers halat. Ugyanez a helyzet az ivóvízzel. Kizárólag palackos ásványvizet igyunk, fogmosásra is azt használjuk.

Kiutazásunk előtt tájékozódjunk helyi szokásokról, vallásról, nemzeti ünnepekről. Amennyiben a célország vallása megkövetelni, tartsuk be az öltözködési és viselkedési normákat. Nekünk kell alkalmazkodnunk a vendég ország szokásaihoz. Ez nem csupán illem, jómodor vagy a kultúra , vallás tisztelete, hanem sokkal több annál. Jelentős biztonsági kockázat, ha a szokásjogot vagy a vallásból eredő szabályokat figyelmen kívül hagyjuk. Ilyen például a muszlim vallású országokban a nők fejének és vállának eltakarása, a templomba, imaházba való szabályok betartása, az étkezési szokások figyelembe vétele.

A világ számos országában kommunikálhatunk angolul, de nem árt a legalapvetőbb köszönéseket és néhány szavas nyelvtudást szerezni az adott ország szókincséből. Ez gesztusértékkel is felér.

Utazáskor gyakran nem is gondolunk arra, hogy más országokban a hazaitól eltérő a hálózati feszültség, illetve a hálózati csatlakozók típusa is eltér attól, amit itthon megszoktunk. Számos országban emiatt hálózati átalakítót kell használnunk, és az sem mindegy, milyet. Mindenképpen járjunk utána ennek és szerezzük be a megfelelő átalakítót.

4.1 Politikai berendezkedés, gazdasági fejlettség

A felkészülés része, hogy nézzünk utána a célország politikai rendszerének, valamint az ország gazdasági helyzetének. Attól függően, hogy mennyi időre utazunk ki, elegendő pénzt vigyünk magunkkal. Az éttermek árai, a szolgáltatások árai szinte mindenhol kikereshetők, ez támpontot ad nekünk. A legmegfelelőbb, ha bankkártyát és készpénzt is viszünk magunkkal. Ezeket soha ne tartsuk egymás mellett, a készpénzt is több helyen tároljuk. A bankkártyáról készpénzt felvenni nem ajánlatos utcai atm-ben, sokkal biztonság egy bankfiókban felvenni. Bankkártyás fizetés esetén ellenőrizzük az összeget, mielőtt jóváhagynánk a fizetést.

4.2 Jogszabályok- hazai, közlekedési szabályok

Magyar állampolgárként külföldön a hazai és a külföldi jogszabályok is vonatkoznak ránk. Példának okáért, ha egy országban legális a könnyű drogok fogyasztása az adott ország állampolgárai számára, az nem jelenti azt hogy a magyar állampolgárok számára is az. Tehát ha egy ilyen országban legalizált drogot fogyaszt egy magyar állampolgár, az számára illegális, büntetendő cselekedet. Legyünk tisztában a törvényekkel, a jogainkkal, kötelezettségeinkkel és azokat külföldön is tartsuk be[4].

3 Egy fertőző betegség megszokott és rendszeres előfordulása egy adott népesség körében, egy meghatározott földrajzi területen. Ilyen például a malária Afrika déli részén.

4 *Területi és személyi hatály*

***3. §** (1) A magyar büntető törvényt kell alkalmazni*

a) a belföldön elkövetett bűncselekményre,

5. Külföldi tartózkodás egyéb kockázatai

5.1 Reptéri biztonság

A reptéren (természetesen máshol sem) soha ne hagyjuk! őrizetlenül poggyászunkat és figyeljünk a pontos indulásra. A gép indulása előtt két órával érkezzünk meg a reptérre. Sok kellemetlenségtől megkíméljük magunkat, ha elolvassuk és követjük az utazási tanácsokat. Ezeket a következő linken olvashatjuk: https://www.bud.hu/utazas/utazas_elott/poggyasz_es_biztonsagi_ellenorzes/utasbiztonsagi_ellenorzes

5.2 Külföldi bankkártyahasználat

Külföldi utazásunk előtt telefonon keressük fel bankunkat és jelentsük be a várható kiutazásunkat. Ennek elmulasztása esetén megtörténhet, hogy külföldi készpénzfelvétel vagy bankkártyás fizetés esetén automatikusan zárolják kártyánkat. Rendkívül óvatosan és alaposan átgondolva használjuk bankkártyánkat fizetés céljára. Nem szabad megfeledkezni arról sem, hogy a készpénzfelvételnek is díja van, mely függ a felvett összeg mennyiségétől . Banktól függően a következő linken lehet megtekinteni hogy mennyibe kerül ez a költség: https://www.napi.hu/magyar_vallalatok/bankkartya-kulfold-arfolyam.686581.html Utazásunk előtt győződjünk meg a kártya érvényességi idejéről, arról hogy a kártyahasználati limitek külföldön is érvényesek-e. Érdemes elmenteni azt a telefonszámot, mellyel külföldről is le lehet tiltani a bankkártyát amennyiben elveszítjük vagy ellopják tőlünk.

5.3 Külföldi vásárlások veszélyei

Legjobb, ha külföldön mindig van nálunk készpénz, valamint bankkártya is. Esetleges nem várt technikai probléma esetén jobb felkészülni arra, hogy hagyományos módon is fizetni tudjunk. A legújabb kártyákkal már érintéssel is fizethetünk, nem kell kiadni azt a kezünkből, ami egy távolkeleti bazárban nem tűnik biztonságosnak.

5.4 Külföldi szórakozás veszélyei

Külföldi szórakozás alkalmával az óvatosságot mindig tartsuk szem előtt. Kerüljük a túlzott mennyiségű alkohol fogyasztását, soha ne szakadjunk el társainktól, ne induljunk egyedül az éjszakába, illetve vissza a szállásra. Szórakozások alkalmával keletkező új barátságainkat kezeljük kellő óvatossággal, hiszen nem ismerjük múltjukat, előéletüket, szokásaikat, szándékaikat, vigyázzunk magunkra. Sokan rossz szándékkal próbálnak barátkozni, leitatni, bedrogozni, elcsábítani. Teendők bűncselekmény áldozatává válás esetén : Amennyiben külföldön bűncselekmény áldozatává válnánk, a következő szabályok vonatkoznak ránk és az ügy menetére: https://net.jogtar.hu/jogszabaly?docid=a0500135.tv

---

b) a Magyarország területén kívül tartózkodó magyar felségjelű úszólétesítményen vagy magyar felségjelű légi járművön elkövetett bűncselekményre,

c) a magyar állampolgár által külföldön elkövetett olyan cselekményre, amely a magyar törvény szerint bűncselekmény.

(2) A magyar büntető törvényt kell alkalmazni

a) a nem magyar állampolgár által külföldön elkövetett cselekményre is, ha az

aa) a magyar törvény szerint bűncselekmény, és az elkövetés helyének törvénye szerint is büntetendő,

ab) * állam elleni bűncselekmény, - kivéve a szövetséges fegyveres erő ellen elkövetett kémkedést és a kémkedést az Európai Unió intézményei ellen - tekintet nélkül arra, hogy az az elkövetés helyének törvénye szerint büntetendő-e,

ac) a XIII. vagy a XIV. Fejezetben meghatározott bűncselekmény, vagy egyéb olyan bűncselekmény, amelynek üldözését törvényben kihirdetett nemzetközi szerződés írja elő.

b) a magyar állampolgár, a magyar jog alapján létrejött jogi személy és jogi személyiséggel nem rendelkező egyéb jogalany sérelmére nem magyar állampolgár által külföldön elkövetett olyan cselekményre is, amely a magyar törvény szerint büntetendő.

(3) A (2) bekezdésben meghatározott esetekben a büntetőeljárás megindítását a legfőbb ügyész rendeli el.

6. Hazajutás esetleges nehézségei

A hazatérés joga minden állampolgárt megillet. Abban az esetben is, ha okmányait elvesztette vagy ellopták. Ilyen esetben a konzuli szolgálat segítségét kell kérni.

Ellopott/elveszett okmányok: Amennyiben megrongálódik, elveszik, ellopják okmányainkat, a konzuli szolgálat segítségét vehetjük igénybe. Erről minden információ megtalálható a következő oldalon: https://konzuliszolgalat.kormany.hu/uti-okmanyok-elvesztese-kulfoldon A külképviseletek elérhetőségét itt lehet megtalálni: https://www.kormany.hu/hu/kulgazdasagi-es-kulugyminiszterium/kulkepviseletek

7. Összefoglalás

Végezetül néhány gondolat. Ha külföldre utazunk, alázattal viselkedjünk az adott országban, a fent említett szokások és szabályok betartásával, hiszen vendégek vagyunk. Külföldön nem kizárólag saját magunkat, az iskolánkat, munkahelyünket, városunkat képviseljük, hanem Magyarországot. Bármilyen probléma, deviáns viselkedés, szabályszegés esetén nem azt fogják mondani, hogy XY tette, hanem azt, hogy a magyarok. Ez minősít bennünket ugyan, de legfőképpen az országunkat is. Felelősséggel tartozunk viselkedésünkért és a rólunk kialakított képért. Külföldön lenni sokszor más világ, az új élmények, színes helyek, eltérő kultúra lenyűgöző és varázslatos lehet számunkra, de soha nem szabad megfeledkezni a biztonságról sem.

Felhasznált irodalom

https://konzuliszolgalat.kormany.hu
https://konzuliszolgalat.kormany.hu/a-regisztraciorol
https://net.jogtar.hu/jogszabaly?docid=a1600073.tv
https://europa.eu/youreurope/citizens/travel/entry-exit/eu-citizen/index_hu.htm
https://eub.hu/veszelyes-a-kulfoldi-munkavallalas-es-tanulas/

NBSZK

NEMZETBIZTONSÁGI
SZAKKOLLÉGIUM

nbszk.head@0gmail.com

NemzetbiztonsagiSzakkollegium

nke_nbszk

nemzetbiztonsági-szakkollégium

Biztonság, védelem, nemzetbiztonsági tudatosság