HADMÉRNÖK
VÉDELEMINFORMATIKA
15. évfolyam (2020) 3. szám 179–196.
DOI: 10.32567/hm.2020.3.10

Horváth József[1]

A repülés elleni kibertámadás

Cyberattack Against Aviation

Korábbi cikkeimben több alkalommal foglalkoztam a repülés elektronikai zavarásával, ebbe beleértve az eddig már megtörtént esetek összegyűjtését, illetve a repüléssel kapcsolatos tevékenységek különböző helyszínein (repülőtéri rendszerek, repülésirányítás, radar- és kommunikációs rendszerek stb.) történő elektronikai zavarás hatásának elemzését. Ebben a cikkben a repülés elleni támadás egy másik módját, a napjainkban kiemelt témának számító kibertámadás eseteit vizsgálom. Számos példát lehet találni megtörtént esetekről, amelyek eddig nem okoztak tragédiát, azonban sajnos ez könnyen megtörténhet a jövőben. Ahhoz, hogy a jövőben alkalmazható védelmi megoldásokat találjunk, elemezni kell a már megtörtént eseményeket.

Kulcsszavak: **kibertámadás, hackertámadás, repülés, zsarolóvírus**

In my previous articles I have dealt with the electronic jamming of aviation several times, for instance, I collected and analysed the effects of electronic jamming at different locations of aviation related activities (airport systems, flight control, radar and communication systems, and so on). In this article, I investigate another type of attacks against aviation, a hot topic: cyberattacks. There are many examples of events that have not yet caused tragedy, but unfortunately this can easily happen in the future. In order to find future protection solutions, we need to analyse what has already happened.

Keywords: **cyberattack, hacker attack, aviation, ransomware**

Bevezetés

A cikk szorosan kapcsolódik a korábban végzett, a *Repülőterek, mint kritikus infrastruktúra védelme az elektronikai zavarás vonatkozásában* című kutatásomhoz. A kutatás során foglalkoztam a repüléssel és a repülőterekkel mint kritikus infrastruktúrával,[2] vizsgáltam az elektronikai zavarás valós eseteit,[3] illetve elemeztem az elektronikai zavarással történő támadás és az ellene történő védekezés lehetséges módjait.[4]

[1] Független szakértő, e-mail: horvath0101@gmail.com, ORCID: https://orcid.org/0000-0002-2743-3522
[2] Horváth József: A repülőtér, mint kritikus infrastruktúra. *Sereg Szemle,* 15. (2017), 3–4. 30–47.
[3] Horváth József: A repülés elektronikai zavarásának valós esetei. *Repüléstudományi Közlemények,* 30. (2018), 2. 7–24.
[4] Horváth József: *A repülés elektronikai zavarás elleni védelme.* Repüléstudományi Szemelvények, 2018. Elérhető: www.repulestudomany.hu/kiadvanyok/RepSzem-2018.pdf (A letöltés dátuma: 2019. 06. 04.)

Az elektronikai zavarás[5] az elektronikai hadviselés[6] egyik funkciójának, az elektronikai ellentevékenységnek[7] fontos területe, az elektronikai megtévesztés[8] és az elektronikai pusztítás[9] mellett. Az elektronikai hadviselés részletesebb bemutatása a téma vonatkozásában azért fontos, mert számos publikációban az elektronikai hadviselést a kiberhadviselés részeként sorolják fel. Itt fontos megjegyezni, hogy a „különböző katonai feladatok egyik alkotó eleme az elektronikai hadviselés (EHV), amely napjaink konfliktusaiban folyamatosan jelen van, a műveletтervezési folyamatokban és a feladatok végrehajtása során hatássokszorozó,[10] hatásnövelő képességként veszik figyelembe. Korábban az információs műveletek,[11] az ellenséges légvédelem lefogása[12] vagy a célmeghatározás/céltervezés[13] szerves alkotóelemeként tekintettek rá, míg napjainkban a gyakran emlegetett Anti-Access – Area-Denial (hozzáférést gátló – területmegtagadó, A2/AD) eljárás szerves részeként is kezelik."[14] Mind magyar,[15] mind külföldi kutatók[16] publikációiban is találhatunk utalást a kiberhadviselés és az elektronikai hadviselés közötti összefonódásra.

Napjaink egyik leggyakrabban emlegetett támadási módszere az informatikai rendszerek ellen alkalmazott kibertámadás. Számos magyar kutató foglalkozott már a repülés, a légiirányítás, a repülőterek elleni támadásokkal, illetve az ezen támadások elleni védelemmel,[17] akik elsődlegesen a korábbi években, évtizedekben jellemző támadási és védelmi megoldásokat vizsgálták, ebbe már beleértve a drónok alkalmazása által jelentett veszélyeztetettséget is.[18] Magyarország hálózati és információs rend-

5 Electronic Jamming, EJ.

6 Az elektronikai hadviselés „olyan hatás-alapú katonai tevékenységek/műveletek összessége, amelyek elektromágneses környezetben, az elektromágneses energia tudatos használatával biztosítják az elektromágneses műveletek részeként végrehajtott támadó és védelmi jellegű hatások/célok elérését". *Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína.* 2. kiadás. 2015.

7 „Az elektronikai zavarás az elektromágneses energia szándékos kisugárzása, visszasugárzása vagy visszatükrözése azzal a céllal, hogy korlátozza vagy megakadályozza az ellenség által használt elektronikai eszközök, berendezések és rendszerek rendeltetésszerű működését." *Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína* i. m. (6. lj.)

8 Electronic Deception, ED.

9 Electronic Neutralisation, EN.

10 A műveletтervezés során sok esetben az angol terminológiában alkalmazott „Enabler" szóval párosítják.

11 Information Operations, INFOOPS.

12 Suppression of Enemy Air Defence, SEAD.

13 Targeting, AAP-6 (2011).

14 Horváth József: *A Magyar Honvédség elektronikai hadviselési képességének fejlesztése szoftverrádiók alkalmazásával.* Doktori értekezés. Nemzeti Közszolgálati Egyetem, Budapest, 2018. Elérhető: www.uni-nke.hu/document/uni-nke-hu/horvath_jozsef_sandor_doktori_ertekezes_2018.pdf (A letöltés dátuma: 2019. 06. 04.)

15 Kovács László: Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232. Elérhető: www.hadmernok.hu/171_17_kovacs.pdf (A letöltés dátuma: 2019. 06. 04.)

16 Julian Turner: *The new battlefield: the race to integrate cyber and electronic warfare.* 2018. Elérhető: https://defence.nridigital.com/global_defence_technology_special/the_new_battlefield_the_race_to_integrate_cyber_and_electronic_warfare# (A letöltés dátuma: 2019. 06. 04.)

17 Szabó Sándor – Tóth Rudolf: Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények,* 25. (2013), 2. 89–113. Elérhető: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-07-Szabo_Sandor-Toth_Rudolf.pdf (A letöltés dátuma: 2019. 07. 06.); Balogh Zsuzsanna: AIGIS – A repülőterek védelmében. *Repüléstudományi Közlemények,* 23. (2011), 2. Klnsz. Elérhető: http://epa.oszk.hu/02600/02694/00055/pdf/EPA02694_rtk_2011_2_Balogh_Zsuzsanna.pdf (A letöltés dátuma: 2019. 07. 06.); Kovács Zoltán: Repülőtéri létesítmények fizikai védelme IED ellen. *Repüléstudományi Közlemények,* 26. (2014), 2. 106–113. Elérhető: http://epa.oszk.hu/02600/02694/00065/pdf/EPA02694_rtk_2014_2_106-113.pdf (A letöltés dátuma: 2019. 07. 08.)

18 Makkay Imre: Drónok harca. *Repüléstudományi Közlemények,* 27. (2015), 1. 61–72. Elérhető: https://epa.oszk.hu/02600/02694/00067/pdf/EPA02694_rtk_2015_1_061-072.pdf (A letöltés dátuma: 2019. 07. 10.)

szerek biztonságára vonatkozó stratégiája szerint a kibertér „globálisan összekapcsolt, decentralizált, folyamatosan változó elektronikus információs rendszerek, valamint ezen rendszereken keresztül adatok és információk formájában megjelenő társadalmi és gazdasági folyamatok együttesét jelenti".[19] A kibertámadás tehát e rendszerek és folyamatok elleni támadást jelenti.

Visszautalva az előző bekezdésben ismertetett elektronikai zavarásra, kihangsúlyoznám, hogy jelentős veszélynek értékelhető, és nehezen elhárítható, amennyiben egy repülőtér ellen azonos időben hajtanak végre kibertámadást és elektronikai zavarást.

Amennyiben általánosságban vizsgáljuk a kibertámadásokat, kijelenthető, hogy számos ok miatt hajtottak már végre ilyen támadást, az okok között szerepel a bosszú/megtorlás, az eltérő gondolkodásmód vagy vallás, illetve természetesen az anyagi haszonszerzés. A korábban végrehajtott kibertámadások között az egyik legismertebb ilyen eset az Észtország elleni támadás 2007-ben. Ennek kiváltó oka az a kormányzati döntés volt, miszerint a Tallinn középpontjában álló szovjet katona szobrát át kell helyezni a közeli katonai temetőbe. A szobor a helyi orosz kisebbségnek a felszabadítót, azt észt többségnek azonban az elnyomót képviselte. Az észt nacionalisták és az oroszbarát csoportok között is fontos vita zajlott a szoborral kapcsolatban. A szobor eltávolítása április 26-án kezdődött, a környéken békés tüntetések zajlottak, amelyek hamarosan erőszakos megmozdulásokká fajultak, ezek felett a rendőrség másnap reggelre szerezte vissza a kontrollt. A számítógépes támadások 2007. április 27-én kezdődtek, és 22 napon keresztül tartottak. A támadások során változatos módszereket alkalmaztak különböző méretben és szervezettségben, amelyek alapvetően a kormányzati szolgáltatások ellen irányultak. Mivel azonban a támadások sikeresen korlátozták ezeket a kormányzati rendszereket, az jelentős kihatással volt az átlagemberekre és az üzleti életre is.[20]

Az Észtország elleni támadás elkövetőjeként Oroszországot nevezte meg számos szakmai szervezet, azonban a különböző kibertámadásokkal kapcsolatban meg kell említeni számos egyéb csoportot, szervezetet is, így többek között a semelyik államhoz sem köthető Anonymous hackercsoportot, az Oroszországhoz kapcsolódó Fancy Bear csoportot, az Észak-Koreához kapcsolt Lazarus hackercsoportot, illetve az Amerikai Nemzetbiztonsági Ügynökséget.[21]

A repülés kibertámadással befolyásolható rendszerei

A repülés teljes folyamata során alkalmazott rendszereket, szolgáltatásokat számos szempont szerint lehet csoportosítani. Én az alábbi megbontást alkalmazom, kiegészítve a véleményem szerint még a témához kapcsolódó területekkel:

[19] 1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról. Elérhető: www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf (A letöltés dátuma: 2019. 07. 10.)

[20] Rain Ottis: *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: 2019. 09. 14.)

[21] National Security Agency, NSA.

- Repülőgépek, repüléshez kapcsolódó eszközök, rendszerek (repülőgépek és elektronikai rendszerei, radarok, radarrendszerek, világítórendszerek stb.) tervezése, gyártása, üzemeltetése.
- „A légitársasági utasfuvarozás, utashely-foglalás, tarifálás, jegykiállítás.
- Repülőtéri utaskezelés (induló- és átszállójegy-, valamint poggyászkezelés, beszállókártya és más forgalmi vonatkozások: repülőgép súly- és egyensúly-számítása, rakodástervezés, konténeres rendezés).
- Légiáru (cargo) -helyfoglalás, tarifálás, okmányolás, raktári funkciók, járat-előkészítés, különleges árukategóriák, valamint a cargo kapcsolatrendszere a nemzetközi ügynökségi disztribúcióval, vámmal, repülőtéri funkciókkal stb.
- Légitársasági és repülőtéri automatizálás (nemzetközi poggyászkeresés és adminisztráció, utast és poggyászt összekötő és biztonsági megfeleltető megoldások, fizikai poggyászosztályozás és -irányítás, járatinformációs rendszerek.
- Légitársasági operatív üzemirányítás (útvonal-, hálózattervezés, menetrend- és géprotáció-tervezés, menetrendszerkesztés és napi operatív menetrendi funkciók, repülőgépek műszaki karbantartásának tervezése és termelésirányítási rendszerek, hajózószemélyzet-tervezés és -vezénylés, navigációs rendszerek (útvonal- és üzemanyag-tervezés, repülési feltételek vizsgálata, például meteorológia), digitális föld–levegő kapcsolat)."[22]

Mint az a felsorolásból is látható és kikövetkeztethető, minden rendszerben ott van az informatika, minden eleme befolyásolható lehet, akár egy részegység működésének átprogramozásával, akár egy teljes rendszerbe történő behatolással és a rendszer irányításának átvételével. Lényeges az is, hogy egy társaság rendszere, a társaság méretétől függően akár az egész világra kiterjedhet. Minél nagyobb egy rendszer, annál sérülékenyebb, annál nehezebb a védelme, hiszen nem lehet mindenre kiterjedő védelmi rendszert üzemeltetni, annak humán, pénzügyi és technikai erőforrásigénye miatt. Természetesen nem szabad elfelejtenünk, hogy minden rendszerben ott van a legfontosabb összetevő, az ember is, aki a pszichológiai befolyásolás[23] célpontjává válhat.

Fontos azt is számításba venni, hogy a fenti rendszerek különböző, más szervezetek által üzemeltetett elemekkel, hálózatokkal vannak kapcsolatban. Az ezekben lévő informatikai hiányosságok, illetve az ezek ellen indított támadások hatása kihatással van a kapcsolódó más rendszerekre, szolgáltatásokra, így a repülésre is.

A repülés elleni támadások

Amikor a repülőterek és repülésirányítás sérülékenységét vizsgáljuk, számos természetes és mesterséges okot lehet felsorolni. Ernszt Ildikó *A nemzetközi légiközlekedés*

[22] Gonda Zsuzsanna: *Repülési informatika.* Bicske, SZAK, 2005.
[23] Social Engineering.

védelme című könyvében a légi terrorizmussal kapcsolatban az alábbi cselekményeket határozta meg mint elkövetési módokat:

- „repülőgép eltérítés;
- repülőterek elleni támadás;
- repülőgépek felrobbantása;
- repülőterek kiszolgáló területei elleni támadások;
- repülőgépek lelövése;
- egyéb, gépek ellen elkövetett bűncselekmények, incidensek, szabotázs akciók".[24]

Korábbi cikkemben számos esetet mutattam be végrehajtott fizikai támadásokról, illetve vizsgáltam elektronikai zavarással kapcsolatos incidenseket.[25] Fontos azt megjegyezni, hogy az elektronikai zavarással, illetve kibertámadásokkal kapcsolatban még nem történt haláleset, míg a fizikai támadások számos emberéletet követeltek. Ezen esetek közül megemlíthetjük az 1972. május 30-án az izraeli Lod repülőterén elkövetett támadást, amelynek 26, az 1975. december 29-én a New York LaGuardia repterén történt támadást, amelynek 11, az 1982. augusztus 7-én a török Esenboğa nemzetközi repülőtéren történt támadást, amelynek 9, az 1983. július 25-én, az Orly repülőtéren történt támadást, amelynek 8 halálos áldozata volt, a számos sérült mellett. Ezen esetek mellett több olyan esemény is történt, amelyek elemzésével számos tanulmány foglalkozott már, így a 2001. szeptember 11-i, az Amerikai Egyesült Államok ellen elkövetett repülőgép-eltérítéses támadás, illetve a 2016 márciusában Brüsszelben, a repülőtéren elkövetett kettős robbantás.[26]

Az Európai Uniós Hálózat- és Információbiztonsági Ügynökség[27] a repülőterek működését befolyásoló, rosszindulatú, szándékos tevékenységeket – beleértve a fizikai és az informatikai jellegű támadásokat is – az alábbiak szerint csoportosította:

- Túlterheléses támadás (Denial of Service [DoS]).
- Szoftverhiba kiaknázása.
- Jogok/jogosultságok nem megfelelő használata.
- Hálózati behatolás/támadás.
- Pszichológiai támadás (befolyásolás).
- Lehallgatás eszközökkel.
- Fizikai hozzáférés.
- Rosszindulatú szoftverek az informatikai eszközökön (beleértve a személyzet és az utasok eszközeit is).
- Fizikai támadás a repülőtér ellen.[28]

[24] Ernszt Ildikó: *A nemzetközi légiközlekedés védelme.* Károli Gáspár Református Egyetem, Állam- és Jogtudományi Kar, Budapest, 2010.
[25] Horváth (2018) i. m.
[26] *Öt híres reptéri terrortámadás.* 2016. Elérhető: http://mult-kor.hu/ot-hires-repteri-terrortamadas-20160322?pIdx=1 (A letöltés dátuma: 2019. 09. 14.); *Itt a biztonsági kamera felvétele az Orly repülőtéren történt támadásról.* Origo, 2017. Elérhető: www.origo.hu/nagyvilag/20170321-itt-biztonsagi-kamera-felvetele-a-parizsi-orly-repuloteri-tamadasrol.html (A letöltés dátuma: 2019. 09. 14.)
[27] European Union Agency for Network and Information Security, ENISA.
[28] ENISA. 2016.

A repülőterek tervezése és kialakítása című könyvben a szerzők külön fejezetben foglalkoznak a repülőtér létesítése során figyelembe veendő szempontokkal. A tervezés egyik eleme, hogy a repülőtér személyzete, a repülőtérrel kapcsolatban állók részt vegyenek egy közös gondolkodáson (brainstorming), amelyen azt elemzik, hogy hogyan lehetne a repülőteret megtámadni, és ez alapján alakítsanak ki védelmi megoldásokat. E szempontok között szerepel többek között az informatikai rendszer elleni behatolás tesztelése.[29]

A repülés elektronikai zavarásának valós esetei című cikkemben már foglalkoztam a repülés elemei (repülőgépek, repülésirányítás stb.) elleni támadásokkal, legfőképpen az elektronikai zavarás elemzésével. A fent említett cikkben részletesen bemutattam a megtörtént elektronikai zavarásokat, illetve érintőlegesen foglalkoztam a kibertámadásokkal is. A napjainkban megtörtént kibertámadásokat a következő alfejezetben mutatom be részletesen.

A repülés elleni kibertámadás valós esetei

Napjainkban a repülőterek ellen számos esetben követnek el kibertámadást, amelynek során elsődlegesen a földi kiszolgáló rendszerek elleni támadások a jellemzők. Ismertté vált kibertámadások a repülés vonatkozásában:

1. Atatürk és Sabiha Gökçen nemzetközi repülőtér, Isztambul, Törökország (2013.)

2013. július 26-án mindkét nemzetközi repülőtér működése órákra szünetelt, az útlevélkártya- és a bevándorlási rendszerek leálltak, illetve az induló gépek sem szállhattak fel. Helyi sajtóorgánumok szerint a rendszerleállás oka az Isztambuli Tartományi Biztonsági Rendszer elleni kibertámadás volt, azonban ezt a hivatalos szervek nem erősítették meg.[30]

2. Norwich nemzetközi repülőtér, Norwich, Egyesült Királyság (2015.)

Egy angol férfi az adatbázisok lekérdezésén alapuló SQL-injekcióval támadta a Norwich Nemzetközi Repülőtér weboldalát 2015 szeptemberében, a Norfolk és Norwich Egyetemi Kórház weboldalát pedig 2015 novemberében. A támadás során készített videókat feltette a YouTube videómegosztó oldalra, amelyekben lépésről lépésre bemutatta a támadásokat. Mivel kevés figyelmet fordított a biztonsági megoldásokra, a hatóságok képesek voltak visszakövetni az általa hagyott nyomokat, és őrizetbe vették. A bírósági tárgyaláson elmondta, hogy először tájékoztatta az érintett vállalatokat, azonban azok figyelmen kívül hagyták az emailjeit. A repülőtér weboldala három napig nem volt elérhető a támadás következtében, az okozott kárt közel 37 ezer GBP-re becsülték.[31]

[29] Penetration test, pentest.; Robert Horonjeff et alii: *Planning & Design of Airports.* McGraw-Hill Companies Inc., 2010.

[30] *Virus attack strikes at both Istanbul airports.* Doğan News Agency, 2013. Elérhető: www.hurriyetdailynews.com/virus-attack-strikes-at-both-istanbul-airports-51449 (A letöltés dátuma: 2019. 10. 20.)

[31] Catalin Cimpanu: *Hacker "His Royal Gingerness" Jailed for Cyber-Attack on UK Hospital, Airport.* 2017. Elérhető: www.bleepingcomputer.com/news/security/hacker-his-royal-gingerness-jailed-for-cyber-attack-on-uk-hospital-airport/ (A letöltés dátuma: 2019. 10. 20.)

3. Zaventem nemzetközi repülőtér, Brüsszel, Belgium (2016.)

2016. március 22-én, a több mint 30 halálos áldozatot követelő, a Zaventem repülőtéren, illetve a Maalbeek metróállomásnál elkövetett robbantásos ISIS[32]-merényletek után egy pittsburgh-i, 14 éves tinédzser hackertámadást indított a repülőtér weboldala ellen. A támadással kapcsolatban a hivatalos szervek kijelentették, hogy a fiatal nem terrorista indítékkal követte el az amúgy sikertelen támadást, bár további információt nem közöltek annak céljáról.[33]

4. Perth repülőtér, Perth, Ausztrália (2016.)

A 2016 márciusában végrehajtott támadás során egy vietnámi személy, felhasználva egy beszállító hozzáférési jogait, támadást indított Ausztrália negyedik legnagyobb repülőtere ellen. A repülőtér informatikai csapata értesítette az ausztrál kibervédelmi központot, valamint a rendőrséget. Közös erővel megállapították az elkövető személyét, illetve azt, hogy a támadás célja hitelkártyaadatok megszerzése volt, azonban a támadás során végül csak a repülőtér biztonsági rendszerével kapcsolatos iratokat szereztek meg. Radaradatok, illetve az utasok adatai nem voltak veszélyben.[34]

5. Heathrow repülőtér, London, Egyesült Királyság (2016.)

Bár nem kibertámadás a most ismertetett eset, azonban mindenképpen meg kell említenünk véleményem szerint. A Heathrow repülőtéren belső nyomozást indítottak, mivel Nyugat-Londonban találtak egy pendrive-ot, amelyen 2,5 GB-nyi biztonsági információ volt. Az adatok között térképek, videók, dokumentumok voltak, közte azon intézkedések, amelyekkel a brit királynőt és az általa használt repülőtéri utat védték.[35]

6. Chopin repülőtér, Varsó, Lengyelország (2016.)

2016 júniusában a varsói Chopin repülőtéren a repülőgépek földi kiszolgálását támogató – a LOT Lengyel Légitársaság[36] által működtetett – informatikai rendszert kibertámadás érte. A kibertámadás nem érintette a levegőben lévő gépeket, de a felszállásra tervezettek közül 10 járatot törölni kellett, illetve több gép esetében késések történtek. Mintegy 1400 utast érintett, közülük számos utasnak hotelt kellett keresnie.[37]

7. Ho Si Minh-város – Son Nhat és Hanoi – Noi Bai repülőterek, Vietnám (2016.)

2016 júliusában Vietnám két repülőtere, a Ho Si Minh-városban található Son Nhat és a Hanoiban található Noi Bai repülőterek elleni hackertámadással körülbelül 100 repülőgép menetrendjét befolyásolták a támadók. Bár a repülőterek üzemeltetésében kritikus rendszerelemekhez nem fértek hozzá, a repülőgépek indulását és érkezését

[32] Islamic State of Iraq and Syria, Irak és Szíria Iszlám Állama, ISIS.

[33] *Belgium: Pittsburgh Youth Linked To Cyberattack On Brussels Airport.* 2017. Elérhető: https://pittsburgh.cbslocal.com/2017/02/09/belgium-pittsburgh-youth-linked-to-cyberattack-on-brussels-airport/ (A letöltés dátuma: 2019. 10. 20.)

[34] Warwick Ashford: *Perth airport security plans stolen by Vietnamese hacker.* 2017. Elérhető: www.computerweekly.com/news/450431587/Perth-airport-security-plans-stolen-by-Vietnamese-hacker (A letöltés dátuma: 2019. 10. 20.)

[35] Warwick i. m. (34. lj.); Warwick Ashford: *Heathrow to probe leak of security files.* 2017. Elérhető: www.computerweekly.com/news/450429079/Heathrow-to-probe-leak-of-security-files (A letöltés dátuma: 2019. 11. 05.)

[36] LOT Polish Airlines.

[37] *Hacking attack grounds 1,400 passengers at Warsaw airport.* Deutsche Welle, 2015. Elérhető: www.dw.com/en/hacking-attack-grounds-1400-passengers-at-warsaw-airport/a-18530180 (A letöltés dátuma: 2019. 11. 05.)

mutató kijelzők használhatatlanok voltak, a jegykezelést pedig manuálisan végezték, mivel a „check-in" rendszer sem működött. A fenti okok miatt jelentős járatkésések alakultak ki.[38]

1. ábra

Várakozó utasok a Son Nhat repülőtéren a kibertámadást követően.

Forrás: *More than 100 flight delayed due to cyber-attacks at Vietnam's airports.* 2016. Elérhető: www.thanhniennews.com/society/more-than-100-flight-delayed-due-to-cyberattacks-at-vietnams-airports-64772.html (A letöltés dátuma: 2019. 11. 05.)

8. Bécs repülőtér, Ausztria (2016.)

2016 szeptemberében egy török hackercsoport indított támadást a bécsi repülőtér informatikai rendszere ellen, a csoport bejelentése szerint mintegy válaszul az iszlám és a török nemzet elleni támadás miatt. Az osztrák hatóságok szerint a támadási kísérletet sikerült elhárítani.[39]

[38] *More than 100 flight delayed due to cyber-attacks at Vietnam's airports.* 2016. Elérhető: www.thanhniennews.com/society/more-than-100-flight-delayed-due-to-cyberattacks-at-vietnams-airports-64772.html (A letöltés dátuma: 2019. 11. 05.)

[39] *Turkish hacker group says it was behind airport cyber attack.* 2016. Elérhető: www.thelocal.at/20160908/turkish-hacker-group-claims-responsibility-for-cyber-attack-on-airport (A letöltés dátuma: 2019. 11. 05.)

9. Boryspil nemzetközi repülőtér, Kijev, Ukrajna (2017.)

2017 júniusában Ukrajna számos vállalatát és szervezetét érte hackertámadás. A kormányzati szervek mellett a Nemzeti Bank és más nemzeti hitelintézetek, az ukrán Posta, az Antonov repülőgépgyár, a Csernobil zárt zóna, valamint a Kijevben található Boryspil nemzetközi repülőtér is a támadás áldozatává vált. Ebben az esetben a repülőtér hivatalos weboldala vált elérhetetlenné, illetve nem működtek a repülőgépek indulását és érkezését mutató kijelzők.[40]

10. Hartsfield-Jackson nemzetközi repülőtér, Atlanta, USA (2018.)

A repülőtér ellen elkövetett támadást „váltságdíj" megfizettetése érdekében követték el. Azért, hogy elkerüljék a teljes rendszeren történő elterjedést, a repülőtér biztonsági megoldásként lekapcsolta a wifihálózatát. Így képesek voltak megvédeni nemcsak a saját rendszereiket, de a repülőtéri szolgáltatók és az utasok eszközeit, rendszereit is.[41]

11. Cleveland Hopkins nemzetközi repülőtér, Cleveland, Egyesült Királyság (2018.)

A támadás eredményeképpen a repülőtér e-mail-fiókja, az utasinformációs és a csomagokkal kapcsolatos kijelzők váltak használhatatlanná. A hivatkozott forrás szerint zsarolóvírussal történt a támadás, a követelt összeget bitcoinban kérték.[42]

12. British Airways légitársaság (2018.)

2018. augusztus 21. – szeptember 5. között létezett egy biztonsági rés a légitársaság weboldalán és mobilapplikációjában, amelynek révén számos utas személyes és pénzügyi (bankkártya) adata került illetéktelen kezekbe. Az ellopott adatok között nem voltak útlevél- és utazási információk.[43]

13. Air Canada légitársaság (2018.)

A légitársaság bejelentése alapján 2018. augusztus 22. és 24. között szokatlan bejelentkezési tevékenységet észleltek, emiatt 1,7 millió felhasználói fiókot zároltak. E felhasználói fiókok közül kb. 20 ezer fiók adatait lophatták el, amelyek tulajdonosait tájékoztatták. A vizsgálat szerint az incidens egyik lehetséges oka az applikáció gyenge jelszórendszere volt, mivel 6-10 karakterből álló jelszavakat fogadott el, azonban csak betűt és számot, speciális karaktert nem. A probléma azért vált súlyossá, mert az ellopott adatok között nemcsak a különböző okmányok, bankkártyák számai voltak, de ezen okmányok másolatai is elérhetőek voltak, amennyiben az ügyfél feltöltötte azokat. Így ezen adatlopás következtében az ügyfelek még akár bankkártyacsalással is szembesülhetnek a jövőben.[44]

[40] Lizzie Dearden: *Ukraine cyber attack: chaos as national bank, state power provider and airport hit by hackers.* Independent, 2017. Elérhető: www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html (A letöltés dátuma: 2019. 11. 05.)

[41] Joseph De Avila – Cameron McWhirter: Atlanta Hit With Cyberattack. *The Wall Street Journal,* 2018. Elérhető: www.wsj.com/articles/atlanta-hit-with-cyberattack-1521823062 (A letöltés dátuma: 2019. 11. 05.)

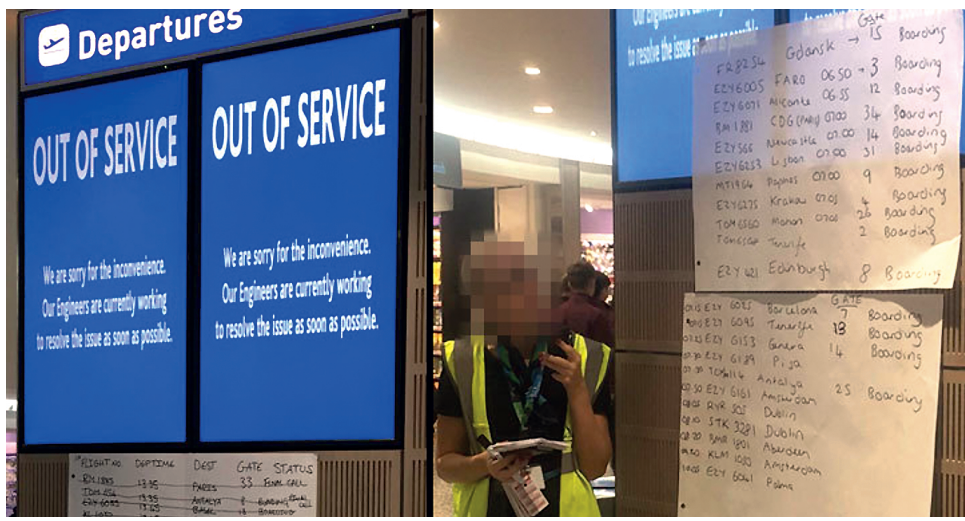
[42] Paul Orlousky: *City officials: No hacking, no ransom demanded in Cleveland Hopkins International Airport malware incident.* 2019. Elérhető: www.cleveland19.com/2019/04/26/live-ransomware-demand-is-behind-cyber-attack-cleveland-hopkins-airport/ (A letöltés dátuma: 2019. 11. 12.)

[43] *British Airways breach: How did hackers get in?* BBC News, 2018. Elérhető: www.bbc.com/news/technology-45446529 (A letöltés dátuma: 2019. 11. 12.)

[44] *Air Canada app data breach involves passport numbers.* BBC News, 2018. Elérhető: www.bbc.com/news/technology-45349056 (A letöltés dátuma: 2019. 11. 12.)

14. Bristol repülőtér, Bristol, Egyesült Királyság (2018.)

2018 szeptemberében elkövetett támadás következtében a repülőtéri utasinformációs rendszer kijelzői váltak használhatatlanná, így a repülőtéri dolgozók táblák segítségével próbálták az utasokat tájékoztatni mind a csomagfelvételről, mind az indulási időkről. A támadás során zsarolóvírust alkalmaztak az elkövetők, azonban a repülőtér illetékeseinek bejelentése alapján nem került kifizetésre semmilyen összeg. A támadás által okozott rendszerleállás két napig tartott, addigra sikerült azt helyreállítani. A repülőtér vizsgálatot indított annak kiderítése érdekében, hogy hogyan jutott be a vírus a rendszerbe.[45]



2. ábra

Szükségmegoldás az utasok tájékoztatására a bristoli repülőtéren, a kibertámadást követően.

Forrás: Wang i. m. (45. lj.)

15. Cathay Pacific légitársaság (2018.)

A Cathay Pacific légitársaság esetében vizsgálat indult az utasok adatainak helytelen kezelésével kapcsolatban, mivel az számos útlevélszám, bankkártyaszám kiszivárgását eredményezte.[46]

16. Isavia reptérüzemeltető vállalat, Reykjavík, Izland (2019.)

2019 júniusában az izlandi Isavia vállalat weboldalát érte elosztott túlterheléses támadás,[47] amelynek eredményeképpen az oldal több órára elérhetetlenné vált.[48]

[45] Wang Wei: *Ransomware attack takes down Bristol airport's flight display screens.* 2018. Elérhető: https://thehackernews.com/2018/09/cyberattack-bristol-airport.html (A letöltés dátuma: 2019. 11. 12.)

[46] *Cathay Pacific faces probe over massive data breach.* Reuters. 2018. Elérhető: www.reuters.com/article/us-cathaypacific-cyber/cathay-pacific-faces-probe-over-massive-data-breach-idUSKCN1NB0JY (A letöltés dátuma: 2019. 11. 12.)

[47] Distributed Denial of Service, DDoS.

[48] *Cyber attack on Isavia website.* 2019. Elérhető: www.isavia.is/en/corporate/news-and-media/news/cyber-attack-on-isavia-website (A letöltés dátuma: 2019. 11. 12.)

17. Ben Gurion nemzetközi repülőtér, Tel-Aviv, Izrael

A repülőtéren az év minden napján 24 órás munkarendben egy informatikai biztonsági műveleti központ[49] üzemel, amelynek feladata a jelentős számú támadási kísérlet elhárítása. A központ a repülőtér és a határátkelő biztonságáért felel, de nem felelős a repülőtársaságok biztonságáért, az a saját felelősségük. A forrás szerint napi 3 millió támadási kísérletet kell elhárítaniuk, amelynek nagy része bot támadás.[50]

18. A fedélzeti rendszer támadása a repülés során

Több publikációban is megjelent, hogy voltak próbálkozások a repülőgépek rendszerébe történő behatolásra. A Boeing cég nyilatkozata alapján a repülőgép utasainak szórakoztatására kialakított rendszer független a repülőgép repülési és navigációs rendszereitől, azaz hamisak azok a kijelentések, hogy azon keresztül támadhatók a létfontosságú rendszerek.[51]

19. Repülőtéri biztonsági rendszer számítógépéhez történő hozzáférés árusítása

A McAfee biztonsági cég fedezte fel és jelentette be, hogy egy orosz nyelvű online piactéren feltört számítógépekhez tartozó hozzáféréseket árusítanak. E számítógépek egyike egy amerikai repülőtér biztonsági és épületautomatizálási rendszeréhez tartozó számítógép, a vételár pedig 10 USD volt.[52]

Az ismertetett esetek elemzése és a repülés elleni informatikai támadások lehetséges okai

A repülés elleni kibertámadás hátterében számos ok állhat. A korábbi alfejezetben felsorolt példák esetében ismertettem a lehetséges indítékokat, amelyek között egyaránt megtalálható a kíváncsiságból, a támadó saját tudásának tesztelése érdekében elkövetett támadás, illetve ténylegesen bűnözői célú, például váltságdíjért elkövetett támadás. Több esetben történt az eltérő vallás vagy gondolkodásmód miatti támadás is.

Az informatikai támadások esetében mindenképpen meg kell említeni az etikus hackertevékenység kérdését is. Számos esetben lehet olvasni arról, hogy az elkövető – mint az a 2. számú esetben is történt – az első támadások, behatolások után tájékoztatta az érintett vállalatokat a biztonsági résekről. Egy adott idő elteltével ellenőrizte, hogy történtek-e lépések a felfedett biztonsági problémák megszüntetésével kapcsolatban. Mivel nem tapasztalt változást, újra és újra behatolt, ekkor azonban már módosításokat is végrehajtott. Ilyen esetek Magyarországon is történtek, különböző vállalatok vonatkozásában. Az elkövetők védekezésül azt hangoztatták, hogy ők jót akartak, illetve etikus hackerként tekintenek magukra. Ezen okok miatt

[49] Security Operations Center, SOC.

[50] Shoshanna Solomon: *Israeli airports fend off 3 million attempted attacks a day, cyber head says.* 2019. Elérhető: www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says/ (A letöltés dátuma: 2019. 11. 12.)

[51] Evan Perez: *FBI: Hacker claimed to have taken over flight's engine controls.* 2015. Elérhető: http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html (A letöltés dátuma: 2019. 11. 18.);

[52] Michael Kan: *Hackers Sold Remote Access to Major Airport for Only $10.* 2018. Elérhető: https://uk.pcmag.com/news-analysis/116329/hackers-sold-remote-access-to-major-airport-for-only-10 (A letöltés dátuma: 2019. 11. 18.)

mindenképpen fontos tisztázni, hogy mi is az etikus hacker feladata, milyen határok között tevékenykedik.

Az etikus hacker egy képzett informatikai szakember, aki rendelkezik a szükséges ismeretekkel, nemcsak az elvégzendő feladat szakmai részével, de a vizsgálandó rendszerrel kapcsolatban is. „Az etikus hackerek állhatnak munkaviszonyban, valamely vállalkozás alkalmazásában, de külsős partnerként, megbízási szerződéssel is elláthatják feladataikat. Bármelyik foglalkoztatási formában is dolgoznak, a vállalkozás és az etikus hacker között bizalmi kapcsolat jön létre, amelynek fenntartása mindkét fél érdeke, és amelyhez az etikus hacker részéről egy rendkívül erős titoktartási kötelem társul."[53] A fentiek alapján egyértelműen látható, hogy az öncélúan, a saját ismeretek tesztelése, alkalmazása során egy adott rendszerbe történő behatolás jogi értelemben nem fogadható el, annak jogi következményei alól a felfedett sérülékenység bejelentése sem mentesít. Fontos azt is figyelembe venni, hogy a teljes rendszer ismeretének hiányában az is előfordulhat, hogy tudtán kívül a behatoló a rendszerben komoly problémát generál.

Itt kell megjegyezni, hogy Magyarországon lehetőség van a feltárt informatikai biztonsági rések anonim módon történő bejelentésére. Jelenleg ezt a Nemzetbiztonsági Szakszolgálat Nemzeti Kibervédelmi Intézet honlapján keresztül lehet megtenni.

A 3. számú esetben véleményem szerint egyértelműen arról beszélhetünk – és ezt a nyilatkozatok is alátámasztják –, hogy a fiatal megpróbált úgymond a „zavarosban halászni", azaz olyan időpontban elkövetni egy támadást, amikor a felelős szervezetek valószínűsíthetően más problémával vannak elfoglalva, ebben az esetben a robbantások utáni helyzet feletti kontroll fenntartásával, visszaszerzésével. Egy másik lehetséges magyarázat pedig az lehet, hogy a káoszban elkövetett támadással nem publikus adatokhoz, információhoz akart volna hozzájutni.

Érdekes eset az adatok elvesztésével kapcsolatos 5. sz. incidens is. Ideális esetben az adatok lemásolás nélkül jutnak vissza az adatgazdához, azonban mivel ebben nem lehetünk biztosak, a teljes védelmi rendszert át kell dolgozni, ami jelentős erőforrást köt le, hiszen az új tervek kidolgozását követően a módosított eljárásokat be is kell gyakorolni. Mindenképpen vizsgálni kell ilyen esetben, hogy a pendrive-ra az adatok dokumentáltan kerültek-e fel, az hogyan kerülhetett ki az objektumból, illetve aggodalomra ad okot az is, hogy a pendrive nem volt titkosítva.

Az eltérő gondolkodásmód, más nemzet vagy ideológia elleni támadás példája a 8. számú pontban bemutatott, a bécsi repülőtér ellen elkövetett támadás.

A 13. és 15. számú esetek alapján azzal a problémával is foglalkozni kell, hogy az egyes szervezetek vajon elegendő erőforrásokat biztosítanak-e az információbiztonsági kérdésekre, megfelelő védelmi megoldásokat alkalmaznak-e.

A többi esetben egyértelműen a zsarolással történő pénzszerzés volt az indíték, emiatt szerepelt a célok között például a hitelkártyaadatok, személyes információk megszerzése. A kibertámadásokat általánosságban elemezve kijelenthető, hogy

[53] Horváth Katalin: Az etikus hacker szerzői jogi kockázatai. *Iparjogvédelmi és Szerzői Jogi Szemle,* 11. (2016), 4. 44–58. Elérhető: www.sztnh.gov.hu/sites/default/files/files/kiadv/szkv/szemle-2016-04/03-horvathkatalin.pdf (A letöltés dátuma: 2020. 01. 15.)

e támadások célja elsődlegesen pénzügyi adatok megszerzése. Egy 2018-ra vonatkozó elemzés szerint a kibertámadások 76%-a irányult erre a területre.[54]

A különböző célokat többféleképpen lehet csoportosítani, én a kutatásaim eredményeinek, valamint a korábban elvégzett „Etikus hacker" tanfolyamon szerzett ismereteim felhasználásával az alábbiak szerint kategorizáltam:

- pénzszerzés;
- információszerzés;
- saját tudás, képesség tesztelése:
  - elismertség;
  - tapasztalatgyűjtés;
  - erőfitogtatás;
  - hibafeltárás;
- politikai, ideológiai, vallási ok;
- szándékos károkozás.

A fenti felsorolás nem tükrözi az incidensek típus szerinti elosztását, mivel – figyelembe véve a korábbi tapasztalatokat – nagyon nehéz pontosan megállapítani a valós támadások számát. Ennek több oka is van, egyrészt nem minden esetben derül fény az elkövetett kibertámadásra, másrészt, ha a felhasználónak fel is tűnik, hogy valami nincsen rendben a rendszerével, nem biztos, hogy utánajár a dolognak, amennyiben a rendszere továbbra is használható. Erre egy példa az alábbi eset.

Az amerikai kormányzat, az amerikai repülési szervezetek és cégek, valamint a repülésben dolgozó személyek (pilóták, légiirányítók, mérnökök stb.) által üzemeltett, 1976-ban létrehozott, de azóta már nemzetközivé vált Légi Közlekedési Biztonsági Jelentési Rendszer[55] adatbázisában 2020. 04. 19-én a kibertámadással kapcsolatos keresőszavak[56] alkalmazása során a vírus szóra kaptam egyetlen informatikával összefüggő találatot. A 2018-ban, USA-ban történt eseményről készült jelentés alapján egy adatbázist tároló eszköz valószínűleg vírussal fertőződött, azonban ez nem volt tényszerűen alátámasztva, a jelentésben szerepel, hogy valaki mondta ezt a bejelentőnek. A bejelentő a napi munkája során látta, hogy az egyik ilyen eszközre kézzel írott papírra van felírva, hogy senki ne használja, azonban ez a papír néhány nap múlva már nem volt az eszközön. A bejelentő állítása szerint a papírt akár a szél is lefújhatta. A bejelentő nem tudta, hogy azok a repülőgépek, amelyekre ezt az adatbázist feltöltöltötték, megfertőződhettek-e a vírussal, illetve ha igen, az milyen hatással lehet a navigációs berendezésekre. A jelentés nem tér ki arra, hogy tettek-e további lépéseket az esettel kapcsolatban. Mivel a bejelentő nem tudta, mi lenne a teendő, jelezte az esetet az „Üzemeltetésnek".[57]

[54] Rob Mardisalu: *14 Most Alarming Cyber Security Statistics in 2019*. 2020. Elérhető: https://thebestvpn.com/cyber-security-statistics-2019/ (A letöltés dátuma: 2020. 04. 19.)
[55] Aviation Safety Reporting System, ASRS.
[56] Cyber, IT attack, malware, ransome, virus.
[57] *1508587 számú jelentés.* Aviation Safety Reporting System. Elérhető: https://titan-server.arc.nasa.gov/ASRSPublicQueryWizard/QueryWizard_Filter.aspx (A letöltés dátuma: 2020. 04. 19.)

Következtetések

Számos esetleírást lehet találni a repülés egyes elemei ellen elkövetett kibertámadásokról, amelyeket a fentiekben ismertettem. Véleményem szerint azonban további olyan esetek is lehetnek, amikor nem történt bejelentés, vagy észre sem vették, hogy kibertámadás történt az adott rendszer ellen. Ennek oka lehet egyrészt a felhasználók képzetlensége, azaz fel sem ismerik az árulkodó jeleket, másrészt a védelem kialakításának és fenntartásának költségei miatt a védelmi megoldások hiánya. Számos felmérés igazolta, hogy a legtöbb felhasználó – ebbe beleértve a magánszemélyeket és a vállalatokat egyaránt – az informatikával kapcsolatos védelmi költségeket általában megpróbálja alacsony szinten tartani.

Problémát jelent az is, hogy az elektronikai és informatikai rendszerek fejlődése töretlen, egyre jobban körbevesznek minket ezen eszközök és rendszerek közötti hálózatok, amelyek számos sérülékenységgel rendelkeznek. A sérülékenységek kiaknázására számos módszer létezik, az alkalmazandó eljárásokra a különböző internetes fórumokon, weboldalakon könnyen lehet oktatóanyagot találni. Számos leírásban olvasható az, hogy az egyes, hackerkedéssel foglalkozó személyek fórumokról, videómegosztó oldalakról szerzik ismereteiket, illetve itt osztják meg tapasztalataikat.

Véleményem szerint a repülés elleni kibertámadások ellenszerét – hasonlóan a más rendszerek ellen elkövetett kibertámadások elhárításához – ebben az esetben is a hatékony biztonsági rendszerek alkalmazásának és a felhasználók magas szintű informatikai ismeretének ötvözése jelenti. Véleményem szerint a felhasználók – ebbe beleértve a magánszemélyeket és a vállalatokat is – gondolkodásmódjában jelentős változást kell elérni, mivel mindenkinek el kell fogadnia, hogy a megfelelő védelem megvalósítása alapvető elvárás az informatikai rendszerek vonatkozásában. Ugyanezen felhasználókkal azt is el kell fogadtatni, hogy nem elég beszerezni a védelmi rendszereket, azokat naprakészen kell tartani és megfelelő tudással üzemeltetni kell.

Felhasznált irodalom

1508587. számú jelentés. Aviation Safety Reporting System. Elérhető: https://titan-server.arc.nasa.gov/ASRSPublicQueryWizard/QueryWizard_Filter.aspx (A letöltés dátuma: 2020. 04. 19.)

Air Canada app data breach involves passport numbers. BBC News, 2018. Elérhető: www.bbc.com/news/technology-45349056 (A letöltés dátuma: 2019. 11. 12.)

Balogh Zsuzsanna: AIGIS – A repülőterek védelmében. *Repüléstudományi közlemények,* 23. (2011), 2. Klnsz. Elérhető: http://epa.oszk.hu/02600/02694/00055/pdf/EPA02694_rtk_2011_2_Balogh_Zsuzsanna.pdf (A letöltés dátuma: 2019. 07. 06.)

Belgium: Pittsburgh Youth Linked To Cyberattack On Brussels Airport. 2017. Elérhető: https://pittsburgh.cbslocal.com/2017/02/09/belgium-pittsburgh-youth-linked-to-cyberattack-on-brussels-airport/ (A letöltés dátuma: 2019. 10. 20.)

British Airways breach: How did hackers get in? BBC News, 2018. Elérhető: https://www.bbc.com/news/technology-45446529 (A letöltés dátuma: 2019. 11. 12.)

Cathay Pacific faces probe over massive data breach. Reuters. 2018. Elérhető: www.reuters.com/article/us-cathaypacific-cyber/cathay-pacific-faces-probe-over-massive-data-breach-idUSKCN1NB0JY (A letöltés dátuma: 2019. 11. 12.)

Cimpanu, Catalin: *Hacker "His Royal Gingerness" Jailed for Cyber-Attack on UK Hospital, Airport.* 2017. Elérhető: www.bleepingcomputer.com/news/security/hacker-his-royal-gingerness-jailed-for-cyber-attack-on-uk-hospital-airport/ (A letöltés dátuma: 2019. 10. 20.)

Cyber attack on Isavia website. 2019. Elérhető: www.isavia.is/en/corporate/news-and-media/news/cyber-attack-on-isavia-website (A letöltés dátuma: 2019. 11. 12.)

Dearden, Lizzie: *Ukraine cyber attack: chaos as national bank, state power provider and airport hit by hackers.* Independent, 2017. Elérhető: www.independent.co.uk/news/world/europe/ukraine-cyber-attack-hackers-national-bank-state-power-company-airport-rozenko-pavlo-cabinet-a7810471.html (A letöltés dátuma: 2019. 11. 05.)

De Avila, Joseph – Cameron McWhirter: Atlanta Hit With Cyberattack. *The Wall Street Journal,* 2018. Elérhető: www.wsj.com/articles/atlanta-hit-with-cyberattack-1521823062 (A letöltés dátuma: 2019. 11. 05.)

Hacking attack grounds 1,400 passengers at Warsaw airport. Deutsche Welle, 2015. Elérhető: www.dw.com/en/hacking-attack-grounds-1400-passengers-at-warsaw-airport/a-18530180 (A letöltés dátuma: 2019. 11. 05.)

Horváth Katalin: Az etikus hacker szerzői jogi kockázatai. *Iparjogvédelmi és Szerzői Jogi Szemle,* 11. (2016), 4. 44–58. Elérhető: www.sztnh.gov.hu/sites/default/files/files/kiadv/szkv/szemle-2016-04/03-horvathkatalin.pdf (A letöltés dátuma: 2020. 01. 15.)

Ernszt Ildikó: *A nemzetközi légiközlekedés védelme.* Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar. Budapest. 2010.

Gonda Zsuzsanna: *Repülési informatika.* Bicske, SZAK, 2005.

Horváth József: A repülőtér, mint kritikus infrastruktúra. *Sereg Szemle,* 15. (2017), 3–4. 30–47. Elérhető: https://honvedelem.hu/files/files/110551/sereg-szemle_2017_3_4_internetre.pdf (A letöltés dátuma: 2019. 06. 04.)

Horváth József: A repülés elektronikai zavarásának valós esetei. *Repüléstudományi Közlemények,* 30. (2018), 2.7–24. Elérhető: http://epa.oszk.hu/02600/02694/00077/pdf/EPA02694_rtk_2018_02_007-024.pdf (A letöltés dátuma: 2019. 06. 04.)

Horváth József: *A repülés elektronikai zavarás elleni védelme.* Repüléstudományi Szemelvények, 2018. 9–24. Elérhető: www.repulestudomany.hu/kiadvanyok/RepSzem-2018.pdf (A letöltés dátuma: 2019. 06. 04.)

Horonjeff, Robert – Francis X. McKelvey – William J. Sproule – Seth B. Young: *Planning & Design of Airports.* McGraw-Hill Companies Inc., 2010.

Horváth József: *A Magyar Honvédség elektronikai hadviselési képességének fejlesztése szoftverrádiók alkalmazásával.* Doktori értekezés. Budapest, Nemzeti Közszolgálati Egyetem, 2018. Elérhető: www.uni-nke.hu/document/uni-nke-hu/horvath_jozsef_sandor_doktori_ertekezes_2018.pdf (A letöltés dátuma: 2019. 06. 04.)

Itt a biztonsági kamera felvétele az Orly repülőtéren történt támadásról. Origo, 2017. Elérhető: www.origo.hu/nagyvilag/20170321-itt-biztonsagi-kamera-felvetele-a-parizsi-orly-repuloteri-tamadasrol.html (A letöltés dátuma: 2019. 09. 14.)

Kan, Michael: *Hackers Sold Remote Access to Major Airport for Only $10.* 2018. Elérhető: https://uk.pcmag.com/news-analysis/116329/hackers-sold-remote-access-to-major-airport-for-only-10 (A letöltés dátuma: 2019. 11. 18.)

Kovács László: Az elektronikai hadviselés jelene és lehetséges jövője. *Hadmérnök,* 12. (2017), 1. 213–232. Elérhető: www.hadmernok.hu/171_17_kovacs.pdf (A letöltés dátuma: 2019. 06. 04.)

Kovács Zoltán: Repülőtéri létesítmények fizikai védelme IED ellen. *Repüléstudományi Közlemények,* 26. (2014), 2. 106–113. Elérhető: http://epa.oszk.hu/02600/02694/00065/pdf/EPA02694_rtk_2014_2_106-113.pdf (A letöltés dátuma: 2019. 07. 08.)

Magyar Honvédség Összhaderőnemi Elektronikai Hadviselés Doktrína. 2. kiadás. 2015.

Makkay Imre: Drónok harca. *Repüléstudományi Közlemények,* 27. (2015), 1. 61–72. Elérhető: https://epa.oszk.hu/02600/02694/00067/pdf/EPA02694_rtk_2015_1_061-072.pdf (A letöltés dátuma: 2019. 07. 10.)

Mardisalu, Rob: *14 Most Alarming Cyber Security Statistics in 2019.* 2020. Elérhető: https://thebestvpn.com/cyber-security-statistics-2019/ (A letöltés dátuma: 2020. 04. 19.)

More than 100 flight delayed due to cyber-attacks at Vietnam's airports. 2016. Elérhető: www.thanhniennews.com/society/more-than-100-flight-delayed-due-to-cyberattacks-at-vietnams-airports-64772.html (A letöltés dátuma: 2019. 11. 05.)

Orlousky, Paul: *City officials: No hacking, no ransom demanded in Cleveland Hopkins International Airport malware incident.* 2019. Elérhető: www.cleveland19.com/2019/04/26/live-ransomware-demand-is-behind-cyber-attack-cleveland-hopkins-airport/ (A letöltés dátuma: 2019. 11. 12.)

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: 2019. 09. 14.)

Öt híres reptéri terrortámadás. 2016. Elérhető: http://mult-kor.hu/ot-hires-repteri-terrortamadas-20160322?pIdx=1 (A letöltés dátuma: 2019. 09. 14.)

Perez, Evan: *FBI: Hacker claimed to have taken over flight's engine controls.* 2015. Elérhető: http://edition.cnn.com/2015/05/17/us/fbi-hacker-flight-computer-systems/index.html (A letöltés dátuma: 2019. 11. 18.)

Securing Smart Airports. European Union Agency For Network And Information Security, 2016. DOI: https://doi.org/10.2824/865081

Solomon, Shoshanna: *Israeli airports fend off 3 million attempted attacks a day, cyber head says.* 2019. Elérhető: www.timesofisrael.com/israeli-airports-fend-off-3-million-attempted-attacks-a-day-cyber-head-says/ (A letöltés dátuma: 2019. 11. 12.)

Szabó Sándor – Tóth Rudolf: Repülőterek kialakítása, létesítményeinek kritikus elemei, védelmük lehetséges műszaki megoldásai. *Repüléstudományi Közlemények,* 25. (2013), 2. 89–113. Elérhető: www.repulestudomany.hu/kulonszamok/2013_cikkek/2013-2-07-Szabo_Sandor-Toth_Rudolf.pdf (A letöltés dátuma: 2019. 07. 06.)

Turkish hacker group says it was behind airport cyber attack. 2016. Elérhető: www.thelocal.at/20160908/turkish-hacker-group-claims-responsibility-for-cyber-attack-on-airport (A letöltés dátuma: 2019. 11. 05.)

Turner, Julian: *The new battlefield: the race to integrate cyber and electronic warfare.* 2018. Elérhető: https://defence.nridigital.com/global_defence_technology_special/the_new_battlefield_the_race_to_integrate_cyber_and_electronic_warfare# (A letöltés dátuma: 2019. 06. 04.)

Virus attack strikes at both Istanbul airports. Doğan News Agency, 2013. Elérhető: www.hurriyetdailynews.com/virus-attack-strikes-at-both-istanbul-airports-51449 (A letöltés dátuma: 2019. 10. 20.)

Warwick, Ashford: *Perth airport security plans stolen by Vietnamese hacker.* 2017. Elérhető: www.computerweekly.com/news/450431587/Perth-airport-security-plans-stolen-by-Vietnamese-hacker (A letöltés dátuma: 2019. 10. 20.)

Warwick, Ashford: *Heathrow to probe leak of security files.* 2017. Elérhető: www.computerweekly.com/news/450429079/Heathrow-to-probe-leak-of-security-files (A letöltés dátuma: 2019. 11. 05.)

Wei, Wang: *Ransomware attack takes down Bristol airport's flight display screens.* 2018. Elérhető: https://thehackernews.com/2018/09/cyberattack-bristol-airport.html (A letöltés dátuma: 2019. 11. 12.)

Jogi forrás

1838/2018. (XII. 28.) Korm. határozat Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról. Elérhető: www.kormany.hu/download/2/f9/81000/Strat%C3%A9gia%20honlapon%20k%C3%B6zz%C3%A9t%C3%A9telre-20180103_4829494_2_20190103130721.pdf (A letöltés dátuma: 2019. 07. 10.)