HADMÉRNÖK
VÉDELEMINFORMATIKA

19. évfolyam (2024) 4. szám 167–182.
DOI: 10.32567/hm.2024.4.12

Paráda István,[1] Tóth András[2]

A NATO katonai légi szállítási képességek kibervédelmi aspektusai

Cybersecurity Challenges for NATO Military Air Transport Operations

Absztrakt

A légi közlekedési ágazat egyre nagyobb mértékben támaszkodik a technológiára, ami aggodalomra ad okot az államilag támogatott kibertámadásokkal kapcsolatban, ami a katonai és polgári légi közlekedés számára is kihívást jelent a kiberbiztonság terén. Ez a cikk a NATO katonai légi teherszállítási képességeit elemzi. A kutatás a releváns polgári légi közlekedési kibertámadásokat vizsgálja mint esettanulmányok, a NATO katonai légi szállítás potenciális kiberfenyegetései tükrében. Mindezeket összegezve a szerzők következtetéseket vonnak le azok hatásairól. Ezután elemző-értékelő módszerrel meghatározzák a kibertéri eszközök kategóriáit, amelyek kulcsfontosságúak a légi közlekedési informatikai infrastruktúra védelméhez, és katonai vonatkozásban kiemelik az IT-OT és Platform közötti különbségeket, átfedéseket. Ezenfelül mind a polgári, mind a NATO katonai légi közlekedési rendszereinek kibertámadásokkal szembeni hatékony védelme módjainak átfogó bemutatására törekednek, ami nélkülözhetetlen a biztonságos légi közlekedési rendszer biztosítása és a fejlődő kiberfenyegetések kezelése miatt.

Kulcsszavak: NATO katonai légi teherszállítási képességek, polgári légi közlekedési kibertámadások, Boeing, Airbus, kiberbiztonsági kihívások, IT-OT-Platform

[1] Informatikai műveleti tiszt, NATO Támogatási és Beszerzési Ügynökség, e-mail: paradaistvan@gmail.com
[2] Egyetemi docens, Nemzeti Közszolgálati Egyetem, e-mail: toth.hir.andras@uni-nke.hu

Abstract

The aviation industry's increasing reliance on technology has led to concerns about state-sponsored cyberattacks, which pose cybersecurity challenges for both military and civil aviation. This paper analyses NATO's military air cargo capabilities. It examines relevant civil aviation cyberattacks as case studies in light of potential cyber threats to NATO military aviation. Summarising these findings, the authors conclude their implications. They then use an analytical-evaluative method to identify categories of cyberspace assets that are key to protecting aviation IT infrastructure and highlight the differences and overlaps between IT-OT and Platforms in a military context. In addition, a comprehensive presentation of ways to effectively defend civil and NATO military aviation systems against cyberattacks will be presented, which is essential to ensure a secure aviation system and address evolving cyber threats.

Keywords: NATO military air cargo capabilities, civil aviation cyberattacks, Boeing, Airbus, cybersecurity challenges, IT-OT-Platform

Bevezetés

Ahogy a technológia egyre inkább integrálódik a légi közlekedési ágazatba, az olyan iparági és katonai szereplők számára, mint a NATO, elengedhetetlenné válik, hogy prioritást adjanak a kiberbiztonsági intézkedéseknek. Geopolitikai fronton az államilag támogatott kibertámadások egyre nagyobb aggodalmakat vetnek fel a lehetséges ártalmaik miatt. A digitális rendszerekre való fokozott támaszkodás azonban olyan kiberbiztonsági kihívásokat is jelent, amelyeket kezelni kell, különösképpen a katonai képességek szemszögéből vizsgálva.

A cikk legfontosabb kutatási kérdése, hogy a polgári légi közlekedésben az informatikai rendszerek és infrastruktúra kiberbiztonsági sebezhetőségeinek és fenyegetéseinek azonosítása, elemzése és kezelése milyen kihívásokat tartogat, különös tekintettel a NATO katonai légi szállítási képesség tükrében. A NATO katonai légi szállítási képességek részletes bemutatásának segítségével a kutatás célja az, hogy átfogó képet adjon a katonai légi szállításról és annak potenciális kiberbiztonsági sebezhetőségeiről. Az informatikai rendszerek integrációjának és a digitalizáció folyamatos térnyerésének köszönhetően a civil légi közlekedéshez hasonlóan a katonai légi közlekedési ágazat (és ezáltal a katonai légi szállítás) is egyre nagyobb kockázatnak van kitéve a kiberfenyegetésekkel szemben, ami nagymértékben befolyásolhatja a repülésbiztonságot és az üzemeltetést. E kiberfenyegetések kezelése érdekében a fejlett kiberbiztonsági protokollok és a személyzet folyamatos oktatása kulcsfontosságú lehet az informatikai infrastruktúra védelmében.

A kutatás során alkalmazott módszertanként elsődlegesen a nemzetközi és a kevésbé jellemző hazai releváns szakirodalmak és információt biztosító oldalak elméleti áttekintésével, feldolgozásával a NATO katonai légi szállítási képességének elemeit mutatjuk be. Mivel a NATO katonai légi szállítási képességek és a kiberbiztonság közötti kapcsolatot feltáró adatok és infomációk többnyire nem publikusak,

így elemzési módszertan, illetve esettanulmány a releváns polgári légi közlekedés és kibervédelem kapcsolatában jelenik meg a cikkben. Ezt követően vázoljuk a kiberbiztonság jelentőségét és kihívásait a katonai légi szállítási műveletekben, meghatározzuk a kibertéri eszközök kategóriáit, majd átfogó ajánlásokat teszünk a kockázatok lehetséges csökkentésére.

A NATO katonai légi szállítási képessége

A hatékony stratégiai légi szállítási képességek létfontosságúak annak biztosításához, hogy a NATO-szövetségesek és partnerek gyorsan be tudják vetni haderejüket és felszereléseiket, ahol szükség van rájuk. Ez az oka annak, hogy egyes NATO-szövetségesek és partnerek egyesítik erőforrásaikat annak érdekében, hogy a Szövetség profitálhasson a közösségből, az interoperabilitásból és a méretgazdaságosságból. Az erőforrások összevonása révén a NATO-országok a méretgazdaságosság előnyeit élvezik, és lehetőségük nyílik arra, hogy olyan eszközöket kollektíven szerezzenek meg, amelyek megvásárlása az egyes országok számára megfizethetetlenül költséges lenne.

Jelenleg három kezdeményezés létezik, amelyek célja a Szövetség és a részt vevő partnerországok stratégiai légi szállítási képességeinek biztosítása:

- a Stratégiai Légi Szállítási Megoldás (SALIS) kezdeményezés,
- a Stratégiai Légi Szállítási Képesség (SAC)
- és a Multinacionális Többfeladatú Tanker Szállítási (MRTT) Fleet (MMF).

Minden program sokoldalú és rugalmas képességeket kínál, beleértve a NATO-műveletek és -küldetések támogatását, orvosi segítség szállítását, polgári és katonai betegek evakuálását, polgári és katonai felszerelések szállítását, humanitárius segélynyújtást katasztrófák után és levegő-levegő utántöltés biztosítását. A NATO stratégiai légi szállítási kezdeményezései közé tartozik a szoros együttműködés más nemzetközi szervezetekkel, köztük az Európai Unióval (EU), az Egyesült Nemzetek Szervezetével (ENSZ) és az Afrikai Unióval (AU).[3]

SALIS

A Strategic Airlift International Solution (SALIS) kilenc ország támogatási partnersége, amely Antonov AN–124–100 típusú repülőgépeket bérelve garantált hozzáférést biztosít akár öt repülőgéphez – ezek közül három válság esetén néhány napon belül küldetésre készen áll, kettő a rendelkezésre állás függvényében – nemzeti, NATO- és EU-műveletek és -küldetések támogatására. A Támogatási Partnerség – amelyet a NATO Támogatási és Beszerzési Ügynökség (NSPA) kezel – egy többnemzetiségű együttműködési mechanizmus, amelyet két vagy több NATO-tagország kezdeményezésére hoztak létre, amelyek közös támogatási és szolgáltatási tevékenységeket kívánnak szervezni. 2021 októberében az NSPA ötéves szerződést írt alá a németországi

[3] NATO 2024a.

székhelyű Antonov Logistics Salis céggel. Ez felváltja a korábbi SALIS-szerződéseket, amelyek közül az utolsó 2021 decemberében járt le. A jelenlegi szerződés az AN–124-es[4] repülőgépeken kívül más nagy teherszállító repülőgépeken is rakománykapacitást biztosít, beleértve az IL–76-ot,[5] a készlet erejéig. E szerződés értelmében a SALIS-ban részt vevő országok garantált hozzáférést kapnak a stratégiai légi szállítási képességekhez a túlméretezett rakományok esetében, az éves repülési órakvóta alapján. A képességet napi szinten a Stratégiai Légiszállítási Képesség koordinálja, amely a hollandiai Eindhovenben található európai mozgáskoordinációs központtal (MCCE) közösen működik. Az NSPA kezeli a SALIS szerződést a részt vevő országok nevében, és támogatást nyújt a SALIS Támogatási Partnerségnek.[6]

SAC

A második kezdeményezés, amelynek célja a NATO-szövetségesek és partnerek számára a stratégiai légi szállításhoz való hozzáférés biztosítása, a Stratégiai Légiszállítási Képesség (SAC), amely három Boeing Globemaster III C–17[7] szállítórepülőgépet vásárolt a 12 NATO-szövetségesből álló csoport nevében. Az első C–17-est 2009 júliusában adták át, a második és a harmadik repülőgép 2009 szeptemberében és októberében követte. A légi járművet a Magyar Honvédség 47. Repülőbázisán Pápán a SAC hadműveleti ága, a katonai Heavy Airlift Wing (HAW) üzemelteti. A Stratégiai Légiszállítási Képesség (SAC) egy multinacionális kezdeményezésben részt vevő három katonai Boeing C–17 Globemaster III nagy hatótávolságú teherszállító repülőgépből álló egység, amely megfelel a stratégiai és taktikai légi szállítási követelményeknek. Minden tag nemzete a rendelkezésre álló repülési órák egy részét birtokolja, amit a nemzeti NATO-, ENSZ- és EU-vállalásaik teljesítésére használnak fel. A legújabb fejlemények közé tartozik, hogy a SAC-nemzetek C–17 repülőgép-kiképzési szimulátor üzembe helyezését teszik lehetővé a pápai repülőbázison. A szimulátor kezdeti működési képessége a tervek szerint 2025.[8] A HAW-t az összes részt vevő ország katonai személyzete működteti, és küldetései támogatják a nemzeti követelményeket. A műveletek közé tartozott a Nemzetközi Biztonsági Segítő Erők (Afganisztán), a Koszovói Erők (KFOR), a líbiai Unified Protector hadművelet támogatása, a Haitin és Pakisztánban nyújtott humanitárius segítség, az afrikai békefenntartás, valamint a lengyel hatóságoknak nyújtott segítség a szmolenszki légi katasztrófát követően Oroszországban. Két humanitárius

[4] Az Antonov An–124 Ruszlan (NATO-kódja: Condor) a kijevi Antonov tervezőirodában az 1970-es évek második felében Viktor Tolmacsov főkonstruktőr irányításával kifejlesztett, teljesen fémépítésű, félhéjszerkezetű, felsőszárnyas elrendezésű, behúzható futóművel rendelkező, kétáramú gázturbinás sugárhajtóművel, hermetikusan zárható kabinnal és nem hermetikus tehertérrel rendelkező, merevszárnyú teherszállító repülőgéptípus.

[5] Az Il–76 a Szovjetunióban, az Iljusin tervezőirodában az 1960-as évek végén kifejlesztett négyhajtóműves közepes teherszállító repülőgép.

[6] Hood 2009.

[7] A C–17 Globemaster III (beceneve: Moose = „Jávorszarvas") az amerikai McDonnell Douglas, majd később a Boeing Integrated Defence Systems által kifejlesztett, részben fém, részben kompozit anyagokból épített, félhéjszerkezetű, felsőszárnyas, behúzható futóművel, nagy kétáramúsági fokú gázturbinás sugárhajtóművekkel, hermetikusan zárható kabinnal és tehertérrel rendelkező, harcászati teherszállító feladatkörre kifejlesztett, a levegőben utántölthető, nagy hatótávolságú (stratégiai), merevszárnyú teherszállító repülőgéptípus.

[8] Szarvas 2008: 72–74.

SAC-repülést szerveztek a 2017-es Irma hurrikán után Barbadoson és Guadalupe-on elszenvedett áldozatok megsegítésére. A SAC emellett alapvető egyéni védőfelszereléseket szállított több tagjának a Covid–19 2020-as csúcspontja idején. 2021-ben a SAC járatokat küldött Afganisztánba, hogy evakuálják az embereket (a szövetséges és a partnerországok, valamint a NATO-hoz és a SAC-hoz kötődő afgánok személyzetét) az afgán kormány és az afgán nemzetvédelmi és biztonsági erők összeomlását követően. 2022-ben a SAC tűzoltó egységeket szállított Romániából Franciaországba, hogy segítsenek az erdőtüzek leküzdésében. A Törökországot 2023 februárjában sújtó pusztító földrengésekre válaszul a SAC kilenc küldetést hajtott végre, hogy Finnország, Hollandia, Románia, Svédország és az Egyesült Államok nevében 340 tonna sürgős felszerelést és személyzetet szállítson az országba.[9]

A HAW multinacionális repülőszemélyzete a C–17-es légi és szárazföldi küldetések teljes spektrumát biztosítja, beleértve a légi utántöltést, ejtőernyő-ledobást, rohamleszállást és minden időjárási körülmények közötti műveleteket, nappal vagy éjszaka alacsony és közepes fenyegetettségű környezetekben. A HAW több mint 30 000 órát repült, és kiemelkedően magas (> 80%) átlagos küldetési képességet ért el a SAC flottájában a NAM karbantartás támogatásával. A magas bevetési képességi arány azt jelenti, hogy a repülőgépek készen állnak a SAC nemzet küldetésének késedelem nélküli végrehajtására. A HAW minden kontinensre szállított rakományt, és szállított utasokat.[10]

A NATO Légiszállítási Program (NAMP) egy multinacionális szervezet a NATO támogatási és beszerzési programján belül. A NAMP kezeli és támogatja a C–17-es flottát, amelynek repülőgépei Magyarországon vannak bejegyezve. A NATO nemzetközi állománya a NAMP szervezeti struktúrán belül pénzügyi, logisztikai és adminisztratív szolgáltatásokat nyújt a Heavy Airlift Wing számára. A Heavy Airlift Wing felelős a küldetések végrehajtásáért az előre egyeztetett repült óraelosztásnak megfelelően. A multinacionális SAC Irányítóbizottság átfogó felelősséggel tartozik a program irányításáért és felügyeletéért, és meghatározza a követelményeket. A NATO Támogatási és Beszerzési Ügynökség (NSPA) Légiszállítási Programja (NAMP) kezeli és támogatja a SAC légi szállítási eszközeit, valamint adminisztratív támogatást nyújt a pápai légi bázison működő Heavy Airlift Wing számára.[11]

MRTT

A Multinacionális Többfeladatú Tanker Transport (MRTT) Fleet (MMF) stratégiai szállítási, légi utántöltési és egészségügyi evakuálási lehetőségeket biztosít a részt vevő országok számára. A program az egyetértési megállapodásban (Memorandum of Understanding) körvonalazott összevonási és megosztási koncepción alapul, amelyben a részt vevő országok összevonják a repülőgépeket és megosztják a költségeket, miközben kihasználják a méretgazdaságosság előnyeit. A 111 tonnás alapüzemanyag-kapacitás

[9] Nyitrai 2016: 80–81.
[10] Siposné 2019: 32–33.
[11] Szászi 2015: 221–223.

lehetővé teszi, hogy a repülőgépek kiválóan teljesítsenek a levegő-levegő utántöltési feladatokban anélkül, hogy további üzemanyagtartályokra lenne szükség. Ezenkívül körülbelül 2200 liter/perc maximális üzemanyag-áramlási sebességet tud biztosítani egy gém vagy egy tömlő és szívócső segítségével, és gyorsan meg tudja tölteni az összes, az MMF-országokban készleten lévő és a legtöbb NATO-n belül használt repülőgépet (F–16, F–35, C–17, Eurofighter, Tornado és Gripen).[12]

Az MRTT-flotta a NATO egyik jól látható projektje, amelynek célja a felszerelések, a képzés, a doktrínák és az eljárások egységességének kiaknázása a méretgazdaságosság és az interoperabilitás biztosítása érdekében. A flotta a NATO tulajdonában van, és a NATO Támogatási és Beszerzési Ügynöksége (NSPA) irányítja. Az NSPA MMF csapata az NSPA központjában található, Capellenben, Luxembourgban, de mások más helyekről is nyújtanak támogatást, például Eindhovenből, Köln-Wahnból, Bonnból és Getaféből. Az NSPA ezt a támogatást a részt vevő országoknak a Multinacionális Többfeladatú Tanker Szállítási Flottatámogató Partnerségen keresztül biztosítja.

A flottát a részt vevő országok katonáiból álló Multinacionális Többcélú Tanker Transport Unit (MMU) üzemelteti. Az egység székhelye a hollandiai Eindhovenben található Fő Operatív Bázison (MOB) és Kölnben, a Forward Operating Base-en (FOB) található.[13]

1. táblázat: A NATO légi szállítási képességek repülőgépeinek összehasonlítása

NATO légi szállítási képesség	**SAC**	**MRTT**	**SALIS**
Repülőgéptípus	Boeing Globemaster III C–17	Airbus A330–200	Antonov An–124–100
Hosszúság	53,04 m	59 m	68,96 m
Szárnyfesztávolság	51,74 m	62 m	73,3 m
Magasság	16,79 m	16,8 m	21,08 m
Maximális felszálló tömeg	265 352 kg	242 000 kg	405 000 kg
Teherszállítási/utaskapacitás	77 500 kg – 170 000 kg	253–277 utas	150 000 kg
Maximális sebesség	830 km/h	913 km/h	850 km/h

Forrás: a szerzők szerkesztése

A kiberbiztonság jelentősége és kihívásai a polgári és katonai légi szállítási műveletekben

A polgári légi közlekedési szektor elleni támadás az előző fejezetben is részletezett NATO katonai képességekre is hatással lesz, ezért átfogó választ igényel. A polgári és katonai légi közlekedési rendszerek kölcsönös függősége miatt a kibertámadás ellen egyik sem védekezhet elszigetelten. Az új fejlett technológiák és kommunikációs rendszerek fejlődésével a kézi folyamatok helyett a hatékonyabb automatizált

[12] NATO 2022: 1–2.
[13] Oppelaar 2023: 25–31.

folyamatok, kommunikáció és tárolás irányvonal a meghatározó. Ezek a technológiai fejlesztések növelik a légi forgalmi irányító rendszer kapacitását és javítják a biztonságot. A következő polgári képességek azonban szintén jelentős kibervédelmi aggályokat vetnek fel, és ha összekapcsolódnak, hatással lesznek a NATO műveleti képességeire.

A mai digitális korban a katonai műveletek nagymértékben támaszkodnak fejlett technológiákra és hálózati rendszerekre. Az előző fejezetben említett katonai légi szállítási képességek döntő szerepet játszanak a globális mobilitásban és az erőkivetítésben, lehetővé téve a személyzet, a felszerelés és a készletek gyors mozgását. Ahogy a katonai légi szállítási képességek technológiailag fejlettebbé válnak, a kiberfenyegetésekkel szemben is sebezhetőbbek. A fejlődő kiberfenyegetettségi környezet jelentős kockázatokat hordoz a katonai légi szállítási képességekre nézve. Látható tehát, hogy a kockázatkezelés egyre inkább tudományos alapokra helyeződve nyújt segítséget, különösen az informatikai rendszerek,[14] ezáltal a légi szállítási képességek sebezhetőségének kezelése terén. Az ellenfelek, az államilag támogatott szereplőktől a hacktivistákig, igyekeznek kihasználni a hálózati rendszerekben rejlő sebezhetőségeket. A katonai légi szállítási képességek elleni sikeres kibertámadásnak messzemenő következményei lehetnek, beleértve a stratégiai szállítási műveletek megzavarását, az érzékeny információk ellopását, a küldetéstervezési rendszerek kompromittálását vagy a repülőgépek repülési irányításának szabotálását. Ezért a robusztus kibervédelem fenntartása elengedhetetlen a katonai légi szállítási műveletek biztonságának és ellenálló képességének biztosításához. A jelenlegi konfliktusok és jövőbeli válságok valószínűleg tartalmaznak kiberelemeket. A NATO műveletei nagymértékben támaszkodnak a számítógépes hálózatokra, ezért a kibertér figyelembevétele a biztonság kiépítése és fenntartása során alapvető követelmény. A kibertér saját területként való elismerésének következményei a Szövetség fókuszát az „információbiztosítás" helyett a „küldetésbiztosítás" felé helyezték át. A kibervédelmet túl gyakran a biztonság és a hadviselés önálló megközelítéseként értelmezik. Az ukrán válság megmutatta, hogy a kibervédelmet átfogóbb stratégiai és operatív koncepcióba kell integrálni.[15]

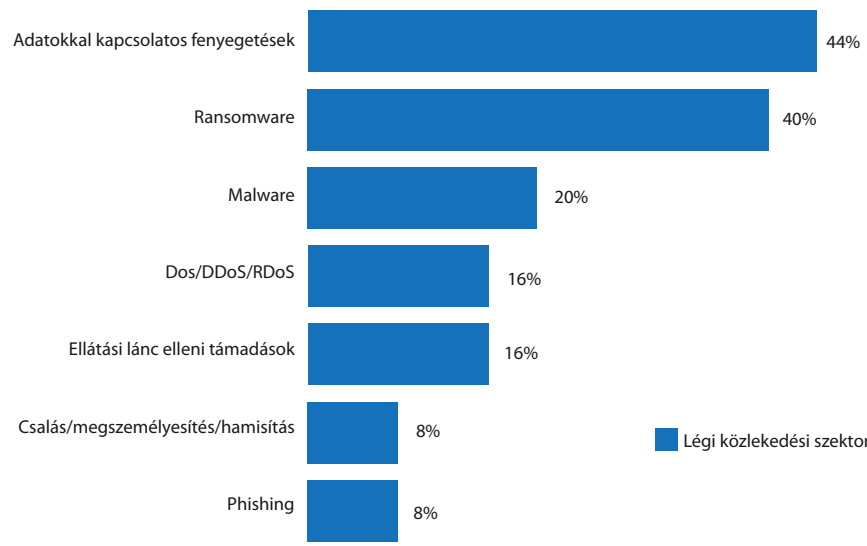
Polgári légi közlekedési kibertámadások kronológiája a NATO katonai légi szállítás potenciális kiberfenyegetései tükrében

A nemzeti légi közlekedési rendszerek kiberfenyegetésekkel szembeni védelme az állam előjoga és felelőssége. Nemzetközi dimenziója azonban megköveteli olyan iránymutatások és eljárások kidolgozását és végrehajtását, amelyek elősegíthetik a globális légi közlekedési rendszer zökkenőmentes rugalmasságát. A globális légi közlekedési rendszer az információs és kommunikációs technológia egyik legösszetettebb és legintegráltabb rendszere a világon. Kritikus infrastruktúraként potenciális kibertámadási célpont. A repülést fenyegető kiberalapú fenyegetések fejlődnek, és számuk növekszik, és ezek a fenyegetések számos forrásból származhatnak, beleértve a bűnözői és terrorista csoportokat, külföldi nemzeteket, bennfenteseket és másokat. Meg kell

[14] Megyeri–Farkas 2017.
[15] Bhargava 2024: 90–93.

érteni, hogy az információs rendszerek közötti növekvő összekapcsolhatóság egyre nagyobb lehetőségeket kínál a kibertámadások számára. Azt is meg kell jegyezni, hogy a polgári és katonai repülés felhasználói és érdekelt felei közötti kölcsönös függőségek növelik a köztük lévő bizalom szükségességét, mivel a légi forgalmi irányítási rendszer képessége a kibertámadások elleni védekezésre csak annyira jó, mint a leggyengébb láncszem a légi közlekedésben. A légi forgalmi irányítási rendszer elleni esetleges kibertámadás nemcsak a polgári és katonai repülések biztonságos lebonyolítását és irányítását akadályozná, hanem alááshatja a Szövetség és tagállamai általános biztonsági és ellenálló képességébe vetett bizalmat is.[16]

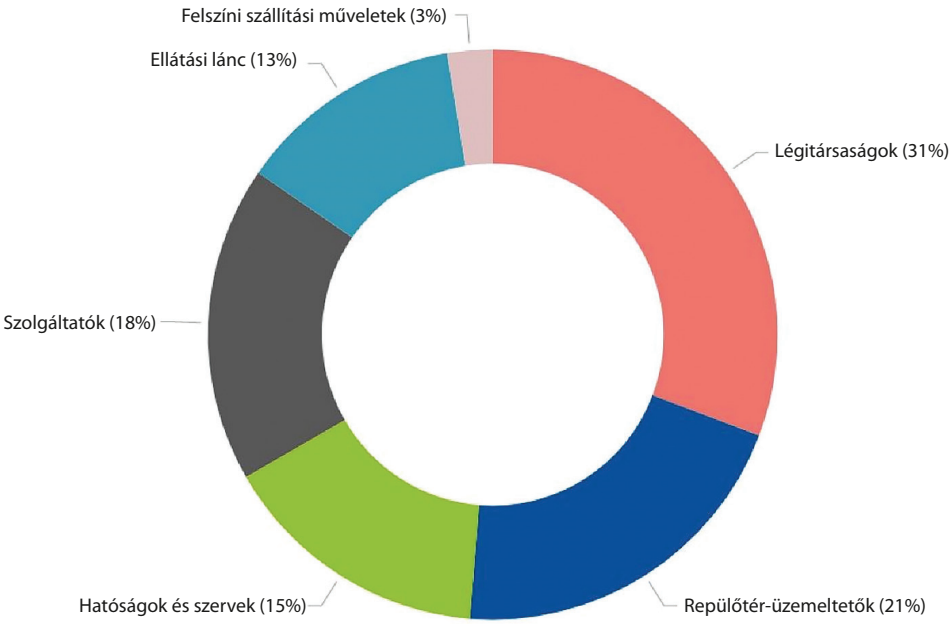
Az ENISA és az Eurocontrol adatai szerint a légtérhasználók/légitársaságok a támadások elsődleges célpontjai. Az ENISA és az EU repülésbiztonsági ügynöksége által az OSINT-en keresztül gyűjtött adatok szerint a légi közlekedési ágazat legfőbb kiberfenyegetéseit az adatokkal kapcsolatos fenyegetések (45%), a ransomware (36%) és a rosszindulatú programok (23%) jelentik. A légi közlekedési szektorban előforduló zsarolóprogram-esetek többségében a támadást adatokkal kapcsolatos fenyegetések követik, mint például az adatok kiszűrése és kiszivárogtatása, így ebben a két kategóriában jelentős az átfedés.[17]



1. ábra: Légi közlekedés elsődleges kiberfenyegetései 2022
Forrás: Theocharidou et al. 2022

Az Eurocontrol jelentése szerint 2022 januárja és júniusa között a legfontosabb célpontok a légtérhasználók, a repülőterek, az eredeti gyártók/ellátási lánc, a légi navigációs szolgáltatók és a polgári légi közlekedési hatóságok.[18]

[16] Elochukwu 2022: 3–5.
[17] Theocharidou 2022: 27–29.
[18] Illing–Dawn 2023.



2. ábra: Az ENISA fenyegetési tájképe: Légi közlekedési kibertámadási célpontok ágazati jelentés
Forrás: Theocharidou et al. 2022

A 2. és 3. táblázat a releváns polgári légi közlekedési iparhoz köthető kibertámadásokat mutatja be,[19] amelyek a NATO katonai légi szállítási képességek eszközparkját figyelembe véve szoros kapcsolatban állnak a NATO katonai légi szállítás potenciális kiberfenyegetéseivel.

2. táblázat: Boeing-kibertámadások kronológiája

Boeinggel kapcsolatos kibertámadások	
Időpont	**Leírás**
2018	A Boeing céget 2018 márciusában sújtotta WannaCry vírus általi informatikai támadás. A Microsoft Windows XP szoftverének sebezhetőségeit kihasználva a WannaCry néven ismert kibertámadás globális szinten jelentős zavarokat okozott. Számos számítógépet támadott meg. Célja az volt, hogy megakadályozza a felhasználók számára az adatok elérését, amíg nem teljesítik a váltságdíjat, gyakran kriptovalutában (Gates 2018).

[19] Hunorfi–Paráda–Farkas 2024.

Boeinggel kapcsolatos kibertámadások	
Időpont	**Leírás**
2019	2019-ben egy spamkampány a Boeing 737 Max legfrissebb balesetét aknázta ki a kártékony szoftverek ellen. A 360 Threat Intelligence Center szakértői egy spamkampányt észleltek, amely arra törekedett, hogy kihasználja a Boeing 737 Max két balesetét. A kampány mögött kétes szereplők „info@isgec[.]com" fiókkal küldtek e-maileket, amelyek témája „Fwd: Airlines plane crash Boeing 737 Max 8". A leveleket állítólag egy „Joshua Berlinger" nevű magánnyomozó küldte, és arra próbálták ösztönözni a címzettet, hogy nyissa meg a mellékelt JAR-fájlt. A kutatók felfedezték, hogy ennek a kampánynak az a célja, hogy a „H-WORM" Remote Access Trojan (RAT) vírust egy káros JAR-fájl mellékletén keresztül juttassa el a címzett számítógépére (Anomali Threat Research 2019).
2021	A 2020 végén kirobbant SolarWinds-kibertámadás hatással volt a Boeingra is. A támadók az IT-szolgáltató, a SolarWinds szoftverfrissítéseit manipulálták, hogy hozzáférjenek a cégek rendszereihez. Az ilyen típusú támadás során a Boeing, mint a legnagyobb felhasználó, veszélybe került (Robin 2023).
2022	2022. november 2-án több Jeppesen-szolgáltatás is leállásra kényszerült. A Jeppesen a Boeing teljes tulajdonában áll, élen jár a légi navigációs szolgáltatások terén. Navigációs adatbázisokat, repüléstervezési alkalmazásokat kínál EFB-khez, valamint portfóliójába tartozik a NOTAM-kezelés is (Thurber 2022; Klint 2022; Britton 2022).
2023	2023. október 27-én a Boeing neve feltűnt a LockBit weboldalán, ahol november 2-ig adtak határidőt a cégnek a kapcsolatfelvételre és a tárgyalások megindítására, hogy elkerüljék a nyilvánosságra kerülő adatokat, amelyek súlyos károkat okozhatnak. A csoportnak jelentős mennyiségű érzékeny adatot sikerült megszereznie. Rövid időre a Boeing lekerült a LockBit áldozatai közül, de november 7-én újra felbukkant, amikor a csoport jelezte, hogy a cég figyelmen kívül hagyta figyelmeztetéseiket. November 10-én a LockBit közzétette weboldalán az összes olyan adatot, amely a Boeingtól származik, köztük IT-menedzsmentszoftverek biztonsági mentései és monitoring-, valamint auditeszközök naplói. Egy hackercsoport körülbelül 50 GB nyers adatot szivárogtatott ki a Boeingtől, miután az nem volt hajlandó kifizetni. A szivárgás során talált Citrix eszközök biztonsági másolatai arra utalnak, hogy a LockBit kihasználhatta a Citrix Bleed sebezhetőséget (CVE-2023-4966), ennek bizonyítékát október 24-én fedezték fel (Ilascu 2023; Raj 2023).

Forrás: a szerzők szerkesztése

3. táblázat: Airbus-kibertámadások kronológiája

Airbusszal kapcsolatos kibertámadások	
Időpont	**Leírás**
2019	Az Airbus 2019-ben bejelentette, hogy egy „adatvédelmi incidens" történt, amely során támadók hozzáfértek egyes rendszereihez, és nem hivatalos hozzáférést szereztek érzékeny információkhoz (Duvelleroy 2019).
2023	2023-ban az Airbus adatszivárgást vizsgált, amely állítólag több ezer beszállítót érint. A kiberbiztonsági incidens vizsgálata azért volt szükségszerű, mert a hírek szerint egy hacker a cég 3200 szállítójáról tett közzé információkat a sötét weben. Egy „USDoD" becenevet használó fenyegetőző a BreachForums-on közzétette, hogy hozzáférést kapott egy Airbus internetes portálhoz, miután feltörték egy török légitársaság alkalmazottjának fiókját. A Hudson Rock jelentése szerint a hacker azt állította, hogy több ezer Airbus-eladóról rendelkezik adatokkal, köztük nevekkel, címekkel, telefonszámokkal és e-mail-címekkel (Antoniuk 2023).

Forrás: a szerzők szerkesztése

Következtetésként megállapítjuk, hogy mivel a NATO katonai légi szállítási képességek eszközparkját az adott polgári légi közlekedési ipari szereplők biztosítják, nagymértékben fennáll a lehetősége, hogy esetenként (minden technikai körülmény és paraméter együtt állásának teljesülése során) a kibertámadások és fenyegetések befolyásolják a NATO katonai légi szállítási képességeinek műveleteit.

A NATO légi közlekedési képességei és rendszerei kibertéri eszközeinek csoportosítása és kibertámadásokkal szembeni hatékony védelmének módja

A 2023-as vilniusi NATO-csúcstalálkozón a szövetségesek új koncepciót hagytak jóvá a kibervédelemnek a NATO általános elrettentő képességéhez és védelmi helyzetéhez való hozzájárulásának fokozására. A vilniusi csúcstalálkozón a szövetségesek megismételték és megerősítették a kibervédelmi ígéretet, és ambiciózusabb célok mellett kötelezték el magukat a nemzeti kibervédelem prioritásként való megerősítésére, beleértve a kritikus infrastruktúrákat is.[20] A 2024-es washingtoni NATO-csúcstalálkozón a szövetségesek megállapodtak abban, hogy létrehozzák a NATO Integrált Kibervédelmi Központot a hálózatvédelem, a helyzetfelismerés és a kibertér mint műveleti terület megvalósítása érdekében.[21]

A csúcstalálkozón elfogadott kibervédelmi intézkedések felismerték, hogy a manapság használt fegyverek és küldetésrendszerek többségét az internet előtti világra tervezték. Az implicit feltételezés az volt, hogy rendszereink alapvetően megengedő kibertérkörnyezetben működnek. Sok rendszerünket évtizedekkel ezelőtt tervezték, és egyáltalán nem meglepő, hogy senki sem tudta megjósolni a kibertértartomány robbanásszerű növekedését és jelentőségét. Amikor a rendszertervezők a fegyverrendszerek információbiztonságának valamilyen formáját fontolgatták, a mérnökök általában azt feltételezték, hogy a határhálózat védelme távol tartja az ellenfeleket, így a fegyverrendszer által látott környezet továbbra is megengedő és védett lesz a hálózati védelemben. Ezek az implicit feltételezések hamisnak bizonyultak. A NATO légi közlekedési képességei és rendszerei már nem biztonságosak, mivel a kibertámadások üteme naponta növekszik a katonai, kormányzati és polgári szektorban.[22]

Mivel minden modern fegyverrendszer (például a NATO légi korai figyelmeztető és szövetségi földi megfigyelőrendszerei, valamint a továbbfejlesztett légi és földi örökölt rendszerek) egyszerre létezik mind a fizikai (légi, szárazföldi és tengeri), mind a kibertér területén, a kibertámadások közvetlenül érintik a hadviselési rendszereket. Számos hozzáférési pont létezik, amelyeken keresztül az ellenfelek megtámadhatják ezeket a rendszereket a kibertéren keresztül. Bármilyen fizikai kapcsolat, amely adatokat továbbít, vagy bármilyen antenna, amely integrált processzorral rendelkezik, potenciális út a támadó számára. Nyilvánvaló példák közé tartoznak a karbantartási és logisztikai rendszerek, a rádiók és az adatkapcsolatok, valamint más rendszerek,

[20] NATO 2023.
[21] NATO 2024b.
[22] Kalivoda–DeFazio 2017.

amelyek összekötik a kezelőket és a platformokat (például repülőgépek vagy fegyverek). Természetesen ezek a dolgok még bonyolultabbak, hiszen ezek a sérülékenységek nem statikusak, hanem folyamatosan változnak. Minden szoftverfrissítés, minden új képesség és minden új berendezés új sebezhetőséget jelenthet. A bonyolultság további növelése érdekében számos kritikus küldetésfüggőség a katonai befolyáson kívül esik, amelyek a kereskedelmi rendszerekkel kapcsolatosak. Mivel a sérülékenységek skálája rendkívül széles, először is meg kell határoznunk, mi a legfontosabb.

Mielőtt meghatározzuk, hogyan kell a NATO-nak megvédenie légi közlekedési képességeit és rendszereit, a kibertéri eszközöket a következő három nagy területre kategorizáltuk:

- Hagyományos IT: magában foglalja az IP-alapú hálózatokat, beleértve a NATO kombinált légi műveleti központjait és egyéb személyzeti és logisztikai rendszereket. Ezek főleg irodai és adminisztratív célú rendszerek IT-támogatását foglalják magukba, amelyek közvetetten kapcsolódnak a NATO kombinált katonai légi műveleteihez, vagy általánosságban bármilyen katonai művelethez.
- Működési technológia OT: számítógéppel vezérelt fizikai folyamatok vagy más típusú vezérlőrendszerek, valamint IP-alapú specifikus szoftverek vagy hálózati rendszerek. Ezek főként a katonai műveleti célú rendszerek üzemeltetését, IT-támogatását foglalják magukba, amelyek az előző kategóriához képest már közvetlenül kapcsolódnak a katonai műveletek végrehajtásához, azok speciális leszűkült tartományi értelmezéséhez, valamint azok sikeres végrehajtásához.
- Platformok: tartalmazza a repülőgépeket, hajókat, tankokat és minden más fegyverrendszert, amelyet a Szövetség és tagjai üzemeltetnek.

Míg a kibervédelmi szakértők jól ismerik a hagyományos IT-rendszerek védelmét, és kezdenek az OT védelmére összpontosítani, a platformok védelmével kapcsolatos munkát még vizsgálni kell. Ezt szem előtt tartva, a NATO légi közlekedési képességei és rendszerei kibertámadásokkal szembeni hatékony védelmének legjobb módja a mélyreható védelem, az ellenálló képesség és a fejlett védelmi intézkedések kombinációja. Mindegyik megközelítés szükséges, és egyik sem elegendő önmagában. Ezért a NATO-nak és tagjainak a maximális hatékonyság érdekében össze kell kapcsolniuk ezeket egy koherens egésszé.[23]

- A mélyreható védelem számos IT-rendszerrel kapcsolatos megoldást jelent, amelyeken az ellenfélnek át kell jutnia, ez biztosítja a kezdeti védelmet, és blokkolja a legtöbb kevésbé kifinomult támadást. A jó mélyreható védekezésnek több összetevője van. Az első egy határvédelem, amely távol tartja a képzetlen támadók alacsony szintű támadásait. A jó védelem számos konfigurált határolással rendelkezik, hogy megakadályozza az oldalirányú mozgást, a privilégiumok fokozódását és az érzékeny adatok kiszűrését. A sebezhetőségkezelés a vállalatokon belül is része a mélyreható védelemnek, és a védőknek nemcsak a sebezhetőségeket kell kizárniuk, hanem le kell állítaniuk a szükségtelen folyamatokat és alkalmazásokat is, hogy megszüntessék a támadási felület nagy részét. Ennek megvalósításához hatékony és biztonságos rendszertervezésre

[23] Bryant 2016: 10–13.

van szükség, amely figyelembe veszi a kibervédelmi szempontokat a tervezési folyamat során.

- Az ellenálló képesség megakadályozza, hogy az ellenfelek elérjék céljaikat, amikor megtámadják a NATO és a tagállamok rendszereit. A NATO és tagállamai légi közlekedési rendszereinek védelmében az ellenálló képességhez flexibilitásra, a támadási felületek csökkentésére és a kibertámadásokra való dinamikus reagálásra lesz szükség. A rugalmas globális légi közlekedési rendszerhez többletkapacitásra lesz szükség a flexibilitásból következő redundanciák biztosításához. Ezenkívül heterogén rendszernek kell lennie, védhető területekre bontva. Ahhoz, hogy dinamikusan reagálhassanak a kibertámadásokra, a globális légi közlekedési rendszer védelmezőinek jobb helyzetfelismerést kell kialakítaniuk saját hálózatukkal kapcsolatban, és fejleszteniük kell hírszerzési képességeiket, hogy megértsék, mit terveznek a potenciális ellenfelek.
- A fejlett védelmi intézkedések az ellenfelek megtalálásával és legyőzésével megnehezítik a támadó számára, hogy elég sokáig a rendszerben maradjon és ezáltal károkat okozzon. Fontos megjegyezni, hogy ezek nem mindig jelentenek valós idejű megfigyelést és manőverezést, hanem időszakos ellenőrzésekre is támaszkodhatnak bizonyos típusú rendszerek esetében, ahol a valós idejű megfigyelés nem praktikus vagy nem követelmény. A fejlett védelmi intézkedések három összetevőből állnak: manőverező erők, érzékelők és eszközök. A manőverező erők az aktív védelem sikeres végrehajtásához szükséges képzett személyzet. Nemcsak a hagyományos informatikai rendszereket kell érteniük, hanem ismerniük kell az OT- és platformrendszereket is. Ennek a manőverező erőnek a fejlesztésére szükség van, de el kell látni őket a rejtett kibertámadók megtalálásához szükséges érzékelőkkel is. Ezeknek az érzékelőknek túl kell lépniük a szabványos behatolásérzékelő rendszereken. Amint egy támadást észlelnek, a manőverező erőknek szükségük lesz a megfelelő eszközökre, hogy képesek legyenek legyőzni a betolakodót.

Végül figyelembe kell venni a repülésbiztonságot és azokat a folyamatokat, amelyek biztosítják a repüléstechnikai termékek, alkatrészek és berendezések légi alkalmasságát. A fent felsorolt katonai és polgári rendszerekhez hasonlóan a légi alkalmassági bizonyítványokhoz használt berendezéseket is kibertámadások érik. Ezért az ebben a dokumentumban javasolt kibervédelmi intézkedéseknek a légi alkalmassági folyamatokra is vonatkozniuk kell.[24]

Összegzés

A polgári légi közlekedés működési környezetének jelenlegi változásai erősen integrált és kölcsönösen függő számítógépes és digitális hálózatokat eredményeznek mind a repülőgépek fedélzetén, mind a légi forgalmi irányító létesítményekben, ami belső

[24] Bryant 2015: 90.

biztonsági réseket okoz. A NATO-nak ezért meg kell védenie légi közlekedési képességeit és rendszereit a kibertámadásoktól a mélységi védelem, az ellenálló képesség és a fejlett védelmi intézkedések kombinációjával. Továbbá, mivel a polgári légi közlekedési rendszerek elleni támadás a katonai repülést is érinti, átfogó megoldásra van szükség.

Ahogy a NATO az „információbiztosításról" a „küldetésbiztosításra" helyezi a hangsúlyt, tagjainak fontolóra kell venniük kibertéri eszközeik besorolását hagyományos információs technológia, operatív információs technológia vagy platformok kategóriájába, hogy jobban megvédjék őket a kibertámadásoktól, ahogyan azt a jelen dokumentum javasolja.

Jelenleg nincs közös jövőkép, stratégia, cél, szabvány, megvalósítási modell vagy nemzetközi politika, amely meghatározná a légi közlekedés kibervédelmét. A biztonságos légi közlekedési rendszer biztosítása és a fejlődő kiberfenyegetéssel való szembenézés az összes érdekelt fél közös felelőssége, beleértve a kormányokat, a légitársaságokat, a repülőtereket és a gyártókat.

A következő generációs és továbbfejlesztett örökölt rendszerek csak fokozzák a jövőbeli kibervédelmi problémákat, mivel egyre inkább hálózatfüggővé válnak. Ezért kulcsfontosságú lesz, hogy a kibervédelmi tesztelés része legyen a NATO és tagállamai légi alkalmassági tanúsítási folyamatának.

A katonai légi szállítási képességek nélkülözhetetlen szerepet játszanak a globális katonai műveletekben, és ezeknek a képességeknek a kiberfenyegetésekkel szembeni védelme rendkívül fontos. Egy holisztikus kibervédelmi stratégia megvalósításával, amely magában foglalja az átfogó kockázatértékelést, a biztonságos hálózati architektúrát, a biztonságos kommunikációs csatornákat, a hozzáférés-ellenőrzési mechanizmusokat, az incidensreagálási tervezést, a képzési és figyelemfelkeltő programokat, az ellátási lánc biztonsági intézkedéseit, valamint a folyamatos ellenőrzést és auditálást, a katonai erők jobban tudják biztosítani légi szállítási képességeik rugalmasságát és hatékonyságát. Ezeknek a kiberbiztonsági intézkedéseknek a folyamatos adaptálása és fejlesztése elengedhetetlen az újonnan megjelenő kiberfenyegetések leküzdése és az erős védelem fenntartása érdekében a gyorsan változó digitális környezetben.

A polgári és katonai légi közlekedési rendszerek kölcsönös függősége miatt a kibertámadás ellen egyik sem védekezhet elszigetelten. A polgári légi közlekedési szektor elleni támadás a NATO katonai képességeire is hatással lesz, ezért átfogó választ igényel. A polgári képességek szintén jelentős kibervédelmi aggályokat vetnek fel, és ha összekapcsolódnak, hatással lesznek a NATO műveleti képességeire.

A cikk a 2024. október 15-i II. Alverad-Bánki Nemzetközi Kiberbiztonsági Konferencián elhangzott előadás kivonata.

Felhasznált irodalom

Anomali Threat Research (2019): Weekly Threat Briefing: Spam Campaign Uses Recent Boeing 737 Max Crashes to Push Malware. *Anomali,* 2019. március 19. Online: https://www.anomali.com/blog/weekly-threat-briefing-spam-campaign-uses-recent-boeing-737-max-crashes-to-push-malware

ANTONIUK, Daryna (2023): Airbus Investigates Data Leak Allegedly Involving Thousands of Suppliers. *The Record,* 2023. szeptember 12. Online: https://therecord.media/airbus-data-leak-suppliers-breachedforums

BHARGAVA, Amit Kumar (2024): Cybersecurity in Aerospace: A Military Perspective. *Blue Yonder,* 1(1). Online: https://journals.capsindia.org/index.php/byj/article/view/48

BRITTON, Niki (2022): 'Cyber Incident' Affected Flight Planning. Boeing Subsidiary Jeppesen Apparently Targeted. *AOPA,* 2022. november 9. Online: www.aopa.org/news-and-media/all-news/2022/november/09/cyber-incident-affected-flight-planning

BRYANT, William D. (2015): Resiliency in Future Cyber Combat. *Strategic Studies Quarterly,* Winter, 87–107. Online: www.airuniversity.af.edu/Portals/10/SSQ/documents/Volume-09_Issue-4/Bryant.pdf

BRYANT, William D. (2016): Mission Assurance through Integrated Cyber Defense. *Air & Space Power Journal,* 30(4), 5–17. Online: www.airuniversity.af.edu/Portals/10/ASPJ_Spanish/Journals/Volume-29_Issue-3/2017_3_04_bryant_s_eng.pdf

DUVELLEROY, Matthieu (2019): Airbus Statement on Cyber Incident. *Airbus,* 2019. január 30. Online: www.airbus.com/en/newsroom/press-releases/2019-01-airbus-statement-on-cyber-incident

GATES, Dominic (2018): Boeing Hit by WannaCry Virus, But Says Sttack Caused Little Damage. *The Seattle Times,* 2018. március 28. Online: www.seattletimes.com/business/boeing-aerospace/boeing-hit-by-wannacry-virus-fears-it-could-cripple-some-jet-production/

HOOD, James D. (2009): *NATO Strategic Airlift: Capability or Continued US Reliance?* Maxwell Air Force Base, Air Command and Staff College Air University. Online: https://apps.dtic.mil/sti/tr/pdf/ADA539589.pdf

HUNORFI, Péter – PARÁDA István – FARKAS Tibor (2024). Kiberbiztonsági kihívások a légi közlekedésben. *Hadmérnök,* 19(1), 101–120. Online: https://doi.org/10.32567/hm.2024.1.6

ILASCU, Ionut (2023): LockBit Ransomware Leaks Gigabytes of Boeing Data. *Bleeping Computer,* 2023. november 12. Online: www.bleepingcomputer.com/news/security/lockbit-ransomware-leaks-gigabytes-of-boeing-data/

ILLING, Dawn (2023): The Cyber Threat Landscape Of The Aviation Sector. *Skyradar,* 2023. március 28. Online: www.skyradar.com/blog/the-cyber-threat-landscape-of-the-aviation-sector

KALIVODA, Michal – DEFAZIO, Alexander (2017): Defending NATO's Aviation Capabilities from Cyber Attack. *JAPCC,* 2017. január. Online: www.japcc.org/articles/defending-natos-aviation-capabilities-from-cyber-attack/

KLINT, Matthew (2022): Breaking: Boeing's Jeppesen Subsidiary Hit with Potential Ransomware Attack. *Live and Let's Fly,* 2022. november 3. Online: https://live-andletsfly.com/boeing-jeppesen-ransomware-attack/

MEGYERI Lajos – FARKAS Tibor (2017): Kockázatkezelés, tudomány vagy kuruzslás? *Hadmérnök,* 12(3), 198–209. Online: https://real.mtak.hu/64731/1/1.Farkas_Hadm%C3%A9rn%C3%B6k2017.pdf

NATO (2022): *Multi Role Tanker Transport Capability (MRTT-C) Factsheet.* Online: www.nato.int/nato_static_fl2014/assets/pdf/2022/9/pdf/2209-factsheet-mrtt.pdf

NATO (2023): *Vilnius Summit Communiqué*. Online: www.nato.int/24cps/ge/natohq/official_texts_217320.htm
NATO (2024a): *Strategic Airlift*. 2024. március 7. Online: www.nato.int/cps/en/natohq/topics_50107.htm
NATO (2024b): *Washington Summit Declaration.* 2024. július 10. Online: www.nato.int/cps/cn/natohq/official_texts_227678.htm
Nyitrai Mihály (2016): Eredmények a szövetséges stratégiai légi és tengeri szállítóképesség erősítése terén. *Hadtudományi Szemle,* 9(2), 73–94. Online: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/14008
Oppelaar, Isaiah (2023): NATO's Multinational MRTT Unit An Update and Case Study for Future Defence Cooperation. *The Journal of the JAPCC,* 35, 25–31. Online: www.japcc.org/articles/natos-multinational-mrtt-unit/
Raj, Aaron (2023): Boeing Hack: Should the Airline Manufacturer Negotiate with Cybercriminals? *Tech Wire Asia,* 2023. november 6. Online: https://techwireasia.com/2023/11/boeing-hack-should-the-airline-manufacturer-negotiate-with-cybercriminals
Robin, Miriam (2023): Cyber Risk Disclosures in Crosshairs as SEC Charges SolarWinds with Fraud. *Intelligize,* 2023. november 16. Online: www.intelligize.com/cyber-risk-disclosures-in-crosshairs-as-sec-charges-solarwinds-with-fraud/
Siposné Kecskeméthy Klára (2019): A NATO biztonsági beruházási programja Magyarországon. *Honvédségi Szemle,* 147(2), 27–40. Online: https://real.mtak.hu/125189/
Szarvas László (2008): *Stratégiai Légi Szállítási képesség – egy új többnemzeti megoldás*. *Nemzet és Biztonság,* 1, 60–76. Online: www.nemzetesbiztonsag.hu/cikkek/szarvas_laszlo-strategiai_legi_szallitasi_kepesseg___egy_uj_tobbnemzeti_megoldas.pdf
Szászi Gábor (2015): A Magyar Honvédség légiszállító képességének változása napjainkig, a fejlesztés jövőbeni lehetpségei. *Economica,* 8(4/2), 216–227. Online: https://doi.org/10.47282/ECONOMICA/2015/8/4/2/4607
Theocharidou, Marianthi – Stanic, Zoran – Drougkas, Athanasios – De Sousa Figueiredo, Ricardo – Tsekmezoglou, Eleni – Naydenov, Rossen – Lella, Ifigeneia – Malatras, Apostolos szerk. (2022): *ENISA Threat Landscape: Transport Sector.* ENISA. Online: https://doi.org/10.2824/553997
Thurber, Matt (2022): Jeppesen Planning, Chart Products Suffer 'Technical Issues'. *AIN Online,* 2022. november 4. Online: www.ainonline.com/aviation-news/business-aviation/2022-11-04/jeppesen-planning-chart-products-suffer-technical-issues
Ukwandu, Elochukwu – Ben-Farah, Mohamed Amine – Hindy, Hanan – Bures, Miroslav – Atkinson, Robert– Tachtatzis, Christos – Andonovic, Ivan – Bellekens, Xavier (2022): Cyber-Security Challenges in Aviation Industry: A Review of Current and Future Trends. *Information,* 13(3), 3–5. Online: https://doi.org/10.3390/info13030146