REPÜLÉSTUDOMÁNYI KÖZLEMÉNYEK
35. évfolyam (2024) 2. szám 135–148. • DOI: 10.32560/rk.2024.2.10

Horváth Gábor

Kibervédelmi kockázatértékelés a légi forgalmi irányításban: az európai metodika

A légi forgalmi szervezéssel összefüggő rendszerek (ATM) digitalizációja, a szolgáltatásorientált architektúrák és az adatmegosztásra épülő modellek bevezetése jelentősen növeli a rendszerek összetettségét és kibervédelmi kitettségét. Jelen publikáció átfogóan elemzi a modern ATM-rendszerek kibervédelmi kihívásait, különös tekintettel a kockázatértékelési módszertanok (például SecRAM) gyakorlati korlátaira, a kommunikációs protokollok (ADS-B, CPDLC) sérülékenységeire, valamint az ellátási láncok és a rendszer-integráció által okozott dominóhatásokra. A tanulmány bemutatja a Horizon Europe SEC-AIRSPACE projekt innovatív megközelítését, amely nem új módszertan, hanem a meglévő kockázatkezelési eljárások kiegészítését célozza. A projekt fő újdonságai közé tartozik egy holisztikus ATM-taxonómia kidolgozása, a virtualizált környezetek és a humán tényezők figyelembevétele, valamint a dinamikus kockázatmonitoring bevezetése. Az eredmények hozzájárulnak egy kiberreziliens ATM-ökoszisztéma kialakításához, amely képes a folyamatosan változó fenyegetettségi környezetben is fenntartani a légi közlekedés kiemelkedő biztonsági színvonalát.

Kulcsszavak: *kibervédelem, kibervédelmi kockázatértékelés, légiforgalom-szervezés, ATM, air traffic management*

1. Bevezetés

A légiforgalom-szervezés (ATM[1]) egy rendkívül összetett, globális léptékű infrastruktúra, amelynek elsődleges célja a légi forgalom biztonságos és hatékony áramlásának szavatolása [1]. Az ATM-rendszerek egyre szorosabb összekapcsolódása és növekvő komplexitása azonban új, rendszerszintű kockázatokat generál. Az új technológiák, mint az adatmegosztás-alapú szolgáltatási modellek, a szolgáltatásorientált architektúrák, valamint az adatok intenzív megosztása a különböző szereplők között, jelentősen átalakítják a jelenleg ismert ATM működését [2]. Ezek a fejlesztések ugyanakkor dinamikusabb légtér- és ATM-szolgáltatás-menedzsmentet igényelnek, amely a kibervédelmi fenyegetések új generációjának teszi ki a rendszereket. Amennyiben ezekre a fenyegetésekre nem megfelelően reagálnak, az akár katasztrofális következményekhez is vezethet [3].

[1] Air Traffic Management.

Jelen tanulmány célja, hogy analizálja a nemrégiben elindított Horizon Europe SEC-AIRSPACE[2] projekt megközelítését, amelynek középpontjában egy reziliens ATM-rendszer megvalósítása áll, különös hangsúlyt fektetve a kibervédelmi kockázatok mérséklésére és az érintettek kockázattudatosságának növelésére. Az eredmények figyelembevétele mellett további fontos célkitűzés a következtetések értékelése a katonai ATM vonatkozásában.

2. Kihívások

Az előző fejezetben hivatkozott SEC-AIRSPACE projekt az Európai Unió fiskális támogatásával rendelkező, feltáró jellegű *(Exploratory Research)* kutatás, amely a SESAR Digitális Európai Égbolt (Digital European Sky) program keretében, az úgynevezett *Virtualisation And Cyber-Secure Data-Sharing* zászlóshajó-kezdeményezés részeként fut 2023. szeptember 1. és 2026. február 28. között. Jelen fejezetben a projekt által feltárt kihívásokat elemezzük.

2.1. Az ATM-rendszerek kibervédelmi kockázatértékelése

A kibervédelmi kockázatértékelés mára általánosan elfogadott megközelítéssé vált a digitális információra, adatmegosztásra és szolgáltatásalapú architektúrákra épülő ágazatokban, beleértve a kritikus infrastruktúrákat is [4]. A légi közlekedés és azon belül a dinamikus, integrált légiforgalom- és légtérmenedzsment (ATM) sem kivétel [5]. Európában az ATM-ágazat kutatás-fejlesztési (K+F) tevékenységeinek jelentős része a SESAR Joint Undertaking keretében zajlik. A szervezet kibervédelmi eljárásrendje kiemeli, hogy a biztonsági erőfeszítéseket a legsérülékenyebb pontokra kell koncentrálni, és a kockázatértékelést már a K+F-fázisban el kell végezni, különösen technológiailag összetett architektúrák és új technológiák bevezetésekor [6].

A gyakorlatban alkalmazott ATM-kockázatértékelési módszerek azonban továbbra is széttagoltak, mivel nincs univerzális, egységesen elfogadott megoldás az ATM-rendszerek sokféleségére [7]. Az európai ATM K+F-projektek többsége a Security Risk Assessment Methodology (SecRAM) eljárást alkalmazza, amelyet a SESAR fejlesztett ki [6]. Hasonló megközelítéseket más szektorokban is használnak, például az ISO/IEC 27005 és a NIST SP 800-30 szabványokat [8]. Függetlenül a választott módszertantól, elengedhetetlen a rendszer architektúrájának és működésének teljes körű megértése, valamint a védendő kritikus eszközök azonosítása, ami előfeltétele a kockázatok helyes értelmezésének és a megfelelő ellenintézkedések kiválasztásának.

Egy nemrégiben publikált tanulmány szerint azonban a SecRAM-gyakorlók gyakran nehézségekbe ütköznek – különösen a kritikus eszközök azonosításában, valamint a releváns fenyegetések és kockázatok meghatározásában az általuk fejlesztett technológiák és folyamatok kapcsán [9]. További problémák is jelentkeznek az ATM-rendszerek komplexitásának növekedésével, különösen a virtualizált szolgáltatások terjedésével, amelyek keretében a rendszerek közötti határok elmosódnak [10]. Az Európai Unió Repülésbiztonsági Ügynöksége (EASA) és a Stratégiai Együttműködési Platform (ESCP) több szereplője olyan új javaslatot tett a szabályozási keret egyszerűsítésére és harmonizálására, amely nemzetközi együttműködést,

[2] Projekt ID: 101114635.

szervezetek közötti kockázatmegosztást és átfogóbb értékelési módszerek szükségességét hangsúlyozza [11].

A jelenlegi kiberkockázati modellek több szempontból is jelentős továbbfejlesztést igényelnek: folyamatszervezési, modellezésmetodológiai és átfogó rendszerszemléleti vonatkozásban egyaránt. Egyrészt a veszélyforrások rendkívül gyors ütemben változnak és fejlődnek, ami szükségessé teszi a kockázatbecslések folyamatos, valós idejű frissítését lehetővé tevő hatékonyabb módszertani megközelítéseket. Másrészt napjaink kiberfenyegetései már nem kizárólag az informatikai rendszerekre korlátozódnak, hanem komplex módon érintik a humán erőforrásokat és a kiberfizikai rendszerek teljes spektrumát is. Harmadrészt a jelenleg alkalmazott modellek jelentős része nem veszi kellő mértékben figyelembe a kézzelfogható és immateriális eszközök sebezhetőségét a teljes ellátási lánc valamennyi pontján. Tudományos szempontból kiemelendő, hogy a komplex rendszerek sebezhetősége több kritikus ponton is megmutatkozhat: a rendszereket üzemeltető humán tényezőkön, a kiberfizikai interfészeken vagy akár a beszállítói hálózat bármely elemén keresztül is kompromittálhatják rosszindulatú szereplők [12]. Az FP7 GAMMA projekt hangsúlyozza, hogy bármely ATM-biztonsági megoldásnak figyelembe kell vennie az új fenyegetések által okozott kockázatprofil-változásokat; egyetlen csomópont elleni támadás rövid idő alatt dominóhatással megbéníthatja az egész ATM-rendszert és a teljes légi közlekedési rendszert [13]. Az ilyen szempontokat a SecRAM jelenleg nem fedi le megfelelően, mivel alig vagy egyáltalán nem támogatja a kritikus eszközök azonosítását virtualizált környezetekben, a kibertámadások láncreakcióinak elemzését vagy a kockázatok dinamikus vizsgálatát.

A kibervédelmi kockázatértékelések ritkán történnek meg valós időben – jellemzően csak egy alkalommal, a rendszer fejlesztésekor és/vagy évente egyszer az üzembe helyezés után. A modern elvárások szerint a kockázatelemzési folyamatokat az eddigieknél lényegesen gyakrabban, optimális esetben valós idejű rendszerként szükséges működtetni, különösen azon ágazatokban, ahol magas fenyegetettséggel és kockázattal kell számolni. Ennek során jelenthetnek segítséget az automatizált technológiai megoldások – kiváltképp a mesterséges intelligencia (MI) alkalmazására épülő rendszerek – elsősorban a behatolásérzékelés, a kártékony programok azonosítása, valamint az ipari vezérlőrendszerek védelme terén. Mindazonáltal a mesterséges intelligencia alkalmazása a szisztematikus kockázatértékelési folyamatokban továbbra is relatíve újszerű kutatási és fejlesztési területnek tekinthető, különösen a légiforgalom-szervezés kontextusában. Az ATM-rendszerekben rejlő potenciális előnyök kiaknázása ugyanakkor különleges jelentőséggel bír, tekintettel e kritikus infrastruktúrák komplex biztonsági követelményeire és társadalmi fontosságára.

2.2. Az ATM-rendszerek sebezhetőségei és fenyegetettségei

A jövő légi forgalmi irányításának víziója megnövelt rendszerszintű interdependenciát és szolgáltatási integrációt feltételez, amely lehetővé teszi a légi navigációs szolgáltatók (ANSP[3]), a légitársaságok, a repülőterek és a jövőbeni ATM-adatszolgáltatók[4] számára az információk és szolgáltatások megosztását korábban nem ismert, innovatív módokon. Ez elkerülhetetlenül

[3] Air Navigation Service Provider.
[4] ATM Common Information Service Provider.

növeli az ATM-rendszerek potenciális kiberfenyegetettségét, mivel ezek a rendszerek korábban a zárt szabványok és az úgynevezett szigetüzem használata révén védtek a támadásokkal szemben. Az interoperabilitás növelése és a költségcsökkentés iránti igény fokozza a kereskedelmi forgalomban kapható (COTS[5]) alkatrészek alkalmazását, amelyeknek az integrációja új, összetett szolgáltatások vagy rendszerek létrehozása során komoly biztonsági kockázatot jelenthet. Az ATM egyik ismert példája az IP-protokollcsalád bevezetése a jövőbeni kommunikációs infrastruktúrában (FCI[6]). További kockázati tényező a különböző polgári és katonai szereplők, valamint a földön és az űrben telepített kommunikációs, navigációs és megfigyelőrendszerek közötti integráció [7].

Az elmúlt évtizedben egyre csak nőtt az ATM-rendszerek kibervédelmi sebezhetőségével összefüggő érdeklődés. Az úgynevezett etikus hackerek egy kutatócsoportja bemutatta, hogy mennyire könnyen és milyen olcsón lehet manipulálni az olyan meglévő, föld-levegő irányú biztonságkritikus adatátviteli protokollokat, mint például az ADS-B (Automatic Dependent Surveillance–Broadcast) és a CPDLC (Controller Pilot Data Link Communications) [14]. Ezen túlmenően már 2014-ben az IOActive nevű cég feltárta, hogy több SATCOM[7]-eszköz *firmware*-je súlyos sebezhetőségeket tartalmaz, amelyek lehetővé tehetik a támadók számára, hogy átvegyék az irányítást az adatkapcsolat felett, közvetlen veszélyt jelentve a légi közlekedés biztonságára [15]. Ehhez hozzájárul a különböző globális navigációs helyzetmeghatározó rendszerek (GNSS[8]) egyre gyakoribb zavarása, ami napjainkban komoly hatást gyakorol a légi forgalomra a Baltikum térségében [16].

2.3. A kibertámadások láncreakciós hatásai az ATM-rendszerekben

Általánosságban kijelenthető, hogy a légi forgalom szervezését irányító rendszerek fejlődése inkrementális, a kiberrezilienciát nem, vagy nem kellő súllyal faktorizálták, és a tervezés során nem fektettek kellő figyelmet a globális összekapcsoltsággal összefüggő kihívások kezelésére [5]. Az utas- és áruforgalom növekményével együtt járó digitalizációs igények új rendszerek létrehozását indikálják, amelyek a működési hatékonyság növelését priorizálják. Emellett az exponenciálisan növekvő adatforgalom új üzleti modellek megjelenését teszi lehetővé, amelyek csak más ágazatokkal való fokozott kapcsolat révén hasznosíthatók hatékonyan.

A légi forgalom hagyományos irányítórendszereinek fokozatos átállása a fejlettebb megfigyelő- és kommunikációs rendszerekre – modern adatátviteli hálózatokon keresztül – alapvetően alakítja át a légi közlekedési környezet biztonsági értékelését. Ez azonban az örökölt rendszereket – amelyeket inkább a repülésbiztonsági követelmények figyelembevétele mellett fejlesztettek – sebezhetővé teheti, és kézenfekvő támadási vektort biztosíthat a rosszindulatú aktoroknak [17].

Ez a rendszerintegráció kiterjesztett ellátási láncokat eredményez, amelyekben minden résztvevő a másik fél szolgáltatásaira és az ATM-szereplők, az ipari partnereik és a kapcsolódó ellátási láncaik közötti interakciókra van utalva. Ennek eredményeként az ellátási lánc biztonsága komoly kockázatot hordoz magában, mivel számos sebezhető pontot kínál

[5] Commercial-Off-The-Shelf.
[6] Future Communication Infrastructure.
[7] Satellite Communications.
[8] Global Navigation Satellite System.

rosszindulatú szereplők számára. Mindent figyelembe véve – a kiberfizikai rendszereket is beleértve – a hardver- és szoftverelemek összessége bizonyos mértékű támadási veszélynek van kitéve. Az ellátási lánc biztonságát ezért nem csupán a már működő rendszerekre, hanem minden olyan elemre is ki kell terjeszteni, amely az adott rendszer előállítását és működtetését valamilyen mértékben támogatja [4].

Az ATM-architektúrák és azok ellátási láncai eddig kevés figyelmet kaptak, pedig ezek alapos értékelése és megértése kulcsfontosságú a kiberkockázatok felmérésében. Ez lehetővé teszi a lehetséges láncreakciós hatások azonosítását, valamint a megfelelő megelőző és védelmi intézkedések meghozatalát.

2.4. Biztonsági intézkedések az ATM-rendszereket fenyegető veszélyek mérséklésére

A polgári légi közlekedés területén a kibervédelmet az ICAO Annex 17 szabályozza, amelyet Európában a közös követelményrendszert rögzítő rendelet, valamint a NIS2 irányelv ültet át a gyakorlatba, előírva a légi navigációs szolgáltatók számára a vonatkozó biztonsági követelményeket. Mivel az ANSP-k alapvető szolgáltatóknak minősülnek, számukra kötelező a NIS2 irányelv alkalmazása [18]. A szabályozási környezet összetett, ugyanakkor arra kötelezi a légi navigációs szolgáltatókat, hogy a biztonságot átfogó, holisztikus szemlélettel kezeljék, figyelembe véve az emberi tényezőket, a folyamatokat és a technológiai megoldásokat [19].

Azok az ATM-egységek, amelyek a SecRAM-módszertant alkalmazzák, a magas és közepes szintű kockázatok kezelésére általában a SESAR által kidolgozott minimum biztonsági intézkedések halmazából (MSSC[9]) választják ki a megfelelő védelmi stratégiákat [20]. Ez a megközelítés azonban problémákat vethet fel, mivel az MSSC elsősorban informatikai rendszerekre vonatkozó, magas szintű biztonsági kontrollokat tartalmaz, amelyek nem megfelelő alkalmazása akár biztonsági és/vagy védelmi összeférhetetlenségeket is eredményezhet az ATM-rendszereken belül. Emellett hiányoznak a világos iránymutatások arra vonatkozóan, miként lehet ellenőrizni, hogy a beszállítók valóban megvalósítják-e a szükséges biztonsági intézkedéseket, különösen a légi közlekedési ágazatban, ahol a külső szoftverszállítók számára alig, vagy egyáltalán nincs jogi kötelezettség a biztonságos szoftverek szállítására [21].

2.5. Személyre szabott kibervédelmi képzés és tudatosság az ATM-szervezetek számára

A kibervédelem hatékony megerősítése átfogó, holisztikus szemléletet kíván, amely nem csupán technikai biztonsági intézkedéseket alkalmaz a kockázatok csökkentésére, hanem a társadalmi, emberi és szervezeti tényezőket is figyelembe veszi a rendszerek védelme során. Jól ismert tény, hogy az emberi tényező jelentős szerepet játszik a kiberkockázatok kialakulásában: a kibervédelmi incidensek mintegy 95%-a emberi hibára vezethető vissza [22]. Ugyanígy a súlyosabb adatvédelmi események többsége is szervezeti, folyamati vagy emberi

[9] Minimum Set of Security Controls.

mulasztás eredménye. Ennek következtében számos kibertámadás kifejezetten az embereket célozza, kihasználva a felkészültség hiányát vagy az alacsony tudatosságot [23].

A modern kibervédelmi technológiák egyre inkább az automatizálásra, a mesterséges intelligenciára és fejlett logikai rendszerekre támaszkodnak annak érdekében, hogy támogassák vagy akár részben kiváltsák az emberi beavatkozást. Ugyanakkor a képzési módszerek fejlődése nem tart lépést ezekkel a technológiai újításokkal: mivel egyre többen dolgoznak hibrid vagy teljesen távmunkaalapú környezetben – légi forgalmi irányítás esetében virtualizált irányítóközpontokban [24] –, különösen fontos, hogy az ATM-szektorban dolgozók kibervédelmi tudatossága és általánosságban a biztonsági kultúra fejlődjön.

Habár jelenleg is zajlanak képzések és tudatosságnövelő programok a kockázatok mérséklése érdekében, ezek módszertani fejlettsége gyakran elmarad a kívánatostól. A főként hagyományos oktatási formák – például tanfolyamok vagy képzési pályák – csak korlátozottan kapcsolódnak a valódi kockázatokhoz, így nehezen mérhető, hogy mennyire járulnak hozzá a tényleges kockázatcsökkentéshez [25]. Az ATM-rendszerekben a valós légi forgalmi helyzetek szimulációja már a gyakorlati képzés része, azonban – különösen katonai környezetben – ritka, hogy ezek a szimulációk kiberfenyegetéseket is tartalmazzanak.

3. Előretekintés: a SEC-AIRSPACE-megközelítés

Az előzőleg bemutatott kihívások kezelése érdekében a SEC-AIRSPACE projekt a következő, egymásra épülő stratégiai célkitűzéseket határozta meg:

1. a jelenlegi és jövőbeli légi forgalmi irányítási rendszerek kibervédelmi kockázatkezelési mechanizmusainak szisztematikus továbbfejlesztése és optimalizálása;
2. az ATM-ökoszisztémabeli szereplők kibervédelmi tudatosságának és érettségi szintjének célzott növelése, különös tekintettel a humán tényezőkre.

A projekt hosszú távú stratégiai víziója egy olyan kiberreziliens légi forgalmi irányítási rendszer megvalósítása, amely hatékonyan kezeli a virtualizációból eredő kockázatokat, valamint az ATM-infrastruktúra komponensei és az érintett szereplők közötti egyre intenzívebbé váló adatmegosztásból fakadó biztonsági kihívásokat. E rendszer kialakítása során kiemelt figyelmet kap a technológiai megoldások és a humán tényezők szinergiájának szavatolása, valamint az európai légtérhasználat biztonságának komplex megközelítése.

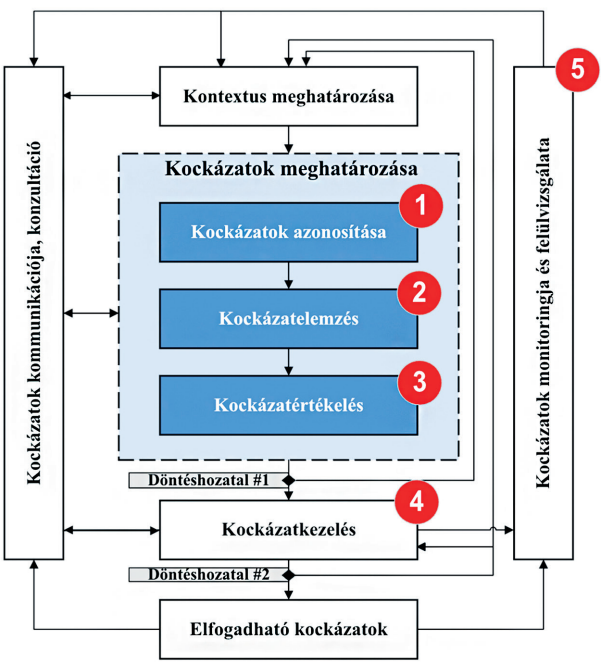
3.1. A kibervédelmi kockázatkezelés fejlesztése

Az 1. ábrával szemléltetett SEC-AIRSPACE projekt célja, hogy a jelenleg alkalmazott módszertanokat és bevált gyakorlatokat olyan kulcsfontosságú építőelemekkel egészítse ki és fejlessze tovább, amelyek hatékonyabbá teszik a kibervédelmi kockázatok kezelését az ATM területén. A projekt nem egy teljesen új módszertan kidolgozására törekszik, hanem olyan kiegészítések megalkotására, amelyek révén pontosabb és megbízhatóbb becslések készíthetők a jövőbeli ATM-forgatókönyvek kockázataira vonatkozóan.

A SEC-AIRSPACE elsősorban egy olyan átfogó taxonómiát dolgoz ki, amely a jövőbeni ATM-rendszerek elemeinek modellezését szolgálja. Ez a taxonómia holisztikus szemléletet

követ, lehetővé téve az ATM-ellátási lánc teljes körű ábrázolását, beleértve mind a kézzelfogható, mind az immateriális eszközöket, továbbá az emberi, eljárási és szervezeti tényezőket is. Emellett támogatja az összetett rendszerek, szolgáltatásorientált architektúrák, virtualizált elemek, valamint az ATM-szereplők közötti adatmegosztási interfészek megfelelő leírását. A cél, hogy a kiberkockázatok értékelése az összetett ATM-rendszerekben pontosabbá váljon, és lehetőség nyíljon a láncreakciós hatásokkal járó kibertámadások következményeinek részletes elemzésére is.

Másodsorban, a korszerű kibervédelmi kockázatkezelési életciklusokat holisztikus módon kell elemezni, vagyis minden lehetséges kockázati forrást figyelembe kell venni, beleértve az informatikai rendszerek integrációjából származó, a kiberfizikai és a vezérlőrendszerekhez, valamint az emberi tényezőkhöz kapcsolódó kockázatokat is. Egy átfogó kockázatértékelésnek minden típusú vagyonelemre ki kell terjednie. Például a HERMENEUT európai uniós projekt rámutatott arra, hogy az immateriális javak – mint a márka, a hírnév vagy a humán tőke – kiemelt jelentőségűek [26]. A DOGANA projekt pedig a humán kockázatok úgynevezett *social engineering*[10] alapú becslésére dolgozott ki módszertant [27]. A SEC-AIRSPACE ennek megfelelően iránymutatásokat készít az ATM-rendszerek sérülékenységeinek és gyengeségeinek azonosítására, különös tekintettel az emberi, eljárásrendi és szervezeti tényezőkre.



1. ábra
Az ISO/IEC 27005 ajánlás SEC-AIRSPACE-szemlélet szerinti értelmezése [a szerző]

[10] Az informatikában a *social engineering* (fordításban néha társadalommérnökség vagy pszichológiai befolyásolás) olyan támadási módszert jelent, ahol nem valamilyen technológiai sebezhetőséget használnak ki, hanem a számítógépet használó személyt tévesztik meg.

Harmadsorban, az ATM-rendszerek magas fokú összekapcsoltsága miatt a virtualizációból és a láncreakciós hatásokból – vagyis más szervezeteket, illetve szektorokat érintő másodlagos következményekből – eredő kockázatokat értékelni kell. A SEC-AIRSPACE áttekinti az ilyen események megelőzésére alkalmazott meglévő megközelítéseket, és új elemzéseket nyújt az azonosítási, összefüggés-feltárási és kockázatcsökkentő mechanizmusokról. A projekt egyik fő hozzájárulása egy olyan modell lesz, amely az ATM-rendszerkomponensek, illetve az ATM-rendszerek és más – különösen kritikus – infrastruktúrák közötti függőségeket vizsgálja.

Negyedik lépésként, a kibervédelmi kockázatok azonosítása után célzott biztonsági intézkedéseket kell bevezetni a kockázatok elfogadható szintre történő csökkentése érdekében. A SEC-AIRSPACE ennek támogatására új, ajánlott biztonsági intézkedéscsomagot dolgoz ki az ATM-rendszerek számára, amely az előző lépésekben feltárt fenyegetések mérséklésére szolgál. Ezek az intézkedések a meglévő legjobb gyakorlatokon – például az ISO/IEC 27005 szabványon vagy az MSSC ajánlásain – alapulnak, de igazodnak a jövőbeli ATM-rendszerek speciális igényeihez.

Végül a SEC-AIRSPACE célja a kockázatok folyamatos nyomon követésének és felülvizsgálatának fejlesztése egy dinamikus monitorozási és felülvizsgálati módszer bevezetésével, amelyet kifejezetten az ATM-rendszerek sajátosságaira szabnak. Ez a módszer az ATM-rendszerek adatmodelljeit használja bemeneti adatként, majd ezeket sémaszerűen kockázatértékelési algoritmusokká alakítja, amelyeket kockázati indikátorokhoz rendel. Ennek eredményeként lehetővé válik a kockázati szintek dinamikus mérése és megjelenítése.

3.2. A kibervédelmi tudatosság és érettség növelése

A SEC-AIRSPACE projekt keretében a People Analytics (PA) módszertanát alkalmazzák a légiforgalom-szervezés vonatkozásában, ami lehetővé teszi a személyre szabott, kontextusérzékeny képzési programok kialakítását [28]. A People Analytics és a Learning Analytics integrációja révén pontosan meghatározható, hogy mely tudásterületek, munkakörök és képzési módszerek járulnak hozzá a leghatékonyabban a kibervédelmi kultúra fejlesztéséhez [29]. Az így kialakított rendszer elősegíti a humán eredetű kockázatok csökkentését, valamint célzott, a munkavállalói csoportok sajátosságaihoz igazított képzési javaslatokat kínál. A folyamat főbb lépései az alábbiak szerint foglalhatók össze:

- A kritikus eszközök és a szükséges tudás meghatározása: a SecRAM-módszertan alkalmazásával azonosítják azokat a legfontosabb eszközöket, amelyekhez kapcsolódóan megállapítják a szükséges ismereteket és készségeket.
- Persona-modellek kialakítása: a humánerőforrás-adatok és az információbiztonsági értékelések alapján meghatározzák a különböző alkalmazotti csoportokat, valamint azok kockázati profilját.
- A People Analytics módszertan alkalmazása: a tanulásmenedzsment rendszeréből származó egyéni képzési adatokat, a humán erőforrás vonatkozásában keletkezett információkat, valamint az ATM-szervezet képzési katalógusát integrálják.
- Képzési javaslatok kidolgozása: az elemzés eredményeként természetes klasztereket és személyre szabott képzési javaslatokat alkotnak meg, amelyek a legmagasabb kockázatú területekre fókuszálnak.

- Képzési szolgáltatók bevonása: a megalkotott képzési javaslatok átadhatók a képzést lebonyolító szervezeteknek, amelyeknek a visszajelzései tovább tökéletesíthetik az információbiztonsági értékelési módszertanokat.

Ez a komplex megközelítés biztosítja, hogy a képzési folyamatok valóban a szervezet kockázati profiljához igazodjanak, és a humán tényezők figyelembevételével növeljék az ATM-szektor kibervédelmi érettségét.

3.3. A projekt esettanulmányai

A SEC-AIRSPACE projekt esettanulmányai több szempontból is jelentős szerepet töltenek be a kutatásban. Egyrészt megalapozzák és kontextusba helyezik a vizsgálati tevékenységeket, másrészt lehetőséget biztosítanak a projekt során elért kulcsfontosságú eredmények validálására. Emellett az esettanulmányok kiemelt fontosságúak a projekt eredményeinek bemutatása és tudományos kommunikációja szempontjából is.

Az első esettanulmány a légi forgalmi irányítók és pilóták közötti, kezdőponttól végpontig tartó adatáramlást vizsgálja egy jövőbeli, 4D trajektória alapú[11] üzemeltetési forgatókönyv keretében. Ebben a modellben a hagyományos hangalapú utasításokat digitális üzenetküldés váltja fel, amelyhez nyilvánosan elérhető, IP-alapú kommunikációs infrastruktúrákat alkalmaznak. A második esettanulmány egy virtuális irányítóközpont koncepcionális architektúrájának elemzésére fókuszál, amely a SWIM[12] alapelvei szerinti adatcsere-protokollokat, valamint nyílt, szolgáltatásorientált architektúrákat használ.

Mindkét esettanulmány olyan ATM-forgatókönyvet mutat be, amely digitális infrastruktúrákra és korszerű szolgáltatásnyújtásra épül, ezáltal új típusú kibervédelmi fenyegetéseket és kockázatokat vet fel. Ezek az esetek egyúttal szorosan illeszkednek a SESAR Digitális Európai Égbolt fejlesztési víziójához, hozzájárulva a jövő légiforgalom-irányítási rendszereinek biztonságos és innovatív kialakításához.

3.4. Katonai ATM-vonatkozások

A SEC-AIRSPACE projekt kontextusában különös figyelmet érdemel a katonai légi forgalmi és légvédelmi irányítás, valamint a polgári ATM-rendszerek közötti interakció, amely további kibervédelmi kihívásokat generál. A két rendszer integrációja jelentős komplexitásnövekedést eredményez, különösen a jelenlegi európai geopolitikai helyzetben, ahol a légterekkel kapcsolatos biztonsági követelmények fokozottan előtérbe kerültek.

A katonai légi járművek üzemeltetése során három meghatározó korlátozási tényező azonosítható, amelyek jelentős mértékben befolyásolják a kibervédelmi kockázatok jellegét

[11] Egy légi jármű 4D trajektóriája három térbeli dimenzióból, valamint a negyedik dimenzióként értelmezett időből áll. Ez azt jelenti, hogy bármilyen késés a trajektória (vagy pálya) torzulásának tekinthető, ugyanúgy, mint egy magasságváltozás vagy a vízszintes pozíció módosulása. A légi forgalmi irányítók taktikai beavatkozásai ritkán veszik figyelembe a teljes pályára gyakorolt hatást, mivel az előretekintési idő viszonylag rövid, jellemzően körülbelül 20 perc.

[12] System Wide Information Management.

és kezelhetőségét. Elsőként kiemelendők az intézményi korlátozások, amelyek értelmében a katonai repülőeszközökre nem teljeskörűen alkalmazhatók a polgári légi közlekedés szabályozói, tekintettel arra, hogy ezen eszközök elsődleges rendeltetése az adott állam szuverenitásának biztosítása. Másodsorban az operatív korlátozások kontextusában megállapítható, hogy a védelmi és biztonsági fenyegetettségek olyan műveleti imperatívuszokat generálnak, amelyeknek a katonai légi járművek esetében maradéktalanul érvényesülniük kell, ami az ATM-intézkedések vonatkozásában speciális kezelési protokollokat és körültekintő megfontolásokat tesz szükségessé. Harmadsorban számításba kell venni a technikai korlátozásokat, amelyek következtében a katonai repülőeszközök műszaki felszereltsége küldetésorientált, így az ATM, valamint a kommunikációs, navigációs és megfigyelési rendszerek fedélzeti implementációja egyes esetekben objektív korlátokba ütközhet.

A polgári-katonai együttműködés kulcsfontosságú a jövőbeli ATM-rendszerek rezilienciájának biztosításában. A MITRANO[13] program keretében tesztelt Mission Trajectory koncepció célja, hogy harmonizálja a katonai műveleti követelményeket a polgári légi forgalmi szolgáltatásokkal. A missziótrajektória definíció szerint minden katonai művelethez egyedileg meghatározott és minden repülésre egyeztetett útvonal, amellyel összefüggésben a felhasználó – vagyis ebben az esetben a katonai légi forgalom – vállalja, hogy az egyeztetett útvonalat le is repüli, és ezért cserébe a légi navigációs szolgáltató és az érintett repülőtér kötelezettséget vállal az útvonal támogatására. A MITRANO tapasztalatainak függvényében a civil-katonai interakció számtalan potenciális biztonsági problémát vet fel, amelyek közvetlen kibervédelmi vonzatokkal rendelkeznek:

- A chicagói egyezmény nem vonatkozik az állami légi járművekre [30], így a katonai személyzet nincs mindig megfelelően felkészítve a polgári légi forgalmi irányítás szabályaira és eljárásaira. Hasonlóképpen, a polgári irányítók általában nem ismerik a katonai légi forgalmi irányítási eljárásokat.
- Koordinációs problémák: amennyiben egy másik állam katonai légi járművei az államhatárhoz közel tevékenykednek, a kommunikációs lánc szükségtelenül hosszúvá válhat. Még a belföldi katonai tevékenységek során is előfordulhat, hogy a polgári irányítók nem tudják könnyen beszerezni a szükséges információkat a civil és katonai egységek közötti alacsony interoperabilitási szint miatt [31].
- A nemzetközi vizek feletti műveleteket érintő eltérő szabályozások jelentős bizonytalanságokat okozhatnak, különösen a NOTAM-ok helytelen közzététele esetén [32].

A kibertér és a légtér biztonságának konvergenciája új, integrált szemléletmódot követel meg. A korszerű katonai légi járművek fejlett avionikai rendszerekkel vannak felszerelve, amelyek működése nagymértékben támaszkodik összekapcsolt hálózatokra a navigáció, a kommunikáció, valamint a fegyverrendszerek irányítása során. Az ilyen rendszerek elleni kibertámadások potenciálisan veszélyeztethetik a műveleti képességeket, illetve a küldetések sikeres végrehajtását. Ennek következtében a katonai szervezetek robusztus kibervédelmi

[13] A Mission Trajectory in ATC and Network Management Operations projekt célja olyan megoldások kidolgozása, amelyek támogatják a trajektóriák kezelését, valamint a hálózati szintű és légiforgalom-irányítási műveletekben a közös döntéshozatalt, beleértve a katonai légtérhasználat fejlett tervezési elveit is.

intézkedéseket alkalmaznak – beleértve a tűzfalakat, a behatolásérzékelő rendszereket és a titkosítási protokollokat – a kritikus légi közlekedési infrastruktúra védelme érdekében.

A SEC-AIRSPACE projekt keretében a katonai és polgári légiforgalom-irányítási rendszerek integrációja kiemelt jelentőségű. A kibervédelmi kockázatok értékelése során elengedhetetlen figyelembe venni a hadműveleti követelményeket, a katonai légtérhasználat dinamikus jellegét, valamint az eltérő szabályozási környezetből fakadó sajátosságokat. Az Európai Unió által támogatott kezdeményezés holisztikus kockázatértékelési megközelítése lehetővé teszi a civil és katonai rendszerek közötti interfészeken keresztül jelentkező biztonsági kihívások azonosítását és kezelését. Ezáltal biztosítható, hogy a jövő digitális európai légtere képes legyen mind a polgári, mind a katonai felhasználók igényeit harmonikusan integrálni, miközben a kibervédelem megfelelő szintje is garantált marad.

4. Következtetések

A légiforgalom-szervezés és ezen belül a légi forgalmi irányítás környezete napjainkban egyre komplexebb struktúrát mutat. Az új piaci szereplők megjelenése, a kibővült szolgáltatási paletta, az integrált technológiai megoldások térhódítása, a virtualizációs folyamatok és a fokozódó adatmegosztási gyakorlatok bevezetése következtében az ATM-rendszerek és azok kritikus infrastrukturális elemei korábban nem tapasztalt kiberfenyegetéseknek és biztonsági kockázatoknak vannak kitéve. A légi közlekedési rendszerek megfelelő védelmének szavatolása érdekében az üzemeltetőknek, legyen az katonai vagy polgári, rendszeres és módszeres biztonsági kockázatelemzést szükséges végezniük, majd az azonosított kockázati tényezők mérséklésére célzott védelmi intézkedéseket kell implementálniuk.

A következtetések során érdemes hangsúlyozni, hogy a technológiai megoldások – így a különféle biztonsági kontrollmechanizmusok – önmagukban nem elégségesek a kiberfenyegetések hatékony elhárításához. Abban az esetben, ha a védelmi rendszerek kompromittálódnak, az üzemeltetőknek képesnek kell lenniük a jogosulatlan behatolások időben történő észlelésére, a személyzet azonnali riasztására, a káros következmények hatékony lokalizálására, valamint a meglévő vészhelyzeti tervekre alapozott helyreállítási és kárcsökkentő intézkedések haladéktalan foganatosítására. A kiberreziliencia megteremtése ezért átfogó, holisztikus megközelítést igényel a biztonsági kockázatmenedzsment területén, amelyben fontos az üzemeltető személyzet tudatosságának fejlesztése és célirányos képzése.

A SEC-AIRSPACE projekt legjelentősebb hozadéka a kiberreziliencia szintjének számottevő növekedése lesz; a rendszerszintű, holisztikus kiberbiztonsági kockázatkezelési metodika alkalmazásával a kibertámadások korai szakaszban történő felismerésének és elhárításának valószínűsége jelentősen fokozódik. Hosszabb időtávlatban a projekt eredményei hozzájárulnak ahhoz, hogy a polgári és a katonai ATM-szolgáltatások még kibertámadások vagy a digitális információs lánc váratlan zavarai esetén is biztonságosan működhessenek, garantálva ezáltal, hogy a légi közlekedés a jövőben is megőrizhesse kiemelkedő pozícióját a legbiztonságosabb közlekedési formák sorában.

Felhasznált irodalom

[1] Palik M., *A repülésirányítás alapjai.* Budapest, Dialóg Campus, 2018.

[2] T. De Zan, F. d'Amore, F. Di Camillo, „The Defence of Civilian Air Traffic Systems From Cyber Threats," *Instituto Affari Internazionali,* 2015. Online: https://www.iai.it/sites/default/files/iai1523e.pdf

[3] E. Harison, N. J. Zaidenberg, „Survey of Cyber Threats in Air Traffic Control and Aircraft Communications Systems" *Cyber Security: Power and Technology,* 2018, pp. 199-217. Online: https://doi.org/10.1007/978-3-319-75307-2_12

[4] P. Cornish szerk., *The Oxford Handbook of Cyber Security.* Oxford University Press, 2021. Online: https://doi.org/10.1093/oxfordhb/9780198800682.001.0001

[5] S. Roy, B. Sridhar, *Cyber- Threat Assessment for the Air Traffic Management System: A Network Controls Approach.* NASA, 2016. Online: https://doi.org/10.2514/6.2016-4354

[6] *SecRAM 2.0. Security Risk Assessment Methodology for SESAR 2020.* SESAR Joint Undertaking, 2017. Online: https://www.sesarju.eu/sites/default/files/documents/transversal/SESAR%202020%20-%20Security%20Reference%20Material%20Guidance.pdf

[7] *Air Traffic Management – A Cybersecurity Challange.* Eurocontrol, 2021. Online: https://www.eurocontrol.int/publication/air-traffic-management-cybersecurity-challenge

[8] K. Hemsley, R. Fisher, „A History of Cyber Incidents and Threats Involving Industrial Control Systems," in *Critical Infrastructure Protection XII. ICCIP 2018. IFIP Advances in Information and Communication Technology, vol 542.* J. Staggs, S. Shenoi szerk. Cham, Springer, 2018, pp. 215–242. Online: https://doi.org/10.1007/978-3-030-04537-1_12

[9] K. Bernsmed, G. Bour, „An Evaluation of Practitioners' Perceptions of a Security Risk Assessment Methodology in Air Traffic Management Projects," *Journal of Air Transport Management,* 102. évf. 2022. Online: https://doi.org/10.1016/j.jairtraman.2022.102223

[10] Horváth G., „A helyszíntől független repülőtéri irányítás katonai alkalmazhatóságának vizsgálata a kapcsolódó SESAR-projekt tapasztalatainak tükrében," *Repüléstudományi Közlemények,* 34. évf. 2. sz. pp. 95–106. 2022. Online: https://doi.org/10.32560/rk.2022.2.8

[11] *Opinion 03/2021. Management of Information Security Risks.* European Aviation Safety Agency, 2021. június 11. Online: https://www.easa.europa.eu/en/document-library/opinions/opinion-032021

[12] K. Charitoudi, A. Blyth, „A Socio-Technical Approach to Cyber Risk Management and Impact Assessment," *Journal of Information Security,* 4. évf. 1. sz. pp. 33–41. 2013. Online: https://doi.org/10.4236/jis.2013.41005

[13] J. de Haan, „Specific Air Traffic Management Cybersecurity Challenges: Architecture and Supply Chain," *Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops.* New York, Association for Computing Machinery, 2020. pp. 245–249. Online: https://doi.org/10.1145/3387940.3392223

[14] A. Gurtuv, E. Sofie, „Demonstrating ADS-B AND CPDLC Attacks with Software-Defined Radio," in *IEEE 2020 Integrated Communications Navigation and Surveillance Conference (ICNS).* Herndon, 2020. Online: https://doi.org/10.1109/ICNS50378.2020.9222945

[15] R. Santamarta, *A Wake-up Call for SATCOM Security (Technical White Paper).* IOActive, 2014. Online: https://ioactive.com/wp-content/uploads/2018/05/IOActive_SATCOM_Security_WhitePaper.pdf

[16] R. Milne, „Russian GPS Jamming Threatens Air Disaster, Warn Baltic Ministers", *Financial Times,* 2024. április 28. Online: https://www.ft.com/content/37776b16-0b92-4a23-9f90-199d45d955c3
[17] G. Lykou, G. Iakovakis, D Gritzalis, „Aviation Cybersecurity and Cyber-Resilience: Assessing Risk in Air Traffic Management," in *Critical Infrastructure Security and Resilience, Advanced Sciences and Technologies for Security Applications.* D. Gritzalis, M. Theocharidou, G. Stergiopoulos szerk. Cham, Springer, 2019, pp. 245–260. Online: https://doi.org/10.1007/978-3-030-00024-0_13
[18] Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve (2022. december 14.) az Unió egész területén egységesen magas szintű kiberbiztonságot biztosító intézkedésekről, valamint a 910/2014/EU rendelet és az (EU) 2018/1972 irányelv módosításáról és az (EU) 2016/1148 irányelv hatályon kívül helyezéséről (NIS 2 irányelv) (EGT-vonatkozású szöveg).
[19] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály) (EGT-vonatkozású szöveg)
[20] *Minimum Set of Security Controls, D05-006, Edition 00.06.00.* SESAR, 2013.
[21] K. Bernsmed, M. G. Jaatun, P. H. Meland, „Safety Critical Software and Security – How Low Can You Go?," in *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC).* London, 2018, pp. 1–6. Online: https://doi.org/10.1109/DASC.2018.8569579
[22] *The Global Risks Report 2025, 20th Edition.* Cologny, World Economic Forum, 2025. Online: https://reports.weforum.org/docs/WEF_Global_Risks_Report_2025.pdf
[23] *The CEO's Guide to Cybersecurity.* Boston Consulting Group, 2021. Online: https://media-publications.bcg.com/BCG-Executive-Perspectives-CEO-Guide-to-Cybersecurity.pdf
[24] G. Horváth, „The Cybersecurity Aspect of Remote Tower Optical Systems," *Acta Avionica,* 25. évf. 1. sz. pp. 45–54. 2023. Online: https://doi.org/10.35116/aa.2023.0006
[25] E. Frumento, *The Role of Social Engineering in the Evolution of Attacks.* Figshare, 2020. Online: https://doi.org/10.6084/M9.FIGSHARE.12369248.V1
[26] E. Frumento, C. Dambra, „The HERMENEUT Project: Enterprises Intangible Risk Management via Economic Models based on Simulation of Modern Cyber Attacks," in *Proceedings of the 5th International Conference on Information Systems Security and Privacy ICISSP.* Prague, SciTePress, 2019, pp. 495–502. Online: https://doi.org/10.5220/0007413504950502
[27] *aDvanced sOcial enGineering And vulNerability Assesment Framework.* 2018. Online: https://doi.org/10.3030/653618
[28] A. Tursunbayeva, S. Di Lauro, C. Pagliari, „People Analytics – A Scoping Review of Conceptual Boundaries and Value Propositions," *International Journal of Information Management,* 43. évf. pp. 224–247. 2018. Online: https://doi.org/10.1016/j.ijinfomgt.2018.08.002
[29] T. Elias, *Learning Analytics: Definitions, Processes and Potential.* The Landing-Athabasca University, 2011. Online: https://landing.athabascau.ca/file/download/43713
[30] M. Bourbonniere, „Military Aircraft and International Law: Chicago Opus 3," *Journal of Air Law and Commerce,* 66. évf. 3. sz. pp. 885–978. 2001. Online: https://scholar.smu.edu/jalc/vol66/iss3/2

[31] J. N. Bradbury, „ICAO and Civil/Military Coordination," in *Automation and Systems Issues in Air Traffic Control.* J. A. Wise, V. D. Hopkin, M. L. Smith szerk. Berlin, Heidelberg, Springer, 1991, pp. 301–319. Online: https://doi.org/10.1007/978-3-642-76556-8_30
[32] B. A. Berman, R. K. Dismukes, K. K. Jobe, *Performance Data Errors in Air Carrier Operations: Causes and Countermeasures.* NASA, 2012. Online: https://human-factors.arc.nasa.gov/publications/NASA_TM2012-216007.pdf

Cybersecurity Risk Assessment in Air Traffic Management: The European Methodology

The digitalisation of Air Traffic Management (ATM) systems, the introduction of service-oriented architectures, and data-sharing models significantly increase system complexity and cybersecurity exposure. This paper comprehensively analyses the cybersecurity challenges of modern ATM systems, with particular focus on the practical limitations of risk assessment methodologies (e.g. SecRAM), vulnerabilities in communication protocols (ADS-B, CPDLC), and the cascade effects caused by supply chains and system integration. The study presents the innovative approach of the Horizon Europe SEC-AIRSPACE project, which aims to enhance existing risk management procedures rather than developing new methodologies. The project's key innovations include the development of a holistic ATM taxonomy, consideration of virtualised environments and human factors, and the implementation of dynamic risk monitoring. The results contribute to establishing a cyber resilient ATM ecosystem capable of maintaining the exceptional safety standards of air transportation even in a continuously evolving threat landscape.

Keywords: *cybersecurity, risk assessment, air traffic management, ATM*

Horváth Gábor	Gábor Horváth
doktori hallgató	PhD student
Nemzeti Közszolgálati Egyetem	Ludovika University of Public Service
Katonai Műszaki Doktori Iskola	Doctoral School of Military Engineering
horvath.gabor@uni-nke.hu	horvath.gabor@uni-nke.hu
orcid.org/0000-0002-2939-1426	orcid.org/0000-0002-2939-1426

Jelen mű a Kulturális és Innovációs Minisztérium Doktori Program Doktori Hallgatói Ösztöndíj Programjának a Nemzeti Kutatási, Fejlesztési és Innovációs Alapból finanszírozott szakmai támogatásával készült.