

GULYÁS ATTILA\*

# NYELVI MODELLEK ALKALMAZÁSA A KIBERVÉDELEMBEN

II. RÉSZ

**A** tudományos közlemény második részében összefoglalom az LLM és a kibervédelem lehetséges kapcsolódásait, bemutatom a védelmi szektorban elérhető, megvalósítható eljárásrendeket és megoldásokat.

## A GÉPI TANULÁS LEHETSÉGES TÁMOGATÁSA A KIBERBIZTONSÁG NÖVELÉSE ÉRDEKÉBEN

A világháló a 21. századra a globális kereskedelem, a társas-szociális kapcsolattartás és a katonai alkalmazások kommunikációs terévé vált. A kézzelfogható fizikai (hardver-) követelmények, amelyek a múlt évszázad technológiai szemléletét alapvetően meghatározták, a Moore-törvény [1] alapvetései és predikciói alapján a hardverelemek számítási kapacitásai – a hagyományos chiptechnológia gyártástechnológiája mellett is – jelentősen felülvizsgálandók. Az új, úgynevezett diszruptív technológiák – mint a nagy nyelvi modellek (LLM – *Large Language Models*), a kvantumtechnológiai adatátvitel, kvantum számítástechnika – olyan gyorsan jelennek meg és olyan mélységben forgatják fel a számítástechnikában a megszokott fizikai kereteket, hogy e folyamatok végkimenetelét megjósolni lehetetlen feladat. Ugyanakkor ez a rakétasebességű fejlődés nem jár együtt a szakmai területek, a kibervédelem szabályozóinak fejlesztésével, annak finomhangolása lassabban halad: rendkívül gyors az adott hardver vagy szoftver (vagy mindkettő) termékciklusa, sokszor a megszokott mérnöki diszciplínáktól idegenek a tématerületek, a gyors tervezésből és kivitelezésből, tesztekkel adódóan elnagyolt vagy hiányzó koordináció a fejlesztői elemek között, a folyamatok működési komplexitása nagymértékben megnehezíti a szabályozói környezet kialakítását. Ugyanakkor a szabályozó közeg fejlesztése egyaránt igényli a kemény (hard) jogi szabályozók és a puha (soft) szakmai szabályozó keretek tervezését, alkalmazását is. Ezért a világ gazdaságilag

vezető államai, államszövetségei megkezdtek-folytatták a diszruptív technológiák szabályzó környezetének tervezését, kialakítását és alkalmazását.

1. ÁBRA.  
(Illusztráció: Shutterstock)

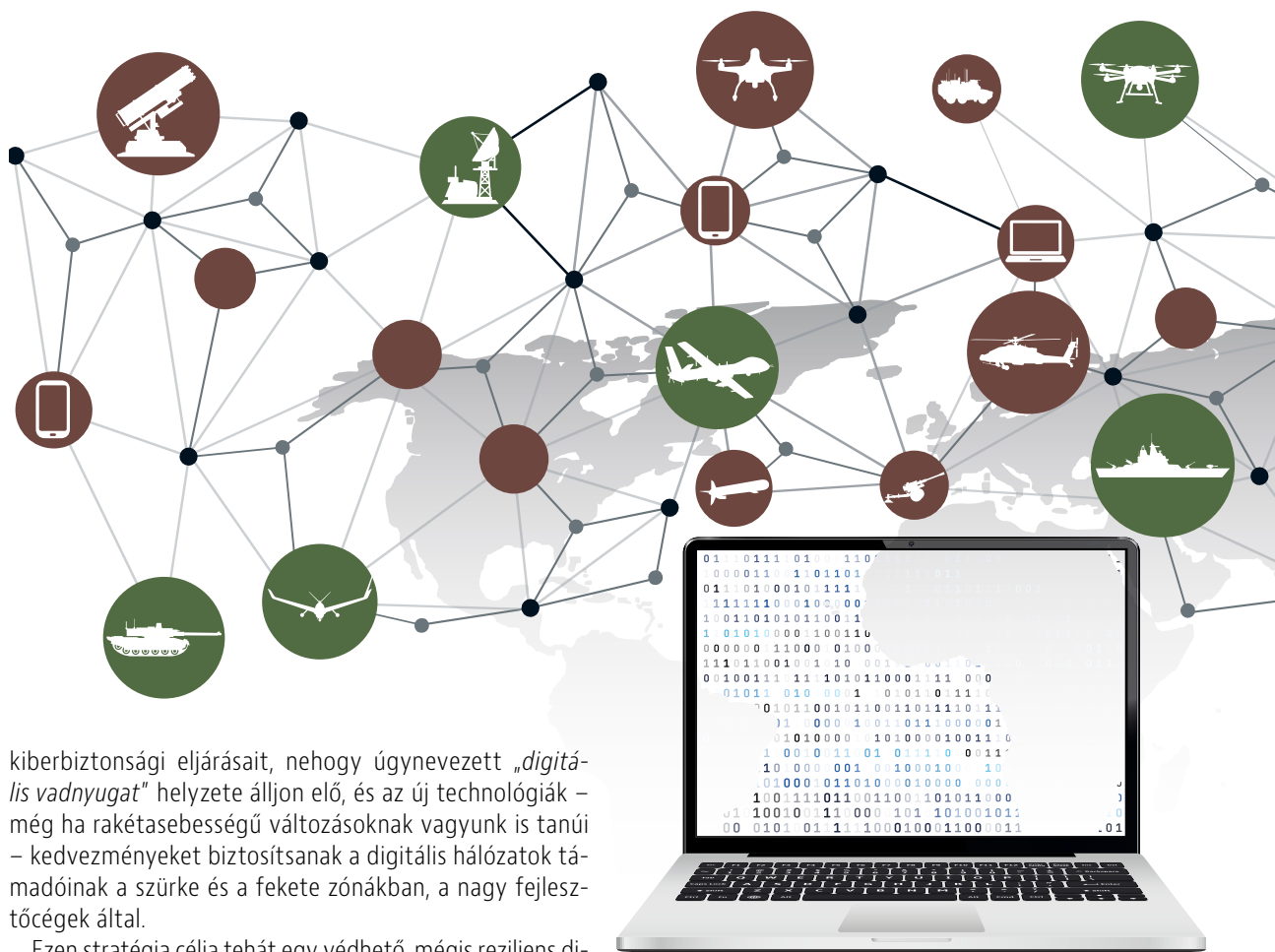
## A KIBERBIZTONSÁGRA VONATKOZÓ AMERIKAI ÉS EURÓPAI UNIÓS SZABÁLYOZÁSI KERETEK VIZSGÁLATA

Úgy vélem, nyilvánvaló, hogy a világ technológiailag vezető műszaki vállalkozásai – a gépi tanulás fejlesztése mellett elkötelezett cégek – elsősorban három földrész szellemileg és gazdaságilag tőkeerős nemzetei közül kerülnek ki. Az Amerikai Egyesült Államok, az Európai Unió tőkeerős és nagy műszaki tervezői hagyományokkal rendelkező országai (Németország, Franciaország, Olaszország, a Benelux államok stb.) és nem utolsósorban Kína álltak az élen a nyelvi modellek fejlesztésében 2025 őszén. Ehhez kapcsolódóan a kibervédelem, a kibertudatosság fejlesztése hatékony szabályozási környezetet igényel, annál is inkább, mivel az LLM fejlesztésének felgyorsulása közel évtizedes történelmet tud maga mögött, és nyilvánvaló, hogy a részletes szabályozó környezet kialakítása hatással lesz a gépi tanulás fejlődésére, annak irányaira és a fejlesztések spektrumára is a kibervédelem támogatásában. Az LLM kibervédelmi alkalmazásának vizsgálatához elsőként az USA és az EU kibervédelmi stratégiáját, valamint néhány EU-tagállam stratégiáját ismertetem pár gondolatban.

Az USA 2023-ban adta ki a Nemzeti Kibervédelmi Stratégiáját, [2] mely rögzíti, hogy az újabb, a diszruptív technológiák megjelenésével párhuzamosan alapvető kibervédelmi szabályozórendszer-módosítást kell elvégezni, amely a világ teljes digitális ökoszisztémáját érinti. Ezen szabályozórendszer-módosítás olyan irányú legyen, hogy a folyamatoknak előnyösebb helyzetbe kell hoznia a felhasználókat és a végpontok kibervédelméért felelős szervezeteket, gyártó vállalkozásokat, azaz a hálózatok

\* Ezredes, csoportfőnök,  
Híradó, Informatikai és  
Információvédelmi  
Csoportfőnökség,  
Honvéd Vezérkar,  
Magyar Honvédség.  
ORCID:  
0000-0001-5774-5757





2. ÁBRA.  
(Grafika: Győri László)

kiberbiztonsági eljárásait, nehogy úgynevezett „*digitális vadnyugat*” helyzete álljon elő, és az új technológiák – még ha rakétasebességű változásoknak vagyunk is tanúi – kedvezményeket biztosítsanak a digitális hálózatok támadóinak a szürke és a fekete zónákban, a nagy fejlesztőcégek által.

Ezen stratégia célja tehát egy védhető, mégis reziliens digitális környezet kialakítása, amelyben nagy szerepet kap a vállalati és a személyes adatok elektronikus információbiztonságának növelése, védelme és annak elkerülése, hogy kibertámadás esetén a hibák és az incidensek kezdeményezése végzetes láncreakcióhoz vezessen, azaz katasztrofális, visszafordíthatatlan eseményekhez. [3] Ebben a közegben értelmezhetőek leginkább a mesterséges intelligenciával (MI) kapcsolatos kutatások eredményei, amelyek fokozzák a lehetséges védelmi megoldások skálázhatóságát, azok összetettségén keresztül. A stratégia szerint a szabályozói környezet átalakításának úgy kell megvalósulnia, hogy a végfelhasználói felelősségnek csökkennie kell, míg a digitális szféra legjobban pozícionált szereplőinek magasabb felelősségvállalására van szükség a digitális reziliencia növekedése érdekében. Hiszen az egyének, a kis- és közepes vállalkozások, az államigazgatási apparátus elemei, a stratégiai közműszolgáltatók (pl. villamosművek, gáz- és olajipari vállalkozások, nukleáris komplexumok, a kritikus infrastruktúra elemei) korlátozott kiberbiztonsági erőforrásokkal rendelkeznek, ugyanakkor a saját és a velük összekapcsolt digitális hálózatukat érintő döntéseik kiemelten negatív következményekkel járhatnak a teljes társadalomra vonatkoztatva.

E stratégia pilléreit az alábbiak szerint határozták meg. A legfontosabb feladatok a kritikus infrastruktúra védelme, a hatékony válaszlépések megfogalmazása kibertámadások esetén, a digitális környezet formálása az adatkezelők felelősségének a növelésével, biztonságosabb IoT- (*Internet of Things*, magyarul *A dolgok internete*) eszközök fejlesztése,

se, az LLM fejlesztéseinek nagyobb arányú és szabályozott integrálása az adatok kiberbiztonsági védelmi folyamataiba, és nem utolsósorban, országhatárokon átívelő nemzetközi partnerség a közös kiberbiztonsági védelmi célok elérésére.

Visszatérve az európai szárazföldre, az Európai Kiberbiztonsági Ügynökség (*EU Agency for Cybersecurity*) 2023 márciusában adta ki kiberbiztonsági előjelzését [4], amiben 11 fő kockázati területet jelöltek meg mint kiberbiztonsági szempontból elsődlegesen veszélyeztetett területeket. [5] Ezek közül kiemelem a szoftverfejlesztői lánc kompromittálódását, amelynek máris vannak jelei a távol-keleti alkalmazások (hardver- és szoftverelemek) telepítésekor, üzemeltetésekor.

Másik jelentős terület az ellátási láncok sérülékenysége, amely szintén súlyos veszélyeket rejt magában, különösen az alkalmazói szoftverkörnyezetnek a diszruptív technológiákkal való együttes alkalmazása esetében. [6] Ugyanakkor mind a 11 terület élénk figyelmet és azonnali beavatkozás igényel. Az EU válasza az ellátási-lánc-biztonsági szabályok szigorítása, a *zero-trust-policy* (zéró bizalom elv) bevezetése mind a polgári [7], mind a NATO oldaláról [8] a katonai beszerzések területén. [9]

A digitális hálózatok szabályozói környezete kiberbiztonságának kialakításában jelentős lépés volt a 2016. évi NIS (Network Information Security) szabályrendszer elfogadása (2016/1148. EU irányelv). [10] A NIS1 meghatározta



az uniós kiberstratégiát, a kiberbiztonság kereteit, ugyanakkor, mivel ez egy irányelv, ezért az EU-tagállamok szabádon értelmezheték annak tételeit. Ez összetett stratégiák elfogadásának, illetve eltérő szabályozási lehetőségeknek nyitott utat. [11] Az orosz–ukrán háború tapasztalatai alapján a nemzeti kiberstratégiák revíziója, a kibervédelem megerősítése alapjaiban igényelte az EU-s szabályozói környezet átalakítását. 2022 végén, hosszas EU-s egyeztetéssorozatot követően új szabályzók jelentek meg, a NIS2 irányelvek (2022/2555. EU irányelv). [12] Ebben a hibrid térben jelentkező fenyegetettségekre adott nemzeti válaszok egységesítésére, a szabályzók finomhangolására tettek kísérletet a jogalkotók.

A NIS2-ben már hangsúlyosan jelenik meg az ellátási-lánc-biztonság kiberoldali megteremtése, és egyértelmű műszaki javaslatokat határoznak meg (24. cikk 2. bekezdés): kockázatelemzés, eseménykezelés és központosított jelentési kötelezettség, szabályzatok és eljárásrendek kriptográfiája stb. [13] Látható tehát, hogy egyrészt a NATO keleti határainál zajló háború kiberincidensei, de nem kisebb részben a diszruptív technológiák, benne kiemelten a gépi tanulási modellek nagyarányú fejlesztése, azok alkalmazása alapvetően változtatta meg a digitális hálózatokkal összefüggő gondolkodást, és nyilvánvalóvá vált az igény a kiberbiztonság uniós védelmi képességének és szintjének növelésére.

Az MI-kutatás oldaláról azt kell vizsgálnunk, hogy a kiberbiztonsági szabályzók tételei hogyan jutnak érvényre a gépi tanulási modellek fejlesztésekor, milyen lépéseket lehet előtervezni és elvégezni annak érdekében, hogy az LLM a jelenleginél nagyobb hatásfokkal támogassa a digitális hálózataink kibervédelmét. A 2024 márciusában elfogadott EU MI jogszabálya [14] e területen is segítségünkre van abban az értelemben, hogy az MI etikus fejlesztésre, üzemeltetésére, egyszóval annak átfogó alkalmazására tesz iránymutatásokat. [15]

E jogszabály alapján a kockázatokat, fenyegetettségeket 4 alapvető kategóriába soroljuk be: minimális, korlátozott, magas és elfogadhatatlan szintű kockázatok. [16] A jogszabály részletesen levezeti, mely kategóriába mely fenyegetettség-csoport tartozik. A jogszabályt 2026-tól kell teljeskörűen alkalmazni az EU tagországaiban. [17]

Természetesen az EU-tagországok külön-külön is megalkották MI-stratégiájukat. Olaszország a 2024–2026-os időszakra [18] külön stratégiákat fogalmaz meg a kutatás-fejlesztés, a kormányzati adminisztráció, a kis, közepes- és nagyvállalkozások (üzleti élet), emellett az oktatás-képzés szakterületeinek stratégiai szintű felügyeletére.

Magyarország 2025 szeptemberében újította meg és adta ki MI-stratégiáját, [19] amely alapvető tudományos-műszaki-társadalmi területeket jelöl ki, mint az MI-alkalmazás szempontjából nagy odafigyelést és körültekintést igénylő szakterületek. A magyar stratégia alapján az MI használatát ösztönözni kell a gépgyártás- és ipari gyártástámogató autonóm rendszerek fejlesztésében, az adatvezérelt egészségügyben, a digitális agráriumban, az államigazgatásban, az energetikában és a logisztikában, valamint a közlekedés szabályozásában, irányításában.

Németország 2020-ban adta ki stratégiáját, [20] amely alapvetően a fent említett országokban és folyamatokban részletezettekhez hasonlóan tervez a következő 10 éves ciklusban. A német cél, hogy az MI-kutatásban európai, sőt világszinten élenjáró nemzetté váljon („AI – Made in Europa”), jelentős francia támogatással, hogy eredményesen használja az MI-t a tudásátadásban, az oktatás-képzés területein, a polgári és védelmi ipari automatizálásban, a kutatás-fejlesztésben és nem utolsósorban az adatbiztonság területein, a kiberbiztonság megteremtésében is. [21]

Franciaország határozottan kiáll az MI-fejlesztések mellett. Emanuel Macron elnök a 2025 februárjában tartott EU MI konferencián [22] sürgette a közös EU-s MI-stratégia jelentősebb anyagi/pénzügyi támogatását, pénzügyi források bevonását az MI európai fejlesztéseibe. [23]

Látható tehát, hogy a felsorolt stratégiák alkotói ugyan nem látnak a jövőbe, mégis kereteket kívánnak szabni az MI felhasználásának, kitekintéssel a jelenleg elképzelt lehetőségekre. Ugyanakkor, ahogyan már bemutattam, az MI-kutatás, az LLM fejlődése – egyelőre – nem szorítható korlátok közé. Mint diszruptív technológia, gyakorlatilag nem

3. ÁBRA. (Illusztráció: Shutterstock)



látható, milyen irányban fejlődik és legfőképpen, hogy milyen ütemben. A fejlődés iránya tehát nem jelezhető előre, különösen annak fényében, hogy mind Amerikában, mint Európában, de Kínában is csillagászati összegeket fektetnek be e kutatási terület mind nagyobb arányú fejlesztésébe. [24] A továbbiakban azt vizsgálom, hogyan alkalmazható az LLM a hálózataink kibervédelmében.

### A GÉPI TANULÁSI MÓDSZEREK LEHETSÉGES FELHASZNÁLÁSI LEHETŐSÉGEI A KIBERBIZTONSÁG TÁMOGATÁSÁBAN

Ahogy a napi életünk egészét behálózzák a digitális informatikai hálózatok, azok felhasználása folyamatossá vált, így ezen hálózataink védelme, a digitális biztonság, vagy más néven a kiberbiztonság tudatossága, a védelmi képességünk fokozása alapkövetelmény minden felhasználó számára. Vizsgáljuk hát meg, melyek a leggyakoribb fenyegetettségek ezen digitális hálózatokban. A gyakori fenyegetések egyes elemei közé tartoznak azon kártékony célra tervezett alkalmazások, programok, amelyek magukban foglalják a vírusokat, zsarolóprogramokat, hálózati „worm”-okat, férgeket, az adathalászat más eljárásait, a megtévesztő eszközöket. [25]

Ezen támadási módok mélyebb megértése nagyban elősegíti a támadásokra való felkészülést, a megelőzést vagy – ha a hálózati behatolás megtörtént – a védekezés lépéseit. [26] Ezért a hálózatvédelem aktív eszközei, pl. a tűzfalak nagyarányú alkalmazása, az adatok titkosítása, a víruskeresés és behatolásdetektálás, illetve az incidensmenedzsment és a kockázatkezelési gyakorlatok levezetése alapvetés a rugalmas és adaptálható, személyre szabott kibervédelem megtervezésekor, kialakításakor. Ugyanakkor belátható, hogy a digitális technológiák fejlődésével a kiberbiztonsági kihívások is változnak, szintet lépnek, és az arra adott válaszokban a modern technológia vívmányainak az alkalmazására lehet szükség. Tehát a proaktív intézkedések – bevonva az LLM támogatását – jelentős szerepet játszanak a dinamikus és adaptív védelem kialakításában és fenntartásában, jelen korunk változó digitális környezetében.

Első és talán legalapvetőbb feladat a hálózatokban a kibertámadások felismerése. Ebben jelentős támogatást képes nyújtani a gépi tanulás általi felkészülés, az előkészületek. Az intelligens algoritmusok képesek felügyeletet biztosítani és azonosítani a mintázatokat a hálózati forgalomban, az adatcserében és a gyanúsnak ítélt adatcsomagokat alaposabb vizsgálat alá vonni. [27] Az MI képes nagy sebességű hálózatellenőrzésre és a rendellenességek azonosítására, amit az emberi vizsgálatok keretei között nem tudnának elvégezni. A mintavételezést követően az MI-vezérelt védelmi rendszer javaslatokat tud megfogalmazni a hálózatüzemeltető (ember) felé arról, milyen lépést tart arányosnak. A feldolgozott adatokból a gépi tanulás képes következtetések levonására, statisztikák készítésére, [28] azaz tanul a korábbi incidensekből, valamint fel tudja használni ezen ismereteket egy újabb interakció esetében.

Fontos hangsúlyozni, hogy a detektálás és a jelzés szintjét biztosítják az MI-támogatott kibervédelmi eljárások. [29] A döntéseket a digitális hálózatot üzemeltető mér-



nöki állomány hozza meg, akiknek alapvető tevékenysége a sérülékenységvizsgálat, melynek célja feltárni a támadási lehetőségeket, a réseket a védelmi rendszerekben, annak érdekében, hogy a lehetséges behatolási pontokat időben fel lehessen térképezni. Ezen tevékenység támogatására az MI, ezen belül a gépi tanulási modellek nagy támogatást képesek nyújtani a korábbi behatolási minták vizsgálatával. Az MI alkalmas figyelmeztetésre és azonnali beavatkozásra jogosulatlan hozzáférés megkísérlése vagy gyanús bejelentkezési kísérletek sorozatos ismétlése esetében. Ily módon lehetőséget biztosíthat a szenzitív adatok megőrzésére különböző adatvédelmi protokollok, adattitkosítási eljárások használatával. [30] Az MI képes az ütemezett, automatizált hardver- és szoftverellenőrzésre, ami feltárja a lehetséges hálózati sérülékenységet akár a gyártói biztonsági frissítések áttekintésével is. Ezen „szkenelés” az adott digitális hálózat szegmenseinek különböző pontjain helyezhető el, akár a hálózatokon belüli, további zárt hálózatrészek (DMZ – demilitarizált zóna, zárt belső VPN – Virtual Private Networking, [31] azaz már átvizsgált és megbízhatónak azonosított hálózatrész). Az összegyűjtött adatok, információk lekérdezhetőek, statisztikai célokból újjászervezhetőek, ezen keresztül felhasználhatóak a gépi tanulás feladataira (központosított naplózó, monitoring és eseménykezelő rendszerek).

A gépi tanulással felderíthetővé válnak a hálózaton, az eszközökön levő elsődleges és további operációs rendszerek platformjai, a megfelelő jogosultságok rendelkezésre állásával megvalósulhat az operációs rendszerek, patchek folyamatos, naprakész ellenőrzése annak érdekében, hogy a gyenge beállításokat naplózzuk, felderítsük, rögzítsük. A gépi tanulási eljárások képesek a sérülékenységet a nemzetközi ajánlás szerinti CVE (Common Vulnerabilities and Exposures: megszokott sérülékenységek és sebezhetőségek) [32] alapján kockázati osztályokba rendezni (kritikus, magas, közepes, alacsony), ahol a kritikus és a magas sérülékenységek hibajavítását elsődlegessé kell tenni. [33]

Abban az esetben, ha megtörténik az incidens, a gépi tanulási eljárások a már rendelkezésre álló incidensadatokból, adatbázisokból, váratlan eseményekről és támadási



módszerekről összeállított mentésekből, elemzésekből segítenek azonosítani a támadókat. A gépi tanulási modellek képesek a nagyméretű naplófájlok áttekintésére az emberi vizsgálatok töredékideje alatt, és ezzel nagyban elősegítik az incidensek kategorizálását, a támadók és a támadási eljárások azonosítását, ezen keresztül gyorsabb és hatékonyabb felderítését. Ide tartozik a hibás, téves riasztások naplózása és adatbázisba gyűjtése, amely nagymértékben támogatja a további incidenskezelés folyamatát. [34] A gépi modellek a támadási minták, mintázatok átfogó analízisével az üzemeltetői mérnöki állományt képes támogatni egyszerűsített összefoglalók összeállítása révén. [35]

A gépi tanulás automatizált folyamatai tekintetében – a digitális hálózatok védelme érdekében – kiemelten fontos az LLM gyors adatfeldolgozó képessége a biztonsági akadályok javításában. A hagyományos statikus alkalmazásbiztonsági eszközök a kódok elemzését követően listázzák a javításra váró biztonsági réseket, majd a mérnöki állománynak személyesen be kell avatkoznia ezek elhárítására; ez idő- és energiaigényes folyamat. [36] Léteznek gépi tanulási módszerekre építő alkalmazások, algoritmusok, amelyek az emberi feldolgozási időnél sokkal rövidebb idő alatt elemzik a rendelkezésre álló kódokat, kódcsoporthatásokat, és javaslatot is tesznek azok javítására. [37]

Fontosnak tartok néhány gondolatot szentelni a kiberhírszerzés (CYBINT – *Cyber Intelligence*) témakörének is, ami – katonai hírszerzési értelemben – szorosan kapcsolódik a fent bemutatott, tárgyalt tématerületekhez. A kiberhírszerzés célterületét a digitális hálózatokban üzemelő, az informatikai hálózatokban üzemelő, felhasznált, vizsgált munkaállomások, munkaállomás-csoportok, belső (DMZ) hálózatok képezik, melyek mélyreható ismerete, feltérképezése alapvető műveleti érdek mind a hálózatainkat védő, mind a támadó tevékenységek folyamán. A CYBINT e hálózatokon keresztül elérhető: olyan adatok, információk megszerzésére irányul, amelyet az információ birtokosa (információgazda) nem kíván megosztani más, külső személlyel vagy hálózattal, tehát azok védelme kiemelt fontossággal bír. Ily módon a szükséges információ megszerzése történ-

het a digitális hálózatba való betöréssel, de akár a hálózatok és az azokat alkotó számítógépes munkaállomások által kisugárzott jelekből történő adatszerzés útján is.

Itt figyelemmel kell lenni a folyamatosan jelen lévő, rejtett fenyegetésként értékelendő folyamatokra [38] (APT – *Advanced Persistent Threats*). Az APT olyan támadási forma, amely nem titkolt célja, hogy a behatolást követően a penetrált rendszerben minél több adatbáziscsoportot, rendszerelemet érjen el, a hosszan tartó jelenlétét képes legyen biztosítani, egyfajta „alvó ügynökként”, amely a megfelelő feladatszabás alapján mozgósítható. [39]

Az APT-csoportok – a célok alapján – négy osztályba sorolhatóak. [40] Az első csoport az állami tulajdonú információkat célozza meg. A második csoport a motiváción alapuló támadási cselekményeket tartalmazza. Továbbá lehet a cél pusztán a hálózatbetörés, a behatolás igénye mint szakmai kihívás. A negyedik csoport célja lehet a behatolást követően az adott rendszerben való rombolás, adattörés, adatelbirtoklás vagy manipuláció igénye. A gépi tanulás segíti az APT-re való felkészülést a rendelkezésre álló rejtjelkulcsok gyors áttekintésével, megfejtésével, a biztonsági rések önműködő és rövid időintervallum alatti felderítésével és naplózásával, az elhárításhoz szükséges információk gyors kinyerésével. A gépi tanulási eljárások lehetővé teszik – APT esetén – az információk megosztását más hálózati szereplőkkel, annak érdekében, hogy más, eltérő digitális hálózatokban a behatolásdetektálás egy magasabb szinten jelentkezzen.

A biztonságtudatosság oldaláról vizsgálva az informatikai hálózati folyamatokat, fontosnak tartom megjegyezni, hogy az MI-rendszerek, benne a gépi tanulás eljárásai, nem helyettesíthetik a józan emberi döntéseket. [41] Hogy ez így marad-e a következő rövid időintervallumban (2-5 év), nem látható, olyan nagy léptékű és gyors ennek a diszruptív technológiának a térnyerése. Ami különös figyelmet igényel, a közösségimédia-platformokon elkövetett káros cselekmények [42] visszaszorítása, a jelszavak ellopása, ellesése, a megtévesztésen alapuló csalások (*social engineering*) csökkentése, az IT (*Information Technology*)

5. ÁBRA.

(Grafika: Győri László)

6. ÁBRA. Az Európai  
Kiberbiztonsági  
Ügynökség logója  
(Forrás: Wikipedia)



-személyiséglopás és a hozzá kapcsolódó káros tevékenységek, vagy a hivatalos információk nyilvános hálózaton való megosztása. [43]

A katonai vezetési és irányítási (C2 – *Command and Control*) rendszerek egyre inkább felhasználják a digitális hálózatok nyújtotta szolgáltatásokat, a modern hadszíntéren a kölcsönösen összekapcsolt és illesztett információs hálózatok, rendszerek alkotják a vezetéstámogatás gerincét. Ennek megfelelően, a C2-t támogató híradó és informatikai rendszerek összeállítását úgy kell megtervezni, hogy az egységes egészbe foglalja a harcászati, a hadműveleti és a stratégiai vezetési elemek (szakasz, század, ezred, dandár, hadosztály, hadtest, harcászati, hadműveleti és stratégiai felsővezetés vezetési pontjainak hálózata) teljes egészét. Belátható, hogy ez szervezési, de műszaki értelemben is jelentős erőösszpontosítást igényel, hiszen a vezetési rendszer elemei – ilyen kiterjesztett volumenben – bizonyosan felhasználnak a rendelkezésre álló vezetékes és vezetékek nélküli átviteli csatornák összetett rendszerét, azaz részletes tervezés szükséges a rádió, a rádiórelé, a rez- és optikai kábelekkal összekapcsolt, a műholdas adatátvitelt is felhasználó összetett információs rendszerek kialakítására. Ezen vezetési rendszerek zárt, minősített, rejtjelezett adatátvitelt biztosítanak, korlátozott kijárással a világháló felé, amely ugyan redukálja a behatolást, de nem teszi lehetetlenné. A szigorú hálózatkiakítási rendszabályok, a munkaállomásokon alkalmazott fizikai, személyi, dokumentum- és elektronikus információvédelmi szabályzók ugyanakkor szavatolják az illegális tevékenységek korlátok között tartását. A C2 programokban hasznos támogatást képes nyújtani a gépi tanulás, mivel az nemcsak a kibervédelmi tevékenységeket végzi, végezheti el, hanem a hálózati adatforgalom szervezésében, az adatátviteli csatornák skálázhatóságában (pl. alá- és fölérendeltség prioritizálása, adatcsere sebessége) is képes támogatásra. Összességében a C2 rendszerek automatizálásában és a hálózati forgalommenedzsmentben az emberi tevékenységeknél összehasonlíthatatlanul gyorsabban és megbízhatóbban képes döntések előkészítésére.

## ÖSSZEGZÉS

A gépi tanulás mint műszaki megoldás forradalmasítja a digitális hálózatokban végzett összes cselekményt. Ebbe beleértendő az emberi hang értelmezése, azaz annak megértése, az emberi gondolkodás modellezése és a mélyebb megértésen keresztül a hangfeldolgozás automatizálása, a gondolkodás felgyorsítása olyan széles körű, mélykutatásokból (adattápanyászat) előálló adathalmazok, adatbázisok folyamatos

eléréséből eredő helyzeti előnnyel, amely nagyban támogatja az emberi döntéselőkészítést. [44] Az LLM megjelenik a digitális hálózataink minden szolgáltatásában, az egyének és a vállalkozások online életében, az adatbázis-kutatás támogatásával a döntési folyamatok felgyorsításában. Miért lenne más a kibervédelem, a hálózataink széles körű vizsgálata és káros tartalmak elleni védelme? Egyértelműnek tartom, hogy a kibervédelem területén is nagyban lehet és kell is támogatást igényelni az LLM szolgáltatásaiból.

Úgy vélem, a továbblépést, a további fejlődést szavatolja, ha az LLM felhasználását a kibervédelmi szférában legalább két terület fejlesztésében felgyorsítjuk. Elsőként meg kell teremteni, pontosítani kell, illetve skálázhatóvá kell tenni a gépi tanulás szabályozását a kibervédelmi területen. A nagy fejlesztő vállalkozások, tőkeerős nemzetek máris tettek és tesznek lépéseket egyfajta szabványosításra a gépi tanulási eljárások automatizálására és szabályozására. Itt az a kitétel, hogy a gépi modellek vezető szerepet töltenek be a tanulási folyamatokban, de a döntéselőkészítést követően mindig kell lennie emberi beavatkozási lehetőségnek, tehát olyan döntési pontnak, ahol az emberi elme beavatkozik és meg-hozza a döntést a további lépésekről. [45]

Másrészről a kutatásoknak, benne a gépi tanulás védelmi (katonai és rendvédelmi) jellegű felhasználásáról szóló vizsgálatoknak arra kell választ találniuk, hogyan lehet a katonai vezetési rendszerek automatizált kiberműveleti folyamatait az LLM támogatásával úgy meghatározni, hogy az a kibervédelem szabályzóit a maximális szinten fenntartsa. Ugyanakkor a katonai döntéshozóknak – mint legfelsőbb szintű döntési elemeknek – képesnek kell lenniük a gépi tanulás támogatásával előállított adathalmazok felett is önálló döntéseket hozni, azaz az automatizálásnak, a gépi döntések autonómiájának bizonyos határokat kell szabni. [46]

Ez az összetett feladatrendszer nagy odafigyelést igényel a tervezés oldaláról is, hiszen tekintettel kell lennünk az adott nemzet önálló műveletei kibervédelmének LLM támogatásától egészen a több hadszínteres, egyesített NATO-műveletek eredményes végrehajtására is. Úgy gondolom, a gépi tanulás a kibervédelemben ezen a műveleti spektrumon teljesebb csak ki igazán, hiszen a NATO Híradó és Informatikai Ügynökség (NCIA – *Communications and Information Agency*) kibervédelmi erőfeszítéseinek a gépi tanulás oldaláról való támogatásához ezen a szinten kell igazán a komplex támogatás. [47]

A továbbiakban tehát e kettős vizsgálati terület korrelációja hozhatja meg a kívánt eredményeket a gépi tanulás kibervédelmi tervezésének (katonai) vonatkozásában. Mindkét terület további kutatást és – a műszaki eljárások kidolgozását követően – jelentős számú vizsgálati eljárás kidolgozását, [48] végrehajtását igényli annak érdekében, hogy a későbbi, a kialakított polgári és/vagy hon- és rendvédelmi információ hálózatunk a rendszer (műszaki) optimumán működjék. ■

A 2022-2.1.1-NL-2022-00012 azonosító számú *Kooperatív Technológiák Nemzeti Laboratóriuma projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási, Fejlesztési és Innovációs Alapból nyújtott támogatásával, a 2022-2.1.1-NL Nemzeti Laboratóriumok Létrehozása, Komplex Fejlesztése pályázati program finanszírozásában valósul meg.*

## HIVATKOZÁSOK

- [1] Hronszy I.: A prekompetitív innováció iparági szintű megszervezhetőségéről a Moore törvény története alapján. In: Inzelt Annamária – Bajmócy Zoltán (szerk.): Innovációs rendszerek. Szereplők, kapcsolatok és intézmények. JATEPress, Szeged, 2013, 144–145. <https://eco.u-szeged.hu/kutatas-tudomany/tudomanyos-kozlemenyei/innovacios-rendszerek/hronszy-imre> (Letöltve: 2026.01.19.)
- [2] Molnár D. – Nagy G.: A 2023-as amerikai kibertérrel kapcsolatos stratégia áttekintése és értékelése. Hadtudomány folyóirat 2023/3, 88–100. DOI: <https://doi.org/10.17047/Hadtud.2023.33.E.90> (Letöltve: 2025.02.14.)
- [3] Vikman L.: Az információs technológiák fejlesztésének és kereskedelmének aktuális biztonsági és szabályozási kérdései. 2023. In: Kibertéri műveletek és ellenálló képesség, a kibertéri műveletek egyes állami és jogi kérdései. Gondolat kiadó 2024, 215–230. <https://s2prodstorage.blob.core.windows.net/s2cmsblob/Files/Kiadvanyok/Kibert%C3%A9r%C3%B3l%20a%20ellen%C3%A1ll%C3%B3s%C3%A9g%C3%A9rt%C3%A9kel%C3%A9se.pdf?sp=r&st=2025-03-25T09:37:58Z&se=2035-03-25T16:37:58Z&spr=https&sv=2024-11-04&sr=c&sig=PAOb3jtCphbbzRgBEutrTUH2uSjRNnF3G8dVaL8Y3Z0%3D> (Letöltve: 2026.01.19.)
- [4] ENISA (Európai Unió). <https://www.enisa.europa.eu/> (Letöltve: 2025.01.12.)
- [5] ENISA, Identifying Emerging Cyber Security Threats and Challenges for 2030. 2023.07.22. <https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Foresight%20Cybersecurity%20Threats%20for%202030.pdf> (Letöltve: 2025.01.23.)
- [6] EU Cybersecurity Strategy. 2025.02.11. <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy> (Letöltve: 2025.01.02.)
- [7] Europe's Digital Decade. 2025.02.11. [https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future\\_en](https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/shaping-europes-digital-future_en) (Letöltve: 2025.01.22.)
- [8] A NATO hivatalos internetes oldala 2025.02.01. [https://www.nato.int/cps/en/natohq/topics\\_78170.htm](https://www.nato.int/cps/en/natohq/topics_78170.htm) (Letöltve: 2025.01.25.)
- [9] Damiano, S. – Scatto, E.: L'approvazione della nuova Cyber Defence Policy, definita ora "Comprehensive", è stata presentata come una necessità vista l'escalation di ransomware e altri attacchi che hanno preso di mira infrastrutture critiche e istituzioni democratiche. I capisaldi 2021.06.17. <https://www.agendadigitale.eu/sicurezza/nato-la-nuova-cyber-defence-policy-ecco-le-priorita-della-leanza-nella-difesa-dello-spazio-cibernetico/> (Letöltve: 2025.02.22.)
- [10] Az Olasz Köztársaság hivatalos internetes oldala, 2025.02.08. <https://www.itgovernance.eu/it-it/nis-directive-it> (Letöltve: 2025.01.31.)
- [11] Szádeczky, T.: Az IT biztonság szabályozása. Beau Bassin GlobeEdit, 2018, 66–120. [https://real.mtak.hu/80757/1/978\\_620\\_2\\_48764\\_1\\_u.pdf](https://real.mtak.hu/80757/1/978_620_2_48764_1_u.pdf) (Letöltve: 2025.01.30.)
- [12] Az ENTRUST vállalkozás hivatalos internetes oldala. NIS2. 2025.02.02. <https://www.entrust.com/it/resources/learn/nis-2> (Letöltve: 2025.01.31.)
- [13] Kis M. et al.: A NIS2 hazai bevezetésének folyamata és kockázatai. Hadmérnök folyóirat 2024/3, 169–175. DOI: 10.32567/hm.2024.3.10 (Letöltve: 2025.03.31.)
- [14] EU Artificial Intelligence Act. 2024. márc. <https://artificialintelligenceact.eu/the-act/> (Letöltve: 2025.01.30.)
- [15] EU AI Act summary. 2024. márc. <https://artificialintelligenceact.eu/wp-content/uploads/2024/11/Future-of-Life-InstituteAI-Act-overview-30-May-2024.pdf> (Letöltve: 2025.02.21.)
- [16] European Commission: AI Act 2024. <https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai> (Letöltve: 2025.01.31.)
- [17] Bederna, Zs.: A mesterséges intelligencia rendszerek megfigyelése. Hadmérnök folyóirat 2024/3, 121–124. <https://folyoirat.ludovika.hu/index.php/hadmernok/article/view/7676/6193> (Letöltve: 2025.01.31.)
- [18] Strategia Italiana per l'Intelligenza Artificiale 2024-2026. AGID. [https://www.agid.gov.it/sites/agid/files/2024-07/Strategia\\_italiana\\_per\\_l\\_Intelligenza\\_artificiale\\_2024-2026.pdf](https://www.agid.gov.it/sites/agid/files/2024-07/Strategia_italiana_per_l_Intelligenza_artificiale_2024-2026.pdf) (Letöltve: 2025.02.11.)
- [19] Innovációs és Technológiai Minisztérium: Magyarország mesterséges intelligencia stratégiája. 2025. szept. <https://cdn.kormany.hu/uploads/document/c/c0/c0d/c0dfdbd37cfa520ae37361a168d244c85e7295af.pdf> (Letöltve: 2025.01.31.)
- [20] Federal Government of Germany: Artificial Intelligence Strategy of the German Federal Government 2020 update. <https://doi.org/10.71063/DJTTT.2025.1104> (Letöltve: 2025.01.31.)
- [21] German platform for AI: Political strategies for AI. Federal Ministry of Education and Research. <https://doi.org/10.70315/uloap.ulahu.2025.0202001> (Letöltve: 2025.02.04.)
- [22] European Union AI Summit Paris France. 2025.02.10–11. <https://www.elysee.fr/en/sommet-pour-l-action-sur-l-ia> (Letöltve: 2025.03.21.)
- [23] Greenacre, M.: Macron calls for ambitious EU innovation strategy in AI, cleantech, defence. Science and Business, 2025.01.09. <https://sciencebusiness.net/news/eu-budget/macron-calls-ambitious-eu-innovation-strategy-ai-cleantech-defence> (Letöltve: 2025.04.11.)
- [24] Access Partnership: Trump announces private-sector \$500 billion investment in AI infrastructure 2025.01.22. <https://accesspartnership.com/opinion/access-alert-trump-announces-500-billion-ai-infrastructure-project/> (Letöltve: 2025.01.22.)
- [25] Wang, A. et al.: Large language models that replace human participants can harmfully misportray and flatten identity groups. Nature Machine Intelligence, Princeton University, 2025.02.17. doi.org/10.17605/OSF.IO/7GMZQ (Letöltve: 2025.01.23.)
- [26] Silva, G., Westphall, C.: A survey of large language models in cybersecurity. 2024.02.26., 2–4 doi.org/10.48550/arXiv.2402.16968. (Letöltve: 2025.03.17.)
- [27] Jian, L.: Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering, 2018/12, 1462–1474. <https://doi.org/10.1631/FITEE.1800573> (Letöltve: 2025.02.17.)
- [28] Deepaa, S. et al.: Intelligent network intrusion prevention feature collection and classification algorithms. Algorithms, 2021/8. <https://doi.org/10.3390/a14080224> (Letöltve: 2025.02.17.)
- [29] Bereczki, D. et al.: A mesterséges intelligencia helye és szerepe az államok és társadalmak 21. századi biztonságában. In: Farkas Ádám et al. (szerk.): Kibertéri műveletek és ellenálló képesség. A kibertéri műveletek egyes állami és jogi kérdései. Gondolat Kiadó, 2024, 206–208.
- [30] ITIL – az informatikaszolgáltatás módszertana, 2002 novemberében. KFKI Számítástechnikai Rt. Verzió: 3.1. Módszertani összefoglaló. [https://itsmf.hu/documents/itil2modszertan\\_osszefoglalo\\_v3.1.pdf](https://itsmf.hu/documents/itil2modszertan_osszefoglalo_v3.1.pdf) (Letöltve: 2026.01.19.)
- [31] DMZ. <https://doi.org/10.1055/a-2661-5109> (Letöltve: 2025.01.12.)
- [32] CVE-2006-2370. <https://doi.org/10.1055/a-2661-5109> (Letöltve: 2025.01.12.)
- [33] Tihanyi N. et al.: Biztonsági tesztelés a gyakorlatban. Nemzeti Közszerológiai Egyetem, Budapest, 2014, 10–14. [https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/biztonsagi-tesztelés-a-gyakorlatban.original%20\(1\).pdf](https://kti.uni-nke.hu/document/vtkk-uni-nke-hu/biztonsagi-tesztelés-a-gyakorlatban.original%20(1).pdf) (Letöltve: 2025.02.17.)
- [34] Incidens-menedzsment gyakorlat. ÁROP – 2.2.21 Tudásalapú közszolgáltatási előmenetel. Nemzeti Közszerológiai Egyetem, 2019, 24–31. [https://nkepro.uni-nke.hu/xmlui/bitstream/handle/123456789/12921/Incidens-menedzsment%20gyakorlat\\_2019.pdf?sessionid=7AEFA90780807C0CDE8BAC5C89F14401?sequence=1](https://nkepro.uni-nke.hu/xmlui/bitstream/handle/123456789/12921/Incidens-menedzsment%20gyakorlat_2019.pdf?sessionid=7AEFA90780807C0CDE8BAC5C89F14401?sequence=1) (Letöltve: 2025.01.30.)
- [35] EU 01/2021 Irányelvet. Az adatvédelmi incidensek bejelentésével kapcsolatos példákrol elfogadás időpontja: 2021. dec. 14. Változat 2.0. [https://www.edpb.europa.eu/system/files/2022-09/edpb\\_guidelines\\_012021\\_pdbnotification\\_adopted\\_hu.pdf](https://www.edpb.europa.eu/system/files/2022-09/edpb_guidelines_012021_pdbnotification_adopted_hu.pdf) (Letöltve: 2025.01.27.)
- [36] 7/2024. (VI. 24.) MK rendelet a biztonsági osztályba sorolás követelményeiről, valamint az egyes biztonsági osztályok esetében alkalmazandó konkrét védelmi intézkedésekről. MK Rendelet 2024. <https://net.jogtar.hu/jogszabaly?docid=a2400007.mkf> (Letöltve: 2025.01.30.)
- [37] Elektronikus Információs rendszerek és Szervezetek kibertérrel kapcsolatos követelménykatalógusának alkalmazási útmutatója. Verzió 1.0. Nemzeti Kibervédelmi Intézet, 2024, 24–26. <https://nki.gov.hu/wp-content/uploads/2024/10/Biztonsagi-esemenyek-kezelese-ver-1.0.pdf> (Letöltve: 2025.01.23.)
- [38] Agresti, E. et al.: Global Cyber Security Centre: Advanced Persistent Threat. Buyer's Guide. [https://www.gsa.gov/system/files/APT\\_Buyers\\_Guide\\_v2\\_July\\_2022.pdf](https://www.gsa.gov/system/files/APT_Buyers_Guide_v2_July_2022.pdf) (Letöltve: 2025.01.11.)
- [39] Regeski, B.: Four Chinese APT Groups Target Critical Infrastructure Disruption 2024.12.16. <https://thisac.org/threat-intelligence/four-chinese-apt-groups-target-critical-infrastructure-disruption/> (Letöltve: 2025.01.27.)
- [40] Murtaza, A.: Critical Analysis on Advanced Persistent Threats 05/2016 DOI:10.5120/ijca2016090784. [https://www.researchgate.net/publication/303325167\\_Critical\\_Analysis\\_on\\_Advanced\\_Persistent\\_Threats](https://www.researchgate.net/publication/303325167_Critical_Analysis_on_Advanced_Persistent_Threats) (Letöltve: 2025.01.30.)
- [41] Horváth K. – KIFÜ: Közérthetően az IT biztonságról. Információ és IT-biztonság fejlesztése a közigazgatásban. Budapest 2013, 29–31. [https://kifu.gov.hu/wp-content/uploads/2022/03/IT\\_brosura\\_v7.pdf](https://kifu.gov.hu/wp-content/uploads/2022/03/IT_brosura_v7.pdf) (Letöltve: 2025.02.13.)
- [42] Muha L.: Az informatikai biztonság egy lehetséges rendszertana. Szekcióülés II – Információbiztonság, 2008, 141–147. <https://real.mtak.hu/11147/1/1228872.pdf> (Letöltve: 2025.01.25.)
- [43] Gyarak R.: A biztonság tudatosság szerepe, avagy kérdések a kibertérrel kapcsolatban. 2022. nov. DOI:10.32577/mr.2022.2.16 [https://www.researchgate.net/publication/365328721\\_A\\_biztonsagtudatosság\\_szerpe\\_avagy\\_kerdések\\_a\\_kibertérrel\\_kapcsolatban](https://www.researchgate.net/publication/365328721_A_biztonsagtudatosság_szerpe_avagy_kerdések_a_kibertérrel_kapcsolatban) (Letöltve: 2025.04.30.)
- [44] Medhat, S.: Innovation and digital technologies underpinning NATO's warfare development agenda. Science in Parliament 2023/3. <https://www.scienceinparliament.org.uk/wp-content/uploads/2024/05/Innovation-and-Digital-Technologies-Underpinning-NATOs-Warfare-Development-Agenda.pdf> (Letöltve: 2025.01.30.)
- [45] NATO's strategy for digital transformation. 2024.10.22. <https://www.ingocd.org/strategy-for-digital-transformation/> (Letöltve: 2025.01.31.)
- [46] Soare, S.: Digitalisation of Defence in NATO and the EU: Making European Defence Fit for the Digital Age Research paper. 2023.08.10. <https://www.iiss.org/research-paper/2023/08/digitalisation-of-defence-in-nato-and-the-eu/> (Letöltve: 2025.02.14.)
- [47] Digital transformation 2024. <https://www.act.nato.int/activities/digital-transformation/> (Letöltve: 2025.01.31.)
- [48] NCIA delivers AI Masterclass to NATO Senior Leadership, 2025.01.21. <https://www.ncia.nato.int/newsroom/news/ncia-delivers-ai-masterclass-to-nato-senior-leadership> (Letöltve: 2025.03.15.)