Molnár Anna✧

# Az Európai Unió mesterséges intelligenciával kapcsolatos diplomáciai tevékenysége*

DOI 10.17047/HADTUD.2024.34.2.35

Jelen kutatás azt vizsgálja, hogy az Európai Unió (EU) kiberdiplomáciai tevékenységei hogyan terjednek át fokozatosan a digitális diplomáciára és így a mesterséges intelligenciával (MI) kapcsolatos diplomáciai területekre. A kutatás fókuszában a mesterséges intelligenciáról szóló uniós rendelet bemutatása áll. Mivel e területen a globális gazdasági szereplők és a nagyhatalmak közötti feszültségek egyre gyakoribbak, így nagyobb szükség van a mesterséges intelligenciával kapcsolatos nemzetközi tárgyalások folytatására és a megállapodások megkötésére is.

Jelenleg az EU aktív szerepet kíván betölteni nem csupán a kiberbiztonságot, hanem a digitális diplomáciát és a mesterséges intelligenciát érintő nemzetközi tárgyalások területén is. Napjainkban a mesterséges intelligenciával kapcsolatos diplomácia részben a kiberdiplomáciától függetlenül, részben azzal párhuzamosan fejlődik.

KULCSSZAVAK: Európai Unió, mesterséges intelligencia, kiberdiplomácia, szabályozás, digitalizáció

## *European Union Diplomacy on Artificial Intelligence*

*This paper examines the process through which the existing EU-level cyber-diplomacy gradually is branching out to artificial intelligence (AI)-diplomacy. This research focuses on the presentation of the new AI regulation of the EU. Through an analysis of this process it is also reasoned that more attention needs to be paid to cyber- and AI-diplomacy if the discourse on the EU digital sovereignty is to be analysed. As tensions among the public stakeholders and superpowers are increasingly frequent, the need for continuing international talks and for making agreements is growing.*

*Currently, the EU has taken an active role to have an impact on global governance concerning not only cyber security, but also the issue of artificial intelligence. Meanwhile,*

✧ Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar – *National University of Public Service, Faculty of Military Science and Officer Training;* e-mail: molnar.anna@uni-nke.hu; https://orcid.org/0000-0002-7958-6985

* A TKP2021-NVA-16 számú projekt a Kulturális és Innovációs Minisztérium Nemzeti Kutatási Fejlesztési és Innovációs Alapból nyújtott támogatásával, a TKP2021-NVA pályázati program finanszírozásában valósult meg. A tanulmány eredeti változata a RII Forum 2024 konferenciakötet számára készült angol nyelven.

*artificial intelligence diplomacy is evolving, partly independently of, and partly in parallel with cyber diplomacy. At the EU-level, the issue of strategic autonomy and European sovereignty gained momentum following the worsening security environment in the European neighbourhood. Nowadays, these concepts are often used as synonyms, or with broader meaning, as referring not only to defence, but also to economic developments, energy security, digitalisation and technological advancement. Digital sovereignty cannot be established without capacity to act on, and regulate areas related to artificial intelligence.*

KEYWORDS: *cyber-diplomacy, artificial intelligence, AI regulation by the EU*

### *Bevezetés*

Napjainkban a mesterséges intelligencia (MI) területén a technológiai fölény kérdése a geopolitikai hatalmi verseny fontos elemévé vált. Bár továbbra is az USA és Kína a digitális technológiák fejlesztésének a legfontosabb globális szereplői, az MI-hatalom fontosságáról szóló nemzetközi politikai narratíva számos nagyhatalom, így például Oroszország esetében is megjelent.[1] Az Európai Unió (EU) – elsősorban gazdasági és normatív szerepéből következően – a mesterséges intelligenciával kapcsolatban kevésbé geopolitikai, inkább a szabályozást és a fogyasztóvédelmet előtérbe állító álláspontot képvisel. Napjainkban az EU átfogó megközelítése az érték- és az érdekalapú megközelítés között próbál egyensúlyt teremteni e területen is. Bár az európai digitális szuverenitásról uniós szinten is széleskörű diskurzus bontakozott ki,[2] a feltörekvő technológiákba történő jelentős pénzügyi befektetések és fejlesztések nélkül az EU szabályozási erőfeszítései könnyen kudarcot vallhatnak.[3]

A mesterséges intelligenciához kapcsolódó tevékenységek szorosan kapcsolódnak az Unió digitális és kiberbiztonsági politikájához mind az intézményfejlesztés, mind pedig a szabályozási területeken. Noha az EU digitális biztonsággal kapcsolatos első kezdeményezései az 1990-es évek végén kezdődtek, a kiberbiztonság átfogó jogi, politikai és intézményi kerete csak a közelmúltban alakult ki. A kibertérrel kapcsolatos fenyegetésekre és kockázatokra a nagyszabású kibertámadások növekvő száma hívta fel a figyelmet Európa-szerte, különösen a 2007-es észt magán- és közszférát ért DDoS-támadásokat (*distributed denial of service*) követően.[4]

Mivel a kibertámadások a nemzeti határokon is könnyen áthatolnak, alapvető fontosságúvá vált az EU átfogó kiberbiztonsági szabályozásrendszerének és ökoszisztémájának létrehozása.[5] Mindezzel összefüggésben uniós szinten számos, a kiberbiztonságra vonatkozó jogi szabályozást és stratégiát fogadtak el. Érdemes például megemlíteni az EU két kiberbiztonsági stratégiáját (2013 és 2022), a globális hatással is bíró általános adatvédelmi rendeletet (GDPR, 2016) vagy a 2022-ben elfogadott, digitális szolgáltatások egységes piacáról szóló rendeletet (Európai Parlament és a Tanács [EU] 2022/2065 rendelete).[6]

1 Kollár 2020/a és 2020/b; Franke 2021, 6; Calderaro, Blumfelde 2022; Wang et al. 2024

2 Franke 2021; Perucica, Andjelkovic 2022; Leite 2021.

3 Calderaro, Blumfelde 2022; Pavlidis 2024.

4 Kasper, Osula, Molnár 2021.

5 Carrapico, Barrinha 2018; Csernatoni 2024, 299.

6 Christou 2018; Franke 2021, 6; Kasper, Osula, Molnár 2021.

Jelen kutatás azt vizsgálja, hogy az Európai Unió kiberdiplomáciai tevékenységei hogyan terjednek át fokozatosan a digitális diplomáciára és így a mesterséges intelligenciával (MI) kapcsolatos diplomáciai területekre. A kutatás fókuszában a mesterséges intelligenciáról szóló uniós rendelet bemutatása áll.

Az európai kiberdiplomácia a kibertérrel és a kiberbiztonsággal kapcsolatos diplomáciai erőfeszítésekként értelmezhető. A kapcsolódó érdekeket és célokat az EU vagy a tagállamok kiberbiztonsági stratégiái határozzák meg. Mivel a mesterséges intelligencia alkalmazásával kapcsolatos kockázatok egyre nőnek, és a nemzetközi rendszer szereplői, azaz az államok, a nemzetközi szervezetek és a csúcstechnológiai globális vállalatok közötti feszültségek is egyre gyakoribbak, így szükségessé vált a kibertér biztonságát célzó nemzetközi tárgyalások folytatása, valamint a digitalizáció és a mesterséges intelligencia biztonságos használatáról szóló megállapodások megkötése. Miközben az EU aktív szerepet kíván betölteni nem csupán a kiberbiztonságot, hanem a mesterséges intelligenciát érintő nemzetközi tárgyalások területén is, a digitális diplomácia és a mesterséges intelligenciával kapcsolatos diplomácia a kiberdiplomáciával párhuzamosan fejlődik.

Noha az EU, mint „sui generis" multilaterális szereplő, egyre aktívabb nemzetközi tevékenységet folytat a digitális diplomáciai szektorban is, továbbra is kérdéses, hogy az ún. „brüsszeli hatás" (*Brussels effect*) a globális MI-kormányzás esetében, a normatív hatalom modelljének megfelelően, hatékony lehet-e vagy sem.[7] A „brüsszeli hatás" fogalma kiemeli, hogy az EU mint befolyásos nemzetközi szereplő, a szabályozás és a puha hatalmi eszközök révén modellértékű lehet a külső szereplők számára. E koncepció szerint a „brüsszeli hatás" az európaizálódás külső dimenziójaként is felfogható. Mindez azt is jelenti, hogy az EU az adatvédelemtől a fogyasztóvédelemig, a környezetvédelemtől a trösztellenes szabályozáson át az online gyűlöletbeszéd korlátozásáig számos szakpolitikai területre hatást tudott gyakorolni a saját területén kívül is, mivel a multinacionális vállalatok nem csupán az EU-n belül, hanem a globális tevékenységük során is átvették az uniós normákat.[8]

Uniós szinten a stratégiai autonómiával és az európai szuverenitással kapcsolatos diskurzus a romló biztonsági környezet következtében egyre hangsúlyosabbá vált. E fogalmakat eredetileg a biztonsági és védelmi kérdésekkel kapcsolatban említették. A Krím-félsziget orosz annektálása (2014) és az ukrajnai átfogó orosz katonai támadás (2022) következtében kialakult háború jelentősen felgyorsította ezeket a folyamatokat. 2016-ban a Brexitről szóló népszavazás is lendületet adott az uniós szinten integráltabb védelempolitika kialakításának és a stratégiai autonómia megerősítésének.[9] Az európai stratégiai autonómiát az önálló cselekvési képességként, valamint az európai szuverenitás előzményeként magyarázzák. Manapság ezeket a fogalmakat gyakran szinonimaként vagy tágabb értelemben használják, és nemcsak a védelemre, hanem a gazdasági fejlődésre, az energiabiztonságra, a digitalizációra és a technológiai fejlődésre is utalnak.[10]

7 Manners 2002.

8 Bradford 2019.

9 Béraud-Sudreau and Pannier 2021.

10 Molnár, Jakusné Harnos 2023.

A technológiai függetlenség megszerzését célzó digitális (vagy technológiai) szuverenitás koncepciója az EU kulcsfontosságú célkitűzése lett. Ebben a tekintetben a biztonság kérdése szorosan kapcsolódik a szuverenitáshoz. Az EU digitális függősége a külföldi vállalatoktól még mindig meghatározó.[11] A digitális szuverenitás nem teremthető meg anélkül, hogy az EU ne lenne képes önállóan cselekedni és fejleszteni ezeket az innovatív technológiákat, valamint szabályozni a digitális ágazathoz kapcsolódó területeket (például a mesterséges intelligencia területén is). Ez a fajta szuverenitás nemcsak a szabályozás, hanem a digitális környezet ellenőrzésének képességét is jelenti. 2020-ban az Európai Parlament közzétett egy dokumentumot a digitális szuverenitásról. E dokumentum definíciója szerint a digitális szuverenitás „Európa azon képességét jelenti, hogy önállóan cselekedjen a digitális világban".[12] Az EU kibervédelemre vonatkozó politikája (2022) szerint a digitális szuverenitás megvalósítása érdekében az Uniónak és tagállamainak önállóan kell fejleszteniük a kettős felhasználású potenciállal is rendelkező csúcstechnológiákat. E területeken a mesterséges intelligencia rendszerek kulcsszerepet játszanak.[13]

Napjainkban a digitális területen jelentős beruházási szakadék tátong az EU és a vezető technológiai hatalmak, például az USA és Kína között. Mivel az európai gazdaságot a Covid-19 járvány, az ukrajnai háború és az ezzel kapcsolatos energiaválság is súlyosan érintette, gyors és hatékony beavatkozás vált szükségessé. Közhelynek számít, hogy a digitális beruházások kulcsfontosságúak a gazdasági növekedés szempontjából, és a mesterséges intelligencia rendszerek a termelékenységre gyakorolt pozitív hatásuk következtében forradalmi szerepet játszanak a digitalizációban. Az eddigi beruházások és fejlesztések ellenére amerikai cégek még mindig 6%-kal nagyobb mértékben használják a mesterséges intelligenciát mint uniós versenytársaik. Az európai kitettséget jelentősen növeli, hogy az uniós vállalatok főként külföldi cégek által fejlesztett mesterséges intelligencia-rendszerekre támaszkodnak. Az Európai Beruházási Bank elemzése és adatai azt mutatják, hogy az EU a legmodernebb digitális technológiák fejlesztésében és előállításában továbbra is elmarad az USA-tól és Kínától.[14]

### *Kiberdiplomácia és digitális diplomácia*

A nagyszabású kibertámadások következtében az EU hatáskörébe tartozó valamennyi kulcsfontosságú szakpolitikai területen kiberbiztonsági döntéshozatali folyamtok és intézményrendszer (ökoszisztéma) alakult ki. E folyamatoknak köszönhetően – a szubszidiaritás elvével összhangban – a kiberbiztonság többszintű kormányzási (MLG) rendszere fejlődött.[15] A kiberdiplomácia az EU külpolitikai eszköztárának is kulcsfontosságú elemévé vált.[16] Mind a kiberdiplomácia, mind pedig

11 Digital Dependence Index: Measurement of Digital Dependence. 2024.

12 European Parliament 2020, 1.

13 European Commission 2022, 1 és 5.

14 European Investment Bank 2024.

15 Carrapico, Barrinha 2018, 1–2; European Court of Auditors 2019, 12.

16 Kasper, Osula, Molnár 2021; Molnár, Mártonffy 2022.

a digitális diplomácia a nemzetközi szereplők közötti koordinációra és együttműködésre összpontosít. A nemzetközi tárgyalások a gazdaság és a társadalom digitalizációjának, az új technológiáknak, valamint a technológiai fejlődéssel kapcsolatos egyéb fenyegetéseknek és következményeknek a nemzetközi összefüggéseit érintik.[17]

Annak ellenére, hogy az információs és kommunikációs technológiai (ITC) eszközök egyre gyakoribb alkalmazása a hagyományos diplomácia minden szintjén megfigyelhető, a kiberdiplomácia és az e-diplomácia (elektronikus vagy diplomácia 2.0) két különböző fogalom. Az e-diplomácia a digitális technológiák diplomaták általi használatára utal,[18] és általában aktív internetes jelenlétet és a stratégiai kommunikáció előmozdítását jelenti a közösségi médiaplatformokon.[19] Az MI-eszközök (például az MI-alapú adatelemzés) integrálása a döntéshozatali folyamatokba jelentősen támogathatja a diplomáciát is. Ebben a tekintetben a mesterséges intelligencia eszközei tovább növelhetik e digitális eszközök hatékonyságát, ugyanakkor veszélyt is jelentenek a nemzetközi kapcsolatokra és a diplomáciára általában.[20]

A kiberdiplomácia fogalma a diplomáciai eszközök átfogó használatára és diplomáciai célok végrehajtására utal, a kiberbiztonsági stratégiákban meghatározott nemzeti vagy uniós érdekek és célok támogatása érdekében. Ezek a tevékenységek a nemzetközi kiberbiztonsági kérdésekre terjednek ki, beleértve a mesterséges intelligenciával kapcsolatos témákat is.[21] A kiberdiplomácia fő célkitűzései a bizalomépítést, a kapacitásépítést, a kiberhadviselés, a kiberterrorizmus és a kiberbűnözés elleni küzdelmet, az adatvédelmet, az internet szabadságát, valamint a globális kormányzás előmozdítását tartalmazzák a nemzetközi jog és az emberi jogok érvényesítése érdekében.[22]

Bár az európai uniós kiberdiplomácia a közös kül- és biztonságpolitikán belül és annak kulcsfontosságú elemeként, a közös biztonság- és védelempolitikával (KBVP) összefüggésben fejlődött, a kiberbiztonsággal kapcsolatos nemzetközi tárgyalások az egységes belső piac és a bel- és igazságüggyel kapcsolatos területeket is érintik. Az egységes belső piac digitalizációjával kapcsolatos nemzetközi tárgyalások a digitális diplomácia területére vezetnek át. Az utóbbi évtizedben az Európai Külügyi Szolgálat (EKSZ) és az Európai Bizottság a kiberdiplomácia és a digitális stratégiai kommunikáció kulcsfontosságú szereplőivé váltak. Az uniós tagállamok 2015-ben úgy döntöttek, hogy megerősítik az EKSZ-en belül a kiberdiplomáciai képességeket.[23] 2019-ben az EU kidolgozta a kiberdiplomáciai eszköztárat, amely átfogó diplomáciai választ jelentett a kibertér stabilitásának előmozdítása érdekében. Ugyanebben az évben az Európai Tanács úgy döntött, hogy a korlátozó intézkedések (szankciók) alkalmazását a rosszindulatú kibertevékenységekkel szemben is kiterjeszti.[24] Mivel a fejlett mesterséges intelligencia termékek gyakran kettős felhasználású

17 Cirnu, Georgescu 2023, 127.

18 Barrinha, Renard 2017.

19 Ostwald, Dierkes 2018, 203–206; Kasper, Osula, Molnár 2021; Molnár, Mártonffy 2022.

20 Duberry, 2023.

21 Barrinha, Renard 2017, 355–356.

22 Renard, 2018; Kasper, Osula, Molnár 2021; Molnár, Mártonffy 2022.

23 Council of the European Union 2017a; Bendiek, 2018, 1-2; European Court of Auditors 2019, 50.

24 Council Decision (CFSP) 2019/797; Council Regulation (EU) 2019/796; European Commission 2019, 8.

technológiák is lehetnek, azok a rosszindulatú kibertevékenységeket és a támadó kiberműveleteket is támogathatják; így a kiberdiplomáciai eszköztár a mesterséges intelligenciával kapcsolatos kibertechnológiák felhasználására is alkalmazható. Ezek a technológiák támogathatják a stratégiai hírszerzési és döntéshozatali folyamatokat a kritikus területeken, így egy rosszindulatú vagy támadó kibertevékenység hatékonyabbá tehető a fejlett MI technológiák felhasználásával.[25]

2022 júniusában a Tanács elfogadta az uniós digitális diplomáciáról szóló következtetéseit. A dokumentum hangsúlyozza, hogy a digitális diplomácia célja az EU digitális ügyekben betöltött globális szerepének erősítése, különösen stratégiai jelentőségű és sérülékeny országokban. Kiemelten fontos a jogállamiság, az emberi jogok és a demokratikus elvek védelme a digitális térben. Az EU támogatja a digitális technológiák emberközpontú és emberi jogokon alapuló megközelítésének érvényesítését a multilaterális fórumokon, illetve a szabad, biztonságos és stabil internetet, valamint az etikus technológiai szabványok kialakítását. Törekszik az ENSZ fenntartható fejlődési céljainak érvényesítésére, és a digitális infrastruktúra fejlesztésére a Global Gateway stratégia mentén. Az uniós digitális diplomácia az innovációbarát és emberközpontú technológiairányítást részesíti előnyben. Az EU szorgalmazza a digitális szabályozás fejlesztését, valamint az adatbiztonságot és a magánélet védelmét. Az uniós digitális diplomácia támogatja a klímasemleges gazdaságot elősegítő digitális megoldásokat. A közös biztonság- és védelempolitika részeként ösztönzi a kiberbiztonság és a hibrid fenyegetések elleni védelmet, és előmozdítja a globális szabályozási tevékenységeket a digitális technológiák terén.[26] A digitális diplomáciai célokkal összhangban, 2022 szeptemberében az EU irodát nyitott San Francisco-ban az EU és az Egyesült Államok közötti digitális diplomácia terén folytatott együttműködés megerősítésére. A kaliforniai Szilícium-völgyben létrehozott iroda lehetőséget biztosított a technológiai vállalatokkal és döntéshozókkal közvetlen kapcsolatok kiépítésére a hatékony és harmonizált szabályozási környezet kialakítása érdekében.[27]

### *Az EU mesterséges intelligencia szabályozása*

Az Európai Bizottság 2021-ben terjesztette elő az új szabályozási keretre vonatkozó javaslatát, a mesterséges intelligenciáról szóló jogszabálytervezetet *(AI Act).* Hosszas viták után az EP 2024 márciusában fogadta el a rendelet végleges változatát, az EU Tanácsa pedig májusban hagyta azt jóvá. Nem véletlen, hogy Thierry Breton, a belső piacért felelős biztos kijelentette, hogy „Európa globális szabályalkotó lett a mesterséges intelligencia területén".[28] Az EU „sui generis" nemzetközi szereplő ezáltal is támogatja a megbízható mesterséges intelligenciára vonatkozó globális szabályozási normák terjedését.

Az uniós MI-rendeletben szereplő definíció összhangban áll az OECD által kidolgozott definícióval. E meghatározás szerint „az MI gépi alapú rendszer, amelyet

25 Kasper, Osula, Molnár 2021; Molnár, Mártonffy 2022; Ntalampiras, Misuraca, Rossel 2022, 5; Visvizi et al. 2024.

26 Európai Unió Tanácsa 2022.

27 European External Action Service 2022.

28 Breton 2024.

különböző autonómiaszinteken történő működésre terveztek, és amely a bevezetését követően alkalmazkodóképességet tanúsíthat, és amely a kapott bemenetből – explicit vagy implicit célok érdekében – kikövetkezteti, miként generáljon olyan kimeneteket, mint például előrejelzéseket, tartalmakat, ajánlásokat vagy döntéseket, amelyek befolyásolhatják a fizikai vagy a virtuális környezetet".[29] Egyszerűbben fogalmazva az MI „az adatok, az algoritmusok és a gépi tanulás, valamint a számítástechnikai teljesítmény kombinációja", ahogyan azt Thierry Breton 2020-ban megfogalmazta.[30]

Az emberközpontú és kockázatalapú megközelítést alkalmazva, a rendelet célja, hogy szabályozási keretet biztosítson a megbízható mesterséges intelligencia alapú technológiák fejlesztéséhez, valamint az európai értékek, etikai és emberi jogok védelméhez, ugyanakkor ne akadályozza a technológiai fejlődést. Az új szabályozás összhangban áll az Európai Bizottság által felkért független, magas szintű MI-szakértői csoport által kidolgozott és javasolt etikai iránymutatásokkal. A szakértői csoport hét, nem kötelező erejű etikai elvet határozott meg a mesterséges intelligencia használatára vonatkozóan: 1) az emberi cselekvőképesség és felügyelet; 2) a műszaki stabilitás és biztonság; 3) a magánélet védelme és adatkormányzás; 4) az átláthatóság; 5) a sokszínűség, a megkülönböztetés tilalma és méltányosság; 6) a társadalmi és környezeti jóllét; valamint 7) az elszámoltathatóság.[31]

A kockázatalapú megközelítéssel összhangban a mesterségesintelligencia-rendszerek három kategóriába sorolhatók az általuk létrejövő kockázat mértéke szerint: alacsony, nagy és elfogadhatatlan kockázatúak. A minimális kockázatú mesterségesintelligencia-rendszerek nagyon enyhe átláthatósági ajánlásokat igényelnek. A nagy kockázatú mesterségesintelligencia-rendszerek használata fokozott átláthatóságot kíván. Az elfogadhatatlan kockázatú mesterségesintelligencia-rendszerek (például a kognitív magatartási manipuláció és a társadalmi pontozás) használatát az új rendelet tiltja. Az uniós és nemzeti joggal összhangban álló jogszerű értékelési gyakorlat azonban megengedett. A rendelet megemlíti az egyes mesterségesintelligencia-modellek rendszerszintű kockázatát is.[32] A szöveg nagy része a nagy kockázatú mesterségesintelligencia-rendszerek szabályozásával foglalkozik. „Az átláthatóság azt jelenti, hogy az MI-rendszereket olyan módon kell fejleszteni és használni, amely lehetővé teszi a megfelelő nyomon követhetőséget és megmagyarázhatóságot, miközben tudatosítja az emberekben, hogy MI-rendszerrel kommunikálnak vagy lépnek kapcsolatba, valamint megfelelően tájékoztatja az alkalmazókat az MI-rendszer képességeiről és korlátairól, az érintett személyeket pedig jogaikról."[33]

Fontos hangsúlyozni, hogy az új rendelet komoly korlátokat tartalmaz a kettős felhasználású mesterségesintelligencia-rendszerek gyakorlata tekintetében is. A végleges szöveg hangsúlyozza, hogy hatálya nem terjed ki azokra a területekre, amelyek a tagállamok kizárólagos hatáskörei közé tartoznak, mint például a nemzetbiztonság, a katonai vagy a védelemi területek. Az új rendelet nem vonatkozik azokra

29 Az Európai Unió Hivatalos Lapja 2024, 46.
30 Breton 2020.
31 Az Európai Unió Hivatalos Lapja 2024, 8.
32 Az Európai Unió Hivatalos Lapja 2024, 9.
33 Az Európai Unió Hivatalos Lapja 2024, 8.

a mesterségesintelligencia-modellekre, amelyeket kizárólag katonai vagy védelmi célokra fejlesztettek ki és használnak.[34] Ez teljes mértékben összhangban áll a Lisszaboni Szerződéssel, mivel az EUSZ 24. cikkének (1) bekezdése szerint a KKBP és a KBVP területén a jogalkotási aktusok elfogadása kizárt. Bár az új MI-rendelet szövege nem említi kifejezetten az MI-rendszerek kettős felhasználását, a 124. cikk foglalkozik ezzel a területtel. Az eredetileg katonai, védelmi vagy nemzetbiztonsági célokra kifejlesztett, de később polgári célokra használt mesterségesintelligencia-rendszerek esetében az új rendeletet alkalmazni szükséges.

Az MI-rendszerek kettős felhasználásával kapcsolatban a rendelet a következőket határozza meg: „Ha és amennyiben az MI-rendszereket katonai, védelmi vagy nemzetbiztonsági célokra hozzák forgalomba, helyezik üzembe vagy használják módosítással vagy anélkül, azokat ki kell zárni e rendelet hatálya alól, függetlenül attól, hogy az említett tevékenységeket milyen típusú szervezet végzi, így például attól, hogy közjogi vagy magánjogi szervezetről van-e szó. Ami a katonai és védelmi célokat illeti, az ilyen kizárást mind az EUSZ 4. cikkének (2) bekezdése, mind az EUSZ V. címe 2. fejezetének hatálya alá tartozó tagállami és közös uniós védelmi politikának a nemzetközi közjog hatálya alá tartozó sajátosságai indokolják; ez utóbbi tehát a megfelelőbb jogi keret az MI-rendszereknek a halálos erő alkalmazásával összefüggésben, valamint más MI-rendszereknek a katonai és védelmi tevékenységekkel összefüggésben történő szabályozásához. Ami a nemzetbiztonsági célokat illeti, a kizárást indokolja mind az a tény, hogy a nemzetbiztonság az EUSZ 4. cikke (2) bekezdésének megfelelően továbbra is a tagállamok kizárólagos felelőssége, mind a nemzetbiztonsági tevékenységek sajátos jellege és operatív szükségletei, valamint az e tevékenységekre alkalmazandó különös nemzeti szabályok. Mindazonáltal, ha egy katonai, védelmi vagy nemzetbiztonsági célokra kifejlesztett, forgalomba hozott, üzembe helyezett vagy használt MI-rendszert ideiglenesen vagy tartósan más – például polgári vagy humanitárius, bűnüldözési vagy közbiztonsági – célokra használnak, az ilyen rendszer e rendelet hatálya alá tartozik. Ebben az esetben az MI-rendszert nem katonai, védelmi vagy nemzetbiztonsági célokra használó szervezetnek biztosítania kell az MI-rendszer e rendeletnek való megfelelését, kivéve, ha a rendszer már megfelel e rendeletnek. A kizárt – nevezetesen katonai, védelmi vagy nemzetbiztonsági – célból és egy vagy több nem kizárt – például polgári vagy bűnüldözési – célból forgalomba hozott vagy üzembe helyezett MI-rendszerek e rendelet hatálya alá tartoznak, és e rendszerek szolgáltatóinak biztosítaniuk kell az e rendeletnek való megfelelést. Ezekben az esetekben az a tény, hogy egy MI-rendszer e rendelet hatálya alá tartozhat, nem érintheti azt a lehetőséget, hogy a nemzetbiztonsági, védelmi és katonai tevékenységeket végző szervezetek – az e tevékenységeket végző szervezet típusától függetlenül – olyan MI-rendszereket használjanak nemzetbiztonsági, katonai és védelmi célokra, amelyek használata nem tartozik e rendelet hatálya alá. Azon polgári vagy bűnüldözési célból forgalomba hozott MI-rendszerek, amelyeket módosítással vagy módosítás nélkül katonai, védelmi vagy nemzetbiztonsági célokra használnak, nem

34 European Parliament, 2024.

tartozhatnak e rendelet hatálya alá, függetlenül az említett tevékenységeket végző szervezet típusától."[35]

A mesterséges intelligenciáról szóló rendelet végrehajtásának támogatása érdekében 2024 januárjában az Európai Bizottságon belül létrehozták az Európai Mesterséges Intelligenciával Foglalkozó Hivatalt (*European Artificial Intelligence Office*). Az új hivatal fő feladata a megbízható mesterséges intelligencia fejlesztésének és használatának támogatása, valamint a nemzetközi együttműködés erősítése.[36]

### *Mesterségesintelligencia-diplomácia*

Míg a kiberdiplomácia a nemzetközi kapcsolatokban egyfajta eszközként és mechanizmusként szolgál a kiberbiztonsági fenyegetések nemzetközi szintű elhárítására, addig a mesterségesintelligencia-diplomácia azokra a nemzetközi tárgyalásokra és diplomáciai erőfeszítésekre utal, amelyek célja, hogy nemzetközi megállapodások szülessenek a megbízható, biztonságos, etikus és emberközpontú, az emberi jogokat és a nemzetközi jogot tiszteletben tartó mesterséges intelligencia használatára vonatkozó normákról és szabályokról. Mivel a mesterséges intelligencia által vezérelt kibertámadások a kiberfenyegetések új típusát jelentik, így akár a mesterséges intelligenciával kapcsolatos diplomácia a kiberdiplomácia szerves részének is tekinthető. A valóságban azonban ez nem így van, mivel a mesterségesintelligencia-diplomácia koncepciója önállóan, a kiberdiplomáciával és a digitális diplomáciával párhuzamosan fejlődik, a mesterséges intelligencia biztonságos használatát hangsúlyozva.[37]

Miközben az EU a mesterséges intelligenciáról szóló jogszabály kidolgozásán dolgozott, más nemzetközi szereplők, például az Egyesült Királyság és az Egyesült Államok, elsősorban nemzetközi szintű tárgyalásokat és megállapodásokat szorgalmaztak. Az EU céljai előmozdítása érdekében részt vett ezeken a tárgyalásokon. A katonai területen a felelősségteljes mesterséges intelligencia használatáról (REAIM 2023) szóló első csúcstalálkozót Hollandia és Dél-Korea szervezte Hágában, 2023 februárjában. A csúcstalálkozó fórumot biztosított a különböző érdekelt felek számára a katonai felhasználású mesterséges intelligenciával kapcsolatos témák megvitatására.[38] A REAIM 2023 csúcstalálkozó során az USA támogatta a „Mesterséges intelligencia és a gépi autonómia felelős katonai alkalmazásáról" szóló politikai nyilatkozatot. E nyilatkozat (jogilag nem kötelező érvényű iránymutatás) fő célja, hogy konszenzust alakítson ki a mesterséges intelligencia katonai felhasználásával kapcsolatos felelős állami magatartásról. Az USA rendszeres párbeszédet kívánt előmozdítani a nyilatkozat végrehajtásáról.[39]

2023 novemberében az Egyesült Királyságban, a Bletchly Parkban rendezték meg az első mesterséges intelligenciával kapcsolatos biztonságpolitikai csúcstalálkozót. A helyszín a második világháború idején a brit kódfejtők központja volt.

35 Az Európai Unió Hivatalos Lapja 2024, 45.

36 Béraud-Sudreau, Pannier 2021.

37 Marwala 2023; Visvizi, et al. 2024; Radanliev 2024.

38 Government of the Netherlands 2023.

39 U.S. Department of Defense: 2023.

A csúcstalálkozó végén 28 ország és az EU aláírta a bletchly-i nyilatkozatot. A találkozón nemcsak az EU képviselői, hanem néhány tagállam, például Németország, Franciaország, Olaszország, Spanyolország, Hollandia és Írország is részt vettek.[40] Az Európai Bizottság elnöke, Ursula von der Leyen a csúcstalálkozón javasolta, hogy a mesterséges intelligencia használatára vonatkozó nemzetközi irányítási rendszer 4 pillérre támaszkodjon. E pillérek tartalmazzák 1) egy független tudományos közösség létrehozását, amely képes a mesterséges intelligencia rendszerek értékelésére; 2) nemzetközileg elfogadott eljárások kidolgozását a mesterséges intelligencia biztonságának tesztelésére; 3) eljárások kidolgozását a mesterséges intelligencia által okozott incidensek jelentésére és nyomon követésére; 4) és egy nemzetközi riasztórendszer létrehozását. Ezek az elvek az Európai Bizottságon belül a mesterséges intelligenciával foglalkozó hivatal létrehozásának is alapelvei.[41]

Az ENSZ Közgyűlése 2024 márciusában elfogadta az első határozatot a mesterséges intelligenciáról. A nem kötelező érvényű határozat fő célja volt, hogy „megragadják a biztonságos és megbízható mesterségesintelligencia-rendszerek lehetőségeit a fenntartható fejlődés érdekében", és biztosítsák, hogy a mesterségesintelligencia-rendszerek (a nem katonai területen) teljes életciklusuk során „emberközpontúak, megbízhatóak, magyarázhatóak, etikusak, befogadóak legyenek, teljes mértékben tiszteletben tartsák, előmozdítsák és védjék az emberi jogokat és a nemzetközi jogot, megőrizzék a magánéletet, fenntartható fejlődésre orientáltak és felelősek legyenek (...). Kiegyensúlyozott és integrált módon; elősegítsék a digitális átalakulást; előmozdítsák a békét; leküzdjék az országok közötti és az országokon belüli digitális szakadékot; és előmozdítsák és védjék az emberi jogok és alapvető szabadságok élvezetét mindenki számára, miközben az embert tartsák a középpontban." Az állásfoglalást az Egyesült Államok javasolta, és Kína, valamint több mint 120 másik tagállam támogatta. A kormányokat arra kérték, hogy az állásfoglalással összhangban vezessék be saját, a mesterséges intelligenciára vonatkozó szabályozásaikat.[42] 2024 áprilisában az Egyesült Királyság és az Egyesült Államok egyetértési nyilatkozatot írt alá a közös munkáról és a fejlett mesterséges intelligencia tesztjeinek kidolgozásáról.[43]

2024 márciusában az Európai Parlament jóváhagyta az átfogó MI-rendeletet, amely a világon az első jogilag kötelező érvényű MI-technológiát érintő jogszabály. Az uniós jogszabály jelentősége abban rejlik, hogy az EU különleges szereplője a nemzetközi kapcsolatoknak, mivel szuverén államokból áll, de a tagállamok szuverenitásuk egy részét megosztják egymással. Különleges jellemzői alapján az EU a nemzetközi kapcsolatokban különálló entitásnak is tekinthető. Ezért ez az új szabályozási keret az államközi kapcsolatokra is alkalmazható, és az úgynevezett brüsszeli hatás kézzelfogható eredménye lehet. Mivel az MI-rendelet az Európai Gazdasági Térségről szóló megállapodás hatálya alá tartozik, így az EU-n kívül, az EGT országokban is alkalmazandó, ezért hatása már hatálybalépésekor is szélesebb, mint a saját tagállamai. Emellett fontos megjegyezni, hogy a csatlakozni vágyó országok

40 Gov.uk 2023.

41 European Commission 2023.

42 United Nations 2024.

43 U.S. Department of Commerce 2024.

egyik feltétele az uniós joganyag nemzeti jogba történő harmonizációja, így a MI-rendelet átvétele és alkalmazása.

Napjainkban az EU mesterségesintelligencia-politikája főként olyan belső politikai területekre terjed ki, mint a belső piac, a digitális egységes piac vagy a bel- és igazságügy, de olyan kevésbé integrált területekre is vonatkozik, mint a tudománypolitika, az oktatás vagy az egészségügy. Az uniós intézmények a külkapcsolatokban a mesterséges intelligencia diplomáciai kérdését külön képviselik, mint a megbízható mesterséges intelligenciára vonatkozó európai megközelítés nemzetközi fórumokon való előmozdításának eszközét.[44] Mivel az egyes MI-termékek polgári és katonai célokra egyaránt használható kettős felhasználású technológiának tekinthetők,[45] az MI-politika egyre inkább kapcsolódik az EU kialakulóban lévő védelmi politikájához és védelmi iparpolitikájához.

Számos külpolitikai dokumentum és stratégia – például a kiberbiztonsági stratégia (2013, 2020), a kiberdiplomáciáról szóló tanácsi következtetések (2015), az európai mesterségesintelligencia-stratégia (2018) és a digitális diplomáciával kapcsolatos tanácsi következtetések (2022, 2023) – írja le az EU nemzetközi szerepét a kibertérben. Általánosságban ezek a dokumentumok kiemelik a szabad és nyitott internet védelmének fontosságát, a nemzetközi jog, a felelős állami magatartás koncepciójának és a kibertérben hozott bizalomépítő intézkedések előmozdítását. E stratégiák az EU nemzetközi kapcsolatainak erősítését javasolják.[46] Nem véletlen, hogy az első európai MI-stratégia hangsúlyozza, hogy az EU-nak globális szinten az MI etikus felhasználásáról szóló vita élére kell állnia. Az MI-stratégia egyensúlyt kíván teremteni az innováció előmozdítása és az EU alapvető értékeinek és normáinak tiszteletben tartása között.[47]

Almada és Radu (2023) tanulmányukban azzal érvel, hogy a mesterséges intelligenciáról szóló rendelet valószínűleg ki fogja váltani a brüsszeli hatást, és ennek következtében más szereplők is követni fogják az EU elveit. Ez azonban mellékhatásokkal fog megvalósulni, hiszen az MI-rendelet az EU termékbiztonsági jogszabályainak része, és így az emberi jogi kérdésekkel gyengébb a kapcsolata. Az EU nemzetközi hatásának megerősítése érdekében támogatja azokat a nemzetközi erőfeszítéseket, például az Európa Tanács keretében folyó tárgyalásokat a mesterséges intelligenciáról szóló egyezményről szóló megállapodás érdekében, amelyek hozzájárulnak a mesterséges intelligenciáról szóló jogszabály elveinek nemzetközi szintű alkalmazásához.[48]

### *Összegzés*

Az átfogó MI-rendelet jelentős előrelépést jelent a mesterséges intelligencia biztonságos használatát segítő uniós intézmény- és szabályozási rendszer létrehozása terén. Bár célja az európai értékek és a technológiai innováció előmozdítása, a rendelet etikai

44 European External Action Service 2023.

45 Ambrus 2020.

46 Rehrl 2018 25; Council of the European Union 2018, 8; European Parliament 2020.

47 European Commission 2018.

48 Almada, Radu 2024.

normáinak hatékony végrehajtása és az új mesterséges intelligenciával kapcsolatos kockázatértékelési folyamat megfelelő alkalmazása továbbra is kérdéseket vethet fel.

Az EU emberközpontú megközelítésével a technológiai fejlődés akadályozása nélkül kívánja előmozdítani a megbízható mesterséges intelligencia fejlesztését. Az új rendelet az átláthatóságra, az elszámoltathatóságra és az emberi felügyeletre helyezi a hangsúlyt. A mesterségesintelligencia-rendszerek széles körű alkalmazása azonban még mindig kritikákat és aggodalmakat vált ki az adatvédelemmel és a kettős felhasználású termékekkel kapcsolatban. A technológiai szuverenitás koncepciójának megvalósításához ez a rendelet önmagában nem elegendő: egyrészt kulcsfontosságú a végrehajtása, másrészt az EU-nak több pénzügyi forrást kell biztosítani a feltörekvő technológiák fejlesztésére.[49]

A mesterségesintelligencia-diplomácia koncepciójával összefüggésben az új szabályozás a brüsszeli hatás potenciális megvalósulásának ígéretét hordozza magában, mivel az EU kézzelfogható hatást gyakorolhat a globális mesterségesintelligencia-kormányzásra. Kiemelve e feltörekvő technológiák potenciálisan rosszindulatú jellegét, a mesterséges intelligencia egyszerre tekinthető „áldásnak és átoknak".[50] A globális MI-kormányzási hatás eléréséhez az EU-nak stratégiai partnerségeket kell kialakítania más globális hatalmakkal, nemzetközi szervezetekkel és a technológiai vállalatokkal is.

Noha az átfogó jogszabályi keret szabályozási szempontból a digitális szuverenitás megvalósítását segíti, azonban az EU meghatározó MI-iparág nélkül nem rendelkezhet olyan eszközökkel, amelyekkel valós globális MI-hatalommá válhatna. Ugyanakkor az új uniós szabályozás lehetőséget teremtett arra, hogy az EU aktív szereplője lehessen a mesterséges intelligencia globális irányításáról szóló további nemzetközi tárgyalásoknak.

FELHASZNÁLT IRODALOM

Almada, Marco, Radu, Anca 2024.The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. *German Law Journal,* 25 (4): 646–663. https://doi.org/10.1017/glj.2023.108

Ambrus Éva 2020. Artificial Intelligence as a Dual-use Technology. *AARMS,* 19 (2): 19–28. https://doi.org/10.32565/aarms.2020.2.2

Barrinha, André, Renard, Thomas 2017. Cyber-diplomacy: the making of an international society in the digital age. *Journal of Global Affairs,* 3 (4–5): 353–364. https://doi.org/10.1080/23340460.2017.1414924

Bendiek, Annegret 2018. The EU as a Force for Peace in International Cyber Diplomacy. *SWP Comment,* no. 19, April 2018. 1–8. https://www.swp-berlin.org/fileadmin/contents/products/comments/2018C19_bdk.pdf

Béraud-Sudreau, Lucie and Pannier, Alice 2021. An 'improbable Paris-Berlin-Commission triangle': usages of Europe and the revival of EU defense cooperation after 2016. *Journal of European Integration,* 43 (3): 295–310. https://doi.org/10.1080/07036337.2020.1740215

49 Pavlidis 2024.

50 von Essen, Ossewaarde 2023.

Bradford, Anu 2020. *The Brussels effect: How the European Union rules the world.* New York: Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Breton, Thierry 2020. Europe has everything it takes to lead the technology race. https://www.linkedin.com/pulse/europe-has-everything-takes-lead-technology-race-thierry-breton/

Breton, Thierry 2024. Thierry Breton's Post. https://www.linkedin.com/posts/thierrybreton_aiact-activity-7173645503455252480-xO81?utm_source=share&utm_medium=member_desktop

Calderaro, Andrea, Blumfelde, Stella 2022. Artificial intelligence and EU security: the false promise of digital sovereignty. *European Security,* 31 (3): 415–434. https://doi.org/10.1080/09662839.2022.2101885

Carrapico, Helena, Barrinha, Andre 2018. European Union cyber security as an emerging research and policy field. *European Politics and Society,* 19 (3): 299–303. https://doi.org/10.1080/23745118.2018.1430712

Christou, G.eorge 2019. The collective securitisation of cyberspace in the European Union. *West European Politics,* 42 (2): 278–301. https://doi.org/10.1080/01402382.2018.1510195

Cirnu, Carmen Elena, Georgescu, Alexandru 2023. Complex System Governance Theory and Conceptual Links to Cyber Diplomacy. *Studies in Informatics and Control,* 32 (2): 127–136. https://sic.ici.ro/wp-content/uploads/2023/06/Art.-12-Issue-2-2023.pdf https://doi.org/10.24846/v32i2y202312

Council Decision (CFSP) 2019/797, of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States, https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019D0797&from=EN

Council of the European Union: Council Conclusions on a Framework for a Joint EU Diplomatic Response to Malicious Cyber Activities („Cyber Diplomacy Toolbox") 9916/17. (2017a) http://data.consilium.europa.eu/doc/document/ST-9916-2017-INIT/en/pdf

Council of the European Union: EU Cyber Defence Policy Framework, (as updated in 2018), Brussels, 19 November 2018 (OR. en) 14413/18, http://data.consilium.europa.eu/doc/document/ST-14413-2018-INIT/en/pdf

Az Európai Unió Hivatalos Lapja 2024. Az Európai Parlament és a Tanács (EU) 2024/1689 Rendelet (2024. június 13.) a mesterséges intelligenciára vonatkozó harmonizált szabályok megállapításáról, valamint a 300/2008/EK, a 167/2013/EU, a 168/2013/EU, az (EU) 2018/858, az (EU) 2018/1139 és az (EU) 2019/2144 rendelet, továbbá a 2014/90/EU, az (EU) 2016/797 és az (EU) 2020/1828 irányelv módosításáról (a mesterséges intelligenciáról szóló rendelet)

Council Regulation (EU) 2019/796 of 17 May 2019, concerning restrictive measures against cyber-attacks threatening the Union or its Member States. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0796&from=EN

Csernatoni, Raluca 2024. *Charting the Geopolitics and European Governance of Artificial Intelligence.* Washington D.C.: Carnegie Endowment for International Peace. https://carnegieeurope.eu/2024/03/06/charting-geopolitics-and-european-governance-of-artificial-intelligence-pub-91876

Digital Dependence Index: Measurement of Digital Dependence. 2024, https://digitaldependence.eu/en/

Duberry, Jérőme 2023. AI Diplomacy: what vision for the future of multilateralism? https://genevasolutions.news/science-tech/ai-diplomacy-what-vision-for-the-future-of-multilateralism-1

European Commission: Artificial Intelligence for Europe, Com(2018) 237 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2018:237:FIN

European Commission: EU Policy on Cyber Defence, Brussels, 10.11.2022, JOIN(2022) 49 final. https://www.eeas.europa.eu/sites/default/files/documents/Comm_cyber%20defence.pdf

European Commission: Remarks of President von der Leyen at the Bletchley Park AI Safety Summit, 2 November 2023. https://ec.europa.eu/commission/presscorner/detail/en/speech_23_5502

European Commission: Report on the implementation of the Action Plan Against Disinformation, Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions, Brussels, 14.6.2019 JOIN (2019) 12 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019JC0012&from=EN

European Court of Auditors: Challenges to effective EU cybersecurity policy, Briefing Paper, March 2019. https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_EN.pdf

European External Action Service 2022. US/Digital: EU opens new Office in San Francisco to reinforce its Digital Diplomacy. https://www.eeas.europa.eu/eeas/usdigital-eu-opens-new-office-san-francisco-reinforce-its-digital-diplomacy_en

European External Action Service 2023. Commission welcomes political agreement on Artificial Intelligence Act, https://www.eeas.europa.eu/delegations/ukraine/commission-welcomes-political-agreement-artificial-intelligence-act_en

European Investment Bank: Investment Repot 2023/2024. Transforming for competitiveness. 2024, https://www.eib.org/attachments/lucalli/20230323_economic_investment_report_2023_2024_en.pdf

European Parliament: Artificial intelligence act. In "A Europe Fit for the Digital Age". 2024. https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-regulation-on-artificial-intelligence

European Parliament: Digital Sovereignty for Europe. 2020. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Európai Unió Tanácsa: A Tanács következtetései az uniós digitális diplomáciáról, Brüsszel, 2022. július 18. https://data.consilium.europa.eu/doc/document/ST-11406-2022-INIT/hu/pdf

Franke, Ulrike 2021. *Artificial Intelligence diplomacy. Artificial Intelligence governance as a new European Union external policy tool.* Policy Department for Economic, Scientific and Quality of Life Policies Directorate-General for Internal Policies. https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662926/IPOL_STU(2021)662926_EN.pdf

Gov.uk: The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

Government of the Netherlands: REAIM 2023. https://www.government.nl/ministries/ministry-of-foreign-affairs/activiteiten/reaim

Kasper, Ágnes, Osula, Anna-Maria, Molnár, Anna 2021. EU cybersecurity and cyber diplomacy. *IDP Revista de Internet Derecho y Política,* 34, 1-15 (2021)

Kollár Csaba 2020/a. Kína és a társadalmi kredit rendszere. *Hadtudomány,* 30 (2): 79–97. https://doi.org/10.17047/HADTUD.2020.30.2.79

Kollár Csaba 2020/b. Kína és a társadalmi kredit rendszerének információbiztonsági kérdései. *Biztonságtudományi Szemle,* 2 (2): 93–109.

Leite, Isabel Costa 2021. EU institutions and ICT: a new challenge in transparency and dialogue with citizens. *Transforming Government: People, Process and Policy,* 15 (3): 309–318. https://doi.org/10.1108/TG-10-2020-0301

Manners, Ian 2002. Normative Power Europe: A Contradiction in Terms? *Journal of Common Market Studies,* 40 (2): 235–258 https://doi.org/10.1111/1468-5965.00353

Marwala, Tshilidzi 2023. *Artificial Intelligence in Politics. In: Artificial Intelligence, Game Theory and Mechanism Design in Politics.* Singapore: Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-99-5103-1_4

Molnár, Anna, Mártonffy, Balázs (eds.) 2022. *Cyber diplomacy from the European perspective.* 1st edn. Budapest: Ludovika University Press.

Molnár, Anna, Jakusné Harnos, Éva 2023. The Postmodernity of the European Union: A Discourse Analysis of State of the Union Addresses. *The International Spectator,* 58 (1): 58–74. https://doi.org/0.1080/03932729.2022.2149177

Ntalampiras, Stavros, Misuraca, Gianluca, Rossel, Pierre 2022. Artificial Intelligence and Cybersecurity Research. *ENISA, Research and Innovation Brief,* June 2023. https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research

Ostwald, Kai, Dierkes, Julian Beatus 2018. Canada's foreign policy and bureaucratic (un)responsiveness: public diplomacy in the digital domain. *Canadian Foreign Policy Journal*, 24 (2): 202–222. https://doi.org/10.1080/11926422.2018.1461664

Pavlidis, George 2024. Unlocking the black box: analysing the EU artificial intelligence act's framework for explainability in AI. *Law, Innovation and Technology,* 16 (1): 1–16. https://doi.org/10.1080/17579961.2024.2313795

Perucica, Natasa and Andjelkovic, Katarina 2022. Is the future of AI sustainable? A case study of the European Union, Transforming Government: *People, Process and Policy,* 16 (3): 347–358. https://doi.org/10.1108/TG-06-2021-0106

Radanliev, Petar 2024. Cyber diplomacy: defining the opportunities for cybersecurity and risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing. *Journal of Cyber Security Technology,* 2024: 1–51. https://doi.org/10.1080/23742917.2024.2312671

Rehrl, Jochen (ed.) 2018. *Handbook on cyber security. The Common Security and Defence Policy of the European Union.* 1st edn. Vienna: Directorate for Security Policy of the Federal Ministry of Defence of the Republic of Austria. https://publications.europa.eu/en/publication-detail/-/publication/63138617-f133-11e8-9982-01aa75ed71a1

Renard, Thomas: EU cyber partnerships: Assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society,* 19 (3): 321–337. https://doi.org/10.1080/23745118.2018.1430720

U.S. Department of Commerce: U.S. and UK Announce Partnership on Science of AI Safety, April 1, 2024, https://www.commerce.gov/news/press-releases/2024/04/us-and-uk-announce-partnership-science-ai-safety

U.S. Department of Defense: U.S. Endorses Responsible AI Measures for Global Militaries, 2023. https://www.defense.gov/News/News-Stories/Article/Article/3597093/us-endorses-responsible-ai-measures-for-global-militaries/

United Nations: General Assembly adopts landmark resolution on artificial intelligence, 21 March 2024. https://news.un.org/en/story/2024/03/1147831

Visvizi, Anna, Malik, Rados³aw, Guazzo, Gianluca Maria and Çekani, Vilma 2024. The Industry 5.0 (I50) paradigm, blockchain-based applications and the smart city. *European Journal of Innovation Management,* Vol. ahead-of-print No. ahead-of-print. 10 April 2024. https://doi.org/10.1108/EJIM-09-2023-0826

von Essen, Louisa, Ossewaarde, Marinus 2023. Artificial intelligence and European identity: the European Commission's struggle for reconciliation. *European Politics and Society,* 25 (2): 375–402. https://doi.org/10.1080/23745118.2023.2244385

Wang, Jun, Visvizi, Anna, Fang Nan, Fanchao, Meng 2024. Placing China's Green Technology Innovation in a Context. 475–484. In Visvizi, Anna, Troisi, Orlando, Corvello, Vincenzo (eds): *Research and Innovation Forum 2023.* RIIFORUM 2023. Springer Proceedings in Complexity. Springer, Cham. https://doi.org/10.1007/978-3-031-44721-1_36