Az Európai Unió
Tanácsa

Brüsszel, 2026. július 9.
(OR. en)

11711/26

CYBER 337
JAI 979
TELECOM 383
CSC 483
DATAPROTECT 234
RELEX 990
COSI 111
COPS 434

FEDŐLAP

Küldi:	az Európai Bizottság főtitkára részéről Martine DEPREZ igazgató
Az átvétel dátuma:	2026. július 8.
Címzett:	Thérèse BLANCHET, az Európai Unió Tanácsának főtitkára
Biz. dok. sz.:	COM(2026) 577 final
Tárgy:	A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK Cselekvési terv a kiberbiztonságról és a mesterséges intelligenciáról

Mellékelten továbbítjuk a delegációknak a következő dokumentumot: COM(2026) 577 final.

Melléklet: COM(2026) 577 final

EURÓPAI
BIZOTTSÁG

Strasbourg, 2026.7.7.
COM(2026) 577 final

A BIZOTTSÁG KÖZLEMÉNYE AZ EURÓPAI PARLAMENTNEK, A TANÁCSNAK, AZ EURÓPAI GAZDASÁGI ÉS SZOCIÁLIS BIZOTTSÁGNAK ÉS A RÉGIÓK BIZOTTSÁGÁNAK

Cselekvési terv a kiberbiztonságról és a mesterséges intelligenciáról

1. Bevezetés

Az élvonalbeli mesterséges intelligencia a kiberbiztonság változását jelzi. Az élvonalbeli MI-modellek (azaz a jelenleg rendelkezésre álló vagy fejlesztés alatt álló legfejlettebb MI-modellek) jobb képességeket biztosítanak a felkészültség megerősítéséhez, valamint a fenyegetések észlelésének és az azokra való reagálásnak a javításához, így **példátlan lehetőségeket teremtenek a kiberreziliencia megerősítésére**. Ahogy ezek a képességek tovább fejlődnek[1], a mesterséges intelligencia segítségével a kiberbiztonsági csoportok is gyorsabban és nagyobb léptékben tudnak majd működni, így a szervezetek hatékonyabban tudják majd kezelni a felmerülő fenyegetéseket. Ugyanakkor **a fejlett MI-képességek, amelyek jelenleg** – többek között nyílt forráskódon keresztül – **rendelkezésre állnak, már most is felhasználhatók az EU kiberrezilienciájának megerősítésére**.[2]

Mára **a fenyegetettségi helyzet meghatározó elemévé** vált a mesterséges intelligencia, amely automatizáltabb, skálázhatóbb és kifinomultabb offenzív kiberműveleteket tesz lehetővé, amelybe beletartoznak a kiberbűnözési tevékenységek is.[3] Míg élvonalbeli szintű képességekről jelenleg csak néhány MI-modell és -rendszer esetében beszélhetünk (azaz olyan modellek és rendszerek esetében, amelyek sokféle feladatot képesek ellátni, és amelyek megközelítik, elérik vagy meg is haladják a technika jelenlegi állását)[4], ez a képességbeli eltérés csökken, ahogy a nyílt forráskódú modellek egyre jobbak lesznek. Ennek eredményeként a tényleges élvonalbeli képességek idővel várhatóan egyre hozzáférhetőbbé válnak, többek között a rosszindulatú szereplők, például a kiberbűnözők számára is, akik ezeket a képességeket összetettebb támadások végrehajtására használhatják fel.

Az EU felkészülten lép be ebbe az új paradigmába. Az elmúlt években megvetette az alapokat: a kiberbiztonság kezelésének jogi és operatív alapjait a mesterséges intelligencia korában. A **mesterséges intelligenciáról szóló rendelet** (a továbbiakban: MI-rendelet) a világ első jogilag kötelező erejű kerete az MI-rendszerekből és -modellekből eredő kockázatok kezelésére, beleértve a legfejlettebb általános célú MI-modellekből eredő rendszerszintű kockázatokat, például a rendellenes kiberbiztonsági használat kockázatát is.[5] A **kiberrezilienciáról szóló, 2027 végéig teljeskörűen alkalmazandó rendelet** az ellátási láncok biztonságával foglalkozik; ennek érdekében beépített biztonságot és sérülékenységmenedzsmentet ír elő az uniós piacon forgalmazott szoftver- és hardvertermékek teljes életciklusa során.[6] Az MI-rendelet és a kiberrezilienciáról szóló rendelet együttesen segít biztosítani, hogy az MI-modelleket, valamint a digitális elemeket tartalmazó rendszereket és termékeket a biztonságot szem előtt tartva fejlesszék ki és tartsák fenn. Ezzel párhuzamosan a

[1] Az Egyesült Királyság MI-biztonsági intézetének (AI Security Institute) közelmúltbeli kutatásai arra engednek következtetni, hogy ellenőrzött kiberbiztonsági tesztek során a legfejlettebb MI-modellek már emberi segítség nélkül is képesek egyre hosszabb feladatokat elvégezni. A feladatok becsült hossza, amelyeket képesek ellátni, évek helyett hónapok alatt megkétszereződött, a közelmúlt eredményei pedig arra utalnak, hogy ez az ütem még gyorsulhat.

[2] „AI is changing the economics of vulnerability discovery. Defenders should adapt now" [„A mesterséges intelligencia megváltoztatja a sérülékenységek feltárásának ökonómiáját. A védelmezőknek most kell alkalmazkodniuk"], CERT-EU, 2026. április.

[3] ENISA, *Az ENISA fenyegetettségi helyzetjelentése, 2025.*, 2025. október.

[4] A felhőszolgáltatások és a mesterséges intelligencia fejlesztéséről szóló javasolt rendelet 2. cikkének (4) bekezdésében meghatározottak szerint, COM(2026) 502 final.

[5] (EU) 2024/1689 rendelet.

[6] (EU) 2024/2847 rendelet.

NIS 2 irányelv[7] a **pénzügyi ágazat digitális működési rezilienciájáról szóló rendelettel**[8] együtt kockázatalapú keretet biztosít a kritikus ágazatok kiberbiztonságához. Ezek a jogszabályok szilárd keretet biztosítanak, amely – hatékony végrehajtásuk esetén – helyt tud állni a technológia és a fenyegetések fejlődésével szemben. A **kiberszolidaritásról szóló jogszabály** ezt a keretet olyan operatív mechanizmusokkal egészíti ki, amelyek támogatják a tagállamokat a jelentős és nagyszabású eseményekre való felkészültségben, azok észlelésében és az azokra való reagálásban[9]. Ezek az intézkedések együttesen hozzájárulnak a **felkészültségi unióról szóló stratégia**[10] és az **európai belső biztonsági stratégia**[11] célkitűzéseihez.

A mesterséges intelligencián alapuló fejlett kiberképességek szintén kulcsfontosságú eszközök Uniónk biztonságának garantálásában. Bár ezek a különböző, köztük nyílt forráskódú modellek révén rendelkezésre álló képességek már most is képesek megerősíteni az EU kiberrezilienciáját, az élvonalbeli képességek fejlesztése főként az EU-n kívül zajlik, és rendelkezésre állásukat gyakran nem átlátható, külföldi irányítású folyamatok határozzák meg. E képességek ismerete és az azokhoz való hozzáférés ezért nemcsak digitális reziliencia, hanem Európa technológiai szuverenitásának kérdése is. E szuverenitás megőrzése érdekében az EU-nak biztosítania kell, hogy a mesterséges intelligencián alapuló fejlett kiberbiztonsági képességek elterjedése ne hozzon létre új stratégiai függőségeket. Európának ugyanakkor fel is kell gyorsítania rezilienciáját annak érdekében, hogy lépést tartson ezzel a gyorsan változó fenyegetettségi helyzettel.

Az EU már tett **stratégiai lépéseket a kritikus technológiáktól való függőség csökkentése és a saját fejlesztésű képességek növelése érdekében**. A Horizont Európa és a Digitális Európa programon keresztül az EU már elkezdte finanszírozni a mesterséges intelligencián alapuló fejlett kiberképességek fejlesztését, az Európai Innovációs Tanács Alapja pedig fontos befektetővé vált a mélytechnológiában Európában, többek között a kiberbiztonsággal és az MI-technológiával foglalkozó induló és növekvő innovatív vállalkozásokba történő beruházások révén[12]. Emellett **a felhőszolgáltatások és a mesterséges intelligencia fejlesztéséről szóló, nemrégiben javasolt rendelet**[13] bővítené az uniós adatközpontok kapacitását, valamint a felhőszolgáltatások és a mesterséges intelligencia autonómiáját, ezzel támogatva a mesterséges intelligencia szélesebb körű bevezetését, beleértve a kibertérhez kapcsolódó eszközöket és alkalmazásokat is. Lehetővé tenné az EU számára, hogy kritikus felhő- és MI-kapacitásokra támaszkodjon, így csökkenteni lehetne a geopolitikai és biztonsági kockázatokkal szembeni függőségeket. A javaslat **a mesterséges intelligencia alkalmazásának ösztönzésére irányuló stratégiára** és az **„MI-kontinens” cselekvési tervre** épül, és felismeri különösen azt, hogy nagy kihívásokat kell indítani az élvonalbeli mesterséges intelligencia támogatása és kapacitásbővítése érdekében.

---

[7] Az (EU) 2022/2555 irányelv, amely 11 kiemelten kritikus ágazatot (energia, szállítás, banki szolgáltatások, pénzügyi piaci infrastruktúra, egészségügy, ivóvíz, szennyvíz, digitális infrastruktúra, IKT-szolgáltatások irányítása, közigazgatás és világűr) és hét egyéb kritikus ágazatot (postai és futárszolgáltatások; hulladékgazdálkodás; vegyszerek gyártása, előállítása és forgalmazása; élelmiszer-termelés, -feldolgozás és -forgalmazás; gyártás; digitális szolgáltatók; valamint kutatás) fed le.

[8] (EU) 2022/2554 rendelet.

[9] (EU) 2025/38 rendelet.

[10] JOIN(2025) 130 final.

[11] COM(2025) 148 final.

[12] Sifted, 2026. március 20.: Europe’s most active deep tech investors in 2025 [Európa legaktívabb mélytechnológiai befektetői 2025-ben]; Az EIC 2025. évi hatásvizsgálati jelentése.

[13] COM(2026) 502 final.

Ezekre az erős alapokra építve **az EU-nak most további lépéseket kell tennie azoknak a közvetlen mögöttes problémáknak és lehetőségeknek a kezelése érdekében, amelyeket a mesterséges intelligencia teremtett a kiberbiztonság terén**.

Ez a cselekvési terv **egy kezdeti és célzott válasz a tagállamok és az uniós szervezetek támogatására ezen új helyzet kezelésében**.

Először is, az élvonalbeli mesterséges intelligencia biztonságos és felelősségteljes alkalmazásának biztosítása érdekében az EU fokozni fogja az élvonalbeli mesterséges intelligencia – többek között kiberbiztonsági – értékelésére irányuló kapacitását annak bevezetése előtt. Ez előmozdítja a szigorú külső értékelési folyamatot, valamint a mesterséges intelligencia értékelésének elsőrangú képességét az EU-ban. Az EU emellett meg fogja könnyíteni, hogy az európai szereplők hozzáférjenek a mesterséges intelligencián alapuló fejlett kiberképességekhez, valamint támogatni fogja a rendelkezésre álló MI-modellek kiberbiztonsági felhasználási esetekben történő tesztelésére irányuló erőfeszítéseket.

Másodszor, az EU fel fogja gyorsítani az arra irányuló erőfeszítéseket, hogy támogassa a kritikus ágazatokat és a kkv-kat a mesterséges intelligencián alapuló kiberfenyegetésekre való felkészülésben, többek között kiberbiztonsági alapok bevezetése révén. Ezek használatát az EU a rendelkezésre álló mesterséges intelligencia teljes skálájára építve támogatni fogja a kiberreziliencia megerősítése és a legkritikusabb sérülékenységek orvoslása érdekében.

Harmadszor, az EU növelni fogja a mesterséges intelligencián alapuló megoldások kifejlesztésére és bevezetésére való képességét azáltal, hogy fellendíti a köréjük épülő európai ökoszisztémát, és folytatja saját kapacitásának megerősítését az élvonalbeli fejlesztések terén. Ez utóbbi megvalósításához sürgős, nagyszabású tőkebefektetésekre lesz szükség, hogy ki lehessen építeni Európa saját kapacitásait az élvonalbeli mesterséges intelligencia terén, amivel fellendíthetők az igényeinknek megfelelő európai megoldások.

Végezetül az EU e célkitűzések mentén együtt fog működni hasonlóan gondolkodó partnerekkel annak érdekében, hogy megbízható és biztonságos globális megközelítést mozdítson elő az élvonalbeli mesterséges intelligenciával és a kiberbiztonsággal kapcsolatban.

2. 1. pillér: az élvonalbeli mesterséges intelligencia biztonságossá, hozzáférhetővé és bevethetővé tétele az európai kiberbiztonság érdekében

Mivel a mesterséges intelligencián alapuló fejlett kiberképességeket a közeljövőben akár fegyverként is felhasználhatják kritikus infrastruktúráink és társadalmunk ellen, az EU-nak prioritásként kell kezelnie az e képességekkel kapcsolatos korai tudatosság biztosítását, erősebb technikai kapacitást kell kiépítenie a bennük rejlő kockázatok értékelésére, ki kell alakítania lehetőségeket a kiberbiztonsági célú bevezetésükben rejlő potenciáljuk tesztelésére, valamint egyértelműbb hozzáférési útvonalakat kell meghatároznia a jogszerű kiberbiztonsági célokhoz Európában. E célból, valamint az MI-rendelet által biztosított jogi keretre építve az EU bővíteni fogja a bevezetés előtti értékeléshez szükséges európai kapacitásokat, illetve közös európai megközelítést fog ösztönözni a tesztelési erőfeszítésekhez való hozzáférésre és azok összehangolására vonatkozóan azért, hogy az élvonalbeli mesterséges intelligencia biztonságosan hozzáférhető és használható legyen az európai kiberbiztonság érdekében.

2.1. Az élvonalbeli mesterséges intelligencia által jelentett kockázatok felmérése és enyhítése

Az MI-rendelet követelményeket határoz meg az **MI-rendszerek**[14] kiberbiztonságára vonatkozóan, valamint **előírja a legfejlettebb általános célú MI-modellek szolgáltatói számára, hogy értékeljék és enyhítsék a rendszerszintű kockázatokat**, amelyek többek között a mesterséges intelligencia kibertérben való rendellenes használatából erednek.[15]

2026. augusztus 2-tól a Bizottság elkezdi gyakorolni az MI-rendelet által biztosított felügyeleti és végrehajtási hatásköröket az MI-rendszerek, valamint az általános célú MI-modellek, köztük a kiberbiztonsággal kapcsolatos rendszerszintű kockázatokat jelentő modellek eredményes felügyeletének biztosítása érdekében.[16] Ennek a felügyeletnek részét képezi a modellek képességeivel kapcsolatos kockázatok szolgáltatók általi azonosításának és az e kockázatok enyhítése érdekében általuk végrehajtott intézkedések értékelése. Ezek a követelmények továbbra is arányosak az adott technológia képességeivel.

A felügyeleti és végrehajtási hatásköröket **a Bizottság MI-hivatalának tanácsot adó tudományos testület**, **biztonságos bejelentési csatornák** és **az általános célú mesterséges intelligenciára vonatkozó gyakorlati kódex** fogja támogatni.

2.2. Európai kiválóság kialakítása az élvonalbeli mesterséges intelligencia bevezetés előtti értékelése terén

A kiberbiztonsági célú mesterséges intelligencia biztonságos és felelősségteljes uniós bevezetésének előmozdítása érdekében a szabályozási intézkedéseket **megerősített európai értékelési kapacitásoknak** kell kiegészíteniük. Mivel az MI-képességek fejlődnek, és mivel előfordulhat, hogy rendszerszintű kockázatok nem csak a kiberterületen merülnek fel[17], a külső értékelések elvégzése kezd bevált gyakorlattá válni az élvonalbeli mesterséges intelligencia biztonságának biztosítása érdekében, összhangban a más kockázatos iparágakban kialakított megközelítésekkel. Az MI-rendelet is kiemeli a harmadik félnek minősülő szervezeteken keresztül történő, **a bevezetést megelőző értékelés fontosságát** a rendszerszintű kockázatok értékelése és adott esetben enyhítése érdekében. Eddig az MI-modellek bevezetését megelőző, harmadik fél általi értékelését végző vezető szervezetek többsége az EU-n kívül volt megtalálható. Növekvő jelentőségük miatt kezd sürgőssé válni, hogy ez az értékelési szakértelem és a kapcsolódó infrastruktúra egy része az EU-n belül legyen.

Az EU-nak ezért meg kell erősítenie a rendelkezésre álló szakértelmet annak érdekében, hogy létrejöjjön egy hiteles és versenyképes ökoszisztéma a harmadik félnek minősülő értékelőkből a fejlett MI-képességek értékelése és a kockázatok enyhítése céljából, támogatva a mesterséges intelligenciára vonatkozó uniós irányítási keretbe vetett bizalmat. E célból a Bizottság **kritériumokat fog javasolni a harmadik félnek minősülő értékelők számára az általános célú mesterséges intelligenciára vonatkozó gyakorlati kódex alkalmazásában, és elő fogja**

[14] Az MI-rendelet III. mellékletének részeként a kritikus infrastruktúrákban használt MI-rendszerek nagy kockázatúnak minősülnek, és külön rendelkezések vonatkoznak rájuk, többek között a kiberbiztonságot illetően.

[15] Az MI-rendelet a következő módon fogalmazza meg a „rendszerszintű kockázat” fogalmát: „az általános célú MI-modellek nagy hatású képességeire jellemző kockázat, amely – a modellek jelentős elterjedtsége miatt, vagy a népegészségre, a biztonságra, a közbiztonságra, az alapvető jogokra vagy a társadalom egészére gyakorolt tényleges vagy észszerűen előrelátható negatív hatások révén – olyan jelentős hatást gyakorol az uniós piacra, amely nagy léptékben továbbterjedhet az értéklláncban” (az MI-rendelet 3. cikkének 65. pontja).

[16] A rendszerszintű kockázatot jelentő általános célú MI-modellek azon szolgáltatóira vonatkozó végrehajtási hatáskörök, amelyek nem felelnek meg a rendszerszintű kockázat enyhítésére vonatkozó rendelkezéseknek, magukban foglalják a modellre vonatkozó információk bekérését, a modellhez való hozzáférés kérelmezését értékelések elvégzése céljából, kockázatcsökkentő intézkedések előírását, és végső soron a globális éves árbevétel legfeljebb 3 %-áig terjedő pénzbírság kiszabását, vagy a szolgáltató felkérését a modell forgalmazásának korlátozására, forgalomból való kivonására vagy visszahívására.

[17] Egy másik olyan terület, ahol az általános célú MI-modellek képességei folyamatosan nőnek, és visszaélhetnek velük, ezzel közegészségügyi és közbiztonsági kockázatot okozva, például a biológia.

mozdítani egy szélesebb értékelési ökoszisztéma kialakítását. Ebbe beletartozik majd az értékelők és az érintett szakértők közötti érdemi eszmecserék megkönnyítése az értékelési módszerek javítása és a képesítési követelmények pontosítása érdekében.

Ami **az MI-modellek kifejezetten kiberbiztonsági szempontból történő értékelését illeti**, Európa vezető szerepet játszhatna ezen a területen a magas szintű kiberbiztonsági szakembereivel. Tekintettel a sürgető helyzetre, az EU-nak ki kellene használnia és meg kellene erősítenie ezt a szakértelmet. E célkitűzés elérése érdekében a Bizottság külön felhívást fog közzétenni **az MI-modellek uniós értékelési kapacitásának létrehozására, amelynek a kiberbiztonság a része kell, hogy legyen.** Ez a kapacitás nagymértékben hozzájárulhatna az EU kialakulóban lévő ökoszisztémájához, és épülhetne a tagállamokban kialakulóban lévő MI-értékelési know-how-ra. Támogatni fogja továbbá a Bizottság MI-hivatalon keresztül végzett szabályozási tevékenységeit[18] is azáltal, hogy európai választási lehetőséget biztosít az MI-modellek harmadik fél általi értékelésére és a hozzájuk kapcsolódó kockázatcsökkentő intézkedésekre. Információkkal fog szolgálni a szolgáltatók kockázatkezeléséhez azáltal, hogy független módon értékeli a modellek képességeit és a modellek szolgáltatói által végrehajtott kockázatcsökkentő intézkedések hatékonyságát.[19]

Ez az európai kapacitás támogatni fogja az általános célú MI-modellek szolgáltatóit az MI-rendelet vonatkozó kötelezettségeinek és az általános célú MI-modellek gyakorlati kódexének való megfelelésben.[20] Hiteles és szigorú külső értékelési folyamatot fog biztosítani. Ha elsőrangú értékelési képességek állnak majd rendelkezésre az EU-ban, azok a potenciális rendszerszintű kockázatok megértéséhez is hozzá fognak járulni, többek között a kiberbiztonság, de akár a biotechnológia terén és más területeken is azáltal, hogy korai figyelmeztető jelzéseket adnak a kockázatok azonosításakor.

2.3.A mesterséges intelligencián alapuló fejlett kiberképességekhez való hozzáférés megkönnyítése az EU-ban

A fejlett kiberképességekkel rendelkező élvonalbeli mesterséges intelligenciához való hozzáférést egyre inkább szolgáltatóspecifikus és gyakran nem európai döntések szabályozzák, és egyes szolgáltatók **strukturált hozzáférési programok** (pl. a modellek szakaszos bevezetése) révén korlátozzák a hozzáférést a rendellenes használat kockázatának kezelése érdekében. Bár az ilyen korlátozást indokolhatják biztonsági okok, ez a gyakorlat gyakran nem átlátható az annak meghatározására alkalmazott kritériumok tekintetében, hogy mely szervezetek (köztük vállalatok) és milyen folyamat révén kapnak hozzáférést. Ez akadályozhatja az európai szereplőket, köztük az illetékes hatóságokat és a kritikus infrastruktúrák üzemeltetőit abban, hogy időben kihasználják ezeket az MI-képességeket, és megerősítsék rezilienciájukat.

Sürgősen összehangolt uniós megközelítésre van szükség annak elősegítése érdekében, hogy az érintett **európai köz- és magánszereplők** biztonságosan és indokolatlan késedelem nélkül hozzáférhessenek a szóban forgó élvonalbeli mesterséges intelligenciához. E célból az EU egy

[18] Az általános célú MI-modellekre vonatkozó gyakorlati kódex biztonságra és védelemre vonatkozó fejezete előírja a szolgáltatók számára, hogy megfelelően képzett, független külső értékelőkön keresztül is végezzenek modellértékeléseket (3.5. függelék). Ezek a jelentések ezt követően támogatni fogják az MI-Hivatal szabályozási tevékenységeit, mivel a szolgáltatóknak a külső értékelésekről rendelkezésre álló jelentéseket a jelentésmintával együtt be kell nyújtaniuk az MI-Hivatalnak (7.4. intézkedés).

[19] Az e kapacitás révén végzett értékelések eltérnek majd a 2.4. szakaszban szereplő tesztelési platformon végzett értékelésektől. A platformot elsősorban az MI-modellek kiberbiztonsági alkalmazásainak tesztelésére fogják használni, míg a kapacitás a rendszerszintű kockázat értékelésére és enyhítésére fog összpontosítani a gyakorlati kódexnek való megfelelés támogatása érdekében.

[20] A kapacitás nem megfelelőségértékelő szervezet lesz, és csak az értékelésein keresztül támogatja a megfelelést.

olyan korszerű, kockázatalapú folyamatot fog előmozdítani, amely egyértelmű kritériumokat tartalmaz, és amelyet úgy alakítottak ki, hogy eredményesen csökkentse a rendellenes használat kockázatát.

A Bizottság az Európai Uniós Kiberbiztonsági Ügynökséggel (a továbbiakban: ENISA) együttműködve **a fejlett MI-képességekhez kiberbiztonsági célokból való strukturált hozzáférésre vonatkozóan európai tervet** fog kidolgozni, amely iránymutatásul szolgál majd annak meghatározásához, hogy a fejlett kiberképességekkel rendelkező mesterséges intelligencia szolgáltatói hogyan biztosíthatnak hozzáférést az európai szervezetek, köztük a vállalatok számára, és ezáltal hogyan támogathatják a kiberkockázatok enyhítését.

Ebben az iránymutatásokat tartalmazó dokumentációban szerepelni fognak azok **a kritériumok, amelyeket figyelembe kell venni** ahhoz, hogy az európai szereplőknek hozzáférést nyújtsanak a fejlett kiberképességekkel rendelkező mesterséges intelligenciához. A tervnek ki kell terjednie a különböző típusú szervezetekre (pl. uniós intézmények, tagállami hatóságok, kritikus infrastruktúrák üzemeltetői, kiberbiztonsági szolgáltatók és kutatási szereplők) vonatkozó kritériumokra, és ismertetnie kell e szereplők azonosításának módját. Biztonsági kritériumokat is tartalmaznia kell annak érdekében, hogy a terven keresztül biztosított hozzáférés ne jelentsen indokolatlan kockázatot, valamint kell lennie benne egy **olyan mechanizmusnak is, amely egyszerűsíti a hozzáférés biztosítását** a jogosult szervezetek számára. Ennek a mechanizmusnak elő kell segítenie a szolgáltatók általi korai **tájékoztatást** is a tervezett megbízható hozzáférési programokról, valamint a tudásmegosztást is azon uniós szervezetek között, amelyek hozzáférést kaptak egy adott modellhez vagy rendszerhez.

Bár **új kötelezettségeket nem vezet be a szolgáltatók számára**, a terv támogatni fogja az általános célú mesterséges intelligenciára vonatkozó gyakorlati kódex célkitűzéseit azáltal, hogy meghatározza azokat a lehetséges kockázatcsökkentő intézkedéseket, amelyek kiegészíthetik a rendszerszintű kockázatot jelentő általános célú MI-modellek szolgáltatói által végrehajtandó **rendszerszintű kockázatkezelést**[21].[22] Egy **európai referenciakeret** biztosítása révén a terv a további nemzetközi együttműködés alapjául fog szolgálni.

A tervnek **rendkívüli intézkedéseket is kell tartalmaznia a fejlett kiberképességekkel rendelkező mesterséges intelligenciához való korlátozott vagy visszavont hozzáférés esetére**, hogy meghatározza az uniós szinten végrehajtandó intézkedéseket abban az esetben, ha egy szolgáltató vagy harmadik országbeli hatóság korlátozza vagy visszavonja a releváns modellhez vagy rendszerhez való hozzáférést. Emellett, amennyiben általános felhasználás céljából időben hozzá kell férni az élvonalbeli mesterséges intelligenciához, a Bizottság a tagállamokkal együttműködve meg fogja vizsgálni a rendelkezésre álló finanszírozási eszközök – többek között a közös közbeszerzés – lehetséges felhasználását **az ilyen modellekhez vagy rendszerekhez való közös hozzáférés megszerzése érdekében**.

2.4. A fejlett kiberképességekkel rendelkező mesterséges intelligencia tesztelése a mesterséges intelligencia időben történő és biztonságos kiberbiztonsági bevezetése érdekében

A biztonságos és megbízható élvonalbeli mesterséges intelligenciához való hozzáférést össze kell kapcsolni azzal, hogy képességeit olyan téren is teszteljék, hogy azok alkalmasak-e

[21] Az MI-rendelet 55. cikke (1) bekezdésének b) pontjával összhangban.

[22] Az általános célú mesterséges intelligenciára vonatkozó gyakorlati kódexnek a biztonságról és védelemről szóló fejezete az 5.1. intézkedésben például a biztonság érdekében végzett enyhítő intézkedés példájaként említi a modellhez való hozzáférés szakaszosságának biztosítását.

kiberbiztonsági műveletekben, például a sérülékenységek vizsgálatában, a helyreállításban és a váratlan eseményekre való reagálásban való felhasználásra. Az előnyei kihasználása érdekében a kritikus infrastruktúrák üzemeltetőinek és a hatóságoknak gyorsan meg kell érteniük, hogyan teljesít a fejlett kiberképességekkel rendelkező mesterséges intelligencia realisztikus kiberbiztonsági környezetben, mielőtt érzékeny környezetben bevezetnék. Az ilyen tesztelést **biztonságos és ellenőrzött környezetben** kell végrehajtani.

Annak érdekében, hogy európai szintű szinergiákat teremtsen, az **ENISA** és az **Európai Bizottság Közös Kutatóközpontja** (a továbbiakban: JRC) más érintett bizottsági szolgálatokkal és uniós szervezetekkel, például az uniós intézmények, szervek és hivatalok hálózatbiztonsági vészhelyzeteket elhárító csoportjával (a továbbiakban: CERT-EU), a Bűnüldözési Együttműködés Európai Uniós Ügynökségével (a továbbiakban: Europol) és az ágazati hatóságokkal, valamint a tagállamokkal együttműködve **biztonságos tesztelési platformot fog szervezni a mesterséges intelligencia kiberbiztonsági felhasználási eseteire vonatkozóan[23].** A platform lehetővé teszi majd a résztvevők számára, hogy közös biztonsági és titoktartási szabályok alapján saját modell-hozzáférési kulcsaikat használják, hogy így mind a saját költségeiket fedezzék, a saját eszközeiket használják, és továbbra is felelősséget vállaljanak a tesztelési módszereikért. A tesztelési platformhoz és az összesített eredményekhez való hozzáférést az ENISA-nak kell szabályoznia a JRC-vel együttműködve.

Ez a biztonságos európai tesztelési platform lehetővé fogja tenni azt is, hogy **a mesterséges intelligencia fejlett kiberképességeinek a kritikus infrastruktúrák rendszereibe való bevezetését anélkül teszteljék**, hogy a valós infrastruktúrát kockázatnak tennék ki („**virtuális gyakorlóterek**”[24]). Ez a kezdeményezés **a meglévő virtuális gyakorlóterek kiigazítását és bővítését** fogja előtérbe helyezni a környezetek megkettőzése helyett. Míg például új virtuális gyakorlótereket csak azokban az ágazatokban fejlesztenek majd ki, ahol ilyen képességek jelenleg nem állnak rendelkezésre, az ágazatokon átívelő ipar támogathatná ezt a kezdeményezést azáltal, hogy a meglévő környezeteket célzott vállalások révén integrálja. A közreműködő ágazati szereplők – az alkalmazandó titoktartási szabályokra is figyelemmel – a vonatkozó tesztelési tevékenységekből származó összesített információkat kaphatnának.

E környezet használatának a mesterséges intelligenciának a kiberreziliencia megerősítésére való felhasználása érdekében végzett tesztelése a lényeg, és nem célja az általános célú MI-modellek értékelése az MI-rendeletnek való megfelelés érdekében[25]. Elő fogja mozdítani és fel fogja gyorsítani a mesterséges intelligenciának a kiberrezilienciához való felhasználásával kapcsolatos operatív tapasztalatokat, beleértve az érzékelést, a priorizálást, a fenyegetettséggel kapcsolatos hírszerzést és a reagálást a támadók megelőzése érdekében. Az **ENISA** annak érdekében, hogy Unió-szerte magas szintű kiberbiztonságot nyújtson, a meglévő tudására fog támaszkodni **a rendelkezésre álló MI-modelleknek és -rendszereknek a tágabb**

[23] A JRC által kezelt meglévő platformot korszerűsíteni lehetne az ilyen típusú tesztelés lehetővé tétele érdekében.
[24] A virtuális gyakorlóterek biztonságos és ellenőrzött környezetek, amelyek szimulált formában reprodukálnak digitális rendszereket, hálózatokat vagy infrastruktúrát. Realisztikus körülmények közötti tesztelést tesznek lehetővé, ugyanakkor biztosítják, hogy a környezetben végzett tevékenységek ne érintsenek valós rendszereket vagy szolgáltatásokat.
[25] A mesterséges intelligencia kiberrezilienciai tesztelésének célja annak megértése, hogy egy MI-modell vagy MI-rendszer operatív szempontból alkalmas-e egy konkrét kiberbiztonsági feladat elvégzésére, míg az MI-modelleknek az MI-rendeletnek való megfelelés támogatása céljából történő értékelésének célja, hogy értékelést nyújtson a modellből eredő kockázatokról és a modell szolgáltatója által végrehajtott kockázatcsökkentések hatékonyságáról. A mesterséges intelligencia kiberrezilienciai tesztelése ezért eltér az MI-modelleknek az MI-rendeletnek való megfelelésének támogatása céljából történő értékelésétől, valamint eltérő készségeket és erőforrásokat igényel.

ökoszisztéma számára történő biztonságos használatára vonatkozó iránymutatások és tanácsok közzététele és fenntartása érdekében.

Fő intézkedések:

- **1. fő intézkedés: a Bizottság támogatni fogja az MI-modellek uniós értékelési kapacitásának létrehozását, amelynek magában kell foglalnia a kiberbiztonságot (2027).**
- **2. fő intézkedés: a Bizottság az ENISA-val együttműködve európai tervet fog meghatározni a fejlett MI-képességekhez kiberbiztonsági célokból való strukturált hozzáférésre vonatkozóan annak biztosítása érdekében, hogy az európai szervezetek biztonságosan és időben hozzáférhessenek ezekhez a képességekhez (2026 negyedik negyedéve).**
- **3. fő intézkedés: az ENISA és az Európai Bizottság Közös Kutatóközpontja (JRC) biztonságos tesztelési platformot fog fejleszteni kiberbiztonsági felhasználási esetekhez a fejlett kiberképességekkel rendelkező mesterséges intelligencia számára, hogy fellendítse a mesterséges intelligencia időben történő és biztonságos, kiberbiztonsági célú bevezetését (2026 negyedik negyedéve).**

3. 2. pillér: az EU kiberbiztonsági ökoszisztémájának felkészítése a mesterséges intelligencia korára

Ahogy a fejlett MI-kiberképességek egyre hozzáférhetőbbé válnak és egyre szélesebb körben elterjednek, az EU-nak készen kell állnia arra, hogy kezelje azoknak a gazdaságával és társadalmával szembeni esetleges rendellenes használatát, és biztonságosan használja fel azokat a kiberreziliencia érdekében. A mesterséges intelligencia nagy fokú automatizálással és nagyobb léptékben felgyorsíthatja a sérülékenységek felfedezését, de közben csökkenti is a szakértelmet, az időt és az erőforrásokat, amelyekre a rosszindulatú szereplőknek van szüksége a kifinomult támadások végrehajtásához. Azonnali prioritásként az EU-nak meg kell erősítenie felkészültségét, és támogatnia kell a kritikus ágazatokat az e fenyegetésekhez való alkalmazkodásban. Ebbe beletartozik egyfelől a rendelkezésre álló MI-megoldások kiberbiztonsági műveletekbe való integrálása az MI-modellek teljes skálájára (különös tekintettel a nyílt forráskódú modellekre) támaszkodva, másrészt a legkritikusabb sérülékenységek azonosítására és orvoslására irányuló erőfeszítések felgyorsítása. Az ENISA egyedülálló helyzetben van ahhoz, hogy támogassa az uniós kiberbiztonsági ökoszisztéma átállását a mesterséges intelligencia korára.

3.1. Az EU kiberbiztonsági alapjainak és felkészültségének alkalmazása

Ebben az új technológiai és biztonsági környezetben **a kiberbiztonsági alapok és a felkészültség most minden eddiginél fontosabb**, és a meglévő uniós kiberbiztonsági eszközöket teljes mértékben ki kell használni.

Az EU kiberbiztonsági szabályozási kerete, nevezetesen a **NIS 2 irányelv[26] és a digitális működési rezilienciáról szóló jogszabály** szilárd alapot biztosít a kritikus infrastruktúrák felkészültségéhez a kiberbiztonsági kockázatok valamennyi típusával szemben, beleértve a mesterséges intelligenciával kapcsolatos kockázatokat is. Ezeket a szabályokat ezért a

[26] A NIS 2 irányelv a kiberbiztonsági kockázatkezelés alapjául szolgál: 18 kritikus ágazatban működő, alapvető és fontos szervezet számára írja elő, hogy védjék hálózati és információs rendszereiket, valamint hogy előzzék meg és minimalizálják a váratlan események hatását.

tagállamoknak sürgősen át kell venniük és végre kell hajtaniuk. Emellett a tagállamoknak felügyeleti munkájuk során a fejlett mesterséges intelligenciából eredő kockázatokat is figyelembe kell venniük. Hasonlóképpen, a kritikus ágazatok szereplőinek és a pénzügyi szervezeteknek is felül kell vizsgálniuk és hozzá kell igazítaniuk kockázatkezelési keretrendszerüket az új realitásokhoz, hiszen gyakrabban és nagyobb léptékben számíthatnak a mesterséges intelligencián alapuló kibertámadásokra, valamint a javítási ütem felgyorsításával csökkenteniük kell a javításhoz szükséges időt, és képesnek kell lenniük összetett rendszerek gyors javítására.

A felkészültség további megerősítése érdekében a szervezeteknek következetesen **alapvető kiberhigiéniai intézkedéseket** kell alkalmazniuk, valamint hálózat- és rendszererősítést kell végrehajtaniuk (többek között adott esetben a zéró bizalom elvét alkalmazó megközelítéssel). Meg kell kezdeniük továbbá **a már rendelkezésre álló MI-képességek használatát** is – többek között nyílt forráskódú modelleken keresztül – a sérülékenységek észlelése, valamint a kibertámadások észlelésének és megelőzésének javítása érdekében. Az **uniós szervezetek** – a CERT-EU támogatásával és az Intézményközi Kiberbiztonsági Testület iránymutatásával – e tekintetben jó példával járhatnak elöl az Unió általános kiberbiztonsági helyzetének megerősítése terén, összhangban az uniós szervezetek kiberbiztonságáról szóló rendelettel[27]. A Bizottság arra is határozottan ösztönzi a tagállamokat, hogy teljes mértékben használják ki az **uniós kiberbiztonsági tartalék** átalakítási lehetőségeit a mesterséges intelligencián alapuló kiberfenyegetésekkel szembeni reziliencia növelése érdekében, többek között a sérülékenységi vizsgálatok, az automatizált behatolási tesztelés és a kockázatfigyelés révén, ahonnan a javítási ajánlásokhoz támogatást is kaphatnak.

Emellett – amint azt a **kiberrezilienciáról szóló, 2027. december 11-től teljeskörűen alkalmazandó jogszabály** is tükrözi – továbbra is alapvető fontosságúak a biztonságos beépített fejlesztési gyakorlatok, a szisztematikus sérülékenységmenedzsment, az időben történő javítás és a biztonságos kódolási gyakorlatok, beleértve a sérülékenységek teljes kategóriáinak a kiküszöbölésére irányuló megközelítéseket, például a memóriabiztonságot szem előtt tartó szoftverfejlesztést. A mesterséges intelligenciával kapcsolatos kiberbiztonsági kockázatokat, többek között az adat- és modellmérgezés, az ellenséges támadások és a prompt injekció kockázatát is gondosan értékelni és enyhíteni kell az MI-rendelet vonatkozó rendelkezéseivel összhangban.

Ezen erőfeszítések támogatása érdekében az **ENISA** az európai felügyeleti hatóságokkal és más érintett uniós szervezetekkel együttműködve **megfelelő iránymutatásokat, ajánlásokat, tanácsadókat és bevált gyakorlatokat bocsát majd rendelkezésre és tart fenn annak érdekében, hogy továbbra is védve maradjon a mesterséges intelligencián alapuló fenyegetésekkel[28] szemben, és előmozdítsa az MI-eszközök kiberbiztonsági műveletekbe való biztonságos integrálását.** Ezeknek az iránymutatásoknak és tanácsadóknak figyelembe kell venniük a támadásoknak leginkább kitett kkv-k szükségleteit is. Ezeket az erőfeszítéseket adott esetben akár ágazati kezdeményezésekkel és együttműködési mechanizmusokkal is meg lehetne erősíteni és gazdagítani lehetne olyan területeken, mint például a pénzügy, a közlekedés, az energia, az agrár-élelmiszeripar, az egészségügy[29] és az űrkutatás.

[27] (EU, Euratom) 2023/2841 rendelet.

[28] Ilyen tanácsadásra példa a CERT-EU blogbejegyzése: *AI is changing the economics of vulnerability discovery. Defenders should adapt now* [A mesterséges intelligencia megváltoztatja a sérülékenységek feltárásának ökonómiáját. A védelmezőknek most kell alkalmazkodniuk], 2026. április 21.

[29] A kórházak és az egészségügyi szolgáltatók kiberbiztonságára vonatkozó európai cselekvési terv: COM(2025) 10 final.

Ahogy a technológiák és a kapcsolódó kockázatok tovább fejlődnek majd, **a közös helyzetismeret és a mesterséges intelligencián alapuló kiberbiztonsági fenyegetésekkel kapcsolatos strukturált információmegosztás** a releváns uniós hálózatokon keresztül mind horizontális, mind ágazati szinten fontos szerepet fog játszani a helyzetismeret megerősítésében. Az ENISA-nak meg kell vizsgálnia, hogy miként segítheti elő az MI-szolgáltatókkal való együttműködést a fenyegetettséggel kapcsolatos hírszerzés megosztásának fokozása érdekében.

Hasonlóképpen, a tagállamoknak is ki kell használniuk a kiberbiztonság terén létező uniós szintű struktúrákat **a kritikus infrastruktúrák felkészültségének értékeléséhez** azáltal, hogy együttműködnek különösen a Kiberbiztonsági Együttműködési Csoportban, valamint adott esetben az MI-rendelet alapján létrehozott Mesterséges Intelligenciával Foglalkozó Európai Testülettel.

3.2. A javítási folyamat felgyorsítása: a sérülékenységmenedzsment korszerűsítése a mesterséges intelligenciával kapcsolatos gyors felfedezés érdekében

Az EU kiberbiztonsági helyzete előtt az jelent közvetlen kihívást, hogy **kijavítsák a meglévő sérülékenységeket még azelőtt, hogy azokat széles körben ki lehetne használni**. Mivel a mesterséges intelligencia csökkenti a rosszindulatú szereplők számára a sérülékenységek kihasználásához szükséges időt, az érintett szervezeteknek is fel kell gyorsítaniuk azon képességüket, hogy kellően gyorsan elemezni, rangsorolni és orvosolni tudják a problémákat, illetve be tudják vezetni a javításokat a sérülékenységek kihasználásának megelőzése érdekében.

Korszerűsíteni kell a sérülékenységek meglévő kezelési folyamatait annak érdekében, hogy hatékonyak legyenek a mesterséges intelligenciával támogatott feltárás korában. Az ENISA-nak biztosítania kell, hogy Európa sérülékenységmenedzsmentre szolgáló infrastruktúrája és szolgáltatásai – többek között az Európai Unió biztonságirés-nyilvántartása és a kiberrezilienciáról szóló rendelet egységes jelentéstételi platformja – megfeleljenek a célnak a mesterséges intelligenciával támogatott sérülékenységfeltárás korában, valamint a tagállamokkal együtt meg kell erősítenie az interoperabilitást az uniós, nemzeti és globális sérülékenységplatformok és -adatbázisok között.

Ahogy a sérülékenységi jelentések száma növekszik, a gyártóknak el kell dönteniük, hogy mely hibákat orvosolják először a különböző termékvonalakban, míg a felhasználóknak – különösen az alapvető és kritikus fontosságú szervezeteknek – meg kell határozniuk, hogy mely frissítéseket vezetik be először, gyakran korlátozott erőforrásokkal. El kell érni, hogy a szervezetek a kiberrezilienciáról szóló rendelettel és a NIS 2 irányelvvel összehangolt, egyértelmű, az egész EU-ra kiterjedő, kockázatalapú iránymutatásra támaszkodhassanak annak érdekében, hogy segítségükkel ott lehessen javításokat eszközölni, ahol a legnagyobbak a kockázatok.

A NIS 2 irányelv szerinti kötelezettségeik részeként **a tagállamoknak aktualizálniuk kell a sérülékenységek összehangolt közzétételére vonatkozó nemzeti politikáikat** is a sérülékenységeknek a mesterséges intelligencián alapuló kihasználásának a kezelése érdekében. A Kiberbiztonsági Együttműködési Csoportnak felül kell vizsgálnia a sérülékenységek összehangolt közzétételének a végrehajtására vonatkozó iránymutatását, az EU-nak pedig azt is felül kell vizsgálnia, hogy a sérülékenységek összehangolt közzétételének a keretrendszereit alátámasztó ISO/IEC szabványok továbbra is megfelelnek-e a célnak a jelenlegi fenyegetések fényében. E tekintetben a nemzetközi együttműködés is alapvető fontosságú, mivel ezek a gyakorlatok globálisan alakulnak.

Végezetül a kritikus infrastruktúra biztosítása nem ér véget a sérülékenységek feltárásával vagy a javítások kiadásával. A nagyobb kihívást **ezek alkalmazása** jelenti. Ahogy a mesterséges intelligenciával egyre gyorsabbá válik a sérülékenységek feltárása, a hibajavító csomagok bevezetésének a szűk keresztmetszete is egyre súlyosabbá válik. Az ENISA támogatásával a tagállamoknak ki kell használniuk a meglévő hálózatokat, például a Kiberbiztonsági Együttműködési Csoportot e rendkívül sürgős kihívás kezelése érdekében.

3.3. A gyakorlatba való átültetés: a legfontosabb hibák kijavítása

Az EU-nak nemcsak arra vonatkozóan kell tudást gyűjtenie, hogy a mesterséges intelligencia hogyan erősítheti meg a kiberrezilienciát; ezt **a tudást alkalmaznia is kell ott, ahol a legsürgetőbb szükség van rá**. A kihívást ezért nemcsak a sérülékenységek gyorsabb megtalálása jelenti, hanem azok elemzése, kijavítása és a javítások széles körű bevezetésének a koordinálása is. **Érdemes elsőként a kritikus fontosságú nyílt forráskódú szoftverek esetében cselekedni**, mivel a kritikus infrastruktúra ágazataiban nagy a behatolás. A jelentések szerint a teljes kódbázis 98 %-a nyílt forráskódú, amelyből a kritikus infrastruktúrák ágazata átlagosan a magas vagy kritikus kockázatú sérülékenységgel rendelkező kódbázisok mintegy 80 %-át teszi ki.[30]

A technológiai szuverenitási csomag részeként közzétett, **nyílt forráskódra alapuló uniós stratégia**[31] számos intézkedést tartalmaz a kritikus nyílt forráskódú alkotóelemek biztonságának növelésére és karbantartásának támogatására. Ezzel összefüggésben a Bizottság együtt fog működni az ENISA-val, a tagállamokkal[32] és nyílt forráskódú közösségekkel annak érdekében, hogy kísérleti jelleggel kipróbáljon néhány, kifejezetten a kibertérre és a mesterséges intelligenciára irányuló intézkedést.

Az ENISA a Bizottsággal, a tagállamokkal és a nyílt forráskódú közösségekkel együttműködve fel fogja gyorsítani a kritikus nyílt forráskódú alkotóelemek stratégiában előirányzott feltérképezését, valamint az elfogadott kritériumokon alapuló előzetes lista alapján **kísérleti jelleggel** a kritikus infrastruktúrák szempontjából releváns nyílt forráskódú alkotóelemekre vonatkozó, a **kritikus nyílt forráskód rezilienciájára irányuló kampányt indít**. A kampány eredményei információkkal szolgálnak majd a nyílt forráskódú karbantartási eszköz megvalósításához. A kampány egy önkéntes szponzorálási programból fog állni, amelyben a nyílt forráskódú projekteket olyan szervezetekkel kapcsolják majd össze, amelyek készek szoros partnerségben együttműködni a projektek karbantartóival fenntartásuk és biztonságuk támogatása érdekében. A szponzorok közé tartozhatnak tagállamok, uniós szervezetek (mint például a CERT-EU), kritikus infrastruktúrák üzemeltetői, gyártók és más olyan nyilvánosan vagy zártkörűen működő gazdálkodó egységek, amelyek támogatást tudnak nyújtani, például azáltal, hogy képzett embereket, illetve MI-modelleket és -eszközöket bocsátanak a nyílt forráskódú projektek fenntartói rendelkezésére. A tagállamok és más jogosult felhasználók az **uniós kiberbiztonsági tartalék** keretében megbízható magánszolgáltatók támogatására támaszkodhatnak a kritikus infrastruktúrák nyílt forráskódú függőségeinek sérülékenységi vizsgálata érdekében. Emellett az ENISA össze fogja állítani a

[30] Blackduck, 2026., *Open Source Security and Risk Analysis Report [Jelentés a nyílt forráskód biztonságáról és kockázatelemzéséről]*: a repülő- és űripar, a légi közlekedés, a gépjárműipar, a szállítás és a logisztika esetében például 87 %; a feldolgozóipar esetében 88 %; az egészségügy esetében 88 %; az energia esetében 89 %; az internet és szoftverinfrastruktúra esetében pedig 80 %.

[31] COM(2026) 503 final.

[32] Adott esetben különösen a digitális közjavakkal foglalkozó európai digitális infrastruktúra-konzorciummal (EDIC) együttműködve.

mesterséges intelligencián alapuló szolgáltatások szolgáltatási katalógusát, amelynek célja a nyílt forráskódú sérülékenységek kijavításának és orvoslásának támogatása.

A nyílt forráskódú fenntartók igénybe vehetik a szponzorálási programot és a szolgáltatási katalógust munkájuk sebességének és eredményességének növelése, valamint az MI-modellek fejlődése által felgyorsított kiberkockázatok csökkentése érdekében. A kezdeményezés meg fogja erősíteni a meglévő nyílt forráskódú kormányzást és munkafolyamatokat, valamint próbaként is fog szolgálni Európának a mesterséges intelligenciával támogatott helyreállításra irányuló szélesebb körű erőfeszítéseihez, tovább fejlesztve az Unió operatív know-how-ját. Számos különféle ágazatban hozzá fog járulni a kiberreziliencia megerősítéséhez, többek között a kritikus infrastruktúrák és a kkv-k esetében. Az első kísérleti kampány 2026-ban indul, és amennyiben sikeresnek bizonyul, tovább fogják bővíteni, többek között a nyílt forráskódra vonatkozó stratégiával összefüggésben.

Fő intézkedések

- **4. fő intézkedés: az ENISA az érintett uniós szervezetekkel együttműködve iránymutatást, ajánlásokat, tanácsokat és bevált gyakorlatokat fog közzétenni a mesterséges intelligencián alapuló fenyegetésekkel szembeni védelemről és a mesterséges intelligencia kiberbiztonsági műveletekbe való biztonságos integrálásáról (2026 harmadik negyedévétől).**
- **5. fő intézkedés: a Bizottság, a tagállamok, az ENISA és az ágazat együtt fog működni annak érdekében, hogy a sérülékenységmenedzsment meglévő gyakorlatai és eszközei megfeleljenek a mesterséges intelligencia korának (2026 harmadik negyedévétől).**
- **6. fő intézkedés: az ENISA a Bizottsággal, a tagállamokkal, a nyílt forráskódú közösségekkel, az uniós szervezetekkel és az ágazattal együttműködve el fogja indítani a kritikus nyílt forráskód rezilienciájára irányuló kampány első kísérleti projektjét a javítások felgyorsítása érdekében, többek között a mesterséges intelligencia kiaknázása révén (2026 negyedik negyedéve).**

4. 3. pillér: az európai MI-képességek skálázása a kiberbiztonság érdekében

Egy olyan környezetben, ahol mind a defenzív, mind az offenzív kiberműveletek egyre nagyobb mértékben támaszkodnak a fejlett mesterséges intelligenciára, a mesterséges intelligencián alapuló kiberbiztonsági megoldások kifejlesztésének és alkalmazásának képessége a kiberreziliencia és a kiberszuverenitás stratégiai támogató eszközévé válik. Különösen az érzékeny felhasználási esetekben fontos, hogy az EU olyan szuverén MI-képességekre támaszkodhasson, amelyek megfelelnek a szükséges biztonsági igényeknek, többek között a védelem területén. Az EU-nak most lehetővé kell tennie az európai szolgáltatók, köztük a diszruptív innovátorok számára, hogy Európában fejlesszenek ki, vezessenek be és skálázzanak ilyen fejlett mesterséges intelligenciát. A kibertérre és a mesterséges intelligenciára vonatkozó beruházási stratégiáját kiegészítve az EU-nak össze kell gyűjtenie technológiai ökoszisztémáját annak érdekében, hogy kezelje a legsürgetőbb operatív kiberbiztonsági igényeket, hogy az európai MI-képességek élvonalbelivé fejlesztésére és elterjesztésére irányuló beruházásokat mozdítson elő, valamint fejlessze az ilyen képességek ágazatokon átívelő bevezetéséhez szükséges készségeket.

4.1. A mesterséges intelligencián alapuló kiberbiztonsági megoldások európai ökoszisztémájának fellendítése

Mivel a mesterséges intelligenciát már most is felhasználják rosszindulatú célokra, a szervezeteknek a támadóknál gyorsabban kell haladniuk a rendelkezésre álló, mesterséges intelligencián alapuló kiberbiztonsági megoldások alkalmazása terén a kritikus infrastruktúrák védelme érdekében a különböző ágazatokban. Az EU-nak ösztönöznie kell az európai piacot, hogy a szükséges gyorsasággal és léptékben váljanak elérhetővé ezek az eszközök, valamint támogatnia kell a kritikus infrastruktúráinkban való elterjedésüket is.

Az EU már most is jelentős beruházásokat hajt végre a **saját fejlesztésű, fejlett mesterséges intelligencián alapuló kiberbiztonsági technológiák kutatásának és fejlesztésének**, valamint a mesterséges intelligencia kiberbiztonságának támogatása érdekében, a jelenlegi többéves pénzügyi keret végéig nevezetesen 200 millió EUR összeget szán erre a célra a Horizont Európa és a Digitális Európa program keretében. 2026 végén például három Horizont Európa vezérprojekt indul a digitális folyamatok és rendszerek kibertámadásokkal – többek között ellenséges MI-támadásokkal – szembeni nyomonkövetési, észlelési, reagálási és ön-helyreállítási képességeit szolgáló mesterséges intelligencia fejlesztésének, tanításának és tesztelésének, valamint a folyamatos nyomon követést, megfelelést és automatizált helyreállítást szolgáló generatív MI-eszközök és -technológiák fejlesztésének támogatása érdekében. Az EU a Horizont Európa, a Belső Biztonsági Alap, a Digitális Európa és az Európai Biztonsági Kutatási és Innovációs Közösség révén a bűnüldözés terén is finanszírozza a teljes MI-képességciklust (a kutatástól a tesztelésig, a validálásig és az operatív telepítésig). Hasonlóképpen, az EU az Európai Innovációs Tanácson (a továbbiakban: EIC) keresztül is – többek között az EIC-alap közvetlen befektetései révén – beruházásokat hajt végre európai mélytechnológiai kiberbiztonsági és MI-vállalatokba, 2026-ban és 2027-ben pedig kiterjeszti beruházásait releváns kettős felhasználású és stratégiai védelmi technológiákra is.[33] Konkrétabban, 2026 végéig a Bizottság lehetővé fogja tenni, hogy az EIC-alap a stratégiai védelmi technológia területén induló és növekvő innovatív vállalkozásokba befektethető 100 millió EUR összeg részeként kiberbiztonsági és MI-technológiai vállalatokba fektessen be, és 2027-ben is hasonló támogatást nyújtson. A Növekvő Európa Alap még 2026-ban végre fogja hajtani az első beruházását a stratégiai vállalkozások növekedési szakaszába. Az Európai Unió nemzetközi digitális stratégiájára építve az EU és a tagállamok az EU technológiai üzleti ajánlatát is ki fogják használni a mesterséges intelligencia és a szoftvermegoldások bevezetésének támogatására.

E beruházások kiegészítéseként az Uniónak arra is törekednie kell, hogy tovább **gyorsítsa a fejlett mesterséges intelligencián alapuló kiberbiztonsági képességeknek a mesterséges intelligenciát használó nagyszabású kibertámadásokkal szembeni bevetésével kapcsolatos tudás megosztását**. Napjainkban az EU gazdag ökoszisztémával és tudásbázissal rendelkezik a tudományos körökben, az iparban és a kormányzatban, de a mesterséges intelligencián alapuló kiberbiztonsági megoldások továbbra is széttagoltak, működési környezetben nem tesztelték őket megfelelően, és messze nem alkalmazzák őket széles körben az ágazatokban.[34] Erre példa a sérülékenységek automatizált orvoslása, amely a mesterséges intelligencia korában a kiberbiztonság egyik fő működési szűk keresztmetszete: napjainkban a mesterséges intelligencián alapuló sérülékenységfeltárás gyorsabban halad, mint a mesterséges intelligenciával támogatott helyreállítás, ami strukturális egyensúlyhiányt teremt a támadók javára. Az offenzív mesterséges intelligencia jelentette fenyegetések kezelésére irányuló felhívásokra válaszolva[35] a Bizottság ezért az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont támogatásával és az ENISA-val együttműködve **uniós nagy**

[33] Az EIC-alap – Európai Innovációs Tanács – Európai Bizottság.
[34] Public Letter of Support for a European Grand Challenge in AI and Security [Nyilvános támogató levél a mesterséges intelligenciával és a biztonsággal kapcsolatos európai nagy kihívásról] – Google Dokumentumok.
[35] Ugyanott.

kihívást indít a sérülékenységek mesterséges intelligenciával támogatott orvoslására. Az európai kiberbiztonsági és MI-vállalatokat, a kutatószervezeteket, a kritikus infrastruktúrák üzemeltetőit és a nyílt forráskódú közösségeket e közös küldetés köré tömörítő nagy kihívás támogatni fogja egy olyan MI-rendszer kifejlesztését, amely a helyreállítás teljes életciklusa során képes lesz majd segíteni a kiberbiztonsági csoportokat. A kutatás és a bevezetés összekapcsolásával a nagy kihívás lehetővé teszi majd, hogy az ígéretes megoldásokat realisztikus működési környezetben teszteljék, és végső soron Európa-szerte a szervezetek rendelkezésére bocsássák, hozzájárulva az időben történő helyreállítást akadályozó működési szűk keresztmetszetek csökkentéséhez. Az érdekelt tagállamok felkérést fognak kapni arra, hogy támogassák a tudásmegosztásra irányuló ezen erőfeszítéseket.

4.2. Az európai élvonalbeli képességek kialakítása

Bár a kiberbiztonsági képességekkel rendelkező meglévő MI-modellek és -rendszerek már most is jelentős lehetőségeket kínálnak a kiberbiztonsági műveletekhez, a mesterséges intelligencián alapuló, élvonalbeli kiberképességek szintén nagy potenciált tartogatnak Európa technológiai szuverenitása, biztonsága és védelme szempontjából. Ezért az EU-nak **ki kell fejlesztenie saját szuverén, általános célú, élvonalbeli MI-képességeit** annak érdekében, hogy enyhítse az új függőségek kockázatát attól az immár kritikus stratégiai eszköztől, amely az élvonalbeli MI egyre nagyobb potenciáljával rendelkezik a kettős felhasználást tekintve, és amely jóval túlmutat a kiberbiztonság területén. Ez szélesebb körű, ágazatokon átívelő kihívást jelent gazdaságunk és társadalmunk számára, amelyet a Bizottság továbbra is szorosan nyomon fog követni és kezelni fog annak alakulása során.

A Bizottság már tett konkrét lépéseket annak érdekében, hogy támogassa a kulcsfontosságú európai szereplőket az MI-képességek élvonal felé történő előmozdításában.

- A Bizottság a közelmúltban odaítélte az élvonalbeli MI nagy kihívás díját, amely hozzáférést biztosít az EuroHPC számítási kapacitásához, támogatva egy nyílt forráskódú, fejlett európai MI-modell fejlesztését.[36]
- A mesterségesintelligencia-tudomány európai erőforrásközpontja (a továbbiakban: RAISE) keretében a Bizottság élvonalbeli MI-laboratóriumok hálózatát finanszírozza, hogy ezen a területen is előmozdítsa a kutatást.
- A Horizont Európa program keretében a Bizottság olyan tevékenységeket finanszíroz, amelyek célja, hogy a biztonságos és védett mesterséges intelligenciát élvonalbelivé méretezzék.
- A Bizottság továbbra is együtt fog működni Franciaországgal és Németországgal egy olyan, együttműködésen alapuló erőfeszítés (az európai élvonalbeli MI kezdeményezés) létrehozása érdekében, amellyel kutatási és innovációs kockázatvállalásra törekednek, tehetségeket akarnak vonzani és a kiválásokat szeretnék megkönnyíteni.
- A Bizottság az élvonalbeli MI-fórumon keresztül technikai tanácsadásban részesül.[37]

Ezek a kezdeti lépések fontos alapot teremtenek, de **szemléletváltásra van szükség az ambíciók és az erőforrások terén** ahhoz, hogy Európa élvonalbeli mesterséges intelligenciával kapcsolatos törekvései tartós szuverén kapacitássá és versenyelőnnyé

[36] Commission selects EUROPA consortium as the winner of the Frontier AI Grand Challenge, a project to build European open-source frontier AI model in all 24 EU languages [A Bizottság az EUROPA konzorciumot választotta az élvonalbeli MI nagy kihívás győztesének, azt a projektet, amely az EU 24 nyelvén európai nyílt forráskódú élvonalbeli MI-modell kialakítását tűzte ki célul] | Európa digitális jövőjének megtervezése.

[37] Commission seeks experts for forum on Frontier AI [A Bizottság szakértőket keres az élvonalbeli MI-fórumhoz] | Európa digitális jövőjének megtervezése.

válhassanak. Tekintettel az élvonalbeli mesterséges intelligencia fejlesztéséhez szükséges erőforrások példátlan nagyságrendjére, az élvonalbeli projektek uniós szintű együttműködésen alapuló megközelítést igényelnek. A felhőszolgáltatások és a mesterséges intelligencia fejlesztéséről szóló javasolt rendelet ezeket kiemelt projektként határozza meg, és Uniós számítási erőforrásokat allokál a tagállamok által kiosztottak kiegészítéseként. **A meglévő MI-gyárakat és a jövőbeli gigagyárakat** ki kell használni arra, hogy egy szuverén európai MI- és kiberbiztonsági infrastruktúra részeként szolgáljanak (amelybe beletartoznak a számítások, az adatok és a konnektivitás), valamint az EU-t vezető MI-kontinensként pozicionálják. Ez a konnektivitás előfeltétele a mesterséges intelligenciára kész adatkészletek megbízható megosztásának, az erőforrások határokon átnyúló összevonásának, az ellenőrzött környezetek biztonságos működésének, valamint a szilárd, megbízható és nagy teljesítményű MI-kiberképességek fejlesztésének, tesztelésének, bevezetésének és az azokhoz való hozzáférésnek. A releváns, kiberközpontú MI-gyáraknak megbízható, biztonságos és reziliens adatmegosztási mechanizmusok révén meg kell könnyíteniük a hozzáférést a mesterséges intelligenciára kész, jó minőségű adatkészletekhez (a nyilvános adatoktól az érzékeny ipari[38] és kiberbiztonsági adatokig), valamint adatlaboratóriumaikon keresztül támogatniuk kell az MI-modellek ellenőrzött, elszámoltatható és ellenőrizhető környezetben történő fejlesztését és validálását.

A Bizottság az Európai Versenyképességi Alapon keresztül a szuverén európai MI-kiberképességek fejlesztését is támogatni fogja, többek között a védelem számára, biztosítva, hogy Európa jobban fel legyen készülve stratégiai érdekeinek védelmére és a kritikus függőségek csökkentésére. Ezzel összefüggésben a Bizottság külön munkacsoportot hoz létre az érintett ügynökségekkel, köztük az ENISA-val és az Európai Védelmi Ügynökséggel (a továbbiakban: EDA), valamint a tagállamokkal az élvonalbeli MI-modellek védelmi és kettős felhasználású kritikus rendszerekbe való bevezetéséhez kapcsolódó biztonsági kockázatok kezelése érdekében.

A szuverén élvonalbeli képességek fejlesztése **több százmilliárd eurós beruházási igénnyel jár**, amelyet csak részben lehet a közpénzügyekből fedezni. Sürgősen nagy mennyiségű magánberuházást, valamint különösen kockázati tőkét és saját tőkét kell bevonni, hogy innovatív európai megoldásokat lehessen fejleszteni és skálázni. Számítás, modellek és adatinfrastruktúra nélkül Európa továbbra is arra kényszerül, hogy kiszolgáltatott felhasználója legyen olyan, máshol készített élvonalbeli MI-rendszereknek, amelyeket mások váratlanul kikapcsolhatnak, ami óriási gazdasági és (kiber)biztonsági következményekkel járna. Ugyanakkor, bár meglehet, hogy a saját élvonalbeli MI-kapacitás kiépítésének költségei Európa számára nagyon magasak, ahogy az MI-képességekkel kapcsolatos szakadék egyre nő, annak a költségei még nagyobbak lehetnek, sőt akár évről évre növekedhetnek is, ha nem építik azt ki.

A 2026. június 3-i technológiai szuverenitási csomagjával a Bizottság **konzultációkat indított a tagállamokkal, az Európai Beruházási Bank Csoporttal (a továbbiakban: EBB csoport) és más kulcsfontosságú érdekelt felekkel egy javaslatról, amely egy új európai tőkekapacitás létrehozására irányul**; ez a technológiai szuverenitásunk szempontjából kulcsfontosságú fejlett technológiákba és infrastruktúrába – többek között az olyan digitális technológiákba, mint amilyen például az élvonalbeli mesterséges intelligencia, valamint a tisztaenergia-technológiákba, a biotechnológiába és potenciálisan a védelmi technológiákba – történő nagyszabású tőkebefektetések portfólióját kezelné. E mechanizmus fő előnye az lenne, hogy az uniós szinten már meglévő pénzügyi eszközökkel – például a Növekvő Európa Alappal

[38] Az alkalmazandó jogszabályoknak, többek között az uniós versenyjognak való megfelelés függvényében.

– szinergiában dolgozva vagy azokba fektetve teremtene meg egy kifejezetten szükséges „tőketársbefektetési horgonyt”, amellyel nagy mennyiségű magánberuházást vonnának be. Ez az új stratégiai technológiai tőkefinanszírozási eszköz gyökeres változást hozna az élvonalbeli mesterséges intelligenciába történő nagy uniós beruházásokra irányuló legutóbbi felhívás megválaszolásában. Ami az Európai Versenyképességi Alap InvestEU-eszközét illeti, egy ilyen mechanizmus fontos szervezetté válhatna a fejlett technológiákba és infrastruktúrába történő nagy befektetési jegyekre irányuló stratégiai tőkebefektetések szempontjából.

4.3.A kiberbiztonsági készségek fejlesztése a mesterséges intelligencia korában

A technológia önmagában nem elég Európa sikeréhez. A fejlett MI kiberbiztonsági műveletekben való hatékony és biztonságos bevezetésének a képessége attól is függ, hogy **rendelkezésre állnak-e olyan képzett szakemberek, akik képesek megérteni és biztonságosan használni a fejlett kiberképességekkel rendelkező MI-modelleket**, valamint kezelni az MI-specifikus kockázatokat. Ahogy a kiberbiztonsági csoportok egyre inkább integrálni fogják a fejlett mesterséges intelligenciát, egyre súlyosbodhat a meglévő kiberbiztonsági készséghiány. Az EU-nak ezért meg kell erősítenie kiberbiztonsági munkaerejét azáltal, hogy felvértezi azt a megfelelő, kiberbiztonsághoz szükséges MI-készségekkel.

Az **EU Kiberkészségek Akadémiája**, amely konkrét kiberbiztonsági képzési vállalások és partnerségek köré tömöríti az ipart, a képzési szolgáltatókat és a tudományos intézményeket, megfelelő keretet biztosít ennek az igénynek az uniós szintű kezeléséhez. A Bizottság a tagállamokkal együtt fel fogja használni ezt a növekvő ökoszisztémát arra, hogy a Kiberkészségek Akadémiája keretében célzott intézkedést indítson annak érdekében, hogy képzési programokat dolgozzon ki a kiberbiztonsági szakemberek számára az MI-eszközök használatához. A küszöbön álló MI-készségakadémiával való lehetséges szinergiákat is fel kell tárnia. Emellett az ENISA aktualizálni fogja az **európai kiberbiztonsági készségkeretet**, ami során integrálni fogja a mesterséges intelligenciával kapcsolatos kompetenciákat a meglévő szakmai profilokba, és szükség esetén új szerepeket határoz majd meg.

Fő intézkedések:

- **7. fő intézkedés: a Bizottság az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpont támogatásával és az ENISA-val együttműködve uniós nagy kihívást indít a mesterséges intelligencián alapuló európai kiberbiztonsági megoldások skálázásának elősegítése érdekében (2026 negyedik negyedéve).**
- **8. fő intézkedés: a Bizottság a tagállamokkal együtt arra fog törekedni, hogy hozzáférést biztosítson az MI-gyárak számítási kapacitásához a szuverén számításon alapuló, kiberrezilienciát szolgáló, rendelkezésre álló fejlett és élvonalbeli MI-modellek tesztelése, tanítása és bevezetése érdekében.**
- **9. fő intézkedés: a Bizottság együtt fog működni a tagállamokkal és az iparral (a Kiberkészségek Akadémiája keretében) annak érdekében, hogy képzési modulokat dolgozzon ki a kiberbiztonsági szakemberek számára a mesterséges intelligencia kiberbiztonsági célú használatáról (2026 negyedik negyedéve).**

5. Együttműködés hasonlóan gondolkodó partnerekkel a kiberbiztonság globális megközelítése érdekében a mesterséges intelligencia korában

A mesterséges intelligencia kiberbiztonsági vonatkozásai természetüknél fogva globálisak, mivel az MI-modellek és -rendszerek, a szoftverellátási láncok és a nyílt forráskódú ökoszisztémák határokon átnyúlva működnek. Az egyik joghatóságban kifejlesztett kiberképességekkel rendelkező MI-modell bevezetése világszerte jelentős következményekkel járhat a kritikus infrastruktúrák és vállalkozások biztonságára nézve. A kormányok, a nemzetközi szervezetek és az ipar ezért **közös kihívással néz szembe, és a nemzetközi együttműködés elengedhetetlen** a széttagoltság elkerüléséhez, a megbízható partnerek közötti interoperabilitás előmozdításához, valamint a mesterséges intelligenciával kapcsolatos kiberbiztonsági kockázatok enyhítésére irányuló erőfeszítések egyesítéséhez.

Az EU-nak vezető szerepet kell vállalnia a megbízható mesterséges intelligenciával és a kiberrezilienciával kapcsolatos globális gyakorlatok formálásában, kihasználva **a mesterséges intelligenciára és a kiberrezilienciára vonatkozó uniós szabályozási keretet**. Különösen a hasonlóan gondolkodó partnerek közötti szorosabb együttműködésre van szükség annak biztosítása érdekében, hogy az élvonalbeli MI-képességek biztonságosak maradjanak, és egyúttal rendelkezésre is álljanak a megbízható felhasználásra, ugyanakkor meg lehessen akadályozni, hogy rosszindulatú szereplők visszaéljenek velük. Ez a cselekvési terv egyben felhívás is a nemzetközi partnereink számára, hogy csatlakozzanak a mesterséges intelligencia biztonságára és a kiberrezilienciára vonatkozóan javasolt intézkedések hatásának fokozására irányuló erőfeszítésekhez.

A Bizottság különösen két- és többoldalú fórumokon törekszik e célkitűzések megvalósítására. Továbbra is aktívan részt fog venni a **G7-csoportban a megközelítése előmozdítása érdekében**, többek között a **digitális és technológiai, valamint a kiberbiztonsági munkacsoporton** keresztül, hogy támogassa a fejlett MI-képességekből eredő kiberbiztonsági kockázatok közös értelmezésére irányuló munkát. A Bizottság együttműködést fog ösztönözni a G7-ekkel a szabványokkal és a szóban forgó modellek értékelésével kapcsolatban. Felkéri továbbá a G7-tagokat és más nemzetközi partnereket, hogy vegyenek részt a nyílt forráskódú szoftverek biztonságának támogatására irányuló erőfeszítésekben, és működjenek együtt a sérülékenységmenedzsment gyakorlatainak kiigazítása érdekében. Az EU továbbra is részt fog venni az ENSZ-ben.

Kétoldalú szinten az EU el fogja mélyíteni a partnerországokkal a fejlett mesterséges intelligenciáról és a kiberbiztonságról folytatott eszmecserét, többek között digitális partnerségek, digitális párbeszédek vagy kiberdialógusok révén, és adott esetben prioritásként fogja kezelni a modellek értékelését, a kritikus infrastruktúrák védelmét, a sérülékenységek csökkentését és a kiberreziliencia javítását mint az együttműködés alapvető területeit.

Emellett a **Network of Advanced AI Measurement, Evaluation and Science (a fejlett MI-méréssel, -értékeléssel és -tudománnyal foglalkozó hálózat), amelyet az Egyesült Királyságbeli AISI koordinál**, és amely szorosan együttműködik a partnerországok biztonsági és védelmi intézményeivel, valamint **a Bizottság MI-hivatalával**, fontos platform az élvonalbeli MI-modellek értékelésére szolgáló közös módszertanok kidolgozásához, a bevált gyakorlatok cseréjéhez, valamint a mesterséges intelligencia biztonságával és védelmével kapcsolatos megbízható nemzetközi együttműködés támogatásához.

A Bizottság ösztönözni fogja továbbá a kormányok és a vezető élvonalbeli MI-fejlesztők közötti strukturált párbeszédet az élvonalbeli mesterséges intelligencia biztonságára, értékelésére és felelős bevezetésére vonatkozó közös megközelítések előmozdítása érdekében.

Végezetül, tekintettel az európai és nemzetbiztonságra gyakorolt említett következményekre, az EU meg fogja erősíteni a meglévő információcserét a **NATO**-val a kibertérben rendelkezésre álló élvonalbeli MI-képességekkel kapcsolatos lehetőségekről és kockázatokról,

többek között a NATO mesterséges intelligenciával foglalkozó, hamarosan létrejövő kiválósági központjának kiaknázása révén.

6. Következtetés

Ez a cselekvési terv a folyamatos és összehangolt európai erőfeszítések folytatását jelenti. Ahogy a fejlett MI-képességek fejlesztése tovább fog gyorsulni, valamint új lehetőségek és kockázatok merülnek fel, a Bizottság rendszeresen értékelni fogja a cselekvési terv végrehajtását, és szükség esetén kiigazítja az intézkedéseket annak biztosítása érdekében, hogy az hatékonyan hozzájáruljon a mesterséges intelligencia korának megfelelő biztonságos és reziliens európai ökoszisztéma kialakításához.