NYÍLT LEVÉL

a mesterséges intelligencián alapuló kibertámadásokkal szembeni azonnali nemzeti felkészülés tárgyában

Budapest, 2026. szeptember 2.

Címzettek

Magyar Péter úr Magyarország miniszterelnöke
Forsthoffer Ágnes asszony az Országgyűlés elnöke
Baka András úr Magyarország köztársasági elnöke, a Magyar Honvédség főparancsnoka

---

Tisztelt Miniszterelnök Úr! Tisztelt Elnök Asszony! Tisztelt Elnök Úr!

Azért fordulunk egyszerre Önökhöz, mert az ügy, amelyről írunk, egyetlen tárcához sem tartozik. Össznemzeti ügy. Egyszerre érinti a kormányzati végrehajtást, a törvényhozást és a honvédelmet. Aki csak a saját hatáskörét nézi, az ebben az ügyben senkinek nem felel.

1. Ami 2026. augusztus 27-én történt

Az OpenAI, az Anthropic, a Microsoft, az Amazon Web Services és több mint száz további technológiai vállalat, kiberbiztonsági cég, távközlési és pénzügyi szolgáltató közös nyílt levélben figyelmeztetett arra, hogy a mesterséges intelligencián alapuló kibertámadások hónapokon belül nagyságrendet lépnek, és hogy a védekezés megerősítésére csak korlátozott idő áll rendelkezésre.

Ezek a vállalatok nem érdekeltek a pánikkeltésben. Ők építik ezt a technológiát. Amikor a fejlesztő figyelmeztet a saját terméke kockázatára, azt nem lehet marketingnek nevezni.

A levél nevesített kockázatként említi a kórházakat, a vízműveket és az internet működését. A kormányoktól három dolgot kér: a fenyegetettségi információk megosztási csatornáinak megerősítését, a védekezés összehangolását helyi, nemzeti és nemzetközi szinten, valamint több forrást a kritikus infrastruktúra védelmére.

A figyelmeztetés mögött megtörtént esetek állnak, nem forgatókönyvek:

- 2026 júliusában az OpenAI egyik tesztje során a vizsgált modell kijutott az elszigetelt tesztkörnyezetéből, és egy külső rendszerből szerezte meg a feladat megoldásait.
- 2026 júliusában az Anthropic modelljei internet-hozzáférést kapva három szervezet rendszerébe hatoltak be.
- 2025 novemberében az Anthropic nyilvánosságra hozta, hogy egy kínai állami hátterűnek tartott csoport a Claude modellt használva mintegy harminc vállalatot, pénzintézetet és kormányzati szervezetet támadott meg, és a műveletek túlnyomó részét már a modell hajtotta végre önállóan.
- Az augusztusi nyílt levél hivatkozik amerikai vízellátó rendszerek elleni támadásokra, amelyeknél MI által generált támadókódot használtak.

Ez a lista nyilvános. Az a lista, amelyik nem nyilvános, hosszabb.

2. Ami Magyarországon történt

2026. augusztus 2-án kibertámadás érte a Magyar Államkincstárt. Zsarolóvírus titkosított állományokat több belső rendszerben. A sajtóban megjelent szakértői elemzések szerint a támadás elérhette az agrártámogatási, a nyugdíj- és a családtámogatási adatbázisokat, valamint az önkormányzati számlavezetéshez kapcsolódó rendszereket. A Kincstár közlése szerint adatvesztés nem történt. Ezt a mai napig nem támasztotta alá nyilvános, tételes technikai vizsgálat.

Fontos előzmény, hogy az Állami Számvevőszék már 2019-ben jelezte a Kincstár által átvett informatikai hálózat adatvédelmi kockázatait. A figyelmeztetés megvolt. A hét év nem volt elég idő.

2026. augusztus 27-én, ugyanazon a napon, amikor a világ vezető technológiai vállalatai közösen figyelmeztettek a küszöbön álló MI-alapú támadásokra, a Vezető Informatikusok Szövetsége az Év Informatikai Vezetőjének választotta a Magyar Államkincstár informatikáért felelős alelnökét.

Legyen világos: ez nem a díjazott személyéről szól, és nem is a szakmai szervezet döntéséről, amelynek joga van bárkit elismerni. Arról szól, hogy a magyar közéletben nincs következménye annak, ha egy kritikus állami rendszer elesik. Nincs kivizsgálás, amelynek nyilvános eredménye lenne. Nincs felelős, akit meg lehetne nevezni. Négy héttel egy sikeres támadás után az ország úgy viselkedik, mintha semmi nem történt volna.

Ez a hozzáállás az, ami minket ki fog ütni. Nem a technológiai lemaradás.

3. Egy éve figyelmeztetünk

Farkas Dezső és az IRÁNY a Jövő Párt több mint egy éve, a párt bejelentő videójától kezdve következetesen azt képviseli, hogy a mesterséges intelligencia és a kvantumtechnológia stratégiai ágazat, nem informatikai részkérdés.

2026. február 13-án a gépek közötti gazdaság megjelenéséről és a magyar lemaradásról írtunk. 2026. július 25-én részletesen bemutattuk azt az OpenAI-tesztet, amelyben a modell nulladik napi sérülékenységet talált és használt ki. 2026. augusztus 4-én azonnali kormányzati intézkedéseket sürgettünk, és kértük a kritikus állami, egészségügyi, energetikai, pénzügyi és közlekedési rendszerek valós védelmének felmérését, MI-alapú támadási tesztek elvégzését.

Azóta kormány váltotta a kormányt. Érdemi lépés egyik oldalon sem történt. Ez a levél ezért nem pártkérdésként fogalmazódik meg. Nem az a kérdésünk, hogy ki volt hatalmon, amikor elmulasztották. Az a kérdésünk, hogy **ki fogja megcsinálni**.

4. Miért szuverenitási és nemzetbiztonsági kérdés

Egy ország szuverenitása ma nemcsak a határain múlik. Azon is múlik, hogy ki fér hozzá a nyugdíjasok adataihoz, ki tudja leállítani az áramszolgáltatást, ki tudja megbénítani a kórházi ellátást, és ki tudja manipulálni azokat a nyilvántartásokat, amelyekre a jogállam működése épül.

Az MI-alapú támadás abban különbözik minden korábbitól, hogy gépi sebességgel fut, önállóan alkalmazkodik az akadályokhoz, és több sérülékenységet kapcsol össze egyetlen, többlépéses műveletben. Az emberi támadókra tervezett védelmi eljárások, az emberi ügyeletre és emberi reakcióidőre épített folyamatok ezzel nem tartanak lépést. A Microsoft ezért állít MI-t az MI-vel szembe.

A kvantumtechnológia fejlődése ezt csak gyorsítja. Ha az önálló problémamegoldó képesség és a kvantumszámítási kapacitás összeér, a mai védelmi feltételezéseink egyik napról a másikra érvényüket vesztik. A titkosítás feltörése ehhez nem is szükséges. Elég a kerülőút: a gyengén védett szoftver, az emberi hiba, az ismeretlen biztonsági rés. Arról nem is beszélve, hogy a „harvest now, decrypt later” (HNDL) elv alapján már most gyűjtik a titkosított adatokat. Biztosan tudva, hogy már csak rövid ideig kell tárolni, ugyanis nemsokára fel tudják törni.

A szövetségesi rendszerben Magyarország nemcsak védendő fél, hanem a szövetség biztonságáért felelős fél is. Egy elesett magyar állami rendszer nemcsak magyar probléma. Ezért nem elég, ha az ügyet informatikai üzemeltetési kérdésként kezeljük: honvédelmi és államfői szinten is napirenden a helye. Nem véletlen, hogy az USA és az EU az elfogadott szabályai alapján már 2030-ra teljesen kvantumvédetté akarja tenni a teljes kormányzati hálózatát, amihez minden szükséges időarányos lépést már megtettek.

5. Amit Önöktől kérünk

Nem általános elköteleződést kérünk, hanem határidőhöz kötött, számonkérhető lépéseket. Mivel mindhárman más eszközzel rendelkeznek, mindegyikőjüktől mást kérünk.

Tisztelt Miniszterelnök Úr! A végrehajtás Önnél kezdődik. Öntől azt kérjük, hogy nevezzen meg egy felelőst, aki tárcák felett koordinál, rendelje el a kritikus rendszerek valós védelmének felmérését és MI- és kvantumalapú tesztelését, hozza nyilvánosságra a Kincstárt ért támadás tényeit, és tegye a kibervédelmet önálló, elkülönített költségvetési sorrá. Az alábbi lista 1., 2., 4., 5., 6., 8. és 9. pontja az Ön hatáskörébe tartozik.

Tisztelt Elnök Asszony! Az Országgyűlés nemcsak törvényt hoz, hanem ellenőriz is. Öntől azt kérjük, hogy az illetékes bizottságok tűzzék napirendre a Kincstárt ért támadást és a kritikus rendszerek felkészültségét, hogy az MI által generált kód biztonsági követelményei jogszabályi szintre kerüljenek, hogy a 2027-es költségvetés vitájában a kibervédelmi forrás önálló tételként jelenjen meg, és hogy a Ház határozatban mondja ki: az MI és a kvantumtechnológia stratégiai ágazat. Az alábbi lista 3., 6., 7. és 10. pontja az Ön hatáskörébe tartozik.

Tisztelt Elnök Úr! Ön az államfő és a Magyar Honvédség főparancsnoka. Öntől azt kérjük, hogy főparancsnokként kérjen tájékoztatást a Magyar Honvédség MI-alapú és kvantum kibervédelmi képességéről és arról, hogy egy gépi sebességű támadás esetén milyen reagálási rend áll rendelkezésre, továbbá hogy államfőként emelje pártok feletti nemzeti üggyé a kritikus infrastruktúra védelmét. Az Ön szava az egyetlen ebben az országban, amely mindhárom oldalról meghallgatható marad.

A konkrét lépések, amelyeket kérünk:

30 napon belül

1. **Tételes, nyilvános tájékoztatás a Magyar Államkincstárt ért támadásról:** mikor észlelték, mennyi ideig tartózkodott a támadó a rendszerben, mely adatbázisok voltak elérhetők, történt-e adatkiáramlás, és hány állampolgár érintett. Ahol jogszabály előírja, az érintettek egyedi értesítése.
2. **Nemzeti kibervédelmi felelős kinevezése**, aki tárcák felett koordinál, és akinek neve, hatásköre és beszámolási kötelezettsége nyilvános.
3. **Országgyűlési meghallgatás.** A Nemzetbiztonsági bizottság és a technológiáért felelős bizottság hallgassa meg a Kincstár, a kiberbiztonsági hatóság és a honvédelmi tárca vezetőit. A meghallgatás nyilvános részének legyen írásos összefoglalója.

60 napon belül

4. **A kritikus rendszerek MI- és kvantumalapú támadási tesztje.** Az állami, egészségügyi, energetikai, pénzügyi, közlekedési és vízellátási kritikus rendszerek kötelező, MI-asszisztált red team vizsgálata a Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény és a NIS2 keretrendszer alapján, külső, független szakértők bevonásával.
5. **Mérhető képességi célok kitűzése és nyilvánosságra hozatala:** mennyi idő alatt észlelnénk egy önállóan alkalmazkodó támadást, mennyi idő alatt reagálnánk rá, ki avatkozna közbe éjszaka és hétvégén, és mi történne, ha egy rendszer napokig észrevétlenül lenne veszélyben.

6. **Az MI által generált kód biztonsági követelményeinek szabályozása** az állami rendszerekben és az állami beszerzésekben. Ez az augusztusi nyílt levél egyik konkrét kérése minden szervezet felé.

90 napon belül

7. **Nemzeti MI és kvantum kibervédelmi program**, dedikált és elkülönített költségvetési sorral, beépítve a 2027-es költségvetésbe.
8. **Nemzetközi és vállalati együttműködési megállapodások:** csatlakozás a fenyegetettségi információk megosztási csatornáihoz, valamint keretmegállapodás a vezető MI- és kvantum fejlesztőkkel arról, hogy incidens esetén a magyar védekező szervezetek hozzáférjenek a legfejlettebb reagáló modellekhez. A nyílt levél ezt kifejezetten felajánlja. Élni kell vele.
9. **Post-kvantum kriptográfiai átállási ütemterv** az állami rendszerekre, prioritási sorrenddel és határidőkkel.
10. **Országgyűlési határozat** arról, hogy a mesterséges intelligencia és a kvantumtechnológia stratégiai ágazat, amelynek fejlesztése és védelme kormányzati cikluson átívelő nemzeti feladat.

6. Elismerés

Az IRÁNY a Jövő Párt ebben az ügyben nem ellenfelet keres. Ha ezek a lépések megtörténnek, azt nyilvánosan elismerjük, függetlenül attól, hogy ki hajtja végre. Tőlünk telhetően minden segítséget megadunk ehhez a munkához.

Egyetlen dolgot nem tudunk elfogadni: hogy megint eltelnek hónapok e területen konkrét eredmények nélkül.

Tisztelettel:

Farkas Dezső
IRÁNY a Jövő Párt

Hivatkozott források

1. Telex: Techcégek figyelmeztetnek: fel kell készülni az MI-vel végrehajtott kibertámadásokra (2026. 08. 28.) https://telex.hu/techtud/2026/08/28/techceg-figyelmeztetes-felkeszules-mi-kibertamadas
2. Axios: OpenAI, Anthropic, Microsoft warn of growing AI cyberattacks (2026. 08. 27.) https://www.axios.com/2026/08/27/openai-anthropic-issue-dire-cyber-threat-warning
3. Anthropic: Disrupting the first reported AI-orchestrated cyber espionage campaign (2025. 11.) https://www.anthropic.com/news/disrupting-AI-espionage
4. Economx: Kibertámadás érte a Magyar Államkincstárat (2026. 08. 02.) https://www.economx.hu/belfold/2026/08/02/kibertamadas-magyar-allamkincstar-hacker-oroszorszag/
5. Portfolio: Kibertámadás a Kincstár ellen: a nyugdíj- és a családtámogatási rendszerekhez is hozzáférhettek a hackerek (2026. 08. 11.) https://www.portfolio.hu/uzlet/20260811/kibertamadas-a-kincstar-ellen-a-nyugdij-es-a-csaladtamogatasi-rendszerekhez-is-hozzaferhettek-a-hackerek-megszolalt-a-kincstar-855422
6. Index: Szakértők szerint olyan súlyos hackertámadás érte a Magyar Államkincstárt, ami akár kormányválságot is előidézhet (2026. 08. 05.) https://index.hu/belfold/2026/08/05/magyar-allamkincstar-nemzeti-kifizeto-ugynokseg-orosz-kibertamadas-elemzes-adatvesztes-kormanyvalsag/
7. Bitport: A Magyar Államkincstár adta az Év Informatikai Vezetőjét (2026. 08. 27.) https://bitport.hu/iden-a-magyar-allamkincstar-adta-az-ev-informatikai-vezetojet
8. 2024. évi LXIX. törvény Magyarország kiberbiztonságáról https://net.jogtar.hu/jogszabaly?docid=a2400069.tv