

Az információ hasznosulásának újszerű távlatai a nemzetbiztonságban

Bevezetés

A napjainkban zajló információs társadalmi folyamatok rákényszerítik a nemzetbiztonságért felelős szervezeteket, hogy az információk 21. századi korszerű kezelését és felhasználását érintő aktuális folyamatok, új eljárások és modellek naprakész ismeretén keresztül garantálják hazánk védelmét, érdekeinek érvényesítését. A téma multidiszciplináris kapcsolatainak vizsgálata kiemelt figyelmet érdemel, hangsúlyozottan a kommunikációs, médiatudományi, társadalmi, kulturális, technológiai, szervezet- és vezetés-, valamint döntéelméleti aspektusok. A tanulmány ebben a megközelítésben tekint az információ és a nemzetbiztonság jövőbeli kapcsolatának felértékelődő jelentőségére.

A globális biztonsági helyzet az elmúlt évtizedekben jelentős változáson ment keresztül. Az új típusú kihívások új típusú válaszok adására ösztönözték az államok kormányzatát, különös tekintettel annak katonai, rendészeti és nemzetbiztonsági szolgálatait. Ebben a felgyorsult világban felértékelődött az információk szerepe, és a biztonság megteremtése érdekében kiemelten fontossá vált az információk gyors megszerzése, ellenőrzése, strukturálása, koordinálása és elemzése. Természetesen az előbb említett folyamatok nem öncélú tevékenységek. Annak érdekében kell történniük, hogy adott szervezet, illetőleg annak valamely szervezeti egysége, vagy tovább gondolkodva a kormányzati döntés előkészítésében, a döntéshozatalban résztvevők részére stabil, ellenőrzött és összefűzött információk álljanak rendelkezésre.

Jól látható, hogy a technológiai környezet változásának köszönhetően az információk jelenlegi felhasználási módjaiban bekövetkező módosulások jelentősen – ma még teljességében nem látható módon – alakítani fogják a biztonságért felelős honvédelmi és rendvédelmi szférát, így közvetve tagadhatatlanul hatással lesznek a hadtudomány jövőbeli alakulására, valamint a nemzetbiztonságért felelős szervezetek munkájára, azok hatékonyságára.

A tanulmány célja a technológia változásokra, lehetőségekre és a hozzájuk kapcsolódó állami intézkedésekre való rávilágítás, de nem kívánok foglalkozni a nemzetbiztonsági szakzsargonban gyakran megjelenő úgynevezett hírigény teljesítése érdekében alkalmazható különböző hírszerzési lehetőségek taglalásával, illetőleg a megszerzett hírszerzési információk ellenőrzésével, koordinációjával, strukturálásával, értékelésével, elemzésével.

1. A digitalizáció – az információ széles körű terjedése

A téma széles körű vizsgálatához nélkülözhetetlen az adatok, információk létrejöttének körülményeit alaposan megismerni, hiszen e nívók tudatában lehetséges a nemzetbiztonsági környezetre gyakorolt esetleges hatások pontos feltérképezése.

Életünket teljesen átszövi az információ, amelyet nemcsak keresünk, használunk, hanem szolgáltatunk is magunkról és környezetünkről. De hol és hogyan történik mindez, az interneten, az odakapcsolódó okoseszközeinken vagy csak egy szűk kör által értett és irányított térben? Sok fogalmat használunk a mindennapokban, amely nem rendelkezik olyan pontos meghatározással, amely a felhasználás minden területére igaz és kielégítő válaszokat képes biztosítani. Sokak által ismert mítosz az internetről, hogy a hidegháború „mellékterméke”, az Amerikai Egyesült Államok – az első Szputnyik fellövésére válaszul – kialakította többközpontú, csomagkapcsolt hálózati kommunikációs rendszerét, amely stabil tudományos háttérrel teremtett a TCP/IP¹ szabványnak. (A TCP protokollról szóló, 1974-ben megjelent tanulmányban jelenik meg először az internet kifejezés.) Elmondható, hogy az internet a számítógépek olyan szerveződése, amelyben bármelyik kapcsolt elem képes interakcióba lépni bármelyik másik kapcsolt elemmel.

A következő mérföldkőhöz 1989-ben érkeztünk, amikor Tim Berners-Lee, a CERN² kutatója kidolgozta a web alapelveit. Célja egy globális információs hálózat létrehozása volt a kutatók közötti automatizált információmegosztás érdekében. A CERN 1993. április 30-án a világhálót szabadon elérhetővé tette mindenki számára.³

Az eredetileg nem a nagyközönségnek szánt hálózat viharos sebességgel vált a kommunikáció és az információtovábbítás megkerülhetetlen eszközévé, ami nap mint nap rávilágít az információáramlás új és újabb, eddig ismeretlen lehetőségeire.

Rengetegféle adat létezik, például előzményi adatok, de ismerjük a közösségimédia-alkalmazásokból származó új adatokat, a webalkalmazások kattintási adatait is. Az adatok mennyisége nagyobb, mint valaha, folyamatosan növekvő sebességgel és sokféle formátumban érkeznek. A globális adatszférában az elérhető adatok száma a következő évek során exponenciálisan növekedni fog, és mérete 2025-re az Statista Research Department⁴ prognózisa szerint eléri a 181 zettabyte⁵ mennyiséget.

2. Az információ mint extra tudás

Ez a már-már mérhetetlen adatmennyiség lehetőséget biztosít a virtuális tér szereplőinek – így a nemzetbiztonságáért felelős szerveknek is –, hogy minden olyan információt megismerjenek, megszerezzenek, amely a céljaik szempontjából fontos. Az ezen adatokban rejlő információk kinyerése érdekében megkerülhetetlenek a korszerű technológiai

¹ *Transmission Control Protocol/Internet Protocol*, átviteli vezérlő protokoll/internetprotokoll.

² *Conseil Européen pour la Recherche Nucléaire* (CERN), Nukleáris Kutatások Európai Tanácsa.

³ *The birth of the Web*. CERN, 2022.

⁴ Qlik: *Build trust and drive usage of your data and analytics*. Qlik.com.

⁵ 1 zettabyte = 10^{21} byte.

újdonságok, mint például a mesterséges intelligencia vagy akár a *big data* kezelésében rejülő lehetőségek. De mit is takarnak ezek a fogalmak, amelyeket nap mint nap használunk?

Társadalomtudományi megközelítésből a *big data* az információk, adatok ugrásszerű növekedése miatt bekövetkezett új társadalmi rutinok és megismerési módok együttese, azaz a mennyiségi változás – az adatok növekedése – minőségi változást generál.⁶ Ez azt jelenti, hogy az általunk hagyott „digitális lábnyom” adatait felhasználva az életvitelünket befolyásoló, az információ hasznosulását segítő, a megjelölt és elérni kívánt céloknak megfelelő módosító ingerek érnek mindannyiunkat. A *big data* a természeti és társadalmi folyamatok korábban elképzelhetetlen kiterjedésű és komplexitású modellezését teszi lehetővé.⁷

A *big data* olyan adathalmaz, amely mind méretében, mind képességeit tekintve meghaladja a hagyományosnak nevezett relációs⁸ adatbázisokat. A *big data* fő jellemzői: a nagy kiterjedés, a nagy sebesség és a diverzitás. Az adatforrások oldaláról tekintve a *big data* forrásai összetettek, mert azokat többek között a mobil eszközök, a közösségi média és a tárgyak internete alkotja. Az adatok jelentős része valós időben és gigantikus mennyiségben jön létre, a különböző típusú adatok különböző forrásokból, úgymint: szenzorokból, eszközökből, videókból/hangfájlokból, hálózatokból, naplófájlokból, tranzakciós alkalmazásokból és a közösségi médiából.

A *big data* fő nyeresége nem a mérhetetlen mennyiségű, sebességű és kiterjedésű „adatcunami”, hanem az ezekből kinyerhető érték, az adatok feldolgozása, strukturálása és kezelése következtében előkerülő pluszmondanivaló, amely gyorsabb, többforrású és különböző formátumokból, architektúrákból kinyert extra tartalom. Ezek alapján kijelenthető, hogy a *big data* valódi értékét nem az azt alkotó adatok képviselik, hanem az azokból kinyert információtöbblet. Ugyanakkor ezen extra tudás nemzetbiztonsági alkalmazása során fokozott figyelmet kell fordítani a megfelelő szintű és minőségű humán kontrollra és auditra. Ezenfelül a *big data* nemzetbiztonsági célú felhasználásakor nagy fokú óvatossággal kell tekintenünk az adatok torzulásából fakadó anomáliák lehetőségeinek kiküszöbölésére, illetőleg az emberi és a személyiségi jogokkal⁹ kapcsolatos kérdéskörre. A fentebb jelzett dilemmákat tovább árnyalja, hogy a plusztudáshoz hozzásegítő technológiai háttér biztosítása és annak bevezetése bonyolult, nagy informatikai tudást igényel és drága. Ezzel a problémakörrel a jövőben mindenképpen foglalkozni kell, hiszen a fejlődés gátja, ezáltal a biztonsági deficit oka nem lehet anyagi megfontolású. Az egységes nemzeti fellépés, a meglévő tudás összeadása segítheti a hatékonyságot és a kiadások csökkentését.

Az információk hatékony kinyerése érdekében fontos segítségül hívni a metodikai, technológiai és technikai újdonságokat, mint például a mesterséges intelligencia nyújtotta

⁶ Dessewffy Tibor – Láng László: Big Data és a társadalomtudományok véletlen találkozása a műtőasztalon. *Replika*, (2015), 92–93. 157–170.

⁷ Csepeli György: A szociológia és a Big Data. *Replika*, (2015), 92–93. 171–176.

⁸ A relációs adatbázis táblázatszerkezetbe rendezett adatgyűjtemény.

⁹ A problémakörrel rendszeresen foglalkozik az ENSZ Emberjogi Főbiztos Hivatala, lásd bővebben az A/75/147, az A/HRC/40/63 és az A/73/438 számú jelentést.

lehetőségeket. Ezen potenciálok kihasználása során ugyanakkor fel kell ismernünk azokat a veszélyforrásokat, amelyek a mesterséges intelligenciához kapcsolódó vívmányok alkalmazásából fakadnak, a meglévő társadalmi normáinkra, értékeinkre nézve.¹⁰ Ahhoz, hogy a mesterséges intelligenciában rejlő lehetőségek kiaknázhatóak legyenek, három döntő elemre van szükség: jól definiált problémára, adatokra és meghatározott modellre, amely megfogalmazza a szükségleteket.

A mesterséges intelligencia hangsúlyozott területei közül mindenképpen említést érdemel a gépi tanulás, a neurális hálók, illetőleg a prediktív analízis.

A neurális hálózat programozási technika, gondolkodási módszer, amely napjainkban közismert módszere a mesterséges intelligenciának. A konvencionális programozási szemlélettel szemben, ahol az elérni kívánt cél érdekében szükséges minden részletről az ember hoz döntéseket, a struktúra veszi át ezt a szerepet.

A gépi tanulás olyan alkalmazások fejlesztésére összpontosít, amelyek tanulnak az adatokból, és idővel javítják azok pontosságát anélkül, hogy erre be lennének programozva. Az adattudományban az algoritmus a statisztikai feldolgozási lépések sorrendje. A gépi tanulás során az algoritmusokat arra készítik fel, hogy hatalmas mennyiségű adatban találjanak mintákat és jellegzetességeket annak érdekében, hogy az így megismert új adatok alapján hozzanak döntéseket és fogalmazzanak meg előrejelzéseket. Minél jobb az algoritmus, annál pontosabbak lesznek a döntések és az előrejelzések.

A prediktív elemzés olyan fejlett analitikai technikák együttes használata, amelyek a megszerzett és eltárolt adatokat felhasználják a valós idejű összefüggések feltárására és a jövőbeli történések prognosztizálására. A prediktív elemzés alkalmazása jelentős fordulópont az adatok feldolgozása során, mivel itt találkozunk a klasszikus statisztikai analízis a mesterséges intelligencia által biztosított új lehetőségekkel.

A fentiekből kifolyólag a biztonsági területen dolgozók számára szükséges és elkerülhetetlen, hogy ezen tevékenységeknek, folyamatoknak, jelenségeknek aktív részei legyenek abból a célból, hogy felismerjék azokat a potenciálokat, amelyek alkalmazásával a biztonsági környezet minősége növelhető. Prioritást kell hogy élvezzen a nemzetbiztonsági szakemberek és az informatikai innovációs szakértők napi szintű kapcsolata a felmerülő problémák és a meglévő megoldási lehetőségek minél gyorsabb találkozásának érdekében. Ezt támasztja alá az is, hogy az USA Védelmi Minisztériuma mesterségesintelligencia-stratégiájában megfogalmazta a tudományos, kereskedelmi és nemzetközi szövetségesekkel és partnerekkel való szoros együttműködés szükségességét.¹¹

¹⁰ Négyesi Imre: A mesterséges intelligencia és az etika. *Hadtudomány*, 30. (2020), 1.

¹¹ Department of Defense USA: *Summary of the 2018 Department of Defense's Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity* (2019. február 12.).

3. Állami szerepvállalás, avagy a nemzetbiztonság és az új lehetőségek

Az üzleti élet szereplői versenyképességük megőrzése érdekében már szinte rutinszerűen alkalmazzák a különböző adatkötegek vizsgálatának eredményeként megismert mintákra, szokásokra és beállítottságra vonatkozó információkat. Az ezzel együtt járó útkeresések, az adatfeldolgozási tevékenység, az adatok felhasználásai az elmúlt évtizedekben több alkalommal okoztak felháborodást.¹²

Az ország védelméért felelős szervezetek szempontjából sem megkerülhetők ezek a kérdések, ugyanakkor a társadalom és a biztonsági szervek „békés együttélésének” megőrzése érdekében megfelelő érzékenységgel kell a problémát megközelíteni. Törekedni kell arra, hogy az ilyen típusú nemzetbiztonsági tevékenységekkel kapcsolatban is a lehető legnagyobb legyen a társadalmi elfogadottság. A fejlett informatikai eszközök és módszerek igénybevételével lehetőség nyílt olyan metódusok kidolgozására, amelyek segítségével a személytelenített adatok feldolgozásával, profilok felállításával konkrét biztonsági helyzetek előrejelzése válik lehetővé.

Az állami hatalom gyakorlói, különösen ott, ahol a kutatási-fejlesztési területek kimagaslóak, törekednek a technikai újdonságok és lehetőségek saját szektorukba való beteretelésére. Ezt az állami biztonsági szférában is megjelenő és egyre nagyobb szerepet követelő digitális adatok megnövekedett száma és az így kialakuló adathalmazok is megkövetelik.

Az jól látszik, hogy a mesterséges intelligencia alkalmazása az elkövetkező években, évtizedekben elkerülhetetlen lesz, ugyanakkor használata rengeteg etikai, morális, gazdasági és biztonsági kérdést, problémát vet fel, amelyre a kormányzatoknak valamilyen választ kell adniuk. A kormányzati szervek törekszenek a fenti kérdésköröket – igaz, egyelőre csak alapelvi, irányelvi és stratégiai szinten – megválaszolni.

Az Amerikai Egyesült Államokban a Fehér Ház kiadott 10 alapelvet az állami ügynökségek számára, amelyeket azoknak be kell tartaniuk, amikor új, a magánszektor érintő mesterségesintelligencia-rendeleteket javasolnak.¹³ 2019-ben elnöki rendelet¹⁴ aláírásával indították el az USA mesterséges intelligenciára vonatkozó stratégiai elképzeléseit. A dokumentum kiemeli az amerikai gazdasági és nemzetbiztonsági érdekek megőrzésének, megerősítésének fontosságát a mesterséges intelligencia területén a nemzeti értékekkel és prioritásokkal összhangban.

¹² Glenn Greenwald: *A Snowden-ügy*. Budapest, HVG Könyvek, 2014.; a Cambridge Analytica-botrányhoz lásd Cadwalladr, Carol – Emma Graham-Harris: *Revealed: 50 Million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach*. *The Guardian*, 2018. március 17.; a NameTests.com-kvízekhez lásd: Natasha Lomas: *Yet Another Massive Facebook Fail: Quiz App Leaked Data on ~120M Users For years*. *TechCrunch*, 2018. június 28.

¹³ Russell T. Vought: *Memorandum for the Heads of Executive Departments and Agencies. Guidance for Regulation of Artificial Intelligence Applications*. The White House, 2020.

¹⁴ Executive Office of the President: *Maintaining American Leadership in Artificial Intelligence*. Executive Order 13859 of Feb 11, 2019 (2019. február 14.).

Az Oroszországi Föderáció elnöki hivatala 2019-ben kiadta nemzeti mesterséges-intelligencia-stratégiáját¹⁵ és az annak fejlesztéséről szóló elnöki rendeletet. A stratégia tartalmazza a mesterséges intelligencia fejlesztésének céljait és azon elsődleges célkitűzéseket, amelyeket 2024–2030 között el kell érni, valamint megjeleníti az alábbi alapelveket is: az emberi jogok és szabadságjogok védelme, biztonság, átláthatóság, technológiai szuverenitás és a verseny támogatása.

Kína úgy véli, hogy a globális gazdasági és katonai élmezőnyhöz való tartozás elképzelhetetlen a mesterséges intelligencia területén való kiemelkedő teljesítmény nélkül. Ennek biztosítása érdekében a 2015-ben kiadott *Made in China 2025*¹⁶ program és a 2017-ben megjelent, új generációs mesterséges intelligenciára vonatkozó fejlesztési terv¹⁷ képezi Kína mesterségesintelligencia-stratégiáját. Ezen dokumentumokon keresztül Kína vezetése hangot ad azon elképzelésének, hogy a mesterséges intelligencia fejlesztését a versenyképesség növelése és a nemzetbiztonság védelme szempontjából kiemelten fontosnak tekinti.

Az Európai Bizottság is folyamatosan napirenden tartja mesterséges intelligenciára vonatkozó orientációját. A bizottság mesterséges intelligenciával kapcsolatos közleményében kiemeli, hogy az ott elért eredményeket a polgárok szolgálatába kell állítani, ugyanakkor foglalkozni kell az ehhez kapcsolódó technológiai, etikai, jogi és társadalmi kérdésekkel is, ezzel garantálva az európai értékek tiszteletben tartását.¹⁸ A fenti gondolatok támogatása és a mesterséges intelligencia terjedésének elősegítése érdekében 2020. február 19-én az Európai Bizottság fehér könyvet¹⁹ adott ki, amelyben vázolja a szakpolitikai lehetőségeket.

Az Európai Unió tagjai állami szinten is törekednek a mesterséges intelligenciát, valamint annak fejlesztését, fejlődését keretrendszerbe foglalni.²⁰ A kormányzatok felismerték, hogy a gazdasági potenciálok maximális kihasználása érdekében elengedhetetlen a tudatos és irányított együttműködésre való törekvés az állami, gazdasági, tudományos és társadalmi szereplők között.

Magyarország Kormánya 2020 májusában adta ki a *Magyarország Mesterséges Intelligencia Stratégiája 2020–2030*²¹ címet viselő dokumentumot, amely 2030-ig szóló célokat jelöl ki, és egyben 2025-ig tartó intézkedési tervet vázol fel, annak szem előtt tartásával, hogy a technológia gyors fejlődése okán azt két évente felül kell vizsgálni.

A stratégia három fő szintre osztható. Az első rész, azaz az alapszint a széles társadalmi rétegek számára szóló, a mesterséges intelligenciát ismertető, tudatosító gondo-

¹⁵ Указ Президента РФ от 10 октября 2019 г. № 490 „О развитии искусственного интеллекта в Российской Федерации”. *garant.ru*, 2019. október 14.

¹⁶ State Council: *Made in China 2025*《中国制造 2025》. IoT One, 2015. július 7.

¹⁷ The State Council The People’s Republic Of China: □□□□□□ □□□□□□□□□□□□□□□□. *Gov.cn*.

¹⁸ European Commission: *A European Approach to Artificial Intelligence* (é. n.).

¹⁹ European Commission: *White Paper On Artificial Intelligence—A European Approach to Excellence and Trust*. COM(2020) 65 final (2020. február 19.)

²⁰ Négyesi Imre: A mesterséges intelligencia katonai felhasználásának társadalmi kérdései. *Honvédségi Szemle*, 149. (2021), 1. 133–145.

²¹ *Magyarország Mesterséges Intelligencia Stratégiája 2020–2030*. Innovációs és Technológiai Minisztérium – MI Koalíció, Digitális Jólét Program, 2020. május.

latokat tartalmazza. A második szint a technológiafejlesztésről szól, amely elsősorban a tudományos terület művelőinek releváns. A fejezet bemutatja, hogy milyen algoritmusok, technológiák és eszközök, megoldások vannak jelen a piacon, továbbá ezek alkalmazhatóságának módszereit is ismerteti a dokumentum, a kutatásra és a fejlesztésre fókuszálva. A harmadik rész az alkalmazás, gyakorlati felhasználás lehetőségeit taglalja.²² Az alkalmazás terén elsődleges a várható hozzáadott érték meghatározása egy probléma megoldása kapcsán, másrésztől viszont nélkülözhetetlen először a mesterséges intelligencia segítségével megoldandó konkrét, gyakorlati probléma megfogalmazása.

Megállapítható, hogy a mesterséges intelligencia alkalmazása az országok, kiemelten a nagyhatalmak számára kulcsfontosságú és a magas prioritású ügyek között szerepel, mind politikai, mind gazdasági, mind pedig biztonsági aspektusból. Ahogy Vlagyimir Putyin orosz elnök mondta: „*A mesterséges intelligencia nemcsak Oroszország, hanem az egész emberiség jövője. Óriási lehetőségek vannak, de olyan fenyegetések is, amelyeket ma nehéz előre látni. Aki e téren vezetővé válik, az a világ uralkodója lesz.*”²³

A nemzet biztonságáért felelős biztonsági szervek számára kiemelt feladatnak kell lennie a fentebb taglalt területeken napról napra bekövetkező fejlődés folyamatos monitorozásának annak érdekében, hogy minél hatékonyabban beazonosíthatóak legyenek azok az újdonságok és lehetőségek, amelyek eredményesen támogathatják munkájukat és alkalmasak a meglévő rendszereikbe való biztonságos integrációra.

4. A jövő

Kijelenthetjük, hogy az információs társadalomban beálló változások előidézője, kiindulópontja az információs technológia robbanásszerű fejlődése. Ezzel egy időben a társadalmi normákban, kapcsolatrendszerekben, valamint az emberi értékrendekben beállt és folyamatban lévő változások is tovább árnyalják a képet.

Napjainkban kiemelt jelentőségű a jövő minél pontosabb és biztosabb ismerete, ehhez hozzájárulnak a kommunikációs és információs technológia területein bekövetkező nagy léptékű és viharos gyorsaságú változások, innovációk. Tudnunk kell, milyen megmértetéssel állunk szemben az infokommunikációs technológiák, a működésüket biztosító hálózatok és nem utolsósorban a globalizáció állította helyzetek vonatkozásában, és ezeknek melyek a nemzetbiztonsági aspektusai.

Az infokommunikációs technológiai eszközök és rendszerek terjedésével napjainkban a biztonsági szektorban is kiemelt szerepet kapnak a digitális úton létrejött és megosztott elemek. Ezen terület folyamatosan fejlődik, már létező kommunikációs és információs zónákat integrál, illetve a mindennapi élet új területeire kínál technikai megoldásokat.²⁴ Az így létrejövő adatok és információk kinyerésére az elmúlt néhány évben új, mondhatni

²² Kiemelt területként említi meg a stratégia az egészségügyet, a mezőgazdaságot és az államigazgatást.

²³ CNN: *Who Vladimir Putin Thinks Will Rule the World*. *Edition.cnn.com*.

²⁴ Ilyenek például a teljes körű online gépjárművédelmi rendszerek működését biztosító szisztémák, amelyek már jóval túlmutatnak a „puszta” vagyónvédelmen.

korszakalkotó szféra alakult ki, amely nemzetbiztonsági relevanciákkal is rendelkezik. A biztonsági ágazatban jelenleg igen szűk körűek a tapasztalati értékek, amelyek a jövőben megkerülhetetlenek. Így elsődleges szempont, hogy a nemzetbiztonságért felelős szervezetek az adatgazdálkodási, informatikai és technológiai területen bekövetkezett változások közül kiszűrjék a számukra hasznosítható módszereket, gondoskodjanak azok integrációjáról, esetleges fejlesztéséről.

Összefoglalás, következtetések

Összegzésként megállapítható, hogy az információt és az azzal való gazdálkodásról való gondolkodást egyik tudományág képviselői sem sajátíthatják ki maguknak. Az elért eredmények mihamarabb és minél szélesebb körben történő megosztása jelentős energia-többlettel láthatja el a többi kutatót, ezzel további tudományos eredményeket generálva.

A tudományos együttműködésen túl hangsúlyt kell fektetni a gazdasági, ipari és állami szereplők közötti kooperációra, hiszen ez jelentős indikátora lehet az új technológiák és lehetőségek közös felhasználásának. Ezen együttműködés során a kormányzatoknak biztosítani kell – a szükséges irányvonalak kijelölésével – a megfelelő szintű és hatékonyságú állami kontrollt. Megállapítható, hogy a jelenlegi alapelvi, stratégiai irányítási helyzetből a jövőben el kell mozdulniuk a kormányzatoknak, és gondoskodniuk kell a megfelelő jogszabályi hátterek biztosításáról.

A nemzetbiztonsági szerveknek folyamatosan keresniük kell – a feladatok ellátásának színvonalának fokozása és a fejlődésből fakadó kihívások kezelése érdekében – azokat az alternatívákat, amelyek alkalmasak a biztonsági területekhez kapcsolódó újdonságok bevezetésére. Ezzel párhuzamosan a biztonsági szerveknek nyomatékosan figyelemmel kell kísérniük az információk feldolgozását segítő technológiai vívmányokkal kapcsolatos fejlesztéseikhez fűződő társadalmi reakciókat, a manapság oly népszerű és hangoztatott digitális diktatúra árnyékának elkerülésének érdekében.

Úgy gondolom, hogy végkövetkeztetésként megállapítható, hogy a sikeres jövő csak együtt gondolkodással, együttes fellépéssel és együttműködéssel garantálható, ahogy Vinton Gray Cerf²⁵ mondta: „A mai napi bölcs mondásom nem az lesz, hogy az információ hatalom, hanem az, hogy az információ megosztása hatalom.”

Felhasznált irodalom

- Cadwalladr, Carol – Emma Graham-Harris: Revealed: 50 million Facebook Profiles Harvested for Cambridge Analytica in Major Data Breach. *The Guardian*, 2018. március 17. Online: www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
- Csepeli György: A szociológia és a Big Data. *Replika*, (2015), 92–93. 171–176. Online: www.replika.hu/replika/92-93-12

²⁵ Amerikai matematikus, informatikus, akinek vezető szerepe volt az internet és a TCP/IP készlet megalkotásában.

- Dessewffy Tibor – Láng László: Big Data és a társadalomtudományok véletlen találkozása a műtőasztalon. *Replika*, (2015), 92–93. 157–170. Online: www.replika.hu/replika/92-93-11
- Greenwald, Glenn: *A Snowden-ügy*. Budapest, HVG Könyvek, 2014.
- Négyesi Imre: A mesterséges intelligencia katonai felhasználásának társadalmi kérdései. *Honvédségi Szemle*, 149. (2021), 1. 133–145. Online: <http://doi.org/10.35926/HSZ.2021.1.10>
- Négyesi Imre: A mesterséges intelligencia és az etika. *Hadtudomány*, 30. (2020), 1. 103–113. Online: <http://doi.org/10.17047/HADTUD.2020.30.1.103>

Internetes források

- CNN: Who Vladimir Putin thinks will rule the world. *Edition.cnn.com*. Online: <https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>
- Qlik: Build trust and drive usage of your data and analytics. *Qlik.com*. Online: www.nodegraph.se/how-much-data-is-on-the-internet/
- The State Council The People's Republic Of China: 国务院关于印发 新一代人工智能发展规划的通知. *Gov.cn*. Online: www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm
- United Nations: *Annual Thematic Reports. Special Rapporteur on the Right to Privacy* (é. n.). Online: www.ohchr.org/EN/Issues/Privacy/SR/Pages/AnnualReports.aspx
- Volume of data/information created, captured, copied, and consumed worldwide from 2010 to 2020, with forecasts from 2021 to 2025*. Online: www.statista.com/statistics/871513/worldwide-data-created
- Online: www.gov.cn/zhengce/content/2017-07/20/content_5211996.htm
- European Commission: *A European Approach to Artificial Intelligence* (é. n.). Online: <https://ec.europa.eu/digital-single-market/en/artificial-intelligence#Coordinated-EU-Plan-on-Artificial>
- State Council: *Made in China 2025* 《中国制造 2025》. IoT One, 2015. július 7. Online: www.cittadellascienza.it/cina/wp-content/uploads/2017/02/IoT-ONE-Made-in-China-2025.pdf
- The birth of the Web. *CERN*, 2022. Online: <https://home.cern/science/computing/birth-web>
- Online: <https://edition.cnn.com/2017/09/01/world/putin-artificial-intelligence-will-rule-world/index.html>
- Lomas, Natasha: Yet Another Massive Facebook Fail: Quiz App Leaked Data on ~120M Users For years. *TechCrunch*, 2018. június 28. Online: <https://techcrunch.com/2018/06/28/facepalm-2/>
- Magyarország Mesterséges Intelligencia Stratégiája 2020–2030. Innovációs és Technológiai Minisztérium – MI Koalíció, Digitális Jólét Program, 2020. május. Online: <https://digitalis-joletprogram.hu/files/2f/32/2f32f239878a4559b6541e46277d6e88.pdf>
- Vought, Russell T.: *Memorandum for the Heads of Executive Departments and Agencies. Guidance for Regulation of Artificial Intelligence Applications*. The White House, 2020. Online: www.whitehouse.gov/wp-content/uploads/2020/01/Draft-OMB-Memo-on-Regulation-of-AI-1-7-19.pdf

Jogforrások

- Department of Defense USA: *Summary of the 2018 Department of Defense's Artificial Intelligence Strategy. Harnessing AI to Advance Our Security and Prosperity*. (2019. február 12.). Online: <https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/Summary-of-DoD-ai-Strategy.pdf>

European Commission: White Paper On Artificial Intelligence—A European Approach to Excellence and Trust. COM(2020) 65 final (2020. február 19.) Online: https://ec.europa.eu/info/sites/info/files/commission-white-paper-artificial-intelligence-feb2020_en.pdf

Executive Office of the President: *Maintaining American Leadership in Artificial Intelligence.* Executive Order 13859 of Feb 11, 2019 (2019. február 14.). Online: www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence

Указ Президента РФ от 10 октября 2019 г. № 490 "О развитии искусственного интеллекта в Российской Федерации". *гарант.ру*, 2019. октóбер 14. Online: www.garant.ru/products/ipo/prime/doc/72738946/