ERDÉSZ VIKTOR

A MESTERSÉGES INTELLIGENCIA ALKALMAZÁSA A KATONAI NEMZETBIZTONSÁGI HÍRSZERZÉSBEN

DR. ERDÉSZ VIKTOR

A MESTERSÉGES INTELLIGENCIA ALKALMAZÁSA A KATONAI NEMZETBIZTONSÁGI HÍRSZERZÉSBEN

Katonai Nemzetbiztonsági Szolgálat

Budapest, 2023.

A MESTERSÉGES INTELLIGENCIA ALKALMAZÁSA A KATONAI NEMZETBIZTONSÁGI HÍRSZERZÉSBEN

Szerző:
Dr. Erdész Viktor százados, PhD
egyetemi tanársegéd

Lektor:
Dr. Vida Csaba ezredes, PhD
egyetemi docens

Olvasószerkesztő:
Gál Csaba ny. ezredes

Tördelőszerkesztő:
Tóth Krisztina törzszászlós

A borító tervezője:
Perényi Attila

Felelős kiadó:
Dr. Béres János altábornagy, főigazgató
Katonai Nemzetbiztonsági Szolgálat

A kiadó képviselője:
Dr. Kenedli Tamás ezredes
Katonai Nemzetbiztonsági Szolgálat
Tudományos Tanács titkár

A kiadvány a Katonai Nemzetbiztonsági Szolgálat
Költségvetési Kutatóhely támogatásával készült.

ISBN 978-615-6128-15-7

Nyomdai kivitelező:
HM Zrínyi Geoinformációs és Toborzástámogató Közhasznú Nonprofit Kft.

TARTALOMJEGYZÉK

SZAKMAI ELŐSZÓ

Tisztelt Olvasó!

Örömmel ajánlom *A mesterséges intelligencia alkalmazása a katonai nemzetbiztonsági hírszerzésben* című könyvet minden érdeklődő számára. A szerző hiánypótló művet helyezett az olvasó asztalára, hiszen a témában eddig zömében az információtudomány képviselői jelentettek meg tudományos publikációkat. Az ő munkásságuknak köszönhetően jutottunk el oda, hogy – szilárd technikai alapokon állva – elmozdulhattunk a mesterséges intelligencia stratégiai hírszerzési alkalmazhatóságának vizsgálata felé.

A mű erénye, hogy a nemzetbiztonsági hírszerzést holisztikus egységként kezeli, amelynek küldetése, hagyományai és világos céljai vannak. A fejlődés lehetőségeit ennek szellemében tekinti át a hírszerzés önálló ágaiban és az elemzés-értékelésben, majd megfontolandó ajánlásokat tesz e témákban. Mindezen kérdéskörökben nemzetközi kitekintést nyújt és jól áttekinthetően kivonatolja a jelenlegi technikai lehetőségeket. Mindemellett a mesterséges intelligencia jelenségének általános vizsgálata olyan összefoglalót eredményezett, amelynek ismerete hasznos mindenki számára, aki világunk fontos kérdései iránt érdeklődik.

A mesterséges intelligencia fejlődése napjaink egyik legjelentősebb technológiai és társadalmi jelensége, amelynek vizsgálata, illetve az MI-technológiák alkalmazása a nemzetbiztonsági rendszer számára is nélkülözhetetlenné vált. Az MI adta lehetőségek mély megismerése és kiaknázása olyan terület, ahol a későn lépők és a lemaradók irrelevánssá válnak az egyre éleződő nemzetközi versenyben. A kihívás komplexitása megköveteli a már bevált megoldások felmérését és alkalmazását, valamint a közös gondolkodást nemcsak a nemzetbiztonsági rendszeren belül, hanem a terület kutatóival és szakértőivel is. A nemzetbiztonsági rendszer előtt álló kihívások ismeretében bátran állíthatom, hogy ez a hírszerzők jelenlegi generációjának legfontosabb feladata.

A könyv fontos kiindulópont a nemzetbiztonsági hírszerzés MI-alapúvá tételében. A további kutatások szükségességét aligha kell hangsúlyozni egy olyan dinamikusan változó területen, mint az MI világa, hiszen a kézirat lezárása óta is olyan változásoknak voltunk tanúi – különös tekintettel a generatív mesterséges intelligencia térhódítására –, amelyek bár nem írják felül a szerző által megismertetett alapgondolatokat, mindenképpen új lehetőségeket teremtettek. Ettől függetlenül is valamennyi, a könyvben érintett területen – különösen a hírszerzés önálló ágai és az elemzés-értékelés, valamint a hírszerzés szervezetelméleti vonatkozásai tekintetében – további kutatások szükségesek annak érdekében, hogy a megfogalmazott célok és lehetőségek minél teljesebb mértékben átültethetők legyenek a mindennapi hírszerző munkába.

Bízom benne, hogy a könyv áttanulmányozása még többeket döbbent rá a mesterséges intelligencia fejlődésének jelentőségére, különösen a védelmi szektor döntéshozói és szakértői körében. Meggyőződésem, hogy a műben foglaltak – ha nem is tervrajzul, de – iránytűül szolgálnak a gyakorlati fejlesztések számára is.

Börcsök András ezredes
Katonai Nemzetbiztonsági Szolgálat
igazgató

BEVEZETÉS

A hidegháború lezárultával a nyugati országok nemzetbiztonsági szolgálatai a védelmi szektort érintő általános forráskivonás[1] következtében egyre súlyosbodó emberi erőforráshiánnyal voltak kénytelenek szembenézni. A Szovjetunió széthullásával a Nyugat átmenetileg elvesztette a korábbi, jól meghatározott ellenségképét, a ’90-es években újonnan felmerült, aszimmetrikus kihívások pedig nem jelentettek egzisztenciális fenyegetést. Bár a nemzetközi válságok kezelése új kihívásokat jelentett, de azokhoz új forrásokat nem rendeltek. A folyamattal párhuzamosan kibontakozó információs forradalom paradox módon tovább növelte a szolgálatok leterheltségét, mert az információéhség korszakából rövid idő alatt kellett volna adaptálódniuk az információ túlzott bőségéhez.

Az évtizedes status quóban nem okoztak jelentőst változásokat az olyan békeműveletek, mint a NATO beavatkozása a délszláv háborúkba, vagy az ENSZ keretében megkísérelt 1993–1995-ös szomáliai válságkezelés. A béketámogató műveletek számának hidegháború utáni ugrásszerű növekedése új kihívásokat jelentett ugyan a nyugati haderők és a nemzetbiztonsági szolgálatok számára, de a politikai felső vezetők nem érzékeltek olyan fenyegetést, amely érdemben akár csak lassíthatta volna a forráskivonást, a nemzetbiztonsági szolgálatok vezetői pedig kisebb fejlesztéseket is elégségesnek tartottak annak érdekében, hogy megfeleljenek az új kihívásoknak.

Paradigmaváltást az al-Kaida terrorszervezet 2001. szeptember 11-ei amerikai terrortámadásai jelentettek, amelyeket követően a szolgálatok először az Amerikai Egyesült Államokban, majd a nyugati szövetségi rendszer más államaiban kezdhettek meg új fejlesztéseket. A „terror elleni harc” nem fordította meg ugyan a feladatokhoz képest elégtelen költségvetések trendjét, de a hidegháború vége óta eltelt időszakban első alkalommal jelent meg egy új, dinamikusan fejlődő részterület a nemzetbiztonsági szektoron belül.

Először az amerikai szolgálatok ismerték fel, hogy az al-Kaida sikerét nem az elégtelen mennyiségben rendelkezésre álló információ, hanem éppen a túlzott mértékben beáramló információ feldolgozatlansága tette lehetővé.[2,3] Ezért a terror elleni harcot nem kizárólag új munkatársak felvételével, hanem új, az információfeldolgozás automatizálását segítő, akkor forradalminak számító, részben

[1] The Cost of Intelligence. Federation Of American Scientists, 1996.02.23. https://fas.org/irp/offdocs/int017.html; letöltés: 2018.12.03.

[2] TRAVERS, Russ: A Blueprint For Survival: The Coming Intelligence Failure. Studies in Intelligence, 1997. pp. 35–43. https://www.cia.gov/static/coming-intelligence-failure.pdf; letöltés: 2018.12.03.

[3] KRUYS, George P. H.: Intelligence failures: causes and contemporary case studies. Strategic Review for Southern Africa, Volume 28, Issue 1, 2006. pp. 63–96. https://repository.up.ac.za/bitstream/handle/2263/3078/Kruys_Intelligence(2006).pdf?sequence=1; letöltés: 2018.12.03.

már mesterséges intelligencián[4] (MI) alapuló informatikai eszközök fejlesztésével és beszerzésével látták megvívhatónak. Az ebben az időszakban rendszeresített adatbányász, fordító-, arcképfelismerő, adminisztrációs stb. programok utódjai a fejlett szolgálatoknál már a mindennapi munkavégzés nélkülözhetetlen kellékei.[5] A 2002-es afganisztáni, illetve a 2003-as iraki inváziók a távoli, ismeretlen hadszíntereken végrehajtott nagyszabású hadműveletek és a különleges műveleti erők felderítőbiztosításának és hírszerző támogatásának fejlesztését is szükségessé tették. Az új hadszínterekre telepített nemzetbiztonsági munkatársak és a műveletek honi területekről történő támogatása újabb emberi erőforráskrízist okozott a szolgálatok számára,[6] aláhúzva a technológiai fejlesztések és a szervezeti változtatások szükségességét. A hadszínterekről, válságkörzetekről és az internetről beözönlő adatmennyiség feldolgozása a hagyományos információfeldolgozó, ezen belül elemző-értékelő módszerekkel ellehetetlenült.

A folyamatot az aszimmetrikus hadviselés és a terror elleni harc jelentette kihívások mellé belépő egyéb transznacionális fenyegetések megjelenése, elsősorban a tömegpusztító fegyverek proliferációja és a kibertéri fenyegetések megjelenése mélyítette el. A transznacionális fenyegetések körének kitárulásával párhuzamosan, lényegében Oroszország 2008. augusztusi grúziai katonai intervenciójától kezdődően, illetve – elsősorban az Amerikai Egyesült Államok számára – Kína felemelkedésével egyre gyorsuló ütemben jelentek meg ismét a hagyományos katonai és nemzetbiztonsági kihívások. A régi és az új kihívások, illetve fenyegetések párhuzamos létezésére, sőt egymást erősítő jellegére az „arab tavasz", de különösen a szíriai polgárháború, az ISIL/DAESH[7] terrorszervezet megjelenése, a szíriai–iraki „Kalifátusának" a létrehozása és a nyugati célpontokat támadó külföldi terrorista harcosok megjelenése,[8,9] a tömeges illegális migrációs válság, majd a Krím félsziget elcsatolása és az orosz–ukrán háború figyelmeztet. A folyamatosan bővülő és egyre súlyosbodó válságok az erőforrások szinte napi szintű újracsoportosítását követelik meg a nemzetbiztonsági szolgálatoktól is, lehetetlenné téve a hosszú távú prioritások meghatározását és azok tartását. Ilyen körülmények között a szolgálatok munkatársai számára lehetetlen a korábban megszokott szintű elmélyülés a szakterületeiken, a feladatok végrehajtásának rendje a menedzserszemlélet és a „projektközpontú" munkavégzés felé tolódik. Nincs remény arra sem, hogy a válságok rendeződésével a belátható jövőben csökkenne a szolgálatok munkaterhelése, inkább a feladatok újabb bővülésével kell számolni.

---

[4] Artificial Intelligence – AI.

[5] TAKÁCS Gergely: Big data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában. Előadás a Kutatók éjszakája rendezvénysorozaton. NKE, Budapest, 2018.09.28.

[6] MILLER, Greg: DIA to send hundreds more spies overseas. The Washington Post, 2012.12.01. https://www.washingtonpost.com/world/national-security/dia-to-send-hundreds-more-spies-overseas/2012/12/01/97463e4e-399b-11e2-b01f-5f55b193f58f_story.html; letöltés: 2018.12.03.

[7] Islamic State of Iraq and the Levant/Islamic State of Iraq and Sham. A DAESH a szervezet arab nevének rövidítése.

[8] BARRETT, Richard – EL-SAID, Hamed: Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria. United Nations Office of Counter-Terrorism, July 2017. https://f-origin.hypotheses.org/wp-content/blogs.dir/2725/files/2018/02/ONU_Report_Final_2017.pdf; letöltés: 2018.11.15.

[9] BYMAN, Daniel: Beyond Iraq and Syria: ISIS' ability to conduct attacks abroad. Brookings, 2017.06.08. https://www.brookings.edu/articles/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad/; letöltés: 2018.11.15.

Az új helyzethez történő adaptálódás a technológiai fejlesztésekben élen járó nyugati országok szolgálatai számára is több évtizedes, teljes mértékben máig sem lezárult reformokat tett szükségessé. A reformok az euroatlanti integrációhoz a vasfüggöny lehullását követően csatlakozott országokban, köztük hazánkban is csak részben, jellemzően integrálatlanul és ad hoc jelleggel valósultak meg. A technológiai lemaradás a titkosszolgálati versenyben fontos előnyöktől zárja el a lemaradókat, ugyanakkor kiaknázatlan lehetőségeket is rejt magában.

Az információs társadalom és a kialakuló multipoláris világrend korszakában a nemzetbiztonsági szolgálatok számára tehát egyre növekvő kihívást jelent, hogy időszerű, releváns, elemzett-értékelt információkkal válaszolják meg a felső vezetés információigényeit, valamint megalapozott előrejelzéseket készítsenek számára.

A fentebb vázlatosan felvázolt kihívásokra a szolgálatok létszámának emelése és az új szemléletű munkavégzés mellett a mesterséges intelligenciára épülő szoftverekben rejlő lehetőségek kihasználása ad működőképes válaszokat. A már említett, kezdetleges, MI-alapú szoftverek mellett a 2010-es évek közepére megjelentek a komplex, fejlett MI-re épülő, a nemzetbiztonsági tevékenységet nagyban támogató rendszerek, amelyek a hírszerzés ágait és az elhárítás tevékenységét a korábbinál összetettebb módon képesek támogatni. Ezen eszközök különös ismertetőjegye, hogy azok képesek a nagy adat[10] („big data”) beszerzésére, feldolgozására, kezelésére és elemzés-értékelésére. Ilyen eszközök birtokában nem csak az információszerzés és -feldolgozás kapacitása növekszik meg számottevően, hanem a nemzetbiztonsági műveletek hatékonysága is. Fontos szempont, hogy a nagyadat-alapú befolyásolási műveletek elhárítása hagyományos eszközökkel rendkívüli kihívást jelent, ezért megfelelő technológia nélkül az államok szuverén döntéshozatali képessége is megkérdőjeleződik.

A korszerű szolgálatoknál a fejlesztések fő irányát a nemzetbiztonsági tevékenység minél szélesebb MI-alapú támogatásának kiépítése jelenti.

A könyv témájának fontossága 2017 áprilisában, a prágai ISSWorld Europe nemzetbiztonsági és rendvédelmi konferencia és vásár megtekintése során lett nyilvánvaló számomra. A rendezvényen betekintést nyerhettem az akkor legkorszerűbb, már a fejlett mesterséges intelligencián alapuló technológiát alkalmazó, a szakemberek munkájának hatékonyságát nagyságrendileg növelő, egyúttal a munkavégzésüket és együttműködésüket nagyban könnyítő szoftverrendszerek világába. Felismertem, hogy e szoftverek a hírszerzés valamennyi önálló ága, illetve az elemző-értékelő szakterület jövőjét, egyben legfontosabb kihívását jelentik.

A kutatás jelentős részben a nemzetbiztonsági rendszer működésére irányult, de kizárólag nyílt információkat használtam fel, és maradéktalanul betartottam a minősített adat védelméről szóló, 2009. évi CLV. törvényben foglaltakat.

[10] Big data: nagyméretű komplex adattömeg és feldolgozása, vagyis olyan adatállományok halmaza, amelyek mérete és komplexitása lehetetlenné teszi a feldolgozást a hagyományos adatbázis-menedzsment eszközeivel.
Mi is az a „Big Data”? Fogalmak, definíciók és egyéb tudnivalók. nagy;adat;blog; 2014.03.03. https://nagyadat.blog.hu/2014/03/03/what-is-big-data; letöltés: 2022.11.15.

A posztmodern társadalmak és a formálódó multipoláris világrend korszakában a nemzetbiztonsági szolgálatok számára egyre növekvő kihívást jelent, hogy időszerű és releváns elemzett-értékelt információkkal válaszolják meg a döntéshozók információigényeit és megalapozott előrejelzéseket készítsenek számukra.

A nemzetbiztonsági rendszernek át kell gondolnia, hogy a változó és egyre kiszámíthatatlanabb biztonsági környezetben hogyan képes megfelelni a döntéshozók elvárásainak. Ebben különös szerep hárul az elemző-értékelő szervezetekre, amelyek a stratégiai nemzetbiztonsági hírszerző szolgálatok központi elemei.

A szolgálatok leterheltségének mérséklésére az együttműködés fokozása, a szervezeti átalakítás, a személyi állomány létszámának bővítése és képzése, illetve a technikai fejlesztés jelenthet megoldást.

A nemzetbiztonsági szolgálatok technikai fejlesztésének legígéretesebb iránya az MI-alapú célszoftverek beszerzése és fejlesztése, jelentős mértékben fokozva ezzel a munkavégzés hatékonyságát. Nehézséget jelent a rendelkezésre álló, a szervezet szempontjából releváns megoldások és azok gyártóinak feltérképezése, a reális elvárások megfogalmazása, ami a beszerzéshez szükséges jelentős források megigénylésének elengedhetetlen feltétele. Figyelembe kell venni az új eszközök rendszeresítésének hatásait a szervezeti struktúrára, a személyi állomány napi munkavégzésére és a képzési rendszerre is. A technikai fejlesztések esetében is fontos az integrált megközelítés, elkerülve a felesleges kiadásokat, a hatékonyságot gátló szigetszerű működést, valamint a biztonságvédelmi problémákat.

A téma feldolgozása során elsősorban közelmúltbeli amerikai tapasztalatokat és megközelítéseket mutattam be, illetve megvizsgáltam a hírszerzés önálló ágait érintő legfontosabb kormányzati és magánszektorbeli fejlesztéseket, megközelítéseket. Az volt a célom, hogy az elméleti ismeretek mellett minél több, a gyakorlati megértést is segítő információt adjak át, ezért olyan magánvállalatokon keresztül mutatom be az új technológiákat, amelyek mindenki számára elérhetően és részletesen ismertetik a termékeik és szolgáltatásaik képességeit. Ennek köszönhetően a könyv áttanulmányozása során mindenki kaphat egy általános képet a jelenleg elérhető technológiákról.

Kéziratomat 2022. november 9-én zártam le.

A MESTERSÉGES INTELLIGENCIA FOGALMA, ALTERÜLETEI, ELTERJEDÉSÉNEK NEMZETI BIZTONSÁGI[11] JELENTŐSÉGE

A mesterséges intelligencia fogalma

A mesterséges intelligencia kutatása és fejlesztése a számítógép- és a számítástudomány azon részterülete, amely a rendelkezésre álló adatok alapján *döntéshozatalra képes számítógépes programok* megalkotásával foglalkozik. A döntéshozatal képességével rendelkező szoftverek alkalmazásával az emberi intelligencia felfogást, indoklást, absztrakciót és tanulást igénylő feladatai részben vagy egészben kiválthatók. Általánosan elfogadott definíció híján tehát *MI alatt az emberi cselekvést részben vagy egészben automatikus módon kiváltó gépeket (szoftvereket) értjük*.[12]

Kategóriái:

- szűk (*narrow*) MI: konkrét részterületeken az ember képességeivel összemérhető teljesítményt nyújt, ez a jelenleg elérhető szint;
- általános (*general*) MI: bármilyen feladatot képes az emberi munkaerővel összemérhető színvonalon végrehajtani;
- mesterséges szuperintelligencia: bármilyen feladat tekintetében meghaladja az emberi képességeket.

[11] Különbséget teszek nemzetbiztonság (Intelligence) és nemzeti biztonság (National Security) között. Nemzetbiztonság alatt a hírszerzést és az elhárítást együttesen értem, míg a nemzeti biztonság „tartalma sokkal szélesebb, amelynek része a nemzetbiztonság, de minden más az ország védelméért felelős szervezet is, mint a haderő vagy a rendvédelmi szervezetek is odatartoznak."
VIDA Csaba: A nemzetbiztonsági elméletek alapjai – Szükségesek-e az alapkutatások a nemzetbiztonsági elméletekben? Szakmai Szemle, X. évfolyam 1 szám, 2022. március. pp. 5–21.
https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_1_szam.pdf; letöltés: 2022.10.17.
A biztonság modern értelmezése a biztonság katonai elemei mellett a politikai, a gazdasági, a társadalmi, a környezeti és az informatikai szektort is vizsgálja.
GAZDAG Ferenc – REMEK Éva: A biztonsági tanulmányok alapjai. Dialóg Campus Kiadó, Budapest, 2018. pp. 21–24.
https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12604; letöltés: 2022.10.17.
Ebben a szellemben készült hazánk jelenleg érvényes Nemzeti Biztonsági Stratégiája is.
1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt; letöltés: 2022.10.17.

[12] SCHMIDT, Eric – WORK, Robert – CATZ, Safra – CHIEN, Steve – CLYBURN, Mignon – DARBY, Chris – FORD, Kenneth – GRIFFITHS, José-Marie – HORVITZ, Eric – JASSY, Andrew – LOUIE, Gilman – MARK, William – MATHENY, Jason – MCFARLAND, Katharina – MOORE, Andrew: Final Report. National Security Commission on Artificial Intelligence, 2021.
https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf; letöltés: 2021.03.10.

Az MI elsősorban az alábbi tudományágak eredményeit használja fel és összegzi:

- természetes nyelvek feldolgozása (NLP[13]): a lingvisztika részterülete, amely a számítógépek és az emberek közötti nyelvi kommunikációval foglalkozik;
- tudásreprezentáció:[14] az információ számítógépek számára értelmezhető összeállításával foglalkozik, amelyhez az emberi komplex problémamegoldással kapcsolatos pszichológiai kutatásokat veszi alapul;
- automatikus következtetés:[15] a kognitív tudományok egyik ága, amelynek kutatásai lehetővé teszik a számítógépek számára, hogy önállóan vonjanak le következtetéseket a rendelkezésükre álló információk és tapasztalatok alapján;
- gépi (számítógépes) látás:[16] a digitális kép- és videofeldolgozás segítségével a számítógépek magas szinten képesek érzékelni a környezetüket;
- valamint a robotika.

A mesterséges intelligencia egyik kulcsfogalma az algoritmus. A fogalom megértéséhez Yuval Noah Harari nyújt segítséget. „*Az algoritmus egy tervszerű lépéssor, amelynek segítségével számításokat végezhetünk, problémákat oldhatunk meg és döntéseket hozhatunk. Nem maga a számítás, hanem a módszer, amelyet a számítás elvégzéséhez használunk. Ha például két szám átlagát akarjuk kiszámolni, használhatunk hozzá egy egyszerű algoritmust. Ez az algoritmus így szól: »Első lépés: adjuk össze a két számot. Második lépés: osszuk el az összeget kettővel.« Ha a két szám a 4 és a 8, az eredmény 6 lesz. Ha 117 és 231, akkor 174*."[17]

A *gépi tanulás*[18] (GT) a mesterséges intelligencia kutatásának egyik területe. A GT-rendszerek képesek előre megadott minták alapján önállóan vagy emberi segítséggel szabályszerűségeket felismerni vagy azonosítani. Ennek következtében a rendszer nemcsak megtanulja a kívülről kapott mintákat, hanem képes ezek alapján olyan általánosításokra is, amely szerint – a tanulási szakaszt követően – *új adatokra vonatkozólag is helyes döntéseket tud hozni*. Az ilyen gépek a tapasztalataikat felhasználva, *automatikusan tanulnak és fejlődnek*. A GT-rendszerek működése már nagyban hasonlít az emberi tudatéhoz. A gépi tanulási módszerek legelterjedtebb fajtái a felügyelt és a nem felügyelt, valamint a megerősítéses tanulás.

[13] Natural-language processing.
[14] Knowledge representation.
[15] Automated reasoning.
[16] Computer vision.
[17] HARARI, Yuval Noah: Homo Deus: A jövő rövid története. Animus Kiadó, Budapest, 2016. pp. 79–80.
[18] Machine Learning.

A GT technikái:

- megerősítő tanulás:[19] a gép az általa alkalmazott megoldásokról visszajelzést kap, amelyek alapján megjegyzi a helyes módszereket;
- mély tanulás:[20] a gépeket képessé teszik nagy mennyiségű adat feldolgozására, lehetővé téve számukra, hogy több feladattípust is végre tudjanak hajtani;
- mesterséges neurális (ideg-) hálózatok:[21] az emberi agy ideghálózatainak mintájára megalkotott algoritmusok.

A gépi tanulás olyan algoritmusokat alkalmaz, amelyek emberi beavatkozás nélkül képesek mintázatok felfedezésére, ezáltal adathalmazok jelentésének meghatározására. A gépi tanulást alkalmazó szoftverek felhasználhatók az adathalmazokon belül az összefüggő adathalmazok (clusterek) elkülönítésére és az anomáliák felfedésére, valamint szövegek szemantikai (jelentéstani) elemzésére.[22] A gépi tanulás képességeinek egyik fejlett felhasználása a hangulatelemzés,[23] ahol az algoritmusok a felderített szövegek szemantikai elemzésével következtetnek a tartalmat megosztó személy vagy csoport vélekedésének pozitív vagy negatív voltára egy eseménnyel vagy jelenséggel kapcsolatban.[24] Fontos alkalmazási terület továbbá az entitáskinyerés.[25] A technológia alapjául szolgáló algoritmusok automatikusan felismerik a betáplált dokumentumokban szereplő metaadatokat, személyeket és szervezeteket stb. (entitásokat).

A GT fejlesztésére világszerte szánt összeg becslések alapján az MI-hez köthető befektetések mintegy 60%-át teszi ki.[26]

A fejlett számítógépek továbbra sem rendelkeznek tudattal. Harari szerint a gépek esetében „*az intelligencia elkülönülőben van a tudattól*.” A gépek tudat nélkül is képesek lesznek a legtöbb feladatot jobban végezni az embereknél, „*ezek a feladatok ugyanis mintázatok felismerésén alapulnak, annak terén pedig a nem tudatos algoritmusok hamarosan felülmúlják az emberi tudatot*.”[27]

---

[19] Reinforcement learning.
[20] Deep learning.
[21] Artificial neural network.
[22] TAKÁCS Gergely: Big data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában.
[23] Sentiment analysis
[24] OMAND, David – BARTLETT, Jamie – MILLER, Carl: #Intelligence. London, Demos, 2012. https://demos.co.uk/wp-content/uploads/2012/04/intelligence-Report.pdf; letöltés: 2018.11.05.
[25] Entity extraction.
[26] A mesterséges intelligencia és a gépi tanulás kategóriáival, valamint az érintett tudományágakkal kapcsolatos információk forrása:
TONIN, Matej: Artificial Intelligence: Implications for NATO’s Armed Forces. NATO Parliamentary Assembly, 2019.10.13.
https://www.nato-pa.int/document/2019-stcttc-2019-report-artificial-intelligence-tonin-149-stctts-19-e-rev1-fin; letöltés: 2019.12.06.
[27] HARARI, Yuval Noah: Homo Deus: A jövő rövid története. p. 268.

Az emberi intelligencia felsőbbrendűségébe vetett hit 1997. május 11-én dőlt meg, miután az IBM Deep Blue sakkprogramja legyőzte Garri Kaszparov sakkvilágbajnokot. A mai szemmel már egyszerűnek nevezhető Deep Blue specializált szoftver, másodpercenként 200 millió szituáció kimenetelét képes kiszámolni.[28]

A mesterséges intelligencia új, gépi tanuláson alapuló nemzedéke jelentős továbblépést jelent. A sakknál összetettebbnek tartott go esetében 2016 márciusában – 200 millió néző szeme előtt – kerekedett az ember fölé a mesterséges intelligencia, miután a Google AlphaGo nevű öntanuló rendszere magától tanulta meg a gót, majd legyőzte I Szedolt, a go dél-koreai világbajnokát.[29] A Google DeepMind nevű szoftvere magától tanulta meg az Atari 49 klasszikus játékát, közülük 29-et olyan jól, hogy jobban játssza, mint az emberek. A DeepMind csupán a számítógépes képernyőn megjelenő pixeleket kapta alapul és azt az elvet, hogy minél magasabb pontszámot kell elérnie. A Google eszközei a szakértők szerint mindkét esetben korábban nem látott stratégiákkal álltak elő.[30]

A generikus gépi tanulásban mérföldkőnek tekinthető a Google AlphaZero teljesítménye. 2017 decemberében a szoftver négy órát kapott arra, hogy megtanulja a sakkot, mindössze a szabályok ismeretében. A tanulási folyamat abból állt, hogy a program saját maga ellen játszott. Ezt követően az Alpha Zero legyőzte a Stockfish 8 nevű specializált sakkprogramot.[31]

Az MI-vel szorosan összefügg az 5G technológia és a kvantummechanika. Az 5G technológia lehetővé teszi az okoseszközök tömeges csatlakozását az internethez, létrehozva a dolgok internetét (IoT[32]) és nagyban megnövelve a védelemre szoruló információs hálózatok összetettségét. A hálózaton elérhető eszközök hatványozott növekedése új lehetőségeket kínál a megfigyeléshez is. Az 5G nem tekinthető egyetlen technológiának, valójában információs technológiai ökoszisztémáról van szó, amely lehetővé teszi a vezető nélküli gépjárművek, az új ipari folyamatok,[33] a fejlett logisztikai rendszerek, az új védelmi alkalmazások stb. elterjedését. Az 5G elterjedésével új sérülékenységek is megjelennek.[34,35]

---

[28] Deep Blue. IBM 100. https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/; letöltés: 2021.08.12.

[29] The challenge match. Google DeepMind. https://deepmind.com/alphago-korea; letöltés: 2021.08.12.

[30] MORELLE, Rebecca: Google machine learns to master video games. BBC, 2015.02.25. https://www.bbc.com/news/science-environment-31623427; letöltés: 2021.08.12.

[31] GIBBS, Samuel: AlphaZero AI beats champion chess program after teaching itself in four hours. The Guardian, 2017.12.07. https://www.theguardian.com/technology/2017/dec/07/alphazero-google-deepmind-ai-beats-champion-program-teaching-itself-to-play-four-hours; letöltés: 2021.08.12.

[32] Internet of Things. Az információáramlás ugrásszerű növekedése lehetővé teszi, hogy az ipari termelésben és a hétköznapi életben stb. használt tárgyak egyre növekvő hányada is okoseszközzé váljon (okosgyár, okosotthon, okosváros stb.), valamint kommunikáljon a többi eszközzel és a teljes hálózattal.

[33] Ipar 4.0: a negyedik ipari forradalomban az információs technológia és az automatizálás egyre szorosabb összefonódása újabb robbanásszerű növekedést eredményez a termelés hatékonyságában.

[34] Az Amerikai Egyesült Államok az 5G-ben rejlő információszerző lehetőségekre hivatkozva igyekszik rávenni szövetségeseit, hogy a technológia bevezetése során zárják ki a kínai vállalatokat.

[35] SCHMIDT, Eric et al.: Final Report. National Security Commission on Artificial Intelligence, 2021. p. 51.

A kvantumszámítógépek megjelenése a számítási kapacitások nagyságrendi növekedését vonja maga után,[36] amely felhasználható lehet egyebek mellett a nagy adat elemzésében[37] – a fejlett MI-rendszereknek is hardveres alapjául szolgálva.

Az MI növekvő globális jelentősége, alkalmazásának módjai

Az MI-rendszerek elerjedése elsőként az alacsonyan képzett munkavállalók körében, illetve a fejletlen régiókban okozhat negatív társadalmi folyamatokat, elsősorban a munkanélküliség növekedését. A folyamat hatására a fejlett társadalmakban is növekedhet a bűncselekmények száma, illetve felerősödhet – akár kezelhetetlenné is válhat – a tömeges migráció. Emellett a csúcstechnológiát üzemeltetni képes munkaerő iránti igény nagymértékű növekedésével is számolni kell.

Yuval Noah Harari úgy véli, hogy az MI elterjedésével hosszú távon a jelenlegi munkakörök nagy többségében a „*robotok és a számítógépek (…) hamarosan le is hagyják az embert*." A 21. század legfontosabb kérdése lehet, hogy a társadalmak mihez kezdenek a haszontalanná váló emberekkel. A technológiai fejlődés eredményének három lehetséges eredményét veti fel:

„*1. Az emberek elveszítik gazdasági és katonai hasznosságukat, és a politikai rendszer többé nem tulajdonít nekik különösebb értéket.*

2. A rendszer továbbra is értéket tulajdonít az embereknek kollektíve, az egyéneknek külön-külön azonban nem.

3. A rendszer értéket tulajdonít bizonyos embereknek, ezek azonban nem a széles néptömegeket fogják alkotni, hanem a továbbfejlesztett szuperemberek új elitjét."[38]

A technológia térnyerése tovább növelte a meghatározó nemzetközi politikai szereplők közötti geopolitikai versengést. Technológiai szempontból egyelőre az Amerikai Egyesült Államoké a vezető szerep, de az MI-fejlesztésekre fordított összeg már jelentősen elmarad a kínai beruházásokétól. Európa jelenleg összességében lemaradásban van a két ország mögött. Elsősorban a védelmi szektorban figyelemre méltók továbbá Izrael eredményei (a szoftveripar mellett például az élet kioltására alkalmas autonóm robotok területén). Kiemelkedő Dél-Korea, Franciaország és Kanada szerepe is a fejlesztésekben. Fontos szereplőknek tekinthetők továbbá az Egyesült Arab Emírségek, az Egyesült Királyság, Finnország, India, Japán, Németország és Szaúd-Arábia is.

---

[36] A Google október 23-án bejelentette az úgynevezett kvantumfölény elérését. A vállalat közleménye szerint a Sycamore nevű kvantumprocesszor a jelenlegi legerősebb szuperszámítógépnél másfél milliárdszor gyorsabban végzett el egy számítást.
A Google állítja: elérte a kvantumfölényt. HVG, 2019.10.23.
https://hvg.hu/tudomany/20191023_A_Google_allitja_elerte_a_kvantumfelsobbrenduseget;
letöltés: 2019.12.06.

[37] A jelenleg még kezelhetetlen mennyiségű adat a jövőben feldolgozhatóvá válhat.

[38] HARARI, Yuval Noah: Homo Deus: A jövő rövid története. pp. 264–267.

Először Kanada fogadott el nemzeti MI-stratégiát (2017-ben). Jelenleg 62 állam, köztük Magyarország (28.-ként[39]) rendelkezik MI-stratégiával.[40]

A kormányzati szervezetek mellett a magánszféra szereplői (köztük: Alibaba, Amazon, Apple, Baidu, Facebook, Google, IBM, Microsoft, Netflix, Salesforce, Spotify, Tencent, Twitter, Uber) is dollármilliárdokat fordítanak az MI kutatására és fejlesztésére saját területeiken.

2018-as adatok szerint az MI-vel foglalkozó korai fázisú vállalkozások (startupok) száma egyelőre az Amerikai Egyesült Államokban a legmagasabb (2028), ezt követi Kína (1011), az Egyesült Királyság (392), Kanada (285), India (152), Izrael (121), Franciaország (120) és Németország (111).[41]

Magyarországon 2018 őszén, Palkovics László innovációs és technológiai miniszter kezdeményezésére alakult meg a több mint 150 tagszervezetet (cégeket, kutatóintézeteket, állami intézményeket stb.) számláló Mesterséges Intelligencia Koalíció. A kezdeményezés célja, hogy hazánk az MI-fejlesztések terén az európai élvonalba kerüljön.[42]

A fejlett társadalmak további robbanásszerű fejlődésével, ugyanakkor jelentős kockázatokkal is járhat az úgynevezett *technológiai szingularitás*[43] bekövetkezése. A fogalomnak többféle meghatározása létezik, amelyek közös eleme, hogy a szingularitás bekövetkeztével a tudományos-technológiai-társadalmi fejlődés elér egy olyan szintet, amelynek hatására *az esemény bekövetkezte előtt élő – ideértve a jelenkort is – emberiség számára érthetetlenné válik a szingularitásba belépett emberi civilizáció*. A folyamat kimenetele ennélfogva megjósolhatatlan. A jelenség kezdetével a technológiai fejlődés ellenőrizhetetlenné és visszafoghatatlanná válik, jelenleg elképzelhetetlen változásokat előidézve. A szingularitás fontos jellemzője, hogy a fejlődésnek ezen a szintjén az emberiség már csak a mesterséges intelligencia alkalmazásával lesz képes a fennmaradásához szükséges – szintén MI-re épülő –, létfontosságú rendszerek karbantartására és fejlesztésére. A szingularitással kapcsolatos

[39] ZHANG, Daniel – MISHRA, Saurabh – BRYNJOLFSSON, Erik – ETCHEMENDY, John – GANGULI, Deep – GROSZ, Barbara – LYONS, Terah – MANYIKA, James – NIEBLES, Juan Carlos – SELLITTO, Michael – SHOHAM, Yoav – CLARK, Jack – PERRAULT, Raymond: Artificial Intelligence Index Report 2021. Stanford University Human-Centered Artificial Intelligence, Stanford, CA, March 2021. pp. 155–161. https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf; letöltés: 2021.07.15.

[40] OECD.AI. A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) mesterséges intelligenciával foglalkozó honlapja. https://oecd.ai/en/dashboards; letöltés: 2021.12.29.

[41] A globális versengésre vonatkozó információk és adatok forrása: Winter Academy on Artificial Intelligence and International Law (2019). Az Asser Intézet (T.M.C. Asser Instituut) 2019. február 11–15. között Hágában megrendezett Mesterséges Intelligencia és a Nemzetközi Jog témájú téli akadémiája.

[42] Egy éve alakult meg a mesterséges intelligencia koalíció. Magyarország Kormánya, 2019.10.18. https://2015-2019.kormany.hu/hu/innovacios-es-technologiai-miniszterium/infokommunikacioert-es-fogyasztovedelemert-felelos-allamtitkar/hirek/egy-eve-alakult-meg-a-mesterseges-intelligencia-koalicio; letöltés: 2019.12.06.

[43] A kifejezés a csillagászat által használt gravitációs szingularitásból ered, amely a fekete lyukak közelében fellépő, a jelenleg ismert fizika által modellezhetetlen jelenségekre utal.

elképzelések szerves része a mesterséges szuperintelligencia megalkotása.[44] Yuval Noah Harari a technológiai szingularitás lehetőségének tárgyalásakor felveti, hogy annak bekövetkezése esetén elképzelhető, hogy „*a világunknak értelmet adó összes fogalom – én, te, férfi, nő, szeretet, gyűlölet – irrelevánssá válik. Minden, ami ezen a ponton túl történik, értelmetlen számunkra.*”[45]

Az MI alkalmazása hozzásegíthet a jó kormányzás elveinek megvalósításához az államigazgatásban és az önkormányzati igazgatásban. Az e-közigazgatási[46] rendszerek a szélesebb értelemben vett „okostársadalom” fejlesztésének is fontos eszközei lehetnek.

Az e-közigazgatásban a 2000-es évek eleje óta Észtország tekinthető élen járónak. A balti ország állampolgárai az interneten keresztül végezhetik ügyeiket a nap 24 órájában. Egyedül a házasságokhoz, a válásokhoz és az ingatlanok adásvételéhez szükséges személyesen megjelenni. Az észt állami informatikai rendszerek három alappillére az adatvédelem, a digitális személyazonosítás, valamint a köz- és a magánszféra adatbázisait összekötő internetalapú gerinchálózat.[47] A szerződéskötések elektronikusan történnek, a személyes elektronikus aláírás valamennyi szolgáltatás esetében érvényes. A dokumentumok vonatkozásában mindig a digitális változat számít hitelesnek, így gyakorlatilag megszűnt a papíralapú adminisztráció.[48]

A továbblépést az e-közigazgatás felhőalapúvá tétele[49] jelenti. A biztonság növelése érdekében a rendszert működtető két szervert külön helyszíneken helyezik el. Észtország hosszú távú terve, hogy néhány szövetséges országban e-nagykövetségeket hoz létre a közigazgatás válsághelyzetben történő zavartalan fenntartása érdekében. A kormányzati felhőt a kormány[50] a magánszférával közösen fejleszti. Kiemelt partnerek:

- Cybernetica (észt): megfelelés a nemzeti informatikai biztonsági követelményeknek;
- Dell EMC (amerikai): hardvereszközök;
- Ericsson (svéd): projektmenedzsment, hardver és szoftver;
- OpenNode (észt): a kormányzati felhő önkiszolgáló portálja és online szolgáltatói központja;
- Telia (svéd–finn): a felhőalapú termékek és szolgáltatások üzemeltetése.[51]

---

[44] EDEN, Ammon H. – STEINHART, Eric – PEARCE, David – MOOR, James H.: Singularity Hypotheses: An Overview. Introduction to: Singularity Hypotheses: A Scientific and Philosophical Assessment. Springer, New York, 2012. pp. 1–12. https://repository.essex.ac.uk/9220/1/Singularity%20Hypothesis.pdf; letöltés: 2019.12.06.

[45] HARARI, Yuval Noah: Sapiens: Az emberiség rövid története. Animus Kiadó, Budapest, 2015. pp. 364–365.

[46] E-Governance.

[47] X-Road.

[48] FENYŐVÁRI Bernadett: Az észt e-kormányzás titka. Lechner Tudásközpont, 2019.03.28. http://lechnerkozpont.hu/cikk/az-eszt-e-kormanyzas-titka; letöltés: 2020.03.11.

[49] Estonian Government Cloud.

[50] Az Állami Infokommunikációs Alapítványon (State Infocommunication Foundation) keresztül. A szervezet az adatközpontok létrehozásáért és a felhasználói kapcsolattartás optimalizálásáért felelős.

[51] e-Governance. e-Estonia. Az észt kormány tájékoztató honlapja az e-közigazgatásról. https://e-estonia.com/solutions/e-governance/; letöltés: 2020.03.11.

A japán kormány „Society 5.0" nevű okostársadalom átfogó koncepciójának[52] alapjai a dolgok internete (IoT), a nagy adat, a mesterséges intelligencia és a robotika. A koncepció célja, hogy a társadalom és az ipar jobb megszervezésével a termékek és a szolgáltatások fenntartható módon, a szükséges mennyiségben és időben jussanak el az emberekhez. A fejlesztések fő irányai:

- egészségügy: orvosi adatok (vizsgálatok, kezelések) elektronikus megosztása, a távolról is végezhető egészségügyi szolgáltatások körének bővítése, MI-alapú és robotrendszerek használata a betegápolásban;
- közlekedés: önvezető taxik és buszok alkalmazása elsősorban a vidéki közlekedésben, drónok használata a házhozszállításban, a nagy távolságú szállításban elsősorban az egyetlen emberi vezető által irányított konvojok bevezetését látják hasznosnak;
- infrastruktúra: az utak, a hidak, az alagutak és a gátak állapotának figyelemmel követését és állagmegóvását szenzorok telepítésével, valamint MI-alapú monitoringrendszerekkel és robotokkal végeznék;
- pénzügyi szolgáltatások: a pénzmozgásokhoz blokklánc-technológia[53] alkalmazását tervezik, és előnyben részesítik a készpénzmentes tranzakciókat.[54]

Ausztrália Queensland szövetségi állama sikeresen alkalmazza az MI-alapú rendszereket az adófizetési határidőcsúszások megelőzésére és az adócsalások felderítésére. A nagyadat-alapú statisztikai rendszerekkel képesek előre jelezni a várható késedelmes befizetéseket és időben értesíteni az érintetteket, ezáltal az állami költségvetési bevételek is megbízhatóbban tervezhetők.[55]

Az e-közigazgatás a lehetőségek mellett sebezhetőségeket is hordoz magában, amit mindmáig a 2007-es Észtországi ellen, valószínűsíthetően az orosz kormány által elrendelt, több héten át tartó túlterheléses támadások (DDoS[56]) példáznak a legérzékletesebben. A 2008-as grúziai események pedig azt mutatták be, hogy a kritikus információs infrastruktúrák elleni DDoS-támadások hatékonyan készítik elő és egészítik ki a hagyományos katonai műveleteket is.[57]

---

[52] Az elnevezés az ötödik generációs társadalomra utal, ahol az első generációt a vadászó-gyűjtögető életforma, a másodikat a mezőgazdaság, a harmadikat az ipari forradalom, a negyediket az információs forradalom jellemzi, míg a küszöbön álló okostársadalom az ötödik generáció.

[53] Block chain: először a BitCoin kriptovalutánál használt eljárás, ahol a főkönyvet nem központilag, hanem a felhasználók között elosztva vezetik, nagyban lecsökkentve a manipulálás lehetőségét.

[54] Realizing Society 5.0. A japán kormány tájékoztató brosúrája. https://www.japan.go.jp/abenomics/_userdata/abenomics/pdf/society_5.0.pdf; letöltés: 2020.03.11.

[55] KLEINEMEIER, Michael: How Governments Use AI To Create Better Experiences For Citizens. Forbes, 2019.11.07. https://www.forbes.com/sites/sap/2019/11/07/how-governments-use-ai-to-create-better-experiences-for-citizens/?sh=6bba0cad799c; letöltés: 2020.03.11.

[56] Distributed Denial of Service: szolgáltatásmegtagadással járó megosztott támadás.

[57] Georgia, Russia: The Cyberwarfare Angle. A Stratfor kutatóintézet elemzése. RANE, 2008.08.12. https://worldview.stratfor.com/article/georgia-russia-cyberwarfare-angle; letöltés: 2020.03.12.

A fejlett társadalmakban átmenet zajlik az e-orvoslásból[58] az MI-fejlesztéseket széleskörűen alkalmazó digitális orvoslás irányába. A fő irányokat az elektronikus egészségügyi nyilvántartás és a távorvoslás (telemedicina) jelentik. A fejlesztések eredményeképpen lehetőség nyílik az orvosi vizsgálat, a diagnózis felállítása, a konzultáció, a szaktanácsadás stb. távolról történő elvégzésére. A rendszer használatával – például vészhelyzetben – bármelyik orvos azonnal teljes körű betekintést nyerhet a páciens egészségügyi adataiba. A digitális orvosi adminisztrációval jelentős számú munkaóra takarítható meg például a vények kiállítása során. A rendszer hatékonyságát növeli annak integrálása az e-közigazgatásba, hiszen így a pácienseknek a teljes folyamat során kizárólag a személyazonosító igazolványukra van szükségük. Az e-közigazgatás keretében az állampolgárok számára biztosított eszközök körébe tartozhat például a mentőt egyszerűen kiértesítő okosalkalmazás, amely vészhelyzetben automatikusan vagy a páciens, esetleg hozzátartozója kérésére működésbe hozható. Ennek előnyei közé tartozik, hogy a rendszer pontos helyadatokat közöl a mentést irányítókkal, valamint továbbítja a páciens egészségügyi adatait (vércsoport, allergiák, közelmúltbeli kezelések, gyógyszerezés, terhesség stb.), megfelelő eszközök birtokában (pulzusmérő stb.) pedig aktuális állapotát is.

A fejlesztések forradalmat hoznak az orvosi technológiában is: a gépi látás fejlődésével jelentős előrelépés érhető el például az ultrahang-vizsgálatok, a sebészeti beavatkozások, illetve számos betegség, mint a bőrrák, a cukorbetegség stb. korai jelzése területén. Az MI-alapú rendszerek támogatják a biotechnológiai fejlesztéseket (új gyógyszerek, védőoltások, mesterséges szervek fejlesztése), a robotika pedig a mozgás- és látásszervi betegek állapotát képes jelentős mértékben javítani egyebek mellett művégtagokkal és mesterséges idegpályák létrehozásával. A valós időben vezérelhető rendszerekkel távolról is elvégezhetők összetett műtéti beavatkozások.

A gépi tanulás segítségével az emberi orvosok tudástára is kibővíthető, hiszen így nemcsak a saját, hanem potenciálisan az egész emberiség felhalmozott tudását felhasználhatják a diagnózis felállítása és a kezelés során.[59]

A tőzsdei kereskedésben több mint egy évtizede alkalmaznak MI-alapú automatizált kereskedési rendszereket. Az automatizálás kezdetben elsősorban az egyszerű tranzakciók előre meghatározott végrehajtására korlátozódott, mint például a céláras vétel és eladás. A gépi tanulás eredményeinek felhasználásával emellett lehetőség van a piaci folyamatok nagyadat-alapú elemzésére is. Az ilyen rendszerek az emberi elemzőknél összehasonlíthatatlanul több adat valós idejű vagy historikus feldolgozásával megnövelt hatékonysággal képesek előre jelezni a piaci folyamatokat. A brókercégek, a bankok és az alapkezelők meghatározó többsége egyelőre nem tervezi az emberi irányítás elhagyását a piacon végzett tevékenysége során. Néhány vállalat ugyanakkor – például a Hong Kong-i Aidiya – teljes mértékben áttért az MI-alapú algoritmusokon alapuló automatizált kereskedésre.

---

[58] E-Medicine.

[59] TURRINI, Mauro – MARTORANO, Carmen Miriam: From e-health to digital Health: Telemedicine, Electronic Healthcare File, Artificial Intelligence. Bird&Bird, 2019.06.23. https://www.twobirds.com/en/news/articles/2019/global/from-e-health-to-digital-health-telemedicine-electronic-healthcare-file-artificial-intelligence; letöltés: 2020.03.11.

Az algoritmusokon alapuló kereskedés hatékonyságát egy tanulmány is igazolja, amely összehasonlította a historikus tőzsdeindexeket az algoritmusok szimulált tevékenységével. A Dr. Christopher Krauss vezette kutatócsoport által fejlesztett algoritmus a Dow Jones tőzsdeindex 1992 és 2015 közötti adatainak felhasználásával készített szimulációban évi 73%-os nyereséget ért el, szemben a valóságban megvalósult átlagosan 9%-os piaci növekedéssel.[60]

Az automatikus kereskedés elterjedésének kedvez, hogy a befektetési alapok kezelik az összes tőke mintegy 60%-át, míg az egyéni befektetők mindössze 10%-ról döntenek. Az alapok által kezelt részarány a 2008-as pénzügyi válságot követő évtizedben megduplázódott. Ugyanebben az időszakban a Goldman Sachs befektetési bank 600 brókeri pozíciót szüntetett meg, miközben 200 fővel növelte az informatikai mérnökei számát.

Az MI-alapú tőzsdei elemző algoritmusok két fő területe:

- a technikai elemzés a fundamentumokat (az adott céggel kapcsolatos információkat) figyelmen kívül hagyva kizárólag a piaci mozgásokra vonatkozó adatok elemzésére hagyatkozik;
- a hangulatelemzés a piaci árat befolyásoló érzelmi tényezők nyomon követését végzi például újságcikkekben és a közösségi médiában, a szegmens vezető vállalatai az amerikai Social Market Analytics és a Stocktwits.

Az algoritmusok hatékonyságát ugyanakkor negatívan befolyásolja a hasonló – szintén a piaci folyamatok előrejelzésére szolgáló – alkalmazások egyre növekvő jelenléte a piacokon.

Az elemző algoritmusok legfőbb erőssége, hogy olyan mikrotrendeket is képesek azonosítani, amelyek az emberi elemzők előtt rejtve maradnak. Ugyanakkor bármely nagy adatot feldolgozó MI-alapú rendszerhez hasonlóan az adatok manipulálásával az algoritmusok által előállított eredmény is befolyásolható. Az amerikai Manceps tőzsdei MI-rendszereket fejlesztő vállalat 2019-ben elvégzett kísérletében egy speciálisan erre a célra létrehozott kereskedőrobot (algoritmus) képes volt a többi robot tevékenységét befolyásolni egy szimulált tőzsdei környezetben. A szimulációban a robot kiértékelte más robotok kereskedését és meghatározta, hogy azok milyen tényezőket vesznek figyelembe a döntéseik során. Ezt követően kis összegekkel, kizárólag befolyásolási céllal kereskedett, sikeresen alakítva a piaci folyamatokat. A kísérlet rámutatott az automatizált rendszerek sérülékenységére és az emberi felügyelet szükségességére.[61]

[60] BARLOW, Sonya: Can we trust machines to predict the stock market with 100% accuracy? Metro, 2019.05.06. https://metro.co.uk/2019/05/06/can-we-trust-machines-to-predict-the-stock-market-with-100-accuracy-9325480/; letöltés: 2020.03.11.

[61] KARI, Al – LANDER, Garrett: Could an Adversarial Bot Manipulate the Stock Market? Manceps, 2019.11.18. https://www.manceps.com/articles/experiments/beat-the-bots; letöltés: 2020.03.11.

Az algoritmusokkal folytatott kereskedés veszélyeire figyelmeztet a 2010. május 6-ai ötperces tőzsdei sokk, amelynek során a Dow Jones tőzsdeindex ismeretlen okból közel 9%-ot vesztett értékéből mintegy 1000 milliárd dolláros kárt okozva, majd az index percek alatt visszaállt az eredeti szintre. A szakértők nem tudták megfejteni, hogy mi okozta a váratlan és gyors összeomlást (*flash crash*).[62]

Az MI a tőzsdei visszaélések felderítésére is alkalmazható. Az amerikai Nasdaq elektronikus tőzsdénél a közelmúltban bevezetett, gépi tanuláson alapuló rendszer a piaci folyamatok monitorozásával azonosítja a tőzsde törvénytelen befolyásolását és más csalásokat. A rendszer anomáliákat és más rendellenes kereskedési mintázatokat keres és értesíti azokról a tőzsde munkatársait.[63]

A gépi látás (*machine vision*) magában foglalja a fizikai tárgyak jelenlétét jelző szenzorokat (mozgásdetektorokat), a kamerákat, a képdigitalizáló[64] szoftvereket, a képelemző programokat és számítógépeket, a megjelenítő eszközöket (interfész), illetve egyes esetekben a minták meghatározásához szükséges, gépi tanuláson alapuló algoritmusokat. A gépi látás részterülete a számítógépes látás (*computer vision*), amely kizárólag képek és videók feldolgozására korlátozódik. A gépi látás az Ipar 4.0[65] egyik kulcstechnológiája.

A fejlett gépi látás a gépi tanulás része, míg az egyszerűbb (hagyományos), szabályalapú megoldások az emberek által is felismerhető szimbólumok (karakterek,[66] tárgyak[67] stb.) feldolgozására építő „szimbolikus MI" területe. A GT-n alapuló gépi látást olyan összetett vagy kiszámíthatatlan esetekben alkalmazzák, amelyek programozása túl nehéz lenne szabályalapú algoritmusokkal. Az ilyen kiegészítő megoldások kezelik a zavaró háttereket és az alkatrész részjellemzőiben (anyag, textúra stb.) mutatkozó eltéréseket, értelmezik a hibásan nyomtatott kódokat, valamint karbantartják a vezérlésükre szolgáló alkalmazásokat (pl. az üzem új képadataival képzik önmagukat).

---

[62] COOKE, Sam: Does the adoption of AI open up 'flash crash' trading exposure? Totally Gaming, 2017.09.18. https://totallygaming.com/news/features/does-adoption-ai-open-flash-crash-trading-exposure; letöltés: 2021.08.12.

[63] RENNERT, Aaron: The Nasdaq Exchange Embraces AI: Market Manipulation Mitigation Built for the Future, 2019.08.05. https://www.rebellionresearch.com/blog/the-nasdaq-exchange-embraces-ai-market-manipulation-mitigation-built-for-the; letöltés: 2020.03.11.

[64] Frame grabber.

[65] A negyedik ipari forradalomban az információs technológia és az automatizálás egyre szorosabb összefonódása várhatóan újabb robbanásszerű (akár 15–20%-os) növekedést eredményez a termelés hatékonyságában. Az Ipar 4.0 2025-ig becslések szerint 1200–3700 milliárd dollárt adhat hozzá a világgazdasághoz.

[66] Optical Character Recognition – OCR.

[67] Object Recognition – OR.

A gépi látást jelenleg a feldolgozóipar és a mezőgazdaság használja fel a legszélesebb körben az alábbi részterületek automatizálásához:

- minőségbiztosítási ellenőrzések: az ilyen rendszerek képesek tömegesen,[68] nagy gyorsasággal és minimális hibahányaddal összevetni az ellenőrzésre kijelölt termék kamerával rögzített és digitálisan feldolgozott jellemzőit az adatbázisban szereplő referenciaértékekkel (méret, szín stb.);[69]
- a gyártósorok hibáinak feltárása a hiba keletkezési helyének behatárolásával;
- raktárkészlet-menedzsment: a termékek és a részegységek vonal- és QR-kódjainak[70] leolvasásával a raktárkészlet állapotának nyomon követése és a gyártási folyamatok optimalizálása (egyben minőségbiztosítása, hiszen így garantálható, hogy a megfelelő részegységeket használják fel), valamint a szállítmányok robotizált összeállítása;
- elsősorban a szigorúan szabályozott iparágakban, mint például a gyógyszeriparban, elengedhetetlen a termékek összetevőinek, szériaszámának és lejáratának nyomon követése, amelyet a gépi látás nagyban leegyszerűsít;
- precíziós mérés és kalibráció;
- előrejelző karbantartás:[71] egyéb szenzorok (hő, rezgés stb.) adataival együtt az eszközök állapotának nyomon követése;
- a biztonság növelése például építési területeken vagy az élelmiszerkészletek monitorozásával;
- a mezőgazdaságban a robotizált betakarítórendszerek alkalmazásánál, például a szőlőszemek helyének meghatározásával, valamint gépi látással (pl. drónkamerák felvételeinek felhasználásával) figyelemmel követhető továbbá a termés állapota (a növények fejlődésének nyomon követése, a növényeken megjelenő kártevők detektálása stb.), megoldható az erdők állapotvizsgálata, a tűzterjedés hatékony modellezése és a mezőgazdasági területek részletes elemzése (vegetációs index, talajnedvesség, parlagfű terjedése stb.).[72]

[68] Percenként akár több ezer alkatrész ellenőrzése.
[69] A gépi látás. Műszaki Magazin, 2019.09.28. http://muszaki-magazin.hu/2019/09/28/a-gepi-latas/; letöltés: 2020.03.11.
[70] Quick Response kód: a hagyományos vonalkódoknál lényegesen több információ tárolására alkalmas kétdimenziós pontkód.
[71] Predictive maintenance.
[72] VERES Dóra: Mesterséges Intelligencia a mindennapokban – A magyar fejlesztésű "gépi szemek" már az életünk részei. Portfolio, 2019.11.20. https://www.portfolio.hu/befektetes/20191120/mesterseges-intelligencia-a-mindennapokban-a-magyar-fejlesztesu-gepi-szemek-mar-az-eletunk-reszei-407233; letöltés: 2020.03.11.

1. ábra. Az Industrial Vision termékvizsgálati berendezése[73]

A gépi látás eredményei felhasználhatók továbbá a légi irányításban, a baleseti helyszínelésben, a bűnmegelőzésben (statisztikák elemzésével, viselkedési anomáliák vagy fegyverek fotókon történő detektálásával stb.), illetve mozgási anomáliák (közlekedési káosz, tömegpánik stb.) detektálásában is. Az ilyen rendszereket kiterjedten alkalmazzák a határvédelemben is.[74]

Az MI részterületeként a gépi látás is dinamikusan fejlődő iparág. Termékeinek piaci részesedése 2025-re meghaladhatja a 18 milliárd dollárt. A gépi látás iparág vezető vállalatai: Aquifi (amerikai), Cognex (amerikai), Datalogic (olasz), Industrial Vision (brit), IVISYS (dán–svéd), LMI Technologies (kanadai), Omron Microscan Systems (japán), National Instruments (amerikai), Optotune (svájci), Prophesee (francia), ProPhotnix (amerikai), Sensory (amerikai), Stemmer Imaging (német), USS Vision (amerikai), VAIA Technologies (amerikai), ViDi Systems (svájci). Magyarországon gépi látáson alapuló megoldásokat nyújt: OTT-ONE, iSRV, Dolphio Technologies, SignAll Technologies, 3D Infotech.[75]

[73] Automated Vision Inspection Benches IVS-MALi-A. https://www.industrialvision.co.uk/products/automated-vision-inspection-bench-ivs-mali-a; letöltés: 2020.03.11.

[74] MARR, Bernard: What is Machine Vision And How Is It Used In Business Today? Forbes, 2019.10.11. https://www.forbes.com/sites/bernardmarr/2019/10/11/what-is-machine-vision-and-how-is-it-used-in-business-today/#7317b8276939; letöltés: 2020.03.11.

[75] UMUTCAN, Safak: Machine Vision in 2020: In-Depth Guide. AI Multiple, 2020.09.29. https://research.aimultiple.com/machine-vision/; letöltés: 2020.10.03.

Az egyre összetettebb ipari informatikai megoldások növelik a gazdaság informatikai sebezhetőségét. Egy nemzetállam kritikus ipari infrastruktúrája elleni első támadás a Stuxnet nevű számítógépes féreg[76] 2010 júniusi alkalmazása volt, egyben az első eset, amikor az informatikai támadás közvetlen fizikai rombolást okozott.[77] Hasonló eszközökkel mára teljes iparágak működése szabotálhatóvá vált, az Ipar 4.0 elterjedésével pedig a kibervédelem a nemzeti biztonság alappillérévé válik.

Az alkotó mesterséges intelligencia[78] a különböző művészeti ágakban az emberi teljesítményhez mérhető alkotásokat létrehozó szoftvereket és robotokat jelenti. Az ilyen rendszerek képesek meghatározott vagy véletlenszerű témákban verset, esszét vagy regényt írni, zenei műveket létrehozni és azokat előadni, festményeket alkotni stb.

Az emberekkel folytatott online szöveges vagy szóbeli beszélgetésre alkalmas szoftverek (csetbotok) alkalmazása széles körben elterjedt a szolgáltatói szektorban. A botok hatékonyságát a gépi tanulás, elsősorban a természetes nyelvek feldolgozása[79] nagyban fokozta. A fejlesztések célja, hogy a fogyasztókban az az érzés alakuljon ki, hogy egy emberrel kommunikálnak. A megfizethető árú (legfeljebb havonta néhány száz dolláros költségű), online elérhető csetbotplatformok precízen személyre szabhatók és paraméterezhetők. A keretszoftvereket jellemzően az alkalmazó vállalat, szolgáltatás, webshop stb. karakteréhez, márkaarculatához, imázsához illesztik, meghatározzák a használandó és a kerülendő kifejezések körét, az elvárt hangnemet, miközben biztosított az emberszerű kommunikáció benyomása. A piacon jelenleg elérhető jelentősebb ilyen platformok: Aivo (argentin), Boost.ai (norvég), Botsify (pakisztáni), Chatfuel (amerikai), Flow XO (brit), Hyro (amerikai), Imperson (amerikai–izraeli), Its Alive (francia), ManyChat (amerikai), MobileMonkey (amerikai), Pandorabots (amerikai), Reply.ai (amerikai), Smartloop (amerikai), TARS (indiai).[80]

A befolyásolás jelenleg egyik legfontosabb iránya a mesterséges intelligencia alkalmazásával egyre hitelesebben hamisítható hang- és videofelvételek (*deepfake*, mélyhamisítás) készítése.[81] Alkalmazásukkal az a benyomás alakítható ki, hogy az eljuttatni kívánt üzenetet közismert és befolyásos személyek közvetítik, növelve azok meggyőző erejét. A jövőben várható, hogy a mélyhamisított tartalmakat

---

[76] Computer worm, egy számítógépes vírushoz hasonló, önsokszorozó számítógépes program, amelynek a vírussal ellentétben nincs szüksége gazdaprogramra, önállóan működik.

[77] Iran Confirms Stuxnet Worm Halted Centrifuges. CBS News, 2010.11.29. https://www.cbsnews.com/news/iran-confirms-stuxnet-worm-halted-centrifuges/; letöltés: 2021.12.29.

[78] Creative artificial intelligence.

[79] A technológia képezi a hangulatelemzés alapját is, nagyban növelve a gépi kommunikáció hatékonyságát.

[80] BARKER, Shane: 15 of the Best AI Chatbot Platforms to Increase Your Conversions in 2020. Martech Cube, 2020.07.29. https://www.martechcube.com/best-ai-chatbot-platforms-to-increase-your-conversions-2020/; letöltés: 2020.08.11.
BROOKS, Aaron: 10 Best Chatbot Builders in 2020. Venture Harbour, 2020. https://www.ventureharbour.com/best-chatbot-builders/; letöltés: 2020.03.11.

[81] MIKHEEV, Evgeny A. – NESTIK, Timofey, A.: The Use of Artificial Intelligence Technologies in Information and Psychological Warfare. In: PSYRGGU 2019 – Psychology of subculture: Phenomenology and Contemporary Tendencies of Development. The European Proceedings of Social & Behavioural Sciences, 2019. https://www.europeanproceedings.com/files/data/article/109/5743/article_109_5743_pdf_100.pdf; letöltés: 2020.03.11.

csetbotokba ültetik és ezáltal interaktívvá teszik. Különösen hatásosnak ígérkeznek azok a lehetséges fejlesztések, amelyek ismert személyek digitális modelljeit (avatarjait) használhatják fel. A popkultúra és a mesterséges intelligencia első nagy nyilvánosságot kapott találkozása az 1996-ban elhunyt Tupac Shakur amerikai rapelőadó 2012-es hologramkoncertje volt a kaliforniai Coachella zenei fesztiválon.[82] Az egyre fejlődő technológiával a filmipar is élethűen szerepeltet már elhunyt színészeket vagy fiatalít meg időseket.

Az MI „emberarcúvá" tételének egyik úttörője az új-zélandi Soul Machines vállalat, amely a képességeinek bemutatása keretében létrehozta William Adam (will.i.am) amerikai popelőadó háromdimenziós digitális modelljét. A számítógép képernyőjén megjelenő avatar képes az előadó stílusában, annak kifejezéseivel és mimikájának élethű utánzásával kommunikálni.[83] Az AI Foundation amerikai cég Deepak Chopra amerikai–indiai író digitális mását hozta létre.[84]

A valós személyek digitális másai mellett lehetőség van a fizikai valóságban nem létező, tetszőleges külsejű „személyek" élethű digitális szimulációjára. A Xinhua kínai hírügynökség 2018-ban jelentette be, hogy kínaiul és angolul is beszélő digitális hírolvasóval csökkenti a költségeit.[85]

2. ábra. A Xinhua digitális hírolvasója[86]

[82] Tupac returns from the dead at Coachella. The Guardian, 2012.04.16. https://www.theguardian.com/music/musicblog/2012/apr/16/tupac-coachella; letöltés: 2020.11.16.

[83] The Age of A.I. Soul Machines, 2019.12.19. https://www.soulmachines.com/2019/12/the-age-of-a-i/; letöltés: 2020.03.11.

[84] Deepak Chopra and the AI Foundation Partner to Bring Personal Transformation to Billions with the Power of Deepak's Own AI. Business Wire, 2019.12.05. https://www.businesswire.com/news/home/20191205005164/en/Deepak-Chopra-and-the-AI-Foundation-Partner-to-Bring-Personal-Transformation-to-Billions-with-the-Power-of-Deepak%E2%80%99s-Own-AI; letöltés: 2020.11.16.

[85] BARANIUK, Chris: China's Xinhua agency unveils AI news presenter. BBC, 2018.11.08. https://www.bbc.com/news/technology-46136504; letöltés: 2020.11.16.

[86] HARIDY, Rich: Real "fake news": China introduces AI news anchor. New Atlas, 2018.11.08. https://newatlas.com/china-ai-digital-news-anchor/57158/; letöltés: 2020.11.16.

A dél-koreai Samsung leányvállalata, a STAR Labs szintén valósághű karakterszimulációk fejlesztését végzi.[87]

3. ábra. A STAR Labs karakterszimulációi[88]

A jövőben várható, hogy a közéleti személyiségek egyre szélesebb köre, majd potenciálisan bármely felhasználó rendelkezik majd – akár a virtuális valóságban[89] is megjelenő – digitális mással.

Az alkotó mesterséges intelligencia széles körben felhasználható az írott tartalom automatizált előállításához[90] is. A jelenlegi megoldások elsősorban a marketingszövegek és az újságcikkek keresőmotorokhoz optimalizált (SEO[91]), élvezetesen olvasható és jól érthető, informatív megírását végzik el, évi milliárdos nagyságrendben. Számos hírügynökség és hírlap (egyebek mellett az Associated Press, a The Washington Post és a Reuters) is felhasználja az MI-t a cikkei megírásához. A brit PA Media konglomerátum havi 30 ezer helyi hírt állít elő mesterséges intelligenciával. Az automatizált tartalomtípusok között továbbá vállalati adatsorok, pénzügyi jelentések, e-mailek és csevegő alkalmazások is szerepelnek.

Az írott tartalmak előállítására szolgáló alkalmazások a megrendelő igényeire szabhatók, és a megadott adatbázisok felhasználásával állítják elő a szövegeket. A piacvezető platformok a brit Quill és Wordsmith.

---

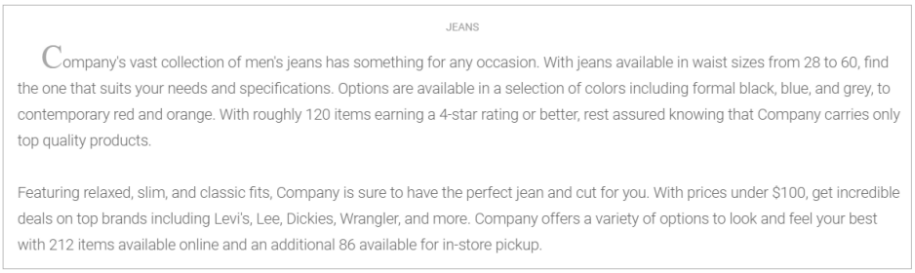
87 SAVOV, Vlad: Samsung Looks Beyond AI With Artificial Humans. Bloomberg, 2020.01.07. https://www.bloomberg.com/news/articles/2020-01-07/samsung-looks-beyond-ai-with-neon-artificial-humans; letöltés: 2020.11.16.

88 PARIKH, Prasham: CES 2020: Samsung STAR Labs Just Created An 'Artificial Human' Called NEON. Mashable India, 2020.01.07. https://in.mashable.com/tech/10199/ces-2020-samsung-star-labs-just-created-an-artificial-human-called-neon; letöltés: 2020.03.11.

89 Virtual Reality – VR.

90 Natural Language Generation – NLG.

91 Search Engine Optimization: az online tartalom előállításánál az internetes keresőmotorok (Google, Bing stb.) algoritmusait veszik alapul azzal a céllal, hogy az adott cég, személy, termék vagy szolgáltatás előrébb jelenjen meg azok keresési eredményeiben.


JEANS

Company's vast collection of men's jeans has something for any occasion. With jeans available in waist sizes from 28 to 60, find the one that suits your needs and specifications. Options are available in a selection of colors including formal black, blue, and grey, to contemporary red and orange. With roughly 120 items earning a 4-star rating or better, rest assured knowing that Company carries only top quality products.

Featuring relaxed, slim, and classic fits, Company is sure to have the perfect jean and cut for you. With prices under $100, get incredible deals on top brands including Levi's, Lee, Dickies, Wrangler, and more. Company offers a variety of options to look and feel your best with 212 items available online and an additional 86 available for in-store pickup.

4. ábra. Példa a Wordsmith által automatikusan előállított tartalomra[92]

Az amerikai Article Forge és Articoolo képes megadott témákban újságcikkeket írni. A szoftverek értelmezik a címet, internetes kereséssel beszerzik a szükséges információt, majd a SEO-irányelveket betartva megírják a cikkeket. A szintén amerikai WordAi képes szavak tetszőleges listájából értelmes mondatokat alkotni. A Scoop.it (amerikai) előrejelző és elemző platformja a tartalom kiválasztásában segíti a marketingeseket.[93]

Az Európai Unió MI-stratégiái

Az Európai Unió Bizottsága az MI-fejlesztések előmozdítása érdekében 2018 áprilisában nyilvánosságra hozta a *Mesterséges Intelligencia Európáért*,[94] 2018 decemberében pedig az *Összehangolt terv a Mesterséges Intelligenciáról*[95] című kommunikációit.[96] A Bizottság 2021-ben ez utóbbi felülvizsgált változatát bocsátotta ki.[97] A Bizottság három pilléren alapuló megközelítést javasolt az állami és a magánberuházások növelése, a társadalmi-gazdasági változásokra történő felkészülés, valamint egy megfelelő etikai és jogi keret kialakítása érdekében. A kezdeményezés kidolgozására azt követően került sor, hogy az európai vezetők jelezték, szükségesnek érzik a mesterséges intelligencia európai megközelítésének kidolgozását. A Bizottság 2019. január 1-jén elindította továbbá a kutatás-fejlesztési programok támogatására

[92] MRUNMAYI, Sapatnekar: 10 Powerful Content Automation AI Tools to Replace Content Writers. Staenz, 2019. https://staenz.com/content-automation-ai-tools/; letöltés: 2020.03.11.
[93] MRUNMAYI, Sapatnekar: 10 Powerful Content Automation AI Tools to Replace Content Writers. Best AI Writing Assistant Software. G2, 2020. https://www.g2.com/categories/ai-writing-assistant; letöltés: 2020.03.11.
[94] Factsheet: Artificial Intelligence for Europe. European Commission, 2019.07.04. https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe; letöltés: 2019.12.09.
[95] Coordinated Plan on Artificial Intelligence. European Commission, 2018.12.07. https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence; letöltés: 2019.12.09.
[96] A Bizottság nem kötelező iránymutatását tartalmazó dokumentum.
[97] Coordinated Plan on Artificial Intelligence 2021 Review. European Commission, 2021.04.21. https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review; letöltés: 2022.07.24.

szolgáló AI4EU[98] projektet. 2019 júniusában az Európai Unió Politikai és Biztonsági Bizottsága[99] első alkalommal vitatta meg formális keretek között a mesterséges intelligencia témáját. A területen az EU szerteágazó munkát végez, érintve többek között a téma elméleti, etikai, ipari és védelmi képességfejlesztési aspektusait, mindezt egyeztetve más nemzetközi szervezetekkel.

Az MI védelmi célú alkalmazásában kiemelt figyelmet kap az érdemi emberi befolyás fenntartása a döntéshozatal során, elsősorban a halálos autonóm fegyverrendszerek kapcsán. Az EU stratégiai jelentőséget tulajdonít az MI katonai alkalmazásának, amelynek fejlesztése szükséges a műveleti fölény megőrzéséhez, továbbá a személyi állomány kitettségének csökkentéséhez.[100] A terület fejlesztése érdekében rendkívül fontos a kutatóintézetek, a közszféra és a magánszektor közötti együttműködés elősegítése. Az EU a tagállamok közös álláspontjának kialakítására törekszik annak érdekében, hogy megkezdhesse az ENSZ keretében végzendő globális egyeztetéseket.

Magyarország Mesterséges Intelligencia Stratégiája

Magyarország Mesterséges Intelligencia Stratégiája 2020 májusában készült el, Magyarország Kormányának szeptember 9-ei határozatával[101] hatályos. A Stratégiát a Mesterséges Intelligencia Koalíció[102] szakértői készítették el az Innovációs és Technológiai Minisztérium[103] (ITM) koordinálásával. Célja, hogy Magyarország felkészüljön az MI jelentette változásokra, és használhassa annak előnyeit.

A dokumentum négy fő fejezetből áll, amelyek közül az első bemutatja az MI fogalmát, valamint globális és hazai jelentőségét, a második összegzi Magyarország meglévő eredményeit, erősségeit, illetve hiányosságait, a harmadik célokat fogalmaz meg, a negyedik pedig cselekvési tervet vázol fel. A Stratégia melléklete tartalmazza a részletes intézkedési tervet, amelyhez felelősöket és határidőket rendel.

Az MI fogalma, globális és hazai jelentősége

A Stratégia rögzíti az MI fogalmát: „*az emberi intelligencia valamely részének leképezésére alkalmas szoftver, amely képes támogatni vagy autonóm módon ellátni észlelési, értelmezési, döntési vagy cselekvési folyamatokat*.” Rögzíti, hogy „*a*

---

98 „Mesterséges Intelligencia Európáért”.

99 Political and Security Committe – PSC: Az EU Tanácsának a közös kül- és biztonságpolitikáért felelős, a tagállamok EU-nagyköveteiből álló konzultatív testülete.

100 Az Európai Védelmi Ügynökség (European Defence Agency – EDA) a témakörben kiadott egy kutatási témajavaslatot „Kommunikációs és radarrendszerek megerősítése a mesterséges intelligenciával bonyolult elektronikai hadviselési környezetben” címmel. „Communications and Radar systems hardened with Artificial Intelligence in contested electronic warfare environment (CRAI)”.

101 1573/2020. (IX. 9.) Korm. határozat Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről. https://njt.hu/jogszabaly/2020-1573-30-22; letöltés: 2022.03.17.
ZHANG, Daniel et al.: Artificial Intelligence Index Report 2021. pp. 155–161.

102 A Koalíció több mint 240 szervezetből és 1000 delegált szakértőből áll.

103 Az ITM 2022. május 24-én megszűnt, jogutódja a Technológiai és Ipari Minisztérium (TIM).

mesterséges intelligencia fogalma alatt a dokumentum során végig az úgynevezett »szűk« mesterséges intelligenciát értjük, vagyis olyan rendszereket, amelyek csak egy-egy területét képesek leképezni az emberi intelligenciának. Az emberi intelligencia teljességét leképezni képes úgynevezett »általános« MI kutatása jelenleg még annyira fejletlen és bizonytalan, hogy az alábbiak nem vonatkoznak rá." Az MI jelentőségét új ipari forradalomhoz hasonlítja, amely ugyanakkor nem természeti, hanem elsősorban emberi erőforrásigényt támaszt. A kibontakozó folyamat „*mindenkit személyesen érint, radikálisan alakítja át a munkaerőpiac elvárásait, új dimenziókat nyit a hatékonyságnövelés terén, és óriási gazdasági növekedési lehetőséget hozhat. Ugyanakkor a fejlődés egy globális versengő környezetben történik, és számos szuverenitási kérdést vet fel. Mindez Magyarország számára történelmi lehetőség és kihívás*."

A 2030-as évek végéig Magyarországon az MI és a technológia által lehetővé tett automatizáció várhatóan 900 ezer munkavállalót érint majd, potenciálisan a munkakörök több mint 40%-a lehet automatizálható. A Kormány a 2020-as évek közepéig a jelenleg betöltött munkakörök 5–10%-os, 2025–2030 között 15–20%-os, a 2030-as években 25–30%-os arányú automatizálásával számol. A kezdetben az elsősorban alacsonyabb hozzáadott értékű, adminisztratív munkaköröket érintő folyamat az időtáv végére a magas komplexitású és felelősséggel járó munkakörökre is kiterjed majd. Az MI-adaptáció nemcsak azért fontos, hogy az érintett munkavállalók továbbra is helyet kapjanak a munkaerőpiacon, hanem azért is, hogy Magyarország fenntarthassa pozícióját a magas hozzáadott értékű munkafolyamatok kiszervezése terén.

Az MI kulcsszerepet játszik a globális és a hazai GDP növekedésében. Az előrejelzések szerint 2030-ra a globális GDP-t 14–16%-kal (13–15 ezer milliárd dollárral) növelheti. Regionális megoszlásban Kínában a GDP-t 26,1%-kal, Észak-Amerikában 14,5%-kal, Észak-Európában 9,9%-kal, míg Dél-Európában 11,5%-kal fogja növelni. Magyarország esetében a dél-európai 11,5%-os GDP-növekedéssel lehet számolni, ami 6400 milliárd forintos kibocsátási többletet teremthet.

A Stratégia megalkotása során az MI-koalíció és a Kormány irányadónak tekintette a mértékadó nemzetközi szervezetek ajánlásait. Ezek közül kiemelt jelentőségű az Európai Bizottság Összehangolt terve a mesterséges intelligenciáról,[104] a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD[105]) MI-vel kapcsolatos ajánlásai,[106] a G20 országcsoport „emberközpontú MI-irányelvei",[107] valamint az UNESCO Általános Konferenciája (Közgyűlése) által elfogadott irányelvek az MI etikájáról.[108]

[104] Coordinated Plan on Artificial Intelligence. European Commission, 2018.12.07.
[105] Organisation for Economic Co-operation and Development.
[106] Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, 2019.05.22. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449; letöltés: 2021.07.12.
[107] G20 Ministerial Statement on Trade and Digital Economy. 3. pont: Human-centered Artificial Intelligence (AI). 2019. június. https://www.mofa.go.jp/files/000486596.pdf; letöltés: 2021.07.17.
[108] Preliminary study on the Ethics of Artificial Intelligence. UNESCO – COMEST, Paris, 2019.02.26. https://unesdoc.unesco.org/ark:/48223/pf0000367823; letöltés: 2021.07.15.

Az MI elterjedése a nemzeti szuverenitásnak is fontos új terepe. Az új technológiák térnyerésével *az adatok válnak a legfontosabb erőforrássá*, ami új kiberbiztonsági, illetve szabályozási kihívásokat és feladatokat jelent.

Hol tartunk?

A mesterséges intelligencia adta lehetőségek széles körű hazai kiaknázása szempontjából előny, hogy a gazdaságban és az állami szektorban élénk, sokszínű és aktív MI-ökoszisztéma működik. A Stratégia külön kiemeli az autonóm járművek fejlesztését,[109] emellett a távközlés, a bank- és biztosítási szektor, a kiskereskedelem, a közlekedés/logisztika, a gyártás, az agrárium, az energetika, az egészségügy és az államigazgatás területén mutathatók fel számottevő, már bevált eredmények. E szektorokban aktív együttműködés jött létre az egyetemi kutatói hálózatok és kiválósági központok, valamint a piaci szereplők között.

Infrastrukturális szempontból jó alapot ad Magyarország európai viszonylatban is jó színvonalú szélessávúinternet-lefedettsége, valamint a már elérhető és a létesítés alatt álló[110] számítási kapacitások. Erősséget jelent a szabályozott elektronikus ügyintézési szolgáltatások (SZEÜSZ-ök) széles portfoliójának megléte is, megkönnyítve a digitális ügyintézésre történő átállást az államigazgatás szereplőinek. Ezek alapja a Központi Azonosítási Ügynök (KAÜ) mint a polgárok elektronikus azonosítását biztosító szolgáltatás.

Gyengeség, hogy a fejlesztések szigetszerűek, azok összehangolásáért egyetlen szervezet sem felelős. A közigazgatási adatvagyon jelenleg csak korlátozottan hozzáférhető. Megoldandó feladat továbbá a dinamikus és a gazdaságilag is életképes startup vállalkozások beindítása, valamint a vállalkozások és a társadalom digitális kompetenciáinak fejlesztése is. Veszélyt jelenthet Magyarország kitettsége a globális szolgáltatóknak, ami nemcsak a sérülékenységeket növelheti, de megnehezítheti a magyar nyelv használatát is a digitális korban. Veszélyt jelent az is, ha a munka kiszervezésben hazánk versenytásaiként jelentkező országok fejlesztési üteme következtében Magyarország lemarad a globális versenyben.

---

[109] Ezen belül legfontosabb a zalaegerszegi autonómjármű- és okosváros-tesztpálya (ZalaZone), amely képes a digitális és a fizikai világ integrációjára a rugalmas tesztelési lehetőségek megteremtése érdekében. Az autonóm járművek közúti tesztelésére vonatkozó szabályozás megléte emellett lehetőséget biztosít az autonóm járművek közúti forgalomban történő, területi és időkorlát nélküli tesztelésére.

[110] A Stratégia öt petaflops (5×10^{15} lebegőpontos művelet másodpercenként) magyarországi szuperszámítási (High Performance Computing – HPC) kapacitás kialakítását írja elő a magyar kutatóhálózat nemzetközi bekapcsolódásának támogatására 2022. március 31-ig. A Kormányzati Informatikai Fejlesztési Ügynökség (KIFÜ) 2022 szeptemberében kezdte meg a „Komondor" szuperszámítógép telepítését a Debreceni Egyetem Szuperszámítógép Központjában.
ÖTVÖS Zoltán: Hamarosan üzembe áll a nagy teljesítményű Komondor. Magyar Nemzet, 2022.10.29. https://magyarnemzet.hu/lugas-rovat/2022/10/levente-es-a-komondor; letöltés: 2022.11.10.

Célok

A Kormány az egészségügyre és a biztonsági szektorra fókuszálva felkészíti az államigazgatást az adat- és MI-vezéreltségre, ezzel is motiválva a társadalom felelős adatvagyon-gazdálkodását. Ehhez a szabályozási (jogi) kereteket is megteremti. Fontos cél az ország digitális szuverenitásának építése is, amelyet a saját erőforrások felhasználása mellett elsősorban az Európai Unió közös digitális piacépítési törekvéseiben történő részvétellel lehet megvalósítani. A Stratégia a 2030. évre[111] a régiós átlagot meghaladó, MI által indukált 15%-os GDP-növekményt, a magyar vállalati szektorban foglalkoztatottanként 26%-os termelékenységnövekedést, valamint egymillió munkavállaló magasabb hozzáadott értékű munkavégzésének megvalósulását jelöli ki fő célként.

Cselekvési terv

A mesterséges intelligencia adta lehetőségek széles körű kiaknázása érdekében először a társadalom felkészítésére, az alapvető feltételek megteremtésére van szükség, amelyeket a Stratégia *alapozó pillérekként* nevesít. Ezen alapvető feltételek belső és külső tényezőkre bonthatók. A belső alapfeltételeket az *MI-értéklánc* elemei teremtik meg:

- adatgazdaság beindítása: az adatfeldolgozást és az adatelemzést végző alkalmazások működéséhez alapvető a magán- és az állami adatokat tartalmazó adattömegek mint a jövő nyersanyagának rendelkezésre állása; elengedhetetlen a jogi szabályozás megléte, az adatgazdák jogainak érvényesülése is; a biztonságos, szabályozott megosztás és a másodlagos felhasználás érdekében adatpiacplatformot kell beindítani; a közszférában keletkezett adatkészletek megosztását a Nemzeti Adatvagyon Ügynökség (NAVÜ)[112] koordinálja majd;

- kutatás-fejlesztés-innováció: az MI kutatási kiválóság technológiai fókuszterületei a gépi érzékelés; a gépi tanuláson alapuló intelligens gyártás és logisztika, az IoT-megoldások fejlesztése; a nyelvtechnológia fejlesztése magyar nyelvre a nagy nyelvek szintjére; az MI megbízhatóságának fejlesztése; az adatok anonimizációját lehetővé tevő technológiák; az MI matematikai alapjainak fejlesztése; emellett az iparági fókuszterületek az egészségügy, a gyártás, az agrárium, az államigazgatás, valamint a hadiipar; a K+F+I-erőfeszítések összehangolását a Mesterséges Intelligencia Nemzeti Laboratórium[113] végzi;

---

111 A 2020-as bázisévhez képest.

112 Megalakult a Nemzeti Adatvagyon Ügynökség. Magyarország Kormánya, 2020.10.20. https://kormany.hu/hirek/megalakult-a-nemzeti-adatvagyon-ugynokseg; letöltés: 2021.05.26.

113 A MILAB 2020 szeptemberében az Eötvös Loránd Kutatási Hálózat Számítástechnikai és Automatizálási Kutatóintézete (SZTAKI) vezetésével jött létre.
A SZTAKI vezetésével elindult a Mesterséges Intelligencia Nemzeti Kutatólaboratórium és az Autonóm Rendszerek Nemzeti Kutatólaboratórium. SZTAKI, 2020.09.25.
https://www.sztaki.hu/kormanyzat/hirek/sztaki-vezetesevel-elindult-az-mi-es-az-autonom-nemzeti-kutatolaboratorium; letöltés: 2021.05.26.

- a technológia alkalmazásának ösztönzése: az MI-fejlesztések minél nagyobb számban történő megvalósulása érdekében szükség van a kísérletező szervezeti kultúra erősítésére (speciális finanszírozási lehetőségekkel is), technológiai piactereket kell létrehozni, valamint tanácsadókat és trénereket kell biztosítani a vállalatok számára; az ITM 2021 MI-alapú vállalati tanácsadó szolgáltatásokat (csetbotokat) fejlesztett,[114] amelyek integrálhatók a tervezett kormányzati hangalapú MI-platformhoz is.

Az *MI-keretek* a mesterséges intelligencia elterjedésének külső feltételei:

- oktatás, kompetenciafejlesztés: a társadalom széles rétegei digitális kompetenciáinak növelése és az MI-ben rejlő lehetőségek és veszélyek tudatosítása mellett szükséges az MI elterjedéséhez elkerülhetetlen adatspecialista, fejlesztői és kutatói szakembergárda célzott képzése, illetve a leszakadásban érintett rétegek[115] támogatása és a tehetséggondozás; e célok támogatása érdekében MI Innovációs Központ jön létre;[116]

- infrastruktúra fejlesztése: a kutatás-fejlesztési tevékenység gépi erőforrásainak (szuperszámítógép, felhőalapú szoftver- és/vagy szolgáltatásrendszer) biztosítása, az MI kutatás-fejlesztés számára releváns adatkészletek kutathatóvá, illetve felhasználhatóvá tétele, célszoftverek rendelkezésre bocsátása, erősen védett virtuális környezetek (Sandbox) és tesztkörnyezetek kialakítása, valamint bekapcsolódás az EU-s MI-kutatásokba és -fejlesztésekbe;[117]

- egyértelmű szabályozási környezet: cél egy általános adatvagyonszabályozási környezet kiépítése, beleértve a közadatvagyon MI-célú felhasználásának támogatását, valamint az etikai keretrendszer[118] kialakítását; ennek érdekében kialakítják a Mesterséges Intelligencia Szabályozási és Etika Tudásközpontot (MISZET).

---

[114] A program első lépéseként a Modern Vállalkozások Programjának virtuális tanácsadója (eMI) 2022 nyarától elérhető.
Új kollégát igazoltunk! Megérkezett eMI, a Modern Vállalkozások Programjának virtuális tanácsadója! Modern Vállalkozások Programja, 2022.08.17.
https://vallalkozzdigitalisan.hu/hirek/hir?id=917; letöltés: 2022.11.10.

[115] Fogyatékkal élők, idősek, digitális analfabéták, alacsony iskolázottságúak.

[116] Az MI-alkalmazások széles körű elterjesztéséért felelős MI Innovációs Központ részeként zalaegerszegi és debreceni székhellyel két akcelerátor központ is megnyílt, ahol a kkv-k konzultációs trénerek segítségével ismerkedhetnek meg az egyes MI-alapú technológiákkal. A közeljövőben továbbá Balatonfüreden létesül hasonló akcelerátor adat és MI-hangsúllyal.
A mesterséges intelligencia stratégia megvalósítása az MI-alkalmazások bevezetését segítő központok létrehozásával folytatódik. MI Koalíció, 2021.06.17.
https://ai-hungary.com/hu/hirek/sajtomegjelenesek-kozlemenyek/a-mesterseges-intelligencia-strategia-megvalositasa-az-mi-alkalmazasok-bevezeteset-segito-kozpontok-letrehozasaval-folytatodik; letöltés: 2021.07.19.

[117] EU Digital Single Market.

[118] MI Etikai Kódex.

Szektorális fókuszok

Magyarország a digitális gazdaságban meglévő erősségei alapján a Stratégia szektorspecifikus fejlesztési fókuszokat határozott meg:

- gyártás és autonóm rendszerek: MI-alapú, folyamatvezérelt, környezettudatos okosgyártás kis-, közép- és nagyvállalati szinten;
- adatvezérelt egészségügy: az egészségügyi adatvagyon felelős használata, a mesterséges intelligencia diagnosztikai és gyógyítási alkalmazásának erősítése, az MI által támogatott orvosi döntéshozatal és orvostechnológiai eszközök fejlesztése és bevezetése;
- integrált, digitális agrárium: a meglévő adatvagyon strukturálása, fejlesztése, robotrendszerek innovációja; az autonóm rendszerek alkalmazásának ösztönzésére Digitális Agrárakadémia,[119] az élelmiszerellátási lánc optimalizálásának elősegítésére Nemzeti Élelmiszerlánc Adatszolgáltatási Központ (NÉAK) jön létre;[120]
- adatvezérelt szolgáltató állam: a közszolgáltatások elektronikus elérésének, digitalizációjának elősegítése, illeszkedve a már meglévő e-közigazgatási rendszerekbe;
- közigazgatási folyamatok (ügyfélszolgálat, határozathozatal, adózás, rendvédelem, határvédelem, katasztrófavédelem, honvédség, nemzetbiztonság) MI segítségével történő automatizációja;
- energetika: adatalapú, személyre szabott energiaszolgáltatás;
- logisztika: a logisztikai adatvagyon felépítése, MI-alapú elosztás bevezetése;
- közlekedés: cél, hogy Magyarország a szektorban az innováció formálójává és nemzetközi pilotok területévé váljon; a fejlesztések fókuszában az okosváros-koncepciók fejlesztése áll, kiemelt figyelemmel a forgalomirányításra.

[119] Az Akadémia tananyagát a szakmában dolgozó szakemberek állították össze a Nemzeti Agrárgazdasági Kamara szervezésében. Célja, hogy a magyar gazdálkodók digitáliskompetencia-szintjét növelve segítse a gazdálkodás hatékonyságát, illetve hogy gépesítéssel és a digitális megoldások elterjedésével csökkentse a munkaerőhiányt.
Digitális Agrárakadémia.
https://www.digitalisagrarakademia.hu/; letöltés: 2021.07.20.

[120] A NÉAK célja, hogy az információk gyűjtésével, elemzésével, majd hasznosításával segítse az élelmiszerlánc-szereplők versenyképességének, tudásszintjének, illetve teljesítményének növelését. Létrehozása 2021 februárjában lépett a megvalósítási szakaszba. A Központ teljes körű megvalósításának végső határideje 2023. december 31.
Új szakaszba lépett a Nemzeti Élelmiszerlánc Adatszolgáltatási Központ projekt. nébih, 2021.02.01.
https://portal.nebih.gov.hu/-/uj-szakaszba-lepett-a-nemzeti-elelmiszerlanc-adatszolgaltatasi-kozpont-projekt; letöltés: 2021.07.20.

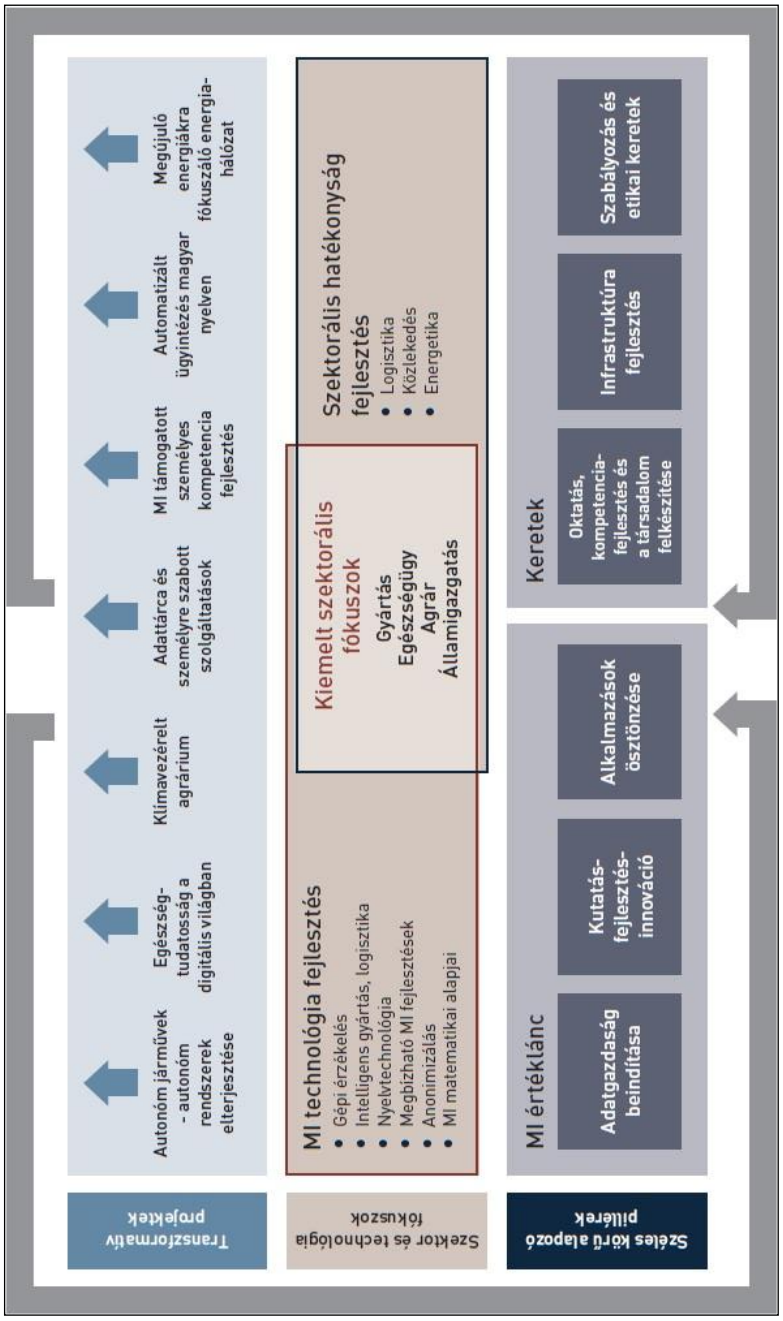
Transzformatív programok

A programok az érintett ágazat átalakulását és a széles társadalom mindennapos MI-alkalmazását célozzák, kiválasztásuknál kiemelten figyeltek azok munkaerőpiaci hatására:

- autonóm járművek: a közlekedés MI-alapúvá tétele mellett a fejlesztések alapul szolgálhatnak a hadiipar számára is;
- egészségtudatosság a digitális világban: a már jelenleg is elérhető (Elektronikus Egészségügyi Szolgáltatási Tér, betegtájékoztatás) és a bevezetés alatt álló új szolgáltatások felügyelt ajánlása és használata; az állami egészségügyi adatbázisok kiegészítése az állampolgári okoseszközök adataival és saját naplózással;
- klímavezérelt agrárium: az éghajlatváltozás hatásainak mérséklése és a károsanyag-kibocsátás csökkentése prediktív, MI-alapú analitikai módszerekkel, a betakarítás idejének optimalizálásával stb.;
- adattárca és személyre szabott szolgáltatások: az EU általános adatvédelmi rendelete (GDPR[121]) érvényesítése érdekében lehetővé kell tenni, hogy az állampolgárok könnyen és biztonságosan eldönthessék, hogy a vállalatok mit tehetnek az üzleti szerződések keretében róluk felvett vagy általuk magukról gyűjtött adatokkal; az adatok kezelésének az állampolgárok számára átláthatóan és ellenőrizhetően kell történnie;
- MI által támogatott személyes kompetenciafejlesztés digitális asszisztenssel;
- automatizált ügyintézés magyar nyelven: a magyar nyelvre optimalizált rendszerek használata az állami és a magán ügyfélszolgálatokban, a nagy elektronikus személyiasszisztens-szolgáltatók (Siri, Alexa, Google Assistant, Cortana) legyenek elérhetők magyar nyelven, az angol nyelvű tartalmak automatikus fordítása a nagy nyelvek szintjén történjen; a kialakításra kerülő megoldások alkalmazhatóvá válhatnak a védelmi és a biztonsági célú alkalmazások esetén is;
- megújuló energiákra fókuszáló energiahálózat: az időjárásfüggő megújuló energiák pontosabb termelési menetrendezése, az okosmérők és az okoshálózat (*smart grid*) technológiák bevezetése.

Az MI-értéklánc és az MI-keretek által megalapozott technológiai és szektorális fókuszterületeket (széles körű alapozó pillérek), a szektor-, illetve a technológiafókuszokat, valamint a társadalmat közvetlenül érintő transzformatív projekteket az ábra foglalja össze.

[121] General Data Protection Regulation, vagyis általános adatvédelmi rendelet, amely 2016. május 24-én lépett hatályba és 2018. május 25-től kell alkalmazni.
Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). https://eur-lex.europa.eu/HU/legal-content/summary/general-data-protection-regulation-gdpr.html; letöltés: 2022.10.25.



5. ábra. Az MI-értéklánc és az MI-keretek által megalapozott technológiai és szektorális fókuszterületek, illetve a társadalmat közvetlenül érintő transzformatív projektek Magyarország Mesterséges Intelligencia Stratégiájában
Magyarország Mesterséges Intelligencia Stratégiája 2020–2030. Digitális Jólét Nonprofit Kft., 2020. május. p. 22.
https://ai-hungary.com/api/v1/companies/15/files/137203/view; letöltés: 2022.03.21.

Összegzés, értékelés

Magyarország Mesterséges Intelligencia Stratégiája korszerű, jól strukturált, átgondolt és közérthetően megfogalmazott dokumentum, amely kiváló alapot ad hazánk digitalizációjának előmozdítására. Hasznosságához nagyban hozzájárul, hogy elkészítésében a szektorban érdekelt szereplők széles köre is aktívan részt vett, ami a jó kormányzás egyéb területei számára is példamutató. A Stratégia jól megragadja az MI okozta változások transzformatív jelentőségét. Ambiciózus, de elérhető célokat fogalmaz meg, amelyek teljesülése nemcsak az ország gazdasági teljesítőképességét növelheti, de nagyban hozzájárulhat ahhoz is, hogy a társadalom felkészültebb legyen a mesterséges intelligencia elterjedésének ma még beláthatatlan következményeire.

A dokumentum készítőinek alapállása, hogy hazánk a nemzetközi közösség teljes értékű, szuverén szereplője, ezért fontos, hogy a partnereinkkel, elsősorban az Európai Unióval szorosan együttműködve, de saját erőforrásainkra és erősségeinkre is építve fejlesszünk.

Az MI-fejlesztések rendkívül szerteágazó világában és a korlátozott erőforrásokra tekintettel különösen hasznos, hogy a fejlesztések irányait a hazai sajátosságokra is tekintettel határozták meg. Biztató, hogy a Stratégia elfogadása óta több intézkedés a koronavírus-világjárvány ellenére is megvalósult.

A MESTERSÉGES INTELLIGENCIA KATONAI ALKALMAZÁSA

A katonai alkalmazás általános trendjei és technológiái

Az MI terjedésével a jelenlegi technológiai színvonalat képviselő haditechnikai eszközök fokozatosan korszerűtlenné válnak, ezzel felborulhat a korábban kialakult katonai erőegyensúly. Az ellenfél képességeit lebénító, meglepetésszerű, gyors lefolyású, új technológiákat alkalmazó hadviselés (*hyperwar*), illetve az ember nélküli (*human off the loop*) technológiák elterjedése várhatóan nagymértékben felgyorsítja a hadviselés műveleti tempóját. A fegyveres konfliktusok kimenetelét meghatározó tényezők száma megsokszorozódik, tovább nehezítve az előrejelzést.

A technológia hatására nemcsak az államok közötti erősorrend változhat meg, de szélsőséges esetben nem állami szereplők is jelentős katonai képességekre tehetnek szert, elsősorban a fejlődő térségekben gyengítve ezzel az államok erőszakmonopóliumát.

A potenciális előnyök, valamint az új technológia kiváltotta biztonsági dilemma az MI területén is fegyverkezési versenyt indítottak el. A szakértők körében általános vélekedés szerint az MI-technológiát nem alkalmazó haderők 10–15 éven belül jelentős hátrányba kerülnek.[122]

Közép- és hosszú távon a fejlett haderők összetételének drasztikus megváltozásával kell számolni. Az intelligens gépek elterjedésével az élőerő létszáma csökkeni fog, és a megmaradt személyi állomány összetétele is változik. Elsősorban az informatikai tudás válik majd nélkülözhetetlenné, míg csökken a fizikai állóképesség jelentősége.[123] A jövő katonáinak egy része az e-sportokban tehetséges fiatalokból kerül majd ki, akik képesek áttekinteni a digitális harcmezőt, alkalmasak több eszköz párhuzamos működtetésére, illetve gyorsan tudnak reagálni az eseményekre.[124]

Csökkenhet a háborúk politikai és anyagi költsége, ha nem lesz szükség a katonák harctéri jelenlétére, és csökkenthető a polgári áldozatok (járulékos veszteségek) száma is. Az MI elterjedésével elérhető hatékonyságnövekedés (adminisztratív feladatok, kiképzés, műveletek stb. költségeinek csökkenése) a katonai összkiadásokat is csökkentheti, de egyelőre nem felbecsülhetők az MI-rendszerek várható fenntartási költségei.

---

[122] Egy lövészkatona például nem lesz képes felvenni a versenyt egy robottal állóképesség, kitartás, túlélőképesség, reakcióidő, pontosság stb. terén.

[123] Bizonyos szintű fizikai állóképességre azonban szükségük lesz a technológiát kezelő katonáknak is, elsősorban annak a pszichés állapotra és a munkabírásra gyakorolt hatásai miatt.

[124] Egy katona irányíthat/felügyelhet például egy szakasznyi vagy századnyi robotot.

Az új MI-rendszerek meggyorsíthatják az információ kinyerését, feldolgozását és terjesztését, a gépi döntéshozatali, illetve döntéstámogató megoldások pedig az emberi döntések minőségét is javíthatják. Becslések szerint az emberi munkaerő a jelenleg rendelkezésre álló információ legfeljebb 20%-át képes feldolgozni. Az MI az alábbi módokon támogathatja a döntéshozatalt:

- az információ vizualizálásával, összegzésével és értelmezésével, az önmagukban értéktelen információk kontextusba helyezésével;
- az adatfolyamokban szereplő releváns információ automatikus kinyerésével (pl. a képi forrású hírszerzés területén a megfigyelési kamerák és a műholdak felvételeinek feldolgozása során);
- az anomáliák kiemelésével (a rendelkezésre álló információ és a referenciaértékek összevetése által);
- a lehetséges helyes cselekvési változatok és azok várható hatásainak bemutatásával;
- előrejelzés biztosításával (pl. az ellenség várható cselekvésével kapcsolatban);
- javíthatják a védelem reagálóképességét nagy sebességű fegyverrendszerekkel (pl. hiperszonikus és kibereszközökkel, valamint energiafegyverekkel) szemben.

A jelenlegi autonóm robotrendszerek[125] használata elsősorban az egyszerű, a fizikailag nehéz vagy a veszélyes feladatok végrehajtásának támogatására korlátozódik. A segítségükkel kiváltható továbbá az emberi erőforrás munkája az egyhangú, egyszerű munkafolyamatok sokszori ismétlését követelő feladatokban is, csökkentve a balesetek kockázatát és felszabadítva az emberi munkaerőt az összetettebb feladatok végrehajtására. A katonai felhasználások között szerepelnek a tűzszerészet, a szárazföldi és a tengeri aknamentesítés, a mentés, a logisztikai támogatás, illetve az egyszerűbb harci feladatok.

A halálos autonóm fegyverrendszerek[126] fejlesztésében élen járó Amerikai Egyesült Államok, Kína és Oroszország ellenzik azok alkalmazásának teljes körű betiltását. Indoklásuk szerint az ilyen eszközök alkalmazásával kevesebb lenne a polgári áldozat a fegyveres konfliktusokban[127] és csökkennének a katonai kiadások. Egyes vélekedések szerint a Nyugat hátrányba kerülhet az etikai kérdéseket a feltételezések szerint kevésbé figyelembe vevő Oroszországgal és Kínával szemben. A technológia ellenzői szerint az autonóm fegyverrendszerek elterjedésével kérdésessé válna a felelősség megállapítása a szabálytalan vagy hibás támadások esetében.[128] A teljesen autonóm vagy széles körű autonómiával felruházott fegyverrendszerek bevetése esetén egyáltalán nincs lehetőség az egyéni büntetőjogi felelősség megállapítására. A fegyvert használó felelőssége kizárólag azon fegyverek alkalmazása esetén állapítható meg, ahol

[125] Robotic autonomous systems.
[126] Lethal Autonomous Weapon System – LAWS.
[127] Érvelésük szerint a megfelelően programozott rendszerek – egyebek mellett az érzelmi faktor kiiktatásával – az embereknél megfelelőbb döntéseket lennének képesek hozni, jobban megfelelve az erkölcsi, etikai és jogi követelményeknek.
[128] Úgynevezett felelősségrevonási hézag (*responsibility gap*).

megvalósul az MI-eszköz feletti érdemi emberi ellenőrzés.[129] A parancsnoki felelősség[130] koncepciója sem alkalmazható a harcos–gép viszonyrendszerben, mert az jelentősen eltér az emberi parancsnok és az emberi alárendelt közötti kapcsolattól. Az autonómia fokai:

- integráció: az emberi kezelők nagyfokú ellenőrzése az autonóm rendszerek felett;[131]
- automatizáció és részleges autonómia: az MI-rendszerek önállóan hozzák a döntéseiket, de az emberi kezelők leállíthatják a tevékenységüket;[132]
- teljes autonómia: az emberek nem vesznek részt a döntéshozatalban és nem áll módjukban az autonóm rendszerek leállítása.[133]

A robothadviselésben hosszú távon nem tartható fenn az érdemi emberi ellenőrzés, hiszen két autonóm roboteszköz összecsapása esetén az autonómia foka kulcstényező: az emberi döntésre várakozó eszköz döntő hátrányba kerül. Harari etikai szempontból is összességében a robotrendszereket látja hatékonyabbnak, hiszen a fejlett algoritmusokkal felszerelt robotrendszerek az embereknél könnyebben hozhatnak a mindenkori hadijognak megfelelő döntéseket.[134]

Az MI-rendszerek elterjedése tovább fokozza a haderők kibervédelmi kihívásait. Az MI-vel támogatott kibervédelmi rendszerek hatékonysága nagyban meghaladja a jelenleg alkalmazott technológiáét. A kiberincidensek feltárása során az MI a nagyadat-elemzés segítségével hatékonyan segíti a szakemberek munkáját.[135]

A haditechnikai fejlődéssel a háborúk megvívása egyre kevésbé zajlik majd emberi időkeretek között. A kiberhadviselés időkerete mindössze percekre szűkülhet le, lehetetlenné téve az emberi tényező érdemi részvételét.[136]

A mesterséges intelligencia segítségével könnyebbé és hatékonyabbá tehetők a kártékony szoftverek szűrésére szolgáló tűzfalak. A káros szoftverek (*malware*) előre meghatározott (betáplált) mintái alapján a célszoftver a már azonosított fenyegetések mellett megtanítható az ismeretlen mintázatok felismerésére is.

Az MI-t alkalmazó viselkedésanalitika a felhasználók rendszerhasználatát elemezve akkor is felismeri (feltételezi) a jogosulatlan tevékenységet, ha a támadók érvényes azonosítókkal rendelkeznek.[137]

---

129 Meaningful human control. Ennek jelentőségét növeli, hogy az ellenőrzés hiányában akaratlagos, de törvénytelen vagy etikátlan halálokozás esetén lehetőség adódhat „rendszerhibára” hivatkozni.
130 Commander’s responsibility.
131 Humans in the loop.
132 Humans on the loop.
133 Humans off the loop.
134 HARARI, Yuval Noah: Homo Deus: A jövő rövid története. p. 267.
135 A katonai felhasználás lehetőségeire vonatkozó információk forrása a NATO Parlamenti Közgyűlése Technológiai és Biztonsági Albizottsága által 2019. október 13-án elfogadott jelentés.
TONIN, Matej: Artificial Intelligence: Implications for NATO’s Armed Forces. NATO Parliamentary Assembly, 2019.10.13.
136 HARARI, Yuval Noah: Homo Deus: A jövő rövid története. p. 266.
137 A NATO tallinni Kibervédelmi Kiválósági Központjának kiadványa.

Az úgynevezett kiber-kiképzőtereken (*cyber range*) az MI segítségével szimulálhatók a kiberincidensek, illetve a kibervédelmi eszközök működése.[138]

Az új technológiák kihívásokat állítanak a meglévő, a hagyományos technológiákra összpontosító fegyverzetellenőrzési rezsimek számára is. Idővel egyes MI-technológiák és -eszközök kettős felhasználású termékeknek minősülhetnek, és kiterjeszthetik rájuk is az ilyen termékek külkereskedelmi forgalmának ellenőrzését célzó intézkedések hatályát.[139]

Az MI-rendszerek katonai felhasználását számos nem technológiai tényező hátráltatja. A technológiát jellemzően olyan magánvállalatok biztosítják, amelyek felett a haderők nem gyakorolnak ellenőrzést, és amelyek a katonaitól merőben különböző szervezeti kultúrát képviselnek. A rendkívül gyorsan fejlődő MI-eszközök rendszeresítését hátráltatják továbbá a merev beszerzési rendszerek is. Az MI-fejlesztések további gátja a megfelelően képzett szakemberek alacsony száma. A haderők helyzete különösen nehéz, hiszen a feladat végrehajtására potenciálisan alkalmas, magas szintű informatikai képzettséggel rendelkező jelöltek jellemzően nem felelnek meg a katonai szervezetek által támasztott magatartási és fizikai követelményeknek. A fejlett haderők jelenleg azt fontolgatják, hogy az MI-rendszerek fejlesztésével és üzemeltetésével kapcsolatos feladatokat részben vagy egészben nem katonákkal hajtják végre, de ennek szervezeti vonatkozásai, személyi követelményei egyelőre nem világosak.[140]

Az MI-algoritmusok programozásához (tanításához) és működtetéséhez nagy mennyiségű megfelelően strukturált adat szükséges. A katonai alkalmazás során a rendelkezésre álló adatmennyiség – például az ellenség harceljárásairól, a műveleti helyzetről stb. – összehasonlíthatatlanul kevesebb a kereskedelmi felhasználási területekhez képest.[141] Az ellenséges megtévesztő tevékenység tovább nehezíti a polgári felhasználású eszközök hatékony szereplését a harcmezőn.

TYUGU, Enn: Artificial Intelligence in Cyber Defence. CCD COE Publications, 2011. https://www.ccdcoe.org/uploads/2018/10/ArtificialIntelligenceInCyberDefense-Tyugu.pdf; letöltés: 2019.12.06.

138 ROUSE, Margaret: Cyber Range. Techopedia, 2012.06.06. https://techopedia.com/definition/28613/cyber-range; letöltés: 2019.12.06.

139 2019 Disruptive Technology for Defence Transformation. A Defence iQ és a brit Védelmi Akadémia 2019. szeptember 24–26-án Londonban rendezett konferenciája.

140 Könnyű amellett érvelni, hogy az IT-szakembereknek nincs szükségük katonai ismeretekre irodai feladataik ellátásához. Nehézséget jelent ugyanakkor, ha nem képesek együttműködni a katonai állománnyal, vagy nem értik azok igényeit, hiszen nincsenek tisztában a feladataikkal. Ennél is jelentősebb kihívás, hogy az IT-szakembereknek sok esetben jelen kell lenniük a hadszíntéren is, ahol önmagukra és társaikra is veszélyt jelenthetnek, amennyiben nem rendelkeznek a kellő ismeretekkel.

141 Tulajdonképpen a háború Carl von Clausewitz által „köd- és felhőszerű lényhez” hasonlított természetéről van szó: a katonai vezetőknek töredékesek a hadműveleti területtel, elsősorban az ellenséggel kapcsolatos információik. Banális példa, miszerint egy IMINT-felvételen kilövés előtt álló sorozatvető-rakétalövedéknek tűnő tárgyról kiderülhet, hogy a valóságban egy fúrt kútról van szó. Az automatikus rendszereket nehéz megtanítani hasonló esetekben a különbség – tapasztalt emberi döntéshozóknak is kihívást jelentő – megállapítására.

Nehézség, hogy a tanulás során az MI-rendszerek gyakran átveszik az emberi előítéleteket és hibákat. Különösen nehéz az olyan algoritmusok fejlesztése, amelyek a korábban ismeretlen problémákat is képesek megoldani. Ez azért fontos feladat, mert a háborúnak és a fegyveres konfliktusnak alapvető ismertetőjegye az állandó változás és kiszámíthatatlanság, ezek leküzdésének évezredek óta a haderő magas szintű felkészültsége és a parancsnokok „jó szemmértéke", vagyis képzettsége és intuíciója volt az egyetlen bevált módszere.

Az MI-rendszerek adatfüggősége megnöveli azok kitettségét a manipulálásnak és a dezinformációnak, mert az adatok kismértékű megváltoztatása is végzetes következményekkel járhat. Kockázatot jelent továbbá, hogy az MI-rendszerek eltulajdonításával vagy kiberhírszerzéssel rendkívül részletes információ nyerhető az azokat alkalmazó szervezetekről és tevékenységükről.

Az MI-rendszerek megbízhatósága jelenleg a katonai alkalmazások széles köre vonatkozásában elégtelen, tekintettel a hibák potenciális következményeire. Jelentős kihívást jelent, hogy az MI-rendszerek döntési folyamatai általánosságban rendkívül nehezen visszakövethetők, aminek következtében e rendszerek lényegében „fekete dobozként" működnek.

Az MI-rendszerek váratlan és tömeges összeomlása (*flash crash*) beláthatatlan következményekkel járhat a korszerű haderők vonatkozásában. A technológia bevezetése ezért kis lépésekben, kísérleti jelleggel kezdődött meg.[142]

NATO

A NATO-tagállamok állam- és kormányfői először a 2021 júniusi brüsszeli csúcstalálkozó zárónyilatkozatában nevesítették az új és felforgató technológiák (EDT[143]) okozta új kihívásokat. A csúcstalálkozó megállapította a kutatás-fejlesztés-innováció jelentőségét a felforgató technológiák nyújtotta lehetőségek kiaknázásban és a kihívások ellensúlyozásában. Megállapodtak egy innovációs alap[144] létrehozásában a kettős felhasználású új és felforgató technológiákat fejlesztő startupok támogatására.[145]

A NATO-tagállamok védelmi miniszterei 2021 februárjában fogadták el a NATO EDT-stratégiáját.[146] A stratégia célja, hogy a NATO képes legyen a felforgató technológiák alkalmazására és az azok elleni fellépésre. Támogatja a kettős felhasználású technológiák fejlesztését és a tagállamok közötti tapasztalatcserét a területen. A stratégia hét kulcsterületet nevesít: mesterséges intelligencia, adat és számítástechnika, autonómia, kvantumtechnológia, biotechnológia és az ember gépi

142 TONIN, Matej: Artificial Intelligence: Implications for NATO's Armed Forces. NATO Parliamentary Assembly, 2019.10.13.

143 Emerging and Disruptive technologies: mesterséges intelligencia, 5G, irányított energiájú és hiperszonikus fegyverek, űreszközök, új anyagmegmunkálási technológiák, kvantummechanika, biotechnológia.

144 Innovation Fund.

145 Brussels Summit Communiqué. NATO, 2021.06.14. https://www.nato.int/cps/en/natohq/news_185000.htm; letöltés: 2021.12.30.

146 Coherent Implementation Strategy on Emerging and Disruptive Technologies.

kiterjesztése, hiperszonikus eszközök, űreszközök.[147] A NATO külön stratégiát is kidolgoz mind a hét terület vonatkozásában. Ezek közül először az MI-stratégia[148] került elfogadásra a védelmi miniszterek 2021 októberi találkozóján. A stratégia az MI felelős felhasználásának elveire, az MI-képességek Szövetség általi kialakítására és az azok elleni védelem lehetőségeire összpontosít.[149]

A NATO feladatának tekinti a kutatás-fejlesztésben meglévő globális fölényének megőrzését, amiben az MI kulcsszerepet játszik. A Szövetség célja, hogy a tagok technológiai fejlettsége közötti különbség ne akadályozza a NATO-haderők interoperabilitását. Tekintve, hogy az MI területén nem kizárólag a tőkeintenzív fejlesztések eredményezhetnek jelentős előrelépést, a Szövetség MI-képességeinek növelésében a kisebb tagállamoknak is jelentős szerepet szánnak. A fejlesztéseket a tagállamok haderői mellett a magánszférával és az Európai Unióval együttműködve tervezik véghezvinni.

Az MI kutatásával számos NATO-szervezet foglalkozik:

- a NATO Tudományos és Technológiai Szervezete[150] az MI és a nagy adat felhasználását a katonai alkalmazások, a döntéshozatal és az autonóm rendszerek területén a kutatás-fejlesztés kiemelt fókuszterületeként jelölte meg; a kutatási területek az MI érdemi emberi ellenőrzése, a kibervédelem és az MI-támogatta információs rendszerek;
- a Szövetséges Transzformációs Parancsnokság[151] több konferenciát szervezett az MI jelentette lehetőségek és kihívások témakörében;
- a NATO Híradó és Informatikai Ügynöksége[152] a nagyadat-elemzés, az adat vizuális megjelenítése és az információs műveletek ellen alkalmazható gépi tanulási megoldások fejlesztésére összpontosít;
- végül a NATO Ipari Tanácsadó Csoportjának[153] kutatásai a nagy adat felhasználási lehetőségeire és az autonóm rendszereknek a NATO tervezési és műveleti rendszerére gyakorolt hatásaira összpontosítottak.

A NATO a nagyadat-kezelési és a gépi tanulási megoldásokat az afganisztáni Határozott Támogatás Műveletben[154] keletkezett adatokban fellépő duplikációk kiszűrésére, illetve az informatikai rendszerek naplófájljaiban (log fájl) megjelenő anomáliák felfedésében is alkalmazta.[155]

---

147 Más források az irányított energiájú fegyvereket is a felforgató technológiák közé sorolják.
148 Summary of the NATO Artificial Intelligence Strategy. NATO, 2021.10.22. https://www.nato.int/cps/en/natohq/official_texts_187617.htm; letöltés: 2021.12.30.
149 Emerging and disruptive technologies. NATO, 2021.06.03. https://www.nato.int/cps/en/natohq/topics_184303.htm; letöltés: 2021.12.30.
150 NATO Science and Technology Organization – NATO STO.
151 Allied Command Transformation – ACT.
152 NATO Communications and Information Agency – NCI.
153 NATO Industrial Advisory Group – NATO NIAG.
154 Resolute Support Mission – RSM.
155 TONIN, Matej: Artificial Intelligence: Implications for NATO's Armed Forces. NATO Parliamentary Assembly, 2019.10.13.

Amerikai Egyesült Államok

Az Amerikai Egyesült Államok biztonság- és védelempolitikai alapelveit a 2022-es Nemzeti Biztonsági Stratégia,[156] a Nemzeti Védelmi Stratégia[157] és a 2018-ban kidolgozott, majd 2019. július 12-én részben nyilvánosságra hozott Nemzeti Katonai Stratégia[158] rögzíti.

A Nemzeti Biztonsági Stratégia három kulcsfontosságú területet állapít meg, amelyek meghatározóak az ország biztonsága szempontjából. Az első és legfontosabb a főként kínai, részben orosz stratégiai kihívásokra történő reagálóképesség fejlesztése, a hazai ipar teljesítőképességének és innovációjának növelése, valamint a klímaváltozás hatásainak csökkentése.

A stratégia alapján az Amerikai Egyesült Államok fő nemzeti érdeke továbbra is a lakosság védelme, a gazdasági lehetőségek bővítése, valamint az amerikai életforma alapját képező demokratikus értékek megvédése. A kitűzött célok elérése érdekében a kormány minden elérhető nemzeti erőforrással és eszközzel erősíteni kívánja az amerikai befolyást és érdekérvényesítést, valamint nemzetközi koalíciót kíván építeni a globális stratégiai környezet alakítása és a közös kihívások kezelése érdekében. Utóbbiak teljesítését a haderő modernizációja által kívánja megvalósítani, amely az elkövetkező nagyhatalmi versenyre történő felkészülés érdekében szükséges.

A Nemzeti Biztonsági Stratégia a Kínai Népköztársaságot jelöli meg a legfontosabb biztonsági kihívásként, ellentétben a korábbi megközelítéssel, amely az orosz és a kínai fenyegetést egy szinten kezelte. A stratégia szerint a Kínával folytatott nagyhatalmi verseny lesz az elkövetkező évtized legjelentősebb kihívása az Amerikai Egyesült Államok számára, mivel az ázsiai országnak a szándéka és a képessége is rendelkezésre áll a globális stratégiai folyamatok befolyásolására. A dokumentum Oroszországot csak korlátozott veszélyként értékeli az amerikai érdekekre vonatkozóan. A stratégia készítői által prognosztizált versenybe az Amerikai Egyesült Államok a szövetséges országokat saját feltételeikkel kívánja bevonni.

A kormány a magánszektor innovatív szereplőit, a stratégiai ágazatok, illetve a feltörekvő technológiák előállítóit modern ipari stratégiával és állami beruházásokkal kívánja ösztönözni. A kormány a hazai termelési kapacitás bővítését törvényekkel is támogatja, így biztosítva a nemzetvédelem szempontjából kritikus technológiák ellátási láncainak védelmét, hogy megbízható gyártási kapacitással rendelkezzen mind belföldön, mind a szövetségesi rendszerben. A haderőtől elvárja, hogy készen álljon fegyveres konfliktusok megvívására, attól történő elrettentésre erőkivetítéssel,

[156] National Security Strategy. The White House, Washington, October 2022. https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf; letöltés: 2022.11.09.

[157] National Defense Strategy of the United States of America. U.S. Department of Defense, 2022.10.27. https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF; letöltés: 2022.11.09.

[158] Description of the National Military Strategy. The JOint Staff, 2018. https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf; letöltés: 2022.08.12.

valamint legyen képes az amerikai állampolgárok és gazdasági érdekek védelmére. A technológia, a kereskedelem és a biztonság fejlesztését kiemelt fontosságúnak tekinti az indiai–csendes-óceáni térségben és Európában egyaránt, amelyeket egymásra kölcsönösen hatást gyakorló régiókként kezel. A dokumentum szerint az amerikai kormány új gazdasági megállapodásokat kíván kidolgozni a partnerországokkal a nagyhatalmi versenyfeltételeinek kiegyenlítése érdekében, valamint új demokratikus rendszereket is keres a törékeny autokráciákkal szembeni ellenállóság, illetve a fejlődés fenntartása érdekében.

Az Amerikai Egyesült Államok kormánya a közös, mindenkit érintő kihívásokra – például az éghajlatváltozás, az élelmiszer-biztonság, a járványok és az infláció – kettős megközelítést kíván alkalmazni. Egyrészről hajlandó együttműködni a versenytársakkal a nemzetközi intézmények és a szabályalapú világrend keretein belül a kihívások kezelésében. Másrészről a szövetségi rendszer vezető demokráciáival egy kölcsönösen előnyöket biztosító kapcsolati rendszert kíván kialakítani a demokratikus értékek felsőbbrendűségének globális demonstrálása érdekében. Az amerikai kormány a demokratikus értékek védelmét helyezi előtérbe és ennek követésére ösztönöz globálisan.

A Nemzeti Biztonsági Stratégia által megfogalmazott főbb célok:

- az Amerikai Egyesült Államok vezető szerepének megőrzése és az amerikai részvétel a világ gazdasági és biztonsági folyamatainak alakításában;
- a Kínával meglévő kapcsolatrendszer alakítása és kezelése;
- vezető szerep biztosítása a tudományos-technológiai területen;
- a nemzetközi szövetségi rendszer újjáépítése;
- a demokrácia megújítása és védelme, valamint a globális egészségbiztonság erősítése;
- a gazdasági válság mélyülésének megállítása és stabilabb világgazdaság kiépítése;
- a klímaválság kezelése és a megújuló energiaforrások széles körű használatának elősegítése.

Az Amerikai Egyesült Államok nem törekszik semmilyen korábbi állapot visszaállítására a nemzetközi színtéren, hanem a külkapcsolatok, a nemzetbiztonság és a belpolitika terén is új megközelítést kíván alkalmazni. Amerika a jövőben magabiztos és erős helyzetből kívánja megközelíteni a világot a demokratikus értékek védelme érdekében. Ennek keretében a kormány nem vehet részt újabb „végtelen háborúban”, és mindent megtesz az afganisztáni konfliktus felelősségteljes lezárása érdekében, hogy az ország ne nyújthasson menedéket az Amerikai Egyesült Államokkal ellenséges szélsőségeseknek.

A Nemzeti Védelmi Stratégia fókuszában az elrettentés és az ellenálló képesség (reziliencia) áll. Az elrettentést a hadviselés valamennyi dimenziójában és a nemzeti erő egyéb eszközeinek, valamint a szövetségi rendszerek alkalmazásának integrált megközelítésével valósítják meg. Kiemelt feladat a haderő ütőképességének növelése

az új technológiák mihamarabbi rendszerbe állításával. Az Amerikai Egyesült Államok biztonságát és technikai fölényét nagyban befolyásolja a gyors technikai fejlődés, illetve a hadviselés új technológiák miatt megváltozott jellege. A stratégia ilyen technológiákként határozza meg a következőket:

- fejlett számítástechnika;[159]
- nagyadat-elemzés;[160]
- mesterséges intelligencia;
- autonómia és robotika;
- irányított energia;
- hiperszonikus eszközök;
- és biotechnológia.

Az Amerikai Egyesült Államok élen jár a fenti területeken történő technológiai kutatásokban és a fejlesztések katonai alkalmazásában. A védelmi minisztérium jelenleg hat új technológia katonai alkalmazhatóságának integrálását végzi:

- mesterséges intelligencia;
- halálos autonóm fegyverek;
- hiperszonikus fegyverek;
- irányított energiájú fegyverek;
- biotechnológia;
- kvantumtechnológia.[161]

A 2018-as katonai stratéga egy olyan haderőt vizionál, amelyik alkalmas képességei korlátlan alkalmazására a Föld valamennyi régiójában, a szárazföldön, a vízen, a levegőben, a kozmikus és a virtuális térben (kibertérben) egyaránt. A stratégia értelmezésében a nagyhatalmi vetélkedés kiújulása testesíti meg a legnagyobb kihívást, amellyel az amerikai haderő szembesül Kína és Oroszország tekintetében. A globális integráció azonban növeli a bizonytalanságot. A stratégia megállapítja, hogy az ellenség földrajzi régiókon átívelő, valamennyi műveleti térben végrehajtott műveletekkel próbálja rombolni a haderő meglévő versenyelőnyét, mindezt egy olyan környezetben, ahol az Amerikai Egyesült Államok honi területe nem biztonságos többé. Az ellenséggel és a versenytársakkal szemben elérendő katonai előny érdekében a stratégia bevezeti az egyesített (összhaderőnemi) összfegyvernemi harc[162] fogalmát, amelyet a valamennyi műveleti térben, az összhaderőnemi képességek integrálásával végrehajtott hadműveleti művészetként definiál. Értelmezésében ez azt is jelenti, hogy a haderő és vezetői ugyanolyan magabiztosan hajtanak végre műveleteket a világűrben és a kibertérben, ahogyan a három hagyományos közegben, a földön, a vízen és a levegőben.

---

159 Advanced computing.
160 Big data analytics.
161 Emerging Military Technologies: Background and Issues for Congress. CRS Report, 2020. https://fas.org/sgp/crs/natsec/R46458.pdf; letöltés: 2021.08.13.
162 Összdimenziós/többdimenziós hadviselés, all-domain/multi-domain warfare.

A katonai stratégia a védelmi stratégia céljainak megvalósításához öt feladatkört határoz meg:

- válasz a fenyegetésekre;
- stratégiai támadás elhárítása, illetve a tömegpusztító fegyverek proliferációjának megakadályozása;
- hagyományos támadás elhárítása;
- a szövetségesek és a partnerek biztonságának védelme;
- háborús küszöb alatti konfliktusok katonai dimenziójának a megvívása.

A stratégia értelmezésében az Amerikai Egyesült Államok területének védelme a haderő olyan tevékenysége, amely felülír valamennyi feladatot, és az összhaderőnemi erő funkciójának mozgatórugója. A haderő alkalmazására a dinamikus haderőalkalmazás módszerét határozza meg, hogy a haderővel történő gazdálkodás keretében előtérbe helyezze a háborúra történő felkészülést, ugyanakkor kielégítse a mindennapi műveletek igényeit is. A stratégia a jövőre vonatkozóan a haderőfejlesztést és a haderőtervezést nevesíti, amely folyamatok keretében tervezi a haderő adaptációját és megújulását a védelmi stratégiában meghatározott halálosabb haderő kifejlesztése érdekében. A haderőfejlesztés célja, hogy a meglévő tervezési, döntéshozatali és haderőgazdálkodási folyamatokat úgy alakítsa át, az jobban lássa el feladatát. A haderőtervezés lehetővé teszi, hogy a haderő alapvetően különbözően, a megszokottól eltérő módon győzze le az ellenséget. A haderő alkalmazásához hasonlóan a haderőfejlesztés és a haderőtervezés végcéljai is a Nemzeti Védelmi Stratégiából vannak levezetve. A stratégia a fejlesztési célok elérésére három módszert ír le: a személyi állomány fejlesztése, az új gondolatok és a felszerelés, amelyek lehetővé teszik a versenyelőny megtartását.

Az Elnöki Hivatal 2020. október 15-én hozta nyilvánosságra a *Nemzeti stratégia a kritikus és a fejlődő technológiák védelmére* című dokumentumot,[163] amely szerint, míg az Amerikai Egyesült Államok az elmúlt évszázad nagy részében technológiai vezető szerepet töltött be, az ország technológiai felsőbbrendűsége ma már vitatott. A tudomány és a technológia területein az amerikai vezető szerep egyre növekvő kihívásokkal néz szembe a stratégiai versenytársak részéről, amelyek felismerik a tudományos és a technológiai előnyöket, ezért hatalmas emberi és anyagi erőforrásokat áldoznak arra, hogy vezető szerepet töltsenek be ezeken a területeken. A dokumentum „államorientált modellek" helyett „piacorientált megközelítést" támogat, mert az állam által irányított rendszerek hulladékot termelnek, és nem ösztönzik az innovációt. Ugyanakkor a stratégia lehetővé teszi a kormány számára, hogy megvédje magát a tisztességtelen versenytől, konkrétan Kínára és Oroszországra utalva.

[163] MORTIMORE, David: National Strategy for Critical and Emerging Tech Strategy Released. The Scuttlebutt Blog, 2020.10.15. https://nps.edu/web/slamr/-/2020-national-strategy-for-critical-emerging-technologies; letöltés: 2022.08.12.

A stratégia szerint a kormányzat az egyes kritikus technológiákat a három szint egyikébe sorolja, támogatva a legmagasabb prioritású területeket. A fennmaradó technológiák esetében az Amerikai Egyesült Államok együttműködik partnereivel, illetve kezeli a technológiai kockázatokat. A dokumentum nem határozza meg, hogy a felsorolt különleges technológiák hová tartoznak a hierarchiában. A stratégia e két pillér köré épül: a nemzeti biztonsági innovációs bázis fejlesztése és a technológiai előnyök védelme. Mindkét kategória feladatok felsorolását tartalmazza – 13, illetve kilenc –, amelyek célja az innovációs folyamat felgyorsítása és az idegen befolyástól való elhatárolása. Az első pillér alatt az államigazgatás a munkaerő és a befektetői bázis kiépítésére összpontosít a magánszektorban, a fejlett minőségi kutatás és fejlesztés fenntartása érdekében. A második pillér arra összpontosít, hogy megakadályozzák a külföldi ellenfeleket abban, hogy megszerezzék az Amerikai Egyesült Államok és partnerei által birtokolt innovációkat. Ennek a pillérnek az elsődleges intézkedései közé tartozik a szellemi tulajdon ellopása elleni nemzetközi normák létrehozása és támogatása, a K+F-folyamat biztonságának növelése és bizonyos technológiák diktatórikus országokba történő exportjának korlátozása.

A stratégia mellékletként felsorolja a Nemzeti Biztonsági Tanács által kritikusnak ítélt 20 technológiát:

- fejlett számítástechnika;
- fejlett hagyományos fegyvertechnológiák;
- fejlett szerkezeti anyagok;
- fejlett gyártás;
- fejlett érzékelés;
- repülőgéphajtómű-technológiák;
- mezőgazdasági technológiák;
- mesterséges intelligencia;
- autonóm rendszerek;
- biotechnológiák;
- kémiai, biológiai, radiológiai és nukleáris technológiák;
- kommunikációs és hálózati technológiák;
- adattudomány és -tárolás;
- megosztottadatbázis-technológiák;
- energiatechnológiák;
- ember–gép interfészek;
- orvosi és közegészségügyi technológiák;
- kvantuminformatika;
- félvezetők és mikroelektronika;
- űrtechnológiák.

Az MI-fejlesztések kormányzati alapdokumentuma a Donald Trump elnök által 2019 februárjában jóváhagyott nemzeti MI-program.[164] Erre épít az amerikai védelmi minisztérium 2018-as MI-stratégiája,[165] amely szerint valamennyi következő generációs haditechnikai eszköz alkalmazza majd az MI-t és képes lesz a nagy adat biztosítására, illetve kezelésére. A stratégia fő fókuszai a technológiai lehetőségek felmérése, a jelenlegi kulcsfontosságú feladatok végrehajtásának támogatása a technológiával, a decentralizált kutatás-fejlesztés alapjainak megteremtése a minisztériumnál, a kritikus humán erőforrások megteremtése, valamint az alkalmazás etikai és biztonsági alapjainak kidolgozása.

A 2019. évi védelmi költségvetési törvény előírta egy szakértői bizottság megalakítását az MI nemzeti biztonsági hatásainak vizsgálatára.[166] A testület 2021 márciusában hozta nyilvánosságra a 756 oldalas jelentését. A dokumentum szerint az amerikai haderő fokozatosan elveszti a technológiai előnyét a nagyhatalmi riválisaival szemben. A folyamat csak abban az esetben fordítható meg, ha az MI-alapú technológiák rendszerbe állítási üteme felgyorsul. Ennek két alapja a vezetés világos elgondolása és az alulról építkező innováció. A korábbi technológiai forradalmakhoz hasonlóan az MI területén folytatott versengést sem a legfejlettebb technológia birtoklása, hanem a technológia legsikeresebb integrálása dönti majd el. A védelmi minisztérium feladata, hogy 2025-ig megteremtse az MI széles körű elterjedésének infrastrukturális, szervezeti és humán feltételeit. A folyamat részeként ki kell vonni a hadrendből mindazokat az eszközöket, amelyek nem alkalmasak arra, hogy részt vegyenek az MI-integrációban, így felszabadítva a forrásokat az új technológia beszerzéséhez. A belátható jövőig az új eszközök általános jellemzője, hogy nem kiváltják, hanem kiegészítik a katonákat, akiknek meg kell tanulniuk feladataik delegálását az MI számára. Az MI jelentette előnyök teljes kiaknázásához együtt kell működni a szövetségesekkel és a partnerekkel is, ellenkező esetben a szövetségi rendszerek interoperabilitása és politikai kohéziója csökken.

Az autonóm fegyverrendszerekkel kapcsolatban a szakértői bizottság álláspontja, hogy amennyiben az alkalmazásukat emberi parancsnok vagy operátor engedélyezte, illetve az eszközök tervezése és tesztelése megfelelően történt, akkor az ilyen fegyverrendszerek alkalmazása nem ütközik a nemzetközi humanitárius jogba. Ennek oka, hogy a megfelelő körülmények között az autonóm fegyverrendszerek alkalmasak a kombattánsok és a civilek megkülönböztetésére, az arányos fegyverhasználatra, illetve megfelelnek az elszámoltathatóság követelményének. A bizottság ezért az amerikai nemzeti biztonsági érdekekkel ellentétesnek ítélné az autonóm fegyverrendszerek használatának globális tilalmát. Egyetértenek ugyanakkor

[164] Donald Trump elnök 2019. február 11-ei, 13859. számú rendelete.
Maintaining American Leadership in Artificial Intelligence. Federal Register, Vol. 84, No. 31, 2019.02.14. pp. 3967–3972.
https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf; letöltés: 2019.12.05.

[165] Summary of the 2018 Department of Defense Artificial Intelligence Strategy – Harnessing AI to Advance Our Security and Prosperity.
https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF; letöltés: 2019.12.09.

[166] National Security Commission on Artificial Intelligence.

az ilyen eszközök alkalmazásának nemzetközi korlátozásával, kiemelten az atomfegyverek, a proliferációellenesség és a bizalomépítés tekintetében.[167]

A védelmi minisztérium 2016-ban hozta létre a Védelmi Fejlesztési Hivatalt,[168] amely kiemelten kezeli az MI-vel kapcsolatos fejlesztéseket. 2018-ban az informatikai főnökség[169] alárendeltségében alakult az Egyesített Mesterséges Intelligencia Központ (JAIC[170]) a technológiával járó lehetőségek kiaknázása érdekében. A JAIC feladata az MI/GT-technológia bevezetése, a minisztérium belső működési rendjének átalakítása és hozzáférés biztosítása a szükséges eszközökhöz és adatbázisokhoz. A szervezet számára a működésének első hat évére 1,75 milliárd dollár költségvetést biztosítottak. A JAIC fő feladata az MI széles körű bevezetésének megalapozása a teljes haderőben. Ennek érdekében pilotprojekteket végeznek MI-alapú eszközökkel, koncepciókkal és alkalmazásokkal, valamint támogatják a sikeres projektek széles körű elterjesztését. Emellett közös fejlesztési platformot (JCF[171]) alakít ki a védelmi minisztérium számára, amely az MI-képességek kifejlesztésének és rendszeresítésének alapja lesz. Segítséget nyújt majd a fejlesztések irányának központosításához, miközben lehetővé teszi a kísérletezés, a fejlesztés és a tesztelés decentralizálását. A JCF a haderő minden szervezete számára használható eszközöket, keretrendszereket, algoritmusokat, forráskódokat és sztenderdeket biztosít majd. Lehetővé teszi, hogy a már működő megoldások minél szélesebb körben alkalmazhatók legyenek az új fejlesztésekben, és fontos szerepet kap az MI-rendszerek fejlesztéséhez nélkülözhetetlen adatbázisok összekapcsolásában is. A JAIC kapcsolatot tart fenn a magánszféra kis-, közép- és nagyvállalataival is, hiszen a legfejlettebb MI-technológiát jelenleg ezek a cégek állítják elő. A haderő álláspontja szerint a polgári cégek fejlesztései például a természetes nyelvek feldolgozása és a gépi látás terén 90%-ban katonai célokra is alkalmazhatók. A magánszférától nemcsak a technológiai megoldásokat, hanem a fejlesztési módszertanukat is igyekeznek átvenni, különös tekintettel a technológiai egységesítési folyamatokra.[172]

2022. február 1-jétől a védelmi miniszterhelyettes alárendeltségében új digitális és MI-biztosi (CDAI[173]) beosztás jött létre. Az új iroda a JAIC utódja.[174]

---

[167] SCHMIDT, Eric et al.: Final Report. National Security Commission on Artificial Intelligence, 2021. pp. 75–106.

[168] Defense Innovation Unit – DIU.

[169] Chief Information Office – DoD CIO.

[170] Joint Artificial Intelligence Center.

[171] Joint Common Foundation.

[172] Build to Scale: Maximizing AI/ML Impact across the DoD. JAIC Public Affairs, 2020.11.13. https://www.ai.mil/blog_11_13_20-build_to_scale_maximizing_al-ml_impact_across_the_dod.html; letöltés: 2021.08.13.

[173] Chief Digital and Artificial Intelligence Officer.

[174] EVERSDEN, Andrew: Pentagon creates new overseer for innovation: chief digital and artificial intelligence officer. Breaking Defense, 2021.12.08. https://breakingdefense.com/2021/12/pentagon-creates-new-overseer-for-innovation-chief-digital-and-artificial-intelligence-officer/; letöltés: 2021.12.09.

Az amerikai haderő MI-vel kapcsolatos legjelentősebb fejlesztései a következők:

- a Fejlett Védelmi Kutatási Projektek Ügynökségének (DARPA[175]) alkalmazása a pilóták harci körülmények közötti célfelderítésének támogatására;[176]

- a légierő a 2028-ra elérni tervezett, az összhaderőnemi hadviselést a kibertérre és az űrre is kiterjesztő új, többdimenziós megközelítés (*multi domain warfare*) kereteiben is alkalmazható vezetés-irányítási rendszere;[177]

- a légierő MI-alapú pilótaképzési rendszere („Skyborg”);

- a szárazföldi haderő „Macroscope” fedőnevű projektje a közösségi média felhasználásával javítja a műveleti terület ismeretét;

- a következő gyalogsági harcjárművel[178] szemben követelmény, hogy az eszköz távolról is irányítható legyen;

- hálózatba köthető mobilérzékelők:[179] légi és földi telepítésű szenzorok hálózata, amely képes a célok mozgás közbeni felderítésére, a célok megfigyelésére, tevékenységének előrejelzésére, fontosság szerinti priorizálására; a szenzorok önállóan, helyi hálózatban vagy egy nagyobb rendszer részeként is működtethetők lennének;

- előrejelző karbantartás:[180] az alkatrészek meghibásodása várható idejének meghatározása a karbantartás ütemezése érdekében; az eljárással kiküszöbölhető a technikai eszközök váratlan meghibásodásából adódó kiesése; a rendszer több forrásból integrálná a rendelkezésre álló adatokat (helikopterek esetében például a fedélzeti diagnosztikai rendszerekből, a repülési naplóból és a logisztikai nyilvántartásból); a rendszer jelenleg tesztelés alatt áll a 160. különleges műveleti repülőezred[181] egyik repülőszázadánál; a szárazföldi haderő az Uptake vállalat programját[182] teszteli az M2 Bradley típusú gyalogsági harcjármű prediktív karbantartásához; a későbbiekben nanoméretű érzékelőkkel tervezik felszerelni a jelentősebb eszközöket – például a hadihajókat –, amelyek adatainak és az eszköz digitális modellje összevetésével még pontosabban jelezhető előre a karbantartás szükségessége, a rendszer az eszközök sérüléseit is képes lenne behatárolni (*damage control*);

- tehetséggondozás: a személyügy számára az MI azonosítaná az előmenetelre alkalmas személyeket és meghatározná a beosztások betöltéséhez szükséges kompetenciákat;

---

175 Defence Advanced Research Projects Agency.
176 Target Recognition and Adaptation in Contested Environments – TRACE.
177 Multi-Domain Command and Control.
178 Next Generation Combat Vehicle – NGCV.
179 Mobile Cooperative and Autonomus Sensors.
180 Predictive Maintenance (experimental) – PMx.
181 160th Special Operations Aviation Regiment, Fort Campbell, Kentucky állam.
182 Asset Performance Management.

- műveletek felderítő-hírszerző támogatása: a többdimenziós hadviselés keretében a döntéshozatal támogatásához hozzájárulna a harcmező (hadszíntér) automatizált felderítő-hírszerző előkészítése[183] is; a rendszer összetevői az MI-alapú felderítés és előrejelzés, valamint a célpontok felderítése és ajánlása, majd az emberi döntéshozó általi kiválasztása; a rendszer alapjául a képi forrású felderítés-hírszerzés (IMINT) MI-alapúvá helyezése szolgálna. Az ISIL/DAESH elleni műveletek során már alkalmazott, az ISR-adatok[184] jobb feldolgozását célzó „Project Maven" fedőnevű rendszert az Amazon, a Google és a Microsoft informatikai vállalatok bevonásával fejlesztik.

A fejlesztések érdekében összehangolják a szövetségi kutatás-fejlesztési központok és laboratóriumok, az egyetemek, a kutatóintézetek, valamint a nemzeti védelmi ipari szövetség[185] tevékenységét.

Az amerikai haderő arra számít, hogy a mesterséges intelligencia tömeges bevezetése átalakítja a döntéshozatali rendszert, ami további kutatásokat tesz szükségessé az emberi információfeldolgozó képesség lehetőségeiről, korlátairól. Az MI-rendszerek tömeges integrációjához emellett az amerikai haderőnél még nem létező rendszertervezői[186] képességek szükségesek. Az MI-alapú technológiák terjedése tovább növeli a hálózatba kötött rendszerek sebezhetőségét is. A kibervédelmi kihívást fokozza, hogy a rendszerek működtetéséhez szükséges adatbázisok elérhetőségét felhő (*cloud*) alapú hozzáféréssel tervezik biztosítani.[187,188]

Egyesült Királyság

A brit kormány biztonság-, védelem-, fejlesztési és külpolitikájának 2021-ben kiadott integrált felülvizsgálata a technológia gyors változását a geopolitikai változásokkal, az államok és a politikai berendezkedések közötti rendszerszintű versengéssel, a transznacionális kihívásokkal, a biológiai biztonsági kockázatokkal, a terrorizmussal és a szervezett bűnözéssel egyenértékű kritikus stratégiai kihívásként azonosítja.[189] Az Egyesült Királyság stratégiai előnyét a gazdaság,

---

183 Intelligence Preparation of Battlefield – IPB.

184 Intelligence, Surveillance, Reconnaisance: hírszerzést, megfigyelést és felderítést végző komplex rendszerek.

185 National Defense Industrial Association – NDIA.

186 System engineering.

187 TONIN, Matej: Artificial Intelligence: Implications for NATO's Armed Forces. NATO Parliamentary Assembly, 2019.10.13.

188 2019. október 25-én az amerikai védelmi minisztérium tízmilliárd dollár értékű megrendelést adott a Microsoftnak a titkosított adatok felhőalapú tárolására.
A Microsoft nyerte a Pentagon 10 milliárd dolláros informatikai pályázatát. hirado.hu, 2019.10.26. https://hirado.hu/tudomany-high-tech/high-tech/cikk/2019/10/26/a-microsoft-nyerte-a-pentagon-10-milliard-dollaros-informatikai-palyazatat; letöltés: 2019.10.26.

189 Global Britain in a competitive age – The Integrated Review of Security, Defence, Development and Foreign Policy. HM Government, March 2021. pp. 17–21. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy; letöltés: 2022.08.12.

a politika és a biztonság területén a tudományos és a technológiai fejlődés segítségével kell fenntartani, amelyet a nemzeti biztonság és a külpolitika integráns elemeként kell kezelni. A stratégia a mesterséges intelligenciát, a kvantumtechnológiát és a biotechnológiát nevesíti kulcstechnológiákként. Célként fogalmazza meg, hogy az ország a szolgáltatások, a digitális technológiák és az adatok globális központja maradjon.

A brit Védelmi Minisztérium 2022 júniusában adta ki dedikált MI-stratégiáját.[190] A dokumentum szerint az Egyesült Királyság ellenségei kihívást jelentenek a szigetország által élvezett technológiai előny szempontjából. Az ország jövőbeni biztonsága, ellenálló képessége és nemzetközi helyzete azon múlik, hogy miképpen képes alkalmazkodni a gyors technológiai változáshoz.

A felforgató technológiák közül a mesterséges intelligencia okozza a legtöbb változást, és teljes iparágak szabályait írhatja át, jelentős gazdasági növekedést generálhat, és a társadalom minden aspektusát átalakíthatja. Az MI védelmi célú alkalmazása során az üzleti életben kifejlesztett megoldásokkal gyorsíthatók a bürokratikus eljárások és növelhető azok hatékonysága, növelhető a döntéshozatal minősége és a katonai műveletek sebessége, fokozható a hálózatos számítógépes rendszerek biztonsága és ellenálló képessége, növelhető a haderő ütőképessége, kitartása, hatóköre és hatékonysága, valamint az ismétlődő, nehéz és veszélyes munkafolyamatok automatizálásával növelhető a katonák biztonsága. Az új technológiák elterjedésével etikai kérdések merülnek fel, és újra kell gondolni a döntéshozatali folyamatokat, de a megszerezhető előnyök és az ellenséges fejlesztések jelentette kihívások miatt a változás feltartóztathatatlan.

A brit haderőnek az ipari kor összhaderőnemi szemléletéről mihamarabb át kell térnie a haderő alkalmazásának integrált megközelítésére, amelyben a mesterséges intelligencia központi szerepet játszik. Az új megközelítés a katonai erő összehangolt alkalmazását írja elő a hadviselés mind az öt dimenziójában (szárazföld, víz, levegő, űr és kibertér) a nemzeti erő egyéb szegmenseivel, elsősorban az iparral és az akadémiai szektorral, valamint a szövetségesekkel.[191] Ennek legfontosabb alapfeltétele az információs előny elérése.

A teljes védelmi szektornak át kell állnia a szoftverek széles körű alkalmazására, és készen kell állnia az algoritmusok folyamatos fejlesztésére az ellenséggel szemben meglévő előny fenntartása és a fenyegetések gyors azonosítása érdekében. Az MI-rendszerekre szakosodott szakértők bevonzása érdekében ösztönzőket, egyebek mellett kiemelt juttatásokat kell biztosítani a számukra. Ki kell alakítani, meg kell tartani és folyamatosan képezni kell a specialista és a generalista szakértői bázist. Minden vezetőnek rendelkeznie kell alapszintű MI-ismeretekkel, a végrehajtó állománynak pedig képesnek kell lennie az új szoftverek és eszközök felhasználói szintű alkalmazására.

[190] Defence Artificial Intelligence Strategy. Ministry of Defence, 2022.06.15. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy; letöltés: 2022.08.12.

[191] Multi-Domain Integration – MDI.

A haderő a személyi állományt követő legfontosabb, stratégiai eszköze az adat, amelynek jobb felhasználása érdekében egyesíteni kell a jelenleg elkülönült adatbázisokat, egységes adatsztenderdeket kell létrehozni, és mindenkinek hozzáférést kell biztosítani a feladatai végrehajtásához szükséges rendszerezett és ellenőrzött adatokhoz.

A mesterséges intelligencia fejlesztése területén az Egyesült Királyság legfontosabb szövetsége az Amerikai Egyesült Államok, amelyet a többi angolszász ország (Ausztrália, Kanada és Új-Zéland) követ. Kiemelt figyelmet kap továbbá a NATO-n belüli együttműködés, Európán belül Franciaország és Németország, az indiai–csendes-óceáni térségben pedig India, Japán és Szingapúr.

A mesterséges intelligenciában rejlő lehetőségek integrált kiaknázása érdekében a Védelmi Minisztérium 2021-ben dedikált központot[192] hozott létre, amely 2022 áprilisában érte el a kezdeti műveleti készenlétet. Feladata, hogy az új kutatások és a stratégiai MI-projektek központjaként irányt mutasson a fejlesztéseknek, miközben egységes MI-szolgáltatások, eljárások és szakértői bázis biztosításával támogatja a haderő alakulatainak és szervezeteinek saját fejlesztéseit. A Védelmi Minisztérium a robotrendszerek fejlesztésére 2020-ban külön kiválósági központot[193] hozott létre.

A központ jelenlegi két kiemelt fejlesztése:

- nanoméretű (kevesebb mint 200 gramm tömegű) drónok fejlesztése a szárazföldi haderő lövészalegységei számára; a kisméretű eszközökre nagy felbontóképességű videokamerák és hőfelderítő rendszerek szerelhetők, így lehetővé teszik a terepakadályok vagy az ismeretlen belső elrendezésű épületek felderítését is; irányíthatók közvetlen vezérléssel és alkalmasak autonóm üzemelésre is;

- a szintén a lövészalegységek számára fejlesztett, ATLAS[194] elnevezésű kezelő nélküli szárazföldi járművek (UGV[195]) gépitanulás-alapú szoftverek segítségével képesek légi és műholdas felvételek alapján autonóm módon felmérni a terepet, és ez alapján navigálni, valamint a saját kameráik alapján azonosítani a fenyegetéseket (járműveket és embereket), illetve az akadályokat; az eszköz GPS nélkül is képes a navigációra.

A Védelmi Minisztérium egyéb fejlesztései:

- a Királyi Haditengerészet „Wilton” fedőnevű projektjének célja autonóm aknavadász hajók fejlesztése; a három hajóból álló rendszerek képesek az aknák és egyéb tengerészeti robbanóanyagok autonóm felderítésére és azonosítására; az eszközök által vontatott felszerelés képes hajóegységek magnetikus, akusztikus és elektromos jellemzőit utánozni, ezáltal elműködtetni az aknákat;

[192] Defence Artificial Intelligence Centre – DAIC.
[193] Expeditionary Robotics Centre of Expertise – ERCoE.
[194] Autonomous Ground Vehicle Projects.
[195] Unmanned Ground Vehicle.

- a Védelmi Hírszerzés[196] „SPOTTER" fedőnevű projektje a képi forrású hírszerzés (IMINT) által beszerzett felvételek gépi tanuláson alapuló feldolgozására irányul; a rendszer képes tárgyak automatikus azonosítására,[197] lehetővé téve helyszínek autonóm monitorozását; a „SQUINTER" projekt szintetikus apertúrájú radarok[198] információjának feldolgozására specializálódott;

- a „SAPIENT"[199] fedőnevű program célja olyan megfigyelőrendszer fejlesztése, amely a videokamerák felvételeit autonóm módon dolgozza fel és képes kisebb döntéseket hozni például a megfigyelés intenzitásának fokozására egy adott területen; a rendszer a helységharc fontos eszköze lehet.

A jelenlegi legfontosabb brit hadiipari fejlesztések:

- az L3Harris Technologies (MADFOX[200]) elnevezésű kezelő nélküli vízijárműve (USV[201]) autonóm megfigyelésre és a saját erők megóvására[202] alkalmas eszköz a haditengerészet és a tengerészgyalogság számára; az első járművet 2021 márciusában adták át a Királyi Haditengerészet részére;[203]

- a HORIBA MIRA iparvállalat VIKING típusjelzésű többfeladatú UGV-je alkalmas utánpótlás szállítására, felderítésre, illetve felszerelhető távolról vezérelt fegyverekkel; a hatkerekes terepjáró eszköz legfeljebb 50 km/h sebességgel haladhat, szállítási kapacitása 750 kg;[204]

- a Digital Concepts Engineering (DCE) X2 és X3 típusjelzésű kisméretű, távvezérléssel és autonóm módon is üzemeltethető UGV-i 250 kg terhet szállíthatnak és három tonnát képesek vontatni; felületükre számos katonai, illetve a mezőgazdaságban, valamint az atomiparban alkalmazott eszköz elhelyezhető;[205]

---

196 Defence Intelligence – DI.

197 Object Recognition – OR.

198 Synthetic Aperture Radar – SAR: A rádiólokátor egy változata, amelyet objektumok (pl. földrajzi területek) kétdimenziós vagy háromdimenziós képének rekonstrukciójára használnak.
SAR (szintetikus apertúrájú rádiólokátor, Synthetic Aperture Radar). A világ működése kislexikon. http://www.vilaglex.hu/Lexikon/Html/SAR.htm; letöltés: 2021.08.13.

199 Sensing for Asset Protection with Integrated Electronic Networked Technology.

200 Maritime Demonstrator for Operational eXperimentation.

201 Unmanned Surface Vessel.

202 Force protection.

203 Maritime Demonstrator for Operational eXperimentation (MADFOX) Uncrewed Surface Vessel, UK. Naval Technology, 2021.10.21.
https://www.naval-technology.com/projects/maritime-demonstrator-for-operational-experimentation-madfox; letöltés: 2022.08.13.

204 VIKING Multirole UGV Platform. Horiba-MIRA, 2022.
https://www.horiba-mira.com/unmanned-ground-vehicles/media-centre/case_study/viking-multirole-ugv-platform/; letöltés: 2022.08.13.

205 DCE's X Series is a range of high capability, affordable, tracked all-terrain unmanned ground vehicles. Digital Concepts Engineering, 2022.
https://dconcepts.co.uk/products/x-series; letöltés: 2022.08.13.

- a Blue Bear Ghost típusú pilóta nélküli repülőrendszere (UAS[206]) alkalmas több pilóta nélküli repülőgép (UAV[207]) egyidejű irányítására;[208] a rendszer képességeinek 2020 októberi bemutatója során hét eszközt irányítottak egy időben;[209]
- az MSubs XLUUV/[210]Manta/S201 elnevezésű 8,9 tonna tömegű, kezelő nélküli tengeralattjárója (UUV[211]) 48 órán keresztül képes autonóm módon tevékenykedni akár 305 méter mélységben.[212]

Kína

A kínai MI-fejlesztéseket segíti a pártállam és a haderő összefonódása az érintett magánvállalatokkal. A tágabb értelemben vett védelmi szféra[213] tekintetében a fejlesztések fő irányát a kibervédelem és a kormányzat társadalomellenőrző tevékenységének támogatása – például az arcfelismerésen alapuló megfigyelőrendszerek – jelentik. Katonai vonatkozásban – az Amerikai Egyesült Államokhoz hasonlóan – Kína is elsősorban a katonai döntéshozatal és az autonóm fegyverrendszerek területén fejleszti az MI-rendszereit. A katonai vezetés elgondolása szerint a haderő MI-alapúvá tételével ellensúlyoznák az amerikai katonai dominanciát.

A kínai vezetés célja, hogy 2020 végére 150 milliárd jüanra (6400 milliárd forintra), 2030-ig ezermilliárd jüanra (45 000 milliárd forintra) növelje gazdasága (szűk értelemben vett) MI-szektorának értékét, amellyel globális vezető szerepre tenne szert e területen. Az MI-re épülő digitális szektor teljes értéke ekkorra tízezer milliárd jüanra nőhet. Kínai várakozás szerint az MI 2025-re már az ország gazdasági növekedésének legfőbb hajtóerejévé válik.[214]

---

206 Unmanned Aerial System – UAS. A UAS pilóta nélküli repülőgépekből (Unmanned Aerial Vehicle – UAV) és a kezelő-/irányítórendszerből áll.

207 Unmanned Aerial Vehicle.

208 Swarming.

209 BALL, Mike: Remote UAS Swarm Launching Technology Demonstrated. Unmanned Systems Technology, 2020.10.30. https://www.unmannedsystemstechnology.com/2020/10/remote-uas-swarm-launching-technology-demonstrated/; letöltés: 2022.08.13.

210 Extra Large Uncrewed Undersea Vehicle.

211 Uncrewed Underwater Vehicle.

212 XLUUV / MANTA / S201. Submergence Group, 2020. https://msubs.com/unmanned-submersibles/xluuv/; letöltés: 2022.08.13.

213 A kínai megközelítés nem különbözteti meg élesen a védelmi és a civil szférát. A fejlesztéseknél elsődleges szempont a technológia elterjesztése, az adatvédelmi kérdésekkel (pl. az új internetes fizetési megoldások, az önvezető gépjárművek, a közlekedésmenedzsment-rendszerek stb. esetében) csak ezt követően foglalkoznak.

214 SHEPPARD, Lindsey R.: Artificial Intelligence and National Security: The Importance of the AI Ecosystem. CSIS, 2018.11.05. pp. 48–51. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181102_AI_interior.pdf; letöltés: 2019.12.09.

Oroszország

Vlagyimir Putyin orosz elnök 2017-ben kijelentette, hogy az MI területén vezető szerepet szerző állam a világ urává válik. Ennek ellenére Oroszország – elegendő anyagi forrás hiányában – nem képes lépést tartani az Amerikai Egyesült Államokkal és Kínával. A magánszektor éves befektetése 2018-as becslés szerint mindössze 700 millió rubel (3,25 milliárd forint) volt a területen; a fejlesztésekben a Védelmi Minisztérium játszik kulcsszerepet. A minisztérium, valamint a haderő és a hadiipari vállalatok tevékenységének összehangolásáért felelős Katonai Ipari Bizottság[215] célja, hogy 2025-re a haderő felszerelésének 30%-a távolról is irányítható legyen. A kormány által az amerikai DARPA mintájára létrehozott Fejlett Kutatások Alapítványa[216] éves költségvetése mintegy négymilliárd rubel (18,52 milliárd forint). Az ügynökség elsősorban az emberi gondolkodás másolása és az adatelemzés területein végez kutatásokat. Deklarált céljai között szerepel továbbá a kép- és beszédfelismerési technológiák, az autonóm fegyverrendszerek irányításának és a fegyverrendszerek teljes élettartamára kiterjedő karbantartási rendszerek fejlesztése.[217]

[215] Vojenno-Promislennaja Komisszija – VPK.
[216] Fond Perszpektyivnih Isszledovanyij.
[217] SHEPPARD, Lindsey R.: Artificial Intelligence and National Security: The Importance of the AI Ecosystem. CSIS, 2018.11.05.

A KORSZERŰ NEMZETBIZTONSÁGI RENDSZER FELÉPÍTÉSE ÉS FELADATAI

Fogalmi alapok

A nemzetbiztonság rendszer szakágai és alapfeladatai

A nemzetbiztonsági rendszert hírszerzésre és elhárításra osztjuk. Kis-Benedek József a hírszerzés fogalmi megközelítésének alapvető kettősségét az amerikai Központi Hírszerző Ügynökséghez (CIA) köthető két meghatározó szerző definícióival érzékelteti. A CIA alapításának történetét feldolgozó Thomas F. Troy szerint a hírszerzés az ellenség megismerése. A hírszerzési ciklus elméleti megalkotójaként ismert Sherman Kent[218] szerint a hírszerzés tudás, szervezet és tevékenység. Kis-Benedek megfogalmazásában Kent „*felfogása szerint a tudás az összegyűjtött információk bázisán készült jelentésekkel egyenlő, a szervezet olyan intézmény, ügynökség stb., amely az információkat gyűjti, elemzi, értékeli és »fogyaszthatóvá« teszi, azaz jelentés formájában megjeleníti, a tevékenység pedig azon eljárások, fogások és módszerek összessége, amelyek segítségével az információk összegyűjthetők.*"

A hírszerzéssel szemben „*az elhárítás alapvetően védelmi természetű. Klasszikus változata magában foglalja a kémelhárítást, az ellenséges (ellenérdekelt) titkosszolgálatok behatolásának megakadályozását, a titkok megőrzését, a tevékenység azonban az aktív és a passzív elemeket egyaránt magában foglalja.* (…) *Mára a tevékenység kiterjed a terrorelhárításra, a kábítószerek és a szervezett bűnözés elleni küzdelemre és a felforgatás elleni védelemre (alkotmányvédelem).*"[219] Szabó Károly szerint „*az elhárítás* (…) *egy legitim állam befolyásoktól mentes működésében közreműködő, a szuverenitás fenntartását veszélyeztető leplezett törekvések és a biztonsági kockázatok azonosítására, felderítésére, továbbá az azonosított ellenérdekelt törekvések megszüntetésére, megszakítására, korlátozására, akadályozására és elhárítására irányuló célirányos, jogszabályokban rögzített tevékenység.*"[220]

---

[218] A történész végzettségű Kent 1942-től a második világháborúban létrehozott Stratégiai Szolgálatok Hivatalánál (Office of Strategic Services – OSS), majd annak utódszervezeténél, a Központi Hírszerző Ügynökségnél (Central Intelligence Agency – CIA) szolgált különböző elemzői beosztásokban. A hírszerzési ciklus mellett a Hírszerző Közösség (Intelligence Community – IC) konszenzusos álláspontját tartalmazó nemzeti hírszerző értékelések (National Intelligence Estimate – NIE) módszertanának kidolgozása is Kent érdeme. A CIA a 2000-ben alapított elemző-értékelő akadémiáját Sherman Kentről nevezte el.

[219] KIS-BENEDEK József: Az emberi erőkkel folytatott információszerzés (HUMINT). In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 154–161. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

[220] SZABÓ Károly: Gondolatok a katonai elhárításról. Szakmai Szemle, 2015. 1. szám. pp. 7–15. https://www.knbsz.gov.hu/hu/letoltes/szsz/2015_1_szam.pdf; letöltés: 2022.10.18.

Vida Csaba a nemzetbiztonság elméleti alapjainak vizsgálata során megállapítja, hogy „*a nemzetbiztonsági elméletek magukban foglalják a stratégiai hírszerzéssel és elhárítással, illetve az elemző-értékelő munkával kapcsolatos elméleteket is.*" Álláspontja szerint a nemzetbiztonsági rendszer „*azt a tudást is jelenti, amely a nemzetbiztonsági tevékenység eredménye*."[221]

Az információs védelem (kibervédelem) új feladatot jelent mind a hírszerzés, mind az elhárítás számára. Szabó Károly *A nemzetbiztonság elmélete a közszolgálatban* című tankönyv elhárításról szóló fejezetében úgy fogalmaz, hogy a kibervédelem a kibertérből érkező támadás elleni védelmi jellegű tevékenység. „*A kibervédelem magában foglalja azon országok, szervezetek és egyének felderítését, akik a kibertérben elkövetett cselekedeteikkel kockázatot jelenthetnek a társadalom szerkezetére és cselekvőképességére, az állami élet működésére és az alkotmányos rend fenntartására. A kibervédelem magában foglalja továbbá a kibertérből való támadások technikáinak tanulmányozását is*."[222]

Az állami (nemzetbiztonsági) hírszerző szervezet tevékenységének alapját a felettes állami szervezetektől érkező feladatok képezik. Elsődleges feladata a döntéshozók megfelelő mennyiségű és minőségű információval történő ellátása. Emellett a nemzeti érdekek érvényesítése érdekében fedett vagy titkos nemzetbiztonsági műveleteket is folytathat.[223] A nemzetbiztonsági szolgálatok a tevékenységük végrehajtásához szükséges információt emberi forrásokból és technikai eszközök felhasználásával szerzik be, amelyek között prioritás nem állítható fel, hiszen kiegészítik és támogatják egymást.[224]

A könyvben részletesen foglalkozom amerikai Hírszerző Közösség működével, ezért szükséges az amerikai és a magyar szakkifejezések közötti különbségek hangsúlyozása és az ellentmondások feloldása. Az amerikai „*intelligence*" kifejezést magyarra általában hírszerzésként fordítjuk, pedig tulajdonképpen pontosabb lenne a nemzetbiztonság[225] kifejezés használata. A fogalmat Martin T. Bimfort részletesen körüljárja, akinek az eredetileg „Titkos!" (SECRET) minősítésű, 1958-ban írt meghatározását 1994-ben tette közzé a CIA. A kezdetben belső használatra szánt feljegyzés jelenleg a CIA hivatalos definíciójául szolgál – a titoktalanítás[226] amerikai példájaként. Bimfort álláspontja szerint az *intelligence* „*a kormányzati külpolitika és a nemzeti biztonság számára fontos, külföldi országokra és az ügynökeikre vonatkozó*

---

[221] VIDA Csaba: A nemzetbiztonsági elméletek alapjai – Szükségesek-e az alapkutatások a nemzetbiztonsági elméletekben? Szakmai Szemle, XX. évfolyam 1. szám, 2022. március. pp. 5–21.

[222] SZABÓ Károly: Az elhárítás. In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 169–208. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

[223] A nemzetbiztonsági szolgálatok alapfeladata az államot fenyegető fenyegetések, kockázatok és kihívások felfedése, illetve meghatározása is, de ez része a döntéshozói hírigény megválaszolásának.

[224] KIS-BENEDEK József: Az emberi erőkkel folytatott információszerzés (HUMINT). In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 154–156.

[225] Nem tévesztendő össze a „nemzeti biztonság" („*national security*") fogalmával.

[226] Desecretization. A titoktalanítás számos előnnyel jár a nemzetbiztonsági szféra számára, amelyek közül a társadalmi elfogadottság növelése mellett a tudományos eredmények jobb felhasználása emelhető ki.

információ gyűjtése és feldolgozása;[227] *a külpolitikai célok előmozdítását támogató, a kormányzathoz nem köthető tevékenységek folytatása;*[228] *valamint a fenti folyamat és termékeinek, valamint az ezekhez köthető személyek és szervezetek védelme*".[229]

Vida Csaba tisztázza a nemzeti biztonság és a nemzetbiztonság közötti különbséget. „*A National Security kifejezés (...) nemzeti biztonságot jelent, amely teljes mértékben nem egyezik meg a nemzetbiztonsággal. A nemzeti biztonság tartalma sokkal szélesebb, amelynek része a nemzetbiztonság, de minden más, az ország védelméért felelős szervezet is, mint a haderő vagy a rendvédelmi szervezetek is odatartoznak*."[230]

Bimfort szerint az elhárítás (*counterintelligence*) az *intelligence* organikus, elválaszthatatlan része, hasonlóan az emberi szervezet fehérvérsejtjeihez és antitestjeihez.[231] A jobb megértés érdekében érdemes megvizsgálni a *counterintelligence* definícióját is, amelyhez segítséget nyújt a CIA által a Nemzeti Biztonsági Tanácshoz[232] 1957-ben felterjesztett, eredetileg „Szigorúan titkos!" (TOP SECRET) minősítésű, 2003-ban közzétett dokumentum. Eszerint az elhárítás „*olyan hírszerző tevékenység*[233] *és az ennek eredményeként elkészült tájékoztató,*[234] *amelynek célja a nemzet biztonságának, valamint külföldi személyzetének és létesítményeinek védelme a kémkedéssel, a kémelhárítással, a szabotázzsal és a felforgatással szemben*".[235] Az ODNI definíciója szerint az „*intelligence*" (egyszerűsítve a hírszerzési információra és a tájékoztatókra utalva) az amerikai nemzeti és belbiztonságra vonatkozó információk összessége.[236] E definíciókból következik, hogy az *intelligence* amerikai értelmezésben lefedi a hazai szaknyelv hírszerzés, elhárítás és terrorelhárítás[237] fogalmait is. Az amerikai Hírszerző Közösség (IC) vizsgálata során a hírszerzés fogalmát a szélesebb, amerikai értelemben használom.

---

227 „Positive intelligence", amelynek fókuszában a szűk értelemben vett hírszerző tevékenység áll, de magában foglalja a kémelhárításhoz szükséges információk beszerzését is.

228 A nemzetbiztonsági szolgálatok műveleti tevékenysége (a szerző megjegyzése).

229 Counterintelligence, vagyis elhárítás (a szerző megjegyzése).

230 VIDA Csaba: A nemzetbiztonsági elméletek alapjai – Szükségesek-e az alapkutatások a nemzetbiztonsági elméletekben? Szakmai Szemle, XX. évfolyam 1 szám, 2022. március. pp. 5–21.

231 BIMFORT, Martin T.: A Definition of Intelligence. Studies of Intelligence, Volume 2, Issue 4, Fall 1958. pp. 75–78.
https://www.cia.gov/static/A-Definition-Of-Intelligence.pdf; letöltés: 2020.04.29.

232 National Security Council.

233 Intelligence activity.

234 Az eredeti szövegben „informational product".

235 Definition of Counterintelligence. National Security Council Intelligence Directive No. 5, 1957.
https://www.cia.gov/readingroom/docs/CIA-RDP85S00362R000600160015-2.pdf; letöltés: 2020.04.29.

236 What is Intelligence? Office of the Director of National Intelligence.
www.dni.gov/index.php/what-we-do/what-is-intelligence; letöltés: 2020.04.28.

237 A megállapítást az is alátámasztja, hogy az amerikai terrorelhárítási rendszer központi szervezetei (a Nemzeti Hírszerző Főigazgató Hivatalának [ODNI] Nemzeti Terrorelhárítási Központja; a Központi Hírszerző Ügynökség [CIA] terrorelhárítási műveleti központja; a Szövetségi Nyomozó Iroda [FBI] Nemzeti Biztonsági Ágazatának Terrorelhárítási Osztálya és terroristák kiszűrésére szolgáló központja; valamint a Terrorelhárítási és Pénzügyi Hírszerző Hivatal) a Hírszerző Közösség részeként tevékenykednek.

A hírszerzési ciklus és kritikája

A könyv megírása során a nemzetbiztonsági hírszerzési ciklus[238] elemeinek Vida Csaba által bemutatott, Sherman Kent munkásságára építő felosztását követtem. Vida Csaba szerint „*a ciklus a következő szakaszokból áll: az információigények fogadásából és a hírszerzés folyamatának megtervezéséből és megszervezéséből (1), az adatszerzésből (2), az információk feldolgozásából és rendszerezéséből (3), az információk elemzéséből-értékeléséből és a tájékoztatók készítéséből (4), valamint végül a döntéshozók (felhasználók) tájékoztatásából (5). A körfolyamat fontos eleme a visszacsatolások*[239] *rendszere, mert minden egyes szakasz között vannak visszautalások az előző […] szakaszokra. Ez biztosítja a ciklus komplex működését.*”[240]

6. ábra. A Sherman Kent által kidolgozott hírszerzési ciklus jelenleg alkalmazott változata[241,242]

[238] Intelligence cycle.
[239] Feedback (a szerző megjegyzése).
[240] VIDA Csaba: A hírszerzési ciklus. In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus, Budapest, 2018. pp. 114–126. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.
[241] ALESSA, Lilian: Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.30.

Dr. Lilian Alessa, az Idahói Egyetem CRC[243] kutatóközpontjának igazgatója *Emberekre támaszkodva: a mesterséges intelligencia sikere vagy bukása az emberi tényezőn múlik*[244] című előadásának alapvetése, hogy az amerikai Hírszerző Közösség mára fulladozik a rendelkezésére álló adatok tengerében. Ennek fő haszonélvezői az Amerikai Egyesült Államok – az előadásban meg nem nevezett – ellenségei, mert a tevékenységükre utaló jelek elvesznek az adattömegben.

Az amerikai hírszerzés rendszere napjainkban is a hírszerző elemzés-értékelés atyjaként számontartott Sherman Kent által kidolgozott hírszerzési cikluson alapszik. A ciklus középpontjában az elemzők állnak, ezért az elemzőkre nehezedő nyomás a hírszerzés teljes rendszerére kihat. A hírszerzési ciklus elméletének megalkotásakor Kent nem láthatta előre az információs korszak eljövetelét, amelynek hatására a hírszerző elemző-értékelők egyre kevésbé képesek elvégezni a rendelkezésre álló információ feldolgozását.[245] A kihívás hatványozottan jelentkezik az anomáliák és a mintázatok detektálása tekintetében.

Az elemzők helyzetét tovább rontja a komplikált bürokrácia és a kevés idő. Mindemellett a technológiai megoldás kulcsát jelentő információtechnológiai szervezeti egységek kis méretű dinamikus csapatokból maguk is hatalmas bürokráciákká nőtték ki magukat.

Dr. Alessa a hírszerzési ciklus jelenlegi alkalmazásának hármas kritikáját fogalmazta meg:

- a ciklust az információigények fogadása és a hírszerzés folyamatának megtervezése és megszervezése (Planning and Direction) indítja el; a valóságban a hírszerzés nagyon kevés fogódzót kap arra nézve, hogy a felhasználóknak mire van szüksége;
- a hírszerzés rendszerét körülményessé teszi és lassítja, hogy a ciklus elemeit egymás után kell végrehajtani;
- a hírszerzés látókörét beszűkíti, hogy a ciklust túlnyomórészt a döntéshozók igényei, elvárásai, „kedvenc témái" határozzák meg; az ennek következtében fellépő feladatorientáltág miatt a hírszerzés nem foglalkozik a rejtett fenyegetések felfedésével.

---

[242] A ciklus elemei: Planning and Direction (az információigények fogadása és a hírszerzés folyamatának megtervezése és megszervezése); Collection (adatszerzés); Processing and Exploitation (az információk feldolgozása és rendszerezése); Analysis and Production (az információk elemzése és értékelése, valamint a tájékoztatók elkészítése); Dissemination and Integration (a döntéshozók/felhasználók tájékoztatása, más megközelítésben a hírszerzési információk eljuttatása a rendeltetési helyükre, azok integrációja). A körfolyamat fontos eleme a visszacsatolások (Feedback) rendszere, mert minden egyes szakasz között vannak visszautalások az előző szakaszokra. Végül az ellenőrzés (Evaluation) járul hozzá a ciklus komplex működéséhez.

[243] A 2014-ben alapított Center for Resilient Communities társadalmi-ökológiai interdiszciplináris kutatásokat végez. Az amerikai Hírszerző Közösség figyelmét elsősorban a rendszertudomány gyakorlati alkalmazásában elért eredmények kelthették fel.

[244] ALESSA, Lilian: Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.30.

[245] Az emberi erőforrás feldolgozóképessége mára elégtelenné vált ahhoz, hogy az adat–információ–tudás–bölcsesség folyamat a kellő időben végbemenjen.

A fenti nehézségek megoldásában a rendszertudomány[246] nyújt segítséget, amely lehetővé teszi az adatok közötti rejtett kapcsolatok feltárását. Így a korábban az adattömegbe vesző kritikus információk – az előadó kifejezésével élve – „elemlámpaként fénylenek az éjszakában".

A hírszerzés önálló ágai

A hírszerzés önálló ágai tekintetében a Nemzeti Közszolgálati Egyetem *A nemzetbiztonság elmélete a közszolgálatban* című tankönyvének – a nemzetközi és a hazai szakirodalomban is általánosnak tekinthető megközelítést követő – felosztását követem. Eszerint az önálló ágak az alábbiak.

Nyílt forrású hírszerzés (OSINT[247]): „*Valamely személy vagy szervezet által közzétett, nyilvánosan, legális eszközökkel megszerezhető vagy korlátozott körben terjesztett, de nem minősített adatoknak a hírszerzési igények kielégítésére, speciális módszertan alapján történő felkutatása, gyűjtése, szelektálása, értékelése és felhasználása*."[248]

Rádióelektronikai felderítés (SIGINT[249]): „*Olyan felderítési nem, amely a külföldi (szemben álló fél) kommunikációs és nem kommunikációs kisugárzó eszközök észleléséből szolgáltat adatokat, információkat*." (…) „*A SIGINT feloszthatói: kommunikációs felderítésre, vagy más néven rádiófelderítésre (COMINT[250]), amely a szemben álló fél kommunikációs rendszereinek lehallgatásával szerez információt; illetve elektronikai felderítésre (ELINT[251]), vagy más néven rádiótechnikai felderítésre, amely a kisugárzott elektromágneses jelek passzív módon történő rögzítéséből, elemzéséből szolgáltat adatot*."[252]

Emberi erőkkel folytatott információszerzés (HUMINT[253]): „*A nemzetbiztonsági tevékenység azon eljárása, amelynek középpontjában az ember áll, akinek ismeretét, képességét a nemzetbiztonsági szolgálatok tervszerűen és szervezett formában használják fel. A HUMINT az e célra képzett adatszerzők tevékenysége, akik az információkat és az adatokat emberektől, az emberek által használt dokumentumokból és a médiából szerzik a szemben álló erők szándékainak, erejének, képességeinek, eljárásainak, taktikáinak megismerésére. A HUMINT az emberi erőforrást eszközként, egyben információ- és adatszerzési módszerként használja fel aktív és passzív módszerekkel a felderítési/hírszerzési igények megvalósítása érdekében.*"

---

246 Systems science.
247 Open Source Intelligence.
248 VIDA Csaba: Nyílt forrású adatszerzés (OSINT). In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 133–141. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.
249 Signals Intelligence.
250 Communication Intelligence.
251 Electronic Intelligence.
252 BALOGH Péter: Rádióelektronikai felderítés (SIGINT). In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 142–154. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.
253 Human Intelligence.

A hírszerzés mellett „*az emberi erőforrások felhasználása ugyanúgy jellemzi az elhárítást is*."[254]

Geoinformációs/térinformatikai hírszerzés (GEOINT[255]): „*Az összes térinformatikai információ együttes ábrázolását jelenti, így a konkrét tereptárgyakon, műtárgyakon, valamint eszközökön túl az adott térségben zajló tevékenységet, hőkisugárzások jeleit, környezeti elemeket és más térinformatikai információkat (például mérési adatokat a terepviszonyokról, távolságokról, a hőmérsékletet, a látható eszközökre és objektumokra vonatkozó információkat) is tartalmazza*."

Képi felderítés (IMINT[256]): Tereptárgyak, objektumok vagy eszközök azonosítása a repülőgépekről és a műholdakról készített fényképek feldolgozásával és értelmezésével speciális tudás és ismeretrendszer alapján. Az IMINT rendkívül szoros kapcsolatban áll a GEOINT-tal.

Kiberhírszerzés (CYBINT[257]): „*Célpontjai maguk a számítógépek és az azokat összekötő hálózatok, köztük az internet. A világháló vonatkozásában a CYBINT abban különbözik az OSINT-tól, hogy a hálózaton keresztül olyan információk és adatok megszerzésére irányul, amelyeket az információtulajdonos nem kíván publikálni, hanem a saját számítógépén vagy zárt hálózaton tárolja. A CYBINT keretében alapvetően a következő háromfajta tevékenységet lehet megkülönböztetni:*

- *a nyílt hálózatokon keresztül olyan információk megszerzése, amelyeket a tulajdonosa nem kíván nyíltan megosztani;*
- *információk megszerzése a zárt hálózatokba történő betöréssel;*
- *a számítógépek és az informatikai hálózatok által kisugárzott jelekből történő adatszerzés*."

Mérés és jelmeghatározó hírszerzés (MASINT[258]): „*...különleges szenzorok alkalmazásával gyűjti az információt a célterületről, a célobjektumról vagy a céltárgyról. A szenzorok jellege alapján különböztetjük meg a MASINT fajtáit, mint:*

- *nukleáris (radioaktív anyagok kisugárzását mérő eljárás, amelyet más néven radiológiai hírszerzésnek is hívnak);*
- *vegyi és biológiai (vegyi és biológiai anyagok jelenlétét megállapító eljárás, amelyet a haderőn belül vegyi felderítésnek tekintenek);*

[254] KIS-BENEDEK József: Az emberi erőkkel folytatott információszerzés (HUMINT). In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 155–156.
[255] Geospatial Intelligence.
[256] Imagery Intelligence.
[257] Cyber Intelligence.
[258] Measurement and Signature Intelligence.

- *energia (energiakibocsátás-mérő eljárás, amely többek között a hőmérséklet-változást is meg tudja határozni, s amelyhez többnyire infrakamerákat használnak, de képes a hőhatással nem járó energiahullámok megállapítására is);*
- *visszatükrözés (az eljárás során egy speciális felületet használnak fel, amelyről a visszatükröződő hangot, az elektromágnesességet, a fényt és az energiahatást mérik);*
- *akusztikus (a hanghatásokat és a hanghullámokat rögzítő eszköz a különböző mechanikus szerkezetek, többek között a motorok hangját deríti fel);*
- *mágneses (a mágneses anomáliák felderítését teszi lehetővé);*
- *mozgás (a célkörzetben bekövetkező mozgásokat vizsgálja, így meg tudja határozni a céltárgyak helyzetváltoztatásait, rögzíteni tudja a vibrációkat);*
- *anyag (a céltárgyak anyagi összetételét vizsgáló eljárás)*."[259]

A SOCMINT

A SOCMINT megjelenése és nemzetbiztonsági jelentősége

Az internetes közösségi média napjainkban meghatározó és egyre növekvő szerepet tölt be a világ szinte valamennyi országának társadalmi, gazdasági és politikai életében.[260] A közösségi média platformokon megosztott tartalmak érdemben befolyásolják a felhasználók vélekedését a világban zajló történésekről, alakítják ideológiai, vallási, szociális stb. nézeteiket. A *közösségi médiából történő adatszerzés* (SOCMINT[261]) ezért a 2010-es évek eleje óta[262] egyre növekvő szerepet játszik a nemzetbiztonsági szolgálatok és a rendvédelmi szervezetek információszerző tevékenységében.

---

259 VIDA Csaba: Egyéb hírszerzési ágak. In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 162–167. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

260 2018 januárjában a Föld 4,021 milliárd lakója rendelkezett internet hozzáféréssel, közülük 3,196 milliárd fő egyben valamely közösségimédia-oldal felhasználója is volt. A közösségimédia-platformok tagjainak száma 2017 óta 13%-kal növekedett. A tanulmány felhasználónak tekinti a közösségimédia-oldalak azon regisztrált tagjait, akik legalább havi rendszerességgel bejelentkeznek a profiljukba.
KEMP, Simon: Digital in 2018: World's internet users pass the 4 billion mark. We Are Social, 2018.01.30. https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018/; letöltés: 2022.04.26.

261 Social Media Intelligence.

262 A SOCMINT fogalmát először a Sir David Omand – Jamie Bartlett – Carl Miller szerzőhármas használta a 2012-ben megjelent #INTELLIGENCE című értekezésében.
OMAND, David – BARTLETT, Jamie – MILLER, Carl: #Intelligence. London, Demos, 2012. https://demos.co.uk/wp-content/uploads/2012/04/intelligence-Report.pdf; letöltés: 2018.11.05.

A közösségimédia-oldalak megjelenése gyökeresen megváltoztatta a felhasználók jelentős hányadának internetezési szokásait. A felhasználók egyre bővülő körében jellemző, hogy az internetes tartalmakat valamely közösségimédia-platformon, elsősorban a Facebookon[263] keresztül fogyasztják. Ennek következtében a tradicionális internetes médiafelületeken – hírügynökségek, újságok honlapjain, blogokon stb. – található információ csak akkor éri el a felhasználók (a tulajdonképpeni társadalom) jelentős részét, ha azok valamely közösségi médiafelületen megjelennek. Hasonló a helyzet az állami szervezetek esetében is, hiszen internetes közösségimédia-jelenlét hiányában egyre kevésbé képesek kapcsolatot tartani az állampolgárokkal.[264]

A véleménybuborékok kialakulása és jelentősége

A közösségi platformok a profitmaximalizálás[265] (a felhasználók számának bővülésével a hirdetési bevételek növekednek) érdekében igyekeznek érdekes, színes, egyben biztonságot nyújtó „felhasználói élményt" nyújtani a számukra. A platformok, elsősorban a Facebook működésének egyik fő jellegzetessége, hogy a felhasználók üzenőfalain megjelenő tartalmak a saját preferenciáik (beállításaik és csoporttagságaik), valamint a böngészési előzményeik alapján a platformok üzemeltetőinek MI-alapú elemző szoftverei által meghatározott egyéni habitusuknak megfelelően jelennek meg. A platformok tehát olyan tartalmakat állítanak össze a felhasználók számára, amelyeket azok az egyre kifinomultabb algoritmusok alapján szívesen megtekintenének, és ezekbe illeszkedve helyezik el – sokszor felismerhetetlenül – a hirdetéseket is. A felhasználók emellett a jellemzően hasonló értékrenddel rendelkező ismerősi körük hozzászólásait és megosztásait is látják.

Az egyénre szabott, MI-alapú tartalomszolgáltatás eredményeként a felhasználók többségének online tartalomfogyasztása – a szolgáltatók által sem kívántan, mintegy járulékos következményként – egyéni és csoportos „véleménybuborékokban"[266] valósul meg. A buborékokban a felhasználók (ismerősök) csoportjai hasonló világnézettel bírnak, a társadalmi jelenségekkel kapcsolatos álláspontjuk konvergál. A saját véleménnyel kapcsolatos folyamatos pozitív visszacsatolás az ismerősi kör, illetve a platformok MI-rendszere által javasolt tartalmak (cikkek, videók, blogbejegyzések stb.) részéről azt az illúziót kelti a véleménybuborékban elhelyezkedő egyének sokasága

---

263 A Facebook 2018 januárjában 2,17 milliárd felhasználóval rendelkezett, ami 15%-os növekménynek felel meg egy év alatt.
KEMP, Simon: Digital in 2018: World's internet users pass the 4 billion mark. We Are Social, 2018.01.30. https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018/; letöltés: 2022.04.26.

264 Vida Csaba részletesen bemutatja a SOCMINT kialakulásának hátterét.
VIDA Csaba: A SOCMINT szerepe az elemző-értékelő munkában. Az új hírszerzési ág elemző-értékelő megközelítése. Szakmai Szemle, XX. évfolyam 2. szám, 2022. június. pp. 5–21. https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf; letöltés: 2022.10.28.

265 A Facebook vállalat 2017-ben 40,653 milliárd dollár bevételre tett szert. A vállalat piaci kapitalizációja 2018. november 15-én 413,395 milliárd dollár volt.

266 A véleménybuborék (*filter bubble*) jelenségét Eli Pariser internetes aktivista alkotta meg.
PARISER, Eli: The Filter Bubble: What The Internet Is Hiding From You. A szerző 2011. június 20-ai előadásának pdf-változata.
http://www.lse.ac.uk/assets/richmedia/channels/publicLecturesAndEvents/slides/20110620_1830_theFilterBubble_sl.pdf; letöltés: 2018.11.22.
A „buborék" kifejezés igen találó, mert lefedi a jelenség valóságtorzító hatását, egyben ráérez, hogy tudatos internetfogyasztással (még) van lehetőségük a felhasználóknak az objektív tájékozódásra.

számára, hogy nézeteik a társadalmi többség álláspontját tükrözik.[267] A közösségi média ezért a posztmodern[268] társadalomszerkezet kialakulását felgyorsítja és a valóság percepciójának nagymértékű torzulását eredményezi.

Részben az online közösségi médiafogyasztás következménye, hogy az objektív, ellenőrzött információ értéke háttérbe szorul, előtérbe helyezve a felhasználók által követett véleményformálókat és a közösségimédia-platformokon meglévő ismerősöket. Az online közösségi hálózatokban – jellemzően a buborékokon belül – egyes személyek másoknál nagyobb befolyással rendelkeznek. Az ilyen véleményformálók a tartalommegosztásaikkal és a hozzászólásaikkal jelentős mértékben alakítják a hálózatok, áttételesen egy-egy társadalmi csoport valóságfelfogását és politikai állásfoglalását. A véleményformálók ezért a befolyásolási törekvések elsődleges eszközei és célpontjai. A posztmodern időszak médiafogyasztását a köznyelvben elterjedt „igazság utáni világ" (*post-truth*) kifejezés[269] jól megragadja.

A véleménybuborékok következtében a közösségi média használata elősegítheti, erősítheti és felgyorsíthatja egyes társadalmi csoportok szegregálódását és az arra fogékony személyek és csoportok eszméinek szélsőségessé, akár erőszakossá válását (radikalizálódását).

OSINT, SOCMINT és PAI

A klasszikus értelemben vett nyílt forrású hírszerzés (OSINT) az internetes tartalmak kinyerésében a keresőoldalak (pl. Google, Bing stb.) által indexelt és ezért látható, online profil létrehozásához nem kötött tartalmakra összpontosít. Az internetezési szokások változásával ez a módszer önmagában egyre kevésbé alkalmas a folyamatosan növekvő mennyiségű információ nyomon követésére és csak áttételesen teszi lehetővé például a véleményformálók azonosítását.

Mint láthattuk, az OSINT komplex tevékenységet takar, amelynek során a nyílt – egyebek mellett az interneten megosztott – információk speciális módszertan alapján történő felkutatását, gyűjtését, szelektálását, értékelését és felhasználását jelenti.

A „*nyilvános forrású információszerző tevékenység*" (PAI[270]) a nyílt adat és információ értékelését nem, vagy csak minimális mértékben foglalja magában. A PAI fókuszában a résztevékenységekhez (pl. SOCMINT) szükséges, illetve a hírigényt megfogalmazó elemző-értékelő, HUMINT-, SIGINT-, terrorelhárító stb. szervezetek tevékenységéből eredő specializáció áll. A nyílt adatszerző tevékenységet

---

267 LOVÁSZ Dávid: A véleménybuborék jelensége a közösségi médiában. Kalauz, 2017. https://kalauz.lib.pte.hu/velemenybuborek-jelensege-kozossegi-mediaban/#dn01; letöltés: 2018.11.14.

268 A modernitás jelenlegi állomásának tekintett, az 1970-es évek óta kibontakozó posztmodern kor leírásakor a mérvadó források a világot leíró úgynevezett metanarratívák érvényvesztését emelik ki. A korszak általános jelenségeként jelenik meg „a kétség, a jövőkép bizonytalansága, a személyiség tartalmainak és kibontakozásának kérdésessége".
Kulturális Enciklopédia: A posztmodern.
http://enciklopedia.fazekas.hu/irodalom/Posztmodern.htm; letöltés: 2018.11.15.

269 Az Oxford University Press által működtetett Oxford Universities honlap a kifejezést a 2016-os év szavának választotta.

270 Publically Available Information – PAI.

végző, többségükben magas szintű informatikai ismeretekkel rendelkező szakembereknek köszönhetően a nyíltan hozzáférhető információk köre jelentősen kibővül. Ennek köszönhető, hogy a PAI és a kiberhírszerzés (CYBINT) határai a külső szemlélő számára elmosódnak. A PAI-szakemberek számára tevékenységük határvonalát a felhasználók által gondatlanul kezelt vagy – akár egy fotón vagy videón – elhelyezett információ jelenti, míg a CYBINT a felhasználó (célszemély vagy látókörbe került személy[271]) által nem publikusan tárolt információt illegálisan szerzi meg.

A PAI-tevékenység során megszerzett információ sokszor – elsősorban harcászati/taktikai szintű felhasználásra – önmagában is felhasználható. Optimális esetben az egyes PAI-információk hadműveleti, illetve hadászati/stratégiai célú felhasználását vagy a felhasználás előkészítését az információk rendszerezésével, szerkesztésével, értékelésével stb. az OSINT-szervezetek (részlegek) végzik. A korszerű nemzetbiztonsági és rendvédelmi tevékenységben az OSINT-tevékenység tehát nagymértékben szegmentálódik, a megszerzett adatok és információk sokfélesége miatt azok – hasonlóan más hírszerzési ágakhoz – már csak azok előzetes feldolgozását követően használhatók fel az összadatforrású elemzés-értékelésben.

A PAI-tevékenység nagymértékű specializációja lehetővé teszi, hogy az részben átvegye más hírszerzési területek, különösen a HUMINT (pl. a célszemély közösségi médiatevékenysége, blogbejegyzései, a vele készített interjúk felhasználása stb.), az IMINT (pl. Google Maps és Bing Maps, internetes fotómegosztó szolgáltatások és az ezeket célzottan felhasználó alkalmazások), valamint a GEOINT (pl. objektumok lokációja vagy infrastruktúrája interneten elérhető információk vagy kereskedelmi műholdfelvételek megvásárlásával) szerepét. Az ilyen lehetőségek kihasználására a technológiát jól ismerő szakértőknek van lehetőségük. A PAI-adatok felhasználásának hatékonysága ugyanakkor abban az esetben maximalizálható, ha azokat a hírszerzési ágak tevékenységének támogatására, illetve az általuk szerzett információ kiegészítésére (pl. kontextusba helyezésére) használják fel. Az összadatforrású szemlélet mellett szól az is, hogy a PAI-információkat sok esetben csak a hírszerzési ágak szakemberei képesek teljes mértékben felhasználni, ahogyan például a nyílt forrásból elérhető képek vagy műholdfelvételek esetében.

A SOCMINT térnyerése

A SOCMINT a PAI-tevékenység közösségi médiára specializálódott része. A közösségi média fontosságára már a 2012-es „arab tavasz” jellegzetességei is felhívták a figyelmet, de a SOCMINT jelenlegi módszertanának kialakulását az ISIL/DAESH által rendkívüli hatékonysággal és profizmussal végzett, toborzó célú médiatevékenység tette szükségessé, amely jelentős részben az internetes közösségi médiában valósult meg. Az ISIL/DAESH-hez csatlakozott több tízezer külföldi

[271] Person of Interest – PoI. A „látókörbe került személy” fogalom használata szerencsésebb, mert segít tudatosítani, hogy egy személy közösségi médiatevékenységének hatóság általi vizsgálata önmagában nem eredményezhet joghátrányt.

terrorista harcos (FTF[272]) közül több ezren európai,[273] észak-amerikai és kaukázusi (oroszországi) muszlim közösségekből érkeztek, akik a terrorszervezet által a Közel-Keleten létrehozott „Kalifátusból" 2012-től kezdődően egyre erősödő, célzott propagandakampányt indítottak otthon maradt hittársaik körében is.

A külföldi terrorista harcosok a nyugati hatóságok számára sokáig láthatatlan vagy marginálisnak értékelt tevékenységének jelentősége a 2014. májusi (majd 2016. márciusi) brüsszeli, a 2015. januári verviersi, a 2015. novemberi párizsi és a 2016. júliusi nizzai terrormerényletek hatására vált nyilvánvalóvá. A támadássorozatot az ISIL/DAESH a közel-keleti „Kalifátusából" irányította. Az európai terrorellenes intézkedések és az ISIL/DAESH iraki és szíriai területei elleni globális fellépés hatására 2015-től előtérbe kerültek a terrorista propaganda által radikalizálódott személyek által magányosan,[274] de a terrorszervezet által támogatottan elkövetett támadások.[275] A közösségi média kiaknázására irányított új kormányzati erőforrások segítségével lehetővé vált egy olyan, párhuzamos társadalom feltárása, amelyben a többségükben Nyugat-Európában született és nevelkedett, arabul csak kis hányadban beszélő fiatal muszlimok az ISIL/DAESH és más terrorszervezetek, egyebek mellett a módszert átvevő al-Kaida ideológiáját magukévá teszik és terjesztik, állampolgárság szerinti hazájuk ellen használva fel azokat. A radikális ideológiák mellett a közösségi hálókon a támadások a válságkörzetekben, elsősorban Afganisztánban, a Közel-Keleten és Észak-Afrikában tökéletesített módszertana mellett a nyugati környezetre szabott harceljárások – például a gázolásos, késeléses (7. ábra) vagy a tömegközlekedési eszközök ellen kidolgozott merényletek – is gyorsan, közérthető (pl. poszteres, piktogramos, infografikai) formában terjednek. A tömegmédiában és a videojátékokban

---

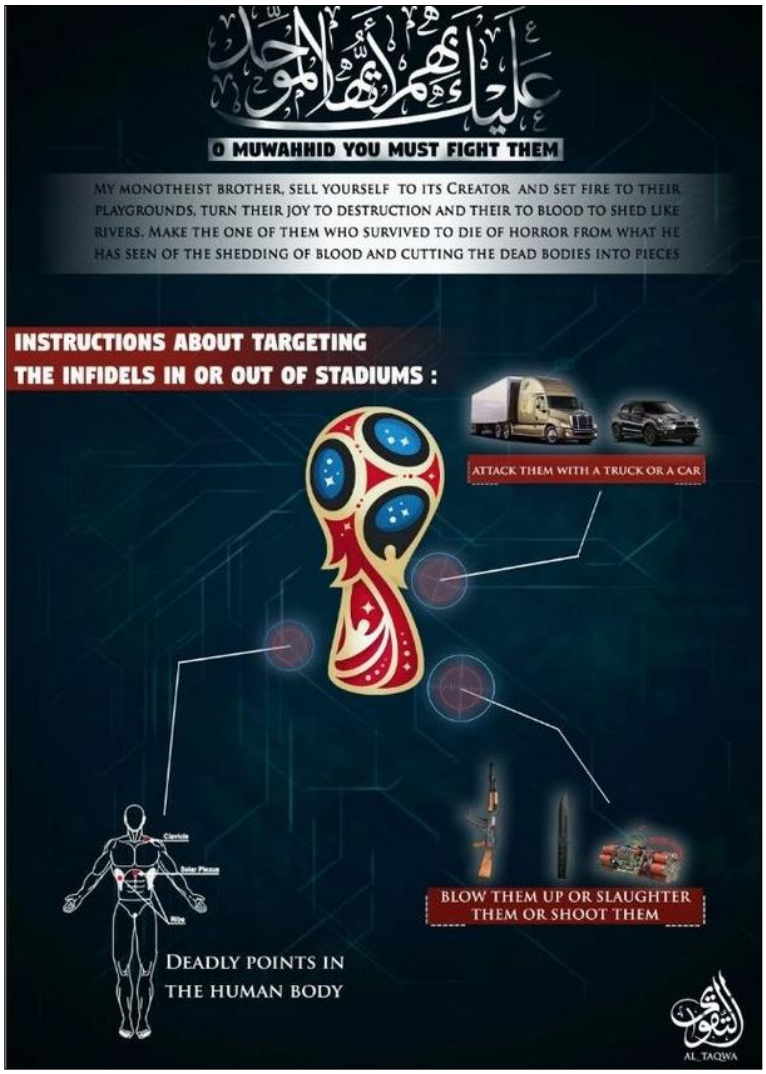
[272] Foreign Terrorist Fighter. Az ENSZ Terrorelhárítási Hivatalának (United Nations Office of Counter-Terrorism) 2017. júliusi jelentése szerint 2011 és 2016 között több mint 25 ezer FTF csatlakozott az ISIL/DAESH-hez.
BARRETT, Richard – EL-SAID, Hamed: Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria. United Nations Office of Counter-Terrorism, July 2017.
https://f-origin.hypotheses.org/wp-content/blogs.dir/2725/files/2018/02/ONU_Report_Final_2017.pdf; letöltés: 2018.11.15.

[273] A hágai Nemzetközi Terrorelhárító Központ (International Centre for Counter-Terrorism – ICCT) 2018. áprilisi értékelése szerint 2012 óta 5000 harcos csatlakozott az ISIL/DAESH-hez Európából.
COOLSAET, Rik – RENARD, Thomas: The Homecoming of Foreign Fighters in the Netherlands, Germany and Belgium: Policies and Challenges. ICCT, 2018.04.11.
https://www.icct.nl/publication/homecoming-foreign-fighters-netherlands-germany-and-belgium-policies-and-challenges; letöltés: 2018.11.15.

[274] Úgynevezett „*lone wolf*" merényletek. Daniel Byman, az amerikai Brookings kutatóintézet 2017. júniusi szenátusi meghallgatásán kifejtette, hogy a magányos merénylők által elkövetett terrortámadásokban tevékeny szerepet játszanak a Közel-Keleten tartózkodó FTF-ek, akik egyebek mellett tanácsokkal látják el a merénylőket a közösségi médián keresztül. A merényletek megelőzésére a szakértő a közösségi média hatékonyabb monitorozását javasolja.
BYMAN, Daniel: Beyond Iraq and Syria: ISIS' ability to conduct attacks abroad. Brookings, 2017.06.08.
https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad; letöltés: 2018.11.15.

[275] Inspired attack. Julian King, az Európai Bizottság Biztonsági Unióért (Security Union) felelős akkori biztosa 2017. decemberi értékelése szerint „*közvetlen kapcsolat áll fenn a közelmúltbeli európai támadások és az ISIL/DAESH-hez hasonló terrorszervezetek által … online terjesztett tartalom között*".
Fighting Terrorism Online: Internet Forum pushes for automatic detection of terrorist propaganda. European Commission, 2017.12.06.
http://europa.eu/rapid/press-release_IP-17-5105_en.pdf; letöltés: 2018.11.15.

megszokott kommunikációs és megjelenítési panelek hatékonyságán túl az volt a nemzetbiztonsági szolgálatok fő felismerése, hogy a közösségi médiában megosztott tartalmak kinyeréséhez a meglévő módszerek elégtelenek.



7. ábra. Példa az ISIL/DAESH által online terjesztett indoktrinációs infografikára[276]

[276] DAVIDSON, Tom: „Attack them with truck or car": ISIS release sick pamphlets with tips on successful terror attacks during World Cup. Mirror, 2018.05.15. https://www.mirror.co.uk/news/world-news/attack-truck-car-isis-release-12541581; letöltés: 2021.04.16.

A SOCMINT módszertana

Hasonlóan az OSINT kezdeti kialakításának idejéhez, a szakemberek ismét a HUMINT már jól kidolgozott módszertanához nyúltak segítségül.[277] A közösségimédia-platformok sajátosságai miatt a SOCMINT-ot megkülönbözteti a klasszikus OSINT-tevékenységtől, hogy az érdemi információ kinyeréséhez felhasználónévhez kötött online profil szükséges. Emiatt az adatszerzőknek a SOCMINT-tevékenységhez olyan fedőprofilokat[278] kell létrehozniuk és működtetniük, amelyek semmit sem árulnak el a valós felhasználókról, de a célszemélyekben és -csoportokban sem keltenek gyanút. Jogi és műveleti biztonsági megfontolásokból a SOCMINT-tevékenység során az adatszerzők fő szabály szerint nem lépnek interakcióba a közösségi médiában. Erre már – indokolt esetben – a virtuális HUMINT-tevékenység során kerül sor. A SOCMINT az OSINT/PAI egyéb területei és a CYBINT között félúton helyezkedik el abban a tekintetben, hogy a nyilvánosan megosztott információk megszerzésére szakosodik ugyan, de a fedőprofilok használatával megtéveszti a közösségimédia-vállalatokat, valamint a célszemélyeket és -csoportokat.

A SOCMINT-forrásból megszerzett információk elemzés-értékelésében nem csak az ilyen információk nagy mennyisége jelent kihívást, hanem azok rendszerezetlensége is. Ennek oka, hogy az egyéb, nyílt forrású információkkal ellentétben a SOCMINT-információk forrásául szolgáló közleményeknek elsődleges célja nem a tájékoztatás, hanem az információt megosztó személyek egyéni, szubjektív véleményének közlése, illetve részvétele a közösségi térben. A tájékoztatási célból megosztott információk is gyakran csak a kontextus ismeretében értelmezhetők, és figyelembe kell venni, hogy azokat nem szakértők, hanem az események résztvevői vagy érintettjei teszik közzé. Ezért az adatgyűjtőknek különös gonddal kell dokumentálniuk a megszerzett információ környezetét leíró adatokat (metaadatokat). Erre azért is szükség van, mert az információk felhasználói jellemzően az internetről fizikailag leválasztott hálózatokon dolgoznak, ahol nincs lehetőség az információ ellenőrzésére az internetes közösségi médián.

A SOCMINT-jelentéseknél az adatgyűjtők számára olyan sablonokat kell rendszeresíteni, amelyek biztosítják a feldolgozáshoz és az elemzés-értékeléshez szükséges metaadatokat, bemutatva az információ környezetét. Ezt indokolja az is, hogy a közösségi média közege dinamikusan változik: a felhasználók (célszemélyek) könnyen változtathatják a felhasználónevüket, a közösségimédia-oldaluk elérhetőségét (urljét), a profilképüket stb., ezért ezeket egy adott időpillanatban rögzíteni kell és meg kell adni azokat az azonosítókat (elsődlegesen a közösségimédia-oldal egyedi azonosítóját, úgynevezett UID-ját[279]), amelyeket a felhasználók nem tudnak módosítani. A közösségi médián megjelenő információ gyakran vizuális jellegű, ezért

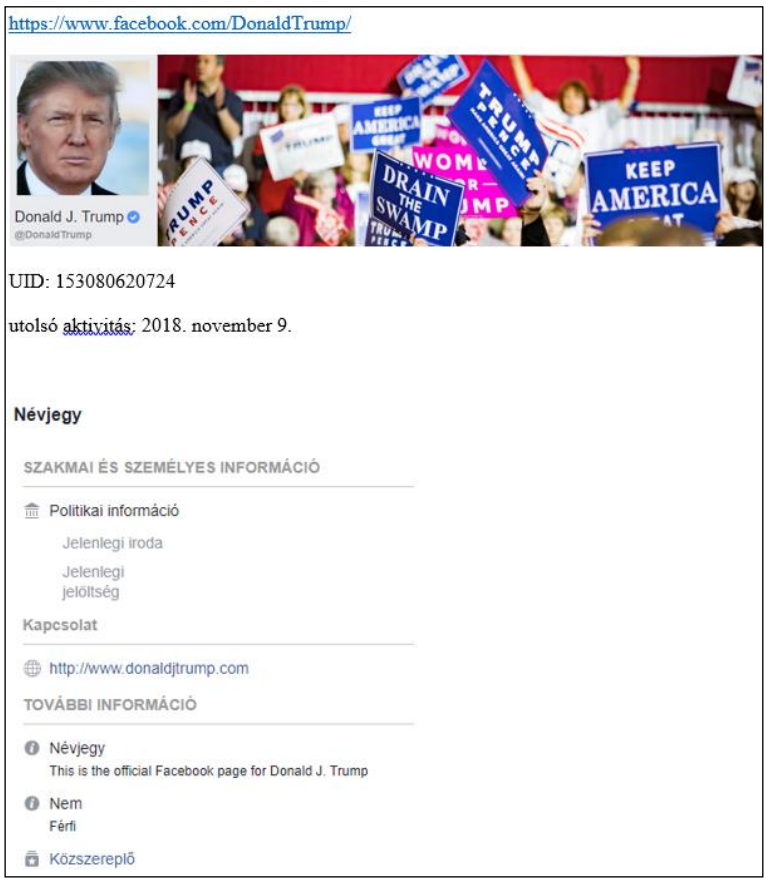
---

[277] A „klasszikus” OSINT-tevékenység kialakítása során például a források osztályozási rendszerét vették át a HUMINT-tól.

[278] Cyber handle.

[279] Unique Identification. Az UID platformonként különböző módokon nyerhető ki, például a Facebook esetében (*profile id, page id*) az oldal forrásának megtekintése mezőben a *profile_id=* szöveget követő szám. Az UID kinyerhető a profilon található fotók elérési útjának kimásolásával is. A UID-ok alapján a Facebook-profil visszakereshető: a *facebook.com/profile.php?id=* szöveget követően be kell illeszteni az UID-ot. Az így kapott elérési út alapján a böngésző címsorába illesztve a keresett Facebook-profil jelenik meg.

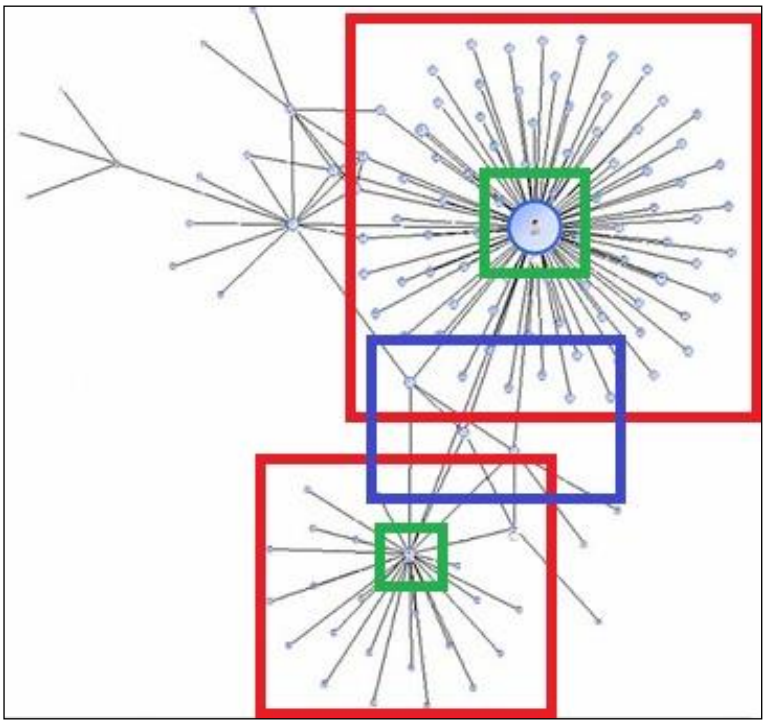
a célszemélyek által megosztott releváns képek és videók rögzítése is szükséges, mert információt hordozhatnak az elemzők és más szakértők számára. Minden szubkultúrának megvan a maga jelképrendszere, amelyek ismerete nélkül nem lehet a közléseiket értelmezni. A célszemélyek a hovatartozásukat vagy egy adott eseménnyel kapcsolatos állásfoglalásukat is gyakran képekkel fejezik ki. Az adatlapnak minimálisan az alábbi ábrán szereplő információkat kell tartalmaznia.



8. ábra. Egy Facebook-profil adatlapja (minta)

Ezután következnek a célszemély vagy -csoport által megosztott információk, az adatlaphoz hasonló formátumban. A megosztott információk esetében mindenképpen rögzíteni kell a megosztás idejét. A megosztott információkat szövegesen is össze kell foglalni. A szöveges összefoglaló minden megállapítását – az értékelést leszámítva – a közösségimédia-profilokon található információkkal kell alátámasztani. Így elkerülhető az adatgyűjtő szubjektivitásának torzító hatása, illetve lehetővé teszi az információk későbbi könnyű visszakeresését, aktualizálását.

A felhasználók által megosztott információk vizsgálatakor az ismerősi körre vonatkozó adatok kiemelt jelentőséggel bírnak. A közösségimédia-ismerősök, illetve az üzenőfalakon hozzászólók és kedvelők metaadatainak (profilnév, UID stb.) automatizált kinyerésével lehetővé válik a kapcsolati hálók felrajzolása és elemzése. Erre a célra számos ingyenes és fizetős szoftver áll rendelkezésre, mint például az IBM i2 Analyst's Notebook programja. A metaadatok szoftveres elemzésével lehetővé válik egyebek mellett a hálózatok kulcsfiguráinak vagy a hálózatok közötti kapcsolattartók azonosítása. Az így megszerzett információk az elemzés hozzáadott értékének tekinthetők, hiszen azok a legegyszerűbb hálózatok kivételével szoftveres segítség nélkül nem lennének láthatók.



9. ábra. Csoportok (piros), csoportvezetők/véleményformálók (zöld) és kapcsolattartók (kék) megjelenítése az IBM i2 Analyst's Notebook programban

A SOCMINT-tevékenység csak akkor lehet igazán eredményes, ha az állandó kapcsolatban áll a hírszerzés más ágaival: azok információit használja fel és saját információival azokat támogatja. Ez azért is fontos, mert a SOCMINT által vizsgált személyek és csoportok közösségi média profiljai sokszor nem utalnak tulajdonosaik valós tevékenységére. Az illegális vagy fedett tevékenységgel gyanúsított célszemélyek vagy csoportok a saját névvel létrehozott profilokat (hivatalos) kapcsolattartásra, az illegális tevékenységgel összefüggésben használt profilokat álnévvel használják.

A profilok felderítéséhez például a nevet vagy álnevet,[280] a mobiltelefonszámot vagy e-mail-címet, illetve fotót tartalmazó minősített információ szükséges. A minősített információ alapján speciális eljárásokkal el lehet jutni a célszemélyek profiljaihoz. A közösségi médián megosztott tartalmak kiegészítő információt jelenthetnek a célszeméllyel kapcsolatban, a nyilvános ismerősi kör és az üzenőfalakon megvalósuló kommunikáció pedig lehetővé teszi a hálózatok felderítését. Az így megszerzett és előértékelt SOCMINT-információ tovább gazdagítja a nemzetbiztonsági szolgálatok és a rendvédelmi szervezetek összadatforrású adatbázisát.

Amennyiben a közösségimédia-profilon olyan derogáló információ kerül megosztásra, amely tulajdonosának erőszakos radikalizmusát vagy illegális tevékenységét bizonyítja, a hatóságok a közösségimédia-vállalathoz fordulhatnak a felhasználó adatainak és kommunikációjának kikérésére. A szolgáltatók erre bírósági úton is kötelezhetők. Derogáló tartalom híján erre nincs lehetőség, ilyenkor offenzív CYBINT-módszerekkel (a fiók feltörésével) lehetséges az adatok beszerzése.

A már felderített vagy egyéb módon meghatározott csoportok monitorozásával lehetőség nyílhat azok tevékenységének előrejelzésére, véleményének nyomon követésére. Indokolt esetben a nemzetbiztonsági szolgálatok vagy a rendvédelmi szervezetek úgy határozhatnak, hogy az üzenőfalakon észlelt negatív folyamatokat – például a csoport radikalizálódását, erőszakossá válását – a közösségimédia-felületen kísérlik meg ellensúlyozni. Ebben az esetben a jól felépített, a csoport karakterébe illő és korábban a csoport érdeklődési körében releváns módon megnyilvánult fedőprofilokkal megkísérelhető a csoportok befolyásolása. Ez kockázatos lépés, mert a fedőprofillal végrehajtott kommunikáció célja nem lehet nyilvánvaló, illetve a véleménynyilvánítást követően a profil legendájának[281] intenzív tesztelésére kell számítani.

Az OSINT/PAI és a SOCMINT helye a nemzetbiztonsági tevékenységben

Nem lehet egyértelműen és általános érvényű állást foglalni abban a kérdésben, hogy az OSINT/PAI-tevékenységnek elkülönülten vagy más hírszerzési ágakba, illetve az elemzés-értékelésbe ágyazva kell-e megvalósulnia. Nézetem szerint az OSINT/PAI a nemzetbiztonsági tevékenység szinte minden szegmensének hasznos, sőt egyre inkább elengedhetetlen eleme, amelynek bizonyos szintű ismerete napjainkban minden műveleti munkatárstól elvárható. A komplex OSINT-, illetve PAI-tevékenység ugyanakkor olyan mértékű specializációt igényel, amely már nem várható el az ágazati szakemberektől, ezért külön szervezeti egységként működtethető optimálisan. A specializáció mértéke indokolhatja az OSINT és a PAI bizonyos szintű szervezeti szétbontását is, hiszen más típusú szakembergárdát igényel a stratégiai/hadműveleti szintű OSINT és az inkább IT-fókuszú PAI.[282] Ennek ellenére indokolt a két tevékenység bizonyos szintű integrációja is, hiszen egymásra kölcsönösen hatnak.

---

[280] Szélsőséges iszlamista harcosok esetében úgynevezett „*kunya*” vagy „*nom de guerre*”.

[281] A profil adatlapjának, a megadott elérhetőségeknek és az azokhoz köthető egyéb közösségimédia-profilok koherens egésze.

[282] Például a közösségimédia-platformok nyújtotta nyílt lehetőségek teljes kihasználásához legalább alapszintű programozói ismeretek szükségesek.

Az OSINT/PAI-tevékenység részének tekinthető SOCMINT szintén speciálisan képzett szakembergárdát kíván, mert a közösségimédia-portálok jellegzetességeinek ismerete, a fejlesztések nyomon követése, valamint a célcsoportok beható ismerete az adat- és információfeldolgozási módszertannal kiegészülve önálló szakmának tekinthető.

A mindennapi feladatok támogatását a merev, bürokratikus jellegű állománytáblákhoz ragaszkodás helyett jobban szolgálná a projektszemléletű megközelítés. Az OSINT/PAI-szervezet egy erre kialakított, elkülönített állománykeretből (poolból) a szervezeti egységek által megfogalmazott, konkrét igényeknek megfelelően szakembereket vagy csoportokat delegálna, amelyek a feladat végrehajtásáig támogatnák a munkát.

Az információs műveletek és a kiberműveletek[283]

Napjainkban a nemzetállamok közötti versengés kiterjed a hálózatos számítógépes rendszerek alkotta virtuális, mesterséges információs térre (a kibertérre). Az utóbbi szűk négy évtizedben kiépült kibertér az óceánokhoz, a légtérhez, a világűrhöz hasonlóan a globális közjavak[284] részévé vált. A kibertérhez történő hozzáférés minden modern nemzetállam alapvető szükséglete, a gazdaság, a társadalom, a politikai rendszer és a haderő működésének feltétele. Az információs tér támadása és védelme a modern nemzetállamok közötti fegyveres konfliktusok részévé vált. Azontúl, hogy a fejlett országok gazdasága kizárólag kibertámadásokkal is rövid idő alatt megbénítható, az információs műveletek eszközeivel a modern haderő hadászati, műveleti és harcászati szinten is sebezhető, így az információs tér közvetlenül is meghatározza a nemzetállamok közötti modern kori fegyveres konfliktusokat.

Az információs műveletek a nemzetbiztonsági rendszer számára is kiemelt és növekvő feladatot jelentenek. Az évtizedek óta tartó folyamatot tovább gyorsítja és mélyíti a mesterséges intelligencia elterjedése, a negyedik ipari forradalom, az IoT, illetve az 5G elterjedése, hiszen mindezek hatására máris alig lehet olyan emberi tevékenységet elképzelni, amelyek ne az információs téren alapulnának.

A kritikus infrastruktúrák és a kibervédelem

Az információtechnológia meghatározó a modern társadalom, gazdaság, állam és haderő működése szempontjából. A számítógépes információs hálózatok az összes társadalmi alrendszer hatékonyságát jelentősen növelik, ugyanakkor függőséget is okoznak. A modern társadalmakban a kritikus infrastruktúrák – „*olyan,*

---

283 A fejezet eredeti formájában 2012-ben, a Felderítő Szemle folyóiratban jelent meg.
ERDÉSZ Viktor – NAGY Viktor: Az információs védelem és az információs műveletek szerepe a nemzetvédelemben. Felderítő Szemle, X. évfolyam 3–4. szám, 2011. szeptember–december, XI. évfolyam 1. szám, 2012. március. pp. 50–62.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2011-3-4-2012-1.pdf; letöltés: 2021.12.16.

284 Global commons.

egymással összekapcsolódó, interaktív és egymástól kölcsönös függésben lévő infrastruktúra elemek, létesítmények, szolgáltatások, rendszerek és folyamatok hálózata, amelyek az ország (lakosság, gazdaság és kormányzat) működése szempontjából létfontosságúak, érdemi szerepük van egy társadalmilag elvárt minimális szintű jogbiztonság, közbiztonság, nemzetbiztonság, gazdasági működőképesség, közegészségügyi és környezeti állapot fenntartásában, és ezért meg kell felelniük az alapvető biztonsági, nemzetbiztonsági követelményeknek".[285] Működésüket a kritikus információs infrastruktúrák, vagyis „*azon infokommunikációs rendszerek, amelyek magukban kritikus infrastruktúrák, vagy ilyenek működéséhez elengedhetetlenül szükségesek*"[286] – teszik lehetővé. Ennek következtében a kritikus információs infrastruktúra információs (kiber-) vagy fizikai támadásával valamennyi nemzeti és nemzetközi kritikus infrastruktúra működése akadályozható vagy megbénítható.

Ilyen támadásokkal – vezető nyugati politikai és katonai vezetők, szakértők véleménye szerint – a tömegpusztító fegyverek hatásához mérhető károk okozhatók.[287] A kritikus nemzeti infrastruktúrák ellen a számítógépes hálózatokon végrehajtott és a kritikus nemzeti információs infrastruktúrákat érő fizikai támadásokkal a modern állam működése rövid idő alatt részben vagy egészben megbénítható. A kibertámadás anyagi és személyi költségei a hagyományos – fegyveres – támadásokkal összemérve minimálisak. A végrehajtást előkészítő felderítés – megfelelő szakmai ismeretek birtokában – akár a nyílt adatforrású hírszerzés (OSINT) módszerével, bárki számára hozzáférhető információk felhasználásával is elvégezhető. A nemzeti kritikus infrastruktúrák közül elsősorban az elektronikus média, a műsorszórás, az internetes média, a pénzügyi szektor, a közlekedés, a telekommunikáció, az internet és a villamosenergia-szolgáltatás elleni kibertámadás okozhat komoly károkat.[288] Az elektronikus közigazgatás fejlesztésével az államigazgatás veszélyeztetettsége tovább növekszik.

---

[285] 2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. https://njt.hu/jogszabaly/2008-2080-30-22; letöltés: 2021.07.24.

[286] Green Paper on a European Programme for Critical Infrastructure Protection. Európai Bizottság, Brüsszel, 2005.11.17. https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en; letöltés: 2021.07.20.

[287] A Center for Strategic and International Studies nevű, washingtoni székhelyű kutatóintézet 2008 decemberében megjelent tanulmánya szerint a kibervédelem fejlesztése az Amerikai Egyesült Államok egyik legfőbb nemzeti biztonsági kihívása, egyenrangú a tömegpusztító fegyverek proliferációjával és a nemzetközi terrorizmussal.
LEWIS, James Andrew: Securing Cyberspace for the 44th Presidency. Center for Strategic and International Studies, 2008.12.08.
https://www.csis.org/analysis/securing-cyberspace-44th-presidency; letöltés: 2021.07.20.
Ezt az álláspontot tükrözi az Amerikai Egyesült Államok kiberműveleti stratégiája (National Cyber Strategy of the United States of America) is.

[288] KOVÁCS László – KRASZNAY Csaba: Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 3. évfolyam 2. szám, 2010. február. pp. 44–56. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/1013; letöltés: 2022.10.25.

Munk Sándor *A kritikus infrastruktúrák védelme információs támadások ellen* című, a Hadtudomány folyóiratban 2008-ban megjelent dolgozatában[289] behatóan foglalkozik az kibervédelem[290] fogalomkörével. Álláspontja szerint a kibervédelem is a kritikusinfrastruktúra-védelem része, feladata a kritikus nemzeti infrastruktúrák kibertámadások elleni, valamint a kritikus informatikai infrastruktúrák kiber- és fizikai hatások (támadások) elleni védelme. Az „*információs hatás az a hatás, amely a veszélyeztetett rendszer által értelmezhető, feldolgozható információt juttat be, vagy a rendszer által kezelt információt, megvalósított információs tevékenységet módosít, töröl az adott (hagyományos információfeldolgozási vagy informatikai) rendszer saját folyamatai, résztevékenységei útján. Ebből következően nem tartom információs hatásnak az elektronikai támadás legtöbb hagyományos lehetőséget, például az elektronikai zavarást, lefogást, megsemmisítést, vagy egy mágneses adathordozó tartalmának külső behatásra történő törlését*." A kibervédelem feladatai közé tartozik „*a kritikus infrastruktúrák elleni információs támadásokat végrehajtók felderítése, az információs támadások detektálása (…), illetve a támadók elleni fellépés*" is. A nemzetközi és a hazai szakirodalomban is elterjedt kibervédelem tehát az informatikai infrastruktúra információs hatások elleni védelmét jelöli.

Az információs műveletek

Ahogy a kritikus nemzeti infrastruktúrák védelmében nélkülözhetetlen a kibervédelem, úgy a modern haderők információs alapokra helyezésével, a hálózatközpontú hadviselés[291] elterjedésével a haderő számára is elkerülhetetlen az információs műveletek,[292] szélesebb körben elterjedt elnevezéssel az információs hadviselés[293] alkalmazása. Az információs műveletek definíciója a Katonai terminológiai értelmező szótár szerint „*Az a törzsfunkció, amelynek célja, hogy az információs környezet elemzése alapján megtervezze és integrálja, majd értékelje az információs tevékenységeket úgy, hogy azok végrehajtása biztosítsa a kívánt hatás elérését a célközönség akaratában, megértésében és képességeiben a küldetés célkitűzéseinek elérése érdekében.*"[294]

---

289 MUNK Sándor: A kritikus infrastruktúrák védelme információs támadások ellen. Hadtudomány, 18. évfolyam 1–2. szám, 2008. pp. 95–106. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/2224; letöltés: 2022.10.27.

290 Cybersecurity. Munk Sándor 2008-as dolgozatában az „információs védelem" kifejezés használatát javasolja, de időközben bevetté vált a „kibervédelem" kifejezés. Az „információs védelem" kifejezés használata azért sem célszerű, mert nehezíti a megértést a hasonló jelentésű, széles körben alkalmazott „információvédelem" kifejezés miatt.

291 Network-centric warfare, network enabled capability, network enabled operations. A hálózatközpontú haderő valós idejű információval rendelkezik mind a saját, mind az ellenséges csapatokról, azok helyzetéről, állapotáról, ezáltal a döntésekre szánt idő drasztikusan lecsökken, a döntések megalapozottabbak lesznek. A virtuális információs hálózatnak köszönhetően nem csupán a hadvezetés, hanem a harcmező minden szintje rendelkezik minden szükséges információval. Erre a hálózatra kapcsolódik a harctér minden szereplője, nemcsak a kémműholdak, a hajók és a harci repülőgépek, de a szárazföldi egységek is, a gyalogos katonáig bezárólag. A hálózatközpontú hadviselés alkalmazása jelentősen növeli a fegyveres erők hatékonyságát.

292 Information Operations – INFOOPS, IO.

293 Information Warfare – IW.

294 BERKÁNÉ DANESCH Marianne (szerk.) – M. SZABÓ Miklós – MEZŐ András (katonai szakmai szerk.): Katonai terminológiai értelmező szótár. Zrínyi Kiadó, Budapest, 2015.

Az információs dimenzióban (kibertérben[295]) megvalósuló információs műveletek a jelenkori fegyveres konfliktusokban a szárazföldi, légi, tengeri, kozmikus műveletek, dimenziók részét képezik. Az információs műveletek magukban foglalják az elektronikai hadviselést,[296] a rádióelektronikai felderítést (SIGINT), a számítógéphálózati műveleteket,[297] a pszichológiai műveleteket, a műveleti biztonságot,[298] a megtévesztést,[299] illetve a katonai információs infrastruktúra fizikai rombolását.[300] Az információs hadviselés elsődleges célja az információs fölény, uralom, és végül a vezetési fölény[301] elérése. A Stuxnet nevű számítógépes féreg megalkotásával a gyakorlatban is lehetővé vált a kritikus infrastruktúra információs infrastruktúrán keresztüli fizikai rombolása. A hadviselés információs dimenziója nem korlátozódik a kritikus katonai infrastruktúrára, annak a kritikus nemzeti infrastruktúrák is részei. Az információs műveletek szerepének növekedése miatt a nemzetközi szakirodalom egyetért abban, hogy a kibertér a hadviselés egy újabb – mesterségesen létrehozott – színtere a szárazföldi, légi, tengeri és kozmikus dimenziók mellett. A NATO 2016 óta tekinti önálló műveleti dimenziónak a kiberteret.[302] A kibertér ellenőrzése nélkül a többi dimenzió feletti ellenőrzés sem lehetséges. Jelentőségét mutatják a NATO-tagállamokban és máshol létrehozott, az információs műveletek irányításáért és összehangolásáért felelős szervezetek, mindenekelőtt az Amerikai Egyesült Államok Kiberműveleti Parancsnoksága (USCYBERCOM[303]). A NATO-hoz újonnan csatlakozott országok közül Lengyelország elsőként, 2010 nyarán hozta létre kibervédelmi központját.[304] A központ a haderő hálózatalapú képességekkel felszerelt zászlóaljának kibervédelmét is biztosítja.

A kibertér

Az információs dimenzió az információs műveletek működési környezete. Haig Zsolt és Várhegyi István *A cybertér és a cyberhadviselés értelmezése* című publikációjukban[305] kifejtik, hogy az információs műveletek fizikai, információs és tudati dimenziókra oszthatók. Az információs műveletek fizikai dimenziója az információs rendszerek elleni fizikai támadásokra és azok ilyen támadások elleni

295 Cyberspace domain.
296 Electronic Warfare – EW.
297 Computer Network Operations – CNO.
298 Operational Security – OPSEC.
299 Deception.
300 AJP 3.10 – Allied Joint Doctrine For Information Operations. NATO, November 2009. https://info.publicintelligence.net/NATO-IO.pdf; letöltés: 2021.07.20.
301 Az információs fölény a saját és az ellenséges erők harctéri környezetének ismerete között fennálló különbséget jelöli. Tartós megléte információs uralomhoz, majd vezetési fölényhez vezet.
302 Cyber defence. NATO, 2021. https://www.nato.int/cps/en/natohq/topics_78170.htm; letöltés: 2021.07.20.
303 United States Cyber Command.
304 ŚWIĄTKOWSKA, Joanna – ALBRYCHT, Izabela – SKOKOWSKI, Dominik: National Cyber Security Organisation – Poland. CCDCOE, Tallinn, 2017. p. 17. https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf; letöltés: 2022.09.12.
305 HAIG Zsolt – VÁRHEGYI István: A cybertér és a cyberhadviselés értelmezése. Hadtudomány, 18. évfolyam elektronikus szám, 2008. https://www.mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf; letöltés: 2021.07.20.

védelmére terjed ki. Az információs műveletek információs dimenziójában folytatott tevékenység az ellenséges információs folyamatok közvetlen fizikai rombolása nélkül korlátozza működésüket,[306] és megakadályozza a saját információs folyamatokra irányuló támadásokat. Végül az információs műveletek tudati dimenziójában folytatott tevékenységek az emberi gondolkodás befolyásolására irányulnak. A nemzetközi és a hazai védelempolitikai elemzésekben is előforduló „cyberspace", „cybertér", „kibertér" stb. kifejezéseknek több értelmezése is lehetséges. A kibertér szigorúan véve az információs műveletek információs dimenziójának felel meg. Ilyen értelemben a kiberteret az elektronikai eszközök és az elektromágneses spektrum segítségével adatok és információk tárolására, módosítására és cseréjére alkalmas, hálózatalapú számítógépes információs rendszerek alkotják. A kibertér az információs műveletek elemei közül az elektronikai hadviselés, a rádióelektronikai felderítés és a számítógéphálózati műveletek működési területe. Az információs műveletekben meghatározó és egyre növekvő jelentőségű számítógéphálózati műveletek a kibertérben folyó információs műveletek szűkebb értelmezését adják. Elemei: a számítógéphálózati támadás,[307] a számítógéphálózati felderítés[308] és a számítógéphálózati védelem.[309] Elsősorban a kibervédelemmel foglalkozó elemzésekben fordul elő a kibertérnek ez a szűkebb értelmezése. Legtágabb értelmezésben a kibertér az információs műveletek információs és tudati dimenziójának is színtere, tehát megfeleltethető a teljes információs dimenzióval. Ez az értelmezés egyszerűsége miatt is egyre elterjedtebbé válik a szakirodalomban. Fontos szempont az is, hogy az információs műveletek által kifejteni kívánt hatás tekintetében nehéz elválasztani egymástól az embert az általa alkalmazott eszköztől.

Kiemelt információs műveleti események

2007. április 26-án több héten át ismeretlen tettesek több százezer, hálózatba kapcsolt számítógép felhasználásával, túlterheléses támadásokkal (DDoS[310]) akadályozták az észt kormány, számos bank, nagyvállalat, illetve a média rendes működését. A támadással Észtország máig Oroszországot vádolja, ám konkrét bizonyítékot nem tud felmutatni. A támadás okaként egy szovjet hősi emlékmű áthelyezését nevezték meg, ami tüntetések sorozatát idézte elő mind Észtországban, mind Oroszországban. Észtország információs infrastruktúrája az egyik legfejlettebb a NATO-ban, így különösen veszélyeztetett az információs műveletek szempontjából. Az Észtország elleni volt az első nagyszabású támadás egy nemzetállam kritikus információs infrastruktúrája ellen.

A Grúzia ellen 2008. augusztus 7-én indított orosz szárazföldi és légi támadás bevezetéseként Oroszország DDoS-támadásokat intézett a grúz kritikus információs infrastruktúrák ellen. A cél kettős volt: az infrastruktúra ellehetetlenítésével a grúz katonai vezetés és a csapatok közötti kapcsolat megzavarása, valamint Grúzia

306 Adatszerzés, adatfeldolgozás, kommunikáció stb. elektronikus úton való, úgynevezett „puha típusú" vagy „*soft kill*" támadással.
307 Computer Network Attack – CNA.
308 Computer Network Exploitation – CNE.
309 Computer Network Defence – CND.
310 Distributed Denial of Service.

elvágása a külvilágtól. Elsősorban a kormányzat és a média internetes oldalait támadták, a grúz internetes oldalak védelmében amerikai és észt számítógépes szakemberek is részt vettek. Az információs támadások segítették Oroszország szempontjából kedvezően alakítani a nemzetközi közvélemény álláspontját a háborúval kapcsolatban. A támadásokat megkönnyítette, hogy Grúzia internetkapcsolata jelentős részben Oroszországon haladt keresztül. A grúz források elhallgattatásával a külvilág nem szerezhetett megbízható híradásokat a háború menetével kapcsolatban, erre csak a hadműveletek befejezése után nyílt mód.[311] A támadások ebben az esetben sem köthetők bizonyítottan az orosz kormányhoz és a haderőhöz. Nemzetközi szakértői vélemények szerint az orosz katonai doktrína része, hogy az információs hadviselési tevékenységet bűnözői vagy terrorista cselekedetnek álcázzák.[312] A Grúzia elleni támadás az első eset, amikor egy nemzetállam egy másik nemzetállam elleni hadművelet előkészítésére és támogatására az információs műveletek eszközeit széles körben alkalmazta.

A Stuxnet nevű számítógépes féreg[313] 2010 júniusában jelent meg. A Stuxnetet a Siemens által fejlesztett, az iráni nukleáris létesítményekben is alkalmazott ipari irányító-ellenőrző program támadására készítették, USB-csatlakozón keresztül juttatták be az iráni nukleáris létesítmények zárt számítógépes hálózataiba.[314] Hírügynökségi jelentések szerint a számítógépes féreg működése következtében késett a bushehri erőmű üzembe állítása,[315] illetve Irán elismerte, hogy a Stuxnet felelős a natanzi urániumdúsító centrifugák részleges leállásáért.[316] A Stuxnet a felfedezése óta több millió számítógépet fertőzött meg, és jelentős károkat okozott Kínában, Indiában, Indonéziában és Pakisztánban.[317] A Stuxnet ellenőrizhetetlen terjedése megerősíti azt a korábbi feltevést, hogy bármely ország, szervezet vagy létesítmény ellen végrehajtott információs támadás az egész információs hadszíntérre hatást gyakorol. A Stuxnet alkalmazása az első támadás egy nemzetállam kritikus ipari infrastruktúrája ellen, egyben az első eset, amikor az információs támadás közvetlen fizikai rombolást okozott.

311 Georgia, Russia: The Cyberwarfare Angle. A Stratfor kutatóintézet elemzése. RANE, 2008.08.12. https://worldview.stratfor.com/article/georgia-russia-cyberwarfare-angle; letöltés: 2020.03.12.

312 Project Grey Goose Phase II Report: The evolving state of cyber warfare. Greylogic, 2009.03.20. http://www.fistfulofgold.com/Documents/ProjectGreyGoose.pdf; letöltés: 2021.07.20.

313 Computer worm, egy számítógépes vírushoz hasonló, önsokszorozó számítógépes program, amelynek a vírussal ellentétben nincs szüksége gazdaprogramra, önállóan működnek.

314 SMITH, David J.: Cyber-War! Tabula, November 8-14, 2010. A Georgian Foundation for Strategic and International Studies tanulmánya. https://gfsis.org.ge/media/download/GSAC/Articles/Cyber-War.pdf; letöltés: 2021.07.20.

315 LAFRANCHI, Howard: Iran's Bushehr nuclear plant delayed: Stuxnet not to blame, official says. The Christian Science Monitor, 2010.10.04. https://www.csmonitor.com/USA/Foreign-Policy/2010/1004/Iran-s-Bushehr-nuclear-plant-delayed-Stuxnet-not-to-blame-official-says; letöltés: 2022.09.12.

316 Iran Confirms Stuxnet Worm Halted Centrifuges. CBS News, 2010.11.29. https://www.cbsnews.com/news/iran-confirms-stuxnet-worm-halted-centrifuges/; letöltés: 2021.12.29.

317 Stuxnet 'cyber superweapon' moves to China. The Sydney Morning Herald, 2010.09.30. https://www.smh.com.au/technology/stuxnet-cyber-superweapon-moves-to-china-20100930-15z8v.html; letöltés: 2022.09.12.

Ukrajna 2014 óta az orosz kiberműveletek állandó célpontja. 2014. március 13-án – három nappal a Krím félsziget státusával kapcsolatban megtartott népszavazás előtt – Oroszország nyolc percig tartó DDoS-támadást indított az ukrán számítógépes és kommunikációs hálózatok ellen annak érdekében, hogy elterelje az ukrán közvélemény figyelmét az orosz csapatok krímbeli jelenlétéről. 2014 májusában, az ukrán elnökválasztást megelőzően a CyberBerkut oroszbarát hackercsoport több – sikertelen – kibertámadást hajtott végre a Központi Szavazási Bizottság rendszerei ellen a szavazás eredményének manipulálása érdekében. 2015 decemberében több mint 230 ezer ukrán polgár tapasztalhatott áramkimaradást, miután a Sandworm Team hackercsoport részéről DDoS-támadás érte három energetikai vállalat telefonos ügyfélszolgálati központjait és elektronikus alállomásait. 2016-ban hasonló támadás érte a kijevi alállomást. 2016-tól kezdve a kibertámadások egyre kiterjedtebbé váltak. 2017 júniusában útjára indult a NotPetyamalware nevű kártékony program, amely a történelem legrombolóbb kibertámadásának bizonyult. A számviteli szoftverbe kódolt kártékony program az ukrán kormányzat, posta, médiaszolgáltatók, pénzintézetek, szállítóvállalatok, illetve az üzleti szféra közel 13 ezer számítógépét fertőzte meg, működésképtelenné téve azok merevlemezeit. A támadás hatásai összesen 65 országra terjedtek ki, tízmilliárd dolláros kárt okozva.[318] Az orosz propagandatevékenység a 2022. február 24. óta tartó ukrajnai háborút megelőzően is folyamatos volt Ukrajnában. Az orosz hackerek az oroszellenes ukrán politikusokat és az ukrán kormányzati honlapokat támadták, illetve oroszbarát tartalmat és álhíreket terjesztettek az ukrán közösségi médiában. A hackereknek sikerült megszerezniük a Donbaszban szolgáló katonák és családtagjaik telefonszámait, amelyekre célzott üzeneteket juttattak el annak érdekében, hogy a katonákat dezertálásra bírják.[319]

A 2022. február 24. óta tartó ukrajnai háború az első jelentős fegyveres konfliktus, amelyben a felek kiterjedt kiberműveleti tevékenységet folytatnak. Oroszország már a tényleges invázió kezdete előtt széles körű kibertámadást indított az ukrán kritikus infrastruktúra (elsősorban energetikai és telekommunikációs vállalatok, pénzügyi szervezetek és médiaszolgáltatók) ellen azzal a céllal, hogy káoszt teremtsen és ellehetetlenítse az ukrán védelmet. Kiberműveleti szempontból kijelenthető, hogy Ukrajna – a nyugati országok és a magánszféra segítségével – a korábbi tapasztalatokra építve jól felkészült az orosz támadásra, amelyek hatásossága elmaradt a korábbi tapasztalatok alapján vártnál. A kiberműveletek önmagukban nem bizonyultak hatékonynak a jól szervezett ukrán védelemmel szemben, és nem kerültek összehangolásra az elektronikus hadviselési tevékenységgel, illetve a precíziós katonai csapásokkal. Az orosz propaganda nem tudott hatékony választ adni az orosz agresszióval kapcsolatban nyilvánosságra hozott nyugati hírszerzési információkkal szemben. Az orosz törekvéseket aláásta továbbá a tömegesen hozzáférhető nyílt

[318] PRZETACZNIK, Jakub – TARPOVA, Simona: Russia's war on Ukraine: Timeline of cyber-attacks. European Parliamentary Research Service, 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf; letöltés: 2022.08.14.

[319] SALT, Alexander – SOBCHUK, Maya: Russian Cyber-Operations in Ukraine and the Implications for NATO. Canadian Global Affairs Institute, August 2021. https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato; letöltés: 2022.08.14.

információ, amelynek forrásai elsősorban ukrán katonák és civilek okostelefonokkal készített videofelvételei, kereskedelmi szolgáltatók szabadon hozzáférhető, nagy felbontású műholdfelvételei, illetve az orosz erők rejtjelezetlen hírközlése voltak. Az orosz információs műveletek sikertelenül kísérelték meg továbbá a végponttitkosított üzenetküldő alkalmazások zavarását is, így az ukrán lakosságot nem sikerült elzárni a külvilágtól.

Az információs műveletek tudati dimenziójában végzett orosz műveletek – bár Nyugaton és Ukrajnában sikertelenül kísérelték meg a közvélemény formálását – az orosz narratívát sikeresen közvetítették mindenekelőtt az orosz közvélemény felé. Az orosz propagandát saját területén jól támogatta a kínai kormányzat is, sikerült továbbá semleges álláspontot kialakítani az indiai, az afrikai és a közel-keleti közvéleményben, illetve néhány latin-amerikai országban. Mindez ugyanakkor csak kisebb részben tekinthető az orosz információs műveletek sikerének.[320]

Az Amerikai Egyesült Államok Kiberműveleti Parancsnoksága

Az Amerikai Egyesült Államok haderejének Kiberműveleti Parancsnoksága (USCYBERCOM) 2010. november 3-án érte el a teljes műveleti készenlétet.[321] A parancsnokság az Amerikai Egyesült Államok haderőnemeinek információs műveleteket végző egységeit egyesítette: a szárazföldi haderő Kiberműveleti Parancsnoksága (Army Forces Cyber Command – ARFORCYBER), a Légierő 24. különleges műveleti wingje (24th SOW), a Haditengerészet Kiberműveleti Parancsnoksága (Fleet Cyber Command – FLTCYBERCOM) és a Tengerészgyalogság Kiberműveleti Parancsnoksága (Marine Forces Cyber Command – MARFORCYBER) összevonásával hozták létre. A USCYBERCOM irányítja és megvédi a haderő hálózatalapú elektronikus információs rendszereit, felkészül a kibertérben végrehajtott műveletek végrehajtására, valamint biztosítja az Amerikai Egyesült Államok és szövetségesei számára a hozzáférést az információs dimenzióhoz. A USCYBERCOM tevékenységét a SIGINT-műveletekért felelős Nemzetbiztonsági Ügynökséggel (NSA[322]) és a Belbiztonsági Minisztérium[323] nemzeti kibervédelemért felelős részlegével[324] összehangoltan végzi. Az információs műveleti képességek fejlesztését az Amerikai Egyesült Államok katonai és civil hálózatalapú elektronikus információs rendszereinek növekvő fenyegetettsége indokolta. A Kiberműveleti Parancsnokság feladata biztosítani, hogy a haderő kibertámadás esetén is képes legyen feladatainak végrehajtására.

320 LEWIS, James A.: Cyber War and Ukraine. CSIS, June 2022. https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash; letöltés: 2022.08.14.
321 Full Operational Capability.
322 National Security Agency – NSA
323 Department of Homeland Security – DHS.
324 National Cyber Security Division – NCSD.

Az Amerikai Egyesült Államok nemzeti kiberműveleti stratégiája

Az Obama-adminisztráció hivatalba lépését követően az amerikai kormányzat jogi munkacsoportot állított fel, amelynek feladata a nemzetközi jogi normák – különös tekintettel az önvédelemhez való jogra és a nemzetközi hadijogra – az információs térben történő alkalmazásának kidolgozása volt. Az Amerikai Egyesült Államok elleni információs támadások elleni védekezés és a válaszcsapás módjait először a 2011. május 18-án nyilvánosságra hozott nemzeti kiberműveleti stratégia[325] rögzítette. A stratégia szerint az amerikai nemzeti kibervédelem a megelőzésre és az elrettentésre épít. A megelőzés alapja a fejlett információs infrastruktúrával rendelkező nemzetek közötti együttműködés, a fejlődő országok segítése és a nemzetközi kibervédelmi képességek fejlesztése. A terroristák és a bűnözők elleni elrettentés keretében a nemzetközi együttműködés kap kulcsszerepet. A stratégia olyan nemzetközi rendészeti együttműködési intézményrendszer felállítását irányozza elő, amely lehetőséget teremt a számítógépes terrorista és bűncselekmények elkövetőinek felderítésére és az ellenük történő fellépésre.

A nemzetállamok elleni kibertéri elrettentés alapja – hasonlóan a nukleáris elrettentéshez – annak biztosítása, hogy az Amerikai Egyesült Államok elleni kibertámadással remélhető nyereségek a várható nyereségekkel összehasonlítva kisebbek legyenek. Az egy nemzetállam által az Amerikai Egyesült Államok ellen indított kibertámadást követő ellencsapás jogi megalapozásaként a stratégia megállapítja, hogy az információs térben zajló tevékenységek is a nemzetközi közösséget alkotó szuverén nemzetállamok felelősségi körébe tartoznak.[326] A stratégia szerint az Amerikai Egyesült Államok vagy szövetségesei elleni kibertámadás esetén az önvédelemhez való jog és a szövetségesi kötelességek értelmében az Amerikai Egyesült Államok minden szükséges diplomáciai, gazdasági, információs[327] és (hagyományos) katonai ellenlépést megtehet. A stratégia alapján az Amerikai Egyesült Államok kibertérbeli támadásra akár hagyományos katonai válaszcsapással is felelhet. A jelenleg érvényes stratégia[328] is hasonló kitételeket tartalmaz.

---

325 International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World. The White House, Washington, May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; letöltés: 2021.07.20.

326 Hasonlóan a terrorellenes háború kezdetén megalkotott normákhoz, amelyek szerint a terroristák, a kiképzőtáboraik stb. akkor is támadhatók, ha azok egy szuverén ország területén működnek, akár annak tudta nélkül is. Az indoklás szerint a szuverenitás előfeltétele a saját terület ellenőrzése, amelyet a stratégia az információs térre is kiterjesztett.

327 A más nemzetek elleni kibertérbeli csapás végrehajtása a USCYBERCOM feladata.

328 National Cyber Strategy of the United States of America. The White House, Washington, September 2018. https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; letöltés: 2021.07.20.

A NATO Kibervédelmi Kiválósági Központja és a stratégiai koncepció információs műveleti vonatkozásai

Az Észtországot 2007 áprilisában és májusában Oroszország irányából ért információs támadásokra válaszul a NATO 2008 januárjában hagyta jóvá a tallinni Kibervédelmi Kiválósági Központ[329] felállítását. A Központ a tényleges működését 2008 szeptemberében kezdte meg. Információs kibervédelmi szervezet, a kibervédelemmel kapcsolatos jogi és doktrinális kérdéseket kutatja, konferenciákat és képzéseket tart. Jelenleg 24 fős személyi állománnyal működik. Költségvetéséhez Magyarország is hozzájárul, és 2021. júliusi információ szerint két szakértőt delegál.

A NATO-tagállamok állam- és kormányfői 2010. november 19-én fogadták el a Szövetség jelenleg érvényes stratégiai koncepcióját,[330] amelyben a korábbinál jelentősen nagyobb súllyal szerepel a Szövetség kibervédelmi képességei megerősítésének szükségessége. A dokumentum az információs támadások lehetséges forrásaiként a külföldi haderőket és titkosszolgálatokat, szervezett bűnözői csoportokat, terrorista- és szélsőséges csoportokat jelöli meg. A kibervédelmi képességek növelése érdekében a stratégiai koncepció a nemzeti erőforrások alkalmazásának – a Szövetség keretein belüli – fokozott összehangolását, a NATO információs műveleti képességeinek központosítását tűzi ki célul. Az Észak-atlanti Szerződés 5. cikkelyére történő hivatkozásnál az elfogadott dokumentumban az eredeti „fegyveres támadás" kifejezés helyett „támadás" szerepel, így értelemszerűen a Szövetségen kívüli információs támadás is a NATO kollektív védelmi rendszerét elsődlegesen szabályozó 5. cikkely hatálya alá esik. A NATO 2010. augusztus 1-jén hozta létre a Nemzetközi Titkárság[331] új típusú biztonsági kihívásokkal foglalkozó részlegét,[332] amelynek első vezetője Iklódy Gábor, az új típusú biztonsági kihívásokkal foglalkozó főtitkárhelyettes volt.

Az amerikai Hírszerző Közösség rendszere

A Hírszerző Közösség (IC) felépítése

Az Amerikai Egyesült Államok globális szerepvállalása a 2001-ben kezdődött afganisztáni és a 2003-tól indított iraki háborúkkal ért el arra a szintre, amikor a polgári és a katonai felső vezetésnek a korábbinál jóval megbízhatóbb és naprakészebb hírszerzési információkra volt szüksége annak érdekében, hogy törekvéseinek megvalósítását hatékonyan menedzselni tudja. Mindez a hidegháború statikusabb, egyetlen fenyegetésre összpontosító hírszerzési világának addig csak részben megkezdődött teljes felszámolását tette szükségessé. Az amerikai Hírszerző Közösség tagszervezeteinek száma, mérete és azok szerteágazó feladatrendszere egyszerre jelent lehetőséget és kihívást a rendszer felhasználói számára, akik a hatékony hírszerzés jelentőségét felismerve aktív szerepet vállalnak annak formálásában.

---

329 Cooperative Cyber Defence Centre of Excellence – CCD COE.
330 Strategic Concept 2010. NATO, 2010.11.19. https://www.nato.int/cps/en/natohq/topics_82705.htm;
331 International Staff.
332 Emerging Security Challenges Division.

Jelenleg az Amerikai Egyesült Államok, Kína és Oroszország rendelkezik a legkiterjedtebb és leghatékonyabb nemzetbiztonsági rendszerrel. Az amerikai társadalomra jellemző transzparencia részben a nemzetbiztonsági szektorra is kiterjed, ezért az amerikai rendszer a leginkább kutatható, emellett a nyugati civilizáció részeként és NATO-tagként hazánk számára az amerikai megoldások vizsgálata a legkézenfekvőbb. Az amerikai Hírszerző Közösség felépítésének, működésének és fejlesztésének vizsgálata azért fontos, mert az jellemzően modellértékű a nyugati nemzetbiztonsági szolgálatok számára, amelyek idővel átveszik az új amerikai megoldásokat. A mesterséges intelligencia nemzetbiztonsági alkalmazásában is az amerikai szolgálatok érték el a leginkább figyelemre méltó eredményeket. Az amerikai módszerek és fejlesztések átvételekor figyelembe kell venni ugyanakkor a hazai nemzeti nemzetbiztonsági sajátosságokat, hagyományokat és a méretbeli különbségeket is.

Az Amerikai Egyesült Államok Hírszerző Közössége – a Nemzeti Hírszerző Főigazgató Hivatalával (ODNI[333]) együtt – 18 nemzetbiztonsági szervezet és ügynökség[334] szövetsége, amelyek önállóan, de szoros együttműködésben végzik az ország nemzetbiztonsági védelmét és külkapcsolatainak alakítását támogató tevékenységüket. A Hírszerző Közösséget jelenlegi formájában Ronald Reagan 1981. december 4-én elnöki rendelettel[335] hozta létre.[336]

A törvényességi felügyelet megoszlik a törvényhozó és a végrehajtó hatalmi ágak között. Az elsődleges kormányzati felügyeletet az elnök által felkért szakértőkből álló Külügyi Hírszerző Tanácsadó Testület,[337] az Egyesített Hírszerző Közösségi Tanács,[338] az Elnöki Hivatalon belül működő Főfelügyelői Hivatal,[339] valamint a Menedzsment és Költségvetési Hivatal[340] gyakorolja. Az IC törvényességi felügyeletét elsődlegesen a Képviselőház Állandó Hírszerzési Bizottsága[341] és a Szenátus Hírszerzési Bizottsága[342] végzi.

---

333 Office of the Director of National Intelligence.

334 Agency: a kifejezés a nemzetbiztonsági tevékenységnek a nemzetközi – és részben a honi – politikai folyamatokat aktívan befolyásoló, azokba beavatkozó jellegét tükrözi (vö: „szolgálat").

335 A rendelet kötelezte a Hírszerző Közösség tagjait, hogy működjenek együtt az elnök és a Nemzeti Biztonsági Tanács (National Security Council – NSC) információigénye kielégítése érdekében. Az IC tevékenységének összehangolása ekkor a rendelet alapján a központi hírszerző igazgató (Director of Central Intelligence – DCI), egyben a CIA főigazgatója feladata volt.
Executive Order 12333 – United States intelligence activities. National Archives, 1981.
https://www.archives.gov/federal-register/codification/executive-order/12333.html; letöltés: 2019.05.11.

336 Az IC létrejöttének alapjául a védelmi miniszteri pozíciót, a légierőt, az Egyesített Vezérkart, a Nemzeti Biztonsági Tanácsot, a CIA-t – mint az Amerikai Egyesült Államok első, békeidőben működő polgári nemzetbiztonsági szolgálatát – és a Nemzeti Hírszerzési Programot (National Intelligence Program – NIP) is létrehozó, 1947-es Nemzeti Biztonsági Törvény (National Security Act of 1947) szolgált.

337 President's Foreign Intelligence Advisory Board.

338 Joint Intelligence Community Council. A félévente ülésező Tanács a kormánynak a Hírszerző Közösség tagszervezeteit irányító tagjaiból – a külügyminiszterből, a pénzügyminiszterből, a védelmi miniszterből, a legfőbb ügyészből (igazságügyi miniszter) és a belbiztonsági miniszterből – áll.

339 Office of the Inspector General.

340 Office of the Management and Budget.

341 United States House Permanent Select Committee on Intelligence. A Bizottság jelenleg (2019 májusából) 22 tagból áll.

342 United States Senate Select Committee on Intelligence. A Bizottság 15 tagból áll.

Az elnök és a Kongresszus az IC felügyeletét és irányítását továbbá két különálló költségvetési program segítségével valósítja meg. A *Nemzeti Hírszerző Programba*[343] tartoznak az IC tagszervezeteinek alaprendeltetés szerinti, az amerikai elnök, valamely szövetségi minisztérium vagy ügynökség, illetve a nemzeti hírszerző főigazgató által kezdeményezett és a Kongresszus által a költségvetés elfogadásának folyamatában jóváhagyott projektek és tevékenységek.[344] A NIP-ből nem finanszírozható a védelmi minisztérium[345] hírszerzési igényeinek megválaszolása, de az IC védelmi minisztérium alárendeltségébe tartozó tagjai[346] jelentős összegekkel részesülnek a NIP-ből, amelyek felhasználásával az ODNI és az IC egésze tevékenységét támogatják. A Nemzeti Hírszerző Program 2021-ben 60,8 milliárd dollárral részesült a központi költségvetésből. A 2022-re vonatkozó költségvetési igény 62,3 milliárd dollár volt.

A *Katonai Hírszerző Programba*[347] a védelmi minisztérium által meghatározott projektek vagy tevékenységek tartoznak, amelyek célja az amerikai haderő által folytatott katonai tevékenységek tervezése és végrehajtása támogatására vonatkozó hírszerzési információk megszerzése. A Katonai Hírszerzési Programot a védelmi miniszter[348] felügyeli és irányítja. A Program költségvetési támogatása 2021-ben 23,1 milliárd dollár volt. A Program költségvetési igénye a 2022. költségvetési évre vonatkozóan 23,2 milliárd dollár.[349]

A Hírszerző Közösség 18 szervezete közül az ODNI és a Központi Hírszerző Ügynökség (CIA) független, kilenc a védelmi minisztérium, hét más minisztérium vagy szervezet alárendeltségében, az ODNI szakmai irányításával tevékenykedik.

A védelmi miniszter összességében a nemzeti hírszerző főigazgatónál (DNI[350]) lényegesen nagyobb befolyással bír a Hírszerző Közösség egésze felett, hiszen a védelmi szektor valamennyi nemzetbiztonsági szervezete az irányítása alatt működik. E jogkörét a hírszerzésért felelős védelmi államtitkáron[351] keresztül gyakorolja.

---

343 National Intelligence Program.

344 A hírszerzési rendszer költségvetési folyamatainak összetettségét jól tükrözi, hogy minden pillanatban nyolc költségvetési év párhuzamos végrehajtása és tervezése zajlik. Az adott költségvetési évben a két megelőző évre elfogadott és az adott év forrásainak felhasználása zajlik, illetve már folyamatban van a következő év költségvetésének kidolgozása a végrehajtó hatalomnál és a Kongresszusnál. Eközben az IC már két évvel előre tervezi a költségvetési forrásigényét a végrehajtó hatalom számára, a végrehajtó hatalom pedig három évre előre már megkezdte a Kongresszusnak benyújtandó költségvetés tervezetét, illetve öt évre előre előzetes tervezést folytat.
LOWENTHAL, Mark M.: Hírszerzés – A titkoktól a politikai döntésekig. Antall József Tudásközpont, Budapest, 2017. p. 96.

345 Department of Defense – DoD.

346 Elsősorban Védelmi Hírszerző Ügynökség (Defense Intelligence Agency – DIA), a Nemzetbiztonsági Ügynökség (National Security Agency – NSA), a Nemzeti Felderítő Iroda (National Reconnaissance Office – NRO) és a Nemzeti Térinformatikai Ügynökség (National Geospatial Intelligence Agency – NGA).

347 Military Intelligence Program.

348 Secretary of Defense.

349 U.S. Intelligence Community Budget. ODNI, 2022.
https://www.dni.gov/index.php/what-we-do/ic-budget; letöltés: 2022.02.16.

350 Director of National Intelligence – DNI.

351 Under Secretary of Defense for Intelligence & Security – USD(I&S).

A Hírszerző Közösség védelmi miniszter irányítása alatt álló tagszervezetei:

- Védelmi Hírszerző Ügynökség (DIA[352]): összadatforrású hírszerző és elhárító szervezet, amely egyben a haderő hírszerzésének stratégiai koordinációjáért felel;[353]
- Nemzetbiztonsági Ügynökség (NSA): az Amerikai Egyesült Államok első számú rejtjelező és rádióelektronikai felderítő (SIGINT) szervezete;[354]
- Nemzeti Felderítő Iroda (NRO[355]): feladata a nemzeti felderítő műholdak tervezése, gyártása és működtetése;
- Nemzeti Térinformatikai Ügynökség (NGA[356]);
- a Szárazföldi Csapatok Hírszerzése (AI[357]): az AI a Szárazföldi Csapatok Vezérkarának[358] felderítőszervezete (G2) – a Vezérkar és a szárazföldi haderőnemért felelős miniszter alárendeltségében;
- 16. Légierő (16th Air Force – 16th AF/Air Force Cyber): a Légierő Parancsnokság[359] és a légierőért felelős miniszter alárendeltségében;
- Űrerő (SF[360]): az Űrerő parancsnoka[361] és a légierőért felelős miniszter alárendeltségében;
- Haditengerészeti Hírszerzési Hivatal:[362] a haditengerészet parancsnoka[363] és a haditengerészetért felelős miniszter alárendeltségében;
- a Tengerészgyalogság Hírszerzése (MCI[364]): a Tengerészgyalogság Parancsnoksága[365] és a haditengerészetért felelős miniszter alárendeltségben.

352 Defense Intelligence Agency.
353 E funkcióját az NSA központjában diszlokáló, a Stratégiai Parancsnokság (US Strategic Command – STRATCOM) alárendeltségében működő Egyesített Hírszerzési, Megfigyelési és Felderítési Funkcionális Komponensparancsnokságon (Joint Functional Component Command for Intelligence, Surveillance and Reconnaissance – JFCC ISR) keresztül végzi.
354 A haderő egyesített funkcionális parancsnokságainak egyike, a Kiberműveleti Parancsnokság (US Cyber Command – USCYBERCOM) 2009-ben vált ki az NSA-ból, de a két szervezetnek egyelőre közös vezetője van. A USCYBERCOM nem tagja a Hírszerző Közösségnek.
355 National Reconnaissance Office.
356 National Geospatial Intelligence Agency.
357 Army Intelligence.
358 Army Staff.
359 Headquarters Air Force.
360 Space Force. A 2019. december 20-án létrehozott haderőnem még nem hozott létre dedikált hírszerző szolgálatot, így egyelőre maga a haderőnem tagja a Hírszerző Közösségnek.
361 Chief of Space Operations – CSO, az Egyesített Vezérkar (Joint Chiefs of Staff – JCS) állandó tagja.
362 Office of Naval Intelligence.
363 Chief of Naval Operations – CNO, az Egyesített Vezérkar (Joint Chiefs of Staff – JCS) állandó tagja.
364 Marine Corps Intelligence.
365 Headquarters Marine Corps – HQMC.

A Szárazföldi Csapatok Hírszerzése, a 16. Légierő, a Haditengerészeti Hírszerzési Hivatal, a Tengerészgyalogság Hírszerzése, valamint a Parti Őrség Hírszerzése kötelékében működő SIGINT- és kriptológiai szervezetek alkotják a Központi Biztonsági Szolgálatot,[366] amely az NSA főigazgatójának alárendeltségében tevékenykedik.[367]

A DNI a Hírszerző Közösség védelmi ágazaton kívüli tagjainak szakmai tevékenységét hangolja össze. Annak ellenére, hogy a DIA, az NSA, az NRO és az NGA az IC egésze számára biztosít információkat, a DNI a tevékenységüket csak a Nemzeti Hírszerző Programon keresztül képes befolyásolni. Tovább szűkíti a DNI mozgásterét, hogy az alárendeltségébe tartozó szervezetek irányítását a felügyelő minisztériumok végzik. A DNI hatáskörébe az alábbi szervezetek tartoznak:

- CIA: független összadatforrású hírszerző és elhárító szervezet, közvetlenül az elnöknek és a Nemzeti Biztonsági Tanácsnak jelent;
- Hírszerzési és Kutatási Iroda (INR[368]): a Külügyminisztérium[369] alárendeltségébe tartozó[370] összadatforrású hírszerző szervezet;
- Hírszerző és Elhárító Hivatal (OICI[371]): fő feladata, hogy hozzájáruljon az Energiaügyi Minisztérium[372] laboratóriumai és erőművei, illetve az azokban dolgozó személyek védelméhez;
- Hírszerző és Elemző Hivatal (I&A[373]): a Belbiztonsági Minisztérium[374] hírszerző szervezete;
- a Parti Őrség Hírszerzése (CGI[375]) békeidőben szintén a belbiztonsági minisztérium alárendeltségében működik;
- Szövetségi Nyomozó Iroda (FBI[376]): a szövetségi rendvédelmi ügynökség egyebek mellett azoknak a hazai és transznacionális hálózatoknak a felderítéséért és felszámolásáért felelős, amelyek szándékkal és képességgel rendelkeznek ahhoz, hogy kárt okozzanak az Amerikai Egyesült Államoknak. Az FBI keretén belül a nemzetbiztonsági tevékenységért – elhárító és terrorelhárító hangsúllyal – dedikált nemzetbiztonsági szolgálat (NSB[377]) felel. Az Iroda az Igazságügyi Minisztérium[378]

366 Central Security Service – CSS.
367 Central Security Service (CSS). NSA, 2019. https://www.nsa.gov/about/central-security-service/; letöltés: 2019.05.13.
368 Bureau of Intelligence and Research.
369 Department of State – DoS.
370 A külügyminiszter irányítási jogköreit az Irodáért felelős államtitkár (Assistant Secretary of State for the Bureau of Intelligence and Research) útján gyakorolja.
371 Office of Intelligence and Counterintelligence
372 Department of Energy – DOE. Az OICI irányítását a nukleáris biztonságért felelős államtitkár (Under Secretary for Nuclear Security and Administrator of the National Nuclear Security Administration) végzi.
373 Office of Intelligence and Analysis. Az I&A nem végez elhárító és fedett információszerző tevékenységet.
374 A belbiztonsági miniszter irányítási jogköreit a hírszerzésért és elemzésért felelős államtitkár (Under Secretary of Homeland Security for Intelligence and Analysis) útján látja el.
375 Coast Guard Intelligence.
376 Federal Bureau of Investigation.
377 National Security Branch.
378 Department of Justice – DoJ.

alárendeltségében hajtja végre feladatait, de a legfőbb ügyész[379] (igazságügyi miniszter) nem rendelkezik közvetlen irányítási jogkörrel a szervezet felett;

- a Kábítószer-rendészeti Hivatal Nemzetbiztonsági Hírszerző Részlege (DEA/ONSI[380]): szintén az Igazságügyi Minisztérium alárendeltségében[381] tevékenykedő rendvédelmi hírszerző szervezet;

- Terrorelhárítási és Pénzügyi Hírszerző Hivatal (TFI[382]): irányítja és felügyeli a Pénzügyminisztérium[383] hírszerzési és rendvédelmi funkcióit azzal a céllal, hogy védelmezze a pénzügyi rendszert a visszaélésekkel szemben, valamint harcoljon a lator államok, terroristák, tömegpusztító fegyverek terjesztői, pénzmosók, drogbárók és más, a nemzetbiztonságot érintő fenyegetések ellen.[384]

A Hírszerző Közösség egésze felett tehát kizárólag az elnök és a Nemzeti Biztonsági Tanács bír irányítási jogkörrel.

A Nemzeti Hírszerző Főigazgató Hivatala

A DNI hangolja össze az IC szervezeteinek a tevékenységét – kivéve a védelmi minisztérium alárendeltségébe tartozókét –, és nemzetbiztonsági kérdésekben közvetlenül az elnöknek és a Nemzeti Biztonsági Tanácsnak jelent. A 2005. április 22-én létrehozott ODNI[385] saját törzsét kivéve nem rendelkezik irányítási és felügyeleti joggal az IC egyetlen szervezete felett sem. Az NSC üléseinek állandó résztvevője, az elnök hírszerzési tanácsadója.[386]

Az ODNI feladatai:

- az IC számára a célok és a prioritások meghatározása, a kapcsolódó iránymutatások – elsősorban a *Nemzeti Hírszerzési Stratégia*[387] és a hírszerzési prioritások[388] – kiadása;

---

379 Attorney General.

380 Drug Enforcement Administration, Office of National Security Intelligence – DEA/ONSI.

381 A Legfőbb Ügyész az FBI és a DEA/ONSI irányítását a nemzetbiztonságért felelős helyettes Legfőbb Ügyészen (Assistant Attorney General for National Security) keresztül gyakorolja.

382 Office of Terrorism and Financial Intelligence.

383 Department of Treasury. A pénzügyminiszter az irányítási jogköreit a terrorelhárításért és a pénzügyi hírszerzésért felelős államtitkár (Under Secretary of the Treasury for Terrorism and Financial Intelligence) útján gyakorolja.

384 A Hivatalt a 2004-es hírszerzési reformtörvény alapján hozták létre.

385 A Hivatal létrehozásáról a 2004-es Hírszerzési Reform és Terrorizmusmegelőzési Törvény (Intelligence Reform and Terrorism Prevention Act of 2004 – IRTPA) rendelkezett. A törvény alapjául az Amerikai Egyesült Államokat ért terrortámadásokat vizsgáló nemzeti bizottság (National Commission on Terrorist Attacks Upon the United States, 9/11 Bizottság) megállapításai szolgáltak. A Hírszerző Közösség reformjára emellett az iraki tömegpusztító fegyverekre vonatkozó hírszerzési információk kezelését vizsgáló bizottság (Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction) 2005. március 31-én a Kongresszus elé terjesztett jelentése bírt meghatározó hatással.

386 Intelligence Advisor.

387 National Intelligence Strategy – NIS.

388 Nemzeti Hírszerzési Prioritások Keretrendszer (National Intelligence Priorities Framework – NIPF). Intelligence Community Directive 204 – National Intelligence Priorities Framework. ODNI, 2015.01.02. https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf; letöltés: 2019.04.26.

- a Nemzeti Hírszerző Program (NIP) felügyelete és irányítása, a NIP költségvetésének a felügyelete;
- az IC tagjai által a nemzeti hírszerzési információk gyűjtésével, elemzés-értékelésével, a tájékoztatók elkészítésével és címzettekhez történő eljuttatásával kapcsolatos feladatok menedzsmentje, irányítása.[389]

Az ODNI közel 2000 munkatársának több mint fele a négy műveleti központ[390] egyikében tevékenykedik:

- Nemzeti Terrorelhárítási Központ;[391]
- Nemzeti Elhárító és Biztonsági Központ;[392]
- Nemzeti Proliferációellenes Központ;[393]
- Kiberfenyegetési Hírszerzési Integrációs Központ.[394]

A négy központ a terrorelhárítás, az elhárítás, a proliferáció, a tömegpusztító fegyverek felderítése és a kibervédelem területén koordinálja az IC tevékenységét.[395]

A döntéshozók és a Hírszerző Közösség közötti kapcsolatért, illetve a hírigények minél jobb megválaszolásáért a területi (ország vagy régió) és funkcionális alapon kinevezett nemzeti hírszerző menedzserek (NIM[396]) felelnek. A pozíció 2005-ös létrehozásakor a DNI a terrorelhárítás, a proliferáció elleni fellépés, Irán és Észak-Korea felelősségi területekre jelölt ki NIM-eket. A két funkcionális NIM egyben a vonatkozó műveleti központ parancsnoki beosztását is betölti.[397] Időközben több új pozíció került létrehozásra, például a Kelet-Ázsiáért[398] és a kiberfenyegetésekért[399] felelős NIM.

---

389 A DNI iránymutatásai az IC egészére, tehát a védelmi ágazatba tartozók részére is vonatkoznak, de ezek – a védelmi miniszter meghatározó befolyása miatt – utóbbiak esetében inkább ajánlásnak tekinthetők.

390 Operations Center.

391 National Counterterrorism Center – NCTC.

392 National Counterintelligence and Security Center – NCSC.

393 National Counterproliferation Center – NCPC.

394 Cyber Threat Intelligence Integration Center – CTIIC.

395 ODNI Factsheet. DNI, 2017.02.14. https://www.dni.gov/files/documents/FACTSHEET_ODNI_History_and_Background_2_24-17.pdf; letöltés: 2019.04.24.

396 National Intelligence Manager.

397 Director of National Intelligence Mission Managers. DNI, 2005.11.15. https://fas.org/irp/dni/icpm/2005-100-2.pdf; letöltés: 2019.04.26.

398 Scott W. Bray, Kelet-Ázsiáért felelős NIM 2017. június 26-i beszéde a Koreai-Amerikai Tanulmányok Intézete rendezvényén.
June 26, 2017 Speech to the Institute for Corean-American Studies: North Korea's Nuclear Weapons and Missile Capability -- Scott W. Bray, National Intelligence Manager for East Asia.
https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2017/3138-speech-to-the-institute-for-corean-american-studies-north-korea-s-nuclear-weapons-and-missile-capability; letöltés: 2019.04.26.

399 Jim Richberg volt kiberfenyegetésekért felelős NIM Linkedin-profilja. https://www.linkedin.com/in/jim-richberg; letöltés: 2019.04.26.

A DNI irányítja továbbá az IC vezető elemzőiből (NIO[400]) és civil szakértőkből álló Nemzeti Hírszerző Tanácsot,[401] melynek feladata az államigazgatás vezetői számára releváns kérdésekben elkészíteni a Hírszerző Közösség álláspontját tükröző nemzeti hírszerző értékeléseket (NIE). A szervezet emellett szakértői támogatást és állásfoglalást nyújt az IC egésze számára.[402] A Tanács hat régióra és öt funkcionális területre bontva végzi munkáját. A részterületek élén egy-egy NIO áll:

- Afrika;
- Kelet-Ázsia;
- Európa;
- Latin-Amerika;
- Közel-Kelet és Dél-Ázsia;
- Oroszország és Eurázsia;
- hagyományos katonai fenyegetések;
- gazdaság;
- tudomány és technológia;
- stratégiai és nukleáris fenyegetések;
- transznacionális fenyegetések.[403]

Az ODNI központja a Virginia állambeli Liberty Crossing településen található. A Hivatal munkatársainak mintegy 40%-a rotációs elv alapján kerül ki a 17 szolgálat valamelyikéből.

Az információigények fogadása, a hírszerzés folyamatának megtervezése és megszervezése

Az IC és a hírszerzési információk felhasználói[404] közötti kapcsolat kulcsfontosságú a polgári és a katonai döntéshozók hírszerző támogatásának hatékonysága szempontjából, ezért a szövetségi állam (tehát nem kizárólag a nemzetbiztonsági rendszer) komplex

400 National Intelligence Officer – NIO. A vezető elemzők irányítása alatt kis létszámú stáb dolgozik.
401 National Intelligence Council – NIC.
402 Az 1947-es Nemzeti Biztonsági Törvény hatályos változata.
National Security Act of 1947.
https://www.intelligence.senate.gov/sites/default/files/laws/nsact1947.pdf; letöltés: 2019.04.25.
403 A CIA által nyilvánosságra hozott NIC-dokumentumokat megosztó honlap.
National Intelligence Council (NIC) Collection.
https://www.cia.gov/library/readingroom/collection/national-intelligence-council-nic-collection;
letöltés: 2019.04.26.
404 Az elsődleges felhasználók az elnök, a Nemzeti Biztonsági Tanács, a kormánytagok, az Egyesített Vezérkar és a Kongresszus.
What is Intelligence? Office of the Director of National Intelligence.
www.dni.gov/index.php/what-we-do/what-is-intelligence; letöltés: 2020.04.28.

összekötői rendszert működtet. Az IC szervezeteinek vezetői által kijelölt kapcsolattartók feladata a felhasználók hírigényének közvetítése az IC felé és az információigények fogadása. A minisztériumok és az érintett kormányhivatalok a főigazgató kérésére szintén kinevezhetnek kapcsolattartásért felelős vezetőt.[405] A kormányzat és a hírszerzés közötti kapcsolatfelvétel lehetőségét nyílt minősítésű rendszereken is biztosítják.[406]

A Hírszerző Közösség által végzett tevékenység irányításának fő eszköze a Nemzeti Hírszerző Program, amelyet a főigazgató a hírszerzési tervezési, modellezési, költségvetési és értékelési rendszer segítségével (IPPBE[407]) állít össze. E rendszeren keresztül járul hozzá a Katonai Hírszerző Program elkészítéséhez is.

Az IPPBE-rendszer négy eleme ciklusban, egymásra hatóan és visszacsatolva működik. A tervezési szakaszban a Főigazgató Hivatala – a szolgálatok vezetői által e célból megküldött értékeléseket alapul véve – elemzi a Hírszerző Közösség képességeit, a hosszú távú hírszerzési trendeket és a várható kihívásokat. Meghatározza a stratégiai jelentőségű témaköröket és összeállítja a felhasználók várható információigényét, majd a hiányosságok felfedése céljából összeveti ezeket a hírszerzés meglévő képességeivel. A modellezés során költséghatékonysági szempontú döntéselőkészítési alternatívákat állítanak össze a főigazgató számára, majd a főigazgató által kiválasztott cselekvési változat alapján összeállítják a Hírszerző Programot. A döntéshozatali folyamat és a Hírszerző Közösség egésze hatékonyságának javítására szolgáló értékelési szakaszban a főigazgató irányelveinek végrehajtását értékelik. E vizsgálat szempontjai a célok teljesülése, a végrehajtás hatékonysága, eredménye (haszna és hiányosságai), illetve költségei. A vizsgálati jelentések fókuszában állhat egyedi főigazgatói döntés végrehajtása,[408] a nemzetbiztonsági szolgálatok költségvetésének felhasználása és teljesítményének általános értékelése,[409] valamint a Nemzeti Hírszerzési Stratégia (NIS) végrehajtása.[410] Az eseti jelentéseken felül a hivatal éves stratégiai értékelést[411] is készít az IPPBE-rendszer valamennyi elemének vonatkozásában.[412]

Az irányítás eszköze a hírszerzési prioritások (feladatok) összeállítása is, amelynek alapja az elnök és a nemzeti biztonsági főtanácsadó, illetve a kormánytagok hivatalosan megfogalmazott igényei. A döntéshozói igények értelmezéséhez hozzájárulnak az IC-tagszervezetek vezetői, a nemzeti hírszerző menedzserek és az IC vezető elemzői is.

---

405 Federal Senior Intelligence Coordinator – FSIC. Munkáját szükség esetén összekötők (Intelligence Point of Contact – IPOC) és koordinációs iroda (Federal Intelligence Coordination Office – FICO) támogatja.

406 Intelligence Community Directive 404 – Executive Branch Intelligence Customers. ODNI, 2013.07.22. https://www.dni.gov/files/documents/ICD/ICD 404-Executive Branch Intelligence Customers.pdf; letöltés: 2019.10.29.

407 Intelligence Planning, Programming, Budgeting, and Evaluation.

408 Strategic Evaluation Report.

409 Budget and Performance Report.

410 NIS Progress Assessment.

411 IC Strategic Assessment.

412 Intelligence Community Directive 116 – Intelligence Planning, Programming, Budgeting, and Evaluation System. ODNI, 2011.09.14. https://www.dni.gov/files/documents/ICD/ICD_116.pdf; letöltés: 2019.11.01.

A főigazgató évente állítja össze és negyedévente – illetve szükség szerint – vizsgálja felül a hírszerzési prioritásokat tartalmazó dokumentumot.[413]

A hírszerzés önálló ágai, az elhárítás, a terrorelhárítás és a kibervédelem[414] területein végzett tevékenység egységes magas színvonaláért az úgynevezett *funkcionális menedzserek*[415] felelősek. E nemzetbiztonsági vezetők szakterületeiken a főigazgató fő tanácsadói, akik az informatikai, a szervezeti, a módszertani, a műveleti eljárási és a kiképzési interoperabilitás javításával növelik az IC egészének hatékonyságát.[416] A funkcionális menedzsereket a főigazgató jelöli ki, a bevett gyakorlat szerint a Hírszerző Közösség legfontosabb tagszervezeteinek vezetői közül. A titkos emberi forrású hírszerző (HUMINT) és a nyílt forrású hírszerző (OSINT)[417] tevékenységért a Központi Hírszerző Ügynökség (CIA); a geoinformációs/ térinformatikai hírszerzésért (GEOINT) és a képi felderítésért (IMINT) a Nemzeti Térinformatikai Ügynökség (NGA); a rádióelektronikai felderítésért (SIGINT) pedig a Nemzetbiztonsági Ügynökség (NSA) vezetője felel. Feladataik több esetben túlnyulnak az IC határain, hiszen az NGA vezetőjének illetékességébe a Földtani Hivatal[418] is beletartozik.[419]

A főigazgató elvárja, hogy a Hírszerző Közösségen belül működő adatszerző, elemző-értékelő és elhárító elemek mind a napi hírszerzési információk,[420] mind a hosszú távú, stratégiai hírszerzési információk[421] és az előrejelzések előállítása során integrált módon tevékenykedjenek,[422] ezért az integrált működésmenedzsmentről szóló utasításában[423] meghatározta, hogy információszerzés csak az elemző-értékelők információigénye vagy útmutatása (az adatgyűjtők által beszerzett információk értékelése) alapján végezhető.[424] Az elhárítás szerepe a folyamatban az információszerző források, módszerek és tevékenységek (műveletek) jelentette sebezhetőségek azonosítása.

---

413 National Intelligence Priorities Framework – NIPF.
Intelligence Community Directive 204 – National Intelligence Priorities Framework. ODNI, 2015.01.02. https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf; letöltés: 2019.04.26.

414 Intelligence function.

415 Functional Managers.

416 Intelligence Community Directive 113 – Functional Managers. ODNI, 2009.05.19. https://www.dni.gov/files/documents/ICD/ICD_113.pdf; letöltés: 2019.10.29.

417 AFTERGOOD, Steven: Open Source Center (OSC) Becomes Open Source Enterprise (OSE). FAS, 2015.10.28.
https://fas.org/blogs/secrecy/2015/10/osc-ose/; letöltés: 2022.02.16.

418 US Geological Survey.

419 LOWENTHAL, Mark M. – CLARK, Robert M.: The Five Disciplines of Intelligence Collection. Thousand Oaks, CQ Press, 2015.

420 Current Intelligence.

421 Strategic Intelligence.

422 Integrated Mission Management.

423 Intelligence Community Directive 900 – Integrated Mission Management. ODNI, 2013.05.06. www.dni.gov/files/documents/ICD/ICD 900 - Integrated Mission Managemement.pdf; letöltés: 2019.10.29.

424 Az utasításban szereplő mondat arra enged következtetni, hogy a DNI által megfogalmazott hírszerzési prioritások (National Intelligence Priorities Framework) alapján az elemző-értékelő szervezetek külön testre szabott információigényeket fogalmaznak meg az adatszerzők számára.

A főigazgató az utasításban szereplő célok megvalósításának felügyeletével dedikált, az integrációért felelős főigazgatóhelyettesi pozíciót[425] hozott létre, akit a nemzeti hírszerző menedzserek tevékenysége támogat.[426]

Az Amerikai Egyesült Államok 2019-es Nemzeti Hírszerzési Stratégiája

Daniel Coats DNI 2019 január 22-én tette közzé a jelenleg érvényes Nemzeti Hírszerzési Stratégiát (NIS). A dokumentum elkészítését a 2004-es hírszerzési reformtörvény írja elő a DNI számára, aki eddig 2005-ben, 2009-ben és 2014-ben készített NIS-t. A stratégiák kiadásával a DNI szakmai és szervezeti iránymutatást ad a Hírszerző Közösség tagjai számára. A dokumentumok egyre magasabb színvonalon integrálják az IC-n belül összegyűlt szaktudást, és a reformok egyik fundamentumává váltak.[427]

A 2019-es dokumentum alapján a Hírszerző Közösség feladata a nemzeti biztonság, a gazdasági erő és a technológiai fölény erősítése világosan megfogalmazott, objektív és független információ biztosításával. A Stratégia három alapfeladatot határoz meg az IC számára:

- *stratégiai hírszerzést*[428] a nemzeti biztonságot és érdekeket meghatározó folyamatok nyomon követésére;
- *előrejelző hírszerzést*[429] az új trendek, a változó körülmények és a váratlan fejlemények vizsgálatára;
- valamint *művelettámogató hírszerzést*[430] a tervezett és a végrehajtás alatt álló katonai, diplomáciai és belbiztonsági műveletek – közvetett és közvetlen – támogatására.

A DNI a Stratégiában négy fő funkcionális részterületet jelölt ki az IC-nek:

- a kiberfenyegetések felderítésére irányuló hírszerzés[431] az állami és a nem állami szereplők kibertérben megvalósított károkozó tevékenysége ellen lép fel;
- terrorelhárítás;
- a tömegpusztító fegyverek és hordozóeszközeik proliferációja elleni hírszerzés;

---

425 Deputy DNI for Intelligence Integration (DDNI/II).

426 Ez alól kivételt jelentenek az elhárító és a terrorelhárító feladatokat ellátó, valamint a proliferáció elleni fellépésért felelős NIM-ek, akik közvetlenül a DNI-nek jelentenek.
Intelligence Community Directive 900 – Integrated Mission Management. ODNI, 2013.05.06.
www.dni.gov/files/documents/ICD/ICD 900 - Integrated Mission Managemement.pdf; letöltés: 2019.10.29.

427 A NIS-ekben szereplő iránymutatásokat jelentős mértékben megfogadta a védelmi szféra is.

428 Strategic Intelligence.

429 Anticipatory Intelligence. Elemei: előrelátás (*foresight*), előrejelzés (*forecast*) és veszélyfigyelmeztetés (*warning*).

430 Current Operations Intelligence.

431 Cyber Threat Intelligence.

- elhárítás és biztonságvédelem az Amerikai Egyesült Államokban illegális információszerzést, az IC tevékenységének megzavarását, külföldi érdek érdekében végzett politikai befolyásolási tevékenységet vagy szabotázst végző ellenérdekelt titkosszolgálatok és nem kormányzati szervezetek (elsősorban terrorszervezetek),[432] valamint az amerikai kormányzat őket akarva vagy akaratlanul segítő munkatársaival szemben.

A felsorolt célok megvalósítása érdekében az IC-nek tovább kell javítania információszerző, információmegosztási és -feldolgozási (elemző-értékelő) képességeit. Ennek részeként a Stratégia további technológiai és szervezeti fejlesztéseket helyez kilátásba.

A szervezeti fejlesztések keretében a DNI meghatározta az IC számára azokat a szervezeti célokat, amelyek az elmúlt évek reformjai során egyes ügynökségeknél beváltak:

- az *integrált műveleti feladatmenedzsment*[433] összehangolja az IC képességeit, tevékenységét és erőforrásainak felhasználását a közös erőfeszítés fokozása érdekében; a DNI kiemeli a műveleti központok jelentőségét e cél elérése érdekében és leszögezi, hogy meg kell találni az egyensúlyt a közös célok minél hatékonyabb elérése és a szervezeti specializáció között; a Stratégia szerint csökkenteni kell az IC-n belüli redundanciát és optimalizálni az erőforrások felhasználását; e területen a DNI sikerként értékeli az iráni nukleáris és az észak-koreai atomfegyver-program nyomon követését, a Malaysian Airlines Kelet-Ukrajnában lezuhant MH–17-es járatával kapcsolatos vizsgálatot, valamint a nyugat-afrikai ebolajárvánnyal szembeni fellépést;

- az *integrált működésmenedzsment*[434] az IC tagjainak művelettámogató tevékenységét hangolja össze, amelynek során a Hírszerző Közösség tagjai megosztják egymással a bevált megoldásaikat, összehangolják a beszerzéseiket, közös sztenderdeket és támogató rendszereket, valamint adatosított szervezeti és egyéni teljesítményértékelő rendszereket dolgoznak ki; a közös erőfeszítések kiemelt részterülete az IC fizikai és informatikai infrastruktúrájának védelme;

- *a sokszínű, befogadó, motivált, lojális és szakértő munkaerő kialakítása és megtartása*; a humánerőforrás elvárt képességeit tekintve a kritikus gondolkodás, az idegennyelv-ismeret, a mérnöki tudományok és a matematika játszanak kiemelt szerepet; a kívánt célok elérése érdekében az IC folyamatos képzéseket biztosít a munkaerő, kiemelten a középszintű vezetők számára, amelynek során a teljesítményorientált, együttműködésre és rugalmasságra építő munkahelyi kultúra elsajátítása a cél; az IC hosszú távú befektetésként kezeli mind a vezető, mind a beosztott állományt, akiknek szakmai életútja során változatos beosztásokat, megfelelő illetményt, valamint a munkahelyi és a magánélet megfelelő egyensúlyát kínálja fel, aminek köszönhetően az IC a legjobb munkaadók között szerepel az amerikai kormányzaton belül;

[432] Összefoglalóan: Foreign Intelligence Entity – FIE.
[433] Integrated Enterprise Management.
[434] Integrated Business Management.

- *új technológiák kutatásával és felhasználásával, az innovatív gondolkodásmód meghonosításával és a nemzetbiztonság elméletének fejlesztésével* a műveleti és a művelettámogató tevékenység javítása; az IC-nek a hagyományostól eltérő, kísérletező gondolkodásmódot kell követnie az új, egyszerűbb, hatékonyabb módszerek bevezetése során, a fejlesztéseknek a mesterséges intelligencia, az automatizáció és az emberi teljesítmény gépi fokozása[435] eredményeinek felhasználásával növelniük kell a Hírszerző Közösség tudását, helyzetértékelését és műveleti tempóját; az új technológiák bevezetése érdekében az IC vezetőinek bizonyos szintű kockázatot kell vállalniuk, tudatában annak, hogy a sikerhez esetleg kezdeti kudarcok vezethetnek; a Stratégia szerint az IC már részben új módszerekkel készíti a nemzeti hírszerző értékeléseket, emellett jelentős előrehaladást értek el a gépi tanulás alkalmazásában a közösségi médiából kinyert információ, a hírforrások, a pénzügyi tranzakciók adatainak és a felhasználók internetes kereséseinek automatizált feldolgozásában, ezáltal a politikai instabilitás előrejelzésében;

- felismerve, hogy az IC sikere azon múlik, hogy a megfelelő személyek a megfelelő időben releváns információval támogathassák a kormányzati döntéshozatalt, *az amerikai nemzetbiztonsági rendszernek* – az információbiztonság fenntartása mellett – *az információmegosztás, a közös feladat-végrehajtás és az integráció erősítésére kell* törekednie; ennek érdekében az információt megfelelő fájlformátumban, metaadatokkal[436] ellátva kell tárolni, növelve annak használhatóságát és lehetővé téve a nemzetbiztonsági folyamatok információközpontúvá tételét; a korszerű adatmenedzsment-rendszerek segítségével az adat könnyen fellelhetővé, elérhetővé és felhasználhatóvá válhat, megnövelt információbiztonság mellett. A fejlett adatkinyerő rendszerekkel fokozható az elemzés-értékelés színvonala, a jelenlegi technológiával nem kimutatható összefüggésekkel és az elemzés-értékelés további hozzáadott értékével fokozva a hírszerzési információk használhatóságát; az információbiztonság mellett *fontos elv a túlminősítés megelőzése és az IC tevékenységének minél átláthatóbbá tétele* a külvilág, elsősorban az amerikai közvélemény számára, aminek érdekében az IC létrehozott egy szabadon hozzáférhető gyűjteményt több ezer oldalnyi nyílttá újraminősített dokumentumából, a hivatalos közleményekből és a nyilvános meghallgatások jegyzőkönyveiből;[437]

- az IC hatékonyságának fokozása a belföldi és a nemzetközi kormányzati, nem állami és magánszektorbeli *partnerekkel folytatott stratégiai együttműködések fejlesztésével*; a nemzetközi partnerekkel elsősorban a terrorelhárítás és a közös katonai műveletek hírszerző támogatásában figyelhető meg az együttműködés javulása.

A Nemzeti Hírszerző Főigazgató Hivatalának Nemzeti Elhárító és Biztonsági Központja 2020 februárjában adta ki a jelenleg is érvényes Nemzeti Elhárító Stratégiát.[438]

---

435 Augmentation, például viselhető okoseszközök, exoskeletonok stb. segítségével.

436 Adat az adatról: az információ megszerzésének vagy a tájékoztató elkészültének idejére, forrásaira, a minősítésre, megoszthatóságra, a készítő személyre stb. vonatkozó adatok.

437 A gyűjtemény a https://icontherecord.tumblr.com/ címen, a Hírszerző Közösség tevékenységével kapcsolatos információ a https://www.intelligence.gov/ címen érhető el.

438 National Counterintelligence Strategy of the United States of America 2020-2022. NCSC, 2020. https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf; letöltés: 2022.08.03.

A megfogalmazott stratégiai célok a nemzeti létfontosságú infrastruktúra védelme, az ellátási láncok védelme, a gazdasági kémkedés elleni fellépés, a honi demokratikus intézmények és folyamatok védelme a külföldi befolyástól, valamint a külföldi kiberhírszerzés és kiberműveletek elleni fellépés. A Stratégia szerint az amerikai nemzeti biztonságot fenyegető külföldi szereplők száma és képességei egyaránt növekednek. A fő kihívást Kína és Oroszország jelentik, amelyek nemzeti erejük teljes tárházát bevetik annak érdekében, hogy kárt okozzanak a globális amerikai érdekekben. A fenyegetést jelentő nemzetközi szereplők a teljes amerikai államigazgatás számára veszélyt jelentenek, mert tevékenységüket nem korlátozzák a nemzeti biztonság szempontjából jelentős szektorokra.

Az MI nemzeti biztonsági vonatkozásaival foglalkozó bizottság megállapításai

A mesterséges intelligencia nemzeti biztonsági hatásainak vizsgálatára létrehozott kongresszusi bizottság[439] 2021 márciusában nyilvánosságra hozott jelentése részletesen kitért a nemzetbizottsági vonatkozásokra is. A dokumentum szerint az MI minden egyéb kormányzati szegmensnél mélyebben érinti a nemzetbiztonsági területet, hiszen a technológia elterjedésével valamennyi emberi és technológiai platform hozzájárul majd a globális információs hálózathoz. A szenzorok száma exponenciális növekedést mutat, ami azzal fenyeget, hogy az adat tömege és változatossága, illetve termelődésének gyorsasága túlterheli az elemző-értékelőket. Az elemzők számára az is kihívást jelent majd, hogy az információt a megfelelő kontextusba helyezzék. Az MI-technológiák segítséget nyújtanak majd a nemzetbiztonsági munkatársaknak az információ fellelésében, az azok közötti kapcsolatok feltárásában, a trendek felvázolásában, valamint az indikátorok és az anomáliák felfedésében. Az MI által támogatott új képességek a hírszerzési ciklus valamennyi elemének javítja majd a teljesítményét. A nemzetbiztonsági szféra számára a számítógépes látás, a biometrikus technológiák (arc-, hang- és járásfelismerés), a természetes nyelvek feldolgozása és az algoritmikus keresés tekinthetők a legfontosabb kulcstechnológiának. A mesterséges intelligencia megteremti a különböző adatfolyamok fúziójának lehetőségét is.

A védelmi minisztériumhoz hasonlóan a Hírszerző Közösség számára is feladat, hogy 2025-ig megteremtse az MI széles körű elterjesztésének humán, infrastrukturális és szervezeti feltételeit. Az IC-nek haladéktalanul meg kell kezdenie a hírszerzési ciklus valamennyi elemének a lehető legszélesebb körű automatizálását. Különös figyelmet kell fordítania arra, hogy az adat és az információ megfelelő feldolgozáson essen át, mielőtt az elemzők elé kerül. A tájékoztatóknak gép által olvashatónak kell lenniük ahhoz, hogy azokat automatikusan lehessen eljuttatni a felhasználóknak. Ennek érdekében a tájékoztatókból ember és gép által olvasható változatokat kell készíteni. A hírszerzés önálló ágainak automatizálását követően meg kell teremteni az ember–gép együttműködés feltételeit az összadatforrású elemzés-értékelésben.[440]

[439] National Security Commission on Artificial Intelligence.

[440] SCHMIDT, Eric et al.: Final Report. National Security Commission on Artificial Intelligence, 2021. pp. 107–118.

A nemzetbiztonság szervezetelméleti vonatkozásai

A nemzetbiztonsági rendszer vizsgálata szempontjából releváns katonai és magánszektorbeli vezetési elvek és szervezeti modellek

A nemzetbiztonsági szolgálatok különleges szerepet töltenek be az állam működésében. Az állami szervezetek többségétől elkülönülten végzett nemzetbiztonsági munkát körülvevő titkosság, a szolgálatok szervezetének és működésének kevés szereplő általi ismerete, illetve a versenyhelyzet relatív hiánya nem kedvez a változások bevezetésének. A 21. század társadalmi és technológiai realitásai ugyanakkor közvetlenül, a fejlődésnek a biztonsági környezetre gyakorolt hatásai pedig – békeidőben – közvetetten hatnak a nemzetbiztonsági szervezetekre. A folyamat a hidegháború végeztével, az információs kor és a legújabb kori globalizáció kezdetével indult be, és folyamatosan erősödő módon kényszeríti a nemzetbiztonsági szektort a változások bevezetésére.

A megváltozott világban a változási kényszer állandóvá vált. A nemzetbiztonsági szervezetek – hasonlóan a katonai szervezetekhez – számára az állandóság, a stabilitás és a tradíciók fontos értékek, így nehezen fogadják el, hogy az új kihívásokra a régi szervezeti struktúrájuk az adott, partikuláris problémára adott, „ad hoc" módosítása nem jelent kielégítő választ. A megváltozott körülményeket jól jelzi, hogy azok hatására a nemzetbiztonsági tevékenység felderítő (hírszerző) szakágának teljes, az elhárító szakág működését részben meghatározó elmélet, a hírszerzési ciklust kritizáló, sőt érvényességét is megkérdőjelező elméletek jelentek meg a 2000-es évek elején. Dr. Vida Csaba *Létezik-e még a hírszerzési ciklus? Miről szól a hírszerzés?* című tanulmányában[441] amellett érvel, hogy a kritikusok által felvetett problémák nem az elmélet hibája miatt, hanem sok esetben a hírszerző szolgálatok hibás, anomáliás működéséből (félelem az információk megosztásától, a döntéshozók közvetlen tájékoztatása az adatszerzők által stb.) erednek. Mindezen problémák akkor jelentkezhetnek, ha a nemzetbiztonsági szolgálatok szervezeti felépítése már nem felel meg teljes mértékben a szolgálatokkal szemben a felső vezetők és a biztonsági kihívások által támasztott követelményeknek.

A nemzetbiztonsági szolgálatok vezetési és szervezeti kultúrája sokban hasonlít a katonai szervezetekéhez. A nemzetbiztonsági tevékenység sajátos, alkotó jellege miatt ugyanakkor a hierarchián alapuló rendszer még a katonai nemzetbiztonsági szolgálatok esetében is fellazul, nagyobb teret engedve az egyéni kezdeményezőkészségnek és a kreativitásnak. A jelenség sok esetben tudattalanul jelentkezik, ami súrlódásokhoz vezethet, hiszen a katonás fegyelem és az alkotói szabadság – kellő vezetői iránymutatás, valamint a megfelelő szervezeti keretek és kultúra hiányában – nehezen összeegyeztethető fogalmak. Az ehhez szükséges lelki állapot leginkább a „rugalmas merevség" önellentmondásával írható le.

[441] VIDA Csaba: Létezik-e még a hírszerzési ciklus? Miről szól a hírszerzés? Felderítő Szemle, XII. évfolyam 1. szám, 2013. szeptember–október. pp. 43–57. https://www.knbsz.gov.hu/hu/letoltes/fsz/2013-1.pdf; letöltés: 2022.10.18.

Porkoláb Imre *A stratégia művészete – Szervezeti innováció kiszámíthatatlan üzleti környezetben – Szun-ce gondolatai alapján* című könyvében[442] – bár nem a nemzetbiztonsági szférára vetítve – a fenti problémakört járja végig. Rámutat, hogy a modern haderőkben csak részben sikerült feldolgozni a porosz vezérkarnak a napóleoni háborúk 1806-os jénai csatájából levont tanulságait, miszerint a korábbi háborúkban elengedhetetlen, merev parancsuralmi rendszer követése nemkívánatos hatással jár, mert akadályozza a győzelmet. A helyzetfelismerésre adott porosz válasz a feladatharcászat[443] volt. Az új megközelítés szerint a katonai vezetőktől már nem a parancsnok puszta, szó szerinti végrehajtását, hanem a feladat sikeres végrehajtását eredményező intézkedések kreatív meghozatalát követelték meg. Minden parancsnoki szint a maga beosztásához illeszkedő, különböző mértékű, számára világos keretekkel rendelkező cselekvési szabadságot élvezett. A diszfunkció abban az esetben keletkezik, ha a feladatharcászat nem váltja fel egyértelműen és világosan a parancsuralmat.[444,445]

Porkoláb Imre áttekinti az iparvállalatok szervezeti fejlődésének főbb lépcsőit is, aminek a jelentőségét az adja, hogy az amerikai nemzetbiztonsági rendszer második világháborút követő kialakítására mélyreható hatást gyakoroltak az iparvállalatok szervezeti modelljei. Ez nem meglepő, hiszen az amerikai vezetés és a közvélemény a második világháborús győzelmet legalább annyira tekintette a kapitalista piacgazdaság diadalának, mint a harcokban részt vevő milliók érdemének. Az amerikai modellt módosításokkal átvették a nyugati szövetségesek, illetve részben a Varsói Szerződés tagállamai és más országok is.

A modern, funkciók (tervezés, gyártás, értékesítés stb.) szerint felépülő, modern monolitikus vállalati modell a 20. század elejére alakult ki. A formális hierarchiára építő vállalatirányítási modelleket követő szervezet kis létszámú felső vezetésből, önálló döntési jogkör nélküli végrehajtók tömegéből, illetve a két csoport között közvetítő, a feladatokat kiosztó, a teljesítményt mérő és az ellenőrzést gyakorló középvezetőkből áll. A monolitikus szervezet első modellje a piramis, ahol a feladatokat a felső vezetés meghatározza, a középvezetők kiosztják, a hierarchia alsó rétege pedig végrehajtja.

A vállalatok növekedésével egyre több szervezeti elem jött létre, amelyek egy-egy funkcionális feladat (termék, szolgáltatás, iparág, pénzügy, gyártás, tervezés stb.) vagy területi divízió köré szerveződtek. Emellett számos új típusú szervezeti elem jelent meg (pl. kutatás és fejlesztés, ellátásilánc-menedzsment, marketing stb.). A második világháború időszakára az amerikai vállalatokban a funkciók számának és diverzitásának növekedése meghaladottá tette a piramisszerkezetet. A monolitikus modellt az 1920-as évektől kezdte el felváltani a napjainkban is leginkább elterjedt, operatív divíziókon alapuló felosztás, ahol a vállalatok szervezeti elemei már termék vagy ügyfél, esetleg régió szerinti felosztás szerint különülnek el. Ebben a modellben

[442] PORKOLÁB Imre: A stratégia művészete – Szervezeti innováció kiszámíthatatlan üzleti környezetben – Szun-ce gondolatai alapján. HVG Könyvek, Budapest, 2019.
[443] Auftragstaktik.
[444] Normaltaktik.
[445] PORKOLÁB Imre: A stratégia művészete – Szervezeti innováció kiszámíthatatlan üzleti környezetben – Szun-ce gondolatai alapján. HVG Könyvek, Budapest, 2019. p. 21.

az egyes divíziók maguk felelősek a saját nyereségükért és veszteségükért.[446] Funkciók közötti szervezeti egységeket hoztak létre annak érdekében, hogy a szervezeti elemek sokasága között együttműködés valósuljon meg. Ezt a megközelítést mátrixmodellnek nevezzük. Az ilyen modellben a divíziók közötti együttműködés komplex és időigényes döntéshozatali folyamatokon alapul.[447]

Az ezredforduló időszakára a hierarchikus struktúrák kezdték elveszíteni az előnyeiket. A túlságosan merev felépítés kedvezett a stabilitásnak, de egyre kevésbé volt képes reagálni a piac gyorsuló változása miatt fellépő új igényekre. A legújabb kihívásra adott választ a decentralizáció és a stratégiai hálózatok megjelenése jelentette. Porkoláb szerint a vállalatirányításra is nagy hatást gyakoroltak a 2003-as iraki háború első, hagyományosnak tekinthető szakaszát követő aszimmetrikus kihívásokra adott amerikai válaszok. Az Irakban állomásozó amerikai különleges műveleti erők parancsnoki beosztását 2006 és 2008 között betöltő Stanley McChrystal altábornagy (2009-től vezérezredes) számára a kezdetektől világossá vált, hogy az iraki ellenállók nem klasszikus katonai, hanem hálózatos szervezeti felépítéssel rendelkeznek, és felismerte, hogy ellenük hatékonyan fellépni csak a különleges erők felépítésének hálózatossá alakításával lehetséges. Egy hálózatot csak egy másik hálózat győzhet le. Célként tűzte ki az információáramlás növelését, ennek érdekében az alárendelt szervezeti elemek számára közös harcálláspontot (fúziós központot) hozott létre. A technológiai lehetőségek kiaknázásával napi rendszerességgel tartott video-távkonferenciát több ezer fő részvételével. Ezeken a konferenciákon a vezetői szándék ismertetése mellett a műveleti tapasztalatok megosztása is megvalósult. Az új megközelítés megteremtette a közös helyzetismeretet, amelynek birtokában már lehetővé vált a döntéseknek a lehető legalacsonyabb szintre történő delegálása. Ekkor jelent meg a „stratégiai tizedes" fogalma annak jelzéseként, hogy az alsóbb vezetői szinteken is elvárássá vált az önálló kezdeményezés és a felelősségvállalás.[448]

A McChrystal tábornok által megteremtett új, küldetésorientált (vagy küldetésalapú) vezetési szemlélet – a porosz feladatharcászat modern változataként – lehetővé teszi, hogy az alacsonyabb szintű vezetők a vezetői szándék ismeretében elviselhessék a káoszt. Kialakult az *in extremis* vezetői szemlélet, amely a kaotikus helyzetekre proaktív módon, a válságok bekövetkezte előtt készül fel. Megvizsgálja, hogy mit kell megőrizni és min kell változtatni. Az új szervezeti kultúra a beosztottaktól is új megközelítést vár el. A hatékony követő jól menedzseli magát, elkötelezett a szervezeti célok és értékek iránt, saját képességeit építi, vállalja a véleményét a vezetőkkel szemben is, és tevékenységét nem szükséges felügyelni. Fontos, hogy a felettesek és az alárendeltek céljai megegyezzenek.

---

446 PORKOLÁB Imre: A stratégia művészete – Szervezeti innováció kiszámíthatatlan üzleti környezetben – Szun-ce gondolatai alapján. HVG Könyvek, Budapest, 2019. pp. 25–28.

447 MINNAAR, Joost: The Evolution Of (Progressive) Scalable Organizational Structures. Corporate Rebels, 2020.11.18. https://corporate-rebels.com/the-evolution-of-progressive-organizational-structures/; letöltés: 2021.12.24.

448 PORKOLÁB Imre: A stratégia művészete – Szervezeti innováció kiszámíthatatlan üzleti környezetben – Szun-ce gondolatai alapján. HVG Könyvek, Budapest, 2019. pp. 131–132.

Az operatív divíziók szerint megosztott vállalati modell és a stratégiai hálózatok ötvözete a komplex adaptív vezetés, ahol a vállalat eltérő rendszereket működtet párhuzamosan. A hagyományos, bürokratikus szervezeti forma biztosítja a stabilitást, míg az adaptív és innovatív szervezeti elemek teszik lehetővé a felkészülést az új kihívásokra.

Porkoláb Imre a szervezeti kultúra megváltoztatását négylépcsős modellként írja le. A kirekesztési lépcsőben az új szervezeti elem munkatársait leválasztják a vállalat egészéről. Az inkubáció során az új szervezeti elem a vezetés védelme alatt alakítja ki a működési rendjét. Az integráció lépcsőjében az új szervezeti elem a vállalat részévé válik. Ez a folyamat legveszélyesebb része, hiszen ekkortól érik támadások a szervezet többi részétől. Ebben a szakaszban elengedhetetlen a szervezet középvezetésének megnyerése az új módszerek hatékonyságával kapcsolatban. Amennyiben ez sikerrel jár, megvalósul a negyedik lépcső, az asszimiláció.[449]

Változásmenedzsment a nemzetbiztonsági rendszerben

A nemzetbiztonsági szervezetekben szükséges változások végrehajtását nagyban megnehezíti, hogy a vezetők és a beosztottak ritkán rendelkeznek a kellő speciális képzettséggel és rutinnal a valódi, átfogó változások véghezviteléhez. A védelmi szektorhoz hasonlóan a nemzetbiztonsági rendszerben is általános a feladatok, a beosztások és az állomáshelyek gyakori változása, ez azonban nem a változások gyors bevezetésének, hanem éppen ellenkezőleg, a tényleges változtatások elodázásának kedvez.

A változtatások tervezésében, vezetésében és menedzselésében meglévő rutintalanság ellenszere lehet, ha a nemzetbiztonsági szektor megkísérel már kidolgozott, az üzleti életben bevált modelleket a saját igényeire szabva alkalmazni. Farkas Ferenc *A változásmenedzsment elmélete és gyakorlata* című könyvében[450] bemutatja Barbara Senior PETS-tesztjét és John Kotter nyolc szakaszból álló változásmenedzsment-modelljét. Mindkettő jól adaptálható lehet a nemzetbiztonsági rendszer igényeihez.

A PETS-teszt a politikai tényezők (Political), a gazdasági tényezők (Economic), a technológiai tényezők (Technological) és a szociokulturális (Sociocultural) tényezők vizsgálatával méri fel a szervezetet érő környezeti hatásokat.[451] A megközelítés szinte változtatás nélkül felhasználható a nemzetbiztonsági szféra számára, hiszen arra hasonló politikai, gazdasági, technológiai és szociokulturális faktorok hatnak, mint az üzleti világ szereplőire. A politikai faktorok közül a legfontosabbak a nemzetbiztonsági tevékenységet szabályozó jogszabályok, stratégiák, mindenekelőtt a nemzeti védelmi stratégia (a katonai nemzetbiztonsági szolgálatok számára a nemzeti katonai stratégia is), a minősített adatok kezeléséről szóló törvények, az ország hivatalos és informális külpolitikai stratégiája, tagsága a nemzetközi szervezetekben és szövetségi rendszerekben,

[449] PORKOLÁB Imre: A stratégia művészete – Szervezeti innováció kiszámíthatatlan üzleti környezetben – Szun-ce gondolatai alapján. HVG Könyvek, Budapest, 2019. pp. 181–193.
[450] FARKAS Ferenc: A változásmenedzsment elmélete és gyakorlata. Akadémiai Kiadó, Budapest, 2013.
[451] FARKAS Ferenc: A változásmenedzsment elmélete és gyakorlata. pp. 51–53.

részvétele a nemzetközi katonai és válságkezelő műveletekben stb. A politikai faktorok közé sorolható a döntéshozók hírigénye és az általuk szabott egyéb feladatok is. A szociokulturális tényezők közül elsősorban az alkalmazottakra és a jelöltekre ható jelenségek és folyamatok, például a nemzetbiztonsági tevékenység társadalmi megítélésének vizsgálata lehet releváns. Az állomány megtartása és a hatékony toborzás érdekében szükséges az általános (munkaerő)piaci folyamatok nyomon követése, hiszen a munkavállalók által támasztott követelmények (versenyképes jövedelem, kulturált elhelyezés, családbarát megközelítés, rugalmas munkaidő, otthoni munkavégzés lehetőségeinek megteremtése stb.) figyelmen kívül hagyása hosszú távon éppen a működésük alapját jelentő minőségi munkaerőtől fosztja meg a szolgálatokat.

A technológiai tényezők szintén messzemenő hatással vannak a szolgálatokra. A változások lassúsága talán ezen a területen a legszembetűnőbb, mert a technológiai versenyben lépést nem tartó, a megújulást halogató szolgálatok kevésbé képesek megtartani az újonnan állományba vett fiatal munkatársakat. A PETS-teszt négy tényezője közül látszólag a gazdasági hat legkevésbé a szolgálatokra, hiszen nem a „piacról élnek", hanem költségvetési forrásból működnek. Valójában az állam teherbíró képessége közvetlenül befolyásolja a szolgálatok működését, a versenytársak között pedig nemcsak rivális (társ)szolgálatok és egyéb szervezetek, hanem piaci szereplők (hírügynökségek, kutatóintézetek, magán titkosszolgálatok és tartalomszolgáltatók) szerepelnek. Nem szabad megfeledkezni ugyanakkor arról, hogy igazi „versenytársaik" az ellenérdekelt és az ellenséges nemzetbiztonsági szolgálatok, a terrorszervezetek és a szervezett bűnözés!

A PETS-teszt elsősorban a változásokat megelőzően, a helyzetismeret növelésére nyújthat hatékony támogatást. A tényleges változások menedzselésére ezt követően John Kotter 1999-ben felállított modellje alapján nyílik lehetőség.

A modell nyolc szakaszból áll:

- az egészséges veszélyérzet felkeltése, a változtatás halaszthatatlanságának érzékeltetése;
- a változást irányító csapat létrehozása;
- a változás jövőképének és stratégiájának kialakítása;
- a változás jövőképének kommunikálása;
- az alkalmazottak felhatalmazása a cselekvésre;
- eredmények elérése rövid távon, gyors sikerek kivívása;
- az eredmények megszilárdítása és további változások kezdeményezése;
- az új megoldások meggyökereztetése a vállalati kultúrában.

Farkas Ferenc Kotter modelljét bemutató esettanulmányában szereplő „Hajóstársaság" által véghezvitt változtatás és a felmerült problémák meglepően jól megfeleltethetők a nemzetbiztonsági rendszer kihívásaira is. A változás halaszthatatlanságának érzékeltetéséről szóló alfejezetben a Hajóstársaság azzal szembesül, hogy az elszállított húszlábas standard konténerek (TEU[452]) száma már nem alkalmas a teljesítmény mérésére, ehelyett a nehezebben nyomon követhető, de releváns adatokat szolgáltató nyereségességet tették mérőszámmá. A nemzetbiztonsági szolgálatoknál a TEU megfeleltethető a jelentésszámnak, míg a profit az átadott információ hasznosságának a döntéshozók szempontjából. Ahogyan a TEU esetében, úgy a jelentésszám nyomon követése is könnyen kivitelezhető, de a szolgálat hasznosságát önmagában talán még kevésbé tükrözi. A nyugati szolgálatoknál gyakori eljárás, hogy például rövid kérdőívekkel visszacsatolási lehetőséget nyújtanak a döntéshozóknak, javítva saját teljesítményük mérésének objektivitását. A teljesítmény mérésében kulcsszerepet játszanak a döntéshozók és a szolgálatok közötti információáramlást megvalósító összekötők is.

A Hajóstársaság külön csapatot hozott létre a változás irányítására. A csapat nem külön szigetként működött, hanem a középvezetőket, az országvezetőket, az ügyfelekkel foglalkozó *account manager*eket, az értékesítési osztályt, valamint a személyügyet és az oktatást végző szervezeti egységeket is bevonta a tevékenységébe.[453] Az esettanulmány a szervezeti sajátosságok figyelembevételével itt is szinte változtatás nélkül felhasználható. Fontos tehát a középvezetők (igazgatók) és az országmenedzserek (területi vezetők: osztályvezetők, iránytisztek) mihamarabbi bevonása, hogy felkészülhessenek a változások kommunikálására és időben jelezzék a problémásnak tartott lépéseket. A nemzetbiztonsági rendszerben az ügyfelek a döntéshozók, ezért az „*account manager*i" feladatokat elsősorban a szolgálatok felső vezetése, illetve különböző (műveleti) szervezeti egységek igazgatói látják el az osztályvezetők támogatásával. Az „értékesítési osztály" részben megfeleltethető az elemző-értékelő (tájékoztató) szervezetnek, hiszen az ő állománya az, amely elkészíti a felhasználók számára a jelentéseket (mint a legtöbb hírszerző tevékenység végtermékét) és tartalmukat esetenként szóban is bemutatja. A felső vezetés szintén rendszeresen végez „értékesítési" feladatokat. A személyügy és az oktatás bevonásának fontossága szintén megkérdőjelezhetetlen. A dedikált *account manager*ek hiánya a nemzetbiztonsági szervezetek hiányosságának tekinthető, mert tevékenységükre egyre fokozódó szükség lenne a döntéshozókkal való közvetlen, intézményesített kapcsolat tartásában. Ezt jól jelzi, hogy a vezetői állomány munkaidejének jelentős részét az *account manager*i tevékenység teszi ki.

A további szakaszok (a változás jövőképének a kommunikálása, az alkalmazottak hatalommal történő felruházása, gyors győzelmek kivívása, az elért eredmények megszilárdítása és az új megoldások meggyökereztetése a szervezeti kultúrában) módosítás nélkül átvehetők a nemzetbiztonsági rendszer számára.

[452] Twenty-foot equivalent unit.
[453] FARKAS Ferenc: A változásmenedzsment elmélete és gyakorlata. pp. 56–58.

Fontos hangsúlyozni – ahogyan Kotter is teszi – az egyes lépések és azok sorrendjének fontosságát, mert a nemzetbiztonsági szervezetek is hajlamosak arra, hogy a könnyebb, gyorsabb és olcsóbb megoldásokat válasszák. Ennek különösen akkor nagy a veszélye, ha a változási kényszer kívülről (a politikai vagy a katonai felső vezetők irányából) származik, és az időfaktor miatt vagy a változás szükségességébe vetett hit hiányában a nemzetbiztonsági szolgálat vezetése látszatmegoldással is megelégszik.

Változás és szervezeti kultúra

A PETS-tesztet és a Kotter-modellt jól kiegészítheti a katonai szervezetek által alkalmazott „gördülő tervezés",[454] ahol a változásokat folyamatosan értékelik, azokról visszacsatolásokat küldenek, és a szervezetet ezek alapján módosítják. A gördülő tervezés mögötti elgondolás lényege, hogy a változás nem egy egyszeri, fájdalmas, senki által nem kívánt és kívülről erőltetett esemény, hanem a sikeres működés alapvető, a szervezetben működő egyének perspektívájából nézve is pozitív, állandó folyamat. Az utóbbi megközelítést tükrözi a nyugati vállalati, katonai és nemzetbiztonsági kultúrában is elterjedt úgynevezett „*off-site*". A tevékenység lényege, hogy a feladat-végrehajtás mindennapi helyszínétől lehetőleg távol (innen az elnevezés) a szervezet teljes egészét reprezentáló csoport, akár a teljes állomány rendszeres időközönként (negyedévente, félévente vagy évente) szekciókra osztva megvizsgálja a szervezet egy-egy részterületének (pl. jelentési rend, az információáramlás, a szervezetek közötti együttműködés rendje, szervezeti kultúra stb.) működését. A csoportok tevékenységét erre speciálisan képzett szakemberek irányítják. E tevékenység lényege a szükségtelen munkafolyamatok kiiktatása, a hibás folyamatok javítása és szükség esetén új folyamatok rendszeresítése. Az összejövetelek végén a résztvevők ajánlásokat fogalmaznak meg a vezetésnek. Az „*off-site*"-ok segítségével racionalizálható a szervezetek működése és kiiktathatók a pusztán megszokásból végzett tevékenységi módok.

Az amerikai hírszerzési reform és tanulságai – a Központi Hírszerző Ügynökség reformja

A 21. század első évtizedében az Amerikai Egyesült Államok Hírszerző Közössége (IC) nemzetbiztonsági szolgálatok laza hálózataként egyre kevésbé volt képes megfelelni a kihívásoknak. A szervezeti összevonások akadályait felismerve az amerikai nemzetbiztonsági vezetés úgy határozott, hogy az IC tevékenységét funkcionálisan, az elvek, a módszerek és az eljárások, összességében a szervezeti kultúra egységesítésével integrálja.[455] A folyamat motorja a Nemzeti Hírszerző

[454] Rolling plan.

[455] E megközelítést a DNI az „Intelligence Enterprise" fogalommal írja le.
Intelligence Community Directive 103 – Intelligence Enterprise Exercise Program. ODNI, 2008.07.14.
www.dni.gov/files/documents/ICD/ICD_103.pdf; letöltés: 2019.10.29.
A Hírszerző Közösség felépítéséről és reformjáról lásd:
ERDÉSZ Viktor: Az amerikai hírszerzési reform és tanulságai. Felderítő Szemle, XVIII. évfolyam 3. szám, 2019. pp. 111–128.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2019-3.pdf; letöltés: 2020.02.14.

Főigazgató (DNI), aki a Hírszerző Közösség tevékenységének szakmai irányítását az eljárások egységesítésére és összehangolására, jog-, hatás- és feladatkörök delegálására, valamint új szervezeti egységek megalakítására szolgáló, az IC egészére vonatkozó utasításokkal[456] valósítja meg. Az utasításokban megfogalmazott általános elveket iránymutatások,[457] eljárások[458] és emlékeztetők[459] részletezik.[460]

Az átláthatóság jegyében az utasítások szabadon elérhetők a Nemzeti Hírszerző Főigazgató Hivatalának (ODNI) honlapján.[461] A titoktalanításnak ez az amerikai gesztusa rámutat arra, hogy a nemzetbiztonsági tevékenységek, módszerek és információk meghatározott köréről folytatott tudományos és közéleti diskurzus, valamint az átláthatóságból eredő társadalmi támogatottság előnyei messze meghaladják a közzététellel járó kockázatokat. E könyv elkészülte is e megközelítés hozadéka.

Az először a 2005-ben közzétett és azóta folyamatosan frissített nemzeti hírszerzési stratégiákban lefektetett elveket elsőként a CIA valósította meg. John Brennan, a Központi Hírszerző Ügynökség volt főigazgatója[462] 2015. március 6-án közzétett, az Ügynökség munkatársainak címzett levelében[463] tájékoztatást adott a CIA küszöbön álló szervezeti reformjáról. Brennan főigazgató szerint a vizsgálatra azért volt szükség, mert a 21. század második évtizedében a döntéshozók érdeklődésére számot tartó folyamatok és események egyre komplexebbé váltak, miközben példa nélküli technológiai fejlődés van folyamatban. A főigazgató 2014 szeptemberében a CIA kilenc felső vezetőjét bízta meg a szervezet korszerűsítésére vonatkozó javaslat előkészítésével. A munkacsoport által a kutatás 90 napja alatt 80 döntéshozóval készített interjú és az Ügynökség 4000 munkatársának javaslatai, valamint a nagyvállalati munkamódszerek tanulmányozása alapján az igazgató 2015 márciusa és októbere között átfogó szervezeti átalakításokat léptetett életbe.

A CIA új alapokra helyezte a humán erőforrás fejlesztési és képzési rendszerét (ún. „tehetségmenedzsment"). Ennek keretében létrehozták a Tehetségfejlesztési Kiválósági Központot,[464] amely a toborzástól kezdve szakirányú és vezetői képzésekkel fejleszti a humán erőforrást. Az új szervezeti egység célja, hogy a munkatársak a szakterületük fejlesztése mellett szélesebb perspektívát kapjanak más szakágak és a CIA egészének tevékenységéről.

---

456 Intelligence Community Directive – ICD.
457 Intelligence Community Policy Guidance – ICPG.
458 Intelligence Community Standard – ICS.
459 Intelligence Community Memorandum – ICM.
460 Intelligence Community Directive 101 – Intelligence Community Policy System. ODNI, 2019.10.22. www.dni.gov/files/documents/ICD/ICD_101.pdf; letöltés: 2019.10.29.
461 Intelligence Community Directives. Office of the Director of National Intelligence. https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives; letöltés: 2019.10.29.
462 Brennan 2013. március 8. és 2017. január 20. között töltötte be a beosztást.
463 BRENNAN, John: Our Agency's Blueprint for the Future (Unclassified Version of March 6, 2015 Message to the Workforce from CIA Director). CIA, 2015.03.06. https://www.cia.gov/news-information/press-releases-statements/2015-press-releases-statements/message-to-workforce-agencys-blueprint-for-the-future.html; letöltés: 2017.06.06.
464 Talent Management Centre of Excellence.

Felismerve, hogy a digitális technológiák fejlődése kihívás és lehetőség is a CIA számára, létrejött a Digitális Innovációs Igazgatóság,[465] melynek feladata az új technológiák – ideértve a kiberképességeket – CIA-n belüli integrálásának felgyorsítása és a digitális hírszerzési módszerek[466] fejlesztése. A CIA – egyben a teljes Hírszerző Közösség – dedikált OSINT-szervezetét az Igazgatóság alárendeltségébe helyezték.[467]

A világpolitikai folyamatok változásának üteme megköveteli, hogy a döntéseket a megfelelő szinten, a szükséges mennyiségű és minőségű információ birtokában, a CIA egészének érdekei figyelembevételével a lehető leggyorsabban hozzák meg. Ennek érdekében Brennan főigazgató úgy határozott, hogy a döntéseket a lehető legalacsonyabb szinteken kell meghozni. A napi feladatok irányítására megerősítette a már meglévő műveleti területért felelős főigazgatóhelyettesi[468] beosztás jog- és hatáskörét, valamint önálló irodát delegált a számára (ún. „vállalati modell"[469]).

Végül a műveleti (a CIA értelmezésében a HUMINT-kapcsolatkezelők és a fedett műveletek irányítói), az elemzői, a tudományos-technikai és a támogató szakembergárda egy részének integrálásával tíz műveleti központot[470] hozott létre (Afrika; elhárítás; terrorelhárítás; kelet-ázsiai és csendes-óceáni térség, Európa és Eurázsia; globális ügyek, Közel-Kelet; Dél- és Közép-Ázsia; illegális fegyverkereskedelem és proliferációellenes tevékenység; nyugati félteke[471]). A központokat – a műveleti vagy az elemző szakterületről érkezett – igazgatók[472] vezetik. A központok felállításával befejezték működésüket a Műveleti és az Elemző Igazgatóság tradicionális, területi feloszlású részlegei (pl. Közel-Kelet, Latin-Amerika, Dél-Ázsia stb.).

Felismerve, hogy a műveleti vagy elemző jellegű feladatokkal kapcsolatos, megalapozott döntéshozatal magas szintű szaktudás nélkül lehetetlen, a műveleti hátterű igazgatóhelyettesek alá elemző, az elemzők alá műveleti hátterű helyetteseket nevezett ki. Az új központokkal párhuzamosan, továbbra is működik az Elemző, a Műveleti, a Tudományos-technológiai[473] és a Támogató Igazgatóság,[474] de azok

---

465 Directorate of Digital Innovation.

466 Digital tradecraft.

467 Az Open Source Centert (OSC) az átalakításkor Open Source Enterprise-á (OSE) nevezték át. AFTERGOOD, Steven: Open Source Center (OSC) Becomes Open Source Enterprise (OSE). FAS, 2015.10.28. https://fas.org/blogs/secrecy/2015/10/osc-ose/; letöltés: 2022.02.16.

468 Deputy Director for Operations – DDO. A CIA harmadik legmagasabb beosztású vezetője a főigazgató (Director of the Central Intelligence Agency –DCIA) és általános helyettese (Deputy Director of the Central Intelligence Agency – DDCIA) után. Az átszervezéskori angol nyelvű elnevezése Executive Director, jelenleg Chief Operating Officer.

469 A műveleti igazgató az ügyvezető igazgatónak, a CIA-igazgató a vezérigazgatónak feleltethető meg az üzleti életben. A döntéshozatali és információmenedzsment-folyamatokat a nagyvállalati módszerek figyelembevételével alakították ki.

470 Mission Center.

471 Western Hemisphere.

472 Assistant Director.

473 Directorate of Science & Technology.

474 Directorate of Support.

a továbbiakban nem a napi folyamatok irányításával, hanem a szakági képzésekkel és stratégiai tervezéssel, valamint az előmeneteli rendszerek működtetésével foglalkoznak (mátrixmodell). A műveleti központok vezetői a műveleti és az elemző igazgatókkal[475] együttműködésben, de a CIA-főigazgatónak alárendelve végzik feladataikat. A műveleti tevékenység magas szakmai színvonalának garantálása a műveleti területért felelős főigazgató-helyettes feladata.[476]

A Brennan főigazgató által életbe léptetett, módosításokkal jelenleg is működő új szervezeti struktúra célja a CIA-n belül egymással párhuzamosan működő, gyakran kontraproduktív, elsősorban a műveleti és az elemzői szervezeti kultúra között húzódó falak lebontása, majd azok felváltása egy egységes „nemzetbiztonsági szakértői"[477] kultúrával. A műveleti központok modelljeként részben a 2001. szeptember 11-ei terrortámadásokat követően létrehozott Terrorelhárítási Központ,[478] illetve a kisebb, szintén a transznacionális fenyegetések – kábítószer-kereskedelem, proliferáció – felderítésére létrehozott, a műveleti és az elemző területeket egyesítő központok szolgáltak.

Az átalakítás másik célja, hogy a CIA részben visszavegye az IC feletti irányítást a Nemzeti Hírszerző Igazgató Hivatalától. A műveleti központokban az amerikai társszolgálatok számos munkatársa dolgozik, így azok az ODNI szintén területi és funkcionális alapon működő központjaival párhuzamosan működnek.

A reform kidolgozása során Brennan főigazgató az amerikai védelmi minisztériumot és a haderő vezetését átszervező, 1986-ban hatályba lépett Goldwater–Nichols-törvényt[479] vette mintául, amely a csapatok vezetését a haderőnemektől a védelmi miniszter közvetlen alárendeltségébe tartozó egyesített hadszíntéri[480] és funkcionális parancsnokságok[481] hatáskörébe helyezte át. A törvény célja a haderőnemek közötti, a vietnami vereség egyik okának tartott versengés hátrányainak kiküszöbölése volt.

---

475 A szakági igazgatók a műveleti központok vezetői (Assistant Director) felett állnak a CIA hierarciájában. CIA Leadership (2018). https://www.cia.gov/about-cia/leadership; letöltés: 2019.05.11.

476 SLICK, Stephen: Measuring Change at the CIA. Foreign Policy, 2016.05.04. http://foreignpolicy.com/2016/05/04/measuring-change-at-the-cia/; letöltés: 2016.06.06.

477 Intelligence officer.

478 Counterterrorism Center.

479 Goldwater-Nichols Department of Defense Reorganization Act of 1986. Public Law 99-433, 1986.10.01. https://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf; letöltés: 2019.05.11.

480 US CENTCOM – US Central Command: Központi Parancsnokság; US NORTHCOM – US Northern Command: Északi Parancsnokság; US SOUTHCOM – US Southern Command: Déli Parancsnokság; US INDOPACOM – US Indo–Pacific Command: Indopacifikus térség Parancsnoksága; US AFRICOM – US African Command: Afrikai Parancsnokság; US EUCOM – US European Command: Európai Parancsnokság.

481 Jelenleg: US Strategic Command – Stratégiai Parancsnokság; US Cyber Command – Kiberműveleti Parancsnokság; US Special Operations Command – Különleges Műveleti Erők Parancsnoksága; US Transportation Command – Szállítási Parancsnokság.

A reformok életbe léptetését követően a Nemzeti Titkosszolgálat[482] és az elhárítás vezetője, valamint több magas beosztású alárendeltjük kérte felmentését, elsősorban a „*need to know*" elvének[483] vélt felrúgását nevezve elfogadhatatlannak. A felháborodásban emellett nagyban közrejátszott az évtizedes – sok esetben a második világháborút is megelőző – struktúrák, bevett gyakorlatok és előjogok megszűnése.[484]

A reformok kritikusai és bírálói is kiemelik a műveleti központok új megközelítését, amely szerint az elemzők közvetlenül is támogatják a HUMINT-munka több mozzanatát. A központokban dolgozó elemzők segítik a HUMINT-szakembereket abban, hogy valóban a releváns információkkal szolgáló személyeket szervezzék be, és hogy a forrásoknak a megfelelő kérdéseket tegyék fel, gyorsan értékelve a megszerzett információ hitelességét. Az elemzők a HUMINT-források beható ismeretével könnyebben értékelhetik a forrás megbízhatóságát és az átadott információ hitelességét. A központok működése emellett nagyban felgyorsítja és elmélyíti az elemzők helyzetértékelését, mert lehetőségük van közvetlenül kommunikálni a CIA külföldi irodáival és állomásaival.

A központok létrehozásával számos vezetési kérdés merült fel mind műveleti, mind elemzői oldalon. Nem világos, hogy a műveleti és az elemző igazgatók hogyan képesek a mindennapi munkában garantálni annak magas szakmai színvonalát. Tisztázásra vár továbbá, hogy végső soron kit terhel a felelősség a világszerte feladatot végrehajtó műveleti tisztek biztonságáért. Az elemző igazgató munkáját hasonlóképpen megnehezíti, hogy az új hierarchiában a műveleti központok vezetői és a CIA-főigazgató közötti kapcsolaton kívül áll, mégis az ő feladata az Ügynökség elemzéseinek minőségbiztosítása.[485]

A reform tehát felgyorsította a napi munkavégzést és lebontotta a szakágak közötti falakat, de új, nem kívánt bürokratikus akadályokat teremtett, megnehezítve a központokban dolgozó szakemberek számára egyebek mellett a saját karrierjük tervezését.[486] A műveleti központok és a szakigazgatóságok párhuzamos működése okozta anomáliák kiküszöbölése érdekében a CIA több ponton módosította és egyszerűsítette a rendszert. Egyebek mellett az egyes hírszerző jelentéseket felülvizsgáló elemzők számát három főben maximalizálták, és egyértelműen a szakigazgatók kompetenciájává tették az előléptetések jóváhagyását.

---

[482] National Clandestine Service: 2015-ig a fedett és titkos hírszerzésért és a hírszerző műveletekért felelős szervezeti egység.

[483] A munkatársak kizárólag a betekintési jogkörüknek megfelelő, a munkavégzésükhöz szükséges minősített információhoz férhetnek hozzá.

[484] IGNATIUS, David: Will John Brennan's controversial CIA modernization survive Trump? The Washington Post, 2017.01.17. https://www.washingtonpost.com/opinions/will-john-brennans-controversial-cia-modernization-survive-trump/2017/01/17/54e6cc1c-dcd5-11e6-ad42-f3375f271c9c_story.html; letöltés: 2017.06.06.

[485] SLICK, Stephen: Measuring Change at the CIA. Foreign Policy, 2016.05.04. http://foreignpolicy.com/2016/05/04/measuring-change-at-the-cia/; letöltés: 2016.06.06.

[486] IGNATIUS, David: Will John Brennan's controversial CIA modernization survive Trump? The Washington Post, 2017.01.17.

A Központi Hírszerző Ügynökség átszervezésének vizsgálata szervezetelméleti szempontból

A CIA átszervezésének folyamata jól hasznosítható például szolgál a korszerű szervezetelméleti modellek alkalmazására a nemzetbiztonsági szervezetek modernizálása során. Hogy megérthessük a szervezetelméleti vonatkozásokat, érdemes megvizsgálni a CIA szervezeti felépítésének közelmúltbeli evolúcióját.

A 10. ábrán a nemzetbiztonsági szolgálatok klasszikus szervezeti modellje látható. A monolitikus szervezet rendszerező elve a funkció: adminisztráció, elemzés-értékelés („*intelligence*", egyben elhárítás), kutatás és fejlesztés, fedett és titkos információszerzés és hírszerző műveletek („*operations*"), illetve a különböző kiegészítő szakterületek. A funkciók között éles határok emelkednek, az elkülönített tevékenységek kizárólag a felső vezetés szintjén érnek össze. A CIA 1996-os szervezeti ábrája a piramismodell kései, fejlett példája.

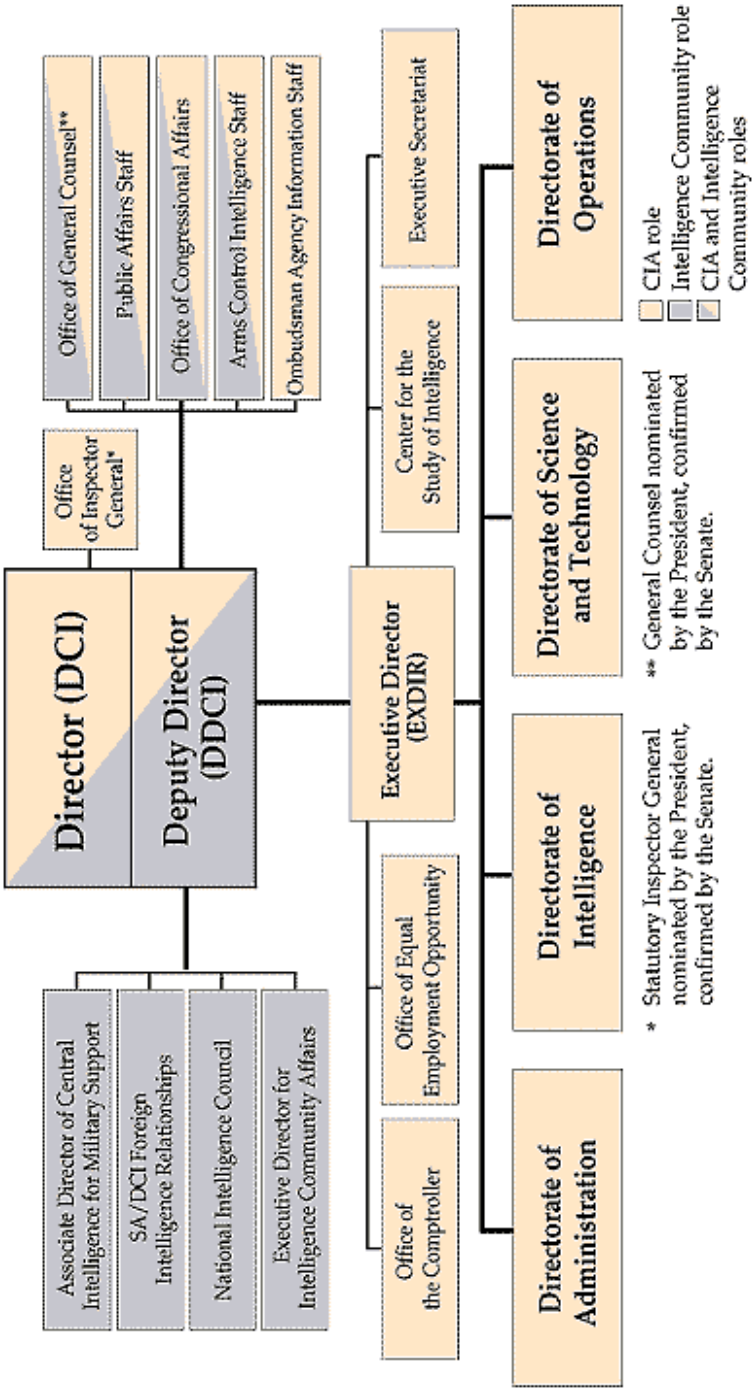
Bár 2009-re az amerikai nemzetbiztonsági rendszer már régen maga mögött hagyta a hidegháborús időket és nyolc éve folytatta a terrorizmus elleni háborút, a szervezet felépítése (11. ábra) alig változott 1996 óta. A CIA felépítését 2009-ben is piramisszerű funkcionális modell jellemzi, miközben új funkciók (pl. az akkorra már megkerülhetetlen OSINT-központ) jelentek meg.

A CIA jelenlegi, a 2015-ben indított reformokat követő szervezeti felépítése már a mátrixszerkezetet tükrözi (12. ábra). A funkcionális és a területi felosztás mellett „*enterprise functions*" elnevezéssel csoportosították a funkciók közötti szervezeti egységeket. Emellett a műveleti központok formájában megjelentek a függetlenül működő – csak a felső vezetésnek alárendelt – operatív divíziók is.

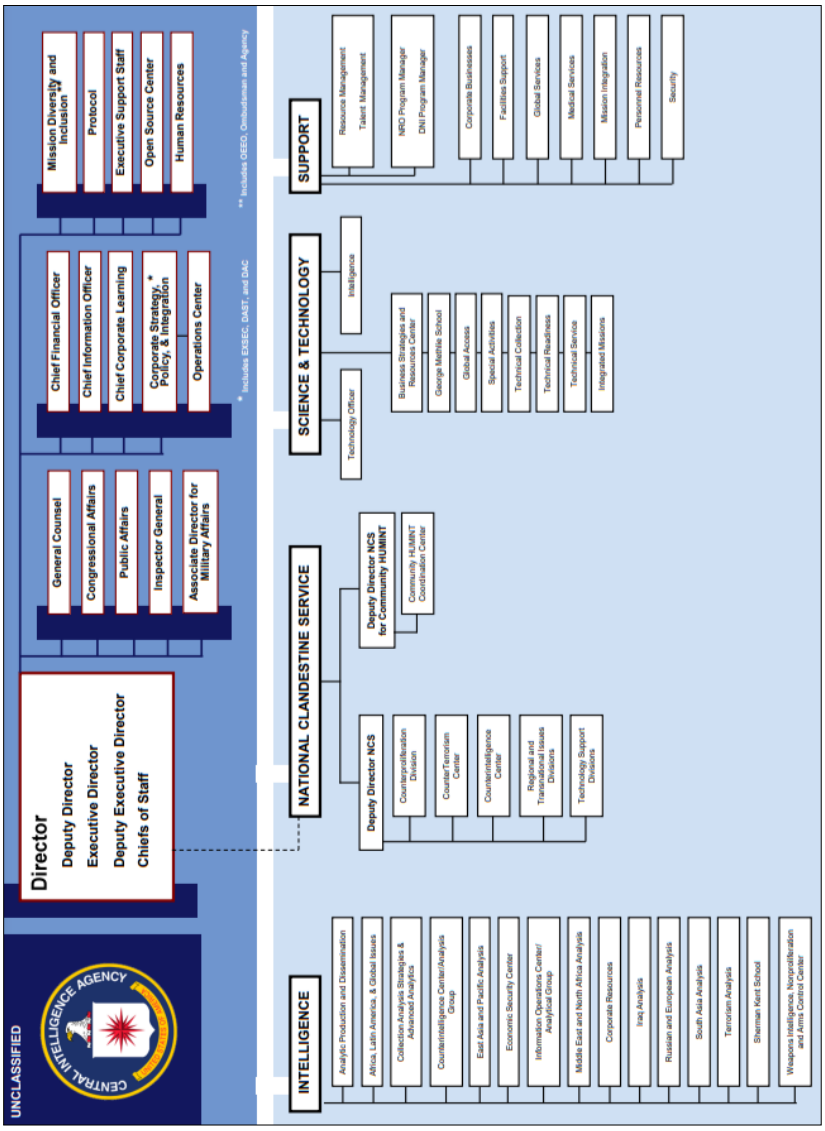
A műveleti központok a stratégiai hálózatok működési modelljét követik, hiszen létrehozásuk, megszüntetésük és átalakításuk viszonylag egyszerű, a központokban az információáramlás gyors,[487] a különböző szakterületek munkatársainak közös helyzetismerete könnyen megvalósítható. A központokban minimális vezetői állomány (parancsnok és helyettese) mellett a feladatharcászat elvei szerint tevékenykedő, a feladataikkal tisztában lévő, munkájukért felelősséget vállaló, egyénileg és csoportban is jól teljesítő szakemberek dolgoznak. A CIA összességében tehát megfelel a komplex adaptív vezetés követelményeinek.

A CIA szervezeti modellje az amerikai Hírszerző Közösségben mára bevetté vált. Az új struktúra kialakításának hosszú halogatása és a reformokkal szembeni belső ellenállás példa arra, hogy a külvilágtól elzárt nemzetbiztonsági szervezetek milyen nehezen képesek a megújulásra.

[487] Az információáramlást pusztán a közös elhelyezés is nagyban elősegíti.

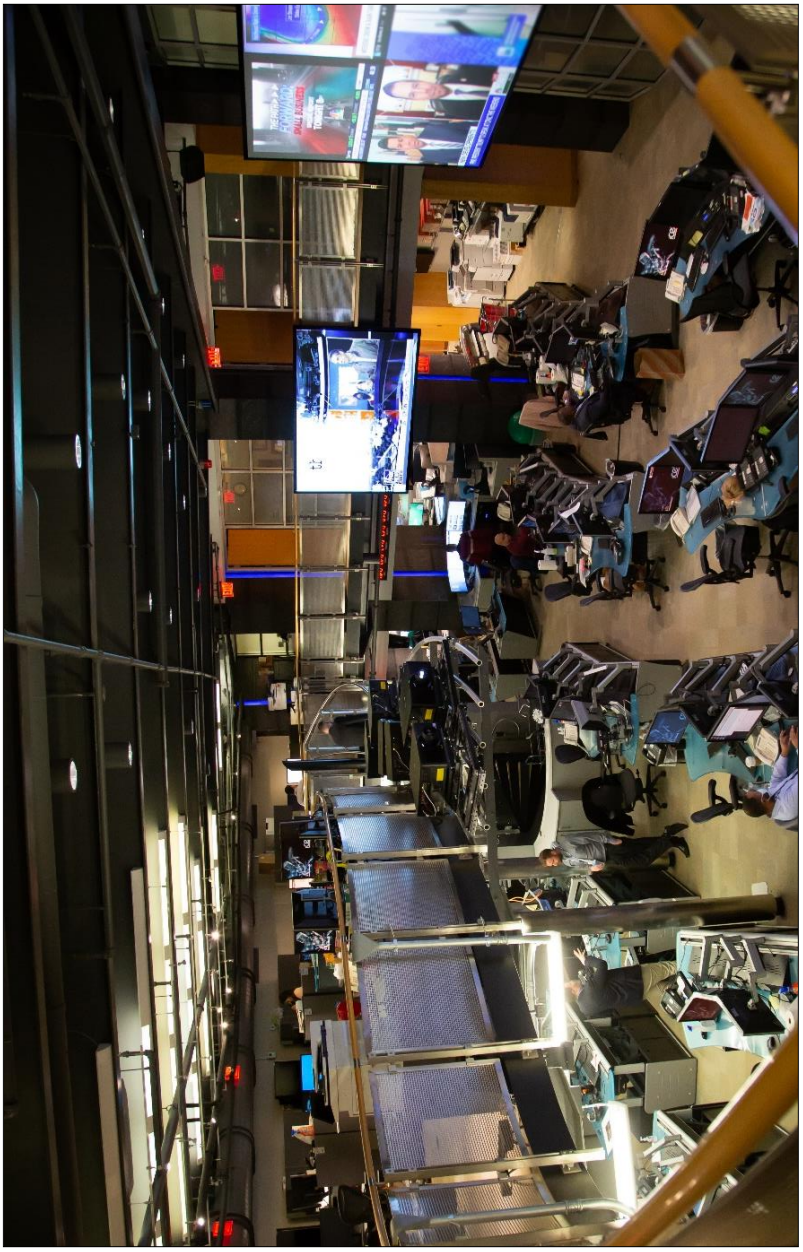


10. ábra. A CIA szervezeti felépítése 1996-ban
https://en.wikipedia.org/wiki/Organizational_structure_of_the_Central_Intelligence_Agency; letöltés: 2021.12.24.



11. ábra. A CIA szervezeti felépítése 2009-ben
https://irp.fas.org/cia/orgchart.pdf; letöltés: 2021.12.25.

12. ábra. A CIA jelenlegi szervezeti felépítése
https://www.cia.gov/about-cia/leadership/cia-organization-chart.html; letöltés: 2019.05.11.



13. ábra. A Nemzeti Hírszerző Főigazgató Hivatalában működő Nemzeti Terrorelhárító Központ műveleti terme
Standing WatcH 24/7: NCTC Operations CentER, ODNI, 2021.04.19.
https://www.dni.gov/files/ODNI/images/news_images/NCTC-Ops-center-2021/303A7706_2.jpg; letöltés: 2021.12.25.

A KORSZERŰ NEMZETBIZTONSÁGI HÍRSZERZŐ ELEMZÉS-ÉRTÉKELÉS RENDSZERE ÉS FELADATAI

Az elemző-értékelő munka fogalma, feladatai és szerepe a hírszerzési ciklusban, valamint hat tevékenységi köre

Amíg a hírszerzés tulajdonképpen egyidős az emberiséggel, az önálló tevékenységként végzett elemzés-értékelés modern jelenség. Ennek két, egymással összefüggő fő oka van: egyrészt a világban zajló folyamatok összetettsége a modern korig nem tette szükségessé a hírek és az értesülések különösebb magyarázatát, másrészt a hírszerzési információk felhasználói jellemzően olyan politikai és katonai vezetők és tanácsadók voltak, aki a széles értelemben vett szakterületüket a kor színvonala szerint szinte mindenki másnál jobban átlátták. A katonai szférát használva példaként: a hírek elsődleges felhasználója a hadvezér volt, aki ismerte a saját és az ellenséges erők helyzetét, a terep sajátosságait, a háború politikai céljait, annak nemzetközi vonatkozásait stb., ezért minden új információt könnyen és egyértelműen képes volt értékelni és a meglévő tudásanyagába elhelyezni. Ez része volt annak a képességének, amit Carl von Clausewitz, Zrínyi Miklós és más szerzők „jó szemmértéknek" (*coup d'œil*) neveztek.

Az 1800-as évek közepétől a helyzet fokozatosan változott, mert az iparosítással járó társadalmi, gazdasági és hadügyi változások miatt a szakterületek száma és mélysége megsokszorozódott, az értesülések mennyisége a döntéshozók számára egyre nehezebben követhetővé vált. A máig tartó folyamat eredményeképpen a hírszerző szervezetek információi önmagukban egyre kevesebbet értek, mert azokat bele kellett volna helyezni a környezetükbe, el kellett volna látni magyarázattal, és mindenekelőtt rá kellett volna mutatni a fontosságukra a döntéshozóknak. Ehhez dedikált szervezetre és speciális eljárásokra van szükség.

A mai értelemben vett elemzés-értékelés a második világháborút követően az Amerikai Egyesült Államokban alakult ki – Sherman Kent munkásságának köszönhetően. A nemzetbiztonsági hírszerző elemzés-értékelés tudományos elméletét magyar nyelven Vida Csaba dolgozta fel. Szerinte „*az elemzés-értékelés egy komplex tevékenységi rendszer. Az elemző-értékelő szervezetek az adatszerzők által összegyűjtött információkat szervezett módon, meghatározott hatáskörökkel, megfelelő tudományos és szakmai ismereteken alapuló eljárások felhasználásával dolgozzák fel. A kapott eredményekből következtetéseket, értékeléseket és előrejelzéseket fogalmaznak meg. Ennek következtében a rendelkezésre álló adatok, információk az elemzés-értékelés során egy – pozitív, értéknövelő – minőségi változáson mennek keresztül. A következtetések, az értékelések és az előrejelzések jelentik a hozzáadott értéket*."

Vida Csaba szerint az elemzés-értékelés a hírszerzési ciklus központi eleme, mert célja és rendeltetése ugyanaz, mint a hírszerzésé, ami nem más, mint megbízható, időbeni, elemzett-értékelt információk biztosítása a felhasználók (döntéshozók) számára a döntések előkészítése érdekében. A hírszerzési ciklus folyamatában „*az elemző-értékelő szervezet fogadja a felhasználók információigényeit, irányítja az adatszerző szervezetek információszerző tevékenységét, feldolgozza az adatszerzők által megszerzett adatokat,*[488] *elemzi-értékeli azokat, valamint a szükséges kérdésekben tájékoztatja a felhasználókat. Tehát az elemző-értékelő munka a hírszerzés keretében folytatott tevékenységi rendszer, amely meghatározott módszerek és elvek alapján mozgatja a hírszerzési ciklust*.” Az elemző-értékelők természetesen nem zárt világban végzik tevékenyégüket, így nemcsak az adatszerzőktől származó információkat használják fel, hanem azokat saját tapasztalataikkal, illetve nyílt információkkal kiegészítik.

A nemzetbiztonsági tevékenység alapja az információ; a nemzetbiztonság valamennyi funkciója információvezérelt. Az adatszerzők által beszerzett információk összességét és a felhasználók információigényét a nemzetbiztonsági rendszer vezetői és az elemző-értékelő szervezetek látják át, ezért ők állnak a hírszerzési ciklus középpontjában.[489]

Az elemző-értékelő munkát hat tevékenységi körre lehet bontani: (1) az információk elemzése-értékelése, vagyis rendelkezésre álló információk komplex vizsgálata; (2) tájékoztatók (jelentések) készítése; (3) elemző-értékelő adattárak vezetése; (4) tájékoztatórendszer működtetése; (5) a hírszerzési ciklus működtetése (vagyis az adatszerzők információszerző tevékenységének irányítása);[490] (6) művelettámogatás.[491]

Elemzés-értékelés az amerikai Hírszerző Közösségben

Az Amerikai Egyesült Államok bő hét évtizede élvezett szuperhatalmi státusa, globális jelenléte és rendkívül szerteágazó nemzeti biztonsági érdekeinek érvényesítése érdekében beszerzett hatalmas és egyre növekvő mennyiségű információ különleges kihívások elé állítja az amerikai Hírszerző Közösség elemző-értékelőit. Ez a tény alighanem hozzájárul ahhoz, hogy az angolszász országokban a

---

[488] Vida Csaba azt is kifejti, hogy az adatfeldolgozás elsősorban az adatszerzők feladata, az elemző-értékelő szervezet az adatfeldolgozás második szakaszát, vagyis a feldolgozott információk rendszerezését végzi el.

[489] Az adatszerzők információszerző tevékenységének irányítása során az elemző-értékelők az adatszerzők egyenrangú partnerei, az elemző-értékelők központi szerepe nem jelent hierarchikus vagy fontossági különbséget.

[490] VIDA Csaba: A hírszerző elemző-értékelő munka alapjai. Felderítő Szemle, XII. évfolyam 3. szám, 2013. december. pp. 90–99.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2013-3.pdf; letöltés: 2022.10.18.

[491] Vida Csaba a nemzetbiztonsági elemző-értékelő művelettámogatás két típusát különbözteti meg: a nemzetbiztonsági (hírszerző és elhárító), valamint a béketámogató/válságkezelő katonai műveletek nemzetbiztonsági elemző-értékelő támogatását.
VIDA Csaba: Művelettámogatás a nemzetbiztonsági elemző-értékelő munkában. Felderítő Szemle, XIV. évfolyam 4. szám, 2015. november. pp. 36–49.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2015-4.pdf; letöltés: 2022.10.18.

hírszerzés fogalmát az információk rendszerezését és értelmezését középpontba helyező „intelligence" kifejezéssel jelölik,[492] szemben az információk (régiesen: hírek) megszerzését előtérbe helyező magyar és német[493] kifejezéssel.

Az amerikai Hírszerző Közösség feladatai és lehetőségei következtében az elemző-értékelő tevékenység valószínűleg az Amerikai Egyesült Államokban a legkiterjedtebb, legkidolgozottabb, a legkutatottabb, ennek következtében pedig szakmailag a legnagyobb hatású. Az amerikai megközelítés vizsgálata ezért annak ellenére is hasznos, hogy világosan látni kell: éppen az Amerikai Egyesült Államok speciális helyzete miatt az amerikai megoldások sehol máshol nem ültethetők át változtatás nélkül a helyi viszonyokra. Különösen a kisebb országok szolgálatainak kell óvatosan közelíteniük az amerikai módszertan átvételéhez, mert az összehasonlíthatatlanul kisebb elemző közösségek számára lehetetlen feladat az amerikai jelentésekre vonatkozó szabályozóknak történő megfelelés. Azt is meg kell jegyezni, hogy bár nem feltétlenül az elemző-értékelők hiányából ugyan, de az amerikai Hírszerző Közösséghez olyan hírszerzési bukások köthetők, amelyek fényében megkérdőjelezhetőnek tűnik az amerikai nemzetbiztonsági rendszer komplexitásának kifizetődősége. Az amerikai hírszerzés képességei és eredményei, valamint az azok mögött húzódó elemző-értékelő szaktudás ugyanakkor szintén elvitathatatlan.

A Nemzeti Hírszerző Tanács

A Hírszerző Közösség elemző-értékelő tevékenységének fő koordináló szerve a Nemzeti Hírszerző Főigazgató irányítása alatt álló, a Közösség vezető elemzőiből (NIO) és civil szakértőkből álló Nemzeti Hírszerző Tanács (NIC[494]). A NIC fő feladata a hírszerző főigazgató támogatása az elnök, a Nemzeti Biztonsági Tanács és a Belbiztonsági Tanács[495] fő hírszerzési tanácsadói funkciójában. A testület elnöke a DNI elemzés-értékelésért felelős helyettese,[496] alelnöke és egyben a napi feladatok végzéséért felelős vezető az ODNI Hírszerző Tanácsáért felelős igazgatója.[497] Az elnök és az alelnök jelöli ki a vezető elemzőket és határozza meg a feladataikat, valamint ők felelősek a Tanács valamennyi jelentésének kiadmányozásáért. A testület elnöke és alelnöke, valamint az illetékes NIO felelősek a nemzeti hírszerző értékelések,[498] valamint a Nemzeti Biztonsági Tanács üléseire és a Kongresszus kérésére készült hírszerző tájékoztatókért. A testület támogatást nyújt a főigazgatónak a nemzeti hírszerzési prioritások éves meghatározásában is. A Hírszerző Tanács információigénnyel élhet a Hírszerző Közösség tagszervezetei felé mind elemzett-értékelt, mind nyers hírszerzési információk vonatkozásában. A testület eredményes feladat-végrehajtása érdekében az IC-tagszervezetek vezetőinek az adott témában

[492] Hasonló értelmű a francia „renseignement" is.
[493] Nachrichtendients, szó szerinti fordításban: „hírszolgálat".
[494] National Intelligence Council.
[495] Homeland Security Council.
[496] Deputy Director of National Intelligence for Analysis.
[497] Assistant Deputy Director of National Intelligence for the National Intelligence Council.
[498] National Intelligence Estimate – NIE: a Hírszerző Közösség álláspontját egy-egy témában tükröző dokumentum. A jelentéseket a NIC állítja össze, de azokat egy másik szakértői csoport, a szintén DNI vezette Nemzeti Hírszerzési Bizottság (National Intelligence Board) hagyja jóvá.

tájékoztatást kell adniuk az információszerzési folyamataik (műveleteik) helyzetéről is, és szükség esetén a Hírszerző Tanács igényei szerint kell alakítaniuk azokat.

A vezető elemzők saját értékeléseket készítenek az elnök napi jelentéséhez[499] és a fő polgári és katonai döntéshozók számára készülő hírszerző feljegyzésekhez,[500] valamint összehangolják az IC stratégiai elemző-értékelő tevékenységét.[501] Az illetékességi területükön szoros kapcsolatot tartanak fenn a döntéshozókkal, az egyetemi és a kutatóintézeti szektorral, valamint saját szakterületükön nemzetközi együttműködést is folytatnak.[502]

Elemzés-értékelés, tájékoztatók készítése

A Hírszerző Közösség szakmai irányítását a DNI, így az elemző-értékelő szakmai sztenderdeket is a főigazgató utasításai[503] rögzítik a teljes IC vonatkozásában.

A hírszerző tájékoztatókkal kapcsolatos alapkövetelményeket a főigazgató elemzői sztenderdeket rögzítő utasítása[504] tartalmazza, amelynek célja azok magas színvonalának biztosítása. A főigazgató öt alapkövetelményt határozott meg.

Objektivitás: az elemzőknek olyan megközelítést, érvelést és módszereket kell alkalmazniuk, amelyek minimálisra csökkentik az előítéleteik[505] és a korábbi elemzői álláspontok befolyását és figyelembe veszik az ezekkel ellentmondó információkat is.

Függetlenség a politikai meggondolásoktól: az elemzői értékelések objektivitását nem befolyásolhatják politikai célok és nézetek vagy a tájékoztatók címzettjeinek (vélt vagy valós) elvárásai.

Időszerűség: a tájékoztatóknak olyan határidővel kell elkészülniük, hogy azok felhasználhatók legyenek a döntéshozatal során („*actionable*”). Az elemző-értékelő szervezetek felelőssége, hogy figyelemmel kövessék a hírszerzési szempontól releváns eseményeket, tisztában legyenek a döntéshozók információigényével és napirendjével, valamint az általános hírszerzési követelményekkel és prioritásokkal.

Összadatforrású szemlélet: a tájékoztatókhoz valamennyi rendelkezésre álló releváns információt fel kell használni. Az elemző-értékelő szervezetek felelőssége az információhiány azonosítása és az együttműködés az adatszerzőkkel a szükséges kiegészítő információk beszerzése érdekében.

---

499 President’s Daily Briefing: az előző napi események és fejlemények rövid összefoglalója.
500 Intelligence Memorandum.
501 Egyebek mellett fenyegetettségértékeléseket készítenek a jelentősebb külföldi befektetések elbírálásához.
502 Intelligence Community Directive 207 – National Intelligence Council. ODNI, 2008.06.09. https://www.dni.gov/files/documents/ICD/ICD_207.pdf; letöltés: 2019.10.29.
503 Intelligence Community Directive – ICD.
504 Intelligence Community Directive 203 – Analytic Standards. ODNI, 2015.01.02. https://www.dni.gov/files/documents/ICD/ICD_203_TA_Analytic_Standards_21_Dec_2022.pdf; letöltés: 2019.10.29.
505 „Bias”.

Megfelelés az elemző-értékelő módszertani sztenderdeknek:

- a tájékoztatókban világosan meg kell adni a felhasznált források, adatok és módszerek minőségét és megbízhatóságát; az információ értékelésének szempontjai azok pontossága, teljessége, megerősítettsége és időszerűsége; a tájékoztatókat lehetőség szerint forrásértékeléssel kell ellátni, aminek alapjául szolgálhat a forrás(ok) befolyásoltságának lehetséges mértéke, hozzáférése, lehetőségei (képzettsége), motivációja és előítéletei; az értékelések kulcsfontosságú pontjainál külön fel kell tüntetni, hogy az elemzők mely források információit mérlegelték a legnagyobb súllyal;

- egyértelműen meg kell jeleníteni és meg kell magyarázni az értékelésekben meglévő bizonytalanságokat, elsősorban az előrejelzések valószínűsége vonatkozásában; az elemzők a felhasznált módszerek (logika), a bizonyítékok (források) mennyisége és minősége, valamint saját témaismeretük függvényében tarthatják megalapozottnak az értékeléseiket és magyarázhatják azok bizonytalanságának mértékét; meg kell továbbá magyarázni a bizonytalan tényezőknek az értékelésekre gyakorolt hatását is (az értékelés milyen mértékben alapul feltételezéseken); szét kell választani az események bekövetkezésének valószínűségét és az értékelés biztosságának/megbízhatóságának mértékét; a főigazgató következetességet vár el a valószínűség fokát tükröző kifejezések használatában, amelyekről táblázatos formában listát mellékelt:

Bekövetkezés valószínűsége	
Százalékosan	**Terminológia**
1–5%	Minimális / Szinte semmi esély (Remote / Almost no chance)
5–20%	Nagyon valószínűtlen (Very unlikely / Highly improbable)
20–45%	Valószínűtlen (Unlikely / Improbable)
45–55%	Megközelítőleg egyenlő esély (Roughly even chance)
55–80%	Valószínű (Likely / Probable)
80–95%	Nagyon valószínű (Very likely / Highly probable)
95–99%	Szinte biztos (Almost certainly)

1. táblázat. Az előrejelzések valószínűségének terminológiája az amerikai Hírszerző Közösségben[506]

[506] Intelligence Community Directive 203 – Analytic Standards. ODNI, 2015.01.02. https://www.dni.gov/files/documents/ICD/ICD_203_TA_Analytic_Standards_21_Dec_2022.pdf; letöltés: 2019.10.29.

- meg kell különböztetni az (elemzett) alapinformációkat, az azokat keretbe helyező, a hiányzó információkat kitöltő és támogató feltevéseket (hipotéziseket), valamint az értékelést; meg kell jeleníteni, hogy a feltevések helyessége vagy egyes jövőbeni események bekövetkezése (indikátorok) mennyiben befolyásolhatja az értékelést;

- az események vagy jelenségek magyarázata és az előrejelzések megfogalmazása során be kell mutatni a lehetséges alternatív hipotéziseket; ez különösen fontos abban az esetben, ha az értékelés bizonytalan vagy jelentősen összetett tényezőkön alapszik, vagy ha alacsony valószínűségű események számottevő, súlyos következményekkel járhatnak; nem szabad elkerülni a nehezen megállapítható valószínűségű értékelések megfogalmazását sem;

- a jelentéseknek a felhasználók igényeinek megfelelő információkat és azok lehetséges következményeit kell tartalmazniuk; a nyers információhoz hozzáadott legfontosabb elemző-értékelő értékek az előrejelzés, a kontextusba helyezés, a fenyegetések, valamint a lehetőségek kiemelése;

- a tájékoztatók legelején közölni kell a világos, fő üzenetet; amennyiben az értékelésben több alternatíva szerepel, az üzenetnek ezek közös elemeit kell megjelenítenie; az értékeléseket a releváns hírszerzési információkkal és következetes érveléssel, félreérthetetlen kifejezésekkel és megfogalmazással kell alátámasztani;

- röviden, de világosan be kell mutatni, hogy az értékelés mennyiben és miért (új információk vagy módszerek felhasználása stb.) felel meg vagy tér el a korábbi tájékoztatókban jelentettektől; közölni kell, ha az adott témában első alkalommal készült jelentés; a periodikus és a napi jelentésekben csak a változásokat kell megjeleníteni az értékelésekben; szintén fel kell hívni a felhasználók figyelmét arra, ha a Hírszerző Közösség egyes tagszervezeteinek értékelése jelentősen különbözik az adott tárgyban;

- a tájékoztatókban szükség és lehetőség szerint vizuálisan – táblázatok, grafikonok, folyamatábrák, képek stb. formájában – is meg kell jeleníteni a lényegi vagy az értékelés alátámasztására szolgáló információkat; ez különösen fontos abban az esetben, ha az értékelés alapjául időbeni vagy térbeni kapcsolatok elemzése szolgál.

A szolgálatok vezetőinek felelőssége, hogy a szervezeteiktől kikerülő tájékoztatók – a szervezet sajátosságainak figyelembevételével – megfeleljenek e sztenderdeknek, feladatuk továbbá a követelmények rendszeres felülvizsgálata és javaslattétel azok megváltoztatására, fejlesztésére. A szolgálatoknál ebből a célból dedikált hivatalt vagy pozíciót hoztak létre. A tájékoztatók elemző sztenderdeknek történő megfelelését a főigazgató integrációért felelős helyettese és az ODNI elemző ombudsmanja[507] felügyeli.

[507] ODNI Analytics Ombuds (a gendersemlegesség jegyében nem használják a férfiakra utaló „ombudsman” kifejezést).

A tájékoztatókban jelentett információk forrásait – a tudományos életben megszokotthoz hasonló, lábjegyzetes formában – a hivatkozások megadásával, illetve a forrás értékelésével[508] kell megjeleníteni. A jelentésben felhasznált források értékeléséről (megbízhatóságuk, információik felhasználása az értékelésben stb.) rövid összefoglaló is készíthető.[509] A tájékoztatók végén közölt hivatkozásokat minden alkalommal meg kell adni, amikor az elemző egy forrásra hivatkozik, vagy amikor az elemzés-értékelés bármely hozzáadott értéke (megjegyzés, feltételezés/hipotézis vagy értékelés) egy adott forrás információin alapszik. A hivatkozásokban az adott információt eredetileg közlő (elsődleges) forrást (tanulmányt, korábbi tájékoztatót stb.) kell megadni a közlés dátumával és az oldalszámokkal. A hivatkozások a forrásdokumentumok minősítését hordozzák. A szerzőt vagy adatgazdát (IC-tagszervezet, ország stb.) szintén meg kell adni. A minősített forrású információk leírásánál minimális követelmény, hogy a kellő betekintési jogosultsággal és hozzáféréssel rendelkező személyek képesek legyenek az eredeti dokumentumot előkeresni vagy azt meg tudják igényelni. A hivatkozások megadása a szanitizált jelentések esetében is kötelező, kivéve a nyilvánosságra hozott példány esetében. A kiegészítő információk megadása – a hivatkozás szabályai szerint szerkesztett – mellékelt forrásjegyzékkel történhet.[510] Azonnali és sürgős jelentések esetén a hivatkozások megadása elhagyható, de 30 napon belül pótolni kell.[511]

Tevékenységük hatékonyságának fokozása érdekében a Hírszerző Közösség elemző-értékelő elemei ismereteik bővítése és más szemléletmódok megismerése érdekében nyíltan együttműködnek az IC-n kívüli hazai és külföldi szervezetekkel és egyénekkel (külső szakértőkkel[512]).[513] A külső szakértőkkel megvalósított együttműködést élesen megkülönböztetik a HUMINT-tól és az OSINT-tól, valamint a külföldi nemzetbiztonsági szolgálatokkal fenntartott hivatalos együttműködéstől. A külsős szakértők nem vonhatók be HUMINT- vagy technikai információszerzési feladatok ellátásába, de a megfelelő betekintési jogosultságok birtokában számukra minősített információk átadhatók és anyagi ellenszolgáltatás is biztosítható. Az elemző-értékelők szakértői együttműködését a szolgálatok vezetése menedzseli és támogatja. Az együttműködés alapfeltétele a kapcsolatfelvételi szándék jelzése az IC többi tagszervezete felé, megelőzve a duplikációt és a többi szervezet tevékenységének akadályozását. Az együttműködésben részt vevők biztonsága és az információvédelem érdekében figyelembe kell venni az elhárítási szempontokat is (kockázatmenedzsment). Ennek részeként a végrehajtásba bevont vezetőket és elemzőket megfelelő felkészítésben kell részesíteni. A megszerzett információkat meg kell osztani a Hírszerző Közösség egészével.[514]

---

508 Source descriptor.
509 Source summary statement.
510 Appended reference citation.
511 Intelligence Community Directive 206 – Sourcing Requirements for Disseminated Analytic Products. ODNI, 2015.01.22. https://www.dni.gov/files/documents/ICD/ICD 206.pdf; letöltés: 2019.10.29.
512 Outside Experts.
513 Analytic Outreach.
514 Intelligence Community Directive 205 – Analytic Outreach. ODNI, 2013.08.28. https://www.dni.gov/files/documents/ICD/ICD 205 - Analytic Outreach.pdf; letöltés: 2019.10.29.

Tájékoztatórendszer működtetése, adattárak vezetése

A Hírszerző Közösség munkatársainak (tehát nem kizárólag az elemző-értékelőknek) tisztában kell lenniük azzal, hogy kik a felhasználóik, milyen információkra van szükségük és milyen határidővel, illetve hogy milyen betekintési jogosultsággal rendelkeznek. Az elemzőknek a tájékoztatók készítése során el kell dönteniük, hogy a jelentés egy adott felhasználó vagy a felhasználók szélesebb köre számára készül, és ez alapján kell megválasztaniuk a felhasznált forrásokat és a tájékoztató minősítési szintjét. A tájékoztatókat úgy kell megszerkeszteni, hogy azok részei vagy egésze a lehető legkönnyebben megoszthatók legyenek a Hírszerző Közösségen kívül is (a jogszabályi követelmények és vezetői döntés megléte esetén minisztériumok és kormányügynökségek, tagállamok hivatalai és helyi szervek, továbbá külföldi országok, valamint a magánszféra és a közvélemény részére). A tájékoztatók információinak pontos forráshivatkozása a megoszthatósági döntések felgyorsítására is szolgál. A jelentések elosztóinak szélesítése érdekében a tájékoztatókból különféle verziók, szanitizált szöveg és összefoglaló is készíthető, de a tájékoztatók különböző minősítésű változatainak tartalma nem mondhat ellent egymásnak.[515] A megoszthatóság növelése érdekében a tájékoztatók összefoglalóját (kivonatát)[516] a lehető legalacsonyabb minősítési szinttel és a lehető legkevesebb kezelési megkötéssel kell ellátni. Ennek elsődleges módja a forrásokra vonatkozó, a műveleti és egyéb szenzitív (pl. a technikai adatszerzőktől származó) információk elhagyása. Az összefoglalók minél szélesebb körű terjesztését az is indokolja, hogy azok a hírszerző előrejelző rendszernek[517] is fontos eszközei.[518]

A tájékoztatórendszer működtetésének alapelve a tájékoztatók felhasználhatóságának maximalizálása. A Hírszerző Közösség tagszervezeteinek a nyers és az elemzett-értékelt információikat egyaránt a nemzeti (adat)vagyon részeként kell kezelniük. Az információk megosztásával nagyobb eséllyel azonosíthatók az Amerikai Egyesült Államok elleni fenyegetések és javulhat az azokkal szembeni fellépés, valamint hatékonyabbá tehető a politikai és a katonai felső vezetés tájékoztatása. Az információ megosztásának két alapelve, hogy az IC tagszervezeteinek kötelessége az információit a jogosultak számára elérhetővé tenni,[519] az arra jogosult szervezetek pedig felelősek azért, hogy a számukra releváns információt felleljék,[520] illetve amennyiben a betekintéshez külön engedélyre van

[515] Intelligence Community Directive 208 – Maximising the Utility of Analytic Products. ODNI, 2017.01.09.
https://www.dni.gov/files/documents/ICD/ICD 208 - Maximizing the Utility of Analytic Products (09 Jan 2017).pdf; letöltés: 2019.10.29.

[516] Tearline. A kifejezés a tájékoztatók nyomtatott verziójának perforáltságára vonatkozik, amelynek segítségével a tájékoztató magasabb minősítésű része (*above the tearline*) könnyen leválasztható az alacsonyabb minősítésű részről, javítva az utóbbi megoszthatóságát.

[517] National Foreign Intelligence Warning System.

[518] Intelligence Community Directive 209 – Tearline Production and Dissemination. ODNI, 2012.09.06.
https://www.dni.gov/files/documents/ICD/ICD 209 Tearline Production and Dissemination.pdf; letöltés: 2019.10.29.

[519] Responsibility to provide.

[520] Responsibility to discover.

szükség, akkor azt megigényeljék.[521] A megosztás automatizált kereséseket[522] is lehetővé tevő adatbázisokon keresztül valósul meg. Az IC tagszervezeteinek vezetői külön személyeket bíznak meg az információk automatizáltan kereshetővé tételére és a megosztási igények elbírálására, valamint az adatbázisok monitorozására és az igények benyújtására, de a főigazgató célja olyan adatbázisok megteremtése, amelyek segítségével a jogosult nemzetbiztonsági munkatársak saját maguk is képesek az információ fellelésére.[523]

```
<teiHeader>
 <fileDesc>
  <titleStmt>
   <title>Shakespeare: the first folio (1623) in electronic form</title>
   <author>Shakespeare, William (1564–1616)</author>
   <respStmt>
    <resp>Originally prepared by</resp>
    <name>Trevor Howard-Hill</name>
   </respStmt>
   <respStmt>
    <resp>Revised and edited by</resp>
    <name>Christine Avern-Carr</name>
   </respStmt>
  </titleStmt>
  <publicationStmt>
   <distributor>Oxford Text Archive</distributor>
   <address>
    <addrLine>13 Banbury Road, Oxford OX2 6NN, UK</addrLine>
   </address>
   <idno type="OTA">119</idno>
   <availability>
    <p>Freely available on a non-commercial basis.</p>
   </availability>
   <date when="1968">1968</date>
  </publicationStmt>
  <sourceDesc>
   <bibl>The first folio of Shakespeare, prepared by Charlton Hinman (The Norton Facsimile,
       1968)</bibl>
  </sourceDesc>
 </fileDesc>
```

14. ábra. Példa automatizáltan kereshető szövegformátumra

Részlet a Text Encoding Initiative (TEI) amerikai tudományos életben alkalmazott formátumának egy példaoldaláról. A szöveg különböző, előre meghatározott rendszer (taxonómia) szerint szervezett metaadatait (cím, szerző, dátum, elosztó stb.) és a szövegben előforduló egyes információkat (nevek, dátumok stb.) kúpos zárójelben jelölt kategóriák jelzik az adatbáziskezelő rendszer keresőprogramja számára.[524]

[521] Responsibility to request. A közös adatbázisokban egyes tájékoztatóknak és más információknak csak a címe, a leírása és egyes metaadatai szerepelnek.

[522] Machine readability.

[523] Intelligence Community Directive 501 – Discovery and Dissemination or Retrieval of Information within the Intelligence Community. ODNI, 2009.01.21. www.dni.gov/files/documents/ICD/ICD_501.pdf; letöltés: 2019.10.29.

[524] A Text Encoding Initiative honlapja. https://tei-c.org; letöltés: 2020.04.27.

A Hírszerző Közösség a hatékonysága és a hasznossága növelése érdekében arra törekszik, hogy ne „fekete dobozként", hanem a felhasználók partnereként, számukra – a konspirációs szabályok megtartásával – a lehető legátláthatóbb módon tevékenykedjen. Ennek feltétele és egyben előnye a felhasználók és igényeik mélyebb ismerete, pozitív hozadéka a politikai, gazdasági és katonai döntés-előkészítési folyamatokban történő érdemi részvétel. Az együttműködés további előnye, hogy a felhasználók tisztában vannak a nemzetbiztonsági rendszer lehetőségeivel, ezáltal pontosabb és testre szabottabb információigényeket fogalmazhatnak meg. Az átláthatóság követelménye a hazai (és a nemzetközi) közvélemény felé is fennáll, itt a fő cél a szolgálatok tevékenységének népszerűsítése, lakossági támogatottságuk és hitelességük növelése. Mindennek ára, hogy nehezebb elkendőzni a hírszerzés hiányosságait és hibáit, emellett csorbulhat a „mindentudás mítosza" is.

A nemzetbiztonsági tájékoztatórendszerek örök dilemmája, hogy miként lehetséges megfelelni a pontosság, a teljesség, az időszerűség és a megbízhatóság egymásnak feszülő követelményeinek. A felhasználók és igényeik közelebbi megismerésével és a hírszerző tájékoztatókban esetlegesen meglévő bizonytalansági tényezők megjelenítésével e dilemmák egy része feloldható.

Az amerikai tájékoztatórendszert áthatja, hogy az nem kizárólag a felső vezetés stratégiai döntés-előkészítését támogatja, hanem a művelettámogatást is szolgálja. Ennek egyik fő eszköze, hogy az elemző-értékelő adattárak információinak elemeit a tájékoztatórendszer részévé tették, így a hozzáféréssel rendelkező – a készítők számára sokszor ismeretlen – szervezetek maguk is kinyerhetik vagy megigényelhetik a számukra szükséges információt. Ezt a megoldást nyilvánvalóan az amerikai államigazgatás rendkívüli komplexitása tette szükségessé.

E komplexitás másik velejárója, hogy az információáramlás elvárt mértékének biztosítása a hagyományos, manuális módszerekkel ma már nem kivitelezhető. A fejezetben megjelenített, a nemzetbiztonsági együttműködést és a tájékoztatást szolgáló automatizált rendszerek pusztán elvi és módszertani alapvetésként, kiindulópontul szolgálnak a tényleges megoldást jelentő, jelenleg még fejlesztés alatt álló vagy a rendszeresítés különböző szakaszaiban lévő, a mesterséges intelligenciára és a nagy adatra építő, felhasználóbarátabb információ- és folyamatmenedzsment, valamint elemző-értékelő fúziós rendszerek számára.

A Hírszerző Közösségben alkalmazott, automatizált kereséseket is lehetővé tevő adatbázisok működtetése a jelenleg alkalmazott technológiával rendkívül magas emberierőforrás-igénnyel bír, ezért a kisebb létszámú szolgálatok számára nem realitás a bevezetésük. E téren is rendkívül ígéretes megoldásokat nyújt ugyanakkor a mesterséges intelligencia alkalmazása.

A MESTERSÉGES IINTELLIGENCIA ALKALMAZÁSI LEHETŐSÉGEI A NEMZETBIZTONSÁGI HÍRSZERZÉS ÖNÁLLÓ ÁGAIBAN

A hírszerzési ágak szenzitivitása értelemszerűen különböző. A nyílt információkon alapuló OSINT/SOCMINT, illetve az IMINT és a GEOINT területein[525] érhető el a legtöbb információ a technológia nyújtotta lehetőségekről. A HUMINT és a SIGINT szakterületekkel kapcsolatban nyíltan kutatható információ már csak a képességek egy részét mutatja be. A CYBINT vonatkozásában kizárólag a kibervédelmi szegmens lehetőségeit ismertetik, míg a MASINT (mint a magánszféra szempontjából a legkevesebb lehetőséget kínáló hírszerzési ág) szinte egyáltalán nem jelenik meg a termékpalettán. A bemutatott termékek és szolgáltatások összességében így is széles perspektívát mutatnak azokról a lehetőségekről, amelyeket a mesterséges intelligencia nyújthat a hírszerzés számára.

A mesterségesintelligencia-alapú célszoftverek felhasználási lehetőségei a nemzetbiztonsági hírszerzésben – az NGA megközelítése a mesterséges intelligencia szerepéről

Susan Kalweit elemző-értékelő igazgató *Műveleti tempó: a gyors és megbízható elemzés biztosításának egyenlete* című előadásában[526] bemutatta a Nemzeti Térinformatikai Ügynökség (NGA) megközelítését a mesterséges intelligencia (MI) jelentette lehetőségek elemző-értékelő szempontú kiaknázására. Elmondta, hogy a szervezet tevékenységének alapját kiterjedt adatbázisa adja. Az adatbázisban 12 millió földrajzi név, 125 millió gravitációs mérési eredmény, négymilliárd légiforgalmi adatelem, 118 millió négyzetkilométernyi pontos sztereografikus[527] képfelvétel, valamint 70 millió hidrográfiai tereptárgyra vonatkozó adat található. Az NGA termékei között repülési, szárazföldi, tengeri és tenger alatti navigációs térképek, repülési információs jelentések, tengeri határok térképei és tengerészeti navigációs veszélyfigyelmeztetések szerepelnek. Az NGA emellett saját és kereskedelmi

[525] A klasszikus értelemben vett IMINT a haderő és a nemzetbiztonsági rendszer műholdfelvételeit, valamint a felderítő-repülőgépek felvételeit dolgozta fel, ezért módszerei és termékei is magas szinten minősítettek. A kereskedelmi IMINT-szolgáltatók saját vagy más vállalatok műholdjainak felvételei alapján dolgoznak, ezért egyedül a módszertanuk egyes vonatkozásait rejtik a nyilvánosság elől. A GEOINT-termékek védettségét elsősorban a felhasználáshoz felhasznált adatbázisok minősítése határozza meg. A kereskedelmi szolgáltatók elsősorban nyíltan hozzáférhető adatbázisokkal dolgoznak.

[526] KALWEIT, Susan: Mission Intensity: Thriving in the Smart Machine Age - The Making of the Equation to Assure Fast and Reliable Analysis. A National Geospatial Intelligence Agency elemző-értékelő igazgatójának előadása az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.29.

[527] A sztereográfiai vetület a gömb síkként történő ábrázolásának módja.
Sztereografikus vetítés - Stereographic projection.
https://hu.abcdef.wiki/wiki/Stereographic_projection; letöltés: 2021.03.14.

műholdfelvételek elemzés-értékelésével, valamint földrajzi, politikai földrajzi, humán földrajzi és katonai térképek készítésével is foglalkozik. Az NGA 90 külföldi partnerrel kötött képfelvételek és térképek megosztására vonatkozó megállapodást.

Az NGA négy technológiai hullámot különböztet meg a geoinformációs/ térinformatikai hírszerzés (GEOINT) fejlődésében:

- az 1940-es évek legvégétől alakították ki a nagy magasságból készült analóg (manuálisan előhívott) képfelvételek elkészítésének és elemzés-értékelésének módszertanát, ilyen képfelvételeket egészen 2005-ig készítettek;
- az 1970-es évek végétől kezdték meg a térképészet, a georeferált[528] digitális információ és a képelemzés integrálását;
- a 2000-es évek elejétől kezdődött a térinformatikai nagy adat felhasználása előrejelző elemző-értékelő modellekhez;
- 2008-tól alkalmaznak mesterséges intelligenciát az elemzés-értékelésben.

Az NGA-nál az MI alkalmazásának elterjedése 2017-ben gyorsult fel annyira, hogy a szervezet végleg maga mögött hagyta a hidegháborúban alkalmazott módszereket. Az MI-t az egyszerűbb munkafolyamatok automatizálásához, illetve a komplex feladatoknál az emberi tevékenység kiegészítéséhez alkalmazzák. A folyamat eredményeképpen a munkatársaknak fel kellett hagyniuk az évtizedes rutinokkal, új gondolkodásmódot kellett elsajátítaniuk. A gépies munkavégzés helyett előtérbe helyeződött a kritikus, kreatív, innovatív gondolkodásmód. A feladatok végrehajtása mára elképzelhetetlenné vált a technológia alkalmazása nélkül, ezért ki kellett alakítani egy új módszertant az ember–gép együttműködés optimalizálására. Az együttműködés kétirányú folyamat, mert az MI-alapú szoftverek támogatják az emberi munkát, az emberi szakértők pedig saját meglátásaikkal és döntéseikkel folyamatosan, direkt módon tanítják az algoritmusokat (direkt gépi tanulás).

Új gondolkodásmódot kellett meghonosítani mind a technológia alkalmazásában, mind a humánmunkaerő-menedzsmentben. Az új munkakörnyezet alapja az adatba mint az NGA fő erőforrásába és az adat feldolgozásához felhasznált szoftverekbe vetett bizalom kialakítása. Ennek érdekében adatmendzsmenttel foglalkozó szakértői csoportokat alkalmaznak, akiknek feladatai közé tartozik az adat hitelesítése is. Ezek a csoportok végzik a mélyhamisított tartalmak szűrését is.

A humán munkaerő kialakításánál inkluzív, a szaktudás széles körét magában foglaló szemléletet követnek. Az elemző-értékelő munkához IMINT- és GEOINT-szakértőkből, adattudósokból, adatmenedzserekből, adatgondozókból[529] és adatgyűjtő szakemberekből álló multidiszciplináris csoportokat hoznak létre. A területi szakértők tekintetében a fókuszt Kínára helyezték.

[528] A georeferálás során a digitálisan készített térkép pixeleihez földrajzi koordinátákat rendelnek.
[529] Data steward.

A fejlesztések során az NGA teljes transzformációja helyett a fokozatos, a vezetés által meghatározott prioritások mentén végrehajtott fejlesztés elvét választották.

A nagy adat alkalmazása növeli az informatikai kockázatokat, ezért az NGA többszintes kibervédelmi rendszert üzemeltet. A védelem része az elemző-értékelőktől elvárt kritikus szemléletmód is.

Az amerikai szolgálatok széleskörűen alkalmazzák a mesterséges intelligencián alapuló szoftverrendszereket, és mind a nyílt, mind a minősített rendszereiken nagy adattal dolgoznak. Számukra a fő kihívást az új technológiához illő eljárások, szervezeti felépítés kialakítása és az emberi munkaerő képzése, összességében a nemzetbiztonsági szervezeti kultúra újraszabása jelenti.

OSINT/PAI

East View Information Services

A minneapolisi East View Information Services az amerikai védelmi szféra nyílt forrású tartalomszolgáltatója. Egyik fő termékük a legnagyobb kínai akadémiai adatbázis, a Kínai Nemzeti Tudás Infrastruktúra (CNKI[530]) licencelt változata. A CNKI-n évente több mint 5000 kutatás-fejlesztési és innovációs tudományos folyóiratban 1,1 millió kutató mintegy hatmillió tudományos publikációt tesz közzé. Az adatbázis cikkei pdf- és xml-formátumban érhetők el, az adatbázisban a keresés több mint 100 kategóriában (kulcsszavak, absztrakt, teljes szöveg, kutatóhely, pénzügyi támogató, szerzők, források) lehetséges. A CNKI egyik fő előnye a cikkek, a kutatók és az intézmények kontextusának, egymás közötti kapcsolatának a feltérképezhetőségében áll. Az adatbázis használatával az East View munkatársai is készítenek elemzéseket a kínai védelmi jellegű kutatásokról. Az elemzésekben a kiemelt szektoroknak a hajógyártás, a rakétatechnológia, a műholdas kommunikáció, a kibervédelem és az egészségügy számítanak. A megjelent tudományos cikkek alapján elemzéseket készítenek a kínai Népi Felszabadító Hadsereg (PLA[531]) szervezeti felépítéséről, tartalékos és félkatonai erőiről, katonai stratégiájáról és doktrínájáról, valamint a közrend fenntartásában betöltött szerepéről is. Elemzik továbbá a PLA jelentette új fenyegetéseket, az alkalmazott új technológiákat és a fejlesztések trendjeit.

Az East View a CNKI mellett más nyílt adatbázisokat is szolgáltat az amerikai védelmi szféra részére. A vállalat globális sajtóarchívumában több mint 80 ország 30 nyelvén az 1700-as évek óta íródott több mint 30 millió oldalnyi kereshető jogvédett sajtóanyag érhető el. Az East View a kínai mellett az orosz nyelvű publikációk terén is fontos szereplőként pozicionálja magát, mindemellett kiterjedt GEOINT-adatbázissal is rendelkezik.[532]

---

[530] China National Knowledge Infrastructure.

[531] People's Liberation Army – PLA.

[532] PITTMAN, Travis: Az East View tartalomszolgáltató vállalat bemutatása. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.30.

A Georgetown Egyetem CSET központja

A washingtoni Georgetown Egyetem kialakulóban lévő technológiákkal és azok biztonsági vonatkozásaival foglalkozó kutatóközpontjának (CSET[533]) adattudományi igazgatója előadásában[534] bemutatta a kutatóhelynek a kínai védelmi célú fejlesztések feltérképezésére irányuló tevékenységét.

A CSET összesen 17 tartalomszolgáltatóval, köztük az East View-val áll szerződésben. A szolgáltatók összesen 28 terabájt szöveges adatot biztosítanak, ami mintegy 14 milliárd oldalnak felel meg. A szövegkorpusz többségét 215 millió, elsősorban angol, kínai és orosz nyelvű tudományos publikáció; több mint ötmillió szervezeti ábra; vállalati és kormányzati pénzügyi tranzakciókra vonatkozó adatok; 250 millió álláshirdetés; 450 millió szakmai életrajz; illetve sajtóadatbázisok és üzleti hírszerzési információk teszik ki. A CSET az adatbázisokból a szervezeti adatok, a hivatkozások, a szóhasználat stb. alapján hálózati kapcsolatokat készít, amelyek alapján jelenleg 678, összesen több mint 207 milliárd sornyi relációs adatot tartalmazó adattáblát üzemeltet. A jól strukturált, megbízható és kifinomult módszerekkel elemzett nagy adat alapján jól megalapozott, mély elemzéseket és értékeléseket képesek készíteni szervezetekről és személyekről. Az évtizedekre visszanyúló adattömeg trendelemzést is lehetővé tesz. Az adattárház karbantartását dedikált szakemberek végzik gépi tanuláson alapuló algoritmusok segítségével. A több ezer virtuális processzor volumenű számítástechnikai kapacitást a Google számítási felhőszolgáltatása[535] biztosítja.

A kutatóhely elsősorban a kínai technológiai fejlesztésekkel foglalkozik, az előadó ebben a témakörben mutatta be a CSET három legfrissebb kutatásának eredményeit. Mindhárom kutatás részben vagy egészben az East View tartalomszolgáltató CNKI adatbázisának feldolgozásán alapult.

Az első kutatás során a CNKI adatbázisából kiszűrték azokat a tudományos publikációkat, amelyek az MI hadászati stabilitásra gyakorolt hatásait vizsgálták. A keresés során 58 ilyen, 2016 és 2020 között megjelent cikket találtak. Az írások elemzése alapján a személyzet nélküli repülőgépek (UAV[536]) és tengeralattjárók (UUV[537]), az intelligens lövedékek, a műholdak, az elektronikus hadviselési eszközök,[538] a hírszerző, megfigyelő- és felderítőeszközök, illetve az automatizált kibervédelem tekinthetők kulcstechnológiáknak. Az írások közül 40 foglalkozott a haderő csapásmérő képességének fokozásával, 28 az MI alkalmazási lehetőségeivel

533 Center for Security and Emerging Technology.
534 MURDICK, Dewey: CSET's Data Science Efforts and Open Source Analysis on China's Emerging Technologies. A CSET adattudományi igazgatójának előadása az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.30.
535 Google Cloud Computing.
536 Unmanned Aerial Vehicle.
537 Unmanned Underwater Vehicle.
538 Az MI-alapú elektronikai hadviselés angol szakirodalmi elnevezése: Cognitive Electronic Warfare.

az ellenséges hadászati erők felderítésére, 11 az erőalkalmazás költségvonzatának csökkentésével, hét pedig a vezetés-irányítási rendszer sebezhetőségének mérséklésével. Az MI-eszközök elterjedése ugyanakkor kihívásokat is jelenthet a korszerű haderők számára. Az 58 kínai publikáció közül kilenc állítja, hogy növekedhet a technikai meghibásodások valószínűsége, nyolc szerint növekedhet a vezetés-irányítási rendszerek sérülékenysége, ugyancsak nyolc cikk foglalkozik a légvédelem hatékonyságának csökkenésével, hat a támadásokra rendelkezésre álló válaszidő csökkenésével, négy pedig a csapásmérési képesség csökkenésével. A publikációkból a CSET arra a következtetésre jutott, hogy a kínai katonai gondolkodók túlbecsülik az amerikai haderő – nyílt források alapján becsült[539] – MI-képességeit.[540]

A CSET a második kutatásban a kínai víruskutatásokat elemezte. A kutatás eredményeképpen megállapították, hogy a témakörben a kínai nyelvű publikációk száma jelentősen meghaladja az angol nyelven írottakét. A kínai kórházak, kutatóintézetek, a vakcinák gyártói, illetve a haderő kutatói a Nyugaton megszokottnál kiterjedtebb együttműködést folytatnak. A kutatóknak széles körű hozzáférésük van a tesztelésekhez szükséges állatokhoz is.

A harmadik kutatás a kínai biztonsági erők 2010 és 2019 között felmerült kutatási igényeit elemezte. A vizsgált szervezetek a haderő (PLA), a Közbiztonsági Minisztérium[541] és a Belbiztonsági Rendőrség[542] voltak.[543] A CSET a globális tudományos adatbázisok alapján 121 ezerre becsüli a világ tudományos klasztereinek[544] számát, amelyek a vizsgált időszakban összesen mintegy 105 millió publikációt tettek közzé. A klaszterek közül 14 500 köthető a kínai biztonsági erőkhöz. E kutatói közösségek összesen 28 387 publikációt készítettek el az MI témakörében, amelyek közül 26 538-at a PLA, 1452-t a Közbiztonsági Minisztérium, 757-et pedig a Belbiztonsági Rendőrség klaszterei tettek közzé. A publikációk a mesterséges intelligencia vegyes felhasználási lehetőségein belül útvonaltervezéssel, célpontkiválasztással, több célpont egyidejű követésével,[545] behatolásérzékeléssel,[546] szteganográfiával,[547] adatelemzéssel, egészségüggyel,

[539] A CSET akadémiai szervezetként nem fér hozzá minősített információkhoz.

[540] A kutatási összefoglaló online is hozzáférhető:
FEDASIUK, Ryan: Chinese Perspectives on AI and Future Military Capabilities. CSET, August 2020. https://cset.georgetown.edu/research/chinese-perspectives-on-ai-and-future-military-capabilities/; letöltés: 2021.03.16.

[541] Ministry of Public Security – MPS.

[542] People's Armed Police – PAP.

[543] A CNKI adatbázisában minimális számú publikáció köthető az Állambiztonsági Minisztériumhoz (Ministry of State Security – MSS), ezért ezt a szervezetet nem vizsgálták.

[544] Klaszter alatt az egyazon tudományos problémával foglalkozó, egymás kutatásaira építő tudományos közösséget értik.

[545] Dewey Murdick kihangsúlyozta, hogy a PLA klaszterei 348 publikációt jelentettek meg a ballisztikus célpontok megkülönböztetésével és a ballisztikus lövedékek útvonaltervezésével kapcsolatban.

[546] Intrusion detection.

[547] A kriptográfiához hasonló titkosítási rendszerek, amelyeknél az üzenet létét is álcázzák (pl. képekbe rejtik az üzenetet). Az ilyen kutatások többségét a Belbiztonsági Rendőrség finanszírozta, amelynek vélhető célja a Kínából küldött rejtett üzenetek felfedése volt.

illetve a mérnöki és az anyagtudományokkal voltak kapcsolatosak. A számítógépes látás fő alkalmazási lehetőségei közül a célpontazonosítással és -követéssel, a hiperspektrális képszenzorokkal,[548] az arc- és ujjlenyomat felismerésével, a testtartás elemzésével, a járművek felismerésével, valamint a hamisítványok kiszűrésével foglalkoztak. A természetes nyelvek feldolgozása[549] területén a kutatások a közösségi média felderítésére, az online hangulatelemzésre[550] és a szövegek kategorizálására összpontosítottak. A robotika területén a vezérlőrendszerek, a kezelő nélküli járművek, az exoszkeletonok (mesterséges külső vázak) és a humaoid robotok jelentették a kutatások fő irányait.

Az amerikai IC-nek a polgári kutatóhelyekkel és a tartalomszolgáltatókkal megvalósuló együttműködésének kiterjedtsége és az ebben rejlő lehetőségek azt jelzik, hogy lehetetlen a szükséges szaktudás és az adatbázisok felhalmozása a szolgálatok falain belül, ezért a nemzetbiztonsági szféra kénytelen nyitni a lehetséges partnerek felé. Ennek az Amerikai Egyesült Államokban jelentős hagyományai vannak, amelyekre építve a korszerű informatikai megoldások birtokában új fejezetet nyithattak. Nem kétséges, hogy a kiterjedt együttműködés számos és súlyos biztonságvédelmi, elhárítási kockázatot rejt magában, de az amerikai megközelítés egyértelműen a kockázatok csökkentését és menedzselését, nem elkerülésüket pártolja.[551] Emögött az amerikai üzleti szemlélet áll, amelyben az elmaradt nyereség is veszteségnek számít, és amelyben olyan nyereségre törekszenek, amely minden, a műveleti tempóból adódó potenciális veszteséget bőségesen ellensúlyoz. Természetesen nem elhanyagolható tényező a kihívás nagysága sem, hiszen a kínai tudományos szakirodalom önmagában is nagy adatot generál, és annak feldolgozása elképzelhetetlen a hagyományos módszereket alkalmazó, egymástól elszigetelt szolgálatok számára.

---

[548] A több mint húsz diszkrét spektrális sávval rendelkező szenzorokat hiperspektrális képszenzorokként is említik.
A Tanács 6/2012/EU álláspontja első olvasatban a kettős felhasználású termékek kivitelére, transzferjére, brókertevékenységére és tranzitjára vonatkozó közösségi ellenőrzési rendszer kialakításáról szóló 428/2009/EK tanácsi rendelet módosításáról. 2012.02.21. p. 17.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:107E:0001:0273:HU:PDF; letöltés: 2021.03.14.

[549] Natural Language Processing – NLP.

[550] Akár a lakosság privát elektronikus levelezésében is.

[551] Emellett érvelt az amerikai nemzeti MI-stratégia bemutatása során Katharina McFarland volt védelmi beszerzésekért felelős államtitkár, a Nemzeti Biztonsági Bizottság a Mesterséges Intelligenciáért (National Commission on Artificial Intelligence) tagja a 2021. március 10-i előadásán.
MCFARLAND, Katharina: Mission Focused: The Mission to Integrate Artificial Intelligence into the Military's Future Battle Rhythm. The Cipher Brief, 2021.03.10.
https://www.thecipherbrief.com/column_article/the-mission-to-integrate-artificial-intelligence-into-the-militarys-future-battle-rhythm; letöltés: 2021.12.22.

Airbus Joint ISR (Európa)

Az Airbus OSINT-platformja az internet keresőmotorok által elérhető területéről (*surface web*), a *deep web*ről és a *dark web*ről is képes nagy mennyiségű, strukturálatlan információ automatikus, felhőalapú gyűjtésére, kinyerésére és elemzés-értékelésére. Felhasználható mind az aszimmetrikus fenyegetések, mind az ellenséges országok és az üzleti riválisok tevékenységének felderítésére. Funkciói között megtalálható az entitáskinyerés (személy, hely, szervezet, esemény, felszerelés), a szemantikai elemzés, az automatikus fordítás, a beszéd szöveggé alakítása, a keresés video- és audiofájlokban, karakterek felismerése képeken és videókban,[552] valamint a beszélő azonosítása.

A szoftverrendszer vizualizációs eszközökkel, egyebek mellett adatvizualizációs felületekkel (*dashboard*okkal) támogatja az információ áttekintését és a hírszerző jelentések készítését. Az információ keresését filterek alkalmazásával,[553] szemantikus kereséssel,[554] kép alapján történő kereséssel, multimédiás kereséssel, entitások térbeli és hálózatos megjelenítésével és az információ statisztikai korrelálásával segíti. Képes az előre meghatározott indikátorok alapján riasztások kiadására, illetve anomáliák azonosítására. Könnyen installálható a meglévő számítástechnikai eszközökre.[555]

British Aerospace Applied Intelligence (Egyesült Királyság)

A 80 ezer főt foglalkoztató British Aerospace (BAe) cégcsoporton belül a hírszerző megoldásokat kínáló részleg 4500 főt foglalkoztat.[556] A BAe IntelligenceReveal nevű, felhőalapú OSINT-rendszere rugalmasan, a megrendelő igényei alapján alakítható ki, az egyes modulok (rendszerezetlen adatok kezelése, kommunikáció elemzése, tudásmenedzsment, biztonságos böngészés, adatbázisok importálása stb.) egyenként is megvásárolhatók. A rendszer alkalmas entitáskinyerésre, témakörök elemzésére és hangulatelemzésre. Az alábbi funkciókkal rendelkezik:

- kampánymenedzsment rendvédelmi szervezetek részére hangulat- és földrajzi elemzéssel;
- nagyszabású rendezvények biztosítása kulcsszavak és célszemélyprofilok monitorozásával;
- témakörök, helyszínek, csoportok kutatása, a fenyegetések rangsorolása (triázsolása), üzenetek és egyéb kapcsolatok figyelése;
- saját erők digitális nyomainak elfedése, csökkentése.

[552] Optical Character Recognition – OCR.
[553] Facet search.
[554] Fejlett keresési technológia, ahol a hagyományos, lexikális kereséssel szemben az MI-algoritmus megérti a keresőfogalmat vagy a kérdést, és ez alapján gyűjti össze a találatokat.
[555] Az Airbus JOINT ISR honlapja. https://www.intelligence-airbusds.com/markets/defence/joint-isr/; letöltés: 2021.12.20.
[556] A BAe Applied Intelligence honlapja. https://www.baesystems.com/en/cybersecurity/home; letöltés: 2021.07.21.

A Whitenoise nevű adatgyűjtő rendszer lehetővé teszi, hogy a rendvédelmi és a nemzetbiztonsági szervezetekkel együttműködő szolgáltatók hozzáférést adjanak saját adatbázisaikhoz.[557]

A rendszer a Twitteren, a Facebookon, a Google+-on és a YouTube-kommentekben megjelent információk, valamint az RSS-hírcsatornákra[558] feltöltött cikkek monitorozására képes. A képességeket demonstrálja, hogy az alapkonfiguráció óránként 100 ezer Twitter-üzenetet képes kezelni. A rendszer alapesetben 50 millió, a maximális konfigurációban 500 millió eseményt képes nyomon követni. Hátránya, hogy a hozzáféréshez a szolgáltatóknak rendelkezésre kell bocsátaniuk az alkalmazásprogramozási felületüket (API).

A BAe teljes körű támogatást ad a rendszer megtervezéséhez és kiépítéséhez, de – tekintve, hogy felhőalapú szolgáltatásról van szó – a megrendelőnek kell biztosítania a hardvereszközöket. Az egyéni rendszerek létrehozásának részeként pilotprogramok lebonyolítását is támogatják és teljes körű képzést nyújtanak.[559]

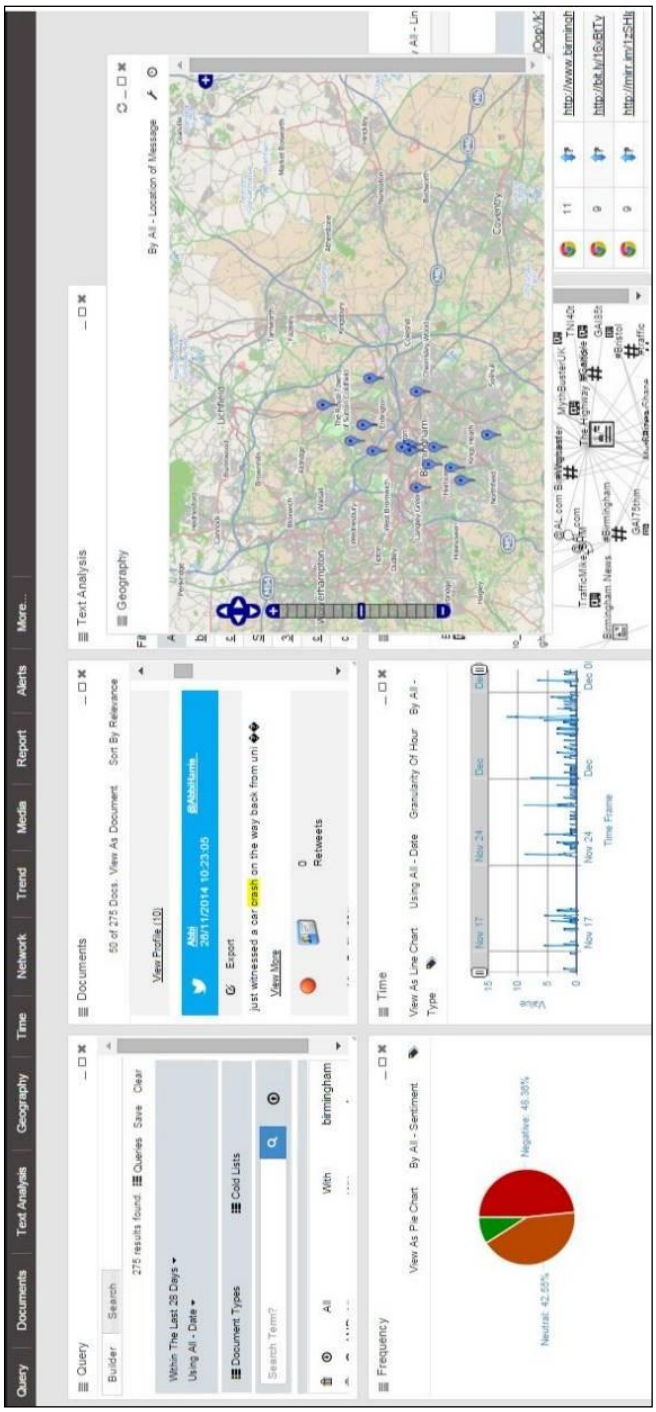
A BAe az IntelligenceReveal rendszert szolgáltatásként árulja. Az alapkonfiguráció használatáért havi 4333 font alaplicencet kell fizetni, amelyhez az első kilenc felhasználóig (kezelőig) felhasználónként további havi 375 font, a tizedik felhasználó fölött felhasználónként havi 200 font licencedíjat kell fizetni (tíz felhasználó esetében tehát havi 7908 fontot). A cég javasolja, hogy a megrendelők legalább öt kezelővel számoljanak, 20 kezelő fölötti rendszer esetén a cég egyéni díjszabást alkalmaz.[560]

[557] Az alkalmazásprogramozási felületen (Application Programming Interface – API keresztül).

[558] Egyes tartalomszolgáltatók RSS-hírfolyamokat osztanak meg, amelyeket RSS-olvasókkal lehet nyomon követni. Az RSS a *real simple sindication*, vagyis az egyszerű hírmegosztás kifejezés rövidítése.

[559] Az IntelligenceReveal OSI-platform brosúrája. https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92253/645404904066643-service-definition-document-2020-07-17-1447.pdf; letöltés: 2021.07.22.

[560] Az IntelligenceReveal OSI-platform díjszabási katalógusa. https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92253/645404904066643-pricing-document-2020-07-17-1455.pdf; letöltés: 2021.07.22.



15. ábra. A BAe IntelligenceReveal rendszerének adatvizualizációs felülete
Az IntelligenceReveal OSI-platform brosúrája.
https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92253/645404904066643-service-definition-document-2020-07-17-1447.pdf;
letöltés: 2021.07.22.

Cobwebs Technologies (Izrael)

A Web Investigation Platform nevű általános OSINT-modul a tömegesen rendelkezésre álló információ rendkívül hatékony kinyerését és integrálását teszi lehetővé. Versenytársai közül kiemelkedik a nem szöveges tartalmak (fotó és videó) kinyerésében, képes arcokat, szövegeket, tárgyakat nagy mennyiségű tartalomból is kiszűrni. A termék gépi tanuláson alapszik, ezen belül a természetes nyelvek gépi feldolgozása és a gépi látás kiemelkedő jelentőségű.

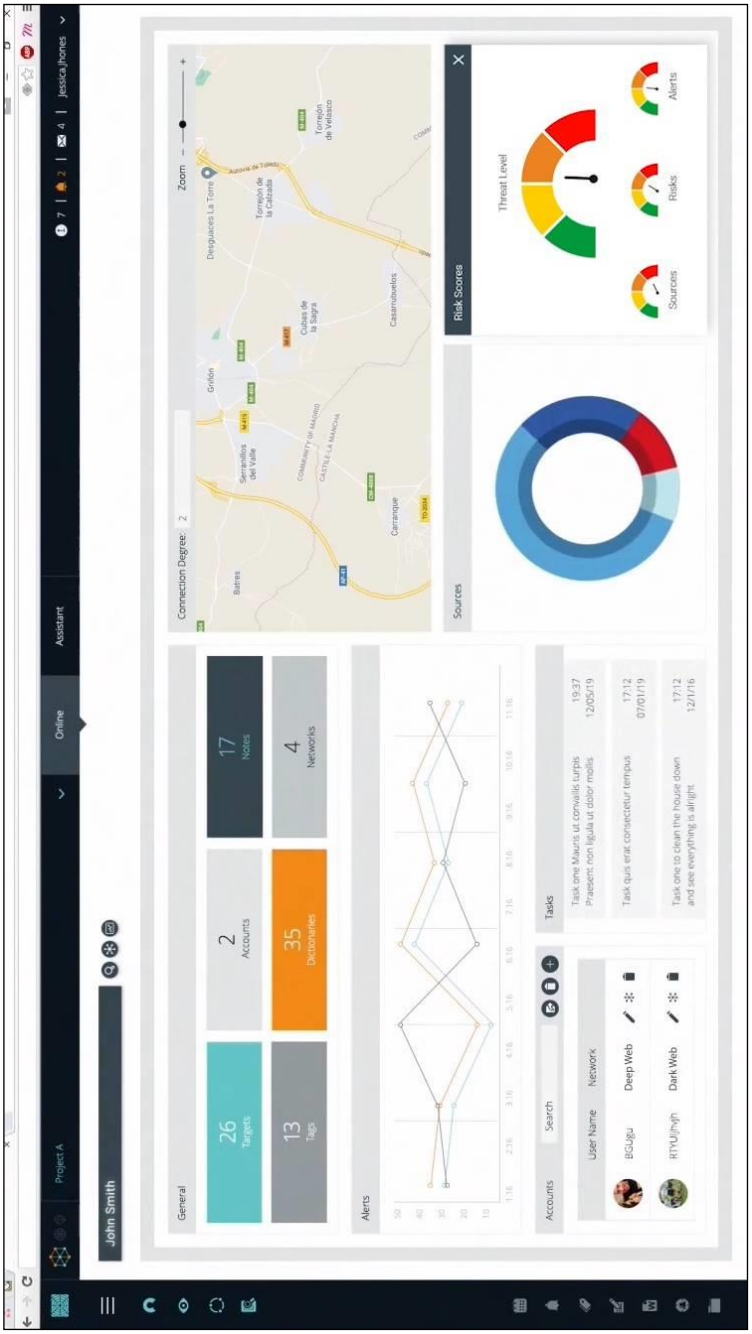
A Cobwebs kiemelkedő képessége, hogy a több cég által kínált virtuális HUMINT-modulon felül képesek a fedőprofilok („virtuális ügynökök[561]") tömeges, teljesen automatikus előállítására és üzemeltetésére, ezáltal a manuálisan működtetett fedőprofiloknál – és az egyéb, nagyadat-kereső szoftvereknél – nagyságrendekkel több információ strukturált, akár automatizált kinyerésére alkalmas, elsősorban a *deep* és a *dark web*ből, a közösségi hálózatokról, valamint a mobiltelefonos alkalmazásokról. Az így kinyert információ tovább pontosíthatja például a migrációs útvonalak és a migránsok szándékának nyomon követését.[562]

A CobWebs további előnye, hogy szükség esetén képes a felhasználói profilok feltörésére is. A cég platformja képes a rendszer elemei közötti webalapú, titkosított kommunikáció biztosítására, ezzel támogatva az optimális munkafolyamatokat (*workflow*). A rendszer képes az előre meghatározott esetekben riasztásokat generálni. A kinyert információkat jól átlátható adatvizualizációs felületeken (*dashboard*okon) a kívánt szempontok szerint (kapcsolati háló, geolokáció, üzenetváltások stb.) vizualizálja. Az érintett funkcionális területeken (terrorizmus, szervezett bűnözés, illegális migráció stb.) a kinyert információk a bíróságok számára is értelmezhető sablonokba exportálhatók.

A Cobwebs Threat Intelligence elnevezéssel dedikált OSINT-modult kínál a fenyegetések valós idejű monitorozására.

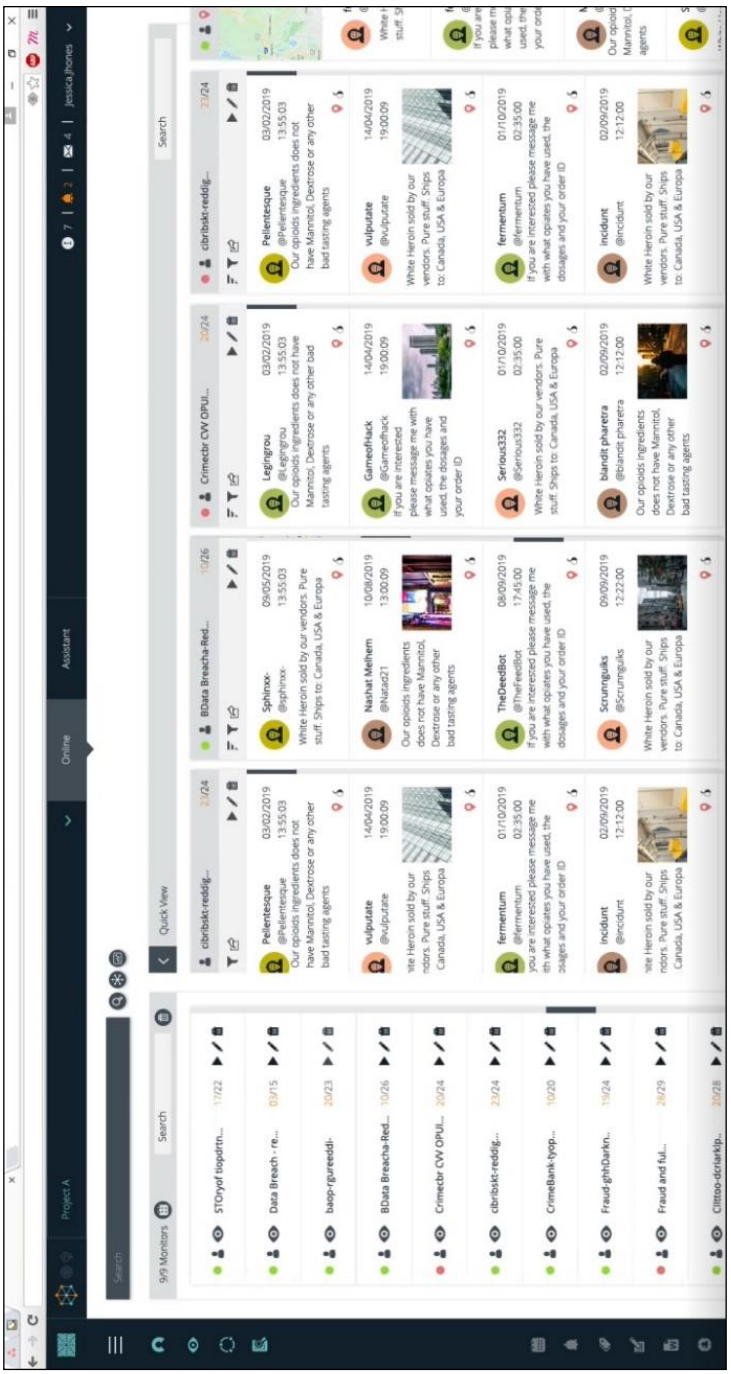
[561] Virtual agent.

[562] Az automatizált fedőprofilok ugyanakkor nem helyettesíthetik minden esetben a kezelő által irányított (fél)automata profilokat, hiszen előbbiek „legendája" könnyen dekonspirálható.

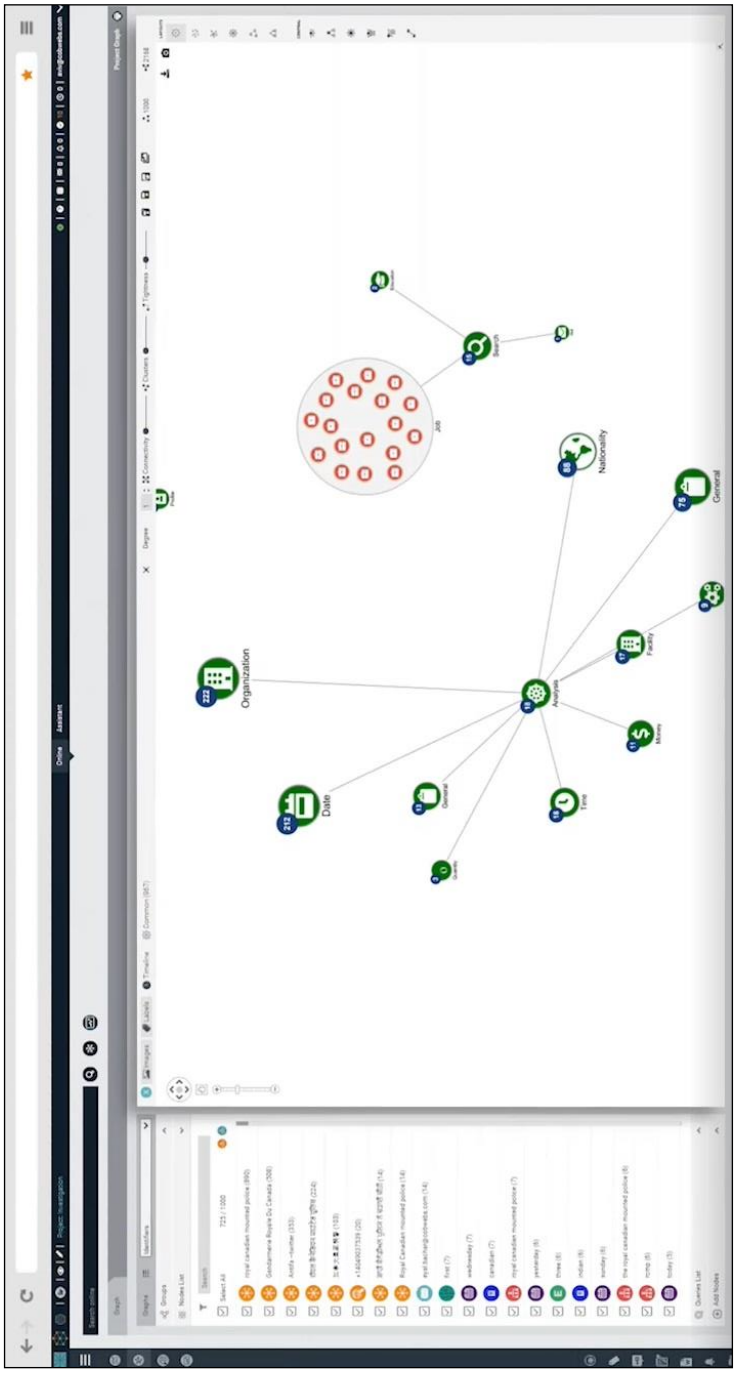


16. ábra. A John Smith nevű célszemélyről rendelkezésre álló információk áttekintő nézete a Cobwebs Web Intelligence modul adatvizualizációs felületén
AI-Powered Web Intelligence: A Cobwebs Technologies honlapja. https://cobwebs.com/; letöltés: 2021.07.21.

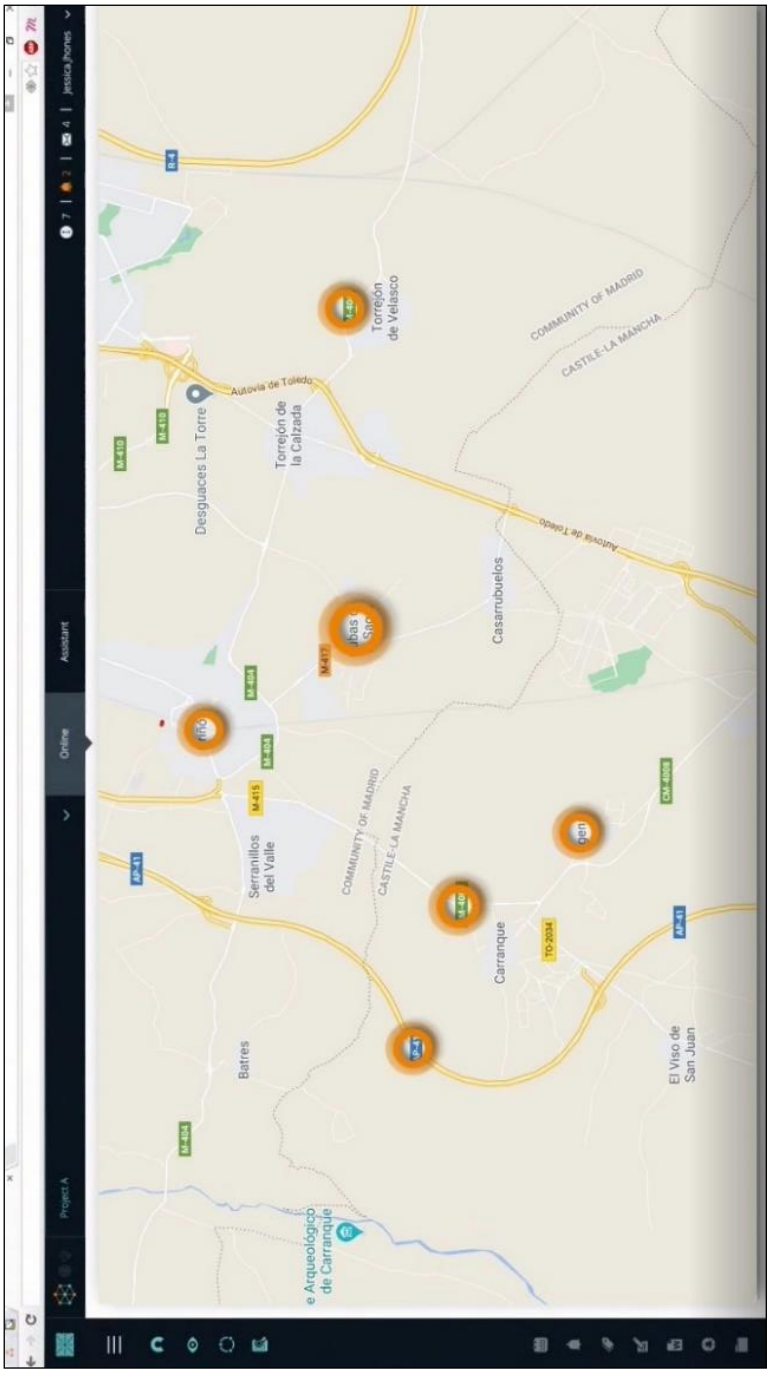
17. ábra. Az entitáskinyerés eredményei a Cobwebs Web Intelligence moduljának adatvizualizációs felületén
AI-Powered Web Intelligence: A Cobwebs Technologies honlapja.
https://cobwebs.com/; letöltés: 2021.07.21.



18. ábra. A célszemélyek profiljai által váltott üzenetek a Cobwebs Web Intelligence moduljának adatvizualizációs felületén
Cobwebs' Threat Intelligence Platform: A Cobwebs Technologies honlapja.
https://cobwebs.com/products/threat-intelligence-solution/; letöltés: 2021.07.21.



19. ábra. A kapcsolati hálózat megjelenítése a Cobwebs Web Intelligence modulján
Cobwebs' Threat Intelligence Platform: A Cobwebs Technologies honlapja.
https://cobwebs.com/products/threat-intelligence-solution/; letöltés: 2021.07.21.



20. ábra. A fenyegetések térképes megjelenítése a Cobwebs Web Intelligence felületén
Cobwebs Threat Intelligence Platform: A Cobwebs Technologies honlapja.
https://cobwebs.com/products/threat-intelligence-solution/; letöltés: 2021.07.21.

A Lynx izolált, titkosított, biztonságos internetes környezete lehetővé teszi a manuális keresések digitális nyomainak minimalizálását. Az automatizált rendszer lehetővé teszi, hogy az OSINT-elemzőknek kevesebbet kelljen foglalkozniuk az energia- és időigényes, nagy körültekintést igénylő műveleti biztonsági rendszabályok betartásával. A kutatáshoz használt fedőprofilok automatikus karbantartása, menedzselése szintén hozzájárul a műveleti biztonsághoz. Az emberi tényező kiváltásával nagyban csökkenthető az internetes keresésekkel járó kockázat.

A Weaver pénzügyi hírszerzési platform a pénzmosás, a pénzügyi csalások és a pénzintézetek elleni kibertámadások és kiberhírszerzés ellen nyújt támogatást.[563]

A Web Investigation Platform felhőalapú alapverziójának havi licencedíja felhasználónként havi 3950 font. Külön költséget számítanak fel a kiegészítő modulokért: a *dark web* modul díja havi 720 font, a tárgyakat és írott karaktereket felismerő modulé 1000 font, a Lynx rendszeré 2000 font, a Weaver modulé 720 font. A Cobwebs egyszeri, 8390 fontos díjat számít fel a rendszer teljes körű üzembe helyezéséért. Az alaprendszer éves költségei így évi 55 790 fontot, a teljes rendszeré 109 070 fontot emésztenek fel. A gyártó a rendszer használatának 2. évétől 8%-os, a 3. évtől 12%-os kedvezményt ad.[564]

Cognyte[565] ***(Izrael–Amerikai Egyesült Államok)***

A Web Intelligence rendszer a nyílt információszerzés teljes spektrumát lefedi:

- nagy mennyiségű harcászati, hadműveleti és hadászati/stratégiai szintű valós idejű (*current intelligence*) és háttérinformációk (*basic intelligence*) folyamatos gyűjtése, szelektálása, továbbítása;
- információ kinyerése a hagyományos internetes médiából, a közösségi médiából, mobiltelefonos alkalmazásokból, valamint a mély és a sötét netről;
- a legyűjtött információ automatikus feldolgozása, profilozás (pl. a fotókon látható objektumok alapján geolokáció beazonosítása, arcfelismerés stb.);
- automatikus entitáskinyerés;
- fordítás 140 nyelvről azok bármelyikére;
- biztonságos browser segítségével fedőprofilokkal fedett kutatások végrehajtása;
- jelentések készítése.[566]

---

563 A Cobwebs Technologies honlapja. https://cobwebs.com/; letöltés: 2021.07.21.

564 A Cobwebs díjszabási brosúrája. https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/715532/220349016606958-pricing-document-2020-07-19-0913.pdf; letöltés: 2021.07.22.

565 A Verint egykori hírszerzési részlege.

566 A Cognyte honlapja: Web Intelligence. https://www.cognyte.com/web-intelligence/; letöltés: 2021.07.21.

Gamma Group (Egyesült Királyság)

A Gamma Group által kínált megoldások lehetőséget adnak a terrorista szervezetek által használt internetes kommunikációs csatornák monitorozására. A *deep* és a *dark web*en zajló, sokszor titkosított csatornák megfigyelését és kinyerését a szoftveres megoldások mellett nagyban támogatják a cég terrorelhárítási szakértőinek háttértudása, a terrorista szervezetek módszereinek nyomon követése is.[567]

MEDUSA (Olaszország)

A MEDUSA integrált OSINT/SOCMINT-platform képes a világháló, ezen belül a közösségi média[568] és a fórumok monitorozására, valamint a legtöbb kereskedelmi böngészőprogram számára hozzáférhetetlen *deep* és *dark web* információinak kinyerésére.[569] A megszerzett információkat elemző-értékelő eszközökkel (grafikonok, térképes és hálózatos megjelenítés, szemantikai és kapcsolati elemzés stb.) kezeli. A rendszer a monitorozott információt folyamatosan gyűjti, így azok az internetről történt eltávolításukat követően is hozzáférhetők maradnak. A MEDUSA – nem részletezett – nyelvi modulokkal is kiegészíthető. Képes szövegben és videóban is keresni. A keresések kulcsszó, a felhasználók által megadott tárgyszó (*hashtag*) vagy földrajzi terület kijelölése[570] alapján történhet. A megszerzett információk hálózatelemzéssel is vizsgálhatók. A rendszer több nyelven képes az adatelemzésre, szemantikai (nyelvi) elemző modulja adatelemek (rekordok) milliárdjait képes elemezni, és ez alapján hangulatelemzést, entitáskinyerést végezni.

A rendszer gépi tanulási algoritmusai képesek a politikai, humanitárius, bűnügyi stb. trendek közel valós idejű nyomon követésére, amelyeket grafikonos és térképes megjelenítéssel vizualizál. Alkalmasak az álhírek és azok készítői azonosítására, a terjedésük nyomon követésére és a kapcsolódó közvélekedés elemzésére.

Az olasz cég teljes körű oktatást nyújt a partnerei számára.[571]

---

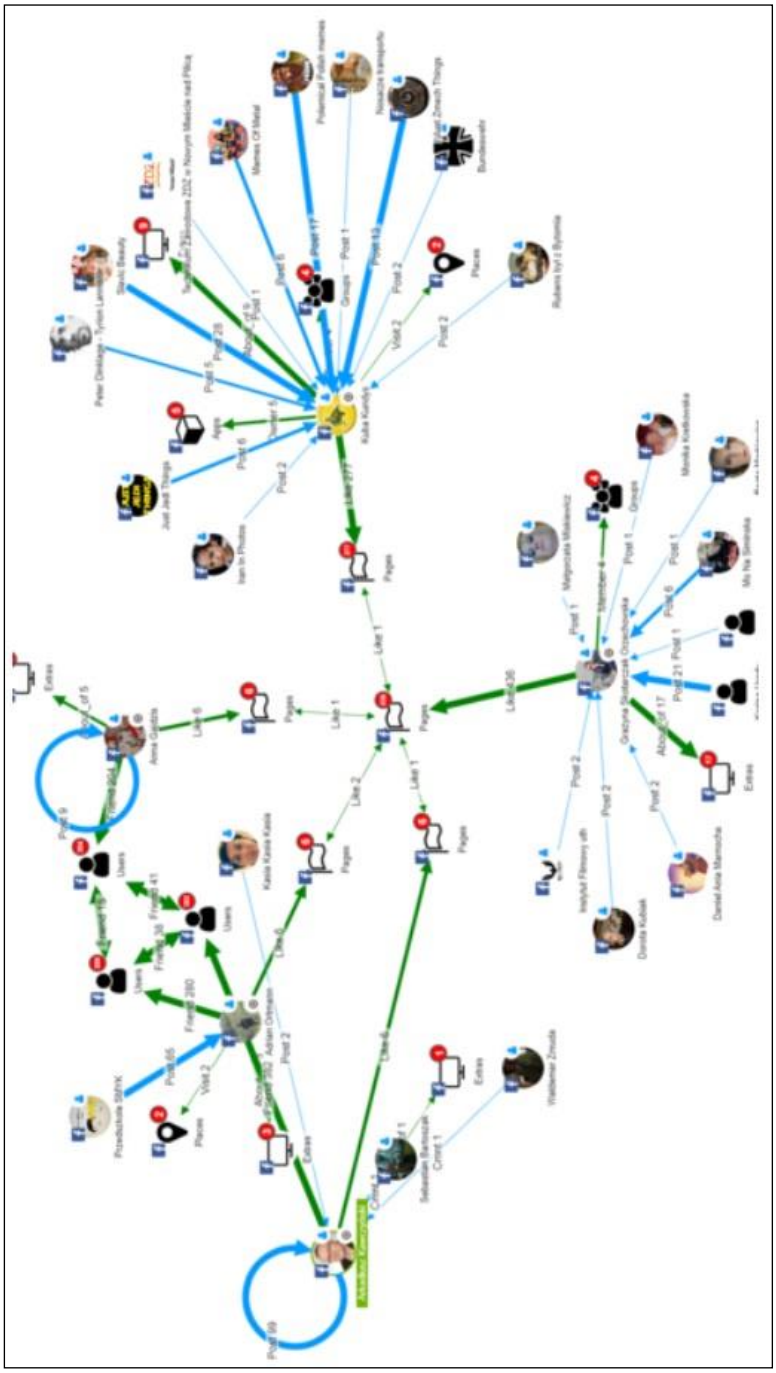
567 A Gamma Group honlapja: Products & Services. https://www.gammagroup.com/ProductsServices.aspx?m=p; letöltés: 2021.07.21.

568 Facebook, Instagram, Twitter, YouTube, LinkedIn, Snapchat, Google+ és Telegram.

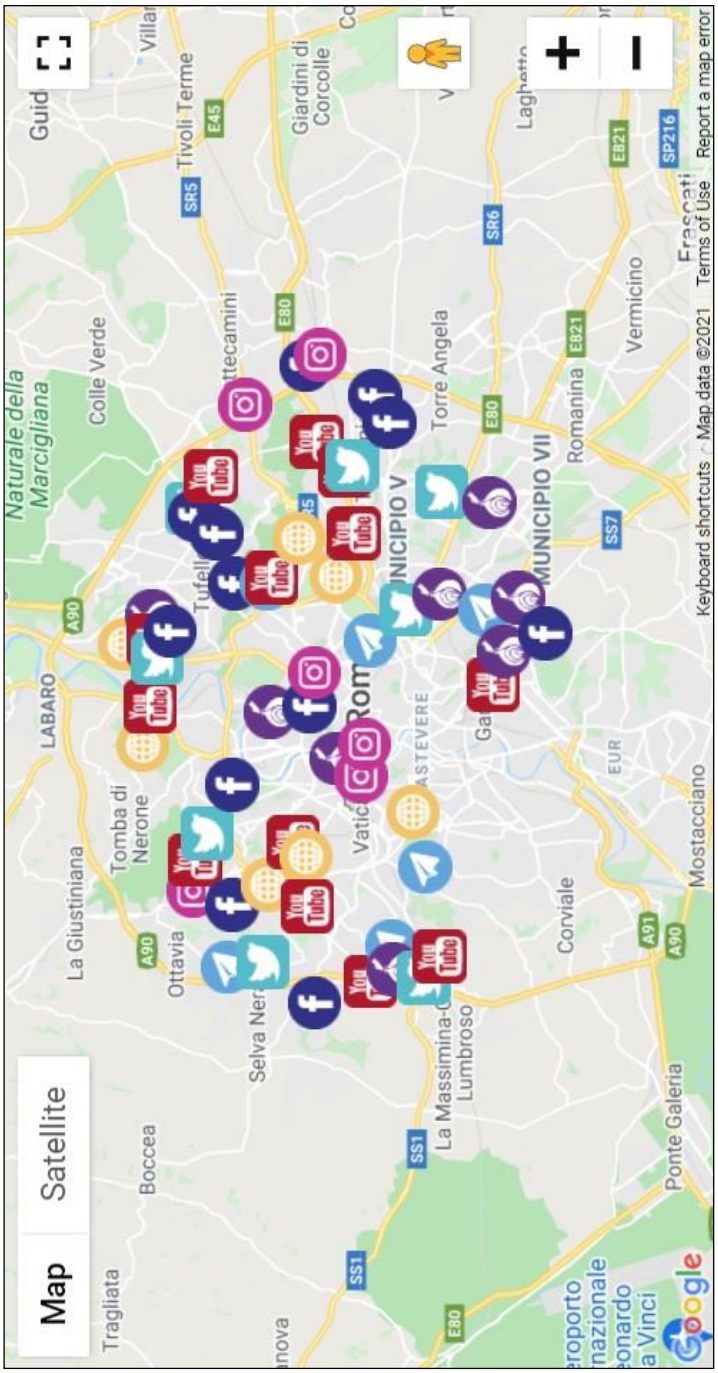
569 Egyebek mellett a *deep* és *dark web*es fórumokra és a .onion tartományra is képes behatolni.

570 Geofencing.

571 A Medusa Labs honlapja. https://www.medusa-labs.com/; letöltés: 2021.07.21.



21. ábra. A Medusa platform hálózatelemző modulja
A Medusa Labs honlapja.
https://www.medusa-labs.com/; letöltés: 2021.07.21.



22. ábra. A vizsgált üzenetek szolgáltatók szerinti bontású térképes megjelenítése a Medusa felületén
A Medusa Labs honlapja.
https://www.medusa-labs.com/; letöltés: 2021.07.21.

HUMINT

Cobwebs Technologies (Izrael)

A Trapdoor modult a SOCMINT- és a virtuális HUMINT-feladatok ellátására fejlesztették ki. A rendszer lehetővé teszi, hogy a kezelők felderítsék a célszemélyeket (akár azok IP-címét is), és biztonságosan, anonim módon, többféle módon kapcsolatba kerüljenek velük. Külön műveletvezető modullal, illetve a digitális nyomok (készülék és böngésző típusa, cookie-k, nyelvi beállítások, időbélyegzők stb.) kinyerésére alkalmas modullal rendelkezik.[572]

Etiya (Törökország)

A török cég kereskedelmi kampánymenedzsment platformja a kampányok megtervezésében, végrehajtásában, menedzselésében és az eredmények mérésében segíti a megrendelőket. Lehetővé teszi, hogy a megfelelő ajánlat a megfelelő közönséghez az arra alkalmas csatornán célzottan jusson el az előre meghatározott időpontban. A platform lehetővé teszi az ajánlatok és a kampányok személyre szabását,[573] a fogyasztói csoportok szegmentálását, a közel valós idejű döntéshozást a kampánymenedzserek részére,[574] illetve javaslatokat tesz a kampány következő lépésére. Az MI-alapú adatelemzésnek köszönhetően a kampányok eredményessége akár személyre szabottan is folyamatosan mérhető. Az eredményességet az előrejelző algoritmusok növelik.

A rendszer felhőalapú szolgáltatásként vagy a megrendelő saját hálózatán is működtethető.[575]

MEDUSA (Olaszország)

A MEDUSA integrált OSINT/SOCMINT-platformja befolyásolási műveletek (kampányok) végrehajtására is alkalmas. A nyílt információk segítségével vagy más módon azonosított célszemélyek, -csoportok és -szervezetek profilozására automatikusan is képes. A MEDUSA képes automatikusan kapcsolatba lépni a célcsoportok tagjaival és hozzájuk az előre meghatározott ellennarratívát eljuttatni. Segítségével nemcsak egyedi bejegyzésekre lehet válaszolni, de alkalmas befolyásolási kampányok megalkotására és üzenetek célzott eljuttatására a célcsoportokhoz.

---

572 Active Web Intelligence: A Cobwebs Technologies honlapja. https://cobwebs.com/products/active-web-intelligence/; letöltés: 2021.07.21.

573 A tartalom személyre szabása több mint 300 paraméter (nem, életkor, lakóhely, jövedelmi szint stb.) alapján történik.

574 A döntéshozatalban a kampányköltségek figyelemmel követését lehetővé tevő modul is segít.

575 Az Etiya honlapja: Easy to use and flexible interface, personalized campaigns. Next generation campaign management. https://www.etiya.com/en/products/campaign-management?gclid=CjwKCAjwi9-HBhACEiwAPzUhHKcGUXLlNfQTKAaL_wNaS1gYxr6bFJpU_3HNhwX7T1rwaA40cA8H2hoCn0kQAvD_BwE; letöltés: 2021.07.22.

A rendszer képes automatikusan és félautomatikusan is létrehozni fedőprofilokat a közösségi média számára. A félautomatikusan létrehozott, HUMINT-kezelők által irányított fedőprofilokkal nagyobb hatékonysággal lehet a radikális, a terrorista és a bűnözői stb. csoportok zárt internetes csoportjaiba behatolni.

A MEDUSA virtuális HUMINT-modulja a kezelő által félautomatikusan létrehozott közösségimédia-profilok segítségével képes a szélsőséges ideológiák (információs hadviselés) terjesztését megfigyelni, az ideológiát semlegesítő információt terjeszteni,[576] illetve a számunkra előnyös információt a csoport tagjaihoz eljuttatni (*campaign*), ezáltal a csoport vagy egy társadalmi réteg véleményét befolyásolni. Az eszközök felhasználásával virtuális befolyásolási műveletek valósíthatók meg.[577]

SIGINT

Airbus Joint ISR (Európa)

A Fortion Electronic Warfare Analyst (EWA) elektronikai felderítési (ELINT) elemzőmodul az elektromágneses sugárzást kibocsátó eszközök azonosítását, helymeghatározását, nyomon követését és jellemzőik meghatározását, valamint az elektronikai harcrend[578] felrajzolását teszi lehetővé. Az elemzéshez rádióforgalmazási adatokat, radarjeleket, zavaróeszközök jeleit, irányvonaladatokat[579] stb. használ fel.[580]

ATIS systems (Németország)

A német cég Klarios nevű szoftvere a távközlési szolgáltatóktól beszerzett és a lehallgatott információ felhasználóbarát, jól átlátható felületen végzett elemzésére, szűkítésére, rendszerezésére és keresésére szolgál. A Klariost országszintű távközlési információk feldolgozására tervezték, ennek megfelelően sok milliárd metaadatot kezel. Alkalmas hangfelismerésre, a földrajzi (térinformatikai) adatok kinyerésére, megjelenítésére, ilyen adatbázisok építésére és importálására. Képes a különböző távközlési módok (PSTN, ISDN, GSM, UMTS, LTE, LTE-A, VoLTE, VoIP, NGN és IP) integrált kezelésére. Összekapcsolható az országos videomegfigyelési, útlevél- és előfizetői adatbázisokkal, illetve a közösségi média felderítésére szolgáló szoftverekkel.

A rendszer Klarios ATIS Interception Management System nevű modulját elsősorban a távközlési társaságok számára tervezték, megkönnyítve számukra a jogszabályban rögzített információátadási kötelezettségeik teljesítését. Működtetése nem jár kapacitáscsökkenéssel a szolgáltatók számára.

---

576 Counter messaging.

577 A Medusa Labs honlapja. https://www.medusa-labs.com/; letöltés: 2021.07.21.

578 Electronic Order of Battle (EOB).

579 Line of bearing.

580 Az Airbus JOINT ISR honlapja. https://www.intelligence-airbusds.com/markets/defence/joint-isr/; letöltés: 2021.12.20.

A rendszer egyszerűsített verziója[581] is rendelkezésre áll, amennyiben az adatok szűkebb körének elemzése is elegendő.[582]

Gamma Group (Egyesült Királyság)

A Gamma Group rádióelektronikai felderítés elleni védelme elsősorban a vezeték nélküli kommunikáció[583] titkosításával és a hamis bázisállomásokkal[584] szembeni védelemmel járul hozzá a kritikus infrastruktúra védelméhez. A cég a területen az alábbi szolgáltatásokat nyújtja:

- GSM/UMTS/LTE/5G és műholdas hálózatok tesztelése;
- telekommunikációs infrastruktúra tervezése és kivitelezése;
- képzések.

A Gamma Group a technikai hírszerzés elleni ellentevékenységben[585] is tud segítséget nyújtani:

- teljes körű biztonsági ellenőrzések végrehajtásával és a biztonsági helyzet értékelésével;
- a rejtett lehallgatóeszközök, kamerák stb. felfedésével;
- a határokon átnyúló ipari kémkedés felfedésével.[586]

Rayzone

Az izraeli cég ECHO nevű webalapú (virtuális) globális SIGINT-rendszere segítségével a világon bárhol képes az okostelefonok metaadatait (hely, idő, híváslista stb.) nagy tömegben kinyerni és azokat fejlett algoritmusokkal (ideértve a hangfelismerést is, amennyiben a hanganyag is rendelkezésre áll) elemezni. A nagyadat-rendszer alkalmas az adott ország valamennyi, okostelefonnal rendelkező internethasználójának a megfigyelésére. A rendszer használatához nem szükséges sem a felhasználó, sem a szolgáltató engedélye. A Rayzone a felhasználói adatokat az automatizált okostelefonos hirdetéseket közvetítő szolgáltatók rendszerein keresztül szerzi be, hirdetőnek álcázva magát. A helyadatok egyméteres pontosságúak.[587,588,589]

---

581 Deployment module.

582 Az ATIS systems honlapja: Klarios ATIS Interception Management System. https://www.atis-systems.com/language/en/klarios-atis-interception-management-system/; letöltés: 2021.07.21.

583 Air interface.

584 Fake base station.

585 Technical Surveillance Counter Measures – TSCM.

586 A Gamma Group honlapja: Products & Services. https://www.gammagroup.com/ProductsServices.aspx?m=p; letöltés: 2021.07.21.

587 A Rayzone Group honlapja: ECHO – Global Virtual SIGINT System. https://rayzone.com/echo-global-virtual-sigint-system/; letöltés: 2021.07.21.

588 GANON, Tomer – RAVET, Hagar: The Rayzone Group's secret cyber intelligence activities revealed. CTech, 2020.12.29. https://www.calcalistech.com/ctech/articles/0,7340,L-3884553,00.html; letöltés: 2021.07.22.

GEOINT/IMINT

NRO Sentient (Amerikai Egyesült Államok)

A Nemzeti Felderítőiroda (NRO) 2010 óta fejlesztett Sentient nevű térinformatikai MI-rendszere képes összevetni a katonai és a kereskedelmi forrásból elérhető műholdképek felvételeit és más IMINT-adatokat SIGINT-, HUMINT- vagy nyílt forrásból származó információkkal. Ezáltal nagy mennyiségű adat feldolgozásával, katalogizálásával, anomáliák kimutatásával támogatja az előrejelzések készítését és a lehetséges cselekvési változatok modellezését. Alkalmas múltbeli események elemzésére és a jelen helyzet ismeretének nagybani növelésére, valamint a felderítő/hírszerző erőforrások jobb kihasználásának elősegítésére. A közeljövőben a rendszer egyebek mellett alkalmassá válhat a haderő diszlokációjának globális valós idejű nyomon követésére, hasonlóan a hajózási vállalatok vagy az autókölcsönzők rendszeréhez.[590]

Airbus Joint ISR (Európa)

A Fortion Image Analyst IMINT-rendszer többforrású adatelemzésre alkalmas: képek, videók, földi mozgó célok felderítésével kinyert információk,[591] automatikus azonosító rendszerek[592] és harcászati adatlinkek[593] információi alapján állíthatók elő a segítségével harcászati, hadműveleti vagy hadászati szintű IMINT-termékek. Alkalmas tárgyak automatikus észlelésére és azonosítására, objektumok elemzésére, célkiválasztásra, műveleti tervezés és kárbecslés támogatására.

Az Image Analyst Lite a nagy felbontású műholdfelvételek gyors megjelenítését és elemzését segíti. Támogatott képformátumok: GeoTIFF, NITF, JPEG2000, ECW, GeoPackage, JPEG, TIFF, USRP, ASRP, CADRG. Vektorfájlformátumok: Shapefile, KML, GDB, GeoPackage, GeoJSON, GPX, GML, OSM. A végterméket az alábbi formátumokban képes elkészíteni: Geospatial PDF, GeoPackage, JPEG2000, GeoTIFF, Shapefile és KML.

A Fortion Image Intelligence Knowledge Database (IMINT KDB) IMINT-tudásadatbázis a szárazföldi infrastruktúrával kapcsolatos információk egyszerű gyűjtését, tárolását, rendszerezését és biztonságos megosztását segíti, valamint lehetővé teszi az IMINT-csoportok és -szervezetek közötti hatékony kollaborációt.

---

589 BREWSTER, Thomas: Exclusive: Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps. Forbes, 2020.12.11. https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/; letöltés: 2021.07.22.

590 SCOLES, Sarah: It's Sentient – Meet the classified artificial brain being developed by US intelligence programs. The Verge, 2019.07.31. https://www.theverge.com/2019/7/31/20746926/sentient-national-reconnaissance-office-spy-satellites-artificial-intelligence-ai; letöltés: 2021.08.13.

591 Ground Moving Target Indicating – GMTI: a radarok egyik üzemmódja, amellyel megkülönböztethetők a célinformációk a háttérzajtól.

592 Automatic Identification System – AIS.

593 Tactical Data Link – TDL, például: Link16 és Link22.

23. ábra. Nagy felbontású műholdfelvétel megjelenítése az Airbus ISR Fortion Image Analyst Lite segítségével
Az Airbus JOINT ISR honlapja.
https://www.intelligence-airbusds.com/markets/defence/joint-isr/; letöltés: 2021.12.20.

A Fortion RECCE Engine adatbázis a légi, a szárazföldi és a haditengerészeti haditechnikai eszközök, valamint a hadászati fegyverek felderítésében és azonosításában segíti az IMINT-elemzőket. A félautomata azonosítási rendszer több mint 1800 haditechnikai eszköz rendszeresen frissített adatait tartalmazza, és lehetővé teszi azok különböző fényviszonyok közötti, 3D-ben történő megjelenítését.

Az Airbus Fortion SuRVIn[594] ABI,[595] InESS[596] és STIC nevű GEOINT adatfúziós rendszerei a valós időben adatot szolgáltató légi, földi, tengeri és űrben telepített ISR-rendszerek képességeinek kiterjesztésére szolgálnak. Segítségükkel a védelmi, a biztonsági és a polgári szférában is megvalósítható az információs és a döntési fölény.

Az ABI harcászati/taktikai, (had)műveleti és hadászati/stratégiai szinten, az InESS hadműveleti és harcászati szinten, míg az STIC elsősorban harcászati szinten (pl. határtérségek ellenőrzés alatt tartására) alkalmazható. A GEOINT-adatok kinyerésében és az így megszerzett szituációs éberség és helyzetkép valós idejű, biztonságos felhőalapú megosztásában és ezáltal a saját és a szövetséges erők közös hadműveleti értékelésének[597] kialakításában nyújtanak segítséget. Lehetséges adatforrások: többek között radar, a légi irányításban alkalmazott automatikus berendezésfüggő légtérellenőrzési adatok[598] és automatikus azonosítórendszerek, SIGINT (ELINT/COMINT), harcászati adatlink, képalkotó szenzorok, földi mozgó célok felderítése.

A megszerzett információkat gépitanulás-alapú viselkedéselemzéssel, anomáliafelismeréssel, aktivitás-előrejelzéssel, illetve statisztikai módszertannal dolgozzák fel. Alkalmasak a teljes hírszerzési ciklus, valamint a döntéselméleti OODA-hurok[599] lefedésére, támogatására. Képesek az automatikus adatgyűjtésre és -feldolgozásra is, emellett szimulációs és kiképzési feladatokra is alkalmazhatók. A rendszerek platformtól függetlenül, tehát például repülőgépre telepítve, régebbi ISR-eszközök kiegészítéseként vagy különálló (*standalone*) rendszerként is alkalmazhatók.

A rendszer további előnye NATO-interoperabilitása, kialakítása megfelel a NATO ISR Interoperabilitási Architektúra[600] követelményeinek. A Szövetség Sigonellában települt RQ–4D Phoenix típusú pilóta nélküli felderítő-repülőgépei[601] által megszerzett adatok feldolgozásában is alkalmazzák. Az Airbus ISR-rendszerei a NATO-sztenderdek szerint nemzeti C4I-rendszerekkel is összekapcsolhatók.

---

594 Surveillance, Reconnaissance, Visualisation, Intelligence.

595 „Aktivitásalapú hírszerző rendszer" (Activity-Based Intelligence – ABI).

596 Integrált ISR-kinyerési keretrendszer (Integrated Intelligence, Exploitation, Surveillance Suite).

597 Common Relevant Operational Picture – CROP.

598 Automatic Dependent Surveillance-Broadcast – ADS-B.

599 Observe, Orient, Decide, Act (megfigyel, tájékozódik, dönt és cselekszik).
DRÓT László: Az OODA hurok (I. rész). Seregszemle, 16. évfolyam 1. szám, 2018. január–március. pp. 143–159.
https://honvedelem.hu/files/files/115176/seregszemle_2018_1.pdf; letöltés: 2021.12.20.

600 NATO ISR Interoperability Architecture – NIIA.

601 NATO Allied Ground Surveillance – AGS.

Az Airbus Smart Report néven saját IMINT/GEOINT elemzési szolgáltatást működtet a védelmi/biztonsági szféra, nemzetközi szervezetek és magánvállalatok számára. A védelmi/biztonsági területen kárbecslést, határtérségek monitorozását, rakétakilövő állások monitorozását, katonai infrastruktúra feltérképezését, valamint a fegyveres erők harcrendjének felvázolását vállalják. A krízis- és katasztrófamenedzsment körébe a természeti károk felmérése, a károsodott termőföld és infrastruktúra felmérése, nagy kiterjedésű tűzvészek monitorozása és előzetes kockázatelemzés tartozik. Az építészet és a várostervezés területén építési területek figyelését, illegális építkezések felderítését, valamint kataszteri felmérést vállalnak. Az energia- és a bányászati szektor számára az olaj- és földgáz-infrastruktúra feltérképezését és biztonságának monitorozását, atomerőművek biztonsági megfigyelését, a szélturbinák optimális helyének kiválasztását, illetve gátak modellezését kínálják.[602]

BlackSky (Amerikai Egyesült Államok)

A BlackSky GEOINT-vállalat a térinformatikai hírszerző szolgáltatások széles spektrumát kínálja kormányzatoknak, valamint magánvállalatoknak és -szervezeteknek. A cég jelenleg 25 műhold,[603] több mint 40 ezer hírforrás, 100 millió mobileszköz, 70 ezer hajó és repülőgép, nyolc közösségimédia-szolgáltató, 5000 környezeti szenzor és több ezer IoT-eszköz adatainak feldolgozásával állítja elő termékeit, amelyeknek fő célja a megrendelők helyzetismeretének növelése. A jövőben 60 saját műhold fellövését tervezi.[604]

A magán hírszerzőcég a mesterséges intelligencia, a felhőmegoldások és a multiszenzoros adatfúzió segítségével fejlett adatelemző szolgáltatásokat nyújt. Lehetőség van a műholdak számára egyedi IMINT-feladatok meghatározására is. A szolgáltatások alapja a Spectra AI MI-alapú elemzőplatform, amely lehetőséget ad a BlackSky adatbázisa alapján globális események és történések figyelemmel követésére. A Spectra lehetővé teszi a szintetikus apertúrájú radarok, a hiperspektrális képszenzorok[605] és a rádiófrekvenciás azonosítást lehetővé tévő szenzorok[606] adatainak elemzését és fúzióját.

---

602 Az Airbus JOINT ISR honlapja.
https://www.intelligence-airbusds.com/markets/defence/joint-isr/; letöltés: 2021.12.20.

603 Köztük az Airbus Pléiades, SPOT6/7, KazEOSat-1 és TerraSAR-X, a 21AT TripleSat, az UrtheCast Deimos-2, valamint a SIIS KOMPSAT műholdjai.
Introducing BlackSky Spectra. BlackSky, 2017.04.04.
https://www.blacksky.com/2017/04/04/introducing-blacksky-spectra/; letöltés: 2021.08.13.

604 SCOLES, Sarah: It's Sentient – Meet the classified artificial brain being developed by US intelligence programs. The Verge, 2019.07.31.
https://www.theverge.com/2019/7/31/20746926/sentient-national-reconnaissance-office-spy-satellites-artificial-intelligence-ai; letöltés: 2021.08.13.

605 Hyperspectral imaging sensors: A több mint húsz diszkrét spektrális sávval rendelkező szenzorokat hiperspektrális képszenzorokként is említik.

606 Radio frequency detection: A rádiófrekvenciás azonosítás (RFID) olyan automatizált adatgyűjtési technológia, amely rádióhullámok segítségével továbbítja az adatokat az olvasó és a címke (*tag*) között a címkézett elem azonosítása, nyomon követése és felkutatása céljából.
RFID kisokos. IBCS Hungary, 2021.02.16.
https://ibcs.hu/tudastar/rfid-kisokos/?gclid=CjwKCAjwsNiIBhBdEiwAJK4khv9W8bvt3S5oNEAPVps99tKM5PYl2PgvPXD8yk3bCGM-KFzwmZfa2hoCHssQAvD_BwE; letöltés: 2021.08.13.

24. ábra. Egy naperőműpark műholdas képe és egy kapcsolódó közösségimédia-bejegyzés a BlackSky platformján
RUSSELL, Kendall: BlackSky to Develop GEOINT Broker Platform for Air Force Research Lab. Via Satellite, 2017.08.30. https://www.satellitetoday.com/government-military/2017/08/30/blacksky-develop-geoint-broker-platform-air-force-research-lab/; letöltés: 2021.08.13.

A megrendelők a vállalat saját internetes platformjain keresztül vehetik igénybe a szolgáltatásokat:

- a *BlackSky Detect* alkalmas objektumok megkeresésére és nyomon követésére globálisan; a megoldást elsősorban kikötők, repülőterek és építési területek üzemeltetőinek és használóinak ajánlják, lehetővé téve a változások figyelemmel követését, azonnali figyelmeztetést a károk bekövetkezésekor, anomáliák felfedezését és a raktárkészletek elemzését;

- a *BlackSky Site Monitoring* kikötők, repülőterek és építési területek megfigyelésére alkalmas;

- a *BlackSky Events* világszerte több millió eseményről tesz elérhetővé információt; riasztást ad események bekövetkezéséről egyebek mellett helyi és globális híroldalak, blogok, járványügyi és természeti vészhelyzeti jelentések, szenzorok, gazdasági és pénzügyi adatbázisok információi alapján; lehetőség van az események tematikus keresésére/figyeltetésére is.[607]

British Aerospace Applied Intelligence (Egyesült Királyság)

A BAe kimondottan a hadműveleti területen települt erők támogatására hozta létre a GEOINT-rendszereit. A rendszerek a légi és a műholdas IMINT-felvételek tömeges és automatikus feldolgozásán keresztül gépi tanulási algoritmusok felhasználásával képesek helyzetismeretet biztosítani, mintázatokat azonosítani és veszélyfigyelmeztetéseket generálni. A GEOINT-rendszerek petabájtos[608] nagyságrendben kezelik az adatokat.

A rendszerek működési elvére példa, hogy képesek észlelni a járművek keréknyomainak szokatlan sűrűsödését egy útkereszteződésben a megfigyelés alatt álló térségben. A rendszer értesíti a GEOINT-elemzőt, aki a rendszerbe táplált egyéb IMINT-információból megállapíthatja, hogy az ellenálló erők házilagos készítésű robbanószerkezeteket telepítettek az út mentén. Az elemző ezt követően képes az információt valós időben megosztani a térségben tevékenykedő saját erőkkel.

A rendszerek emellett alkalmasak a határvédelmi erők támogatására is.

A BAe teljes körű támogatást nyújt a rendszerek használatához. Segítséget nyújt a megrendelők GEOINT-rendszerének korszerűsítéséhez, fotogrammetriai[609] támogatást nyújt a precíziós térképek készítéséhez és segítséget nyújt a precíziós csapásmérésben is. A modulok különálló munkaállomásokon és egy integrált rendszer részeként is működtethetők.

---

607 A BlackSky honlapja. https://www.blacksky.com; letöltés: 2021.08.13.

608 1 petabájt = 1 048 576 gigabájt.

609 A fotogrammetria a távérzékelés tudományága, amely a tárgyakról, illetve a terepről készített fényképek alapján a képeken végzett mérések és számítások segítségével meghatározza a képeken látható valós tárgyak kiterjedéseit.

A GXP Xplorer nevű rendszer képes képekben, a terepre vonatkozó adatokban, videókban, szöveges dokumentumokban, PowerPoint-fájlokban stb. helyre, időre, kulcsszavakra vagy összetett módon keresni.

A SOCET GXP szoftvercsomag repülőgépekről és műholdakról készített képek segítségével képes azonosítani és elemezni a megfigyelt terület sajátosságait és ez alapján GEOINT-jelentéseket készíteni. A program képes képek és videók alapján térképeket készíteni, illetve hosszabb idő elteltével tevékenységi mintázatokat felfedni.[610]

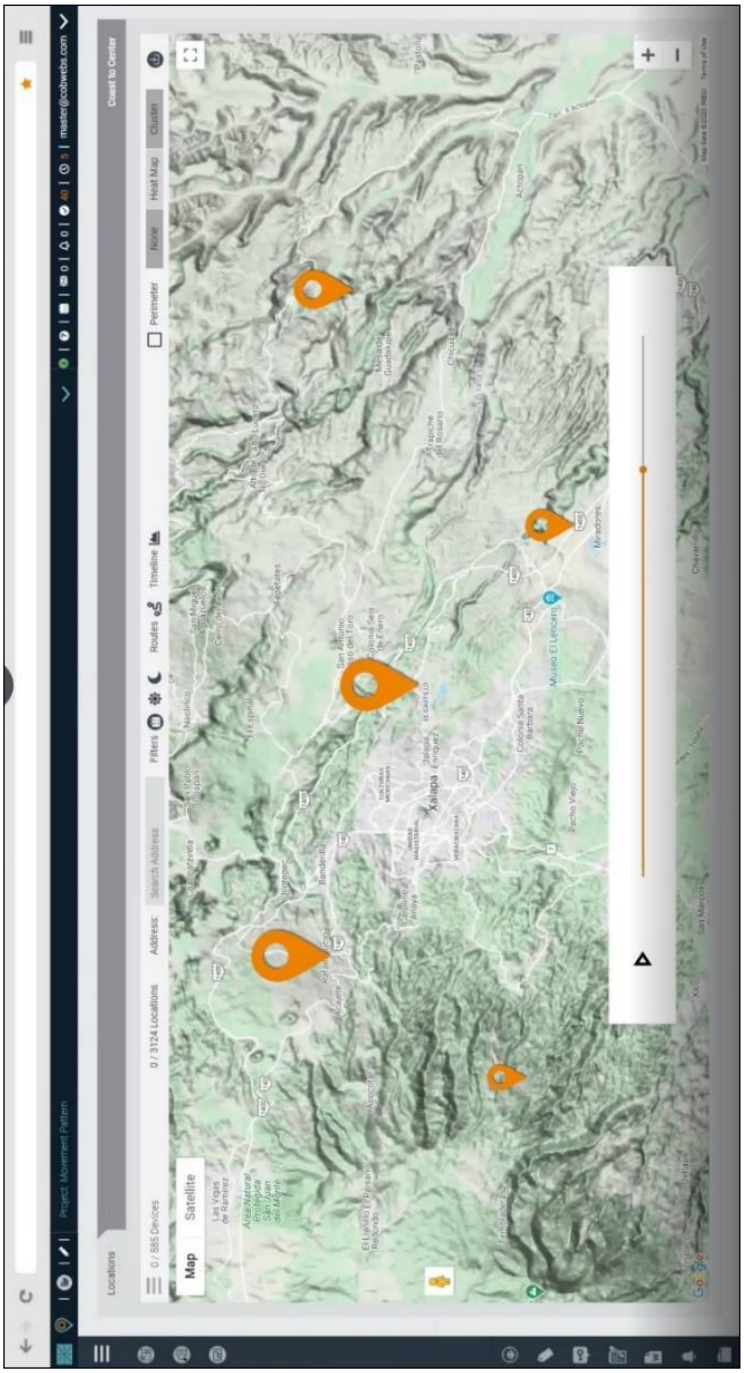
Cobwebs Technologies (Izrael)

A WebLoc a Cobwebs nagyadat-alapú[611] OSINT-alapú térinformatikai hírszerzési platformja. Az elsősorban rendvédelmi, nemzetbiztonsági, határvédelmi, katasztrófa- és járványvédelmi, valamint egészségügyi vészhelyzeti központok számára kifejlesztett rendszer a valós idejű OSINT- és GEOINT-információk, valamint a háttérinformációkat tartalmazó adatbázisok összekötésével generál hozzáadott értéket. A WebLoc interaktív, rétegzett[612] digitális térképekkel és jól áttekinthető felületekkel segíti az információk rendszerezését, megértését és az információalapú döntési folyamatokat.

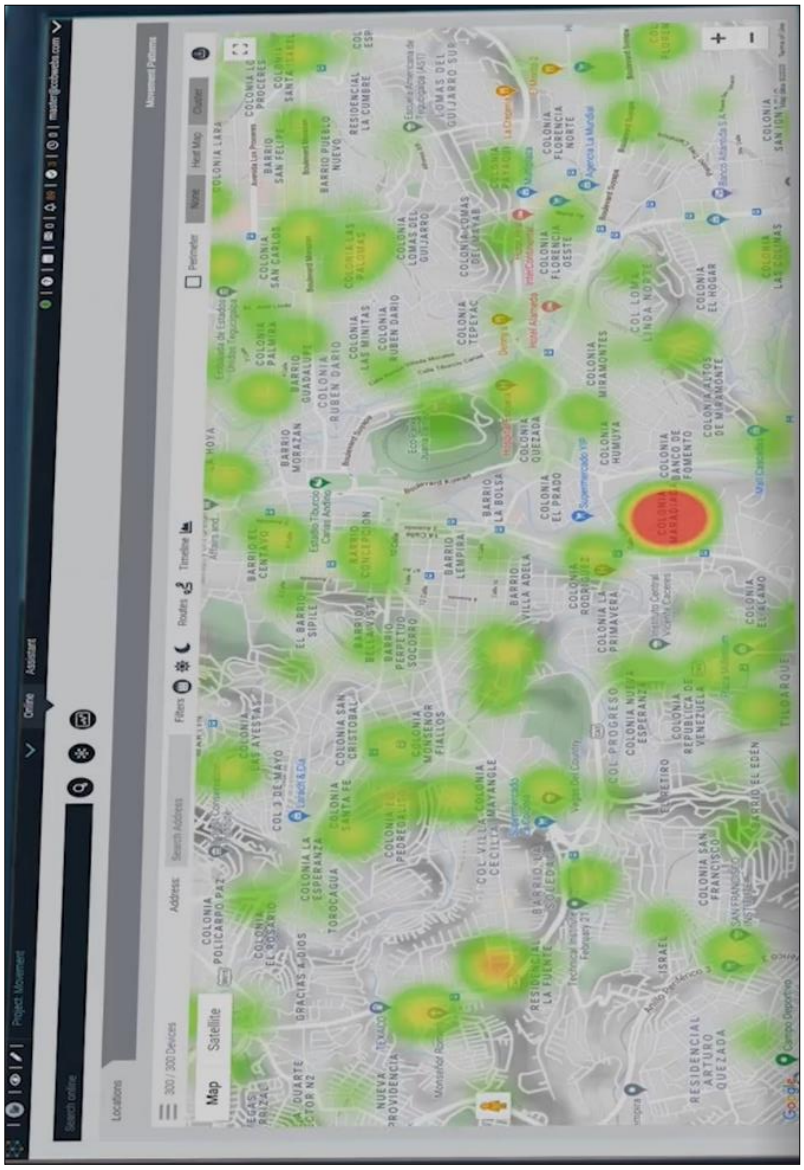
Az OSINT/GEOINT-információk elemzésével mintázatok, trendek és anomáliák mutathatók ki, valamint fenyegetések deríthetők fel. A georeferált és időbélyegzővel ellátott adatok területalapú,[613] idővonalba rendezett (*timelapse*) összevetésével máskülönben rejtett összefüggések is feltárhatók. A rendszer valós időben jeleníti meg a riasztásokat és támogatja a reagálást. A mintázatok segítségével megalkotható a célszemélyek és -szervezetek, -csoportok részletes (demográfiai) profilja, ezáltal előrejelezhetők például a bűncselekmények.

A geoinformációk megjelenítésével a helyszín bejárása nélkül is kialakítható a hely- és helyzetismeret. A rendszer automatikusan képes jelentéseket generálni előre megadott sablonok alapján. Teljes mértékben kompatibilis a cég OSINT-moduljaival.[614]

[610] A BAe Applied Intelligence honlapja: Geospatial Intelligence. https://www.baesystems.com/en-us/product/geospatial-intelligence; letöltés: 2021.07.21.
[611] Több milliárd adatpont kezelésére képes.
[612] Layered.
[613] Georeferált/Geofenced.
[614] A Cobwebs Technologies honlapja. https://cobwebs.com/; letöltés: 2021.07.21.



25. ábra. A georeferált információk térképes, idővonalban (*timelapse*) történő megjelenítése a Cobwebs WebLoc felületén
Location Intelligence System: A Cobwebs Technologies honlapja.
https://cobwebs.com/products/location-intelligence-system/; letöltés: 2021.07.21.



26. ábra. A járványügyi információk térképes megjelenítése a Cobwebs WebLoc felületén
Location Intelligence System: A Cobwebs Technologies honlapja.
https://cobwebs.com/products/location-intelligence-system/; letöltés: 2021.07.21.

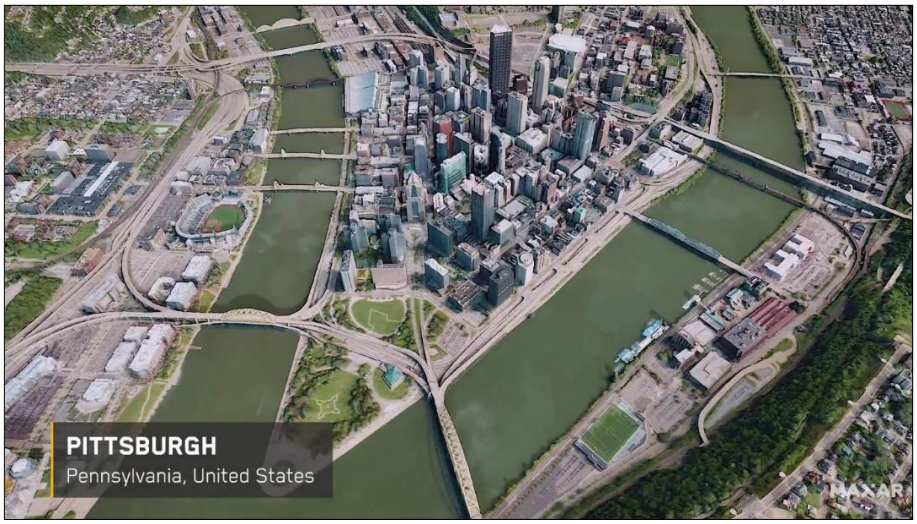
Maxar Technologies (Amerikai Egyesült Államok)

A Maxar űrtechnológiai vállalatcsoport fő profilja műholdak és azok részegységeinek gyártása és üzemeltetése. Az IMINT/GEOINT-üzletág a vállalat saját műholdas képességein alapul.

A Maxar védelmi és hírszerzési GEOINT-üzletága filozófiájának az alapja, hogy a kormányzatok már képtelenek saját forrásból beszerezni a döntéshozók tájékoztatásához szükséges információkat. A Maxar több mint 50 kormányzati partnernek nyújt szolgáltatásokat.

A Maxar legfontosabb kormányzati partnere a Nemzeti Térinformatikai Ügynökség (NGA). Az NGA-nak nyújtott Global Enhanced Geoint Delivery (G-EGD) biztonságos felhőalapú irodai alkalmazásként és válságkörzetekben, illetve katasztrófasújtott területeken is hozzáférhető. A Maxar hozzáférést biztosít a teljes, több milliárd négyzetkilométert lefedő adatbázisához, a legfrissebb felvételek a készítésüket követő két órán belül elérhetők.

A Maxar precíziós térképészeti szolgáltatásai segítségével az 50 cm felbontású, többirányú 3D sztereó műholdképek alapján a Föld teljes felülete interaktívan bejárható és 3D-s térképekké alakítható. A technológia felhasználási területei a várostervezéstől és tereprendezéstől a művelettervezésen és a telekommunikációs rendszerek tervezésén át a valóságnak megfelelő repülőgép-szimulátorokig terjed.



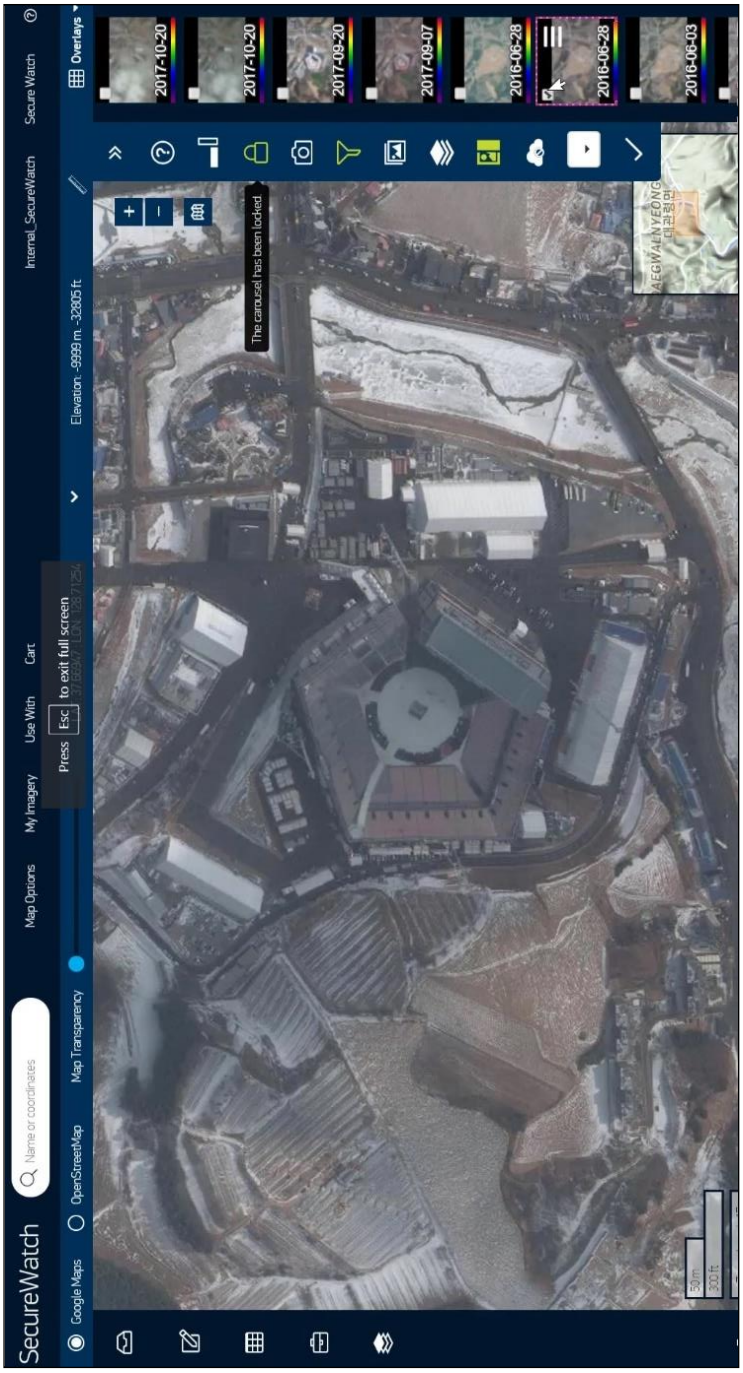
27. ábra. Pittsburgh város élethű, műholdfelvételek alapján készített 3D-s megjelenítése.[615]

[615] A Maxar Technologies honlapja. https://www.maxar.com/; letöltés: 2021.12.22.

28. ábra. A Yosemite Nemzeti Park élethű, műholdfelvételek alapján készített 3D-s megjelenítése.[616]

29. ábra. Műholdfelvételek alapján készített 3D-s térkép felhasználása repülési szimulátorban[617]

[616] A Maxar Technologies honlapja. https://www.maxar.com/; letöltés: 2021.12.22.
[617] Uo.



30. ábra. Változások manuális figyelemmel követése egy meghatározott területen a Maxar SecureWatch felületén
A jobb oldali oszlopban választhatók ki a területről készült korábbi felvételek azok dátuma szerint.
A Maxar Technologies honlapja.
https://www.maxar.com/; letöltés: 2021.12.22.

2021 áprilisában a svéd Saab sikeres teszten demonstrálta a JAS 39E Gripen típusú harci repülőgépnek a Maxar technológiáján alapuló, GPS nélküli navigációs rendszerét. A technológia lényege, hogy a repülőgépen elhelyezett kamera összeveti a repülési útvonal tereptárgyait a Maxar adatbázisával, és ezáltal képes megállapítani a repülőgép pontos térbeli helyét.[618]

A magánszféra számára is elérhető SecureWatch kereskedelmi, felhőalapú GEOINT-szolgáltatás alapja a Maxar 125 petabájtos adatbázisa, amelyben akár 30 cm felbontású felvételek is találhatók, illetve világszinten garantálják az 50 cm felbontást. Az adatbázis 20 évre nyúlik vissza, és naponta hárommillió négyzetkilométernyi új felvétellel egészül ki. A szolgáltatás részeként térképek készítését, automatikus monitorozást és változáskövetést biztosítanak. Az egyszerűen kezelhető interfész segítségével az érdeklődésre számot tartó terület könnyen kijelölhető, a felvételek időpontra és egyéb metaadatok szerint (pl. felhőzet nagysága a felvétel pillanatában, szenzor típusa, felbontás, napszak stb.) szűrhetők. A SecureWatch egyebek mellett navigációs feladatokra, várostervezéshez, illetve vizuális szimulációk készítéséhez is felhasználható.

A Maxar vállalja a megrendelők igénye szerinti GEOINT-jelentések elkészítését is.[619]

Az amerikai vállalat 2021 áprilisában és novemberében is nagy médiavisszhangot kiváltó felvételeket hozott nyilvánosságra az orosz–ukrán határtérségben észlelt orosz katonai csoportosításokról.[620] [621]

Kibervédelem[622]

British Aerospace Applied Intelligence (Egyesült Királyság)

A Cyber Threat Intelligence Service kiberbiztonsági szolgáltatáscsomag a megrendelő régiójára optimalizált információkat biztosít a releváns fenyegetésekről, amelyek az online portálon keresztül akár a kiberbiztonsági esemény időpontjában is lehívhatók, növelve az ellentevékenység hatékonyságát. A BAe nyomon követi a

618 Maxar 3D Data Integrated Into Swedish Gripen Fighter Jet for GPS-Denied Navigation. Maxar Technologies, 2021.10.04. https://blog.maxar.com/earth-intelligence/2021/maxar-3d-data-integrated-into-swedish-gripen-fighter-jet-for-gps-denied-navigation; letöltés: 2021.12.22.

619 A Maxar Technologies honlapja. https://www.maxar.com/; letöltés: 2021.12.22.

620 Satellite images show Russian military buildup along Ukraine border. Reuters, 2021.04.20. https://www.reuters.com/news/picture/satellite-images-show-russian-military-b-idUSRTXBN4Y0; letöltés: 2021.12.22.

621 Russian troops now number 90,000 near Ukraine border after drills, Kyiv says. Reuters, 2021.11.03. https://www.reuters.com/world/ukraine-says-russia-leaves-units-near-its-border-keeps-90000-troops-2021-11-03/; letöltés: 2021.12.22.

622 Nem érhető el nyilvános információ olyan szoftverekről, amelyeket kifejezetten kiberhírszerzési (CYBINT) célokra fejlesztettek ki. Az ilyen eszközök alkalmazása a magánszféra számára illegális, így forgalmazásuk is kizárólag állami megrendelők számára lehetséges. Az ilyen eszközöket zárt szakmai fórumokon és közvetlenül az érdeklődöknek mutatják be, képességeik ipari titoknak minősülnek.

kiberfenyegetést jelentő csoportok és személyek tevékenységét, a céljaikat/ célpontjaikat és az általuk alkalmazott eszközöket és módszereket, folyamatosan frissítve az adatbázist. Segítséget nyújt a hálózatbiztonság magas szinten tartásában is. A kutatási eredményekről néhány naponta elemzést tesznek elérhetővé az ügyfeleiknek, támogatva a fenyegetések nyomon követését végző szakértők munkáját. Külön megrendelésre lehetőség van az elemzések szóbeli prezentációjára és külön vizsgálatok lefolytatására az ügyfelek által kért témakörökben. Az azonosított fenyegetések alapján speciális programkódokat készítenek, megkönnyítve az informatikai rendszerek gyors frissítését és a biztonsági rések megszüntetését. Módszereikkel[623] lehetővé válik a támadók kilétének felderítése is.

A NetReveal a banki csalások megelőzésére és felderítésére szolgál. A rendszer gépitanulás-alapú viselkedésprofilozási és anomália felismerési technikákon alapszik, kiegészítve a BAe saját pénzügyi hírszerzési adatbázisával. Másodpercenként 20 ezer tranzakció biztonságos lebonyolítására képes. A csalásgyanús esetek kivizsgálásában dedikált elemzőmodul nyújt segítséget.[624]

Cognyte[625] (Izrael–Amerikai Egyesült Államok)

A Cognyte kiberfenyegetések elleni rendszere valós időben monitorozza a szervezet informatikai rendszereit, és riaszt a kibertámadások és a kibertéri hírszerzési kísérletek esetén. A biztonsági központ riasztását követően megkezdi a fenyegetés elhárítását és a károk mérséklését.[626] Automatizált elemző és vizsgálati eszközei alkalmasak a támadó és a felderítést végző személy, szervezet azonosítására, így lehetőséget teremtenek az ellentevékenység végrehajtására. A rendszer alapja a kártékony szoftvereket, az ilyen eszközöket alkalmazó szervezeteket és az eljárásokat tartalmazó adatbázis, ami lehetővé teszi a fenyegetések állandó monitorozását.[627]

Gamma Group (Egyesült Királyság)

A Gamma Group kiberbiztonsági szoftveres és konzultációs szolgáltatásai segítségével csökkenthető a védeni kívánt rendszerek sérülékenysége, illetve általa jobb képet kaphatunk a fenyegetések természetéről.

A cég a következő területeken támogatja a kiberbiztonságot:

- hálózatbiztonsági elemzés;
- a fenyegetések feltérképezése;

[623] A kártékony programok működési elvének visszafejtése (*reverse engineering*) és az infrastruktúra pivotálása (*infrastructure pivoting*: az ismert indikátorok alapján az elkövető azonosítását lehetővé tevő elemzési eljárás).

[624] A BAe Applied Intelligence honlapja. https://www.baesystems.com/en/cybersecurity/home; letöltés: 2021.07.21.

[625] A Verint egykori hírszerzési részlege.

[626] Mitigation.

[627] A Cognyte honlapja. https://www.cognyte.com; letöltés: 2021.07.21.

- rendszerek és hálózatok behatolási tesztelése;
- szoftverek sérülékenységének vizsgálata;
- biztonsági műveleti központok létesítése, minősítése;
- informatikai éberségi, kiberbiztonsági szakértői képzések.[628]

MASINT

A mérés és jelmeghatározó hírszerzés (MASINT[629]) fejlődését továbbra is az egyre korszerűbb haditechnikai eszközök és rejtési technológiák rendszerbe állítása, valamint a tömegpusztító fegyverek proliferációja mozdítja előre. A már szolgálatban álló és a következő évtizedekben megjelenő, minden korábbinál gyorsabb és pontosabb fegyverrendszerek miatt a fejlett haderők számára kulcsfontosságú, hogy az ellenséges eszközöket a lehető legtávolabbról érzékelhessék. Ezen a téren a technikai hírszerzés, ezen belül a MASINT szerepe folyamatosan növekszik. A különböző MASINT-eszközök működését a szenzorok fejlődése mellett a számítástechnikai kapacitások bővülése is javítja, ezáltal bő évtizedes távlatban reálissá válhat az ellenséges erők helyzetének valós idejű követése.[630]

A MASINT jövőbeli fejlődését is meghatározza, hogy az általa szolgáltatott információk elsősorban nem önmagukban, hanem az összadatforrású hírszerzés részeként értékesek. Az új szenzortechnológiák vonatkozásában az várható, hogy azok az elektromágneses spektrum eddig nem kiaknázott tartományaiban is képesek lesznek információt gyűjteni. Ennek előnye, hogy az ilyen kibocsátásokat egyelőre a legfejlettebb haditechnikai eszközök esetében sem rejtik. A hírszerzési ág fontos szerepet kap az új eszközök felfedezésében, azok jellemzőinek felderítésében, különösen azokban az esetekben, amikor más forrásból nem, vagy csak korlátozott mértékben áll rendelkezésre információ.[631] Az egyéb területekhez hasonlóan a jövőben magánvállalatok is MASINT-képességek birtokába juthatnak, ami elsősorban az űripar fejlődéséhez járul majd hozzá.[632]

---

628 A Gamma Group honlapja: Products & Services. https://www.gammagroup.com/ProductsServices.aspx?m=p; letöltés: 2021.07.21.

629 Measurement and Signature Intelligence.

630 KAMARA, Hassan M.: Hunting the Adversary – Sensors in the 2035 Battlespace. Military Review – The Professional Journal of the U.S. Army, January-February 2021. pp. 34–41. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Kamara-Hunting-the-Adversary-1.pdf; letöltés: 2021.12.23.

631 Multi-disciplinary Intelligence Analyst – Measurement and Signature Intelligence (MASINT) provides real-time analysis and dissemination to facilitate your Collection Strategy. AUC3I. https://www.auc3i.com/index-114.php; letöltés: 2021.12.23.

632 REDING, D. F. – EATON, J.: Science & Technology Trends 2020-2040. Exploring the S&T Edge. NATO Science & Technology Organization, 2020. p. 78. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf; letöltés: 2021.12.23.

Az elmúlt időszakban nyilvánosságra hozott információk szerint az amerikai haderő több fő MASINT-rendszerét tervezi korszerűsíteni vagy leváltani. Az űrerő új, műholdakra telepített, ballisztikusrakéta-indítást észlelő és követő infravörös rendszert[633] fejleszt. Az első új műhold indítása 2025-re, az első öt, Block0 típusú műholdból álló konstelláció hadrendbe állítása 2030-ig várható. A haderőnem az új típusú rakéták megjelenésével indokolta a fejlesztést. A műholdrendszerhez kapcsolódóan új földi irányítórendszert[634] is kialakítanak, amelynek moduláris technológián alapuló informatikai infrastruktúrája magas szintű kibervédelem mellett lesz képes a műholdaktól származó adatok feldolgozására. A központ egyben az infravörös tartományban működő új generációs felderítési technológiák és az adatfeldolgozásban alkalmazott új szoftverek és algoritmusok tesztelésére és integrálására is alkalmas lesz.[635]

2020 áprilisában az amerikai Haditengerészeti Hírszerzési Hivatal 90 millió dolláros, öt évre szóló szerződést kötött a Lockheed hadiipari vállalattal a szolgálat globális akusztikus hírszerzési rendszerének korszerűsítésére.[636]

633 Next-Generation Overhead Persistent Infrared.

634 Future Operationally Resilient Ground Evolution – FORGE.

635 HARPER, Jon: Space Force Has High Hopes for New Missile Warning Satellites. National Defense, 2021.07.16. https://www.nationaldefensemagazine.org/articles/2021/7/16/space-force-has-high-hopes-for-new-missile-warning-satellites; letöltés: 2021.12.23.

636 NELSON, Matthew: Lockheed to Update Navy MASINT Platform Under Potential $90M Contract. GovCon Wire, 2020.04.07. https://www.govconwire.com/2020/04/lockheed-to-update-navy-masint-platform-under-potential-90m-contract/; letöltés: 2021.12.23.

A MESTERSÉGES INTELLIGENCIA NEMZETBIZTONSÁGI ELEMZŐ-ÉRTÉKELŐ ALKALMAZÁSI LEHETŐSÉGEI

Elemző-értékelő fúziós szoftverek – a Center for Resilient Communities stratégiai hírszerző keretrendszere

A hírszerzés önálló ágaihoz hasonlóan az elemzés-értékelés területén is specializált szoftverrendszerek állnak rendelkezésre. A különböző megoldások fő, egymással gyakran összefüggő funkciói az információ nagy adat alapján végzett, összadatforrású elemzést-értékelést támogató fúziója, a feladatmenedzsment, illetve az adattárházak kialakítása és működtetése.

Dr. Lilian Alessa, az Idahói Egyetem CRC kutatóközpontjának[637] igazgatója *Emberekre támaszkodva: A mesterséges intelligencia sikere vagy bukása az emberi tényezőn múlik*[638] című előadásában kifejtette, hogy az MI nemzetbiztonsági alkalmazásával szemben támasztott reményeknek elsősorban a rádióelektronikai felderítés (SIGINT), a képi hírszerzés (IMINT) és a geoinformációs/térinformatikai hírszerzés (GEOINT) terén elért eredmények adnak alapot. A komplex, strukturálatlan adatvagyonon alapuló, nem technikai területeken ugyanakkor az MI-eszközök felhasználása kevésbé volt sikeres. Ennek fő oka az emberi tényezőben keresendő. Az egyetlen megoldást az elemzők gépi kiegészítése (augmentációja) jelenti, vagyis olyan szoftveres környezetet kell biztosítani a számukra, amely hatékonyan és integráltan támogatja a tevékenységüket.

Az új megközelítés alapfeltételeként olyan keretrendszerre van szükség, amelyben a hírszerzési ciklus valamennyi résztvevője: műveleti tisztek, elemző-értékelők, témaszakértők, vezetők és döntéshozók részt vesznek a kulcsfontosságú indikátorok, vagyis a veszélytényezők kialakulására vagy erősödésére utaló jelek meghatározásában, valamint a fontossági sorrendek felállításában. Az indikátorlista folyamatos karbantartása ahhoz is hozzájárul, hogy az emberek a mesterséges intelligencián alapuló, egyre inkább az automatizálás irányába elmozduló hírszerzési folyamatok középpontjában maradhassanak – azok fő hajtóerejeként.

A hírszerzés adatökoszisztémájának menedzselésére új szakértői csoport, az úgynevezett „*rule manager*ek" kialakítása szükséges. Az ilyen, a hírszerzés rendszerében is jártas adatmenedzserek[639] feladata az adatforrások (adatbázisok),

---

637 A 2014-ben alapított Center for Resilient Communities társadalmi-ökológiai interdiszciplináris kutatásokat végez. Az amerikai Hírszerző Közösség figyelmét elsősorban a rendszertudomány gyakorlati alkalmazásában elért eredmények kelthették fel.

638 ALESSA, Lilian: Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.30.

639 Dr. Alessa szerint a hírszerzés által foglalkoztatott valamennyi szakértő vonatkozásában kiemelten fontos, hogy szorosan a hírszerzés rendszeréhez kapcsolódjanak, mert másképpen nem tudják hasznosítani a tudásukat.

valamint a döntéshozók és az elemző-értékelők információigényének számon tartása, az indikátorlisták karbantartása. Az adatmenedzserek képesek közvetítőként is fellépni az elemző-értékelők és a technikai adatszerzők között az adatszerzők számára testre szabott információigények (gyűjtési igények) megfogalmazásával. Emellett részt vehetnek az elemző-értékelő forgatókönyvek felvázolásában, az új, kialakulóban lévő fenyegetések felfedésében, valamint az adat és az információ vizualizációjában.

Dr. Alessa mondandójának alátámasztására bemutatta az általa vezetett kutatócsoport fejlesztésében létrehozott nagyadat-alapú Stratégiai Hírszerző Keretrendszer[640] elnevezésű adatfúziós rendszer MOSAIC[641] elnevezésű vizualizációs modulját. A 2017 óta 400 szakértő bevonásával fejlesztett MOSAIC a rendelkezésre álló adat térben és időben történő megjelenítésére szolgáló GEOINT-rendszer, amelynek segítségével a vizsgált entitás, jelenség vagy folyamat vizuális (térképes) megjelenítése térben és időben tetszés szerint változtatható. Az időfaktor bizonyos határokon belül a jövőbe is kitolható, lehetővé téve előrejelzések és forgatókönyvek készítését. A MOSAIC fő erőssége éppen a rejtett trendek felfedésében, az előrejelző hírszerzés hatékony támogatásában áll.

A hírszerző szolgálatok és a szervezeti egységek egymástól elkülönített adatbázisai,[642] illetve a betekintési jogosultsági csoportok és szintek jelentette nehézséget azzal küszöbölik ki, hogy a keretrendszer algoritmusainak több verziója fut párhuzamosan az adatbázisokban. A megfelelő betekintési jogosultsággal rendelkező szervezeti egységek információigényeire az algoritmusok által összegyűjtött válaszok valós időben a kormányzati felhőben mozognak.

A MOSAIC három, egymással párhuzamosan futtatott úgynevezett genetikus algoritmuson alapul.[643] A nyílt információk és a rendvédelmi adatbázisok feldolgozásán alapuló projektek egyikének eredményeképpen sikerült eddig nem detektált, alacsony láthatóságú illegális tevékenységeket felderíteni az alaszkai határszakaszon, majd azok ellen hatósági intézkedéseket kezdeményezni. Egy másik projekt olyan indikátorokat detektált amerikai belterületen, amelyek a hadszíntér ellenséges műveleti előkészítésére[644] utalnak. A kutatás által biztosított információk (nem részletezett területeken) megváltoztatták az amerikai vezetés egyes politikáit.

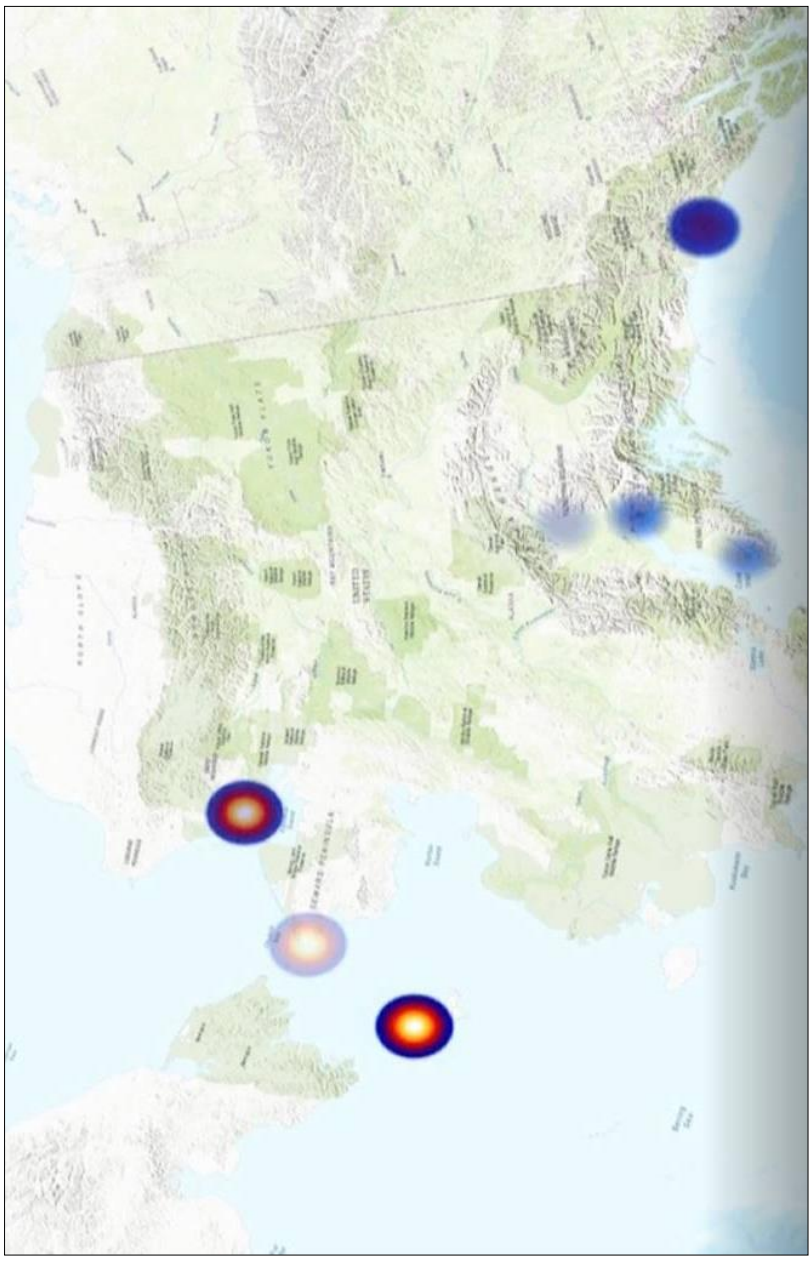
640 Strategic Intelligence Framework.

641 Massive-scale Operational Structural Awareness Intelligence Composite.

642 Az előadó érzékletesen „adatbörtönnek” nevezi az ilyen adatbázisokat.

643 Ezek a keresőszoftverek képesek a biológiai evolúcióhoz hasonló kiválasztódással fejlődni a feladatok végrehajtása során. Az ilyen algoritmusok speciális verziója, az úgynevezett „Evolutionary Generative Adversarial Networks” esetében a fejlesztők egymással versengő algoritmusokat hoznak létre. Erre példa két algoritmus, amelyek egyikének feladata nem létező személyekről fotókat hamisítani, a másiké pedig a hamisítványokat felfedezni. A számítástechnikai adatfeldolgozó képesség a 2010-es évtized közepére jutott el arra a szintre, hogy az 1960-as évek óta fejlesztett genetikus algoritmusok gyakorlati feladatok megoldásához is felhasználhatók legyenek.

644 Operational Preparation of the Battlespace – OPIB.



31. ábra. A MOSAIC adatvizualizációs felülete

ALESSA, Lilian: Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020. október 30.

Dr. Alessa megjegyezte, hogy a hatalmas adatmennyiség miatt a nyílt adatbázisokban futtatott algoritmusok sokkal pontosabb és szélesebb körű eredményeket hoznak, mint a minősített rendszereken kereső társaik.

Az adatbázisok tekintetében elmondta, hogy azok mozgatása nem tanácsos. Az adatok másolása költséges, lassú, sérülékenységet és veszteségeket okoz. Ehelyett a kereső algoritmusokat kell „az adatokhoz mozgatni", tehát olyan megoldásokra van szükség, amelyek a meglévő szervereken alkalmazhatók. Az adatok tisztítását, ezáltal megbízhatóságuk növelését szintén erre specializált algoritmusokkal célszerű megoldani. Nem létezik „elavult adat", tehát mindent tárolni kell, de az archiválást ellenzi, mert az archivált adatokat valójában nem lehet felhasználni.

Az elemzés-értékeléshez használt szoftverek esetében kizárólag a keretrendszer egységesíthető, míg a különböző részfeladatok összessége célszoftverek sokaságával hajtható végre.

Az elemzés-értékelés MI általi fejlesztéséhez elengedhetetlen a bőséges számítástechnikai kapacitás és a magas szintű algoritmusok megléte, de a kulcs a képzett munkaerőben és a nemzetbiztonsági szolgálatok szervezeti kultúrájának megváltoztatásában keresendő. Dr. Alessa megfogalmazásában a nemzetbiztonsági kultúra változtatása ahhoz hasonlatos, mintha megpróbálnánk egy vízcseppet rávenni, hogy „*felfelé folyjék a hegyen*". Ez csak a hegy dőlésszögének megváltoztatásával lehetséges!

Dr. Alessa elmondta, hogy a MOSAIC fejlesztésében részt vevő szakértők többsége olyan nemzetbiztonsági munkatárs, akik új megoldásokat keresnek és arra jutottak, hogy erre csak a tudományos életben van lehetőségük, a szolgálatoknál nem. A különböző szolgálatok munkatársainak együttműködésére szintén csak így nyílik valós lehetőség.

Airbus Joint ISR (Európa)

Az Airbus a Fortion ISR-szoftverrendszer részeként a hírszerzési cikluson belül a hírszerzési folyamat tervezésének, illetve az elemzett-értékelt információk elosztásának támogatására dedikált modulokat fejlesztett Workflow, illetve CSD néven.

A Fortion Workflow fejlesztésekor alapvető szempont volt, hogy a rendszer megfeleljen a NATO adatgyűjtés-koordináló és felderítésikövetelmények-menedzsment (IRM & CM) doktrína[645] követelményeinek, továbbá alkalmas legyen a szervezetek közötti munkafolyamatok összehangolására is. Segítségével a hírszerzés önálló ágainak információszerző és információfeldolgozó tevékenysége

[645] NATO - STANAG 6524 (Restricted): Intelligence Requirement Management and Collection Management – AIntP-16 Edition A: a NATO jelenleg hatályos, korlátozott terjesztésű minősítésű dokumentumát 2018. december 17-én adták ki.

folyamatosan figyelemmel kísérhető annak érdekében, hogy a szervezethez beérkező információigények időben, a döntéshozókat érdemben támogató módon megválaszolásra kerüljenek. A rendszer képes az információigényeket priorizálni, és azok alapján feladatot szab a hírszerző szervezetek számára. A folyamat részeként megállapítja, hogy az információt mely hírszerzési ágak képesek beszerezni, majd az információigényeket lefordítja a feladat végrehajtásába bevont hírszerzési ágak nyelvére.

A Fortion CSD[646] a hírszerzési/felderítési információk biztonságos tárolására, kinyerésére és megosztására szolgáló szoftvermodul. A Worflow-hoz hasonlóan alkalmas a szervezeti egységek és a szervezetek közötti munka- és információmegosztás speciális követelményeinek is megfelelni. Az információ széles körű megjelenési formáit kezeli (pl. képek, dokumentumok, vektorfájlok, videofelvételek és élő videostreamek, földi mozgó célok felderítése, valamint az IRM & CM munkafolyamat fájljai).[647]

Az Intelligence for Decision (I4D) szoftver az önálló hírszerzési ágak információinak fúziójára szolgál. Az információk egységes megjelenítése térinformatikai alapú, az információk elemzése térben és időben zajlik.[648]

British Aerospace Applied Intelligence (Egyesült Királyság)

A LEXI[649] fúziós rendszer segítségével az összadatforrású információk egy képernyőn érhetők el, vizualizálhatók, rendszerezhetők és elemezhetők, akár közel valós időben is. Az interfész könnyen tanulható és kezelhető. A fúziós algoritmusok összevetik a GEOINT-, SIGINT-, PAI- és más strukturált, részben strukturált vagy strukturálatlan információkat, és akár valós időben is lehetővé teszik a célpontok követését és monitorozását. A LEXI kollaborációs lehetőségekkel is rendelkezik, és támogatja a sztenderdizált munkafolyamatokat. A rendszer által kezelt információ megosztható a rendszeren belül vagy exportálható. A rendszer a BAe többi termékéhez hasonlóan felhőalapú és könnyen a felhasználói igényekre szabható. Van lehetőség arra is, hogy a rendszert offline módon alkalmazzák. A műveleti területen dolgozók számára is lehetőség van az adatbázis részéhez vagy egészéhez történő hozzáférésre offline módon is hordozható eszköz (tablet) segítségével, illetve a műveleti területen megszerzett és feldolgozott információk is szinkronizálhatók a központi rendszerrel. A LEXI-t úgy tervezték, hogy az új technológiák (pl. gépi tanulási algoritmusok) könnyen integrálhatók legyenek a meglévő rendszerbe. Könnyen cserélhetők, módosíthatók a rendszer alapját képező adatbáz

646 Coalition Shared Dataserver (szövetségi megosztott adatszerver).
647 Artefact.
648 Az Airbus JOINT ISR honlapja. https://www.intelligence-airbusds.com/markets/defence/joint-isr/; letöltés: 2021.12.20.
649 Lead Exploitation Intelligence.

32. ábra. A LEXI használata hordozható eszközzel[650]

Cognyte (Izrael–Amerikai Egyesült Államok)

A Cognyte elemző-értékelő fúziós rendszerei képesek a hírszerző, illetve az elemző-értékelő ciklusnak megfelelő feladatok integrált, felhasználóbarát végrehajtására. A nagyadat-alapú hírszerző (elemző-értékelő) fúziós és feladatmenedzsment-rendszer nagyban javítja a szervezet számára rendelkezésre álló információ feldolgozását és az adatszerző erőforrások kihasználását. A modullal lehetővé válik az összadatforrású információ hatékony kezelése és fúziója, az adatszerzőknek adott feladatszabás, a felhasználók közötti – csetalapú – kommunikáció, az adatok hatékony és egységes formátumú megosztása, több szempont szerinti elemzése és értékelése, valamint a különböző jelentéstípusok – az adminisztráció (szerkesztő, források, minősítés stb.), illetve az alaki kellékek szempontjából félautomatikus – szerkesztése. Az elemzők által kijelölt információ egyszerűen (*drag and drop* módon) beilleszthető a rendszeresített jelentéssablonokba.

A rendszer elemei közötti összeköttetés (ideértve a műveleti terület számítógépeit is) webalapú, védett összeköttetésen keresztül biztosított, lehetővé téve nemcsak a szervezeti egységek, de a műveleti területen tartózkodó adatszerzők integrált működését is.

A rendszer felhasználóbarát módon, informatikai képzettség nélkül használható. A mesterséges intelligencia segítségével lehetővé teszi a különféle fájlformátumokban – akár strukturálatlanul – rendelkezésre álló nagy mennyiségű információ a hagyományos módszerekkel összehasonlítva jóval hatékonyabb feldolgozását. Megoldást nyújt az egymástól a szervezeti kultúra, a belső szabályzók és a bürokratikus akadályok, valamint

[650] Electronic Systems – What's on show? Farnborough International Airshow 2018. Find out more about the Electonic Systems products on show this year. BAe Systems, 2018.07.23. https://www.baesystems.com/cs/Satellite?c=BAEStandardArticle_C&childpagename=UK%2FBAELayout&cid=1434614801231&pagename=UKWrapper; letöltés: 2021.07.22.

a „*need to know*” elve miatt elzárt rendszerek, szervezetek, a sokféle fájlformátum, a nyers médiatartalmak (videó, hangfelvételek) és a nyelvi gátak jelentette kihívásokra. A rendszer lehetővé teszi a célpontok (témakörök) közel valós idejű elemzését, a rejtett összefüggések (hálózatok) feltárását.

A fúziós rendszer a bekerült információt automatikusan strukturálja (kategóriákba szervezi) és elemzi, kinyerve és csoportosítva az entitásokat (szervezetek, személyek stb.), a földrajzi helyeket, a dátumokat, és azokat hálózatba rendezi. A strukturálatlan és a különféle formátumokban meglévő információt így automatikusan, sztenderdizált módon strukturálja, azokból könnyen kezelhető adatbázist épít. A felhasználó kérésére a szükséges információkat jól áttekinthető, egyoldalas adatvizuálizációs felületen (*dashboard*on) jeleníti meg. A szoftvernek számos hasznos funkciója van, például a szövegekből kinyert földrajzi egységeket képes térképen megjeleníteni. A valós entitások rendszerezéséhez az IBM Analysts' Notebook hálózatelemző szoftver alapfunkcióihoz hasonló képességű, de annál jóval egyszerűbben használható, beépített vizuális kapcsolatelemző megoldással rendelkezik.

A kinyert entitásokat a rendszer „adategységként” kezeli és metaadatokat (pl. információ megszerzésének ideje, forrása stb.) kapcsol hozzájuk, majd azokat valós, a felhasználó által meghatározott entitásokhoz köti. Az entitások kijelölésének alapja lehet a szervezethez beérkező feladat, a szervezet saját adatbázisa (pl. célszemélyek) és egyéb, például a kutatás, elemzés-értékelés során látkörbe került entitások. Az entitások esetében külön kategóriát képez a rendszer által kinyert entitás (adategység) és a felhasználó által meghatározott, az információ csoportosítása szempontjából mérvadó valós entitás.

Az adategységeket a rendszer valós entitásokhoz rendeli, majd az egymással összefüggő – például egy feladathoz kapcsolódó – entitásokat úgynevezett konténerekbe rendszerezi. Az információ e művelet során bármely ponton, tetszőlegesen rendszerezhető és manipulálható, kiegészíthető. A rendszer elemző-értékelő funkciói félautomatikusnak tekinthetők, hiszen elsősorban az információ rendszerezésében, átlátható megjelenítésében segít, másrészt a valós entitások közötti lehetséges kapcsolódásokat mutatja be. Mind az entitáskinyerés, mind a fordítások minősége nagyban fejleszthető a rendszer felhasználók általi tanításával.

Az automatikusan feldolgozott információ strukturálása a felhasználó által meghatározott módon történik. Ennek elsődleges módja az úgynevezett „lekérdezés” (*query*), ami valójában inkább egyedi rendszerezést jelent. Ez az alapja például a feladat értelmezése és a tájékoztatók készítése során az adott témában a rendelkezésre álló információ kigyűjtésének és átlátható formájú megjelenítésének. A lekérdezés kétlépcsős: a rendelkezésre álló információ szűrése után (pl. ország, témakör, tárgykör) összetett keresések hajthatók végre.

A rendszer az adatbázisban szereplő szöveget, képi, video- és audioinformációt entitáskinyeréssel, gépi látással és a természetes nyelvek feldolgozásával értelmezi, rendszerezi, elemzi. Képes a képeken, videókon logókat, írást (pl. falra/molinóra írt arab írást), személyeket, fegyvereket felismerni, videókon helyzeteket (pl. erőszakos esemény vagy orvosi vészhelyzet) felismerni. Az audioanyagokat a rendelkezésre álló nyelvekről automatikusan fordítja angolra és angolul feliratozza.

A rendszer feladatmenedzsment-lehetőségei nagyban megkönnyítik az elemző-értékelők egymás közti és az adatszerzőkkel folytatott együttműködését. Az elemző-értékelők könnyen összeállíthatnak olyan információs csomagokat, amelyekkel támogathatják a műveleti/adatszerző tevékenységet, megkönnyítve az RFI-k megválaszolását, illetve – amennyiben hozzáférnek a rendszerhez – az adatszerzők maguk is könnyen tájékozódhatnak a rendszer segítségével. A modul nagyban megkönnyíti a feladatszabást, mert lehetővé teszi a vezetők számára a végrehajtók kijelölését, a munkacsoportok felállítását és a feladatok leosztását. A felhasználók csetablakon, belső e-mailen és élőszóban is kapcsolatban állhatnak.

A rendszer felhasználóbarát módon, informatikai képzettség nélkül használható. A mesterséges intelligencia segítségével lehetővé teszi a különféle fájlformátumokban – akár strukturálatlanul – rendelkezésre álló nagy mennyiségű információ a hagyományos módszerekkel összehasonlítva jóval hatékonyabb feldolgozását.

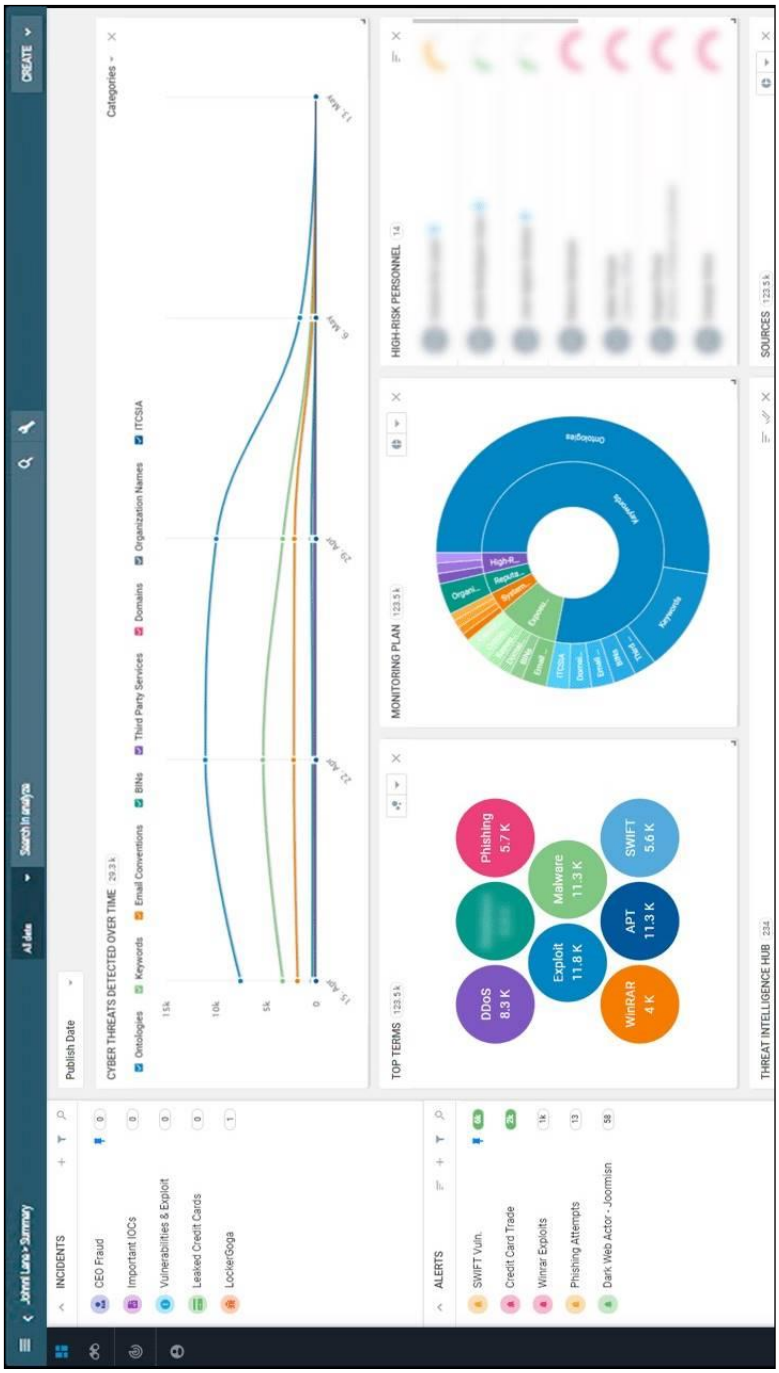
A Cognyte célja a fejlesztés során az volt, hogy a szoftvert a megrendelő nemzetbiztonsági szolgálatok és rendvédelmi szervezetek saját belső hálózataikon, saját szakembereikkel legyenek képesek használni. A program működéséhez nem szükséges, hogy kapcsolatban álljon a cég saját szervereivel. A rendszer védett hálózatként, tűzfallal, kibervédelemmel ellátva, adatdióda (egyoldalú, csak befelé irányuló információáramlassal) vagy az internetről teljesen elzárva (az információ ilyenkor például pendrive-val áramlik) működtethető. A rendszert arra tervezték, hogy az összadatforrású hírszerzés minden ágától, illetve a nemzeti adatbázisokból (telefontársaságok, rendőrség, lakossági nyilvántartás, határátkelők, repülőterek stb.) is képes legyen információt fogadni és azt feldolgozni. Az információáramlás lehet automatikus, alapulhat információkérelmen[651] vagy kézi feltöltésen.

A rendszer képes az összetett, a felhasználó szervezet által meghatározott, személyre szabható biztonsági mátrixok kezelésére a betekintési jogosultságok menedzselése érdekében. A mátrixok három alapeleme a forrás, a minősítés és a feladat („ügy"). Ezek kombinációjával (pl. szigorúan titkos betekintési jogosultsággal rendelkező felhasználó nem láthat egy adott ügydarabot vagy ügyet stb.) magas szinten érvényesíthető a „*need to know*" elv.

A rendszer karbantartásához adatmenedzserekre van szükség. A mindennapi üzemeltetés alapja az úgynevezett „adatmodell-stúdió", amely lehetővé teszi, hogy mély informatikai tudás nélküli adatmenedzserek a rendszert a felhasználó szervezet igényeihez szabják. Itt zajlik annak meghatározása, hogy a szervezet például milyen metaadatokat rendel a személyekhez, mit ért „szervezet" alatt, milyen szervezeteket különböztet meg (pl. szárazföldi haderő, légierő, vezérkar, hadosztály stb.). Az adatmodell-stúdió a gépi tanulás alapmozzanatának tekinthető.[652]

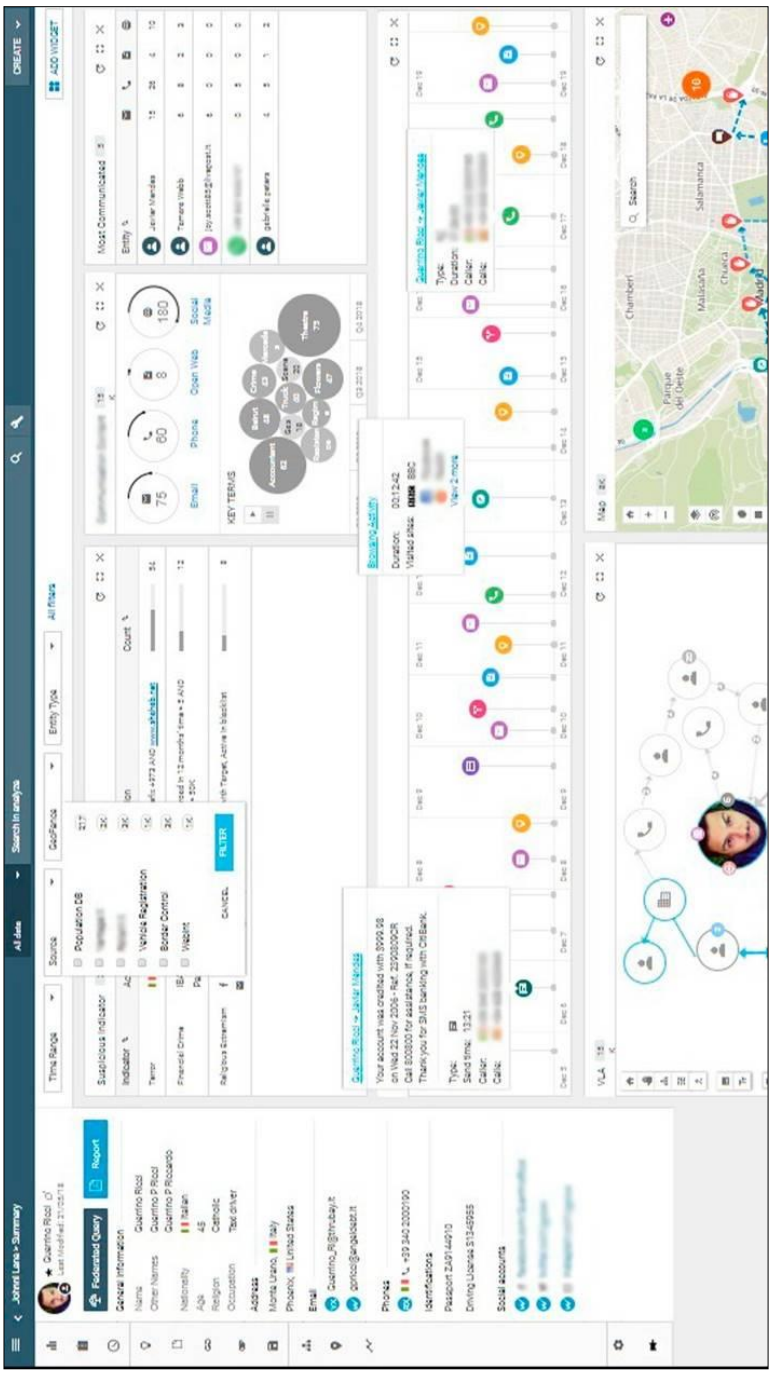
[651] Külső lekérdezés (*federated query*).
[652] A Cognyte honlapja.
https://www.cognyte.com; letöltés: 2021.07.21.

33. ábra. A Cognyte fúziós moduljának áttekintő nézete
A Cognyte honlapja.
https://www.cognyte.com; letöltés: 2021.07.21.



34. ábra. A Cognyte füziós modulján pénzügyi hírszerzési és kiberfényegetésekkel kapcsolatos információk láthatók
A Cognyte honlapja.
https://www.cognyte.com; letöltés: 2021.07.21.

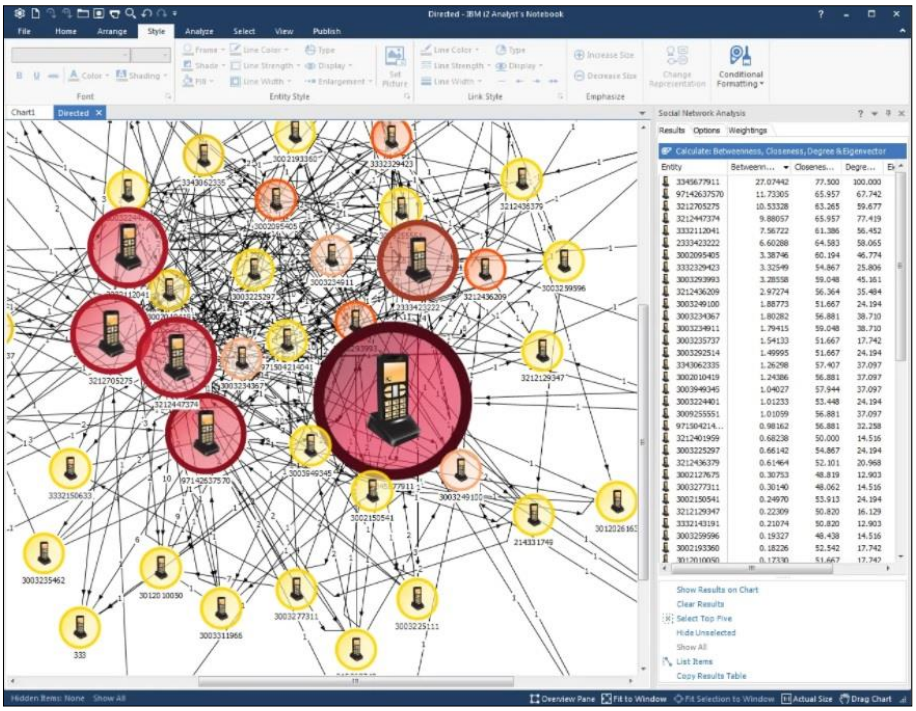
35. ábra. Egy célszemély profiladatai a Cognyte fúziós modulján
A Cognyte honlapja.
https://www.cognyte.com; letöltés: 2021.07.21.



36. ábra. Egy célszemély profiladatai a Cognyte fúziós moduljának adatvizualizációs felületén
A Cognyte honlapja.
https://www.cognyte.com; letöltés: 2021.07.21.

IBM (Amerikai Egyesült Államok)

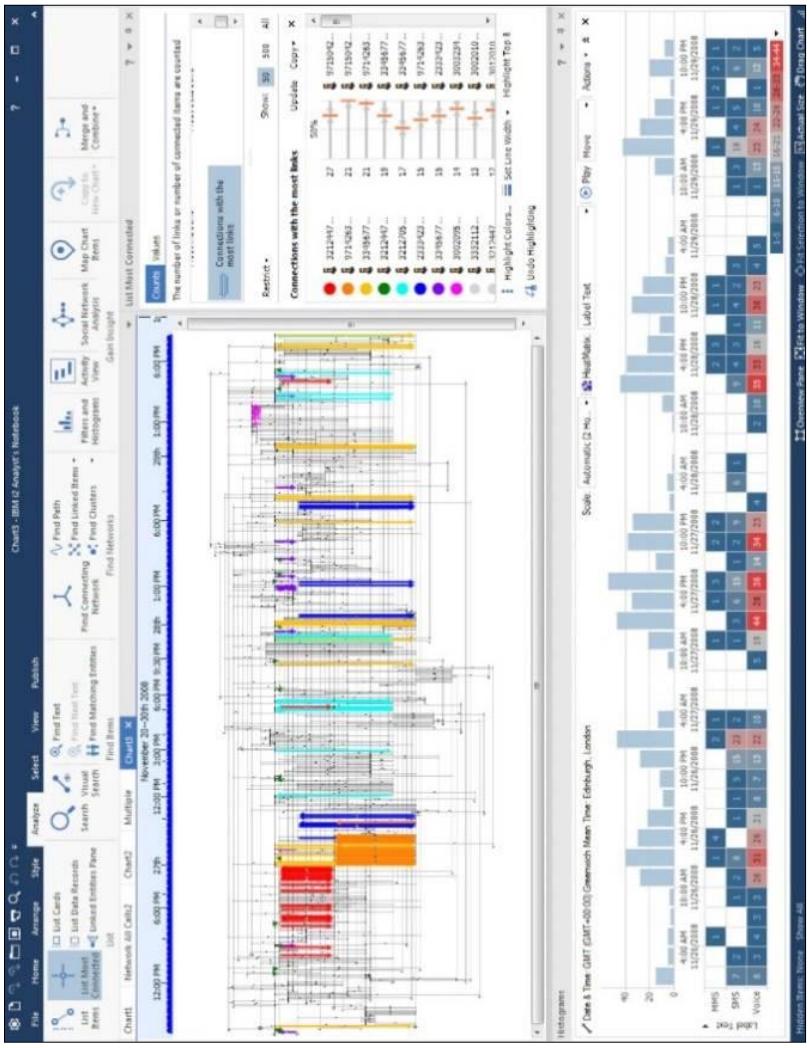
Az IBM Security i2 Analyst's Notebook nevű hálózatelemző szoftver a kategóriájában kiemelkedő képességekkel rendelkezik. Versenytársaihoz hasonlóan elsődleges célja, hogy a bevitt entitások (személyek, csoportok és szervezetek) metaadatai alapján vizualizálja a közöttük fennálló kapcsolatot és annak jellegét, ezáltal más módon feltárhatatlan következtetésekhez segítve az elemzőket. A megjelenítési módok között a hagyományos kapcsolati hálózatelemzési felület mellett földrajzi és időbeli kapcsolatokat, illetve idősorrendet is meg tud jeleníteni, valamint statisztikákat képes készíteni. Fejlett közösségi hálózatelemzési algoritmusai segítenek a csoportokon belüli dinamikák, hierarchiák, a vezetők és az eljárások felderítésében. A szoftvercsomag ára felhasználónként 9274 euró.[653]



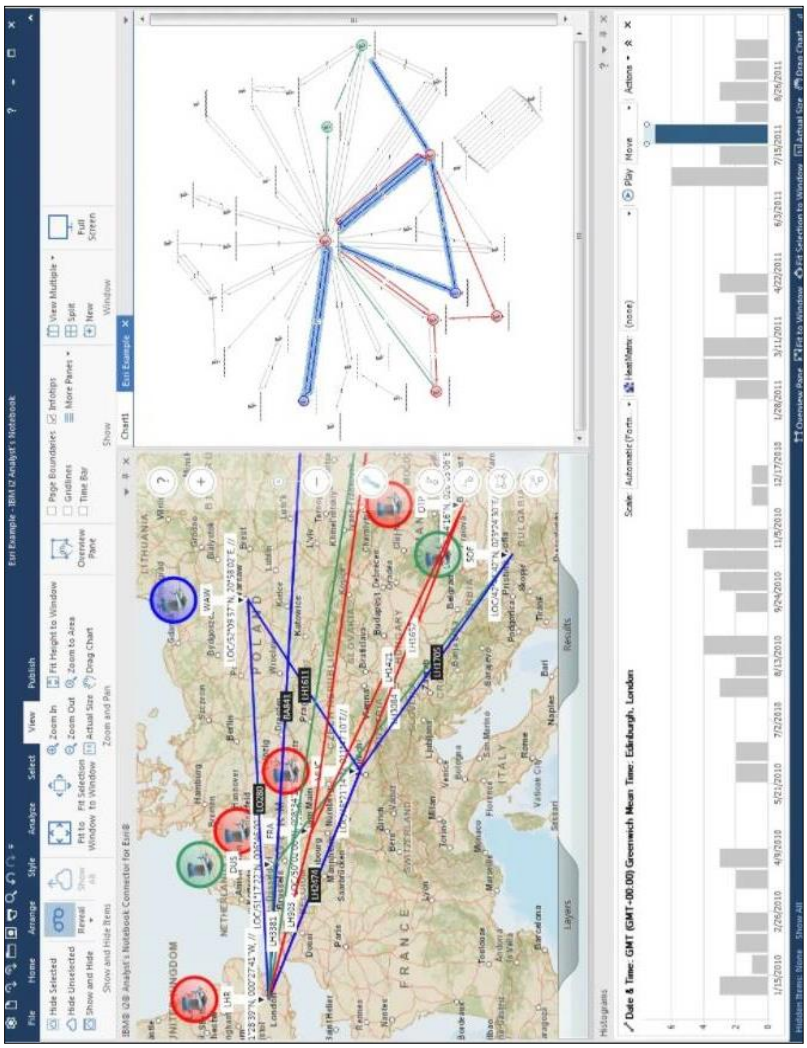
37. ábra. Közösségi hálózat elemzése hívószámok alapján, az IBM Security i2 Analyst's Notebook segítségével[654]

653 Az IBM honlapja: IBM Security i2 Analyst's Notebook. https://www.ibm.com/hu-en/products/i2-analysts-notebook; letöltés: 2021.07.23.

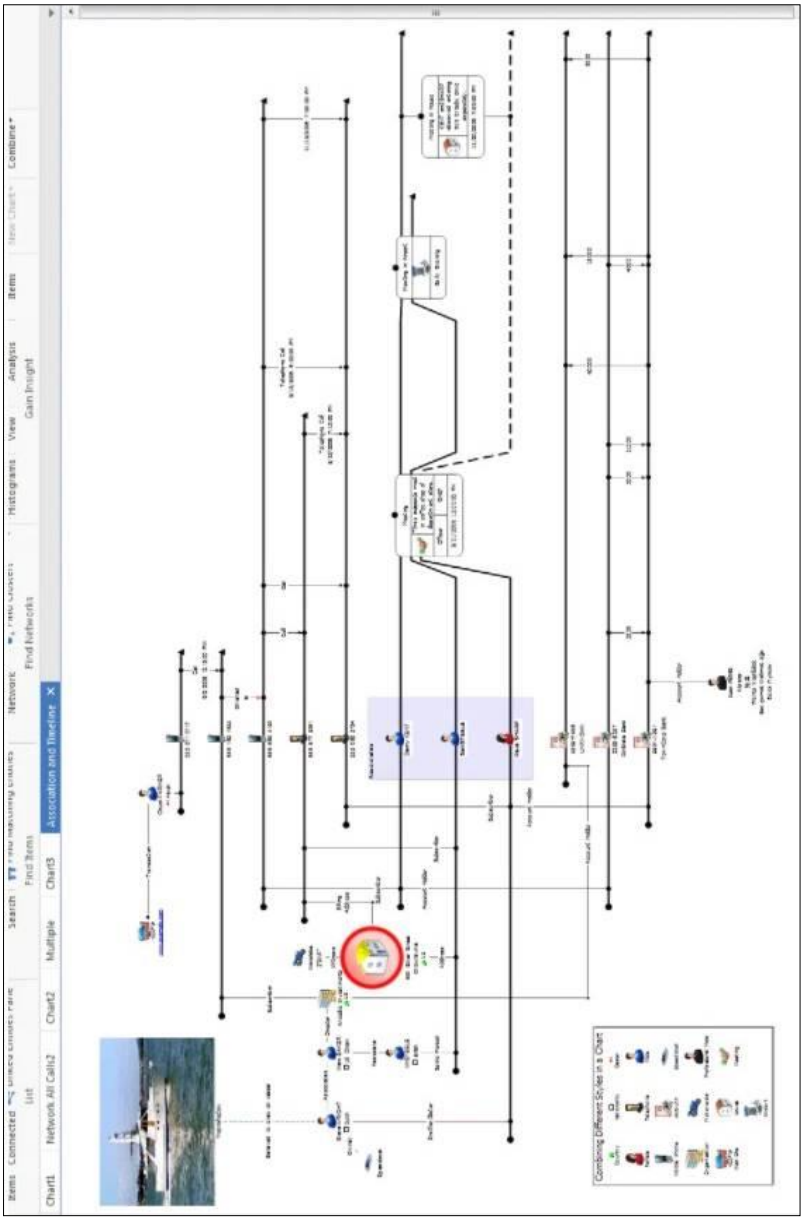
654 Uo.



38. ábra. Entitások közötti kapcsolat felfedése idővonal-elemzéssel, hívásinformációk alapján, az IBM Security i2 Analyst's Notebook segítségével
Az IBM honlapja: IBM Security i2 Analyst's Notebook.
https://www.ibm.com/hu-en/products/i2-analysts-notebook; letöltés: 2021.07.23.



39. ábra. Kapcsolati hálózat megjelenítése idővonalon és térképen, az IBM Security i2 Analyst's Notebook segítségével
Az IBM honlapja: IBM Security i2 Analyst's Notebook.
https://www.ibm.com/hu-en/products/i2-analysts-notebook; letöltés: 2021.07.23.



40. ábra. Kapcsolati hálózat megjelenítése idővonalon, az IBM Security i2 Analyst's Notebook segítségével
Az IBM honlapja: IBM Security i2 Analyst's Notebook.
https://www.ibm.com/hu-en/products/i2-analysts-notebook; letöltés: 2021.07.23.

Palantir (Amerikai Egyesült Államok)

A Palantir[655] vállalat a védelmi szféra felhasználói számára a Gotham fúziós rendszert kínálja. A rendszer alapja a megrendelő központi tudástárát képező strukturált adatbázis (Palantir Data Store). Az adatbázis a megrendelő meglévő hagyományos adatbázisai alapján entitásokra és azok kapcsolataira csoportosítva készül el (adatmodell). A kezdeti adatintegráció néhány hét alatt megvalósítható. Az újonnan beérkező információk folyamatosan gazdagítják, illetve szükség esetén átstrukturálják az adatbázist (dinamikus ontológia). A rendszerben megtalálható valamennyi adatelem egyértelműen köthető az eredeti forrásához. Az adatbázis felhasználásával a különböző területek szakértői és csoportjai közös felületen oszthatják meg információikat és értékeléseiket, illetve képesek projektalapon hatékonyan együttműködni.

A rendszer alapja az információhoz történő biztonságos, felhasználónként, forrásonként vagy adatelemenként (pl. egy épület címe vagy egy gépjármű típusa stb.) beállítható hozzáférés. A biztonságot növeli valamennyi felhasználó és adminisztrátor tevékenységének folyamatos és hamisíthatatlan logolása is. A Gotham segítségével minden felhasználó könnyen hozzáférhet számára rendelkezésre álló valamennyi információhoz. A rendszer képes külső adatforrásokat is a szervezeti adatbázishoz integrálni, azokat külön vagy integráltan, egymást gazdagítva kezelni. A magas fokú biztonság megkönnyíti a szervezetek közötti együttműködést is.

A Palantir tudásmenedzsment-rendszerének segítségével a tudás a szakértők távozását követően is a szervezet birtokában marad. A koncepció középpontjában a felhasználók tevékenységének logolása áll, amelynek segítségével a korábbi munkafolyamatok valamennyi lépése könnyen visszakereshető. Így a korábbi jelentések készítőinek távollétében is könnyen átlátható, hogy azok milyen célból, forrásokból és módszerekkel készültek. A futó projektek és munkafolyamatok a publikálásukig zárt környezetben (*sandbox*) zajlanak, így nem befolyásolják a rendszer működését.

A Gotham alapverziója az információ hálózatos, térképes, adatvizualizációs felületen történő, illetve böngésző megjelenítését teszi lehetővé. A hálózatos megjelenítés az entitások közötti szemantikai kapcsolaton alapul. A megjelenítési módok között idővonal és gyakoriságmegoszlási grafikon (hisztogram) is található. A térképes megjelenítés GEOINT-képességekkel segíti a felhasználókat, lehetővé téve a képek és a térképek összevetését, különböző filterekkel történő gazdagítását, tárgyak helyzetének nyomon követését. A hőtérképüzemmód az entitások elhelyezkedésének sűrűségét jelzi helyszínenként. Az adatvizualizációs nézet[656] segítségével akár több milliárd adatelem is áttekinthető módon csoportosítható.

[655] A palantírok a J.R.R. Tolkien *A gyűrűk ura* trilógiájában szereplő úgynevezett látókövek.
[656] Object Explorer.

Végül a böngészőablakos nézet[657] segítségével a projektek végrehajtásához szükséges adatok a felhasználók igénye szerint csoportosíthatók, az egyes adatcsoportokkal pedig különböző automatikus elemzési műveleteket lehet végeztetni.

A Gotham rendszerhez különböző kiegészítő modulok rendelhetők. Az Ava egy MI-alapú kutatási asszisztens, amely képes a szervezet betáplált komplex és ismétlődő adatelemzési munkafolyamatait automatikusan végrehajtani. Az Ava folyamatosan, automatikusan üzemel és figyelmeztetéseket ad a felhasználóknak az adatbázisokban azonosított entitások közötti új kapcsolatokról. A modul értékes emberi erőforrásokat szabadít fel, amelyeket egyébként az adatbázisokban történő kutatásokra fordítottak volna.

A Table a nagy adat könnyű felhasználását teszi lehetővé. A modul segítségével nem szükséges a nagy adatot külön, specialisták által kezelni. Valamennyi felhasználó képes a számára fontos információ kinyerésére, illetve a ténylegesen fontos adat kiszűrésére az adattömegből (zajból), ezáltal a rejtett tevékenység és az anomáliák felfedésére.

A Dossier megkönnyíti a felhasználók és a csoportok közös, valós időben megosztott munkavégzését. Az így készülő élő dokumentumok a Gotham programban meglévő biztonsági rendszabályok megtartásával, még elkészültük előtt vagy bármelyik verziójukban könnyen megoszthatók.

Az Operations a műveletek tervezésében, végrehajtásában és jelentésében nyújt segítséget. A Map applikáció speciális verziója (Gaia) lehetővé teszi a szervezetek közös biztonságos műveléstervezését, illetve a műveletek valós időben történő figyelemmel követését. A felhasználók egyszerűen, *drag and drop* rendszerben képesek információt megosztani, aminek segítségével megoldható a műveleti és az elemző-értékelő szakértők közötti valós idejű együttműködés.

A Nexus Peering modul lehetővé teszi a globális adatszinkronizálást, így a szervezet távoli térségekben tevékenykedő elemei is biztonságosan részt vehetnek a munkafolyamatokban és folyamatosan rendelkezésükre áll a számukra szükséges információ.[658]

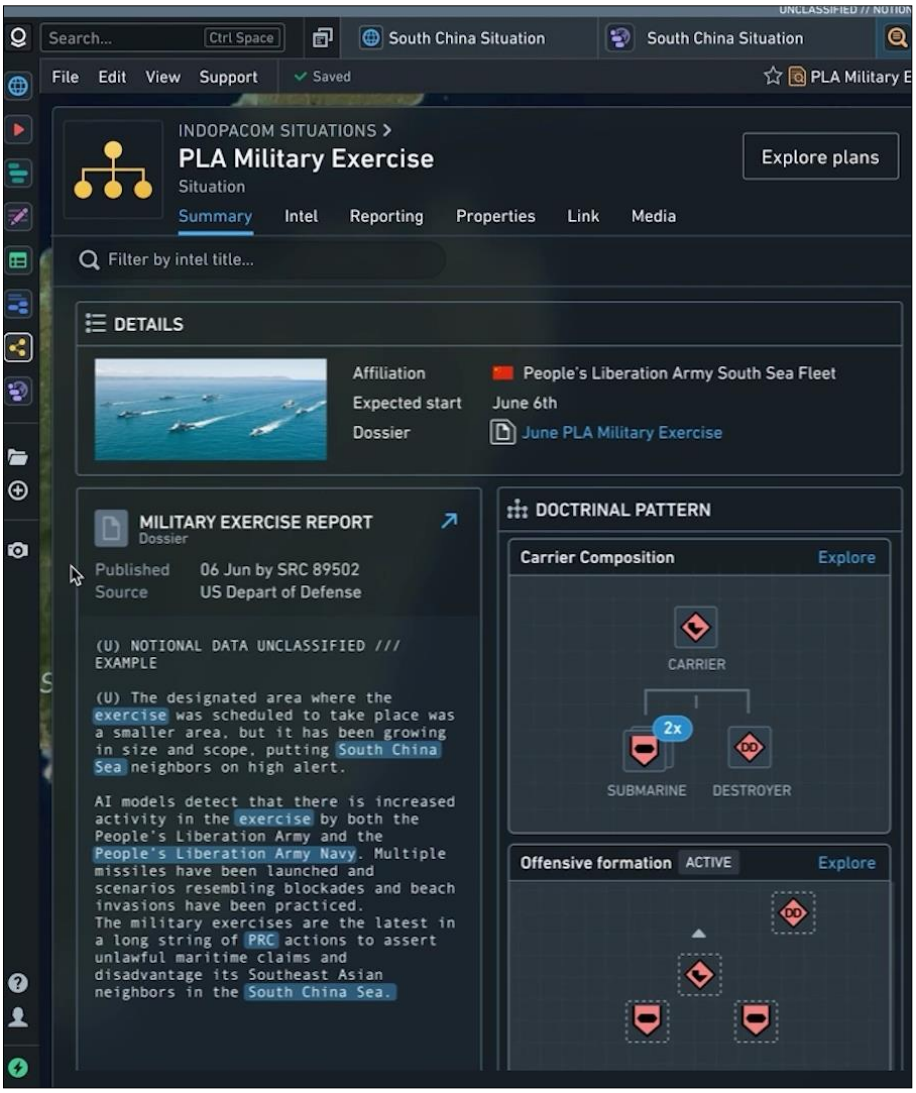
A Palantir Gotham alapkonfiguráció éves licenszdíja munkaállomásonként 66 000 font. A modulok közül az Ava 23%-kal, a Table 13%-kal, a Dossier 11%-kal, a Gaia 26%-kal, a Nexus pedig 27%-kal növeli a díjat. A különböző rendszerkonfigurációk éves díja támogatással együtt a kapacitás függvényében százezer és 750 millió font között változhat.[659]

---

[657] Custom Object View.

[658] Palantir Gotham service definition document (2020). https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92736/668463552506354-service-definition-document-2020-07-13-1355.pdf; letöltés: 2021.12.22.

[659] Palantir software and support pricing document (2021). https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92736/668463552506354-pricing-document-2021-04-15-1025.pdf; letöltés: 2021.12.22.



41. ábra. Kínai haditengerészeti gyakorlatról szóló jelentés és annak gyorselemzése a Palantir Gotham felületén[660]

[660] A Palantir honlapja. https://www.palantir.com/; letöltés: 2021.12.22.

Az amerikai védelmi minisztérium VAULTIS adattárház-rendszere

Az amerikai Altair informatikai vállalat által tervezett VAULTIS adattárház-rendszer segítségével az érintett szervezetek akár több terabájt adat menedzsmentjét is képesek saját rendszereiken elvégezni. Az ajánlott szoftvercsomagok megoldást nyújtanak a túlszabályozott és a valóságban nem alkalmazott adatkezelési szabályok jelentette nehézségekre is.

Az Altair az adatot stratégiai erőforrásként kezeli, amely alapján felső vezetői szintű döntések is hozhatók. Az egyes adatelemek könnyen visszakereshetők, azonosíthatók, növelve azok megbízhatóságát.

A vállalat könnyen telepíthető, a felhasználó által igényre szabható megoldásokat nyújt. Az adatmenedzsment-rendszer képes a strukturálatlan adattömeget strukturálni (*scraping*) és azt a saját adatbázissal összevetni (pl. híváslista összevetése nemzetbiztonsági adatbázissal). Az elemzés felhasználóbarát (*drag and drop*), az elemzés eredményéről a rendszer összefoglalót készít.[661]

A VAULTIS rendszert a védelmi minisztérium 2020 szeptemberében közzétett adatstratégiája[662] is nevesíti. A rendszer elnevezésére szolgáló betűszó kibontása:

- az adat láthatósága (Visible): a felhasználók legyenek képesek arra, hogy a számukra szükséges adatot megtalálják;
- az adat hozzáférhetősége (Accessible);
- az adat érthetősége (Understandable): a felhasználók legyenek képesek az adat tartalmának, környezetének és felhasználhatóságának felismerésére;
- az adatok összekapcsolása (Linked): az adatok közötti kapcsolatok felfedezése;
- az adatok megbízhatósága (Trustworthy);
- interoperabilitás (Interoperable);
- biztonság (Secure): a felhatalmazás nélküli használat és a manipulálás lehetőségének kizárása.[663]

[661] BHATTACHARJEE, Barnil – TIRBASO, James: Activate VAULTIS - Self-Service Data Analytics to Kickstart 2020 DoD Data Strategy Implementation. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020. október 29.

[662] DoD Data Strategy.

[663] Executive Summary: DoD Data Strategy – Unleashing Data to Advance the National Defense Strategy (2020). https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF; letöltés: 2020.12.16.

KÖVETKEZTETÉSEK

A könyv témáját eddigi hazai és nemzetközi szakmai tapasztalataim alapján, a hazai nemzetbiztonsági rendszer előtt is álló személyügyi, szervezeti és technológiai kihívásokat felismerve, a Zrínyi Honvédelmi és Haderőfejlesztési Program által nyújtott lehetőségek minél jobb kihasználásának szándékával választottam ki. Meggyőződésem szerint a nemzetbiztonsági hírszerző elemző-értékelő tevékenység a nemzetbiztonsági rendszer központi eleme, amelynek fejlesztése kulcsfontosságú mind a nemzetbiztonsági rendszer egésze, mind a honvédelem, illetve a magyar államigazgatás korszerűsítése szempontjából.

A könyvben szereplő információk támaszt nyújthatnak a nemzetbiztonsági rendszer szervezeti és technológiai modernizációjának megtervezésében és végrehajtásában, valamint az ahhoz szükséges humán kompetenciák kialakításában. Szándékom szerint a jelenlegi csúcstechnológiát képviselő termékek és szolgáltatások a hírszerzés önálló ágaira és az elemzés-értékelésre bontott bemutatása és értékelése szakmailag jól hasznosítható útmutatót jelent a mesterséges intelligenciát bevezető vagy fejlesztő szervezetek számára.

A mesterséges intelligencia elterjedése paradigmaváltást hoz a társadalomban, a gazdaságban és a védelmi szférában. Az MI lehetőségeinek széles körű alkalmazása behozhatatlan előnyhöz juttatja a technológiát a legteljesebb mértékben integráló államokat és nem állami szereplőket. A globális verseny keretei között a fejlesztésekből kimaradók a lemaradást kockáztatják, illetve elesnek olyan előnyöktől, amelyektől az emberi élet javítása, emberéletek megmentése remélhető. *Az MI elterjedése már 10–15 éves távlatban is döntően megváltoztathatja a világ országainak gazdasági és erősorrendjét,* annak függvényében, hogy az egyes országok milyen ütemben és hatékonysággal képesek kifejleszteni és átvenni az új megoldásokat. Az MI-technológiák birtoklása és alkalmazása hamarosan az államok szuverenitásának alapvető tényezőjévé válik, hiszen a jelentős előnyt birtoklók döntő fölénybe kerülhetnek a lemaradókkal szemben.

A fejlesztések ugyanakkor új függőségekkel és sebezhetőségekkel is járnak, ezeket a konfliktusok minden szintjén hatékonyan ki lehet használni. Az MI csak abban az esetben szolgálhatja hosszú távon a gazdasági és a társadalmi fejlődést, ha tudatában vagyunk az új technológiák jelentette kockázatoknak és aktívan teszünk a biztonságunkért. A magánszféra védelmének új jelentőséget ad, ha az okoseszközeink működési zavara esetén az alapvető szükségleteink kielégítése is lehetetlenné válik.

A mesterséges intelligencia végleg kilépett a számítógépes laboratóriumokból az ipar és a szolgáltatások világába, és küszöbön áll, hogy a magánemberek mindennapjait is meghatározza. Az MI széles körű elterjedése idővel a legmagasabb képzettséggel rendelkezők – orvosok, ügyvédek, közgazdászok stb. – munkavégzését is gyökerestől megváltoztatja, de ez nem feltétlenül jár az emberi munkaerő feleslegessé válásával. Magasabbnak látom annak az esélyét, hogy az ember–gép

együttműködés e téren is a lehetőségek nagyságrendi kibővülését, a magas szintű szolgáltatások elérhetőségének növelését eredményezi majd.

Az MI-eszközök egyik kiemelt alkalmazási formája lehet a befolyásolás, vagyis a befolyásoló fél azon képessége, hogy akaratának teljesítésére bírja a befolyásolt felet. A befolyásolás modern formái szintén kiterjedten alkalmazhatók az egyéni és a csoportos szintek sokaságában, akár a befolyásolt fél tudta nélkül is. A fejlődésnek ebben a szakaszában az is elképzelhetővé vált, hogy az emberi csoportok – akár egyes nemzetállamok – tudtukon kívül is elveszítsék az irányítást saját sorsuk – szuverenitásuk – felett, öntudatlanul is mások érdekeit szolgálva. A mesterséges intelligencia alkalmazásával egyre hitelesebben hamisíthatók hang- és videofelvételek (mélyhamisítás), automatikus képfelismerő megoldások érhetők el, valamint lehetővé válik a közösségi média befolyásolása. Valószínű, hogy már a belátható jövőben is kizárólag MI-rendszerek felhasználásával lesz lehetőség a hamisított hírek kiszűrésére. Az emberi kommunikációt beszédben, írásban és – a számítógép képernyőjén – vizuálisan is tökéletesen utánzó eszközök alkalmazásával tovább növelhető a befolyásolás hatékonysága. Az MI-eszközök sajátossága, hogy a megfelelő erőforrások birtokában semmi akadálya annak, hogy ezek az eszközök használata célzottá és tömegessé váljék a felhasználó törekvéseinek szolgálatában. A befolyásolás észlelésére a jövőben olyan MI-alapú kibervédelmi rendszerekre (tűzfalakra) lesz szükség, amelyek az emberi érzékek által észlelhetetlen jelekből és a vírusadatbázisokhoz hasonló állományok alapján fejlett algoritmusok segítségével szűrik ki a befolyásolási törekvéseket.

Az MI-alapú katonai eszközök térnyerése 10–15 éves távlatban a repülőgépek és a harckocsik tömeges elterjedésének hatásaihoz hasonlítható, a Wehrmacht harckocsijai elleni 1939-es lengyel lovasrohamhoz mérhető hatékonyságúvá degradálva a jelenlegi fejlettségen megrekedő haderőket. Az autonóm fegyverrendszerek képességei folyamatosan fejlődnek, és valószínűleg *csak idő kérdése az emberi felügyelet elhagyása* vagy szimbolikussá válása.

Az MI-rendszerek megoldást kínálnak a modern haderő egyre égetőbb toborzási kihívásaira, hiszen számos, jelenleg még gépek által végzett munkafolyamat végrehajtása egyszerűsíthető vagy automatizálható. A veszélyes feladatok robotizálásával megóvható a személyi állomány. Egyelőre kérdéses azonban, hogy az emberi tevékenység részének vagy egészének kiváltása milyen költségekkel jár. A költségek növekedésére nemcsak anyagi értelemben lehet számítani, hanem a magasan képzett emberi munkaerő tekintetében (adatmenedzserek, technikusok stb.) is. A saját erők megóvásában előrelépést ígérő robotrendszerek vizsgálatakor az ellenérdekelt magas technológiájú fél ilyen rendszerei jelentette fenyegetést is figyelembe kell venni.

Elsősorban a nagyhatalmak közötti, esetleges jelentős fegyveres konfliktus kirobbanása esetén várható a teljes autonómiával ellátott rendszerek bevetése. Az autonóm eszközök esetében az is aggasztó, hogy alkalmazásuk esetén kikerülhető az a morális gát, amelyet az emberi katonák bevetése jelent, könnyebbé téve a vezetők számára a morális kérdések kiiktatását a katonai szükségszerűség fellépése esetén.

A fejlődésben lemaradók helyzete a technológiai szingularitás bekövetkezését követően válik tarthatatlanná. A ma még beláthatatlan képességekkel rendelkező gépi szuperintelligencia által irányított robotizált erőkkel szemben a mai technológiát alkalmazók kilátásai a több száz fős, dárdákkal, íjakkal és kőbaltákkal felszerelt, összehangoltan vadászó homo sapiens hordával szembenéző néhány tucat ősmajoméhoz válhat hasonlatossá.

A mesterséges intelligencia a nemzetbiztonsági szolgálatok tevékenységét is új alapokra helyezi, minőségi és mennyiségi szempontból is paradigmaváltást okozva a nemzetbiztonsági hírszerzés egésze számára. A platformok információmegosztó képességei a hírszerzés ágai közötti együttműködésben is új lehetőséget jelentenek. Az MI által a hírszerzés önálló ágai, illetve a kibervédelem számára nyújtott lehetőségek az alábbiak szerint csoportosíthatók.

A) *Nyílt forrású hírszerzés (OSINT) – nyilvános forrású információszerző tevékenység (PAI)*: Az MI-n alapuló OSINT-rendszerek alkalmasak az interneten fellelhető információk tömeges monitorozására, gyűjtésére, fordítására, rendszerezésére, előértékelésére, illetve elosztórendszereken történő továbbítására. Az adatbázisba került információk könnyen kereshetők. A fejlettebb rendszerek alkalmasak személyek, karakterek[664] (pl. falfirkák) és tárgyak[665] azonosítására képekről és videókról. Az OSINT-rendszerek integráltan vagy külön modul formájában SOCMINT-képességekkel is rendelkeznek.

B) *Közösségi médiából történő adatszerzés (SOCMINT)*: A SOCMINT-rendszerek eleget tesznek a közösségi médiát felhasználó információszerzés speciális követelményeinek. A SOCMINT-információk stratégiai felhasználásához a közösségimédia-profilok manuális, egyenkénti felderítése és monitorozása, valamint elemzés-értékelése önmagában nem elegendő. A SOCMINT-tevékenység során felderített személyek, csoportok és hálózatok száma rövid idő alatt eléri azt a nagyságrendet, amelynek a manuális kezelése meghaladja a nemzetbiztonsági szolgálatok és a rendvédelmi szervezetek korlátozott humán erőforrása kapacitását. Ezért indokolt olyan célszoftverek alkalmazása, amelyek kiváltják az emberi tevékenység egy részét. Számos vállalat kínál ilyen szoftvercsomagokat, amelyek közös jellemzője, hogy integrált megoldásokat kínálnak a SOCMINT- és a PAI-források automatizált felderítésére, az információ kinyerésére és a közösségimédia-oldalak (emellett blogok, csevegőszobák stb.) monitorozására, a kinyert információ ábrákon történő megjelenítésére, elemzés-értékelésére. A szoftvercsomagok egy része fejlett fordítóprogramot is tartalmaz. Általános jellemzőnek tekinthető továbbá a kapcsolati hálózatok felrajzolása, a metaadatok[666] (fél)automatikus kinyerése, illetve a csoportok hangulatelemzése (szentimentanalízise). A legfejlettebb megoldások képesek a közösségi médián fedőprofilok tömeges létrehozására és kezelésére, így nagyban megnövelik a kinyert információ mennyiségét. A megoldás alkalmazása abban az esetben is indokolt, ha a célszemélyek és -csoportok gyakran, nyíltan vagy alacsony szintű műveleti biztonság alkalmazásával kommunikálnak (pl. migráció, tüntetések stb.). A jövőben várható az írott tartalom automatizált

[664] Optical Character Recognition – OCR.
[665] Object Recognition – OR.
[666] A közösségi oldalak felhasználóinak tevékenysége, ismerősi köre stb.

előállítását[667] lehetővé tevő technológiák alkalmazása is, még élethűbb fedőprofilok létrehozása érdekében.

Egyes vállalatok a SOCMINT egy-egy részterületére specializálódnak, mint például a fedőprofilok félautomatikus megalkotása és kezelése. Az ilyen szoftverek lehetővé teszik, hogy a nemzetbiztonsági szolgálatok és a rendvédelmi szervezetek által megalkotott legenda alapján a virtuális személy percek alatt megszülethessen az online térben. A módszerrel biztosítható, hogy nem fordulnak elő a manuális bevitel során szinte elkerülhetetlen apróbb hibák, következetlenségek. A fedőprofilok lehetővé teszik a behatolást a zárt felhasználói csoportokba és a *dark web*re (az internet jelszóval védett, zárt részére). Az alaposan kidolgozott, szoftveresen kezelt és karbantartott fedőprofilokkal lehetőség adódik a közösségi médián zajló illegális vagy ellenérdekelt tevékenység felderítésére és megfigyelésére, a célszemélyek azonosítására és róluk információ kinyerésére.

C) *Emberi forrású hírszerzés (HUMINT)*: Az információs társadalomban a HUMINT-tevékenységet megalapozó legenda megteremtése elképzelhetetlen jól megtervezett és karbantartott digitális jelenlét nélkül. A különböző internetes felületeken megjelenő információnak koherensnek kell lennie, és a közösségi médiában mutatott tevékenységnek valós személy képét kell tükröznie. A célszemélyekben gyanút kelt, ha az őket megközelítő személy nem rendelkezik kiterjedt online jelenléttel. Mindez manuális módszerekkel csak nehezen és időigényesen oldható meg, és nagy a hibázás lehetősége, ezért klasszikus HUMINT-tevékenység esetén is indokolt a virtuális HUMINT adta lehetőségek használata.

A SOCMINT-rendszerek arra is lehetőséget teremtenek a HUMINT számára, hogy új kapcsolatokat derítsen fel és közelítsen meg. Célszerű tehát együttműködést kialakítani a SOCMINT- és a HUMINT-szervezetek között, hiszen a HUMINT-szakemberek ott folytathatják a munkát, ahol a SOCMINT lehetőségei kimerülnek.

D) *Rádióelektronikai felderítés (SIGINT)*: A SIGINT a többi hírszerzési ághoz viszonyítva több adattal dolgozik, ezért az MI-alapú SIGINT-rendszerek elsősorban a beszerzett nagy adat (fél)automatikus feldolgozásában és elemzésében nyújtanak segítséget. Ez különösen fontos a nemzeti távközlési és internetszolgáltatók adatai esetében, elsősorban a metaadatok (hívás ideje és időtartama, a résztvevők földrajzi helye, készülékek és operációs rendszereik típusai stb.) és szelektorok (hívószámok, e-mail címek, közösségi média, illetve csevegőprogram-profilnevek és egyedi azonosítók stb.) miatt. Jellemzően a SIGINT-szoftvercsomagok is képesek hálózatelemzésre, a lehallgatott beszéd szöveggé alakítására és fordítására, valamint hangfelismerésre. Az elemzések alapja itt is az entitáskinyerés.

E) *Képi hírszerzés (IMINT)*: Az MI alkalmazása megteremtette a lehetőséget a műholdak, a felderítő-repülőgépek, a megfigyelőkamerák stb. felvételeinek tömeges és automatikus feldolgozására. Az ilyen rendszerek a betáplált adatbázisok alapján egyre nagyobb pontossággal képesek felfedezni a képeken a különböző objektumokat, ezért az ilyen feladatokban a képességeik már meghaladják az emberi IMINT-elemzőkét.

[667] Natural Language Generation – NLG.

A leghasznosabbak ugyanakkor az IMINT-elemzők asszisztenseként lehetnek, mert a beszerzett képek és az adatbázisok könnyebb kezelhetőségével nagyban megkönnyítik az összetettebb elemzések elvégzését. Már több vállalat kínál olyan szolgáltatásokat, amelyek segítségével nagy felbontású műholdfelvételek érhetők el a Föld bármely pontjáról, amelyeket akár évtizedekkel korábban készített felvételekkel is össze lehet hasonlítani.

F) *Térinformatikai/geoinformációs hírszerzés (GEOINT)*: A GEOINT az információk megjelenítésével, rendszerezésével és összevetésével teremt hozzáadott értéket, ezért az MI felhasználási lehetőségei valószínűleg ezen a területen a legszélesebbek. A GEOINT-szoftverekkel és -szolgáltatásokkal a saját vagy vásárolt műholdfelvételek alapján nagy pontosságú és a valós helyzetet bemutató térképek készíthetők. Mára több vállalat képes a műholdképek és a műholdas radarképek alapján 3D-s térképeket előállítani, amelyek alapján a terep virtuálisan bejártható. Az ilyen nagy pontosságú szoftverek a Föld egész területének lefedésére is alkalmasak lehetnek. A nagy pontosságú, múltbeli információkat is tartalmazó, tetszőleges adatbázisokkal összekapcsolt térképek az anomáliák felfedésében és az előrejelzések készítésében is kulcsszerepet játszanak.

A GEOINT-lehetőségek kiaknázása tekintetében valószínűleg az amerikai Nemzeti Felderítőiroda (NRO) a Google vállalattal közösen fejlesztett Sentient rendszere jelenti a csúcstechnológiát. A Sentient térinformatikai módszerek alkalmazásával a Föld egész területére vonatkoztatva képes valós időben integrálni a hírszerzés valamennyi ágából származó információkat.

G) *Kibervédelem*: A kibervédelmi rendszerek alapjai a kártékony szoftvereket, az ilyen eszközöket alkalmazó szervezeteket és az eljárásokat tartalmazó, a fejlesztők által létrehozott és karbantartott adatbázisok. Valós időben monitorozzák a védett szervezet informatikai rendszereit és riasztanak a kibertámadások és a kibertéri hírszerzési kísérletek esetén. Ezzel egy időben képesek megkezdeni a fenyegetések elhárítását és a károk mérséklését. Automatizált elemző és vizsgálati eszközökkel alkalmasak az elkövető személy vagy szervezet azonosítására, amely alapján ellentevékenységet is végrehajthatnak. A rendszerek alkalmazásával kiberműveleti szimulációk, gyakorlatok és tréningek is végezhetők.

H) *Mérés és jelmeghatározó hírszerzés (MASINT)*: Az egyre korszerűbb és több adatot szolgáló szenzorok információinak hatékony feldolgozásához mára elengedhetetlen az MI-alapú adattárház-rendszerek alkalmazása. A MASINT-információk felhasználásában hatalmas lehetőséget rejtenek magukban a GEOINT-rendszerek, akár a szenzoradatok áttekinthetőségének növelése, akár a más hírszerzési ágak információival történő összevetése tekintetében. Hasonló eredmények lehetnek elérhetők az elemző-értékelő fúziós rendszerek alkalmazásával is.

A fúziós és adattárház-rendszerek segítségével az elemző-értékelők a nagy adat korszakában is minden releváns információ felhasználásával készített, a döntéshozók számára jól hasznosítható jelentéseket készíthetnek. Hagyományos, manuális eszközökkel ez mára csak korlátozottan lehetséges.

A rendszerek közös jellemzője, hogy segítségükkel az információ könnyen áttekinthető, korábban nem észlelt összefüggések is kimutathatók, illetve lehetőséget teremtenek az együttműködésre az elemző-értékelők számára mind a hírszerző szakterületek képviselői, mind az elemző-értékelők csoportjai között, akár a saját szervezeten kívül is. Az együttműködés információmegosztásra, hipotézisek és szinopszisok közös felállítására, vagy akár közös jelentésírásra is kiterjedhet. A rendszerek hasznos funkcionalitásai közé tartoznak a félautomatikus és az automatikus jelentésíró rendszerek, ahol lehetőség van a szolgálatok saját sablonjainak alkalmazására is. A megnövekedett képességek mellett fontos hozadék tehát a manuális részfeladatok végrehajtására fordított idő csökkenése is.

A fúziós rendszerek kollaborációs képességei megoldást jelentenek a hírszerzési ciklus merev értelmezéséből adódó kihívásokra is, mert tetszőlegesen, akár projektalapon összeállított szervezeti egységek vagy munkacsoportok is működhetnek virtuális fúziós központokként. A fejlett technológia támogathatja az elemzőket abban, hogy hatékonyan irányíthassák és támogathassák az adatszerző munkát.

Az MI potenciálisan felhasználható az elemző-értékelő munka valamennyi tevékenységi körében.

a) *Az információk elemzése-értékelése*: Az információ egyszerű és gyors rendelkezésre állása nagyban megkönnyíti az információk pontosítását, a helyes és az elfogadott kifejezések használatát, a helyesírás-ellenőrzést (a szakkifejezések tekintetében is), a távolságmérést, a települések, objektumok, folyamatok térképes megjelenítését. A fejlett rendszerek támogathatják az egyszerű elemző-értékelő eljárások (összehasonlítás, minták stb.) és a kötött eljárások (strukturált jelentések: életrajzok, hadgyakorlatokról és költségvetésekről készített összefoglalók, háttér-tájékoztató jelentések stb.) egységesítését és minőségbiztosítását. Lehetőség van arra is, hogy az elemzők az információt jelentéstervezetekbe (mátrixokba, kockázatelemzési modellekbe, regionális biztonsági komplexum modellekbe stb.) gyűjtsék és rendszerezzék.

b) *Tájékoztatók (jelentések) készítése*: Az alaki és a tartalmi kellékeket tartalmazó sablonok alkalmazása mellett az információk gyors rendelkezésre állása és exportálhatósága, valamint a feladatmenedzsment és a kollaborációs lehetőségek nagyban könnyítik és gyorsítják a jelentésírást. Fontos előny, ha a rendelkezésre álló szűk időkeretet nem tölti ki a meglévő információk gyűjtése és rendszerezése, illetve az adatszerzők irányába szabott információigények (RFI-k) megfogalmazása. Nincs akadálya az egyszerű jelentések (pl. gyűjtések) automatizált elkészítésének sem. Az így felszabadult időkeret az elemzés-értékelés hozzáadott értékeinek (értékelések, következtetések és előrejelzések) megalkotására fordítható. Fontos, de a hagyományos módszerekkel nehezen teljesíthető követelmény a tájékoztatókban szereplő információk vizualizációja, ehhez szintén nagy segítséget nyújthatnak a fejlett rendszerek. A kollaborációs rendszerek lehetővé teszik a tájékoztatók különböző részeinek párhuzamos, minden résztvevő számára átlátható készítését, valamint a jelentések gyors és hatékony ellenőrzését és jóváhagyását is. A hatékony kommunikációs lehetőségekkel a felső vezetés és az elemző-értékelő szervezet

vezetése könnyen megoszthatja a készítőkkel saját értékelését, ami hasznos iránymutatást jelenthet a jelentések készítése során.[668]

c) *Elemző-értékelő adattárak vezetése*: A nagy adat kezelésére alkalmas megoldások több szintű, differenciált, optimalizált lekérdezési lehetőségekkel (pl. információs jellegű és az adatszerzők munkájának értékelésére szolgáló statisztikai jellegű stratégiai jelentésekhez a célország vagy régió hosszú távú folyamatainak nyomon követéséhez szükséges információk stb.) rendelkeznek. Az OSINT-információk automatizáltan is gyűjthetők az elemző-értékelő szervezet külső és belső adattáraiba. Az OSINT és a részben nyílt információkat feldolgozó IMINT és GEOINT további különleges lehetőségeket rejt magában, hiszen alkalmazásukkal a kollaboráció védett, de nem minősített rendszereken is megoldható, gyorsítva és egyszerűsítve a szolgálatokon belüli és kívüli együttműködést is, különös tekintettel a szolgálatok távoli helyszíneken tevékenykedő elemeire. Az OSINT-információk különösen alkalmasak a közös (alapvető) helyzetismeret kialakítására akár a szolgálatokon belül, akár a nemzetbiztonsági rendszer egésze számára, valamint a nemzetbiztonsági rendszer és a döntéshozók között is. A felhőalapú adattárházak nagyban elősegítik a nemzetbiztonsági szolgálatok hazai és nemzetközi együttműködését is, hiszen lehetőség nyílik arra, hogy hozzáférést adjanak az adatbázis tetszőleges részeihez vagy a kívánt információkat egyszerűen exportálják.

d) *Tájékoztató rendszer működtetése*: A feladatmenedzsment és a jelentéskészítő rendszerek lehetővé teszik a protokoll-listák importálását és könnyű karbantartását. Ezek alapján a jelentések elosztói könnyen összeállíthatók, azokra a gépi tanuláson alapuló mesterséges intelligencia javaslatot is tehet. Elsősorban a nyílt információk alapján készített egyszerű jelentések (gyűjtések) esetében nemcsak a készítés, de a küldés is automatizálható. A korszerű adatbáziskezelő rendszerek segítségével a tájékoztatás elmozdulhat a jelentések küldésétől. Az együttműködésre kötelezett szervezetek és a döntéshozók hozzáférést kaphatnak az adatbázis részeihez, így a szükséges információkat maguk is lekérdezhetik és exportálhatják. Ez a megközelítés legkönnyebben a nyílt információk esetében megvalósítható, mert a minősített adatok biztonságos, felhőalapú kezelését lehetővé tevő rendszerek drágák és létrehozásuk nemzeti sztenderdek kialakítását igényli. Közbeeső megoldásként az adatgyűjtés-koordináló és felderítési követelmények menedzsmentje (CCIRM)[669] számára is biztosítható a betekintés, így az egyszerűbb információigényeket az elemző-értékelők bevonása nélkül is megválaszolhatják.

---

[668] A jelenlegi, piramisszerű monolit struktúrákban a jelentések készítői ritkán kerülnek közvetlen kapcsolatba a vezetéssel. A középvezetőkön keresztüli információáramlás túlságosan lassú és esetleges ahhoz, hogy az a napi munkavégzésben részletes iránymutatást nyújthasson.

[669] A NATO-terminológia szerint: Intelligence Requirement Management and Collection Management (IRM-CM). Egyes szövetséges országok a Collection Coordination and Intelligence Requirement Management (CCIRM) megnevezést használják. A CCIRM lehetővé teszi a beérkezett információigények szerinti adatgyűjtést, feladatot szab és irányítja az adatgyűjtést (vagyis feladatot szab a felderítőszervek számára), valamint kapcsolatot tart az együttműködésre kötelezett szervezetekkel.
HORVÁTH Csongor: Az adatgyűjtés-koordináló és felderítési követelmények menedzsmentje. Honvédségi Szemle, 146. évfolyam 4. szám, 2018. pp. 71–78.
http://real-j.mtak.hu/16399/4/Honvedsegi_Szemle_2018_4_teljes_szam.pdf; letöltés: 2021.12.27.

e) *Hírszerzési ciklus működtetése (az adatszerzők információszerző tevékenységének irányítása)*: A fúziós rendszerekkel gyorsítható a feladatok értelmezése és javítható annak színvonala. Az elemző-értékelők vagy a dedikált CCIRM-szervezet könnyen összegyűjtheti a már rendelkezésre álló információkat (az OSINT-szervezet segítségével a nyílt információkat is), valamint meghatározhatja a hiányzó információkat és azok jellegét. A szolgálatok vezetése az információigényeket priorizálhatja, azok megválaszolására szükség esetén egyedi, virtuális munkacsoportokat is létrehozhat, meghatározva azok vezetési rendjét és hatásköreit. Előnyt jelent, ha az érintett állomány folyamatban lévő feladatai könnyen lekérdezhetők, így áttekinthető a leterheltségük, meglévő feladataikat vezetői utasításra későbbre halaszthatják. A hiányzó információk beszerzése érdekében megfogalmazott információigények áttekinthető módon tartalmazhatják a már rendelkezésre álló releváns információkat, ami nemcsak a duplikációk kiszűrését és ezzel a felesleges munkavégzést előzi meg, de elemző-értékelő művelettámogatást is biztosít az adatszerzők részére. A korszerű adatbáziskezelő rendszerekkel könnyen áttekinthető az adatszerző szervezetek és az egyes munkatársak tevékenysége, ezzel növelhető az adatszerző szervezetek információszerző tevékenysége értékelésének objektivitása.

f) *Művelettámogató tevékenység*: Az adatbázisrendszerek alkalmazásával növelhető az adatszerző szervezeteknek nyújtott elemző-értékelő támogatás minősége és mértéke is. Ennek az információigények már meglévő információkkal történő ellátása mellett módja lehet hozzáférés és lekérdezési lehetőségek biztosítása az elemző-értékelő adatbázisok részeihez vagy egészéhez az adatszerzők számára. A hozzáférés az adatszerző műveletekhez is jól hasznosítható lehet. Katonai műveletek esetében a nemzetbiztonsági szervezeteknek a műveletтervezőkkel, valamint a felderítő- és a hadműveleti törzsekkel kell hasonló együttműködést kialakítaniuk. Az adattárakhoz történő differenciált hozzáférés biztosításával a műveletek előkészítése (pl. képzések és a műveletтervezéshez szükséges információk biztosítása formájában) is hatékonyabban támogatható. A művelettámogató tevékenységben is különleges lehetőséget rejtenek magukban az MI-alapú OSINT-, IMINT- és GEOINT-képességek, hiszen könnyen megosztható, kiválóan hasznosítható és akár valós idejű információt is biztosíthatnak.

A platformok információmegosztó képességei a hírszerzés ágai közötti együttműködésben is új lehetőséget jelentenek. Ennek jele a szakterületek közötti határok elmosódása is. A platformok besorolását sokszor a felhasználó képzettsége adja meg. A határok elmosódása távolról sem jelenti ugyanakkor az önálló hírszerzési ágak megszűnését, hiszen a specializált szoftverrendszerek egyre mélyebb szakmai ismereteket követelnek meg a felhasználóktól.

A kereskedelmi forgalomban lévő hírszerzési eszközök és a szaktudás színvonalával csak a nagyhatalmak vetélkedhetnek, de számukra is hasznos és fontos kiegészítést jelentenek azok a lehetőségek, amelyeket a magánvállalatok biztosítanak. A fejlett hírszerzési eszközöket áruló magánvállalatok a kisebb országok nemzetbiztonsági szolgálatai és rendvédelmi szervezeti számára is korábban elképzelhetetlen lehetőségeket jelentenek. A fejlett rendszerek megsokszorozhatják a kisebb országok hírszerző kapacitását is.

Mára már nem a technológia elérhetősége, hanem a bőség zavara és a költségek jelentik a fő kihívást. A költségek tekintetében azt kell mérlegelni, hogy az érintett szolgálat hajlandó-e jelentős mértékben megemelni az informatikai kiadásait a képességei megsokszorozása érdekében. Azt sem szabad elfelejteni, hogy az eszközök fenntartási (karbantartási) költségei is magasak. Ez a gyártónak adott éves licence és a karbantartási díjakon felül a megnövelt létszámú informatikus állomány illetményét is jelenti. A nemzetközi példák alapján elkerülhetetlen az ágazati szakemberek és az informatikusok között közvetítő, a mindennapi karbantartási és rendszerkalibrálási feladatokat a szakmai szervezeteken belül végző adatmenedzseri munkakörök létrehozása is. Összességében hasonlónak látom a helyzetet, mint a fejlett haditechnikai eszköz esetében, ahol az informatikai berendezések és a szoftverek képviselik az eszköz összértékének túlnyomó részét.

A szabadon hozzáférhető termékek és szolgáltatások áttekintése nyilvánvalóvá teszi, hogy a hírszerzés világa mára szinte teljes egészében rendelkezésre áll a nem állami szereplők számára is.[670] A kellő anyagi lehetőségek birtokában bárki számára megvásárolható képességek néhány *niche* terület kivételével lefedik a hírszerzés teljes spektrumát. A magas költségek miatt elsősorban a multinacionális nagyvállalatok és a nemzetközi szervezetek jöhetnek szóba potenciális nem állami vásárlóként. Felmerülhet a terrorista szervezetek és a szervezett bűnözés érdeklődése is, de a fejlett technológiákat kínáló vállalatok arra törekszenek, hogy legitim szereplők maradjanak a hírszerzési piacon, ezért jellemzően együttműködnek a hatóságokkal az ilyen esetek elkerülése érdekében. Elkerülhetetlen ugyanakkor, hogy a fejlett technológiák idővel illetéktelen kezekbe kerüljenek.

A nemzetbiztonsági szolgálatok fejlesztése során figyelembe kell venni, hogy a digitális innováció, a szervezeti akadályok lebontása és a szolgálatok képzési rendszere egymással dialektikus összefüggésben áll, egymásra hatnak és egymást feltételezik. A reform e három alapelemének át kell szőnie nemcsak a különálló szolgálatok, de a teljes hírszerzési rendszer szövetét, különben – egymástól elválasztott szigetekként – nemcsak kudarcra vannak ítélve, de a munkafolyamatok anomáliáit okozhatják és biztonsági kockázatot is jelentenek.

A nemzetbiztonsági szervezetekben az MI hatékony alkalmazásának gátja a 20. századi szervezeti felépítés és munkaszervezés meggyökeresedése. Az elavult szervezeti struktúra ellenérdekeltté teszi a nemzetbiztonsági szolgálatok munkatársait a fejlesztések bevezetésében, ezért a reformok mögött világos és egyértelmű vezetői akaratnak kell állnia. A monolitikus, funkcionális elkülönítést követő modellt fel kell váltania a feladatközpontú felépítésnek, és ki kell egészíteni a stratégiai hálózatok nyújtotta rugalmassággal. A már működő, általános példák felhasználásával az új megoldásokat az adott szolgálat feladatai, szükségletei és lehetőségei függvényében kell átvenni, amihez a vezetés tapasztalatára és akaratára, valamint a változást igénylő végrehajtók dinamizmusára egyaránt szükség van.

[670] A vállalatok a termékeik egy szűk szegmensét kizárólag állami szerveknek értékesítik.

Az elavult szervezeti struktúrának és technológiának köszönhető az eredendően absztrakt hírszerzési ciklus elemeinek merev, bürokratikus értelmezése[671] is. Ennek elsősorban szervezeti és technológiai okai vannak, hiszen fejlett információ- és feladatmenedzsment-infrastruktúra hiányában a szolgálatok arra kényszerülnek, hogy a hírszerzési ciklus elemein – időrabló és az erőforrásokat pazarló módon – egymást követően és egymásra épülően, de lényegében egymástól elszigetelve haladjanak végig. A komplex problémakör fontos része, hogy a ciklus különböző elemeit végző szervezeti elemek között adminisztratív, a „*need to know*" elvére hivatkozó falak emelkednek. Amerikai felfogás szerint az akadály ledöntésének vagy megkerülésének legjobb módja a feladat-, illetve küldetésorientált, több terület képviselőiből álló csoportok alakítása és azok önálló szervezeti egységként kezelése. Megfelelő feltételek esetén egy-egy konkrét feladat végrehajtása során is megoldható lenne a ciklus elemeinek párhuzamos, egymással állandó visszacsatolásban lévő, ezáltal egymás hatékonyságát növelő működése. A szervezeti struktúra közvetlen kapcsolatban áll tehát a technológiai fejlesztések rendszeresítésének ütemével, vagyis a globális versenyképesség fenntartásával.

Az új technológiák bevezetésével a szolgálatoknak folyamatosan felül kell vizsgálniuk szervezeti felépítésüket és eljárásaikat, mert azokat más körülményekre dolgozták ki. A reformok során a belső szabályzókat és eljárásokat nem szabad kőbe vésett kinyilatkoztatásoknak venni, hiszen azokat a múltban, múltbéli helyzetekben hozták annak érdekében, hogy szolgálatok a lehető leghatékonyabban működjenek. Az elődök megoldásai helyett tehát elsősorban a céljaikat kell figyelembe venni. A hírszerzési rendszer és annak története beható ismeretével le kell ásni a folyamatok mélyére, meg kell vizsgálni, hogy azok a jelenben miért és mennyiben szükségesek, és meg kell állapítani, hogy informatikai megoldásokkal mit és hogyan lehet megszüntetni, egyszerűsíteni vagy javítani, illetve milyen új szervezeti elemekre és módszerekre van szükség. Helytelen megoldás, ha a digitális technológiák számára az analóg rendszerek megoldásait vesszük alapul.

A személyi állomány folyamatos képzése nélkül nem képzelhető el a korszerű hírszerzési rendszer hatékony működtetése. A feladatok szerteágazó volta, az új technológiai megoldások tömeges megjelenése és a korábban elkülönült szervezeti kultúrák egyre gyorsuló közeledése szükségessé teszik a stabil szakmai alapok megteremtését és állandó fejlesztését.

Az új szoftvereket nem az informatikusoknak kell használniuk, hanem a zömében még a digitális forradalom előtt szocializálódott elemző-értékelő és műveleti tiszteknek. Ezért az új informatikai képességek bevezetése során fejlesztői és végrehajtói oldalon is nagyfokú rugalmasságra van szükség, a vezetésnek pedig időt és lehetőséget kell biztosítania arra, hogy az érintettek érvényesíthessék szempontjaikat és elsajátíthassák az új eljárásokat.

---

[671] Vida Csaba a hírszerzési ciklust érő kritikák elemezve amellett érvel, hogy „*a ciklus a hírszerzési folyamat elméleti letükröződése és nem a gyakorlati megvalósulása*", „*az elmélet egy keretet biztosít annak érdekében, hogy az adott hírszerző szolgálat hatékonyan és eredményesen működjön, de a gyakorlat során figyelembe kell venni a szolgálat lehetőségeit, képességeit és helyzetét*."
VIDA Csaba: Létezik-e még a hírszerzési ciklus? Miről szól a hírszerzés? Felderítő Szemle, XII. évfolyam 1. szám, 2013. szeptember–október. pp. 43–57.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2013-1.pdf; letöltés: 2022.10.18.

A szervezeti kultúra megváltoztatásának és az új típusú gondolkodásmód minél szélesebb körű meghonosításának fontos eszköze a toborzás kiterjesztése a szolgálatok számára eddig ismeretlen szakterületekre. Ezen a téren különösen nagy hangsúlyt kaptak az adattudósok, az adatmenedzserek és az adatgondozók, akik kulcsfontosságú szerepet töltenek be nemcsak az MI-alapú elemző-értékelő rendszerek üzemeltetésében, hanem a hírszerzés rendszerének adatvezéreltté tételében is. A témában nyilvánosan megnyilatkozó amerikai nemzetbiztonsági vezetők hangsúlyozzák, hogy a speciális tudással rendelkező szakértők csak abban az esetben lehetnek hasznosak a nemzetbiztonsági rendszerben, ha a szolgálatok a tevékenységüket integrálják, vagyis kiterjedt nemzetbiztonsági háttértudást adnak nekik, és csapattagként kezelik őket. Ennek velejárója annak elfogadása is, hogy ezek az elhivatott, de nem a nemzetbiztonsági rendszerben szocializálódott szakemberek maguk is formálják a szervezeti kultúrát.

A nemzetbiztonsági MI-eszközöket előállító vállalatok többsége képzések széles körét is nyújtja, máshonnan nehezen megszerezhető ismereteket biztosítva a szolgálatoknak. Az új szaktudás megszerzése időigényes folyamat, ami szintén a megfontolt ütemű rendszeresítés mellett szól.

A nemzetbiztonsági munkatársak új generációjának tagjai (1) nem igénylik a mindennapi tevékenységük kézivezérlését, (2) ugyanakkor elvárják, hogy vezetőik világos feladatokat szabjanak számukra, (3) azokhoz egyértelmű hatáskört kapjanak, biztosítsák számukra a szükséges anyagi és szellemi eszközöket, kiemelt figyelemmel a képzésekre, és hogy (4) folyamatosan informálják őket a feladatokkal, a munkavégzéshez kapcsolódó együttműködéssel és a folyamatokkal kapcsolatban.

A humán munkaerő túlterheltségét a képzés és a szervezeti átalakítások önmagukban nem szüntetik meg, mert ahhoz nagyban hozzájárul az automatizálás hiánya vagy alacsony foka. Automatizálás hiányában a szolgálatok nem rendelkeznek a korszerűsítés kiterjesztéséhez szükséges kapacitásokkal. Az MI megfontolt, jól előkészített és a megfelelő munkafolyamatokra történő alkalmazása mentesítheti az állományt a rutinmunka – és az adminisztrációs terhek – egy része alól, kapacitást szabadítva fel a komplexebb, magasabb hozzáadott értékét jelentő feladatok végrehajtására.

Az új technológiák bevezetése megfelelő személyi és szervezeti előfeltételeinek elmaradása esetén a költséges fejlesztések nem vezetnek eredményre, sőt akadályozhatják a napi munkavégzést. Különös körültekintést igényel a betekintési jogosultságok érvényesítése az informatikai rendszerekben, amihez az informatikusok és a biztonságvédelmi szakemberek szoros együttműködése szükséges. Ennek elmaradása esetén szinte garantálható a titoksértés, de az ettől való félelem nem jelenthet kifogást a fejlesztések elmaradására. A „*need to know/right to know*” elvét megfelelő informatikai rendszerekkel jobban és biztonságosabban lehet érvényesíteni, mint a szakágak közötti – a hatékonyságot részben feláldozó – bürokratikus falak emelésével. A korszerű, dedikált nemzetbiztonsági szoftverrendszerek megfelelő alkalmazásával az „analóg” megoldásoknál összehasonlíthatatlanul magasabb szintű biztonság érhető el.

Fontos kihangsúlyozni, hogy reformokat folyamatosan, de óvatosan, dinamikus és kísérletező szemlélettel célszerű bevezetni. Az új megoldásokat célszerű kisebb csoportokban, kísérleti jelleggel alkalmazni, az így megszerzett tapasztalatokat szintetizálni, majd az egész rendszerre érvényesíteni. A részterületek reformját és azok egymásra gyakorolt hatását folyamatosan felül kell vizsgálni, lehetővé téve a gyors korrekciót. A kívánt kapacitások és az erőforrások megléte közötti dilemma feloldását a tervszerű kísérletezés jelentheti. A szolgálatok igényeik felmérése és a gyártók feltérképezését követően néhány munkaállomás működtetéséhez szükséges licence megvásárlásával tesztelhetik a lehetőségeket és megvizsgálhatják az új technológia nyújtotta lehetőségek integrálását a tevékenységükbe.

A szolgálatok rendkívül szerteágazó feladatköre miatt a szervezeti, a személyzeti és a technológiai reformokat követően is elkerülhetetlen az aktív együttműködés kialakítása az akadémiai szférával és a kutatóintézetekkel, a technológiai vállalatokkal, valamint a kereskedelemi tartalomszolgáltatókkal. Az együttműködésben a szolgálatoknak kell a vezető szerepet betölteniük, hiszen ők ismerik a döntéshozók információigényét és látják át a nemzeti érdekeket, továbbá a szolgálatok képesek összefogni a saját és a partnerszervezetek tevékenységét. Ideális esetben a szolgálatok biztosíthatják a hatékony együttműködést lehetővé tevő digitális infrastruktúrát is.

IRODALOMJEGYZÉK

1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt; letöltés: 2022.10.17.

1573/2020. (IX. 9.) Korm. határozat Magyarország Mesterséges Intelligencia Stratégiájáról, valamint a végrehajtásához szükséges egyes intézkedésekről. https://njt.hu/jogszabaly/2020-1573-30-22; letöltés: 2022.03.17.

2080/2008. (VI. 30.) Korm. határozat a Kritikus Infrastruktúra Védelem Nemzeti Programjáról. https://njt.hu/jogszabaly/2008-2080-30-22; letöltés: 2021.07.24.

A BAe Applied Intelligence honlapja. https://www.baesystems.com/en/cybersecurity/home; letöltés: 2021.07.21.

A BAe Applied Intelligence honlapja: Geospatial Intelligence. https://www.baesystems.com/en-us/product/geospatial-intelligence; letöltés: 2021.07.21.

A BlackSky honlapja. https://www.blacksky.com; letöltés: 2021.08.13.

A Cobwebs díjszabási brosúrája. https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/715532/220349016606958-pricing-document-2020-07-19-0913.pdf; letöltés: 2021.07.22.

A Cobwebs Technologies honlapja. https://cobwebs.com/; letöltés: 2021.07.21.

A Cobwebs Technologies honlapja: Active Web Intelligence. https://cobwebs.com/products/active-web-intelligence/; letöltés: 2021.07.21.

A Cobwebs Technologies honlapja: AI-Powered Web Intelligence. https://cobwebs.com/; letöltés: 2021.07.21.

A Cobwebs Technologies honlapja: Cobwebs' Threat Intelligence Platform. https://cobwebs.com/products/threat-intelligence-solution/; letöltés: 2021.07.21.

A Cobwebs Technologies honlapja: Location Intelligence System. https://cobwebs.com/products/location-intelligence-system/; letöltés: 2021.07.21.

A Cognyte honlapja. https://www.cognyte.com; letöltés: 2021.07.21.

A Cognyte honlapja: A Cognyte fúziós moduljának áttekintő nézete. https://www.cognyte.com; letöltés: 2021.07.21.

A Cognyte honlapja: Web Intelligence. https://www.cognyte.com/web-intelligence/; letöltés: 2021.07.21.

A Gamma Group honlapja: Products & Services. https://www.gammagroup.com/ProductsServices.aspx?m=p; letöltés: 2021.07.21.

A gépi látás. Műszaki Magazin, 2019.09.28.
http://muszaki-magazin.hu/2019/09/28/a-gepi-latas/; letöltés: 2020.03.11.

A Google állítja: elérte a kvantumfölényt. HVG, 2019.10.23.
https://hvg.hu/tudomany/20191023_A_Google_allitja_elerte_a_kvantumfelsobbrenduseget; letöltés: 2019.12.06.

A Maxar Technologies honlapja.
https://www.maxar.com/; letöltés: 2021.12.22.

A Medusa Labs honlapja.
https://www.medusa-labs.com/; letöltés: 2021.07.21.

A mesterséges intelligencia stratégia megvalósítása az MI-alkalmazások bevezetését segítő központok létrehozásával folytatódik. MI Koalíció, 2021.06.17.
https://ai-hungary.com/hu/hirek/sajtomegjelenesek-kozlemenyek/a-mesterseges-intelligencia-strategia-megvalositasa-az-mi-alkalmazasok-bevezeteset-segito-kozpontok-letrehozasaval-folytatodik; letöltés: 2021.07.19.

A Microsoft nyerte a Pentagon 10 milliárd dolláros informatikai pályázatát.
hirado.hu, 2019.10.26.
https://hirado.hu/tudomany-high-tech/high-tech/cikk/2019/10/26/a-microsoft-nyerte-a-pentagon-10-milliard-dollaros-informatikai-palyazatat; letöltés: 2019.10.26.

A Palantir honlapja.
https://www.palantir.com/; letöltés: 2021.12.22.

A Rayzone Group honlapja: ECHO – Global Virtual SIGINT System.
https://rayzone.com/echo-global-virtual-sigint-system/; letöltés: 2021.07.21.

A SZTAKI vezetésével elindult a Mesterséges Intelligencia Nemzeti Kutatólaboratórium és az Autonóm Rendszerek Nemzeti Kutatólaboratórium. SZTAKI, 2020.09.25.
https://www.sztaki.hu/kormanyzat/hirek/sztaki-vezetesevel-elindult-az-mi-es-az-autonom-nemzeti-kutatolaboratorium; letöltés: 2021.05.26.

A Tanács 6/2012/EU álláspontja első olvasatban a kettős felhasználású termékek kivitelére, transzferjére, brókertevékenységére és tranzitjára vonatkozó közösségi ellenőrzési rendszer kialakításáról szóló 428/2009/EK tanácsi rendelet módosításáról. 2012.02.21.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:107E:0001:0273:HU:PDF; letöltés: 2021.03.14.

A Text Encoding Initiative honlapja.
https://tei-c.org; letöltés: 2020.04.27.

AFTERGOOD, Steven: Open Source Center (OSC) Becomes Open Source Enterprise (OSE). FAS, 2015.10.28.
https://fas.org/blogs/secrecy/2015/10/osc-ose/; letöltés: 2022.02.16.

AJP 3.10 – Allied Joint Doctrine For Information Operations. NATO, November 2009.
https://info.publicintelligence.net/NATO-IO.pdf; letöltés: 2021.07.20.

ALESSA, Lilian: Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.30.

Automated Vision Inspection Benches IVS-MALi-A.
https://www.industrialvision.co.uk/products/automated-vision-inspection-bench-ivs-mali-a; letöltés: 2020.03.11.

Az Airbus JOINT ISR honlapja.
https://www.intelligence-airbusds.com/markets/defence/joint-isr/; letöltés: 2021.12.20.

Az ATIS systems honlapja: Klarios ATIS Interception Management System.
https://www.atis-systems.com/language/en/klarios-atis-interception-management-system/;
letöltés: 2021.07.21.

Az Etiya honlapja: Easy to use and flexible interface, personalized campaigns.
Next generation campaign management.
https://www.etiya.com/en/products/campaign-management?gclid=CjwKCAjwi9-HBhACEiwAPzUhHKcGUXLlNfQTKAaL_wNaS1gYxr6bFJpU_3HNhwX7T1rwaA40cA8H2hoCn0kQAvD_BwE; letöltés: 2021.07.22.

Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet).
https://eur-lex.europa.eu/HU/legal-content/summary/general-data-protection-regulation-gdpr.html; letöltés: 2022.10.25.

Az IBM honlapja: IBM Security i2 Analyst's Notebook.
https://www.ibm.com/hu-en/products/i2-analysts-notebook; letöltés: 2021.07.23.

Az IntelligenceReveal OSI-platform brosúrája.
https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92253/645404904066643-service-definition-document-2020-07-17-1447.pdf; letöltés: 2021.07.22.

Az IntelligenceReveal OSI-platform díjszabási katalógusa.
https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92253/645404904066643-pricing-document-2020-07-17-1455.pdf; letöltés: 2021.07.22.

BALL, Mike: Remote UAS Swarm Launching Technology Demonstrated.
Unmanned Systems Technology, 2020.10.30.
https://www.unmannedsystemstechnology.com/2020/10/remote-uas-swarm-launching-technology-demonstrated/; letöltés: 2022.08.13.

BALOGH Péter: Rádióelektronikai felderítés (SIGINT).
In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban.
Dialóg Campus Kiadó, Budapest, 2018. pp. 142–154.
https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

BARANIUK, Chris: China's Xinhua agency unveils AI news presenter. BBC, 2018.11.08.
https://www.bbc.com/news/technology-46136504; letöltés: 2020.11.16.

BARKER, Shane: 15 of the Best AI Chatbot Platforms to Increase Your Conversions in 2020.
Martech Cube, 2020.07.29.
https://www.martechcube.com/best-ai-chatbot-platforms-to-increase-your-conversions-2020/;
letöltés: 2020.08.11.

BARLOW, Sonya: Can we trust machines to predict the stock market with 100% accuracy?
Metro, 2019.05.06.
https://metro.co.uk/2019/05/06/can-we-trust-machines-to-predict-the-stock-market-with-100-accuracy-9325480/; letöltés: 2020.03.11.

BARRETT, Richard – EL-SAID, Hamed: Enhancing the Understanding of the Foreign Terrorist Fighters Phenomenon in Syria. United Nations Office of Counter-Terrorism, July 2017. https://f-origin.hypotheses.org/wp-content/blogs.dir/2725/files/2018/02/ONU_Report_Final_2017.pdf; letöltés: 2018.11.15.

BERKÁNÉ DANESCH Marianne (szerk.) – M. SZABÓ Miklós – MEZŐ András (katonai szakmai szerk.): Katonai terminológiai értelmező szótár. Zrínyi Kiadó, Budapest, 2015.

Best AI Writing Assistant Software. G2, 2020. https://www.g2.com/categories/ai-writing-assistant; letöltés: 2020.03.11.

BHATTACHARJEE, Barnil – TIRBASO, James: Activate VAULTIS - Self-Service Data Analytics to Kickstart 2020 DoD Data Strategy Implementation. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.29.

BIMFORT, Martin T.: A Definition of Intelligence. Studies of Intelligence, Volume 2, Issue 4, Fall 1958. pp. 75–78. https://www.cia.gov/static/A-Definition-Of-Intelligence.pdf; letöltés: 2020.04.29.

BRENNAN, John: Our Agency's Blueprint for the Future (Unclassified Version of March 6, 2015 Message to the Workforce from CIA Director). CIA, 2015.03.06. https://www.cia.gov/news-information/press-releases-statements/2015-press-releases-statements/message-to-workforce-agencys-blueprint-for-the-future.html; letöltés: 2017.06.06.

BREWSTER, Thomas: Exclusive: Israeli Surveillance Companies Are Siphoning Masses Of Location Data From Smartphone Apps. Forbes, 2020.12.11. https://www.forbes.com/sites/thomasbrewster/2020/12/11/exclusive-israeli-surveillance-companies-are-siphoning-masses-of-location-data-from-smartphone-apps/; letöltés: 2021.07.22.

BROOKS, Aaron: 10 Best Chatbot Builders in 2020. Venture Harbour, 2020. https://www.ventureharbour.com/best-chatbot-builders/; letöltés: 2020.03.11.

Brussels Summit Communiqué. NATO, 2021.06.14. https://www.nato.int/cps/en/natohq/news_185000.htm; letöltés: 2021.12.30.

Build to Scale: Maximizing AI/ML Impact across the DoD. JAIC Public Affairs, 2020.11.13. https://www.ai.mil/blog_11_13_20-build_to_scale_maximizing_al-ml_impact_across_the_dod.html; letöltés: 2021.08.13.

BYMAN, Daniel: Beyond Iraq and Syria: ISIS' ability to conduct attacks abroad. Brookings, 2017.06.08. https://www.brookings.edu/testimonies/beyond-iraq-and-syria-isis-ability-to-conduct-attacks-abroad; letöltés: 2018.11.15.

Central Security Service (CSS). NSA, 2019. https://www.nsa.gov/about/central-security-service/; letöltés: 2019.05.13.

CIA Leadership (2018). https://www.cia.gov/about-cia/leadership; letöltés: 2019.05.11.

CIA Organizational Chart. https://irp.fas.org/cia/orgchart.pdf; letöltés: 2021.12.25.

COOKE, Sam: Does the adoption of AI open up 'flash crash' trading exposure? Totally Gaming, 2017.09.18. https://totallygaming.com/news/features/does-adoption-ai-open-flash-crash-trading-exposure; letöltés: 2021.08.12.

COOLSAET, Rik – RENARD, Thomas: The Homecoming of Foreign Fighters in the Netherlands, Germany and Belgium: Policies and Challenges. ICCT, 2018.04.11. https://www.icct.nl/publication/homecoming-foreign-fighters-netherlands-germany-and-belgium-policies-and-challenges; letöltés: 2018.11.15.

Coordinated Plan on Artificial Intelligence 2021 Review. European Commission, 2021.04.21. https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review; letöltés: 2022.07.24.

Coordinated Plan on Artificial Intelligence. European Commission, 2018.12.07. https://ec.europa.eu/digital-single-market/en/news/coordinated-plan-artificial-intelligence; letöltés: 2019.12.09.

Cyber defence. NATO, 2021. https://www.nato.int/cps/en/natohq/topics_78170.htm; letöltés: 2021.07.20.

DAVIDSON, Tom: "Attack them with truck or car": ISIS release sick pamphlets with tips on successful terror attacks during World Cup. Mirror, 2018.05.15. https://www.mirror.co.uk/news/world-news/attack-truck-car-isis-release-12541581; letöltés: 2021.04.16.

DCE's X Series is a range of high capability, affordable, tracked all-terrain unmanned ground vehicles. Digital Concepts Engineering, 2022. https://dconcepts.co.uk/products/x-series; letöltés: 2022.08.13.

Deep Blue. IBM 100. https://www.ibm.com/ibm/history/ibm100/us/en/icons/deepblue/; letöltés: 2021.08.12.

Deepak Chopra and the AI Foundation Partner to Bring Personal Transformation to Billions with the Power of Deepak's Own AI. Business Wire, 2019.12.05. https://www.businesswire.com/news/home/20191205005164/en/Deepak-Chopra-and-the-AI-Foundation-Partner-to-Bring-Personal-Transformation-to-Billions-with-the-Power-of-Deepak%E2%80%99s-Own-AI; letöltés: 2020.11.16.

Defence Artificial Intelligence Strategy. Ministry of Defence, 2022.06.15. https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy; letöltés: 2022.08.12.

Definition of Counterintelligence. National Security Council Intelligence Directive No. 5, 1957. https://www.cia.gov/readingroom/docs/CIA-RDP85S00362R000600160015-2.pdf; letöltés: 2020.04.29.

Description of the National Military Strategy. The Joint Staff, 2018. https://www.jcs.mil/Portals/36/Documents/Publications/UNCLASS_2018_National_Military_Strategy_Description.pdf; letöltés: 2022.08.12.

Digitális Agrárakadémia. https://www.digitalisagrarakademia.hu/; letöltés: 2021.07.20.

Director of National Intelligence Mission Managers. DNI, 2005.11.15. https://fas.org/irp/dni/icpm/2005-100-2.pdf; letöltés: 2019.04.26.

Disruptive Technology for Defence Transformation. A Defence iQ és a brit Védelmi Akadémia 2019. szeptember 24–26-án Londonban rendezett konferenciája.

Donald Trump elnök 2019. február 11-ei, 13859. számú rendelete.
Maintaining American Leadership in Artificial Intelligence.
Federal Register, Vol. 84, No. 31, 2019.02.14. pp. 3967–3972.
https://www.govinfo.gov/content/pkg/FR-2019-02-14/pdf/2019-02544.pdf; letöltés: 2019.12.05.

DRÓT László: Az OODA hurok (I. rész).
Seregszemle, 16. évfolyam 1. szám, 2018. január–március. pp. 143–159.
https://honvedelem.hu/files/files/115176/seregszemle_2018_1.pdf; letöltés: 2021.12.20.

EDEN, Ammon H. – STEINHART, Eric – PEARCE, David – MOOR, James H.:
Singularity Hypotheses: An Overview. Introduction to: Singularity Hypotheses:
A Scientific and Philosophical Assessment. Springer, New York, 2012. pp. 1–12.
https://repository.essex.ac.uk/9220/1/Singularity%20Hypothesis.pdf; letöltés: 2019.12.06.

e-Governance. e-Estonia. Az észt kormány tájékoztató honlapja az e-közigazgatásról.
https://e-estonia.com/solutions/e-governance/; letöltés: 2020.03.11.

Egy éve alakult meg a mesterséges intelligencia koalíció.
Magyarország Kormánya, 2019.10.18.
https://2015-2019.kormany.hu/hu/innovacios-es-technologiai-miniszterium/infokommunikacioert-es-fogyasztovedelemert-felelos-allamtitkar/hirek/egy-eve-alakult-meg-a-mesterseges-intelligencia-koalicio; letöltés: 2019.12.06.

Electronic Systems – What's on show? Farnborough International Airshow 2018. Find out more about the Electonic Systems products on show this year. BAe Systems, 2018.07.23.
https://www.baesystems.com/cs/Satellite?c=BAEStandardArticle_C&childpagename=UK%2FBAELayout&cid=1434614801231&pagename=UKWrapper; letöltés: 2021.07.22.

Emerging and disruptive technologies. NATO, 2021.06.03.
https://www.nato.int/cps/en/natohq/topics_184303.htm; letöltés: 2021.12.30.

Emerging Military Technologies: Background and Issues for Congress. CRS Report, 2020.
https://fas.org/sgp/crs/natsec/R46458.pdf; letöltés: 2021.08.13.

ERDÉSZ Viktor – NAGY Viktor: Az információs védelem és az információs műveletek szerepe a nemzetvédelemben. Felderítő Szemle, X. évfolyam 3–4. szám, 2011. szeptember–december, XI. évfolyam 1. szám, 2012. március. pp. 50–62.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2011-3-4-2012-1.pdf; letöltés: 2021.12.16.

ERDÉSZ Viktor: Az amerikai hírszerzési reform és tanulságai.
Felderítő Szemle, XVIII. évfolyam 3. szám, 2019. pp. 111–128.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2019-3.pdf; letöltés: 2020.02.14.

EVERSDEN, Andrew: Pentagon creates new overseer for innovation: chief digital and artificial intelligence officer. Breaking Defense, 2021.12.08.
https://breakingdefense.com/2021/12/pentagon-creates-new-overseer-for-innovation-chief-digital-and-artificial-intelligence-officer/; letöltés: 2021.12.09.

Executive Order 12333 – United States intelligence activities. National Archives, 1981.
https://www.archives.gov/federal-register/codification/executive-order/12333.html;
letöltés: 2019.05.11.

Executive Summary: DoD Data Strategy – Unleashing Data to Advance the National Defense Strategy (2020).
https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF;
letöltés: 2020.12.16.

Factsheet: Artificial Intelligence for Europe. European Commission, 2019.07.04. https://ec.europa.eu/digital-single-market/en/news/factsheet-artificial-intelligence-europe; letöltés: 2019.12.09.

FARKAS Ferenc: A változásmenedzsment elmélete és gyakorlata. Akadémiai Kiadó, Budapest, 2013.

FEDASIUK, Ryan: Chinese Perspectives on AI and Future Military Capabilities. CSET, August 2020. https://cset.georgetown.edu/research/chinese-perspectives-on-ai-and-future-military-capabilities/; letöltés: 2021.03.16.

FENYŐVÁRI Bernadett: Az észt e-kormányzás titka. Lechner Tudásközpont, 2019.03.28. http://lechnerkozpont.hu/cikk/az-eszt-e-kormanyzas-titka; letöltés: 2020.03.11.

Fighting Terrorism Online: Internet Forum pushes for automatic detection of terrorist propaganda. European Commission, 2017.12.06. http://europa.eu/rapid/press-release_IP-17-5105_en.pdf; letöltés: 2018.11.15.

G20 Ministerial Statement on Trade and Digital Economy. 3. pont: Human-centered Artificial Intelligence (AI). 2019. június. https://www.mofa.go.jp/files/000486596.pdf; letöltés: 2021.07.17.

GANON, Tomer – RAVET, Hagar: The Rayzone Group's secret cyber intelligence activities revealed. CTech, 2020.12.29. https://www.calcalistech.com/ctech/articles/0,7340,L-3884553,00.html; letöltés: 2021.07.22.

GAZDAG Ferenc – REMEK Éva: A biztonsági tanulmányok alapjai. Dialóg Campus Kiadó, Budapest, 2018. pp. 21–24. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12604; letöltés: 2022.10.17.

Georgia, Russia: The Cyberwarfare Angle. A Stratfor kutatóintézet elemzése. RANE, 2008.08.12. https://worldview.stratfor.com/article/georgia-russia-cyberwarfare-angle; letöltés: 2020.03.12.

GIBBS, Samuel: AlphaZero AI beats champion chess program after teaching itself in four hours. The Guardian, 2017.12.07. https://www.theguardian.com/technology/2017/dec/07/alphazero-google-deepmind-ai-beats-champion-program-teaching-itself-to-play-four-hours; letöltés: 2021.08.12.

Global Britain in a competitive age – The Integrated Review of Security, Defence, Development and Foreign Policy. HM Government, March 2021. pp. 17–21. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy; letöltés: 2022.08.12.

Goldwater-Nichols Department of Defense Reorganization Act of 1986. Public Law 99-433, 1986.10.01. https://history.defense.gov/Portals/70/Documents/dod_reforms/Goldwater-NicholsDoDReordAct1986.pdf; letöltés: 2019.05.11.

Green Paper on a European Programme for Critical Infrastructure Protection. Európai Bizottság, Brüsszel, 2005.11.17. https://op.europa.eu/en/publication-detail/-/publication/4e3f9be0-ce1c-4f5c-9fdc-07bdd441fb88/language-en; letöltés: 2021.07.20.

HAIG Zsolt – VÁRHEGYI István: A cybertér és a cyberhadviselés értelmezése. Hadtudomány, 18. évfolyam elektronikus szám, 2008. https://www.mhtt.eu/hadtudomany/2008/2008_elektronikus/2008_e_2.pdf; letöltés: 2021.07.20.

HARARI, Yuval Noah: Homo Deus: A jövő rövid története.
Animus Kiadó, Budapest, 2016.

HARARI, Yuval Noah: Sapiens: Az emberiség rövid története.
Animus Kiadó, Budapest, 2015.

HARIDY, Rich: Real "fake news": China introduces AI news anchor. New Atlas, 2018.11.08.
https://newatlas.com/china-ai-digital-news-anchor/57158/; letöltés: 2020.11.16.

HARPER, Jon: Space Force Has High Hopes for New Missile Warning Satellites.
National Defense, 2021.07.16.
https://www.nationaldefensemagazine.org/articles/2021/7/16/space-force-has-high-hopes-for-new-missile-warning-satellites; letöltés: 2021.12.23.

HORVÁTH Csongor: Az adatgyűjtés-koordináló és felderítési követelmények menedzsmentje.
Honvédségi Szemle, 146. évfolyam 4. szám, 2018. pp. 71–78.
http://real-j.mtak.hu/16399/4/Honvedsegi_Szemle_2018_4_teljes_szam.pdf; letöltés: 2021.12.27.

IGNATIUS, David: Will John Brennan's controversial CIA modernization survive Trump?
The Washington Post, 2017.01.17.
https://www.washingtonpost.com/opinions/will-john-brennans-controversial-cia-modernization-survive-trump/2017/01/17/54e6cc1c-dcd5-11e6-ad42-f3375f271c9c_story.html; letöltés: 2017.06.06.

Intelligence Community Directive 101 – Intelligence Community Policy System.
ODNI, 2019.10.22.
www.dni.gov/files/documents/ICD/ICD_101.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 103 – Intelligence Enterprise Exercise Program.
ODNI, 2008.07.14.
www.dni.gov/files/documents/ICD/ICD_103.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 113 – Functional Managers. ODNI, 2009.05.19.
https://www.dni.gov/files/documents/ICD/ICD_113.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 116 – Intelligence Planning, Programming, Budgeting, and Evaluation System. ODNI, 2011.09.14.
https://www.dni.gov/files/documents/ICD/ICD_116.pdf; letöltés: 2019.11.01.

Intelligence Community Directive 203 – Analytic Standards. ODNI, 2015.01.02.
https://www.dni.gov/files/documents/ICD/ICD_203_TA_Analytic_Standards_21_Dec_2022.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 204 – National Intelligence Priorities Framework.
ODNI, 2015.01.02.
https://www.dni.gov/files/documents/ICD/ICD_204_National_Intelligence_Priorities_Framework_U_FINAL-SIGNED.pdf; letöltés: 2019.04.26.

Intelligence Community Directive 205 – Analytic Outreach. ODNI, 2013.08.28.
https://www.dni.gov/files/documents/ICD/ICD 205 - Analytic Outreach.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 206 – Sourcing Requirements for Disseminated Analytic Products. ODNI, 2015.01.22.
https://www.dni.gov/files/documents/ICD/ICD 206.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 207 – National Intelligence Council. ODNI, 2008.06.09.
https://www.dni.gov/files/documents/ICD/ICD_207.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 208 – Maximising the Utility of Analytic Products. ODNI, 2017.01.09. https://www.dni.gov/files/documents/ICD/ICD 208 - Maximizing the Utility of Analytic Products (09 Jan 2017).pdf; letöltés: 2019.10.29.

Intelligence Community Directive 209 – Tearline Production and Dissemination. ODNI, 2012.09.06. https://www.dni.gov/files/documents/ICD/ICD 209 Tearline Production and Dissemination.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 404 – Executive Branch Intelligence Customers. ODNI, 2013.07.22. https://www.dni.gov/files/documents/ICD/ICD 404-Executive Branch Intelligence Customers.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 501 – Discovery and Dissemination or Retrieval of Information within the Intelligence Community. ODNI, 2009.01.21. www.dni.gov/files/documents/ICD/ICD_501.pdf; letöltés: 2019.10.29.

Intelligence Community Directive 900 – Integrated Mission Management. ODNI, 2013.05.06. www.dni.gov/files/documents/ICD/ICD 900 - Integrated Mission Managemement.pdf; letöltés: 2019.10.29.

Intelligence Community Directives. Office of the Director of National Intelligence. https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives; letöltés: 2019.10.29.

International Strategy for Cyberspace – Prosperity, Security, and Openness in a Networked World. The White House, Washington, May 2011. https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf; letöltés: 2021.07.20.

Introducing BlackSky Spectra. BlackSky, 2017.04.04. https://www.blacksky.com/2017/04/04/introducing-blacksky-spectra/; letöltés: 2021.08.13.

Iran Confirms Stuxnet Worm Halted Centrifuges. CBS News, 2010.11.29. https://www.cbsnews.com/news/iran-confirms-stuxnet-worm-halted-centrifuges/; letöltés: 2021.12.29.

Jim Richberg volt kiberfenyegetésekért felelős NIM Linkedin-profilja. https://www.linkedin.com/in/jim-richberg; letöltés: 2019.04.26.

June 26, 2017 Speech to the Institute for Corean-American Studies: North Korea's Nuclear Weapons and Missile Capability -- Scott W. Bray, National Intelligence Manager for East Asia. https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2017/3138-speech-to-the-institute-for-corean-american-studies-north-korea-s-nuclear-weapons-and-missile-capability; letöltés: 2019.04.26.

KALWEIT, Susan: Mission Intensity: Thriving in the Smart Machine Age - The Making of the Equation to Assure Fast and Reliable Analysis.
A National Geospatial Intelligence Agency elemző-értékelő igazgatójának előadása az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.29.

KAMARA, Hassan M.: Hunting the Adversary – Sensors in the 2035 Battlespace. Military Review – The Professional Journal of the U.S. Army, January-February 2021. pp. 34–41. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/JF-21/Kamara-Hunting-the-Adversary-1.pdf; letöltés: 2021.12.23.

KARI, Al – LANDER, Garrett: Could an Adversarial Bot Manipulate the Stock Market? Manceps, 2019.11.18.
https://www.manceps.com/articles/experiments/beat-the-bots; letöltés: 2020.03.11.

KEMP, Simon: Digital in 2018: World's internet users pass the 4 billion mark.
We Are Social, 2018.01.30.
https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018/; letöltés: 2022.04.26.

KIS-BENEDEK József: Az emberi erőkkel folytatott információszerzés (HUMINT).
In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban.
Dialóg Campus Kiadó, Budapest, 2018. pp. 154–161.
https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

KLEINEMEIER, Michael: How Governments Use AI To Create Better Experiences For Citizens. Forbes, 2019.11.07.
https://www.forbes.com/sites/sap/2019/11/07/how-governments-use-ai-to-create-better-experiences-for-citizens/?sh=6bba0cad799c; letöltés: 2020.03.11.

KOVÁCS László – KRASZNAY Csaba: Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 3. évfolyam 2. szám, 2010. február. pp. 44–56.
https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/1013; letöltés: 2022.10.25.

KRUYS, George P. H.: Intelligence failures: causes and contemporary case studies.
Strategic Review for Southern Africa, Volume 28, Issue 1, 2006. pp. 63–96.
https://repository.up.ac.za/bitstream/handle/2263/3078/Kruys_Intelligence(2006).pdf?sequence=1; letöltés: 2018.12.03.

Kulturális Enciklopédia: A posztmodern.
http://enciklopedia.fazekas.hu/irodalom/Posztmodern.htm; letöltés: 2018.11.15.

LAFRANCHI, Howard: Iran's Bushehr nuclear plant delayed: Stuxnet not to blame, official says.
The Christian Science Monitor, 2010.10.04.
https://www.csmonitor.com/USA/Foreign-Policy/2010/1004/Iran-s-Bushehr-nuclear-plant-delayed-Stuxnet-not-to-blame-official-says; letöltés: 2022.09.12.

LEWIS, James A.: Cyber War and Ukraine. CSIS, June 2022.
https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/220616_Lewis_Cyber_War.pdf?S.iEKeom79InugnYWlcZL4r3Ljuq.ash; letöltés: 2022.08.14.

LEWIS, James Andrew: Securing Cyberspace for the 44th Presidency.
Center for Strategic and International Studies, 2008.12.08.
https://www.csis.org/analysis/securing-cyberspace-44th-presidency; letöltés: 2021.07.20.

LOVÁSZ Dávid: A véleménybuborék jelensége a közösségi médiában. Kalauz, 2017.
https://kalauz.lib.pte.hu/velemenybuborek-jelensege-kozossegi-mediaban/#dn01; letöltés: 2018.11.14.

LOWENTHAL, Mark M. – CLARK, Robert M.: The Five Disciplines of Intelligence Collection.
Thousand Oaks, CQ Press, 2015.

LOWENTHAL, Mark M.: Hírszerzés – A titkoktól a politikai döntésekig.
Antall József Tudásközpont, Budapest, 2017.

Magyarország Mesterséges Intelligencia Stratégiája 2020–2030.
Digitális Jólét Nonprofit Kft., 2020. május.
https://ai-hungary.com/api/v1/companies/15/files/137203/view; letöltés: 2022.03.21.

Maritime Demonstrator for Operational eXperimentation (MADFOX) Uncrewed Surface Vessel, UK. Naval Technology, 2021.10.21.
https://www.naval-technology.com/projects/maritime-demonstrator-for-operational-experimentation-madfox; letöltés: 2022.08.13.

MARR, Bernard: What is Machine Vision And How Is It Used In Business Today? Forbes, 2019.10.11.
https://www.forbes.com/sites/bernardmarr/2019/10/11/what-is-machine-vision-and-how-is-it-used-in-business-today/#7317b8276939; letöltés: 2020.03.11.

Maxar 3D Data Integrated Into Swedish Gripen Fighter Jet for GPS-Denied Navigation. Maxar Technologies, 2021.10.04.
https://blog.maxar.com/earth-intelligence/2021/maxar-3d-data-integrated-into-swedish-gripen-fighter-jet-for-gps-denied-navigation; letöltés: 2021.12.22.

MCFARLAND, Katharina: Mission Focused: The Mission to Integrate Artificial Intelligence into the Military's Future Battle Rhythm. The Cipher Brief, 2021.03.10.
https://www.thecipherbrief.com/column_article/the-mission-to-integrate-artificial-intelligence-into-the-militarys-future-battle-rhythm; letöltés: 2021.12.22.

Megalakult a Nemzeti Adatvagyon Ügynökség. Magyarország Kormánya, 2020.10.20.
https://kormany.hu/hirek/megalakult-a-nemzeti-adatvagyon-ugynokseg; letöltés: 2021.05.26.

Mi is az a „Big Data”? Fogalmak, definíciók és egyéb tudnivalók.
nagy;adat;blog; 2014.03.03.
https://nagyadat.blog.hu/2014/03/03/what-is-big-data; letöltés: 2022.11.15.

MIKHEEV, Evgeny A. – NESTIK, Timofey, A.: The Use of Artificial Intelligence Technologies in Information and Psychological Warfare. In: PSYRGGU 2019 – Psychology of subculture: Phenomenology and Contemporary Tendencies of Development. The European Proceedings of Social & Behavioural Sciences, 2019.
https://www.europeanproceedings.com/files/data/article/109/5743/article_109_5743_pdf_100.pdf; letöltés: 2020.03.11.

MILLER, Greg: DIA to send hundreds more spies overseas. The Washington Post, 2012.12.01.
https://www.washingtonpost.com/world/national-security/dia-to-send-hundreds-more-spies-overseas/2012/12/01/97463e4e-399b-11e2-b01f-5f55b193f58f_story.html; letöltés: 2018.12.03.

MINNAAR, Joost: The Evolution Of (Progressive) Scalable Organizational Structures. Corporate Rebels, 2020.11.18.
https://corporate-rebels.com/the-evolution-of-progressive-organizational-structures/; letöltés: 2021.12.24.

MORELLE, Rebecca: Google machine learns to master video games. BBC, 2015.02.25.
https://www.bbc.com/news/science-environment-31623427; letöltés: 2021.08.12.

MORTIMORE, David: National Strategy for Critical and Emerging Tech Strategy Released. The Scuttlebutt Blog, 2020.10.15.
https://nps.edu/web/slamr/-/2020-national-strategy-for-critical-emerging-technologies; letöltés: 2022.08.12.

MRUNMAYI, Sapatnekar: 10 Powerful Content Automation AI Tools to Replace Content Writers. Staenz, 2019.
https://staenz.com/content-automation-ai-tools/; letöltés: 2020.03.11.

Multi-disciplinary Intelligence Analyst – Measurement and Signature Intelligence (MASINT) provides real-time analysis and dissemination to facilitate your Collection Strategy. AUC3I. https://www.auc3i.com/index-114.php; letöltés: 2021.12.23.

MUNK Sándor: A kritikus infrastruktúrák védelme információs támadások ellen. Hadtudomány, 18. évfolyam 1–2. szám, 2008. pp. 95–106. https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/2224; letöltés: 2022.10.27.

MURDICK, Dewey: CSET's Data Science Efforts and Open Source Analysis on China's Emerging Technologies.
A CSET adattudományi igazgatójának előadása az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.30.

National Counterintelligence Strategy of the United States of America 2020-2022. NCSC, 2020.
https://www.dni.gov/files/NCSC/documents/features/20200205-National_CI_Strategy_2020_2022.pdf; letöltés: 2022.08.03.

National Cyber Strategy of the United States of America.
The White House, Washington, September 2018.
https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf; letöltés: 2021.07.20.

National Defense Strategy of the United States of America.
U.S. Department of Defense, 2022.10.27.
https://media.defense.gov/2022/Oct/27/2003103845/-1/-1/1/2022-NATIONAL-DEFENSE-STRATEGY-NPR-MDR.PDF; letöltés: 2022.11.09.

National Intelligence Council (NIC) Collection.
https://www.cia.gov/library/readingroom/collection/national-intelligence-council-nic-collection; letöltés: 2019.04.26.

National Security Act of 1947.
https://www.intelligence.senate.gov/sites/default/files/laws/nsact1947.pdf; letöltés: 2019.04.25.

National Security Strategy. The White House, Washington, October 2022.
https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf; letöltés: 2022.11.09.

NATO - STANAG 6524 (Restricted): Intelligence Requirement Management and Collection Management – AIntP-16 Edition A: a NATO jelenleg hatályos, korlátozott terjesztésű minősítésű dokumentumát 2018. december 17-én adták ki.

NELSON, Matthew: Lockheed to Update Navy MASINT Platform Under Potential $90M Contract. GovCon Wire, 2020.04.07.
https://www.govconwire.com/2020/04/lockheed-to-update-navy-masint-platform-under-potential-90m-contract/; letöltés: 2021.12.23.

ODNI Factsheet. DNI, 2017.02.14.
https://www.dni.gov/files/documents/FACTSHEET_ODNI_History_and_Background_2_24-17.pdf; letöltés: 2019.04.24.

OECD.AI. A Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) mesterséges intelligenciával foglalkozó honlapja.
https://oecd.ai/en/dashboards; letöltés: 2021.12.29.

OMAND, David – BARTLETT, Jamie – MILLER, Carl: #Intelligence. London, Demos, 2012. https://demos.co.uk/wp-content/uploads/2012/04/intelligence-Report.pdf; letöltés: 2018.11.05.

Organizational structure of the Central Intelligence Agency. https://en.wikipedia.org/wiki/Organizational_structure_of_the_Central_Intelligence_Agency; letöltés: 2021.12.24.

ÖTVÖS Zoltán: Hamarosan üzembe áll a nagy teljesítményű Komondor. Magyar Nemzet, 2022.10.29. https://magyarnemzet.hu/lugas-rovat/2022/10/levente-es-a-komondor; letöltés: 2022.11.10.

Palantir Gotham service definition document (2020). https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92736/668463552506354-service-definition-document-2020-07-13-1355.pdf; letöltés: 2021.12.22.

Palantir software and support pricing document (2021). https://assets.digitalmarketplace.service.gov.uk/g-cloud-12/documents/92736/668463552506354-pricing-document-2021-04-15-1025.pdf; letöltés: 2021.12.22.

PARIKH, Prasham: CES 2020: Samsung STAR Labs Just Created An 'Artificial Human' Called NEON. Mashable India, 2020.01.07. https://in.mashable.com/tech/10199/ces-2020-samsung-star-labs-just-created-an-artificial-human-called-neon; letöltés: 2020.03.11.

PARISER, Eli: The Filter Bubble: What The Internet Is Hiding From You. A szerző 2011. június 20-ai előadásának pdf-változata. http://www.lse.ac.uk/assets/richmedia/channels/publicLecturesAndEvents/slides/20110620_1830_theFilterBubble_sl.pdf; letöltés: 2018.11.22.

PITTMAN, Travis: Az East View tartalomszolgáltató vállalat bemutatása. Előadás az IDGA Intelligence Analytics Summit rendezvényén, 2020.10.30.

PORKOLÁB Imre: A stratégia művészete – Szervezeti innováció kiszámíthatatlan üzleti környezetben – Szun-ce gondolatai alapján. HVG Könyvek, Budapest, 2019.

Preliminary study on the Ethics of Artificial Intelligence. UNESCO – COMEST, Paris, 2019.02.26. https://unesdoc.unesco.org/ark:/48223/pf0000367823; letöltés: 2021.07.15.

Project Grey Goose Phase II Report: The evolving state of cyber warfare. Greylogic, 2009.03.20. http://www.fistfulofgold.com/Documents/ProjectGreyGoose.pdf; letöltés: 2021.07.20.

PRZETACZNIK, Jakub – TARPOVA, Simona: Russia's war on Ukraine: Timeline of cyber-attacks. European Parliamentary Research Service, 2022. https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf; letöltés: 2022.08.14.

Realizing Society 5.0. A japán kormány tájékoztató brosúrája. https://www.japan.go.jp/abenomics/_userdata/abenomics/pdf/society_5.0.pdf; letöltés: 2020.03.11.

Recommendation of the Council on Artificial Intelligence. OECD Legal Instruments, 2019.05.22. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449; letöltés: 2021.07.12.

REDING, D. F. – EATON, J.: Science & Technology Trends 2020-2040. Exploring the S&T Edge. NATO Science & Technology Organization, 2020. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/4/pdf/190422-ST_Tech_Trends_Report_2020-2040.pdf; letöltés: 2021.12.23.

RENNERT, Aaron: The Nasdaq Exchange Embraces AI: Market Manipulation Mitigation Built for the Future, 2019.08.05. https://www.rebellionresearch.com/blog/the-nasdaq-exchange-embraces-ai-market-manipulation-mitigation-built-for-the; letöltés: 2020.03.11.

RFID kisokos. IBCS Hungary, 2021.02.16. https://ibcs.hu/tudastar/rfid-kisokos/?gclid=CjwKCAjwsNiIBhBdEiwAJK4khv9W8bvt3S5oNEAPV ps99tKM5PYl2PgvPXD8yk3bCGM-KFzwmZfa2hoCHssQAvD_BwE; letöltés: 2021.08.13.

ROUSE, Margaret: Cyber Range. Techopedia, 2012.06.06. https://techopedia.com/definition/28613/cyber-range; letöltés: 2019.12.06.

RUSSELL, Kendall: BlackSky to Develop GEOINT Broker Platform for Air Force Research Lab. Via Satellite, 2017.08.30. https://www.satellitetoday.com/government-military/2017/08/30/blacksky-develop-geoint-broker-platform-air-force-research-lab/; letöltés: 2021.08.13.

Russian troops now number 90,000 near Ukraine border after drills, Kyiv says. Reuters, 2021.11.03. https://www.reuters.com/world/ukraine-says-russia-leaves-units-near-its-border-keeps-90000-troops-2021-11-03/; letöltés: 2021.12.22.

SALT, Alexander – SOBCHUK, Maya: Russian Cyber-Operations in Ukraine and the Implications for NATO. Canadian Global Affairs Institute, August 2021. https://www.cgai.ca/russian_cyber_operations_in_ukraine_and_the_implications_for_nato; letöltés: 2022.08.14.

SAR (szintetikus apertúrájú rádiólokátor, Synthetic Aperture Radar). A világ működése kislexikon. http://www.vilaglex.hu/Lexikon/Html/SAR.htm; letöltés: 2021.08.13.

Satellite images show Russian military buildup along Ukraine border. Reuters, 2021.04.20. https://www.reuters.com/news/picture/satellite-images-show-russian-military-b-idUSRTXBN4Y0; letöltés: 2021.12.22.

SAVOV, Vlad: Samsung Looks Beyond AI With Artificial Humans. Bloomberg, 2020.01.07. https://www.bloomberg.com/news/articles/2020-01-07/samsung-looks-beyond-ai-with-neon-artificial-humans; letöltés: 2020.11.16.

SCHMIDT, Eric – WORK, Robert – CATZ, Safra – CHIEN, Steve – CLYBURN, Mignon – DARBY, Chris – FORD, Kenneth – GRIFFITHS, José-Marie – HORVITZ, Eric – JASSY, Andrew – LOUIE, Gilman – MARK, William – MATHENY, Jason – MCFARLAND, Katharina – MOORE, Andrew: Final Report. National Security Commission on Artificial Intelligence, 2021. https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf; letöltés: 2021.03.10.

SCOLES, Sarah: It's Sentient – Meet the classified artificial brain being developed by US intelligence programs. The Verge, 2019.07.31.
https://www.theverge.com/2019/7/31/20746926/sentient-national-reconnaissance-office-spy-satellites-artificial-intelligence-ai; letöltés: 2021.08.13.

Scott W. Bray, Kelet-Ázsiáért felelős NIM 2017. június 26-ai beszéde a Koreai-Amerikai Tanulmányok Intézete rendezvényén.

SHEPPARD, Lindsey R.: Artificial Intelligence and National Security: The Importance of the AI Ecosystem. CSIS, 2018.11.05. pp. 48–51.
https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/181102_AI_interior.pdf; letöltés: 2019.12.09.

SLICK, Stephen: Measuring Change at the CIA. Foreign Policy, 2016.05.04.
http://foreignpolicy.com/2016/05/04/measuring-change-at-the-cia/; letöltés: 2016.06.06.

SMITH, David J.: Cyber-War! Tabula, November 8-14, 2010.
A Georgian Foundation for Strategic and International Studies tanulmánya.
https://gfsis.org.ge/media/download/GSAC/Articles/Cyber-War.pdf; letöltés: 2021.07.20.

Standing WatcH 24/7: NCTC Operations CentER, ODNI, 2021.04.19.
https://www.dni.gov/files/ODNI/images/news_images/NCTC-Ops-center-2021/303A7706_2.jpg; letöltés: 2021.12.25.

Strategic Concept 2010. NATO, 2010.11.19.
https://www.nato.int/cps/en/natohq/topics_82705.htm;

Stuxnet 'cyber superweapon' moves to China. The Sydney Morning Herald, 2010.09.30.
https://www.smh.com.au/technology/stuxnet-cyber-superweapon-moves-to-china-20100930-15z8v.html; letöltés: 2022.09.12.

Summary of the 2018 Department of Defense Artificial Intelligence Strategy – Harnessing AI to Advance Our Security and Prosperity.
https://media.defense.gov/2019/Feb/12/2002088963/-1/-1/1/SUMMARY-OF-DOD-AI-STRATEGY.PDF; letöltés: 2019.12.09.

Summary of the NATO Artificial Intelligence Strategy. NATO, 2021.10.22.
https://www.nato.int/cps/en/natohq/official_texts_187617.htm; letöltés: 2021.12.30.

ŚWIĄTKOWSKA, Joanna – ALBRYCHT, Izabela – SKOKOWSKI, Dominik:
National Cyber Security Organisation – Poland. CCDCOE, Tallinn, 2017.
https://ccdcoe.org/uploads/2018/10/NCSO_Poland_2017.pdf; letöltés: 2022.09.12.

SZABÓ Károly: Az elhárítás.
In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban.
Dialóg Campus Kiadó, Budapest, 2018. pp. 169–208.
https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

SZABÓ Károly: Gondolatok a katonai elhárításról. Szakmai Szemle, 2015. 1. szám. pp. 7–15.
https://www.knbsz.gov.hu/hu/letoltes/szsz/2015_1_szam.pdf; letöltés: 2022.10.18.

Sztereografikus vetítés - Stereographic projection.
https://hu.abcdef.wiki/wiki/Stereographic_projection; letöltés: 2021.03.14.

TAKÁCS Gergely: Big data (adatvezérelt) elemzési módszerek alkalmazása a nemzetbiztonsági szférában. Előadás a Kutatók éjszakája rendezvénysorozaton. NKE, Budapest, 2018.09.28.

The Age of A.I. Soul Machines, 2019.12.19.
https://www.soulmachines.com/2019/12/the-age-of-a-i/; letöltés: 2020.03.11.

The challenge match. Google DeepMind.
https://deepmind.com/alphago-korea; letöltés: 2021.08.12.

The Cost of Intelligence. Federation Of American Scientists, 1996.02.23.
https://fas.org/irp/offdocs/int017.html; letöltés: 2018.12.03.

TONIN, Matej: Artificial Intelligence: Implications for NATO's Armed Forces.
NATO Parliamentary Assembly, 2019.10.13.
https://www.nato-pa.int/document/2019-stcttc-2019-report-artificial-intelligence-tonin-149-stctts-19-e-rev1-fin; letöltés: 2019.12.06.

TRAVERS, Russ: A Blueprint For Survival: The Coming Intelligence Failure.
Studies in Intelligence, 1997. pp. 35–43.
https://www.cia.gov/static/coming-intelligence-failure.pdf; letöltés: 2018.12.03.

Tupac returns from the dead at Coachella. The Guardian, 2012.04.16.
https://www.theguardian.com/music/musicblog/2012/apr/16/tupac-coachella;
letöltés: 2020.11.16.

TURRINI, Mauro – MARTORANO, Carmen Miriam: From e-health to digital Health:
Telemedicine, Electronic Healthcare File, Artificial Intelligence. Bird&Bird, 2019.06.23.
https://www.twobirds.com/en/news/articles/2019/global/from-e-health-to-digital-health-telemedicine-electronic-healthcare-file-artificial-intelligence; letöltés: 2020.03.11.

TYUGU, Enn: Artificial Intelligence in Cyber Defence. CCD COE Publications, 2011.
https://www.ccdcoe.org/uploads/2018/10/ArtificialIntelligenceInCyberDefense-Tyugu.pdf;
letöltés: 2019.12.06.

U.S. Intelligence Community Budget. ODNI, 2022.
https://www.dni.gov/index.php/what-we-do/ic-budget; letöltés: 2022.02.16.

Új kollégát igazoltunk! Megérkezett eMI, a Modern Vállalkozások Programjának virtuális tanácsadója! Modern Vállalkozások Programja, 2022.08.17.
https://vallalkozzdigitalisan.hu/hirek/hir?id=917; letöltés: 2022.11.10.

Új szakaszba lépett a Nemzeti Élelmiszerlánc Adatszolgáltatási Központ projekt.
nébih, 2021.02.01.
https://portal.nebih.gov.hu/-/uj-szakaszba-lepett-a-nemzeti-elelmiszerlanc-adatszolgaltatasi-kozpont-projekt; letöltés: 2021.07.20.

UMUTCAN, Safak: Machine Vision in 2020: In-Depth Guide. AI Multiple, 2020.09.29.
https://research.aimultiple.com/machine-vision/; letöltés: 2020.10.03.

VERES Dóra: Mesterséges Intelligencia a mindennapokban – A magyar fejlesztésű "gépi szemek" már az életünk részei. Portfolio, 2019.11.20.
https://www.portfolio.hu/befektetes/20191120/mesterseges-intelligencia-a-mindennapokban-a-magyar-fejlesztesu-gepi-szemek-mar-az-eletunk-reszei-407233; letöltés: 2020.03.11.

VIDA Csaba: A hírszerzési ciklus.
In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban.
Dialóg Campus, Budapest, 2018. pp. 114–126.
https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

VIDA Csaba: A hírszerző elemző-értékelő munka alapjai.
Felderítő Szemle, XII. évfolyam 3. szám, 2013. december. pp. 90–99.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2013-3.pdf; letöltés: 2022.10.18.

VIDA Csaba: A nemzetbiztonsági elméletek alapjai –
Szükségesek-e az alapkutatások a nemzetbiztonsági elméletekben?
Szakmai Szemle, X. évfolyam 1 szám, 2022. március. pp. 5–21.
https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_1_szam.pdf; letöltés: 2022.10.17.

VIDA Csaba: A SOCMINT szerepe az elemző-értékelő munkában.
Az új hírszerzési ág elemző-értékelő megközelítése.
Szakmai Szemle, XX. évfolyam 2. szám, 2022. június. pp. 5–21.
https://www.knbsz.gov.hu/hu/letoltes/szsz/2022_2_szam.pdf; letöltés: 2022.10.28.

VIDA Csaba: Egyéb hírszerzési ágak.
In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban.
Dialóg Campus Kiadó, Budapest, 2018. pp. 162–167.
https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

VIDA Csaba: Létezik-e még a hírszerzési ciklus? Miről szól a hírszerzés?
Felderítő Szemle, XII. évfolyam 1. szám, 2013. szeptember–október. pp. 43–57.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2013-1.pdf; letöltés: 2022.10.18.

VIDA Csaba: Művelettámogatás a nemzetbiztonsági elemző-értékelő munkában.
Felderítő Szemle, XIV. évfolyam 4. szám, 2015. november. pp. 36–49.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2015-4.pdf; letöltés: 2022.10.18.

VIDA Csaba: Nyílt forrású adatszerzés (OSINT).
In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban.
Dialóg Campus Kiadó, Budapest, 2018. pp. 133–141.
https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908; letöltés: 2022.10.15.

VIKING Multirole UGV Platform. Horiba-MIRA, 2022.
https://www.horiba-mira.com/unmanned-ground-vehicles/media-centre/case_study/viking-multirole-ugv-platform/; letöltés: 2022.08.13.

What is Intelligence? Office of the Director of National Intelligence.
www.dni.gov/index.php/what-we-do/what-is-intelligence; letöltés: 2020.04.28.

Winter Academy on Artificial Intelligence and International Law (2019).
Az Asser Intézet (T.M.C. Asser Instituut) 2019. február 11–15. között Hágában megrendezett Mesterséges Intelligencia és a Nemzetközi Jog témájú téli akadémiája.

XLUUV / MANTA / S201. Submergence Group, 2020.
https://msubs.com/unmanned-submersibles/xluuv/; letöltés: 2022.08.13.

ZHANG, Daniel – MISHRA, Saurabh – BRYNJOLFSSON, Erik – ETCHEMENDY, John – GANGULI, Deep – GROSZ, Barbara – LYONS, Terah – MANYIKA, James – NIEBLES, Juan Carlos – SELLITTO, Michael – SHOHAM, Yoav – CLARK, Jack – PERRAULT, Raymond:
Artificial Intelligence Index Report 2021. Stanford University Human-Centered Artificial Intelligence, Stanford, CA, March 2021. pp. 155–161.
https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf; letöltés: 2021.07.15.

ÁBRÁK JEGYZÉKE

TÁBLÁZATOK JEGYZÉKE