Dobák Imre -Kenedli Tamás

Információszerzési tendenciák és kihívások a kibertérben rejlő lehetőségek és a mesterséges intelligencia viszonylatában

Military and Intelligence CyberSecurity Research Paper
2023/3.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

1. BEVEZETÉS

Napjaink rendkívül összetett technológiai és biztonsági környezetére sajátos nézőpontból tekintve válhat láthatóvá a társadalom, és az annak érdekei mentén cselekvő (nemzet)biztonsági, valamint a külső környezetben megjelenő gazdasági-technológiai „szereplők" egymással szoros kölcsönhatásban formálódó viszonya. Ebben a megközelítésben a (nemzet)biztonsági ágazat feladata, hogy többek között a változó társadalmi folyamatok és új fenyegetettségek figyelembevételével, a közeli és távoli jövőre vonatkozóan készített értékeléseken keresztül támogassa a döntéshozók munkáját.

A felderítési és információgyűjtési feladatok, majd az elemzett-értékelt információk elősegíthetik az adott társadalom (nemzet) érdekét szolgáló, már a politika szintjén megszülető döntések meghozatalát. Ezen tevékenységek hatékony végrehajtása napjainkban azonban már nem elképzelhető a külső technológiai és információs környezet viszonyaihoz történő alkalmazkodás nélkül. Ennek okai között jelenik meg a kibertér használatának globálisan megjelenő drasztikus növekedése, amely szükségszerűen módosította és folyamatosan formálja a biztonsági szervezetek információszerzési és feldolgozási, elemzési tevékenységét. További tényezőként említhető, hogy amíg a múlt század nagy részében az információs-technológiai fejlődés mozgatórugói túlnyomórészt még a biztonsági ágazatokhoz kapcsolódtak, addig napjainkra a fejlődés centrumai jelentős mértékben a gazdasági és technológiai nagyvállalatok, valamint a tudományos központok környezetében kereshetők.

Evolúciós folyamatként változtak az információk megszerzésének formái is, így szemtanúi lehetünk az "Intel" területek fejlődésének, kibertérben történő specializálódásának, valamint az egyes területeket korábban élesen elválasztó határok elmosódásának. Mindezek kiinduló eleme a digitális és tömegesen rendelkezésre álló adat, illetve információ, amely számtalan formában, akár metaadatként, vagy akár közvetlen, összetett jelentéssel bíró információként alapjává válhatott a nagytömegű adathalmazokra épülő, rendkívül gyorsan berobbanó mesterséges intelligencia térhódításának is.

Jelen tanulmány az „információs tér" nemzetbiztonsági szempontú megközelítésére helyezi a hangsúlyt, felhívva a figyelmet az információgyűjtést formáló különböző tényezők összetett hatásaira. A témakör feldolgozása során a kibertérre egyrészről, mint az információgyűjtés színterére, másrészről, mint a mindennapi életünkben nélkülözhetetlen elemként jelenlévő és – biztonságunkra hatást gyakorló – védendő színtérre (kiberbiztonság) tekintünk.

2. A TECHNOLÓGIAI VÁLTOZÁS, MINT AZ INFORMÁCIÓSZERZÉS FORMÁLÓ TÉNYEZŐJE

A technológia Veblen szerint egységes gazdasági rendet teremt, amiben mindenki egy fogaskerék, és hozzájárul az egész gazdasági rend fejlődéséhez.[1] Az üzleti szabadság fogalma ezzel átalakul, szerepe nem több annál, hogy észreveszi, felismeri azt a feladatot, amit ebben a gépezetben be kell töltenie. A tőkés ezáltal több lesz, mint megszemélyesített tőke, tudatosan vesz részt a fejlődésben és nem öntudatlanul, ahogy azt Smith[2] vagy Hegel leírta a 18. században a „láthatatlan kéz" koncepciójában.

Az információs infrastruktúra ettől kezdve jelentős szerepet kapott az intézményi közgazdaságtani gondolkodásban, annak különböző összetevői kerültek a középpontba az egyes kutatásokban. Az infrastruktúra, mint a különböző „terek" (területek) irányítása, szabályozása, az ezeken a tereken folyó gazdasági-gazdálkodási tevékenység ösztönzése vált az elemzés tárgyává, ami kiegészült a geopolitikai, földrajztudományi vagy katonapolitikai, biztonságpolitikai megfontolásokkal. John Kenneth Galbraith[3] és mások munkáiban az információ áramlásának helyes szervezése, az ennek feldolgozásához szükséges technológiák biztosítása, beleértve a rutinmunkától történő megszabadítást is megerősödött.

Az információs technológiák fejlődése a számítógépek megjelenésének időszakában erősödött fel, majd a múlt század utolsó harmadában vett fordulatot, amikor a személyi számítógépek segítségével és az ehhez kapcsolódó szoftverfejlesztésekkel széles társadalmi csoportok számára is elérhetővé váltak a számítástechnika eredményei. A további fejlődést, a számítógépek az 1980-as évektől kezdődő elterjedését, majd az internet[4] használatának az 1990-es években történő bevezetését követően a keresőmotorok megjelenése ismét új dimenzióba helyezte. Akkoriban kevesen gondoltak arra, hogy a digitális tér egyszer a világpolitika meghatározó eleme lesz, ugyanakkor az USA korabeli kormányzati politikájában már tettenérhető volt, hogy az internetet a globális dominancia egyik eszközének fogja tekinteni.

Ehhez a folyamathoz szorosan kapcsolódott a 21. század elején a közösségi médiaplatformok megjelenése és a robbanásszerű felhasználói körük kialakulása. Folyamatosan fejlődött az internet infokommunikációs alapját képező infrastrukturális háttér is. Ennek eredményeként a „hagyományos" vezetékes összeköttetések mellett egyre nagyobb teret nyert a mobilkommunikáció és a közeljövőben várhatóan az infokommunikációs tér érdemlegesen használatba veszi a világűrt (Föld körül) is. Habár az űrtávközlés elterjedésének

---

1 VEBLEN, Thorstein: *The Theory of Business Enterprise*. London, Routledge, 1978.

2 A „láthatatlan kéz" egy gazdasági kifejezés, amelyet Adam Smith, 18. századi skót közgazdász „A nemzetek gazdagsága" (1776) című művében használt először.

3 GALBRAITH, John Kenneth (közgazdász, diplomata): *Az új ipari állam*. ford. Hantos Éva, Budapest, Közgazdasági és Jogi Könyvkiadó, 1970

4 Pontosabban a ma ismert internetet (World Wide Web) 1989-ben alkotta meg a brit Tim Berners-Lee a svájci CERN kutatóintézetben.

mértéke jelenleg nem prognosztizálható, nem kizárt, hogy a mobilkommunikációhoz nagyon hasonló vagy azt meghaladó dinamikájú fejlődésének lehetünk majd szemtanúi.

Amennyiben az államok működésére, egymás közötti gazdasági és politikai viszonyaira gondolunk, jelentőséggel bír, hogy a 20. században megjelent az „információs szempont" a piacelméletben. William Stanley Jevons gondolata szerint: *„…a piac kommunikációs tér is, és a piaci egyensúlytalanságok oka az elégtelen vagy torz információ."*[5] Miért fontos ez a témánktól látszólag távolabbi kontextusban? A globalizáció és manapság a globális viszonyok nagyhatalmak által történő átalakítása megváltoztatja a nemzetek viselkedését, a hatalom sajátságos összetevőit, a gazdasági, katonai, hírszerzési, technológiai és diplomáciai fölény összekapcsolt jelentőségét. A vezető nagyhatalmak a globális piacok uralására és működésük befolyásolására törekszenek különféle módszerekkel, a globális cselekvőképességhez szükséges földrajzi hozzáférést a globális körzetek uralma biztosíthatja számukra. Megjelenik az a sajátosság, hogy az erőfölény kialakítása során mennyire fontos a mások stratégiai függőségei feletti uralom birtoklása technológiai értelemben is. Mindez a különféle, földrajzilag szétszórt információk összegyűjtésén, értékelésén és elemzésén, valamint célirányos felhasználásán alapul, amiben az előzőleg felsorolt szakterületeken működő szervezetek vesznek részt. Az egyes globális körzetek piaci egyensúlya azon is múlik, hogy az állandóan fejlődő technológiával lépést tartva – az információáramlást beleértve – a többi szereplő szándékainak elfogadását és az ahhoz történő alkalmazkodást hogyan lehet hatékonyabbá tenni. A 21. század társadalmi és gazdasági fejlődésének részeként, a technológia térnyerése a kibertér kiemelt fontosságát erősítette, egyúttal tovább növelte a meghatározó nemzetközi politikai szereplők közötti geopolitikai versengést.

Bill Clinton első elnöki periódusában fogadták el a „The National Information Infrastructure: Agenda For Action (NII)" című dokumentumot, amelyben érdekes gondolatokat találunk a digitalizációhoz, annak fejlesztéséhez kötődő nagyhatalmi törekvésekről, illetve többek között a hozzá kötődő információs infrastruktúráról. *„A fejlett információs infrastruktúra lehetővé teszi az amerikai cégek számára, hogy versenyezzenek és győzedelmeskedjenek a globális gazdaságban […] Az információ a nemzet egyik legkritikusabb gazdasági erőforrása, a szolgáltatóipar és a feldolgozóipar, a gazdaság és a nemzetbiztonság szempontjából egyaránt. […] A globális piacok és a globális verseny korában az információ létrehozására, manipulálására, kezelésére és felhasználására szolgáló technológiák stratégiai jelentőségűek az Egyesült Államok számára"*[6] – állapítja meg mindezt 2003-ban.

A globális technológiai verseny szemléltetésére egy későbbi az Európai Parlament és a Tanács határozatában szereplő gondolatsort is érdemes megemlíteni. „A digitális évtizedhez vezető út"[7] elnevezésű, 2030-ig szóló szakpolitikai programban több fejlesztési célt is előirányoz

---

5 JEVONS, W.: *The Theory of Political Economy*. London, Palgrave Macmillan, 2013.

6 BROWN, Ronald Harmon: *The national information infrastructure: agenda for action*. Executive Office of the President, Information Infrastructure Task Force, 2003. 2. o.

7 Európai Bizottság: Javaslat Az Európai Parlament és a Tanács Határozata *„A digitális évtizedhez vezető út" elnevezésű, 2030-ig szóló szakpolitikai program létrehozásáról*. COM/2021/574 final, 2021. szeptember 15. (https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52021PC0574)

az európai közösség, az egyéntől a vállalkozásokon át a közszolgáltatásokig, úgymint pl. minden európai háztartást „Gigabites" hálózat fed le, és minden lakott területen van 5G lefedettség; rendkívül biztonságos és gyors adatátvitelt biztosító peremcsomópontok telepítése; vagy akár, hogy az uniós vállalkozások 75%-a használjon felhőszolgáltatásokat, nagy adathalmazokat, mesterséges intelligenciát. Ezek együttesen növelhetik a digitális versenyképességet és eredményezhetik a kibertérben rejlő lehetőségek fejlesztését. Mindez rámutat arra is, hogy a geopolitikai küzdelmek egyik legaktuálisabb helyszíne a kibertér lett.

A 4. ipari forradalom (Ipar 4.0[8]) már egy összetett, a digitalizációval támogatott környezetet eredményez számunkra. A digitalizáció és a robotizáció kora, ahol a gazdaság a fizikai világ és a kibertér összekapcsolásával egyetlen intelligens információs rendszerré alakul át többek között a hatékonyság növelése, a globális digitális piacból eredő előnyök kihasználása érdekében. Ezt talán legplasztikusabban az Európai Parlament 2016-ban megfogalmazott állásfoglalása szemlélteti: *„Az ipar 4.0 a termelési folyamatok olyan szervezését írja le, melynek keretében az eszközök önállóan kommunikálnak egymással az értéklánc mentén: a jövő egy olyan „okos" gyárát hozva létre ezzel, amelyben a számítógép-vezérelt rendszerek nyomon követik a fizikai folyamatokat, létrehozzák a fizikai valóság virtuális mását és decentralizált döntéseket hoznak önszervező mechanizmusok alapján."*[9] Az Ipar 4.0 átalakítja a gyártó cégek üzleti modelljeit. Ezek a technológiák támogathatják a termelés rugalmasságát, hatékonyságát és a termelékenységet különböző újonnan megjelenő kommunikációs, információs és információszerző technológiák révén.[10] Dalenogare és szerzőtársai, illetve Bai és munkatársai kutatásai alapján az Ipar 4.0 technológiák közé tartoznak többek között az additív gyártás, a mesterséges intelligencia, a nagyméretű adatok és az analitika, a blokklánc, a felhő, a dolgok ipari internete és a szimuláció.[11] Más felosztás szerint a fizikai technológiák elsősorban a gyártási technológiákra, például az additív gyártásra vagy a szenzorokra és drónokra vonatkoznak. A digitális technológiák főként a modern információs és kommunikációs technológiákra utalnak, mint például a felhőalapú számítástechnika, a blokklánc, a nagy adatelemzés és a szimuláció.[12] Összességében elmondható, hogy a dolgok internete (Internet of Things – IoT), valamint a virtuális és kiterjesztett valóság világában a technológia mindent és mindenkit jól szervezett, egymással folyamatosan kommunikáló entitások interaktív hálózatába kapcsol.[13]

---

[8] Fourth Industrial Revolution (4IR)

[9] *Industry 4.0 - Policy Department Economic and Scientific Policy*. 2016. 22-23. o. (https://www.europarl.europa.eu/RegData/etudes/STUD/2016/570007/IPOL_STU(2016)570007_EN.pdf)

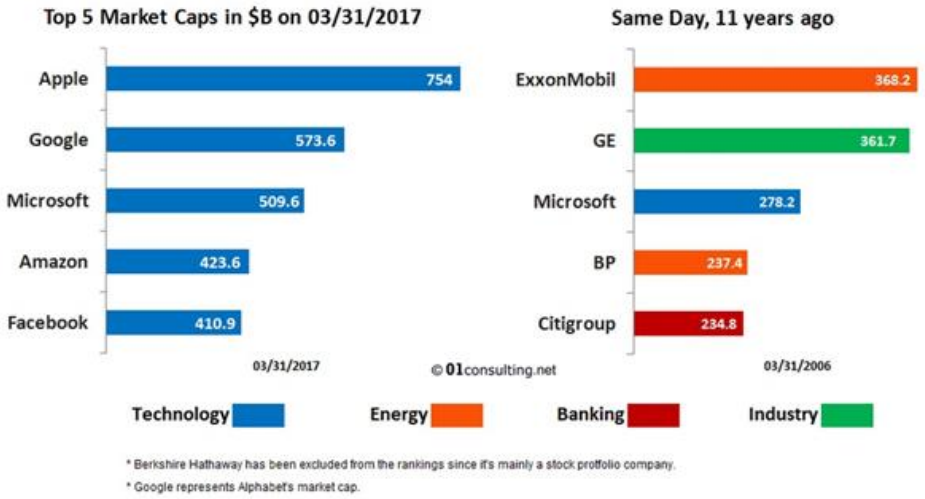
[10] IBARRA, D. – GANZARAIN, J. – IGARTUA, J. I.: Business model innovation through Industry 4.0: a review. *Procedia Manufacturing*, 2018/22, 4-10. o.;
RÜßMANN, M. – LORENZ, M. – GERBERT, P. – WALDNER, M. – JUSTUS, J. – ENGEL, P. – HARNISCH, M.: Industry 4.0: the future of productivity and growth in manufacturing industries. *Boston Consulting Group*, 2015/1, 54-89. o.

[11] DALENOGARE, L.S. – BENITEZ, G.B. – AYALA, N.F. – FRANK, A.G.: The expected contribution of Industry 4.0 technologies for industrial performance. *International Journal of Production Economics*, 2018/204, 383-394. o.

[12] BAI, Chunguang – DALLASEGA, Patrick – ORZES, Guido – SARKIS, Joseph: Industry 4.0 technologies assessment: A sustainability perspective. *International Journal of Production Economics*, 2020/229. 2. o.

[13] ÁRPÁD Zoltán: Intelligens biztonság, hétköznapi problémák – intelligens megoldások. *Szakmai Szemle*, 2018/1. 37. o.

Az előzőekben leírt technológiai fejlődést jól szemlélteti Darius Lahoutifard a 01Consulting LLC alapítójának elemzése, amit 2017-ben a VentureBeat technológiai innovációs weblapon tett közzé.



1. ábra: Az öt legmagasabb piaci tőke alakulása (2017, 2006)

Ha közelebbről szemügyre vesszük láthatjuk, hogy az elemzést megelőző 11 év során a nem technológiai vállalatok többé-kevésbé ugyanabban a fejlettségi tartományban maradtak, míg a technológiai vállalatok rendkívül markáns növekedési ütemet értek el. Utóbbiak közül pl. a Facebook 10.000%-os növekedést produkált. A technológia (szoftverek) egészének uralma időszakában élünk azzal együtt, hogy a szolgáltatásaik sokszor megfoghatatlanok számunkra. Ezek az új technológiák egyre magasabb szintű termelési hatékonyságot tesznek lehetővé. Arra is képesek, hogy drámai módon befolyásolják a társadalmi és környezeti fenntartható fejlődést. Mivel a fejlődő technológiák digitális kommunikáción alapulnak, és működésük fejlett szoftverekhez kötődik, megsokszorozódott az adatkapcsolatok száma, illetve az adatok és információk mennyisége. A Quadron műszaki igazgatójának, Gombás Lászlónak 2017-ben tett megállapítása szerint naponta 60 százalékkal több digitális adatot hoztunk létre, mint tíz évvel korábban egy egész esztendő alatt. Továbbá ezt a tevékenységet több mint negyvenháromszor gyorsabban vagyunk képesek elvégezni.[14] Ezt a meglehetősen összetett folyamatot nevezték el találóan szingularitásnak, amely nem más, mint „egy jövőbeli korszak, amelyben a technológiai változás üteme olyan gyors lesz, a hatása pedig olyan mély, hogy az emberi élet visszafordíthatatlanul átalakul.”[15]

14 Küszöbön a digitális armageddon? *Világgazdaság*, 2017. 09. 22. (https://www.vg.hu/cegvilag/2017/09/kuszobon-digitalis-armageddon)
15 KURZWEIL, Ray: *A szingularitás küszöbén*. Budapest, Ad Astra Kiadó, 2013. 15. o.

2.1. A mesterséges intelligencia hatása, elterjedésének jelentősége nemzetbiztonsági szempontból

A mesterséges intelligencia technológiai hatása kapcsán az egyik leggyakrabban megjelenő félelem a technológiai munkanélküliség, amiből néhány szerző olyan gazdasági állapotra következtet, amiben az ember helyett mindent a gépek végeznek el. A mesterséges intelligencia, és tágabban az információs és kommunikációs technológiák fejlődése felszabadítja az embert a rutinszerű munka alól, és tevékenységét az alkotásra fogja ösztönözni, a helyes döntésre és szemléletre. Azaz egy új típusú munkanélküliség megjelenésének félelme megalapozott, azonban ez nem korlátozódik a technológiai munkanélküliségre. Ugyanis az egyértelműen leírható munkafolyamatokat végző szakmákban dolgozók létszámának jelentős csökkentését, egyes esetekben teljes kiváltásukat eredményezheti. Ez a közeljövő munkaerő piacának jelentős átrendeződését eredményezi. Ez az átrendeződés azokban az országokban nem fog kezelhetetlen elégedetlenséget eredményezni, amely országok MI Stratégiája az emberek új munkaerő-igényekhez történő felkészítését is tartalmazza.

A globalizáció új korszakában ez erősödik fel, mert ez szükséges feltétele a mesterséges intelligenciában rejlő lehetőségek kibontakozásának. A demokrácia feltételezi a következetes értékrendi elköteleződést a döntéshozók, és végső soron minden állampolgár részéről, ehhez is hozzá tud járulni az új technológia. A mesterséges intelligenciából önmagában nem következik az értékrend, ez a technológia lehetőséget ad a jóra és a rosszra történő használatra egyaránt. A közösség „technológiája" az infrastruktúra. A témakör szakértői szerint *„a mesterséges intelligenciát az infrastruktúra egy elemeként érdemes felfogni* (és nem tőkejószágként, magántulajdonként) mert ez segíti a benne rejlő lehetőségek kibontakozását."[16]

A technológia nem spontán és kiszámíthatatlan exogén tényező a politikai gazdaságtan számára, hanem a gazdaságpolitikai irányítás alapvető eszköze, az értékrend érvényesítésének infrastrukturális vonatkozása. A technológia ezért az együttműködést, és nem az elszigetelődést segíti.

A mesterséges intelligencia[17] (MI) kutatás és fejlesztés 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 kiválthatóak. Általánosan elfogadott definíció híján tehát *MI alatt az emberi cselekvést részben vagy egészben, automatikus módon kiváltó gépeket (szoftvereket) értjük*.[18]

---

[16] Trautmann László – Baranyi Dániel Martin – Balogh Attila: *A mesterséges intelligencia és a munka politikai gazdaságtana*. Kézirat, (A mesterséges intelligencia és egyéb felforgató technológiák átfogó hatásainak vizsgálata munkacsoport) 2023.

[17] Artificial Intelligence – AI

[18] Schmidt, Eric – Work, Bob – Catz, Safra – Chien, Steve – Darby, Chris – Ford, Kenneth – Griffiths, Jose-Marie – Horovitz, Eric – Jassy, Andrew – Mark, William – Matheny, Jason – McFarland, Katharina – Moore, Andew: *Final*

Az általános szóhasználatban a „*mesterséges intelligencia*” kifejezést használjuk, ugyanakkor sokkal pragmatikusabb, technológiai oldalról jobban megfogható a „*mesterségesintelligencia-rendszer*” kifejezés, amit az EU jogalkotói használnak.[19] Egyébként ez a meghatározás jobban segíti a témakör megértését is. A „*mesterséges intelligencia*” kifejezés véleményünk szerint félrevezető lehet a jelentés tartalmára vonatkozóan, ugyanis amit ezek a rendszerek elvégeznek, az határozottan közelebb áll a számológépek által végzett tevékenységhez, mint az emberi agyban végbemenő folyamatokhoz. Hozzátéve azt is, hogy a számítógép be- és kimenete sokkal rugalmasabb, mint az egyén hasonló képessége.

A mesterségesintelligencia-rendszer (MI-rendszer) olyan szoftver, amelyet

- *a Gépi tanulási megközelítések, Logikai és tudásalapú megközelítések, Statisztikai megközelítések közül egy vagy több alkalmazásával fejlesztettek (EU rendelet 1. sz. melléklet), és amely*
- *az ember által meghatározott célkitűzések adott csoportja tekintetében olyan kimeneteket képes generálni, például*
  - tartalmat
  - előrejelzéseket
  - ajánlásokat vagy
  - döntéseket, amelyek

  befolyásolják azt a környezetet, amellyel kölcsönhatásba lépnek.

Előzőek közül – nemzetbiztonsági felhasználhatóság szempontjából is – nagy jelentősége van a gépi tanulás alkalmazásának, ami egyfajta neurális hálózatokon alapuló szoftverrendszer[20], egy olyan technológia, amelyet évtizedekkel ezelőtt vezettek be, de a közelmúltban az új, nagy teljesítményű számítástechnikai erőforrásoknak köszönhetően virágzásnak indult. A gépi tanulás algoritmusok használatával azonosíthatjuk a mintákat a megszerzett adatokban, majd ezekkel a mintákkal létrehozhatunk egy előrejelzésekre alkalmas adatmodellt. Az általunk és elvárásaink szerint programozott gépi tanulás eredményeként létrejövő eredmények, az adatok és a tapasztalat mennyiségének növekedésével egyre pontosabbak lesznek. Egy megfelelően elkészített gépi tanulási modell a strukturált és strukturálatlan adatokban egyaránt képes a minták vagy struktúrák azonosítására, így segít azonosítani az adatok mögött rejlő összefüggéseket.

Az MI tipológiája a képességek alapján:

- *Gyenge vagy szűk mesterséges intelligencia (Weak AI or Narrow AI)*

Report: National Security Commission on Artificial Intelligence (AI). 2021. 35.o. (https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf)

[19] *Proposal for a regulation of the European Parliament and of the council laying down harmonised rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts*. COM/2021/206 final, Brussels, 2021. 04. 21. (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206)

[20] COLDEWEY, Devin: *Age of AI: Everything you need to know about artificial intelligence*. 2023. 07. 11., (https://techcrunch.com/2023/07/11/age-of-ai-everything-you-need-to-know-about-artificial-intelligence/)

A gyenge (más néven szűk) mesterséges intelligencia a mesterséges intelligencia olyan típusa, amely képes egy adott feladat intelligens végrehajtására. Jelenleg ezek a legelterjedtebb és elérhető MI által támogatott vagy működtetett rendszerek. A gyenge MI nem képes a saját területén vagy korlátain túl teljesíteni, mivel csak egy adott feladatra tervezték és képezték ki.

– *Általános mesterséges intelligencia, más néven AGI (Artificial General Intelligence)*;

Az MI kutatók egyik elsődleges célja ilyen rendszert létrehozni, jelenleg nem létezik. Sajátossága lenne, hogy képes bármilyen szellemi feladatot emberhez hasonló teljesítménnyel megoldani és végrehajtani.

– *Erős vagy szuper AI (Strong Artificial Intelligence)*

Egyelőre hipotetikusan létezik, az AGI egyik eredményeként jöhet létre. Az erős mesterséges intelligencia célja olyan intelligens gépek létrehozását célozza, amelyek megkülönböztethetetlenek az emberi elmétől, valójában meghaladhatja az emberi készségeket és kognitív képességeket.

A mesterséges intelligenciának csak a következő kategóriái tekinthetők létező rendszereknek és szolgáltatásoknak:[21]

– Reaktív mesterséges intelligencia

A fejlesztők által úgy van programozva, hogy a bemeneti adatok alapján előre meghatározott kimeneti eredményt produkáljon. Tipikusan ilyen MI-vel működnek az előre beprogramozott gyártósori robotok, amelyek az érzékelők jelei alapján tervezik a tevékenységüket. Ezeknek az MI rendszereknek nincs emlékezetük, és nem tanulnak korábbi tévedéseikből, minden alkalommal azonosan viselkednek, nem rendelkeznek a gépi tanulás képességével. Ilyen korlátozott képességű MI például a Deep Blue – az IBM sakkozó szuperszámítógépe 1997-ben (30 db IBM RS/6000 SP processzor, 480 speciális sakk-chip, három rétegre osztható működés, a keresőalgoritmus 40 lépéspár mélységig), vagy a Google/YouTube/Spotify/Netflix ajánlómotorjai[22] (a felhasználói viselkedésre, tevékenységekre és preferenciákra vonatkozó adatok gyűjtésére és elemzésére összpontosít, hasonlóságok alapján következtet).

– Korlátozott memóriájú mesterséges intelligencia

A neve is mutatja, hogy képeségei korlátozottak, tanul a múltból, és a cselekvések vagy adatok megfigyelésével tapasztalásból eredő tudást épít. Előre beprogramozott információkat múltbeli megfigyelési adatokkal kombinálva használja fel előrejelzések készítéséhez és az összetett osztályozási feladatok elvégzéséhez. A rendszer a gépi tanulási képességek miatt fejlettebbnek tekinthető, mint a reaktív MI. Ilyent technológiát használnak az autonóm járműveket irányító mesterségesintelligencia-rendszerekben, valamint ilyenek a mobiltelefon speciális funkciói is, mint például egy videón vagy fényképen a tárgyak azonosítása és kiemelése. Előzőek mellett a „Digidogs" nevű robotkutya-járőr (New York-i rendőrség) is jó példa a korlátozott mesterséges intelligencia alkalmazására.

– Gyenge/szűk mesterséges intelligencia

[21] BALOGH Zsolt György: *Az MI rendszerek ellenőrzése, felügyelete és monitorozása*. Kézirat, (A mesterséges intelligencia és egyéb felforgató technológiák átfogó hatásainak vizsgálata munkacsoport) 2023.

[22] Recommendation engine

A fentebb ismertetett sajátosságok mellett szélesebb körben történő használata valósul meg számos technológiai környezetben. Ilyen a korlátozott, előre meghatározott feladatkörrel működő Apple Siri működtetése, vagy az IBM Watson online soft-computing eszközök, amelyek tartalmaznak szakértői rendszereket, gépi tanulásra képesek, természetes nyelvfeldolgozást végeznek. Egyéb gyenge MI alkalmazásokkal találkozhatunk még vásárlási ajánlómotorokban, autonóm járművekben, beszédfelismerő berendezésekben vagy képfelismerő rendszerekben.

Az MI-ről történő gondolkodásunk során tisztában kell lennünk azzal, hogy az adatvezérelt és az MI-vezérelt döntések megkülönböztetése alapvető fontosságú. Mindkét kifejezés különböző eszközöket tükröz, az előbbi az adatokra, az utóbbi pedig a feldolgozási képességekre fókuszál. Az adatok tartalmazzák a jobb döntéseket lehetővé tevő meglátásokat, a feldolgozás pedig a meglátások kinyerésének és a cselekvésnek a módja.[23]

Az összetett folyamatok révén létrejövő digitális információtömegek feldolgozásához manapság már nem elegendőek az egyén agyi kapacitásai. Az MI-t be lehet tanítani arra, hogy megtalálja az adathalmazokban azokat a szegmenseket, amelyek a legjobban magyarázzák az eltéréseket a finomabb szinteken, még akkor is, ha ezek az emberi felfogásunk számára nem intuitívak. Az MI és a hozzá kapcsolódó munkafolyamat kihasználja az adatokban rejlő információkat, és következetesebb és objektívebb döntéseket hoz. Az újonnan létrejövő MI-rendszerek meggyorsíthatják az információ kinyerését, feldolgozását és terjesztését, továbbá ezzel párhuzamosan a gépi döntéshozatali, illetve döntéstámogató megoldások az emberi döntések minőségét javíthatják.

Az MI az alábbi módokon támogathatja a döntéshozatalt (nemzetbiztonsági fókusszal):[24]

- 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 pl. hatékony hang- és képfelismerés);
- az értékelés-elemzés fárasztó és időigényes feladatának automatizálásával;
- a múltbeli nagymennyiségű (nyers és elemzett) adatok elemzésével (pl. kialakulóban lévő negatív gazdasági, társadalmi, biztonságpolitikai, folyamatok sajátosságainak azonosítása érdekében);
- előrejelző modellek kidolgozásával, alkalmazásával (pl. segíthet a válságok, célszemélyek viselkedésének előrejelzésében);
- az információ vizualizálásával, összegzésével és értelmezésével, az önmagukban értéktelen információk kontextusba helyezésével;
- a lehetséges helyes cselekvési változatok és azok várható hatásainak bemutatásával;
- előrejelzés biztosításával (pl. az ellenség várható cselekvésével kapcsolatban);

[23] Tölgyes László: *Átlátható döntéshozatal támogatása MI segítségével*. ICTGlobal, 2023. 07. 06. (https://ictglobal.hu/iparagi-megoldasok/atlathato-donteshozatal-tamogatasa-mi-segitsegevel/)

[24] Erdész Viktor: *A mesterséges intelligencia felhasználási lehetőségei a korszerű nemzetbiztonsági szolgálatok tevékenységében*. (PhD értekezés) Budapest, Nemzeti Közszolgálati Egyetem, 2022. 73. o. felhasználásával készített kibővített változat. (https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/20521)

– javíthatják a védelem reagálóképességét nagy sebességű fegyverrendszerekkel (pl.: hiperszonikus és kibereszközökkel, valamint energiafegyverekkel) szemben.

Átalakító képességével az MI alkalmazásba vétele forradalmasít(hat)ja a kormányzati rendszereket, köztük a nemzetbiztonsági szolgálatok legkülönfélébb szakrendszereit, kiszolgálhatja a civil társadalom és a gazdaság igényeit.

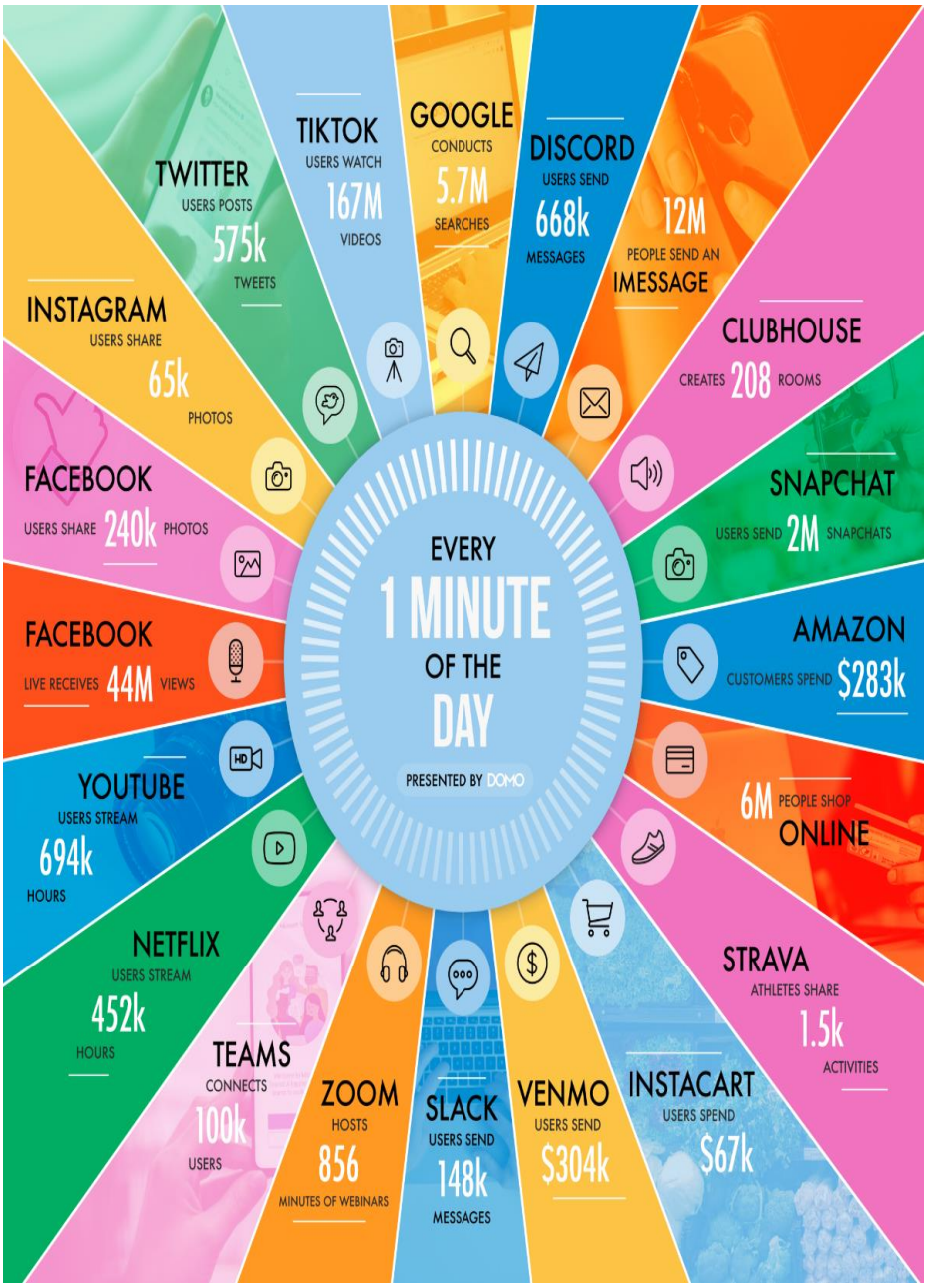
2.2. A Mesterséges intelligencia és a nagy adathalmazok felhasználása a nemzetbiztonsági munkában

A technológia változását bemutató témakörhöz kapcsolódva, annak rendkívüli ütemű fejlődésére utalva fontos megemlíteni az egyes technológiák alkalmazása mögött meghúzódó folyamatokat, az azok kapcsán megjelenő kihívásokat. Ilyen a nagytömegű adathalmazok kitermelődése és a velük történő tevékenység. A technológia fejlődése és a felgyorsult világ eredményeként megjelenő kihívás szemléltetésére egy internetes tevékenységet vizsgáló kutatóközösség megállapításait érdemes elemezni arra vonatkozóan, hogy egyetlen perc alatt mennyi minden történik a világhálón.

A globális internetpopuláció 2016-ban 3,4 milliárd fő volt, ami 2021 júliusára 5,1 milliárd felhasználóra növekedett, és elérte a világ népességének 65%-át, ami 2021 januárjához képest 10%-os növekedés. A felhasználók 92,6%-a mobileszközön keresztül csatlakozott az internethez. A globálisan felhasznált adatmennyiség 2021-ben 79 zettabájt[25] volt, ami az előrejelzések szerint 2025-re 180 zettabájt fölé fog menni. A kihívás mostanság nem az adatgyűjtés és az adatok birtoklása, még ha a sok adat hozzá is járul a sikerhez, hanem az, hogy hogyan tudunk kérdéseket feltenni az összegyűjtött adatokkal kapcsolatban, valamint, hogyan áshatunk mélyebbre azokban, és milyen összefüggések mentén használjuk fel a kitermelt információt minél kisebb időkereten belül.

A világ digitális tevékenységének középpontjában azok a világméretű cégek üzemeltetésében működő mindennapi szolgáltatások és alkalmazások állnak, amelyek életünk alapvető elemeivé váltak. Ezek együttesen elképzelhetetlen mennyiségű felhasználói tevékenységet és kapcsolódó adatokat termelnek. 2021-ben egyetlen perc alatt: 12 millió ember küldött iMessage-t, 6 millió ember vásárolt online, a Microsoft Teams 100.000 felhasználót kötött össze, a YouTube- felhasználók 694.000 videót streameltek, a Facebook Live-ot 44 millióan nézték meg, az Instagram-felhasználók 65.000 fényképet osztanak meg, és a Tiktok felhasználói 167 millió videót néznek meg. Az arányok (adatmennyiség) változásának érzékeltetése érdekében említjük a Twittert, amelyre a 2011-2013-as felmérés időszakában 277 ezerszer posztoltak egyetlen perc alatt, majd ezen interakciók száma 2021-re 575 ezerre nőtt. Egyéb internetes környezetben működő terheltségi adatok összefüggéseinek elemzése érdekében érdemes megtekinteni az alábbi ábrát.

[25] DJURASKOVIC, Ogi: *Big Data Statistics 2023: How Much Data is in The World?* First Site Guide, 2023. 04. 19. (https://firstsiteguide.com/big-data-stats/)



2. ábra: Mennyi adat keletkezik percenként?[26]

Napjainkban a Big Data és az MI egymást feltételezik, és egymásra hatnak. Az MI eredményes alkalmazásához hatalmas adattömegre van szükség mind a rendszerek fejlesztése és tanítása, mind a mindennapi működtetésük során. Kölcsönhatásaikra a nemzetbiztonsági gondolkodásban is találhatunk példát, így akár a szervezetek által folytatott tömeges információkeresést, amely során *„a keresés nem egy konkrét célszemélyre, szervezetre történik, hanem valamely kritériumok szerint egy nagy adathalmazt gyűjt be legtöbbször külső*

[26] *Data Never Sleeps 9.0.* DOMO.com, 2021. (https://www.domo.com/data-never-sleeps#)

forrásokból (is), majd azt feldolgozva az így keletkezett közbenső adatállományból (pl. indexfájlból) szűri ki lekérdezésekkel a kívánt konkrét tartalmat"[27] a további felhasználás, értékelés-elemzés számára. A Big Data hatékony kezelése és kiaknázása mesterséges intelligencia-alapú szoftvereket igényel. Ezáltal a manuális munkafolyamatok részben automatizálhatóak, továbbá az adattömegből korábban nem ismert összefüggések, illetve előrejelzések is kinyerhetők. Az ilyen rendszerek vizualizációs megoldásai segítenek az információ átláthatóvá tételében és támogatják az elemzési, valamint döntéshozatali folyamatokat.

A modern információs társadalmakban a nemzetállamok közötti versengés, és annak részeként megjelenő nemzetbiztonsági tevékenység számára új lehetőségeket és eszközöket teremtett a tömegkommunikáció, különösen a közösségi média fejlődése és egyre növekvő szerepe. Az információtechnológia fejlődése, azon belül kiemelten az okostelefon alkalmazások elterjedése mindenki számára lehetővé tette, hogy figyelemmel kísérhesse mások tevékenységét. A mindenki által érzékelhető információs túlterhelés korszakában ugyanakkor egyre elengedhetetlenebbé válik a fontos eseményekkel kapcsolatos torzításmentes információk beszerzése, valamint az ellenoldal információinak helyes értelmezése. A jelenség nemzetbiztonsági szemléletű figyelembevétele kulcsfontosságú az olyan, meghatározó jelentőségű kérdések elemzésében, mint az országok közötti geostratégiai verseny, a befolyásolásra indított katonai műveletek, a békeműveletek, a globális terrorszervezetek működése, illetve a technológiailag fejlett országok választásai, ezáltal kül- biztonság- és védelempolitikáját befolyásoló belpolitikai folyamatok.

Szakirodalmi források jelzik, hogy az információs és kommunikációs technológia legújabb eredményeivel kiegészített módszerek segítségével lehetővé vált célszemélyek, csoportok vagy egész társadalmak célorientált befolyásolása. Az ennek céljából végzett hatékony stratégiai kommunikáció alapja a műveleti és az információs környezet[28] átfogó ismerete, amelyhez részletes, összadatforrású hírszerzési információkra van szükség. A tevékenység elfedése, az alkalmazott technológia külső együttműködő (pl. kommunikációs) cégek szaktudását és menedzselését igényelhetik. Ezekben az esetekben gyakran adatbróker vállalatoktól szükséges beszerezni a kívánt információkat, majd azokat más külső, illetve saját belső adatforrásokkal sajátságos módszertan[29] alapján összevetve, értékelve-elemezve, az adatmodellezést is alkalmazva alakítható ki a célzott művelet. Ezekben az esetekben a közösségi média (pl. Twitter, Facebook) felületei a befolyásolás, az érdekérvényesítés eszközeként jelenhetnek meg.

A pszichológia a lelki folyamatok megismerésére végzett, mérésekkel foglalkozó területe a pszichometria, az okoseszközök és a közösségi felületek lehetőségeinek kiaknázásával hatékonyabb módszerré vált. A Big Data alapú pszichometria statisztikai modelljeinek

---

[27] VADÁSZ Pál: *A szemantikus keresés módszerei és alkalmazási lehetőségei a védelmi szférában, a közigazgatásban, illetve a gazdasági életben*. (PhD értekezés) Nemzeti Közszolgálati Egyetem, Budapest, 2018. 102. o.

[28] Információs környezet főbb elemei: a kultúra, a lakosság vélekedése, hiedelmei, a térségbeli fő trendek, valamint a meghatározó szereplőkkel és a technikai kommunikációs eszközökkel kapcsolatos információk.

[29] Pl. „OCEAN" vagy „ötfaktoros" modell, amelynek alapját Ernest Tupes és Raymond Christal fejlesztette ki 1961-ben.

megalkotása a milliós nagyságrendű összehasonlított adatmennyiségre épült. A módszerrel egyebek mellett az intelligencia foka, vallás, alkohol-, dohány- és droghasználat, családi állapot is jól felbecsülhető egy személy esetében, továbbá következtetések vonhatók le a profilképek és a kapcsolatok adataiból, valamint az okostelefonok mozgásérzékelőinek adataiból pl. az utazási szokásokra vonatkozóan. Összességében elmondhatjuk, hogy megfelelő mennyiségű adattal több információ szerezhető, mint amennyit az adott személy önmagáról tudni vél.[30] Az eredmények alátámasztják Yuval Noah Harari[31] évekkel korábbi álláspontját arra vonatkozóan, hogy a mesterséges intelligencia algoritmusai jobban ismerik majd a felhasználók szokásait és vágyait, mint önmaguk. A Big Data alapú pszichometria fő felhasználási módja a felhasználói profilok tetszőleges kategóriák szerinti, minél pontosabb szegmentálása, ugyanakkor alkalmas a célszemélyek manipulálására is.

Az MI-rendszerek elterjedése tovább fokozza a nemzetbiztonsági szervek kibervédelmi kihívását is, és az ilyen technológiával támogatott kibervédelmi rendszerek hatékonysága nagyban meghaladhatja a jelenleg használatban lévőkét. A mesterséges intelligencia segítségével hatékonyabbá tehetőek a kártékony kódok szűrésére szolgáló rendszerelemek. A kiberincidensek feltárása során az MI az adatok elemzésének segítségével hatékonyan segíti a szakemberek munkáját. A káros szoftverek (malware) előre meghatározott (betáplált) mintái alapján a célszoftverek a már azonosított fenyegetések mellett megtaníthatóak az ismeretlen, ugyanakkor káros kódot hordozó mintázatok felismerésére. Az MI-t alkalmazó viselkedésanalitika a felhasználók rendszerhasználatát elemezve akkor is felismeri (feltételezi) a jogosulatlan tevékenységet, ha a támadók érvényes azonosítókkal rendelkeznek.[32] Az MI-t tartalmazó rendszerek esetében ugyanakkor különösen fontos a vele kapcsolatba kerülő programozói, üzemeltetői és felhasználói réteg folyamatos felkészítése a technológiából eredő sajátosságok megismerésére. Itt van jelentősége az úgynevezett kiber-kiképzőtereknek (cyber range), ahol az MI segítségével hatékonyabban szimulálhatók a kiberincidensek, illetve a kibervédelmi eszközök működése, azok hibái, valamint begyakorolhatók a megfelelő (hatásos) eljárásrendek.

A fenti képességek kialakítása során az MI-algoritmusok programozásához (tanításához) és működtetéséhez nagy mennyiségű, megfelelően strukturált adatra van szükség. Ezt a nagyon sok adatból álló adatbázist vagy adatkészletet az általánosan rendelkezésre álló megszokott adatbáziskezelő alkalmazásokkal nehéz rendben tartani, hiszen nagy tömegű, nagyfokú változatossággal és komplexitással jellemezhető, gyorsan keletkező és szignifikánsan növekvő adattömegek jelentek meg, amelynek hasznosítására kevés idő áll rendelkezésre.

---

30 KOSINSKI, Michal – STILLWELL, David – GRAEPEL, Thore: *Private traits and attributes are predictable from digital records of human behavior*. Proceedings of the National Academy of Sciences of the United States of America (PNAS), 2013. április 9. (https://www.pnas.org/content/110/15/5802)

31 HARARI, Yuval Noah: *21 lecke a 21. századra*. Central Kiadói Csoport, 2018. 55-60. o.

32 TYUGU, Enn: *Aritificial Intelligence in Cyber Defence*. A NATO tallini Kibervédelmi Kiválósági Központjának kiadványa. 2011. (https://www.ccdcoe.org/uploads/2018/10/ArtificialIntelligenceInCyberDefense-Tyugu.pdf)

A Big Data sajátosságait Doug Laney 2001-es „3V” modelljének továbbgondolásával érdemes meghatározni:[33]

- Volume, azaz mennyiség: az adatok mennyisége napjainkban óriási, és ez exponenciálisan nő;
- Variety, azaz változatosság: rengeteg új adatforrás, adattípus és formátum létezik és születik nap mint nap;
- Velocity, azaz sebesség: az adatok gyors keletkezése, változása, áramlása és feldolgozása;
- Veracity, azaz megbízhatóság: megfelelő adatminőség rendelkezésre állása esetén lehet csak minőségi elemzést végrehajtani az adatokon;
- Value, azaz érték: az adatok hasznosságát mutatja, amely akár az adatelemzés eredményét is jelentheti.

Az adatfüggőség megnöveli a manipulálásból és dezinformációból fakadó kockázatot, ugyanis az adatok kismértékű megváltoztatása is jelentősen befolyásolhatja az MI által alkotott eredményt, ami téves következtetésekre vezethet, torzíthatja az elemzéseink eredményét, a döntéselőkészítést.

Az MI támogatott rendszerek nemzetbiztonsági szakterületen történő felhasználásánál és/vagy üzemeltetésénél különös figyelmet kell fordítani arra, hogy a technológiából fakadó anomáliák még jelen vannak a technológia újszerűsége miatt. Tekintettel az estlegesen előforduló nehezen felmérhető hibák – MI-rendszerek döntési folyamatai visszakövethetőségének kérdései – potenciális következményeire, az alkalmazásba vételük kis lépésekben, jól körülhatárolt területen, kísérleti fázisokat követően célszerű. Az ilyen technológiát tartalmazó rendszerek váratlan és tömeges összeomlása (flash crash) rendkívül súlyos következményeket okozhat egy korábban más módon, jól felépített, stabil működési környezet esetében is. Fontos még egy biztonsági szempontra különösképp felhívni a figyelmet, ez pedig az MI-rendszerek kiberhírszerzés által, vagy más módszerrel történő megszerzése révén történő adatszivárgás problematikája. Ugyanis a felépített rendszerből rendkívül részletes információ nyerhető ki az adott szervezetről, illetve annak tevékenységéről.

2.3. Adathalmazok és a kriptográfia jelentősége

Az adataink illetéktelen megismerése elleni védelem egyik eszköze a titkosítás, ami matematikai módszerekkel védi az érzékeny elektronikus információkat, beleértve az általunk böngészett biztonságos webhelyeket, és az általunk küldött e-maileket, az adatkommunikációnkat is. A széles körben használt nyilvános kulcsú titkosítási rendszerek – amelyek olyan matematikai megoldásokra támaszkodnak, amelyeket még a leggyorsabb hagyományos számítógépek is megoldhatatlannak találnak – biztosítják, hogy a védendő webhelyek és üzenetek hozzáférhetetlenek maradjanak a nemkívánatos harmadik fél számára.

[33] COSO IT: *Explanation of 3V's Model of Big data Given by Doug Laney*. (https://www.cosoit.com/explanation-of-3v-model-of-big-data; SHERIFF, Shanawat: Understanding The 5Vs Of Big data; https://acuvate.com/blog/understanding-the-5vs-of-big-data/)

Ugyanakkor a technológia fejlődése rávilágított, hogy az adataink védelme (fájlok, adatfolyam) során azt is szem előtt kell tartani, hogy adataink a (kiemelten a fájljaink) a jövőben is védetten maradjanak. Ezért a tárolt és partnereinkkel megosztott adatok vonatkozásában ismerettel kell rendelkeznünk arra vonatkozóan, hogy az egyes fájljaink titkosítása során használt eljárások egy ellenérdekelt félnél használatba vehető technológiai háttér mellett védettnek tekinthetőek-e, vagy fennáll a veszélye, hogy ezen adatok belátható időn belül megismerhetővé válnak.

A kriptográfia szó eredete a görög elrejtés és írás szavakból ered, az információ továbbításának és tárolásának folyamata olyan módon, hogy ne tudjon hozzáférni egy ellenérdekelt harmadik fél. Mindkét folyamatban jelentőséget kap a kibertér, nemcsak mint kommunikációs közeg, hanem mint az MI-vel támogatott nagy adatfeldolgozás módszertana és azok hatásai a tevékenységre.

A hagyományos kriptográfia kulcsokat előállító matematikai technikák segítségével titkosítja és visszafejti az adatokat. Ezeket az algoritmusokat úgy tervezték, hogy a kulcs ismeretének hiányában ne legyen megismerhető az információtartalom, így a titkosított adatok információtartalmához az illetéktelen hozzáférés megnehezül. Mindazonáltal, ahogy a számítógépek egyre erősebbek, a hagyományos titkosítás egyre sebezhetőbbé válik a brute force támadásokkal szemben, amelyek magukban foglalják az összes lehetséges kulcskombináció kiértékelését, amíg meg nem találják a megfelelőt.

A kvantumkriptográfia ezzel szemben a kvantumfizikai elveket alkalmazza feltörhetetlen kulcsok létrehozására. A kvantumkriptográfia fotonok[34] segítségével továbbítja az információkat, és ezeknek a részecskéknek a kvantumtermészete biztosítja, hogy minden, az átvitel lehallgatására tett kísérletet észleljen. Ennek eredményeként a kvantumkriptográfia lényegében feltörhetetlen biztonságot nyújt, mivel az üzenet elfogására tett kísérletek elkerülhetetlenül megzavarják a fotonokat, és figyelmeztetik a címzettet egy lehallgató jelenlétére. Összefoglalva, a hagyományos titkosítás matematikai megközelítéseket alkalmaz a kulcsok generálására és az adatok védelmére, míg a kvantumkriptográfia a kvantumfizikai elveket alkalmazva állítja elő ezeket. Míg az előzőre csak algoritmikus védelem áll rendelkezésre, az utóbbinál fizikai elvek adják az adatok biztonságát és sérthetetlenségét.

2.4. Az adatok illetéktelen megismerésének kezelése magas kvantumvédelemmel, a kvantum-reziliencia kialakítása

Bár a kvantumkriptográfia még gyerekcipőben jár, a benne rejlő lehetőségek óriásiak. Az előrejelzések szerint a jövőben számos alkalmazásban fogják használni, beleértve egyebek mellett a hálózatbiztonsági, banki és katonai alkalmazásokat. Egyik legjelentősebb előnye, hogy ellenáll a feltörésnek és a lehallgatásnak. Ennek eredményeként a kvantumkriptográfia várhatóan fontos szerepet fog játszani a kiberbiztonság jövőjében. Arra lehet számítani, hogy

[34] A fotonok polarizációjával megvalósított kulcscseréről MAVROEIDIS – VISHI – ZYCH – JØSANG: The Impact of Quantum Computing on Present Cryptography című írásában olvashatunk. *International Journal of Advanced Computer Science and Applications*, 2018/3. 7. o. (https://arxiv.org/pdf/1804.00200.pdf)

egyre többen ismerik fel előnyeit, ugyanakkor számos kihívással kell foglalkozni, mielőtt széles körben alkalmazható lenne.[35] (A US National Institute of Standards and Technology (NIST) bejelentette, hogy egy új posztkvantum kriptográfiai szabvány váltja fel a jelenlegi nyilvános kulcsú titkosítást. A CISA és a NIST nyomatékosan javasolja, hogy a szervezetek már most kezdjék el az átállásra való felkészülést a Post-Quantum Cryptography Roadmap követésével.[36])

A kihívások egyike annak biztosítása, hogy a kvantumkulcs szétosztás (QDK[37]), protokollok nagy távolságokban is használhatóak legyenek. Jelenleg ezeknek a protokolloknak a hatótávolsága korlátozott a szolgáltatás romlása miatt. Ugyanakkor a műholdalapú kommunikáció vagy a kvantumátjátszók használata megoldhatja ezt a problémát a jövőben. Egy további nagyon szükséges fejlesztés az egyfoton detektorok teljesítmény-megbízhatóságának javítása QKD-ban, ami a jövőben is folyamatos kutatási terület lesz. Az érzékenység javítása vagy a zajszint csökkentése is nagyban hozzájárulhat a technológia hatékonyabbá tételéhez a jövőben. Továbbá a hibajavítás javítása és az oldalsó csatornás támadások megelőzése is olyan fejlesztések, amelyeket a jövőben a Quantum kriptográfiában látni fogunk.[38]

Egy megfelelően felépített kvantumszámítógép más technológián alapul, mint a mai hagyományos számítógépek, gyorsan megoldhatja a titkosítással összefüggő matematikai problémákat, feltörve a titkosítási rendszereket. A tudósok véleménye eltérő, hogy mennyi idő múlva jelenhetnek meg ezek kvantumszámítógépek. A tudósok egy része húsz évvel későbbre prognosztizálja, másik részük véleménye szerint ez néhány év múlva is bekövetkezhet. Mivel az elmúlt évben némi előrelépés történt a kvantumszámítás terén, érdemes áttekinteni az alábbi ábrát.

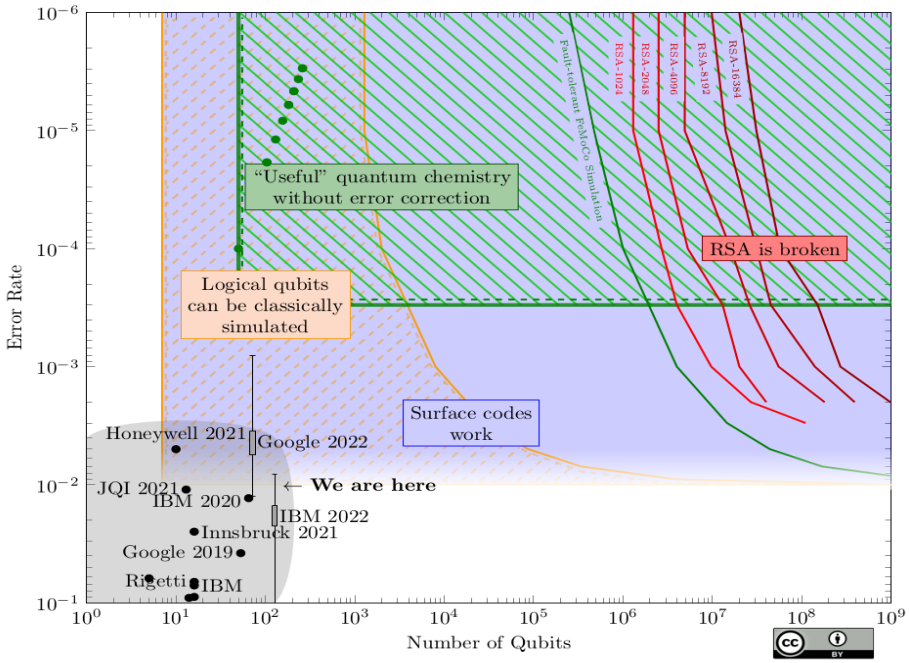
---

[35] *Post-Quantum Cryptography – Integration study*. (https://www.enisa.europa.eu/publications/post-quantum-cryptography-integration-study)

[36] *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. (https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms);
Prepare for a New Cryptographic Standard to Protect Against Future Quantum-Based Threats. (https://www.cisa.gov/news-events/alerts/2022/07/05/prepare-new-cryptographic-standard-protect-against-future-quantum-based-threats)

[37] QDK: Quantum Key Distribution. Egy biztonságos kommunikációs módszer a titkosítási kulcsok cseréjére, amelyek csak megosztott felek között ismertek. A kvantumfizikában fellelhető tulajdonságokat használja fel a kriptográfiai kulcsok bizonyítható és biztonságot garantáló módon történő cseréjére. (https://www.techtarget.com/searchsecurity/definition/quantum-key-distribution-QKD)

[38] IMAM, Sonia: *Exploring the revolutionizing world of quantum cryptography*. 2023. 04. 12. Purevpn, (https://www.purevpn.com/blog/quantum-cryptography/)



3. ábra: A kvantumszámítástechnika helyzete 2022-ben[39]

Magyarázat: A qubit az adatok alapegysége a kvantumszámítógépben, kapu pedig egy qubitre alkalmazott művelet. Ahhoz, hogy a kvantumszámítógépek hasznosak legyenek, több qubitre van szükségünk, de szükségünk van jobb fizikai és azok összekapcsolásából származó logikai qubitekre is. Egy RSA-2048[40] feltöréséhez több mint 2,1 milliárd kapura lenne szükség egymás után. Mindehhez a Moore-törvény[41] szerinti skálázásra van szükségünk, hogy a kvantumszámítógépek valaha is hasznosak legyenek.

A diagram kék tartománya az, ahol a fizikai qubitek elég jók ahhoz, hogy logikai qubiteket képezzenek egy felületi kódban. A diagram sárga csíkos régiója az, ahol nem tudjuk az összes fizikai qubitet szimulálni, de olyan kevés a logikai (hibajavított) qubit, hogy klasszikusan bármilyen hibajavított algoritmust szimulálhatunk. A piros vonalak a Shor-algoritmus minimális követelményeit mutatják a különböző méretű RSA-kulcsok feltöréséhez. A zöld csíkos régió azt mutatja, hogy hol tudunk kvantumszámítógépekkel megoldani néhány kémiai problémát anélkül, hogy teljes hibajavításra lenne szükség. (Ugyanakkor a zöld pontok bizonyos specifikus problémák erőforrásainak számítanak.) **A zöld csíkos régión kívül és a zöld vonaltól balra** egy olyan régiót jelöl, ahol nem tudunk olyan kvantum algoritmust futtatni, amely felülmúlja a klasszikus számítógépeket. Azonban új algoritmusokat fedezhetünk fel, amelyek kvantumszámítógépen futhatnak ebben a régióban.

---

[39] Samuel Jaques az oxfordi egyetem munkatársa rendszeresen értékeli a kvantumszámítástechnika helyzetét, legutóbbi megállapításai elérhetőek a https://sam-jaques.appspot.com/quantum_landscape_2022 oldalon.

[40] RSA: Rivest-Shamir-Adleman algoritmus

[41] Előrejelzése a tranzisztorszám növekedésére vonatkozik. Lásd: Encyclopædia Britannica: *Moore's Law*. (https://www.britannica.com/technology/Moores-law)

Tudományos szempontból ezeknek a számítógépeknek hatalmas szerepe lesz majd, mert az eddig megválaszolhatatlan, nagy számításigényű kérdésekre választ adhatnak. Nemzetbiztonsági szempontból is kiemelt jelentőséget kell, hogy tulajdonítsunk ezen technológiai vívmánynak. A szakértők elemzése rávilágít, hogy a kvantumszámítógépek szélesebb publikum általi elérése kapcsán könnyen feltörhetővé válnak a jelenleg védettnek tartott rendszerek.

Ezen túlmenően legalább akkora veszélyt jelent, hogy a védett információk titkosításának feltörésén keresztül lehetőséget biztosít az ellenérdekelt felek számára az információtartalom megismerésére.[42] További veszélyt jelent, ha ezen információkat közzéteszik a teljes internetközösség számára. A kiberbűnözői körök számára értékes zsarolási alapot képezhet az ilyen típusú információk birtoklása, továbbá a versengő titkosszolgálatoknak is hasznos adatokat, értékelt információkat hordozhat pl. személyre, csoportra, kormányzati szereplőre, vagy akár technológiára vonatkozóan. A fentiek alapján elmondható, hogy emelkedik az úgynevezett HNDL (Harvest Now, Decrypt Later) -támadások kockázata.[43]

A kvantumszámítástechnika fejlődése számos jelenleg használatban lévő kriptográfiai algoritmust veszélyeztethet a világon. Ezeket az algoritmusokat szélesebb körben használják a digitális információk védelmére, azonban a hatékony védelemük érdekében kvantum-rezisztens változatokra történő lecserélésük a jövőben elengedhetetlen. Azoknak a szoftvercsaládoknak, amelyek fejlesztése évekig tartott, de a védelmi algoritmusai már nem elégségesek, azoknak a lecserélése az eddigi költségek és a hosszú átfejlesztési időszak figyelembevétele mellett nem lehet opció, ezért azok kvantumszámítógép-alapú támadások elleni védelmét szükséges kialakítani. A kvantum-rezisztens cryptography[44] célja az, hogy olyan titkosítási rendszert építsenek ki, ami védettséget nyújt mind a klasszikus vagy kvantum számítógépek számítási képessége mellett, továbbá együtt tud működni a meglévő kommunikációs protokollokkal és a meglévő hálózatokon használható. Egyre inkább fontossá válik a posztkvantum algoritmusokra való áttérés, illetve a kriptoközösségek orientálása[45] az átállásra.

„Mivel a kvantumszámítógépek technológiai valósággá válhatnak, ezért fontos tanulmányozni a kvantumszámítógéphez hozzáféréssel rendelkező ellenfelekkel szemben alkalmazott kriptográfiai sémákat. Az ilyen sémák tanulmányozását gyakran post-quantum kriptográfiának nevezik. A technológia iránti igény abból adódik, hogy számos népszerű titkosítási és aláírási séma (ECC és RSA alapú séma) feltörhető a Shor-algoritmus segítségével a jelenleg működő kvantumszámítógépek alkalmazásával. Léteznek példák olyan sémákra,

---

[42] *Előírás lett a poszt-kvantumtitkosítás*. (https://biztonsagportal.hu/eloiras-lett-a-poszt-kvantumtitkositas.html)

[43] SPARKES, Matthew: *Spies may be storing data to decrypt with a future quantum computer*. 2021. 10. 12. (https://www.newscientist.com/article/2293341-spies-may-be-storing-data-to-decrypt-with-a-future-quantum-computer/)

[44] Poszt kvantum titkosítás (amit kvantum-rezisztens titkosításnak is neveznek)

[45] Alapvető dokumentuma: Migration to Post-Quantum Cryptography: Preparation for Considering the Implementation and Adoption of Quantum Safe Cryptography. NIST special publication 1800-38A, https://www.nccoe.nist.gov/crypto-agility-considerations-migrating-post-quantum-cryptographic-algorithms (Letöltés ideje: 2023.07.27.)

amelyek a mai ismereteink szerint biztonságosak a kvantumellenfelekkel szemben, a McEliece és a rács alapú sémák, valamint a legtöbb szimmetrikus kulcsú algoritmus."[46]

Algorithm	Type	Task	Usage in quantum world
AES	symmetric key	encryption	longer key size is needed
SHA-2, SHA-3	-	hash function	Longer fingerprint size is needed
RSA	public key	digital signature key exchange	Insecure
ECDSA ECDH (Elliptic curve)	public key	digital signature key exchange	Insecure
DSA (Finite fields)	public key	digital signature	Insecure

4. ábra: Kvantum-biztonságos és kvantum-tört kripto algoritmusok[47]

Szakértők folyamatosan kutatják azt, hogy a meglévő kriptográfiai technikákat hogyan kell módosítani annak érdekében, hogy képesek legyenek megbirkózni a jövőbeli kvantumellenfelekkel. Tekintettel arra, hogy a jövőben adataink a kvantumtámadásokkal valószínűleg sebezhetők lehetnek, az NSA bejelentette, hogy áttér a kvantumrezisztens algoritmusokra.[48] Ajánlásai alapján minden szervezetnek fontolóra kellene vennie, hogy a hagyományos eljárások esetén az aszimmetrikus kulcshosszok hosszának növelése védelmet nyújthat a hibajavított kvantumszámítógépek korai verziói ellen, ugyanis ezeknek a kulcsoknak a feltöréséhez sokkal több qubitre van szükség. Ahol lehetséges, törekedni kell a szimmetrikus kriptográfia használatára. Rendelkezésre állnak nyílt webkörnyezetben olyan kriptográfiai szoftverkönyvtárak[49], amelyek segítik a felhasználást és telepítést.

A téma fontosságát mutatja az is, hogy a NIST CSRC (Computer Security Resource Center) már 2016 óta foglalkozik a kérdéssel.[50] Az első időszakban sokan nem tulajdonítottak nagy jelentőséget a témának, inkább a tudományos közegre bízták annak a kezelését és kutatását. Az MI támogatott rendszerek napi életbe történő felhasználatának fejlődési üteme rávilágított arra, hogy egyes technológiák fejlődési sebessége központilag, kormányzati szinten közvetlenül nem befolyásolható, de alkalmazására szabályozott keretek alakíthatók ki. Ez az analógia a

---

[46] BERNSTEIN, Daniel J.: *Introduction to post-quantum cryptography.* Department of Computer Science, University of Illinois at Chicago, 2009. (http://www.pqcrypto.org/www.springer.com/cda/content/document/cda_downloaddocument/9783540887010-c1.pdf)

[47] Kvantum-biztonságos és kvantum-tört kripto algoritmusok tanulmány alapján összeállított ábra. Forrás: *Quantum-Safe Cryptography*. (https://cryptobook.nakov.com/quantum-safe-cryptography)

[48] *NSA Suite B Cryptography*. Archived from the original on 1 January 2016. Retrieved 29 December 2015. (https://web.archive.org/web/20160101091229/https:/www.nsa.gov/ia/programs/suiteb_cryptography/)

[49] IANIX: *PQCrypto Usage & Deployment*. Updated: 2023. 06. 26. (https://ianix.com/pqcrypto/pqcrypto-deployment.html)

[50] National Cybersecurity Center of Excellence: *Conference 2016 Cybersecurity Brainstorm*. 2016. 09. 12. (https://www.nccoe.nist.gov/get-involved/attend-events/2016-cybersecurity-brainstorm)

kvantumszámítógépekre szintén alkalmazható. Ez azonban nem tudja a használatba vételt, illetve elterjedés gátját állni, ugyanakkor jelentős mértékben lelassíthatja azt. Mindezzel lehetőséget teremt arra, hogy a társadalmi reziliencia az elvárt szintet elérje.

2022 júliusában az USA-ban működő National Cybersecurity Center of Excellence tesztelést követően kiválasztotta azokat a titkosítási algoritmusokat, amelyek a jövőben felépítésük miatt ellenállóak lehetnek egy kvantumszámítógép jövőbeli támadásával szemben. A kiválasztott négy titkosítási algoritmus (Ccrystals-Kyber, Crystalls-Dilithium, Falcon és Sphincs+[51,52]) a következő években hivatalosan is a NIST posztkvantum kriptográfiai szabványának részévé vállhat. Fontos ez azért is, mert a mindennapos használatban lévő digitális rendszerek (pl. email-szoftverek, banki szolgáltatások) védelme, működésfolytonosságuk fenntartása elemi érdek. Fenti algoritmusokat két tipikusan titkosítást használó feladatra tervezték: egyrészt általános titkosításra, amely a nyilvános hálózaton keresztül küldött információk védelmére szolgál; másrészt a személyazonosság hitelesítéshez használt digitális aláírások védelmére. Kifejlesztésük fontos ismérve, hogy több ország és számos intézmény szakértői hozták létre.

A magyar kormányzat is felismerte a szabályozás fontosságát. A jogalkotó a 2013. évi L. törvény módosításával előírja, hogy a hatálya alá tartozó elektronikus információs rendszerek teljes életciklusában meg kell valósítani és biztosítani kell a poszt-kvantum titkosítási alkalmazással történő zárt, teljes körű, folytonos és kockázatokkal arányos védelmét.[53] A kormányzat részéről történő hatékony ellentevékenységek kereteinek alakításához és időszaki aktualizálásához sok hasznos információval szolgálhatnak a nemzetbiztonsági szolgálatok.

2.5. A kibertér, mint az információszerzési ágak formáló tényezője

A digitális függés kialakulásának egyik legjobb történelmi példája, a geopolitikai küzdelmek egyik legaktuálisabb helyszíne, a kibertér. Az elnevezés mögött több tudományági érintettség is megjelenik, és kimondottan multidiszciplináris fogalommal állunk szemben. A témakör tudományelméleti feltérképezését Kelemen Roland kellő alapossággal megtette „A kibertér jellemzőinek biztonság központú vizsgálata”[54] című írásában. Hosszas tudományelméleti, jogi fejtegetés helyett egyetértünk azzal, hogy a kibertér különböző kommunikációs rendszerek önálló belső tereiből épül fel, amelyek további téregységekre bonthatók. *„A kibertér így az információk és a kommunikáció áramlásának egyfajta koncepcionális tereként jellemezhető,*

[51] NIST: *NIST Announces First Four Quantum-Resistant Cryptographic Algorithms*. 2022. (https://www.nist.gov/news-events/news/2022/07/nist-announces-first-four-quantum-resistant-cryptographic-algorithms)

[52] Strukturált rácsokon és hash függvényeken alapuló algoritmusok.

[53] *Magyar Közlöny* 2021. évi 231. szám. 2021. 12. 17 https://magyarkozlony.hu/dokumentumok/c7e1e8606dd1361a72d77734515809ee71c76f6e/megtekintes

[54] KELEMEN Roland: A kibertér jellemzőinek biztonság központú vizsgálata. *Jog-Állam-Politika*, 2023/1. 75-90. o. (http://real.mtak.hu/165609/1/JAP_2023_01_KELEMEN_ROLAND.pdf)

amely a digitális világ hardver eszközei, a számítógépek szoftverei, a telekommunikációs hálózatok és az emberi elme szerves kombinációjából jött létre."[55]

A folyamatosan bővülő kibertér és a kibertérben nyújtott szolgáltatások köre, annak egyes szereplői közvetlen hatással vannak az egyén éntudatára, gondolkodására, a közösségre, illetve annak társadalmi helyzetére, szerepére. Ahogy Manuel Castells spanyol szociológus írja – a hálózathoz tartozás a létezés fokmérőjévé vált,[56] ahol a *„hálózati társadalom testetlenné teszi a hálózati viszonyokat"*.[57] A kibertérben az emberek információkat osztanak meg, üzleti tevékenységet folytatnak, szórakoznak és a mindennapi életüket is megélik, amelynek során elektronikus eszközökön, hálózatokon és számítógépeken keresztül kommunikálnak, távolról (személyes jelenlét nélkül) kapcsolódnak egymáshoz. Az általuk használt virtuális terek lehetőséget kínálnak az adatok tárolására, feldolgozására és megosztására, az elektronikus kereskedelemre, a közösségi média használatára és sok egyéb tevékenységre. Ezekbe a folyamatokba kapcsolódhatnak be a nemzetbiztonsági szolgálatok különféle céljaik mentén, az egyes információszerzési ágak sajátságos kifejlesztett eszközrendszerei, és az azokat különféle módszertani elvek alapján működtető személyek.

2.5.1. Nyilvánosan elérhető információk

Manapság egyre több kormányzati szereplő, vállalat és egyén csatlakozik az internethez, használja annak szolgáltatásait, egyúttal telekommunikációs és informatikai eszközökön keresztül saját tevékenységét kitükrözi a digitális térbe. Ezek az adatok nyilvánosan elérhető információkká[58] válnak, és különféle kapcsolatokat alkotnak egymással. Valójában a nyilvános forrású információ elnevezés egy gyűjtőfogalom, amely a különböző nyilvános forrásokban található adatok körét fedi le. Forrásai a teljesség igénye nélkül:[59] blogok, digitális újságok, sajtótájékoztatók, tudományos publikációk, ipari értékelések, szabadalmak, műszaki adatok (stb.).

Valójában a PAI tevékenység szolgáltatja a nyílt forrású hírszerzés alapanyagait, amelyek számos hírszerzési termék összeállításának alapját képezhetik a nemzetbiztonsági tevékenység során. A kibertérben számos fenyegetést hordozó entitás – kiberbűnözők, szervezett bűnöző csoport, terroristasejt – megjelenik és kommunikál, használja a digitális teret a nemzetbiztonságot veszélyeztető kommunikációra, tervezésre és cselekvésre.

A digitális világban az információfelhasználó kormányzati szervek, köztük a nemzetbiztonsági szolgálatok tevékenységéhez fontosnak ítélt adat bizonyos része valamilyen formában vagy összefüggésben megtalálható. Ezek képezhetik a később módszeresen

---

[55] JAKOBI Ákos – LENGYEL Balázs: Egy online közösségi háló offline földrajza, avagy a távolság és a méret szerepének magyar empíriái. *Tér*, 2014/1. 43. o.

[56] PINTÉR Róbert: Úton az információs társadalom megismerése felé. In: PINTÉR Róbert (szerk.): *Az információs társadalom – Az elmélettől a politikai gyakorlatig*. Budapest, Gondolat-Új Mandátum, 2007. 25. o.

[57] CASTELLS, Manuel: *Az évezred vége – Az információ kora: Gazdaság, társadalom és kultúra III. kötet*. Budapest, Gondolat Kiadó, 2007. 433. o.

[58] Publically Available Information

[59] Babelstreet: Publicly Available Information Explained. (https://www.babelstreet.com/blog/pai-explained)

kialakított tudásuk összetevőit. 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.[60]

2.5.2. Nyílt forrású hírszerzés (OSINT[61])

Az OSINT a 21. századra a nemzetbiztonsági tevékenység meghatározó módszerévé vált, több területen is jelentős segítséget ad a nemzetbiztonsági szervezeteknek feladataik eredményes végrehajtásához.[62] A hírszerző, felderítő szervezetek számára az OSINT tulajdonképpen egy adatszerző „szervezet" olyan távoli térségek esetében, ahol nem rendelkeznek egyéb képességgel, és amely azonnal és lényegében kockázatok nélkül képes az információgyűjtésre.[63]

Az OSINT legegyszerűbb megfogalmazásában *„hírszerzés a nyilvánosság számára elérhető forrásból"*[64]*,* írja Polmar és Alen 1997-ben megjelent könyvében. Vida Csaba (2013) tanulmánya alapján : *„Az OSINT-tevékenység: az önálló nyílt adatszerző tevékenység 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 felkutatását, gyűjtését, szelektálását, értékelését és felhasználását jelenti".* Összességében elmondható, hogy a szakirodalmakban számos meghatározással találkozhatunk, gyakran változó fogalmi összetevőkkel. Ezekre jelenlegi tanulmányunkban nem térünk ki, az azonban fontos számunkra, hogy az OSINT tevékenység egyik megjelenési terepe a kibertérhez és annak szereplőihez kötődik. A kibertérhez kötődés okán érdemes megemlíteni, hogy az OSINT mint legális passzív módszer és a hacking, mint illegális aktív tevékenység között is összemosódnak időnként a határvonalak. Ugyanis több az OSINT tevékenységhez kötődő nyílt forrású eszköz (pl. Google-dorking vagy a Shodan) alkalmas sebezhetőségek feltárására, majd ennek felhasználásával illegális adatszerzésre.

Az OSINT jelentőségének további növekedését nagyban segítheti a technológia (MI képességek) fejlődése, amellyel az OSINT több részfeladata (keresés, elemzés, értékelés) automatizálhatóvá tehető. Az OSINT-tevékenység egyik legfőbb területe a közösségi terek, például a Facebook, LinkedIn, Instagram, számtalan blog, fórum, csevegőfelület (stb.) figyelése és vizsgálata. Az OSINT keresési eszköztára igen gyorsan változik. Erre a célra kifejlesztett keresők segítségével nemcsak naprakész adatokhoz juthatunk, hanem azokat feldolgozva rejtett összefüggéseket is feltárhatunk. A közösségi média keresőalkalmazásokkal történő figyelése általában úgy történik, hogy egy vagy néhány paraméter ismeretében találjuk meg a

---

60 ERDÉSZ Viktor: *A mesterséges intelligencia felhasználási lehetőségei a korszerű nemzetbiztonsági szolgálatok tevékenységében*. (PhD értekezés) Budapest, Nemzeti Közszolgálati Egyetem, 2022. 108-109. o.

61 Open Source Intelligence

62 MEZEI József: A szervezetrendszerek módosítása, strukturális válaszok. In: DOBÁK Imre (szerk.): *Nemzetbiztonság a 21. század elején*. Budapest, 2022. 95. o.

63 KENEDLI Tamás: A nyílt forrású információszerzés (OSINT). In: Dobák Imre (szerk.): *A nemzetbiztonság általános elmélete*. Budapest, Nemzeti Közszolgálati Egyetem, 2014. 170. o.

64 POLMAR, Norman – ALLEN, B. Thomas: *Spy Book: The encyclopedia of Espionage*. London, Greenhill Books (Random House), 1997. 414. o.

többi releváns adatot. Adat-, illetve szövegbányász eszközökkel ezekből – akár rejtett – összefüggéseket tárhatunk fel, és előrejelzéseket készíthetünk.[65]

A továbbiakban vegyünk sorra néhány példát az OSINT-tevékenység támogatására. Az amerikai védelmi szféra nyílt forrású tartalomszolgáltatója a minneapolisi East View Information Services. Egyik termékük a Kínai Nemzeti Tudás Infrastruktúra (CNKI[66]) licenszelt változata, ami a legnagyobb kínai akadémiai adatbázis. Évente több mint 5000 kutatás-fejlesztési és innovációs tudományos folyóiratban 1,1 millió kutató mintegy hatmillió tudományos publikációt tesz közzé. Fő előnye a cikkek, a kutatók és az intézmények kontextusának, egymás közötti kapcsolatának feltérképezhetőségében áll. Az East View további nyílt adatbázisokat is szolgáltat az amerikai védelmi szféra részére (GEOINT adatbázissal is rendelkezik). A vállalat globális sajtóarchívumában több mint nyolcvan ország 30 nyelvén az 1700-as évek óta íródott, több mint 30 millió oldalnyi jogvédett, kereshető sajtóanyag érhető el. Az East View a kínai mellett az orosz nyelvű publikációk terén is fontos szereplőként aposztrofálja magát.

Az East View-val és további 17 tartalomszolgáltatóval áll szerződésben a washingtoni Georgetown Egyetem kialakulóban lévő technológiákkal és azok biztonsági vonatkozásaival foglalkozó kutatóközpontja (CSET[67]). A szolgáltatók összesen 28 terabájt szöveges adatot biztosítanak, ami mintegy 14 milliárd oldalnak felel meg. A 215 millió szövegcorpus többségét elsősorban angol, kínai és orosz nyelvű tudományos publikáció; több mint ötmillió szervezeti ábra, […] illetve sajtóadatbázisok és üzleti hírszerzési információk teszik ki. A jól strukturált, megbízható és kifinomult módszerekkel elemzett nagy adat alapján, jól megalapozott, mély elemzéseket és értékeléseket képesek készíteni szervezetekről és személyekről.[68]

Ugyancsak hatékony eszköz az Airbus OSINT-platformja, ami az internet keresőmotorok által elérhető területéről (surface web), a deep webről és a dark webről is képes nagy mennyiségű, strukturálatlan információ automatikus, felhő alapú gyűjtésére, kinyerésére és elemzés-értékelésére. Az információ keresését egyebek mellett filterek alkalmazásával, szemantikus kereséssel valósítja meg. A folyamat során az MI-algoritmus értelmezi a kérdést, és ennek alapján gyűjti össze a találatokat. 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, valamint a beszélő azonosítása.

Végezetül érdemes még megemlíteni BAE Systems plc[69] cégcsoporton belül a BAE Systems IntelligenceReveal Search & Analysis module nevű, felhő alapú a hírszerző tevékenységet támogató OSINT rendszerét, amely rugalmas modulkialakításokkal rendelkezik.

---

65 VADÁSZ: i. m. 70. o.

66 China National Knowledge Infrastructure

67 Center for Security and Emerging Technology

68 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. október 30.

69 *BAE Systems*. (https://www.baesystems.com/en/digital/solutions/by-business-objective/building-a-unified-intelligence-picture-from-communications-data-and-beyond)

Alkalmas nem rendszerezett adatok kezelésére, kommunikáció elemzésére, tudásmenedzsment támogatásra, biztonságos böngészésre, adatbázisok importálására. Mindezeken felül lehetőséget teremt entitáskinyerésre, témakörök elemzésére és hangulatelemzésre. A rendszer a Twitteren, a Facebookon, a Google+-on és a YouTube kommentekben megjelent információk, valamint az RSS-hírcsatornákra feltöltött cikkek monitorozására ugyancsak képes.

2.5.3. A közösségi hálózatokból történő információszerzés (SOCMINT[70])

Az előző témakörben ismertetett OSINT tevékenység keretében bemutatott rendszerek általában rendelkeznek SOCMINT képességekkel (önálló vagy integrált formában). A nyílt forrásból történő információgyűjtésen belül mintegy részterület jelenik meg a közösségi média oldalairól történő információgyűjtés. Erdész Viktor megfogalmazása szerint *„a SOCMINT, az OSINT […] 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*".[71] Az előző rendszerszintű pozícionálás és mellette a tényleges tevékenység leírására Teodor Tropotei és Ioan Deac művében kaphatunk választ, amely szerint „a SOCMINT a közösségi oldalakon lévő online adatok azonosításával, gyűjtésével, összeállításával, hitelesítésével, ellenőrzésével és elemzésével foglalkozik, amely során beavatkozó és nem beavatkozó módszereket alkalmaz."[72]

A SOCMINT célterületeként megjelenő internetes közösségi média egyre növekvő szerepet tölt be a világ szinte valamennyi országának társadalmi, gazdasági és politikai életében, folyamatosan formálja, átalakítja a társadalom rétegeiben megjelenő kommunikációt. Az online közösségi hálózatban általában olyan csoportosulások láthatók, amelyek tagjai közös érdeklődési kör mentén szerveződnek, és lehetőség van az internetes alkalmazáson keresztül történő interakciókra (többek között kommunikációkra).[73] Résztvevői életük történéseinek egyre nagyobb részét osztják meg a hatalmas digitális közösségek szereplőivel. A megosztott tartalmak érdemben befolyásolhatják a többi felhasználó vélekedését és cselekedeteit. Az emberek ma már sokkal több személyes információt osztanak meg önmagukról, barátaikról és kapcsolati hálózataikról, mint korábban, ehhez új és változatos módszereket, platformokat használnak fel. Manapság a tradicionális internetes médiafelületeken közzétett információk is akkor tudnak nagyobb hatásfokkal célt érni, amennyiben becsatornázzák őket valamely közösségi média platformra.

Tendenciaként megfigyelhető, hogy a közösségi platformok üzemeltetése során a tartalomszolgáltatók MI alapú elemző szoftvereinek egyre kifinomultabb algoritmusai eleve olyan tartalmakat állítanak össze a felhasználók részére, amiket azok szívesen megtekintenek. Az egyénre szabott tartalomszolgáltatás egyik velejárója, hogy a közzétett információról

---

70 Social Media Intelligence

71 ERDÉSZ Viktor: A SOCMINT helye, szerepe az összadatforrású hírszerzésben. *Felderítő Szemle*, 2018/4. 27-40. o.

72 TROPOTEI, Teodor – DEAC, Ioan: Social Media in Intelligence Analysis. *Strategic Impact*, 2019/1-2. 70. o.

73 VARGA Gábor: *Közösségi hálózatok II. A követelménymodul megnevezése: Távközlési szaktevékenységek.* Budapest, Nemzeti Szakképzési és Felnőttképzési Intézet, 2008. 34. o.

történő közösségi kommunikáció „véleménybuborékokban”[74] valósul meg. A véleménybuborékban történő kifejezés maga után vonja a hasonló érdeklődésű és nézetű személyek csoportba rendeződését is. Mindez részvételi, egyúttal információszerzési lehetőséget biztosíthat a nemzetbiztonsági szakemberek számára is olyan esetekben, amikor a nemzet biztonságát érintő kérdésekben kell tájékozódniuk.

Ahogy a társadalom a kor technológiai környezetének megfelelően fejlődik, és új rendszereket, módszereket alkalmaz a kommunikáció és az információmegosztás során, létfontosságú, hogy a nemzetbiztonsági szolgálatok is folyamatosan lépést tartsanak ezekkel a változásokkal. Tevékenységük során azonban nem árt tudatosan figyelemmel lenni a SOCMINT alkalmazásának alapelveire[75], amelyek tevékenységük során szempontként kell, hogy megjelenjenek.

A közösségi hálózatok működésük miatt (azonnali frissítések megvalósítása), a SOCMINT során egyfajta valós idejű információszerzési lehetőséget biztosítanak a nemzetbiztonsági szakemberek számára. A közösségi hálózatokhoz kapcsolódó felhasználók a szolgáltatók technológiai környezete és egyebek mellett az okostelefonok használata miatt információszolgáltatóvá, véleményformálóvá válnak, hozzájárulnak a folyamatban lévő események megértéséhez, elemzéséhez. Példaként említhető a 2011-es londoni zavargások és az Arab Tavasz[76] eseményeinek valós időben történő közzététele, amivel azonban így elősegítette a nemzetbiztonsági szervek információgyűjtését is, illetve megkönnyítette a válságkezeléshez szükséges intézkedések rangsorolását.

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.[77] Célszerű lehet mérlegelni azt is, hogy más információszerzési ágak lehetőségeihez képest milyen esetekben kerülhet előtérbe a SOCMINT.

A SOCMINT előnyének kell tekinteni:[78]

- olyan információk is megszerezhetők, amely más hírszerzési ággal nem, vagy nagyon nehezen begyűjthetők;
- egy-egy eseményről a bekövetkezésének időszakában lehet – több forrásból származó, más-más szempontok alapján létrehozott – információt beszerezni;
- hatalmas mennyiségű információ szerezhető vele viszonylag rövid időn belül;
- sok esetben költséghatékonyabb más hírszerzési ághoz képest.

---

74 Filter bubble

75 Részleteiben megismerhető: OMAND, David – BARTLETT, Jamie – MILLER, Carl: *A balance between security and privacy online must be struck*. London, Demos, 2012. 11. o.

76 Az ISIL/DAESH által végzett, toborzó célú médiatevékenység.

77 ERDÉSZ (2022): i. m. 114. o.

78 VIDA Csaba: A SOCMINT szerepe az elemző-értékelő munkában című írásából származó módosított változat. *Szakmai Szemle*, 2022/2. 18-19. o.

A SOCMINT egyik fő előnye, hogy nagy mennyiségű adatot és információt használ[79] és szolgáltat, amely viszonylag könnyen elérhető, tárolható vagy terjeszthető. Kulcskérdés azonban, hogy hogyan jutunk el a kívánt információ megszerzéséig, ugyanis, ha nem megfelelő információs kapcsolatokon keresztül haladunk és jutunk el a célzott információforrásig, a végkövetkeztetésünk is téves lehet. Mivel rengeteg információ keletkezik az információgyűjtés során és vár elemzésre-értékelésre, megoldásokat kell kidolgozni arra vonatkozóan, miképp tudják azokat a nemzetbiztonsági szakemberek átalakítani a munkájukhoz alkalmas alapanyaggá.

Fontos megjegyezni, hogy a közösségi oldalakon történő információszerzéshez kötődő alkalmazott adatgyűjtési stratégiák (kényelmi minták, véletlenszerű mintavétel), hatékonysága elmarad a reprezentatív mintákétól, ami a levonható következtetések minőségét is lerontja az elemzés során.

A közösségi média monitorozására, az onnan történő információszerzésre, majd az értékelés-elemzés elvégzéséhez megfelelően kialakított, a médiaplatformokhoz illeszkedő, azok változásait lekövető szoftverkörnyezetet és szolgáltatástartalmat szükséges igénybe venni. Ezeket az eszközrendszereket célirányosan fejlesztik a nemzetbiztonsági felhasználók számára is (ilyen például a Medusa Labs SOCMINT platformja[80]). A rendszer gépi tanulási algoritmusai képesek különféle trendek (pl. politikai, bűnügyi stb.) közel valós idejű nyomon követésére, az eredmények megjelenítésére, szereplők azonosítására, illetve kapcsolataik nyomon követésére és a kapcsolódó vélemények elemzésére. A rendszer a monitorozott információt letölti és eltárolja, így akkor is felhasználható, amikor a tartalom már nem elérhető a weben. Képes adatelemzésre, nyelvi elemzésre, entitáskinyerésre, az összefüggések alapján hangulatelemzésre. Tartalmaz továbbá az elemzéshez szükséges eszközöket is (pl. grafikonok, térképes és hálózatos megjelenítés, szemantikai és kapcsolati elemzés). A hangulatelemzés során hatékonyan alkalmazhatók a gép tanulási algoritmusok, amelyek segítségével bizonyos tulajdonságokat és jellemzőket (strukturálatlan adatokat) kereshetünk egy szövegben. A lényeg, hogy statisztikailag korreláljanak egy általunk keresett, meghatározott bizonyos érzelemmel vagy hangulattal, amit a gépi tanulási algoritmus az adatgyűjtést követően automatikusan osztályoz számunkra. Összefoglalva elmondható, hogy a SOCMINT eszköztára és annak szolgáltatástartalma folyamatosan változik és a közösségi oldalak térhódításával együtt fejlődik, illetve a kibertér változó viszonyaihoz illeszkedik.

2.5.4. Geoinformációs/térinformatikai hírszerzés (GEOINT[81])

A geoinformációs termékek előállításának elsődleges célja a műveleti terület vizualizációja, a harcmező jellemzőinek realisztikus bemutatása minden szinten (hadászati, hadműveleti és harcászati) és minden térképi méretarányban. A speciális geoinformációs termékek jellemzője

[79] A nagy adatokat termelő közösségimédiát aktívan felhasználók száma 2023 júliusában elérte a 4,88 milliárd főt világszerte. Lásd: *Datareportal*. (https://datareportal-com.translate.goog/global-digital-overview?_x_tr_sl=auto&_x_tr_tl=hu&_x_tr_hl=hu#:~:text=Roughly%204.66%20billion%20people%20around)

[80] *Medusa Labs*. (https://www.medusa-labs.com/)

[81] Geospatial Intelligence.

az informatikai eszközök és módszerek integrált alkalmazása az adatok előállítása, elemzések végrehajtása során, a fejlett technikájú érzékelők/szenzorok adatainak feldolgozása, a geoinformációs adatok széles skálájának használata, valamint a harmadik és a negyedik dimenzió szemléltetése, bemutatása.[82]

Korunk technológiai fejlődése során az GEOINT (és IMINT) szakterületek a műholdak, a felderítő repülőgépek, a megfigyelő kamerák felvételeinek tömeges feldolgozásával és a térinformatikai adatok gyors megjelenítésével folyamatosan növelik hatékonyságukat. A támogató szoftverekkel és szolgáltatásokkal – a saját vagy vásárolt műholdfelvételek felhasználásával – nagy pontosságú és a valós helyzetet bemutató térképek készíthetők. A szoftverkörnyezet általában más adatbázisokhoz is hozzákapcsolható és múltbeli információkkal is összevethető, ami az anomáliák felfedésében és az előrejelzések készítésében kulcsszerepet játszhat.

A GEOINT tevékenységek lehetőségeinek kiaknázása tekintetében valószínűleg az amerikai Nemzeti Felderítő Iroda (NRO) 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.

A GEOINT rendszerek általában petabájtos[83] nagyságrendű adatkezelésre is alkalmasak. Az ilyen 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, ami különösen fontos lehet például a katonai műveleti területen[84] a hírszerző erők munkájának ellátása során.

A világszerte megtalálható számos szolgáltató és szoftverkörnyezet közül érdemes megemlíteni még a Cobwebs vállalat[85] nagy adat alapú (többmilliárd adatpont kezelésére képes) térinformatikai hírszerzési platformját a WebLoc-ot. A programkörnyezet interaktív, rétegzett digitális térképekkel és jól áttekinthető felületekkel segíti az információk rendszerezését, megértését és a döntési folyamatokat. Az OSINT/GEOINT-információk elemzésével mintázatok, trendek és anomáliák mutathatók ki és fenyegetések deríthetők fel, a háttérinformációkat tartalmazó adatbázisok összekötésével generálva hozzáadott értéket, majd valós idejű riasztásokat a felhasználók felé. A nemzetbiztonsági szakember számára a georeferált és időbélyegzővel ellátott adatok terület alapú, idővonalba rendezett összevetésével fedhet fel rejtett összefüggéseket. A technológia fontos előnye, hogy a műveleti erők kockázatvállalása nélkül, geoinformációk megjelenítésével, a helyszín bejárása nélkül is kialakítható a hely- és helyzetismeret a megfigyelt térségről.

---

[82] Koós Tamás: A geoinformációs támogatás korszerű elemei, avagy új színfoltok a geoinformációs támogatás palettáján. *Hadmérnök*, 2009/4. 230. o.

[83] 1 petabájt = 1 048 576 gigabájt.

[84] British Aerospace Applied Intelligence (Egyesült Királyság) hadműveleti területre fejleszt ilyen technológiát.

[85] Cobwebs Technologies honlapja: https://cobwebs.com/

2.5.5. Képi felderítés (IMINT[86])

A GEOINT témakörnél leírt megállapítások és összefüggések mellett elmondható továbbá, hogy egy MI-vel támogatott térinformatikai rendszer a nagymennyiségű adatfeldolgozási, katalogizálási anomáliák kimutatásával támogatja az előrejelzések készítését és a lehetséges cselekvési változatok modellezését. Működésekor tereptárgyak, objektumok, vagy eszközök azonosítása során képes összevetni a különféle forrásból beszerzett műholdképek felvételeit más IMINT, SIGINT, HUMINT, vagy OSINT adatokkal. Alkalmas múltbeli események elemzésére, illetve a jelenlegi helyzet pontosabb megismerésére.

Fenti technológia alkalmazására példaként említhetjük az Airbus Joint ISR Fortion Image Analyst rendszerét, ami több forrású gépi tanuláson alapuló adatelemzésre alkalmas. Ilyenek lehetnek a képek, videók, földi mozgócélok felderítésével kinyert információk,[87] automatikus azonosító rendszerek[88] és harcászati adatlinkek információi. Egyebek mellett alkalmas tárgyak automatikus észlelésére és azonosítására, objektumok elemzésére, illetve célkiválasztásra. A rendszer elemeként kifejlesztésre került egy félautomata azonosítási rendszer, ami több mint 1800 haditechnikai eszköz rendszeresen frissített adatait tartalmazza és lehetővé teszi azok különböző fényviszonyok közötti, 3D-ben történő megjelenítését.[89]

2.5.6. Rádióelektronikai felderítés (SIGINT[90])

A SIGINT-re a nagy mennyiségű technikai és egyéb (pl. közlemény) típusú adatok jellemzőek, amely területeken kiemelt szerepe lehet a MI alapú SIGINT-rendszerek fejlesztésének és rendszerbe állításának. A SIGINT-hez sorolható adattípusok széles köre (pl. metaadatok: a kommunikáció időpontja, időtartama, kommunikáció földrajzi helye, azonosításhoz szükséges különböző azonosítók, stb.) mellett fontosnak tartjuk kiemelni, a folyamatosan fejlődő elemzési-feldolgozási képességeket. Napjainkban már „jellemzően a SIGINT- szoftvercsomagok is képesek hálózatelemzésre, a lehallgatott beszéd szöveggé alakítására és fordítására, valamint hangfelismerésre. Az elemzések alapja itt is az entitáskinyerés."[91]

Az arra feljogosított szervezetek számára lehetőség van például az ECHO nevű web alapú (virtuális) globális SIGINT-rendszer segítségével a világon bárhol 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 nagy adat kezelési lehetőség a rendszert alkalmassá teszi az adott ország valamennyi, okostelefonnal rendelkező internethasználójának a megfigyelésére.[92]

---

86 Imagery Intelligence.

87 Ground Moving Target Indicating – GMTI: a radarok egyik üzemmódja, amellyel megkülönböztethetők a célinformációk a háttérzajtól.

88 Automatic Identification System – AIS.

89 Airbus: *Fortion RECCE Engine – Identify mobile targets at first sight*. (https://www.intelligence-airbusds.com/markets/defence/joint-isr/mono-domain-exploitation/fortion-recce-engine/)

90 Signal intelligence.

91 ERDÉSZ (2022): i. m. 239. o.

92 Rayzone Group: *ECHO – Global Virtual SIGINT System*. (https://rayzone.com/echoglobal-virtual-sigint-system/)

A nemzetbiztonsági szolgálatok a távközlési szolgáltatóktól beszerzett és lehallgatott adatok és információk elemzésére már piaci, kész megoldásokat is alkalmazhatnak. Ilyen a Klarios nevű német szoftver, amit az adatok elemzésére, szűkítésére, rendszerezésére is felhasználhatnak. Mindehhez egy felhasználóbarát, jól átlátható felületet kapnak, amelyen kereséseket is végezhetnek. A programozók a rendszerbe sok milliárd metaadat feldolgozását tették lehetővé, ezért egy adott ország távközlési információinak feldolgozására is alkalmas. Szolgáltatásai között szerepel a hangfelismerés, a földrajzi (térinformatikai) adatok kinyerése, megjelenítése, ilyen adatbázisok létrehozása és importálására. „Képes a különböző távközlési módok (PSTN, GSM, VoIP, stb.) integrált kezelésére is. Összekapcsolható az országos video-megfigyelési, útlevél- és előfizetői adatbázisokkal, illetve a közösségi média felderítésére szolgáló szoftverekkel.”[93]

Egy katonai szakterületen működő nemzetbiztonsági szolgálat számára a Fortion Electronic Warfare Analyst (EWA) elektronikai felderítési (ELINT) elemzőmodulja nyújthat segítséget az elektromágneses sugárzást kibocsátó eszközök azonosítása, helymeghatározása, nyomonkövetése és jellemzőik meghatározása érdekében. Mint Erdész V. megfogalmazza már többször hivatkozott munkájában, a rendszer az elektronikai harcrend felrajzolását is lehetővé teszi. „Az elemzéshez rádióforgalmazási adatokat, radarjeleket, zavaróeszközök jeleit, irányvonal adatokat stb. használ fel.”[94]

2.5.7. Kiberhírszerzés (CYBINT[95])

Célterülete maguk a számítógépek és az azokat összekötő hálózatok, illetve sajátságosan az internet. A hálózatokon keresztül olyan, a számítógépeken tárolt információk és adatok megszerzésére irányul, amelyeket az információ tulajdonosa nem kíván közzétenni, ezért saját számítógépén vagy zárt hálózaton tárolja. Az információk megszerzése történhet zárt hálózatokba történő betöréssel, illetve a számítógépek és az informatikai hálózatok által kisugárzott jelekből történő adatszerzés által.

Számos formája közül, jelen tanulmányban csak példaként egyik jellemző megvalósulási lehetőségét emeljük ki, a hosszantartó, kifinomult adatszivárogtatást célzó támadást (APT). Az APT-t az angol Advanced Persistent Threat szóból képezték, amit magyar nyelvre fordítva folyamatosan jelenlévő, rejtett fenyegetésként jelent. Az APT elsősorban kibertéri adatszerzést célzó olyan támadási forma, aminek célja, hogy a feltört rendszeren belül minél több rendszerelemet érjen el, valamint a hosszan tartó rejtett jelenlétét fenntartsa. Sok esetben a rendszerekből, rendszerekről megszerzett információt ki is szivárogtatja.

Az APT csoportok céljait négy kategóriába sorolhatjuk:[96]

- az állami tulajdonú információk ellopását célzó kiberkémkedés;
- a motiváción alapuló kiberbűncselekmények;

---

[93] *Klarios ATIS Interception Management System*. (https://www.atissystems.com/language/en/klarios-atis-interception-management-system/)

[94] Airbus: *Airbus JOINT ISR*. (https://www.intelligence-airbusds.com/markets/defence/joint-isr/)

[95] Cyber Intelligence

[96] Advanced Persistent Threat (APT) felhasználásával. Crowdstrike: *Advanced Persistent Threat (APT)*. 2022. június 15. (https://www.crowdstrike.com/cybersecurity-101/advanced-persistent-threat-apt/)

- a hacktivizmus;
- a megtámadott rendszerekben végrehajtott rombolás.

A támadásforma komplexitása is utal a támadócsoport felkészültségére, pénzügyi és humánerőforrás-igényére is. Ebből adódóan az APT csoportok mögött sok esetben nagy bűnözői körök, illetve kormányzati szervezetek állhatnak. Az MI felhasználásával – CYBINT keretén belül – a rejtjelkulcsok gyors megfejtése, biztonsági rések automatizált felderítése, a célhálózatok gyors és automatizált felderítése, a releváns információk kigyűjtése, majd feltűnés nélküli továbbítása további fejlődésen mehet keresztül. A CYBINT vonatkozásában kizárólag a kibervédelmi szegmens lehetőségeivel kapcsolatban lehet némi információt megosztani a nyilvánossággal, az MI nyújtotta további lehetőségekről a fejlesztők kormányzati szervek részére célzottan nyújtanak tájékoztatást, így mi sem mélyedünk el jobban a témakörben.

3. A TÁRSADALOM, MINT AZ INFORMÁCIÓSZERZÉS RÉSZESE ÉS FORMÁLÓ TÉNYEZŐJE

Napjainkra általánosnak tekinthető, hogy a társadalom tagjai a kibertér biztosította nyílt, széles körben elérhető forrásai felé fordulnak a biztonságukat érintő információk miatt. Ennek okai között különösen a közösségi felületek nyújtotta lehetőségek keresendők, hiszen annak felhasználói nem csak az információk fogyasztói, hanem létrehozói is lehetnek. Az új információk és a közösség véleményének, tapasztalatának megismerésére főként a kritikus helyzetekben (pl. konfliktusok, járványok, katasztrófák) kerül előtérbe. Ezekben az időszakokban, hirtelen jelentős igény merül fel akár az egyének, akár a társadalmi és állami szervezetek oldaláról a pontos és hiteles információk iránt. Felületként elsődlegesen a közösségi média különböző formái emelhetők ki, megteremtve az infokommunikációs teret az információk gyors megosztásának lehetőségére. A biztonság szolgálatába állítható, tömegesen elérhető, nyílt információk mennyisége azonban számos problémát is felvet.

A tíz éve kirobbant Snowden-botrány világította rá a figyelmet a kibertéri adatgyűjtési és elemzési technikák szerepére, vagy akár a magánszférát érintő elektronikus információs platformok szabályozásának kérdéseire is. Ettől eltérő utat járt be a közösségi médiafelületeken nyíltan elérhető adatok tömeges felhasználásának lehetősége, hiszen az első körben érzékenynek nem tartott adatok (akár metaadatok) tömeges méretekben korábban nem látott összefüggések feltárást teszik lehetővé (lásd. Cambridge Analytica) bortány. Az évtized így a Big Data és a felértékelő OSINT (Open Source Intelligence) még szorosabb összefonódásának az időszaka volt, ahol az azokat alkalmazó ágazatoktól függetlenül egyre fontosabb szerepet kaptak a nyíltan elérhető, adatbázisokká formálódó adatok, számos területen már a mesterséges intelligencia különböző alkalmazásait is felhasználva. A tömeges és nyíltan elérhető adatokban rejlő lehetőségek kiaknázására így szinte minden szereplő lépéseket tett, és az őket érintő irányokban (pl. gazdasági, banki, biztonsági) azokat többek között az előrejelzés céljával alkalmazni.

3.1. Crowdsourcing intelligence

Ami a nemzetbiztonsági megközelítést jelenti, az „előrejelzés" lehetséges víziója a szervezetek rendeltetéséből fakad, amely igénynek a különböző adatszerző és értékelő módszerek kombinációjával igyekeznek eleget tenni. Általánosságban megfogalmazható, hogy feladataik során jelentős mennyiségű adatot kezelhetnek, a zárt adathalmazoktól kezdve egészen a nyíltan elérhető adatok köréig.[97] Speciális módszereik mellett, értelemszerűen nem hagyhatják figyelmen kívül azon nyíltan elérhető adatokat, amelyek már nem az OSINT célirányos megoldásait, hanem az automatizálás irányába mutató, tömeges jellegű feldolgozást és annak új módszereit igénylik. Ebben a tekintetben jelenthet vizsgálatra érdemes példát a Crowdsourcing Intelligence, amely társadalmi közösségeket, egyéneket bevonva ötvözheti a kibertérben, egyéni kommunikációs eszközökkel végzett biztonsági célzatú információgyűjtést.

Országoktól függetlenül a nemzetbiztonsági szereplők sajátossága, hogy információs igényeiket zártan kezelik és csak ritkán osztják meg a nyilvánossággal. Nem hagyhatják ugyanakkor figyelmen kívül, hogy bizonyos, a társadalom széles körét érintő események kapcsán nyílt információs igénnyel fordulnak a társadalom tagjaihoz, segítségüket, részvételüket kérve adott nyílt forrásban elérhető információk megszerzésében. Az általánosan alkalmazott humán és technikai típusú főbb információgyűjtési ágak, így a HUMINT (Human Intelligence), SIGINT (Signal Intelligence), vagy akár az OSINT (Open Source Intelligence) mellett így sajátos elemként figyelhetünk fel a társadalom egyéb területeiről már ismert crowdsourcing módszerének a biztonsági információs igények szolgálatába állítására.

A Crowdsourcing jelensége alapvetően bizonyos részmunkafolyamatok humánerőforrásoknak elosztásos módon történő kiszervezését jelenti, amelyet az online tér globális szintű lehetőségei rendkívüli mértékben felgyorsítottak.[98] A témával mélyebben foglalkozó szakirodalmak fogalmát Jeff Howe nevéhez kötik, aki 2006-ban megjelent cikkében[99] használta üzleti szemléletű megközelítéssel. Az együttműködésen alapuló, elosztott jellegű „munkavégzés" napjainkra már életünk számos tevékenységét átszövi, jelen van többek között a technológiai-infokommunikációs globális nagyvállalati szereplőknél (pl. Facebook, Twitter, Amazon, Apple), de ide sorolható az egyéni hozzájáruláson alapuló, mégis közös produktumot létrehozó, a kollektív tudást szimbolizáló globális Wikipédia példája. Mint egyfajta munkamódszer elterjedten alkalmazzák például a nagy adathalmazokkal dolgozó gazdasági környezetben, ahol bizonyos részadatok feldolgozását már a világ másik felén végeznek. Ebben a vonatkozásban az egyén, mint a tömeg tagja lényegében egy részfeladatot hajt végre, és legtöbbször nem is látja az összképet, a munkája hasznosulásának későbbi eredményeit. A crowdsourcing jelensége nem ismeretlen a tömeg formáló erejéhez kapcsolódó „nyílt

---

97 GRADECKI, J. – CURRY, D.: Crowd-Sourced Intelligence Agency: Prototyping counterveillance. *Big Data & Society*, 2017/1. 2. o. (https://doi.org/10.1177/2053951717693259)

98 STOTTLEMYRE, Steven A.: HUMINT, OSINT, or Something New? *Defining Crowdsourced Intelligence, International Journal of Intelligence and CounterIntelligence*, 2015/3.

99 HOWE, Jeff: *The Rise of Crowdsourcing*. Wired, 2006. 06. 01. (https://www.wired.com/2006/06/crowds/)

forráskódú kormányzás" filozófiája esetében sem, felvetve, hogy a polgárok közvetlenebb módon járulhassanak hozzá a politika alakításához.[100]

Meghatározása kapcsán is több megközelítéssel találkozhatunk a szakirodalmakban, ahol napjaink viszonyaira vonatkoztatva az online tér és az online közösségek elosztott problémamegoldó képességét[101] láthatjuk, amely a közösségek kollektív erejét (akár információgyűjtő, elemző képességét) használja fel, egy meghatározott cél mentén. Mindez arra épít, hogy a széles tömegeket (lényegében elosztott, erőforrásokat) vonjon be az információ megszerzésébe, esetleg annak rendszerezésébe. A nemzetbiztonsági jellegű információgyűjtési terminológiában a crowdsourcing intelligence akár közel is állhatna a HUMINT, illetve az OSINT gondolatiságához, hiszen a humán elem és a nyílt információs jelleg dominál[102], azonban a Crowdsourcing Intelligence során a csoportos tudás és képesség válik meghatározóvá. Szerepe alapvetően az információgyűjtés szakaszához kapcsolódik, amely összefügg azzal, hogy napjainkban maga az adat tekinthető valós erőforrásnak, értéknek, amely első lépéseként annak gyűjtése, majd feldolgozása jelenik meg. Igaz a nagy tömegű adatok feldolgozásánál szintén találunk példát a tevékenység „kiszervezésére", emberi erőforrások közötti „szétosztására", biztosítva, hogy az akár nagytömegben megjelenő adatok adott időtartam alatt megosztott módon feldolgozásra kerülhessenek.[103]

Számos tanulmány foglalkozik a crowdsourcing nemzetbiztonsági vonatkozásával is, jelezve hogy a kibertér és online környezet a nemzetbiztonsági számára is fontos színtérré váltak. Jennifer Yang Hui tanulmányában esettanulmányokkal támasztja alá, hogy a crowdsourcing elveit széles körben használják a nemzetbiztonsági és biztonsági szervezetek tevékenysége során.[104] Magára a módszerre sajátos történeti példaként említhető, hogy a délszláv háború során rádióamatőrök figyelték a NATO, országba berepülő gépeit és továbbították begyűjtött adataikat. Mindez azonban még kívül esett az internet széles körben elterjedt és egyéni mobilkommunikációs eszközökkel rendelkező világán, és csak szűk, megfelelő technikai szakértelemmel és eszközökkel rendelkezők tudtak abban részt venni. Az internet világa fentieket meghaladva napjainkban már lehetővé teszi, hogy egyéni mobilkommunikációs eszközeivel bárki részese lehessen adott információk megszerzésének, továbbításának, becsatornázásának. Mindez azonban csak kellő számú és együttműködő „humánerőforrás" bevonásával lehet hatékony, ahol a résztvevők egy nyíltan megfogalmazott, és általuk is elfogadott cél érdekében vesznek részt a folyamatban.

Nemzetközi példák jelzik, hogy a crowdsourcing módszerének fontos helye és lehetőségei vannak adott, a társadalom biztonságát érintő események kezelésében. Habár ezen példák

---

[100] BOTT, Maja – GIGLER, Björn-Sören –YOUNG, Gregor: *The Role of Crowdsourcing for Better Governance in Fragile State Contexts*. International Bank for Reconstruction and Development, 2014. 3. o. (www.worldbank.org)

[101] BRABHAM, Daren C.: *Crowdsourcing*. Cambridge, MIT Press, 2013. 19. o.

[102] STOTTLEMYRE: i. m. 582. o.

[103] BOUCHART, Marianne: *Crowdsourcing Data at the Guardian Datablog*. (https://datajournalism.com/read/handbook/one/getting-data/crowdsourcing-data-at-the-guardian-datablog

[104] YANG HUI, Jennifer: *Crowdsourcing for National Security*. Policy Report, March 2015, Nanyang Technological University, S. Rajaratnam School of International Studies, 2015. (http://www.jstor.com/stable/resrep05853)

rendkívül sokrétűek, jelen tanulmány a biztonsági kérdéskörre fókuszáló két jelentős irányt különít el:

- Az adott ország és a társadalom tagjainak biztonságát befolyásoló kritikus események (pl. természeti vagy humanitárius krízishelyzet, fegyveres konfliktus, háború) kapcsán az egyének megszólítása, a válságkezeléshez, segítségnyújtáshoz, koordinációhoz, döntésekhez szükséges információk megismerése.
- A bűnüldözési hatóságok, kormányzati szervek munkájának támogatása digitális bizonyítékok átadásával. Ide sorolható például egy-egy lokális biztonsági incidens, vagy akár nagyobb fegyveres konfliktus, háború során az események utólagos feltárását segítő digitális bizonyítékok hatóságoknak történő átadása.

A crowdsourcing intelligence egyedülálló jelentősége így abból adódik, hogy az online tér sajátosságait előnyként kiaknázva:

- bevonja az információs környezet szereplőit;
- ehhez olyan felületeket használ, amelyekkel elérheti a résztvevőket (így ezek többnyire nyílt felületek);
- lehetővé teszi a legkülönbözőbb formában történő információk gyűjtését (pl. kép, videó).

További sajátossága, hogy a széles közönség számára már maga az „információs" igény is nyíltan jelenik meg, a társadalom tagjainak széles bevonását előmozdítva, akár felhívásban, akár erre a célra létrehozott weboldalak alkalmazásában.[105] Megjelenése ugyanakkor nem platformfüggő, így habár legismertebben a közösségi média felületeknél kereshetjük, a témakörben megjelenő webalkalmazások, felületek, mobilalkalmazások jelzik, hogy a módszer számos területen hatékonyan alkalmazható. Gyakran ezen megoldások csak technikai kereteket biztosítanak egy-egy crowdsourcing project végrehajtásának (pl. adott természeti katasztrófa során történő viszonyok pontosabb megismerése), és elválik egymástól a crowdsourcing technológiai környezetét, platformjait, módszereit koncentráló, fenntartó környezet és a tevékenység rendeltetésének célja.

További tipizálás lehet az eseménycentrikusság, illetve geocentrikusság.[106] Míg az első esetben például egy időben (és akár térben) behatárolható biztonsági esemény kapcsán kerül előtérbe a corwdsourcing intelligence jelentősége, addig a második esetben a földrajzi szempont (pl. egy adott területen bekövetkező természeti és humanitárius katasztrófa, vagy akár katonai konfliktus) válik meghatározóvá.

3.2. Az elmúlt időszak példái

A crowdsourcing biztonsági eseményekhez kapcsolódó alkalmazására számos példát láthatunk a nemzetközi forrásokban. Ezek között megjelennek a társadalom biztonságát befolyásoló

[105] Lásd: https://warcrimes.gov.ua/

[106] Erickson tanulmányában ennek 4 típusát különbözteti meg, így a 1. Global (any time, any place) Crowdsourcing, 2. Event-centric Crowdsourcing, 3. Audience-centric Crowdsourcing és a 4. Geocentric Crowdsourcingot. Lásd: ERICKSON, T.: *Geocentric Crowdsourcing and Smarter Cities: Enabling Urban Intelligence in Cities and Regions. Position paper.* 1st Ubiquitous Crowdsourcing Workshop, UbiComp, 2010.

jelentősebb természeti és humanitárius krízishelyzetek, vagy akár fegyveres konfliktusok, és a rendvédelmi szervek munkájának sajátos támogatása. A crowdsourcing módszerével történő adatgyűjtés során fontos cél, hogy pontos, aktuális képet kapjunk egy adott eseményben érintettek segítsék az egyes információk mozaikszerű biztosításával egy teljesebb kép összeállítását.

- Átfogó, a crowdsourcing közösségi gondolkodást elősegítő megoldásokat láthatunk[107] például erőtüzek jelzésére, erőforrások nyomon követésére, szavazásra, adatok térképi vizualizációjára. A jelzett forrásban említett egyik megoldást például a WFP (World Food Programme) használta eredményesen Szomáliában az élelmiszerellátással és hozzáféréssel kapcsolatos információgyűjtési feladatokra.[108]
- A lakosság segítségének kérése, pl. az elkövetők beazonosításában nem új keletű egy-egy bűncselekmény, illetve biztonságot érintő ügy kapcsán. A közösségi oldalakon azonnal megjelenő fényképek, fotók és egyéb adatok, valamint az általánosnak tekinthető kamerás eszközök légkörében mindez azonban másfajta értelmezést nyer. A résztvevők könnyen válhatnak önjelölt nyomozókká és akár egymást tévesen erősítő összefüggések feltárására és megosztására vállalkozhatnak.[109] A 2013-as bostoni Marathon futóversenyen történt robbantásnak, a közösségi média szerepének és a crowdsourcing jelenségének összefüggéseit is már több tanulmány vizsgálta.[110] Az esemény mintegy fordulópontként is értelmezhető a crowdsourcing biztonsági megjelenésére, igaz a maga hibáival, ellenmondásaival. Így például a robbantásokat követően a Reddit és 4Chan közösségi felületeken szerveződő csoportok, rendkívül gyorsan bekapcsolódtak a lehetséges elkövetők felkutatásába, és a hivatalos nyomozás mellett az online térben kialakuló „nyomozói közösség" (amelyet gyakran cyber-vigilante-nak vagy „digilantesnek" is neveznek), segítette a nyomozó hatóságok munkáját.[111] Amíg az FBI a digitális információk átadásában kérte a segítséget, addig – mint Wadhwa írásában megfogalmazza – „két nagyon eltérő folyamat zajlott le […] a tömeges forrásból származó információgyűjtés – hatalmas siker – és a tömeges forrásból származó bűnüldözés – végtelen kudarc."[112] Mindez lényegében azt

[107] Lásd: Innovative Support to Emergencies Diseases and Disasters (InSTEDD): *Tool Directory – Our complete platform of tools.* (https://instedd.org/tool-directory/)

[108] InSTEDD: *Food Security Surveys with Refugees*. (https://instedd.org/project/food-security-surveys-with-refugees/)

[109] McCullagh, Declan: *FBI seeks crowdsourcing help in Boston bombing case: ID these two men!* 2013. 04. 18. (https://www.cnet.com/tech/tech-industry/fbi-seeks-crowdsourcing-help-in-boston-bombing-case-id-these-two-men/)

[110] Nhan, Johnny – Huey, Laura – Broll, Ryan: Digilantism: An Analysis of Crowdsourcing and the Boston Marathon Bombings. *The British Journal of Criminology*, 2017/2. 341-361. o. (https://doi.org/ 10.1093/bjc/azv118); Tapia, Andrea – Lalone, Nicolas: *Crowdsourcing Investigations: Crowd Participation in Identifying the Bomb and Bomber From the Boston Marathon Bombing*. 2019. (https://doi:10.4018/978-1-5225-8362-2.ch072)

[111] Nhan – Huey – Broll: i. m. 341-361. o

[112] Wadhwa, Tarun: *Lessons From Crowdsourcing The Boston Bombing Investigation*. Forbes, 2013. 04. 22. (https://www.forbes.com/sites/tarunwadhwa/2013/04/22/lessons-from-crowdsourcing-the-boston-marathon-bombings-investigation/?sh=361cec8d4424)

jelentette, hogy a rendvédelmi ágazat, az esetleges bizonyítékok körének bővítése érdekében kérte a társadalom tagjainak önkéntes közreműködését (amelyre létre is hoztak egy olyan felületet ahová az emberek feltölthetik digitális adataikat segítve a nyomozást), azonban a csoportok önszerveződése túlterjeszkedve, ártatlanokat is gyanúsnak kiáltott ki.

- Kapcsolódó példaként említhető a 2021. januárban az Egyesült Államokban a Capitoliumnál lezajlott erőszakba fordult megmozdulás is. Az eseményt követően rövid időn belül tömegek mozdultak meg, hogy segítsék a rendfenntartók munkáját a felkelők beazonosításában a közösségi felületekre kiposztolt fényképek és videókon megjelenő személyek beazonosításával, mielőtt még azok lekerültek volna a különböző platformokról.[113]
- A crowdsourcing széles körű biztonsági célú alkalmazására az orosz-ukrán háború is számos példával szolgál, rávilágítva arra, hogy a módszer ilyen mértékben még nem került felhasználásra fegyveres konfliktusban, egyrészről a nyilvánosan elérhető információk digitális bizonyítékként történő gyűjtése, akár közvetlen katonai műveletek támogatása során. Már a háború kezdeti időszakában látható módon felértékelődtek a közösségi média felületei, az okostelefonok felhasználásával készített információk, szöveges üzenetek, képek, videók, elősegítve az orosz erők mozgásának közösségi felületeken való követhetőségét. A témakörben megjelent médiaforrások alapján láthatóvá vált, hogy az ukrán biztonsági szervek is felismerték ennek jelentőségét, így például az Ukrán Biztonsági Szolgálat a STOP Russian War chatbot[114] létrehozásával, az állampolgárok segítségét veszik igénybe az ellenség mozgásának és tevékenységének nyomon követésére, segítve ezzel az ukrán fegyveres szervek tevékenységét.[115] Az ukrán nemzeti rendőrség szintén elindított, egy, a crowdsourcing elveire építő megoldást (Narodnii mesnik / Avanger (Bosszúálló) Bot[116]) elősegítve a lakosságtól érkező jelzések fogadását.[117] Ukrajna, Digitális Transzformációs Minisztériuma pedig az eVorogot (e-enemy) Telegram chatbotot[118] indította el az orosz katonai tevékenységek észlelésére és jelzésére. Ehhez azonban az információt küldő beazonosítása feltételként jelenik meg, amelyhez a Diia elnevezésű digitális ügyintézést biztosító állami szolgáltatás ad megoldást.
- A crowdsourcing ukrajnai biztonsági megjelenésére az "Russia Will Pay" (Oroszország fizetni fog) online projekt[119] is kiemelhető, amely már a háborús károk dokumentálására és későbbi nemzetközi eljárásokra és orosz kártérítésekre felkészülve a károk képi és szöveges dokumentálására irányul. A program a Kijevi Közgazdasági Főiskola (Kyiv

[113] ZEGART, A.: *Spies Like Us: The Promise and Peril of Crowdsourced Intelligence*. Foreign Affairs, 2021. 168. o.
[114] Lásd: https://t.me/stop_russian_war_bot.
[115] KOSTENKO, Aleksei and AFP: *Smartphones, crowdsourcing play crucial role in defence of Ukraine.* 2022. 03. 24. (https://central.asia-news.com/en_GB/articles/cnmi_ca/features/2022/03/24/feature-03)
[116] Lásd: https://t.me/ukraine_avanger_bot.
[117] KOSTENKO: i. m.
[118] Lásd: https://t.me/evorog_bot
[119] Lásd: https://damaged.in.ua/

School of Economics (KSE Institute)), az ukrán Elnöki Hivatal, illetve több ukrán minisztérium közös projektjeként jött létre. Weboldaluk[120] alapján a projekt fő célja, az ország infrastruktúrájában okozott anyagi károk dokumentálása, ellenőrzése, elemzése és becslése, és a lehető legrészletesebb bizonyíthatósága (képekkel, videókkal, lehetséges tanúkkal). A KSE Institute oldalán szereplő közzététel szerint garantálják az adatközlők személyének bizalmasságát. A projekt keretében egy kárnyilvántartás és az anyagi károk összesített adatbázisát hozzák létre, mint megfogalmazzák: *„Az összegyűjtött adatokat és a kárfelmérést az alábbi célokra használják fel:*
1) a háborús bűnök és az emberi jogok megsértésének dokumentálása;
2) az Orosz Föderációval szembeni követelések előterjesztése a nemzetközi bíróságokon az okozott kár megtérítésére: a nemzetközi bíróságok számára benyújtott perekhez összesített bizonyítékra és a sérült tárgyak nyilvántartására van szükség a becslés módszertanának megfelelően;
3) egyéni kártérítésre;
4) háborús jóvátételt és kártérítést kapni az agresszortól Ukrajna újjáépítése érdekében."[121]
A biztonsági szervek által létrehozott oldalak, botok használatát széles körben hirdették, számítva a civil lakosság minél szélesebb csatlakozására. Alkalmazhatóságuk mögött egyértelműen megjelenik a közös cél, a társadalom közös biztonsági érdek mentén történő megszólíthatósága, valamint a társadalom szintjén már meglévő állami szintű digitalizációs megoldások (e-ügyintézés megoldásai). Létrehozásukba bekapcsolódnak a külső infokommunikációs fejlesztői környezet, valamint a tudományos oldal érintett szereplői.

A crowdsourcing biztonsági célú alkalmazásait tekintve, azonban nem csak információgyűjtési területen van jelen, hanem a humán források szakértői jellegű, már meglévő információk feldolgozásába történő bevonására is láthatunk példákat.

- Ide sorolható a Malaysia Airlines Kuala Lumpurból Pekingbe tartó, 2014-ben eltűnt MH370 járatának[122] megtalálása tett erőfeszítés, amely során a műholdképek áttekintésébe emberek milliói kapcsolódhattak be. A műholdüzemeltető által vezetett crowdsourcing projekt talán a legnagyobb közösségi projekt volt, ahol a résztvevők "több millió lehetséges nyomot jelöltek meg" a több mint 1 millió négyzetkilométernyi nagy felbontású műholdfelvételeken.[123] Összességében a nyíltan megfogalmazott közös cél, a szükséges részinformációk nyílt formátumban történő biztosítása látható, az önkéntesség szerepének felértékelődése, valamint a kereskedelmi műholdcég szerepe

[120] Lásd: https://kse.ua/russia-will-pay/
[121] Kyiv School of Economics (KSE): *Russia Will Pay*. https://kse.ua/russia-will-pay/
[122] Three million people join crowdsourcing satellite hunt for missing Malaysia Airlines jet, (AFP), 18. Mar, 2014, South China Morning Post
[123] ArborCarbon: *What is Tomnod?* 2016. 03. 27. https://arborcarbon.com.au/what-is-tomnod/index.html

látható a folyamatban (a DigitalGlobe hozta létre a Tomnod[124] nevű platformot a crowdsourcing számára).

– Ebbe az alkalmazási irányba sorolható az USA rendvédelmi szervei által létrehozott „Texas Virtual Border Watch" határbiztonsághoz köthető megoldás, amely az USA-mexikói határon, kormányzati webalapú megfigyelésből álló kamerákat használva vonja be az internettel rendelkező felhasználó kapcsolatok, akik a videókat nézve jelenthetnek minden olyan bűncselekményt, mint a kábítószer, az csempészetet és az illegális bevándorlást érinti.[125] Ide sorolható az Egyesült Államok Belbiztonsági Minisztériuma által létrehozott Neighborhood Network-t is, ösztönözve a gyanús esetek jelentését.[126]

A crowdsourcing nemzetbiztonsági célú alkalmazásának kutatására is ismertetnek nemzetközi példákat a témakörrel foglalkozó egyes szakirodalmak.[127] Ezek alapvetően a biztonságot fenyegető veszélyek „előrejelzési" lehetőségének kutatásához kapcsolódnak. Ilyen példaként említhető az IARPA (Egyesült Államok kormányának Intelligence Advanced Research Projects Activity nevű szervezete) által finanszírozott, egy évtizede elindított, a George Mason Egyetem SciCast projektje, amely a felhasználók csoportszintű kollektív bölcsességére építve, a nemzetbiztonsági vonatkozású jövőbeli események előrejelzésének lehetőségét kutatta.[128] Mint a témával foglalkozó cikk kifejti a kutatás során a résztvevők szakértelmüket, ismereteik birtokában online előrejelzésként adott jövőbeli eseményekre, bekövetkezésükre fogadhattak.[129] Érdekesség említhető, a szakirodalmakban széles körben ismertetett DARPA Red Balloon Challenge projektje is, ahol léggömbök helyének megállapításában a győztes csapat a közösségi média segítségét használta fel, vagy akár a britt GCHQ 2011-es toborzási kampánya, ahol szintén a közösségi médiát használva egy kód feltörése után juthattak el az érdeklődők a toborzási oldalra.[130]

3.3. A crowdsourcing előnyei és hátrányai

A crowdsourcing alkalmazhatóságának biztonsági/nemzetbiztonsági szempontrendszerhez illesztett előnyei és hátrányai rendkívül összetett képet mutatnak. A módszer során lényegében a zárt (nemzet)biztonsági gondolkodás és a társadalom nyitottsága találkozik. Értelemszerűen

---

[124] Uo.

[125] TEWKSBURY, Doug: Crowdsourcing Homeland Security: The Texas Virtual BorderWatch and Participatory Citizenship. *Surveillance & Society*. 2012/3-4. 249-262. o.

[126] SHIFFMAN, Gary M. – GUPTA, Ravi: Crowdsourcing cyber security: a property rights view of exclusion and theft on the information commons. *International Journal of the Commons*, 2013/1. 106. o.

[127] QUINTO, Joyce Anne – LIM, Aldo Gavril: Toward developing a humanitarian crowdsourcing model: Enabling medical and disaster response through digital collaboration. *Climate, Disaster and Development Journal*, 2016/1. (https://doi.org/10.18783/cddj.v002.i01.a01) GRADECKI – CURRY: i. m.

[128] A https://scicast.org/ weboldal alapján a kutatás finanszírozása befejeződött, a honlap jelenleg passzív

[129] TUCKER, Patrick: *This Is How America's Spies Could Find the Next National Security Threat – A recent breakthrough in online prediction markets promises a better glimpse of the future – paid for by U.S. intelligence.* Defense One, 2014. 02. 20. (https://www.defenseone.com/technology/2014/02/long-overdue-return-crowdsourced-intelligence/79094/)

[130] YANG HUI: i. m.

a nemzetbiztonság szereplői adott nemzeti érdekek, az irányítás szintjéről érkező feladatok mentén végzik tevékenységüket, amelyek alapvetően nem nyilvánosak. Mivel a crowdsourcing intelligence során az információs igények megfogalmazása lényegében nyíltan kell, hogy történjen, azokban az esetekben ahol a biztonság és a hatékonyság érdekében a titkosság fenntartása alapvető szempont, értelemszerűen a crowdsourcing intelligence nem megfelelő forma az információk megismerésére.[131] Más oldalról tekintve ugyanakkor a crowdsourcing nemzetbiztonság megjelenése a „zárt" biztonsági intézményi rendszer és a társadalom közötti egyfajta összekötőelemként is szerepet kaphat.[132] A crowdsourcing előnyeit tekintve, a válságkezelésben történő alkalmazása kapcsán Halder[133] több általánosnak tekinthető előnyt is megfogalmaz, így a reakció idő csökkenése, az információk pontosságának növekedése, illetve egyéb gazdasági, társadalmi és humán előnyök. Más szerzők az alkalmazás előnyei között a tömeg erejében rejlő lehetőségeket, így a munkaerő, a szakértelem és az innováció kihasználását emelik ki.[134]

A pozitívumok mellett azonban sajátos, az alkalmazással szembeni fenntartás is felmerülhet. Ilyen a résztvevők személyes adatai biztonságának, felhasználásának kérdése, amelyet a résztvevők érthető módon titkolni, védeni szeretnének. Az adatgyűjtő megoldásokkal szembeni fenntartások további oka között említhető az is, hogy az akár tömeges jellegű adathalmazokra számos irányból jelentkezhet érdeklődés. Akár a média, akár az üzleti élet szereplői, akár a biztonsági szervek számára értéket képviselhetnek. Közvetve tehát az információk tömeges jellege és aktualitása révén ezen felületek (és a mögöttük álló adatközlők) aktív részeseivé válhatnak egy szélesebb folyamatnak, ahol azonban felmerülhet a névtelenség megtartásának igénye, adataik védelme, biztonságuk garantálása.

Így talán az egyik legfontosabb kérdés, hogy ebben az információgyűjtési módszerben maradhat-e a „tömegben" lévő egyén névtelen, és a végcélhoz a névtelen tömeg részeként „csak" részfeladatok megoldásával, részinformációkkal járul hozzá. Gondoljunk egyik oldalról arra az esetre, amikor egy útvonaltervező megoldás során hozzájárulunk a forgalom mértékének meghatározásához, míg a másik oldalról akár veszélyhelyzetre történő felhívás, vagy akár digitális bizonyítékok hitelessége miatt szükség lehet a névtelenség későbbi korlátozott feloldásának kezdeményezésére. Mindezek közvetlenül is befolyásolhatják a részvételi hajlandóságot, gondolva a személyi adatok védelmének szempontjára, akár a részvevők fizikai biztonságának kérdésére is. Ennek példájaként említhetőek akár a covid-követő applikációk, amely alkalmazásával szemben erős visszatartó erő volt a személyes adatok

---

131 GUPTA, Ravi – BROOKS, Hugh: *Using Social Media for Global Security*. Indianapolis, John Wiley & Sons, Inc., 2013. 27. o.

132 CHIRU, Irena: Engaging Public Support and Awareness in Intelligence: The Demands and Challenges to Developing an Intelligence Culture. *International Journal of Intelligence and CounterIntelligence*, 2016/3. 503-514. o. (https://doi.org/10.1080/08850607.2016.1148484)

133 HALDER, Buddhadeb: *Crowdsourcing collection of data for crisis governance in the post-2015 world: potential offers and crucial challenges*. Proceedings of the 8th International Conference on Theory and Practice of Electronic Governance (ICEGOV '14), New York, Association for Computing Machinery, 2014. 1-10. o. (https://doi.org/10.1145/2691195.2691208)

134 YANG HUI: i. m.

sérülésétől való félelem, de ha napjaink orosz-ukrán háborújára gondolunk egyes területeken a közösségi médiafelületek nyílt használata esetében is visszatartó erő lehet. Mivel ezen alkalmazások a világháló globális légkörében működnek, így a felhasználói bizalom és az adatok védelmének garanciája mind az alkalmazás létrehozójával, mind az adatok felhasználójával szemben kiemelt szerepet kell, hogy kapjon. Adott esetben közös, a fejlesztői és kormányzati szervek szoros együttműködését is láthatjuk.

A crowdsourcing során fontos szempont az adatok aktualitása mellett azok pontossága és hitelessége. A tevékenység sajátosságaként mindezek azonban nem tekinthetőek egyértelműnek, jelen lehet a szándékos megtévesztés vagy a vétlen tévedés lehetősége. Bizonyos típusú crowsourcing megoldásoknál ezek hatásait a többi adat akár semlegesítheti, letisztázhatja, alacsonyabb mennyiségű, illetve tömegesen jelentkező téves adatnál azonban mindez pontatlan, téves végeredményekhez vezet. Míg a biztonságért felelős szervek alapesetben a szakértői jellegű adatokból merítenek, addig a széles körű, nyílt forrásokból származó, számos elemében ellenőrizhetetlen adat felhasználása már új gondolkodást igényel.[135] Bizonyos kritikus helyzetekben (pl. orosz-ukrán háború) ezen adatok szerepe ugyanakkor a szakmai fenntartások ellenére is meghatározóvá és fontossá válhat. Jelen lehet továbbá, hogy a tömeg szintjén jelentkező vélemények milyen mértékben lehetnek akár külső hatástól, a tömeg többi résztvevőjének véleményétől befolyásoltak, mennyire objektívek, vagy akár mennyire torzulnak.

3.4. A crowdsourcing jelentősége és jövője

Egyre nyitottabb világunkban a határokon átívelő infokommunikációs és digitális eszközök biztonsági célú felhasználása egyre meghatározóbbá válik. Segítségükkel nem egyszerűen releváns információk kerülhetnek továbbításra egyik helyről egy másikra (pl. médiatudósítások révén), hanem személyes mobil kommunikációs eszközei révén az egyének által létrehozott információk összesített halmaza új helyzetet, a nagy tömegű adathalmazok kezelésének és feldolgozásának igényét is előrevetítette.

A már gyakorlatban is megjelenő alkalmazások és megoldások mellett a jövőben minden bizonnyal még nagyobb szerep juthat a társadalom széles körét érintő biztonsági problémák, így akár a humán és természeti katasztrófák, a válsághelyzetek kezelése, a terrorizmus elleni küzdelem, vagy akár a radikalizáció visszaszorítása terén. A (nemzet)biztonsági kérdések és az azt gyakran fenntartásokkal kezelő társadalom közötti közeledés akár konkrét platformok formájában történő megjelenése főként a kritikus események bekövetkezése során válhat meghatározóvá. Amíg a biztonságért felelős szervek az aktuális és pontos információk érdekében szükségszerűen fordulnak a tömeg („crowd") tagjaihoz, addig a társadalom biztonságban érdekelt tagjai, közreműködésükkel, és az online közösség rendkívül erejével eredményesen járulhatnak hozzá a biztonság növeléséhez.

Látható módon a crowdsourcing intelligence átszövi mindennapjainkat, kiterjedve a biztonság számos humán és technikai jellegű területére. A nemzetbiztonsági jellegű lehetséges alkalmazásokat tekintve mégis számos olyan szempontot kell figyelembe venni, amely sajátossá

[135] YANG HUI: i. m.

tehetik alkalmazásukat. Habár megjelenésükkel akár az OSINT, akár egyéb kutatások mentén számos felületen találkozhatunk, mégis melyek lehetnek azok a szempontok, amelyek a (nemzet)biztonság lehetséges alkalmazási oldaláról felmerülnek.

1) A nemzetbiztonsági megközelítésről általánosságban elmondható, hogy az érintett szervezetek a feladataik során az információk gyors megszerzésében és értékelésében érdekeltek. Jogszabályi lehetőségeik mentén számos információs körből meríthetnek, ezen információforrások azonban nem kizárólag a titkos információgyűjtésre vonatkozhat, hanem kimeríthetetlen forrásként állnak rendelkezésre a nyílt források.
2) A crowdsourcing szükségessé teszi, hogy a társadalom szélesebb körének megszólítása és bevonása olyan nyíltan definiálható igények, feladatok mentén történjen, amelyekkel azonosulni tud, hiszen csatlakozása önkéntes alapon történhet (pl. bizonyítékok gyűjtése). Mindez kritikus eleme egy crowdsourcing folyamatban, biztosítva a határok, keretek és felületeinek kialakítását, akár az eredmények visszacsatolását is (pl. az egyén által adott részeredményekhez mindenki hozzáfér, vagy már csak annak összesített, kumulált végeredményéhez – „a tömeg bölcsessége”).
3) A „végfelhasználó” és az igénymegfogalmazása alapján a crowdsourcing létrehozója tudja lényegében megteremteni azt az időbeli és térbeli keretet (platformot), amely az adott célnak megfelel. Így azt a kiemelt szempontot érvényesíteni, hogy például csak az adott területen lévő, vagy akár „szakértelemmel” rendelkezők kapcsolódjanak be a folyamatba.

4. ZÁRÓGONDOLATOK

Az új technológiák megjelenése összetett társadalmi, technológiai és gazdasági folyamat, amelynek közvetett hatásai a biztonsági, nemzetbiztonsági ágazatot is érintik. Az információgyűjtés technológiai környezetével párhuzamosan módosulnak az információk megszerzésének lehetőségei, módszerei, ugyanakkor változik az információk védelmének külső környezete, az ezirányú fenyegetettség is.

Fontos tehát a külső környezet változásainak figyelemmel kísérése, és a komplex folyamatok minél teljesebb megértése, nemzetbiztonsági szemmel történő értelmezése. Jelen tanulmány is, mintegy bepillantásként az információs környezet általános áttekintését követően, az információgyűjtés különböző területein már látható változásokat, valamint az emberi tényező megváltozó szerepét kívánta a központba helyezni. Mindezek egyfajta evolúciós folyamatként is értelmezhetők, amelyek központi eleme a kibertér, valamint a mesterséges intelligencia berobbanó szerepe.

Az áttekintett témakörökkel, példákkal a változások, különösen a mesterséges intelligencia dinamikus térhódításának meghatározó szerepét, és a hagyományosnak tekinthető hírszerzési ágakra történő hatásait kívántuk bemutatni. Különösen a tömeges adatok, a nyílt adatforrások, vagy akár az internetes közösségi felületek esetében válik láthatóvá ez a változás. A mesterséges intelligencia által támogatott rendszermegoldásoknál nehéz megfogalmazni, hogy a fejlődés milyen ütemmel folytatódik majd, hogy hogyan alakítja át

mindennapjainkat. Még a hosszabb ideje meglévő technológiák esetében is nehéz prognózist adni a következő 5-10 évre, hiszen alkalmazásukat az új megoldások gyorsan a háttérbe szoríthatják. További fontos kérdéseket vethet fel a nagytömegben már rendelkezésre álló információk még hatékonyabb, automatikusabb feldolgozásának lehetősége, és a nemzetbiztonsági ágazat szempontjából fontos előrejelzések megalkotásának lehetősége, a magasabb szinteken történő döntések meghozatalának információkkal, elemzett anyagokkal történő támogatása.

A technológia fejlődési ütemének bizonytalansága mellett az egyes kormányoknak még inkább nagy felelőssége van az MI fejlődésének megértésében, a biztonsági szempontokat is figyelembe vevő, azonban előremutató alkalmazási környezetének kialakításában. Ennek a mértékének a meghatározása közel sem könnyű feladat. A kormányzat feladata kell, hogy legyen az egyes államok által követendő MI stratégiák megalkotása, időszakos revíziója és az alapdokumentumokban megfogalmazott célok eléréséhez szükséges gazdasági-társadalmi környezet kialakítása. Ugyanakkor fontos kiemelni, hogy az országoknak nemcsak a gazdasági, hanem társadalmi felkészültségétől is függ az, hogy milyen mértékben tudja az MI támogatott rendszereket alkalmazni. Az mindenképp elmondható, hogy a következő években fel fog értékelődni az MI alkalmazásához, fejlesztéséhez szükséges szaktudás, valamint szakértelem, és a technológiailag fejlettebb, innovációösztönző, a K+F-re nagyobb hangsúlyt fektető országok gazdasági előnyökre tudják váltani a meglévő tudáspotenciált.

Azon országok, ahol a technikai eszközpark fejlesztésére kevesebb forrást tudnak elkülöníteni, a felzárkózást a szakértő állomány kinevelése jelentheti, amely csökkentheti a technológiai lemaradás mértékét. A fenti változások nem kerülik el a nemzetbiztonsági ágazatot sem, ahol az MI a technikai területek mellett hatással lehet bizonyos humán területekre, illetve módosulhat a közöttük meglévő kapcsolat. A változások nemcsak a technológia alkalmazására és a fejlesztési irányvonalak meghatározására korlátozódnak majd. A nemzetbiztonsági feladatrendszerbe tartozik a társadalomban jelentkező fenyegetésekre a válaszok megadása, továbbá kormányzati célok támogatása. Mindez szükségszerűen magával vonja az információszerző és információfeldolgozó képesség fejlesztését is. Az adatok megszerzésére és elemzésére MI-val támogatott képességeket kell rendszerbe állítani, hiszen az adatszerzés összetettsége és az adathalmazok nagysága új kihívások elé állítja az információfeldolgozó területeket is.


UNIVERSITY OF PUBLIC SERVICE
LUDOVIKA

Military and Intelligence CyberSecurity Research Paper 2023/3.

Szerző(k) / Author(s):
Dr. Dobák Imre PhD – Dr. Kenedli Tamás PhD

Kézirat lezárásának ideje / Manuscript closing time:
2023.08.15.

Szerkesztők / Editors:
Dr. Farkas Ádám PhD
Dr. Magyar Sánor PhD

Kiadó / Publisher:
Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar
Nemzetbiztonsági Intézet Katonai Nemzetbiztonsági Tanszék
University of Public Service (Hungary), Faculty of Military Sciences and Officer Training, National Security Institute Department of Military National Security

Kiadó képviselője / Representative of the publisher:
Dr. Magyar Sándor PhD

Elérhetőségek /Contacts:
https://nbi.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/researchpaper

farkas.adam@uni-nke.hu | magyar.sandor@uni-nke.hu

1011 Budapest, Hungária krt. 9-11. /9-11. Hungária Blvd., Budapest, H1011

ISSN:
2786-3778

A borító https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security címen elérhető ingyenes háttérkép felhasználásával 2021. február 25-én készült.

The cover was created on 25. February 2021, using a free wallpaper available at https://www.stockvault.net/photo/270507/cyber-security-web-security-network-security.