KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT

XX. évfolyam **1. szám**

FELDERÍTŐ SZEMLE

ALAPÍTVA: 2002

BUDAPEST
2021

A Katonai Nemzetbiztonsági Szolgálat
tudományos-szakmai folyóirata

Felelős kiadó

Dr. Béres János altábornagy, főigazgató

HU ISSN 1588-242X

TARTALOM

KUTATÁS – FEJLESZTÉS

SZAKMATÖRTÉNET

FÓRUM

AZ OLVASÓHOZ

POMOGÁCS PÉTER

A „KIS KÉK EMBEREK”[1] – A KÍNAI NÉPKÖZTÁRSASÁG TENGERI MILÍCIÁJÁNAK TEVÉKENYSÉGE A KELET-KÍNAI- ÉS A DÉL-KÍNAI-TENGEREN

Bevezetés

2009. március 8-án öt kínai hajó kerítette be az Amerikai Egyesült Államok *Impeccable* nevű kutatóhajóját a Dél-kínai-tengeren. Az *Impeccable* fegyvertelen, polgári legénység által működtetett hajó, amely az amerikai haditengerészet Katonai Szállítási Parancsnokságának állományába[2] tartozik. A hajó az incidens időpontjában a Hainan-szigetektől 120 kilométerre délre végzett méréseket, nem messze a kínai Yulin nevű tengeralattjáró-bázistól. A kínai haditengerészet már napokkal korábban figyelmeztette az amerikai egységet, hogy fejezze be tevékenységét és távozzon a térségből, így akár nem is lett volna meglepő, ha hadihajók segítségével igyekeznek távozásra kényszeríteni a kutatóhajót. Őrnaszádok vagy rombolók helyett azonban közönséges halászhajók közelítették meg az amerikai hajót, és egyből az általa víz alatt vontatott szonárberendezésnek igyekeztek nekiütközni hajóikkal. Amikor ez nem sikerült, a halászok fémrudakkal és csáklyákkal próbáltak kárt okozni a mérőeszközben, amíg az *Impeccable* legénysége egy nagy nyomású víztömlőt nem vetett be ellenük. Ezután a kínai hajósok fadarabokat szórtak az amerikai hajó útjába, végül az egyik halászhajó mindössze méterekre közelítette meg, mielőtt az visszavonult volna. Mindezt beavatkozás nélkül kísérte figyelemmel a kínai haditengerészet egy nagyobb hadihajója, nagyjából 100 méter távolságból.[3]

Az incidens csak egy példája volt annak a Dél-kínai-tengeren rendszeresen megismétlődő jelenetnek, miszerint kínai „halászhajók” zaklatnak és üldöznek el más államok lobogója alatt közlekedő polgári hajókat, a Kína saját állítása szerint az érdekeltségébe tartozó vizekről. Ezek a halászhajók és legénységük a kínai Népi Fegyveres Erők Tengeri Milíciájához tartoznak, amelynek létrehozása a kommunista Kína megalapításáig nyúlik vissza.

---

[1] A kifejezést Andrew S. Erickson alkotta a Krím félszigetet megszálló orosz „kis zöld emberek” kifejezésének mintájára.
CAVAS, Christopher P.: China’s 'Little Blue Men' Take Navy’s Place in Disputes. Defense News, 2015.11.02.
https://www.defensenews.com/naval/2015/11/03/chinas-little-blue-men-take-navys-place-in-disputes/; letöltés: 2020.10.25.

[2] United States Navy Military Sealift Command.

[3] GREEN, Michael – HICKS, Kathleen – COOPER, Zack – SCHAUS, John – DOUGLAS, Jake: Counter-Coercion Series: Harassment of the USNS Impeccable. Asia Maritime Transparency Initiative, 2017.05.09.
https://amti.csis.org/counter-co-harassment-usns-impeccable/; letöltés: 2020.11.15.

A Tengeri Milícia létrehozása

A kínai polgárháborút és a Kínai Népköztársaság 1949-es megalapítását követően a Kínai Kommunista Pártnak biztosítania kellett a kontinentális Kína partvonalát, hogy az elmenekült nacionalista erők ne kísérelhessék meg a visszatérést Tajvanról, valamint ne folytathassanak felforgató tevékenységet az ország partjainál. Az erőfölényben lévő nacionalista hadihajók partközeli vizekre történő behatolásának megakadályozása komoly kihívást támasztott a pekingi pártvezetéssel szemben, mivel a kommunista erők abban az időben még csekély haditengerészeti képességekkel rendelkeztek. Pekingnek rövid idő alatt megoldást kellett találnia arra, hogy hogyan vonhatja ellenőrzése alá legalább a partközeli vizeit. A szükség hozta tehát úgy, hogy a fegyveres erők által rekvirált közönséges halászhajókból és halászokból verbuvált milíciát hoztak létre.[4]

A Tengeri Milícia létrehozásának első lépéseként a halászatot a kollektív gazdálkodás keretein belül úgy szervezték újra, hogy a korábbi halászfalvakból munkaközösségeket hoztak létre, amelyeknek a központilag meghatározott vizeken kellett halászniuk, és szintén előre meghatározott mennyiségű halat kellett kifogniuk. A milícia félkatonai jellege azonban már a kezdetektől megmutatkozott, ugyanis létrehozásában részt vettek a kínai Népi Felszabadító Hadsereg Haditengerészetének tisztjei. Így a korábban csak civil tevékenységet végző halászokat politikai oktatás mellett katonai alapkiképzésben is részesítették.

A fő ok a civilek katonai feladatokra történő bevonására az volt, hogy Kína az 1950-es években nem rendelkezett kellő számú hadihajóval, sőt hadiflottájának nagyobbik részét is polgári hajók képezték. A milícia létrehozásának elsődleges célja tehát a gyakorlatilag nem létező haditengerészet védelmi feladatainak ellátása volt, elsősorban a már említett, Tajvanról érkező ellenséges hajókkal szemben. Ezen túlmenően védenie kellett a Dél-kínai- és a Kelet-kínai-tengeren a kínai halászati érdekeket, ugyanis a környező államok halászai is igénybe vették azokat a vizeket, amelyeket a kommunista Kína a saját felségvizeinek tartott. Ráadásul a már akkor is túlhalászott vizeken nagy verseny zajlott a halászok között a halakban bővebb régiók használatért.[5] A Tengeri Milícia létrehozása azonban felhívta a figyelmet a kínai katonai stratégiában bekövetkező fontos változásra is: a halászmilíciák a polgárháborús korszaktól eltérően már nemcsak a partvonalat voltak hivatottak megvédeni a külső behatolókkal szemben, hanem aktív szerepet kellett vállaljanak a távolabbi vizek ellenőrzésében is.[6]

---

[4] GROSSMAN, Derek – MA, Logan: A Short History of China's Fishing Militia and What It May Tell Us. The RAND Blog, 2020.04.06. https://www.rand.org/blog/2020/04/a-short-history-of-chinas-fishing-militia-and-what.html; letöltés: 2020.11.14.

[5] ERICKSON, Andrew S. – KENNEDY, Conor M.: China's Maritime Militia. p. 6. https://www.cna.org/cna_files/pdf/chinas-maritime-militia.pdf; letöltés: 2020.10.25.

[6] GROSSMAN, Derek – MA, Logan: A Short History of China's Fishing Militia and What It May Tell Us. The RAND Blog, 2020.04.06. https://www.rand.org/blog/2020/04/a-short-history-of-chinas-fishing-militia-and-what.html; letöltés: 2020.11.14.

Szervezeti jellemzők

Mára a Tengeri Milícia a kínai védelmi erők jelentős elemévé vált: egy félkatonai tömegszervezetté, amely fenntartja mindennapos gazdasági tevékenységét a fegyveres erőket támogató feladatai mellett. Hatalmas tartalékos erőt képvisel, amely a társadalom alapszintjén szerveződik, mivel egységeit falvak, városok és vállalkozások közösségeiből toborozzák. Területi alapon hozták létre, ezért az egyes egységek felépítése között jelentős különbségek lehetnek, így számos feladatkört tud ellátni. A Tengeri Milícia központjai kikötővel rendelkező part menti települések, ahol jelentős szerepe van a halászatnak, a hajóépítésnek és a hajózásnak, így tapasztalt hajóipari munkások és tengerészek biztosítják az állandó utánpótlást.[7]

A milícia szervezete két főbb komponensből áll. Az egyik a tartalékosokat tömöríti, a másik az aktív szolgálatból leszerelteket. Ez utóbbiak rendszeres kiképzésen vesznek részt, ők alkotják az „elsődleges erőt", amelyet szükség esetén azonnal lehet mozgósítani. A Tengeri Milícia zászlóaljakra, századokra, szakaszokra és rajokra oszlik úgy, hogy egy raj egy hajó legénységéből tevődik össze. A területi szerveződés miatt zászlóaljakat csak a városok tudnak kiállítani, a kisebb halászközösségek tagjaiból legfeljebb csak századokat vagy szakaszokat alakítanak ki. A milíciának félkatonai jellegéből és területi szerveződéséből adódóan kettős parancsnoki lánca van. A Tengeri Milícia irányítása – a szárazföldi milíciához hasonlóan – a városi párttitkár hatáskörébe tartozik, ő egyidejűleg a helyi katonai pártbizottság elnöke is. A mindennapi működés biztosítása a Népi Fegyveres Erők helyi egységének, alegységének a feladata, így nem ritka, hogy egy új század vagy zászlóalj alapítási ünnepélyén a helyi politikai vezető és a katonai parancsnok is részt vesz.[8]

A milícia létszámát csak megbecsülni lehet, mivel nincsenek hivatalos adatok arról, hogy a szervezet hány főt számlál. Kína a 2010-es Fehér Könyvében a Népi Fegyveres Erők Milíciájának létszámát 8 millió főben adta meg,[9] ennek azonban csak töredéke a Tengeri Milícia. A milíciához tartozó hajók számát 20–23 ezer hajóra becsülik,[10] amelyek legénysége összességében akár a százezer főt is elérheti.

---

[7] ERICKSON, Andrew S. – KENNEDY, Conor M.: China's Maritime Militia. p. 1. https://www.cna.org/cna_files/pdf/chinas-maritime-militia.pdf; letöltés: 2020.10.25.

[8] ERICKSON, Andrew S. – KENNEDY, Conor M.: Directing China's "Little Blue Men": Uncovering the Maritime Militia Command Structure. Asia Maritime Transparency Initiative, 2015.09.11. https://amti.csis.org/directing-chinas-little-blue-men-uncovering-the-maritime-militia-command-structure/; letöltés: 2020.10.25.

[9] China's National Defense in 2010. Information Office of the State Council, 2011.03.31. p. 25. https://media.nti.org/pdfs/1_1a.pdf; letöltés: 2020.10.18.

[10] KRASKA, James: China's Maritime Militia Vessels May Be Military Objectives During Armed Conflict. The Diplomat, 2020.07.07. https://thediplomat.com/2020/07/chinas-maritime-militia-vessels-may-be-military-objectives-during-armed-conflict/; letöltés: 2020.10.25.
KORKMAZ, Huseyin: Hybrid warfare and maritime militia in China. Anadolu Agency, 2020.02.07. https://www.aa.com.tr/en/analysis/analysis-hybrid-warfare-and-maritime-militia-in-china/1897259; letöltés: 2020.10.18.

A Tengeri Milícia tehát komoly támogatást biztosít a Népi Felszabadító Hadsereg számára, és a hadiflotta modernizálódásával pedig egyre bővülő feladatkört lát el. Sokoldalúsága és jelentős létszáma miatt a szervezet egyre fajsúlyosabbá válik a dél-kínai-tengeri műveletek során. Az utóbbi években Kína egyre inkább arra törekszik, hogy tengeri nagyhatalommá váljon, ezért a partjait övező tengereken a felségjogi viták egyre gyakrabban kerülnek a nemzetközi figyelem középpontjába. A kialakuló incidensekben a Tengeri Milícia hajói rendszeresen érintettek.

A Tengeri Milíciát és pontos feladatkörét éppen a félkatonai jellege miatt nehéz definiálni. Zeng Pengxiang, Zhousan város helyőrségparancsoka tömören így fogalmazta meg: „*A Tengeri Milícia egy pótolhatatlan fegyveres tömegszervezet, amelyet nem vontak ki a termelésből, és Kína tengeri fegyveres véderejének egy alkotóeleme, amely alacsony láthatóságot és nagy mozgásteret élvez a tengeri jogokat védő akciók során.*”[11]

A Tengeri Milícia szerepe

Hszi Csin-ping 2012-es pártfőtitkári kinevezése és a Központi Katonai Bizottság elnöki hivatalának elfoglalása óta Kína egyre nagyobb erőfeszítéssel törekszik kontinentális hatalomból tengeri nagyhatalommá válni.[12] Az eltelt kilenc évben a Tengeri Milícia egyre nagyobb szerepet kap mint politikai és katonai eszköz Peking dél-kínai-tengeri hatalmi játszmájában, ezért a működésében is változás történt. A 20. század második felében a kínai partközeli vizek ellenőrzése volt a Tengeri Milícia legfőbb kötelessége.[13] Most elsődleges feladata – a szárazföldi milíciától eltérően – azonban már az, hogy az ország területétől távol működő védelmi erőt képezzen, míg a partvédelmi feladatok mára másodlagossá váltak. A part menti vizek ellenőrzése a kínai Parti Őrségre hárul.

A Tengeri Milícia természetesen megmaradt egy fontos tartalékerőnek, amely bármikor mozgósítható háború vagy katasztrófahelyzet idején, valamint továbbra is támogatja a Népi Felszabadító Hadsereg és annak haditengerészete műveleteit, illetve a Parti Őrség tevékenységét. Szerepet kap még a tengeri mentési műveletek során, illetve természetesen maga a Tengeri Milícia is végrehajthat független missziókat, leginkább olyan esetekben, amikor a haditengerészet egységeinek a bevetése katonai konfliktust eredményezhetne.[14]

---

[11] ERICKSON, Andrew S. – KENNEDY, Conor M.: China’s Maritime Militia. p. 1. https://www.cna.org/cna_files/pdf/chinas-maritime-militia.pdf; letöltés: 2020.10.25.

[12] HÁDA Béla: A Kínai Népköztársaság és az Amerikai Egyesült Államok haditengerészeti erőviszonyai – tények és nézőpontok. Stratégiai Védelmi Kutatóintézet, Elemzések 2020/24, 2020.12.04. p. 2. http://real.mtak.hu/120691/1/SVKI_Elemzesek_2020_24_AKinaiNepkoztarsasagesazAmerikaiEgyesultAllamokhaditengereszetieroviszonyaiHadaB..pdf; letöltés: 2020.12.12.

[13] GROSSMAN, Derek – MA, Logan: A Short History of China's Fishing Militia and What It May Tell Us. The RAND Blog, 2020.04.06. https://www.rand.org/blog/2020/04/a-short-history-of-chinas-fishing-militia-and-what.html; letöltés: 2020.11.14.

[14] ERICKSON, Andrew S. – KENNEDY, Conor M.: China’s Maritime Militia. p. 5. https://www.cna.org/cna_files/pdf/chinas-maritime-militia.pdf; letöltés: 2020.10.25.

Mivel a Tengeri Milícia tagjai a kínai társadalom különböző rétegeiből és az ország különböző régióiból származnak, ezért tevékenységi körük és képességeik sokrétűek. Erre építve a szervezet többféle műveletet is képes elvégezni az egyszerűbb logisztikai feladatoktól kezdve a bonyolultabb haditengerészeti támogató műveletekig. A nagyobb, „méretesebb" alapterületű fedélzettel és tágas raktérrel rendelkező halászhajók kiválóan alkalmasak szállítási és utánpótlási feladatokra, például csapatok, járművek, felszerelések, nyersanyagok szállítására.[15] A tengeri mentési feladatok során – és persze a kiképzéskor – gyakorolt mentési és sebesültszállítási tevékenység hasznára válhat a fegyveres erőknek háborús helyzetben is. A Dél-kínai- és a Kelet-kínai-tenger egészén elszórtan elhelyezkedő hajók segíthetik a navigációban és természetesen a megfigyelésben is a fegyveres erők egységeit. A támogatótevékenység magában foglalja a javítási, vontatási, üzemanyag-feltöltési, illetve élelmiszerrel és vízzel történő ellátási feladatokat is, amivel a haditengerészet hajóit tudja segíteni egy, a Tengeri Milíciához tartozó halászhajó. Lehetségesek veszélyesebb feladatok is: konfliktus felvállalása esetén az ellenséges hajók zavarása, mozgásuknak akadályozása, figyelmük elterelése, esetleg tájékozódási és megfigyelési képességük megzavarása például nagy teljesítményű reflektorokkal, füst- és villanógránátokkal.[16]

A milícia speciális egységei még a hagyományos haderő egyes feladatköreit is elsajátítják, mint például egyes rakétavédelmi eszközök használata vagy szabotázsakciók végrehajtása. A legnagyobb hangsúlyt viszont a felderítés és a megfigyelés kapja, mivel a nagy területen szétszórt hajók segítségével Peking teljes megfigyelés alatt tarthatja a Kelet-kínai- és a Dél-kínai-tengert, illetve a polgári hajók felhasználásával a kiemelt jelentőségű célpontok megfigyelése viszonylag gyanútlanul történhet. Védelmi célokra is alkalmasak lehetnek a milícia hajói, mert használhatók a stratégiai fontosságú kikötők és az olajfúró állomások biztosítására is. A katonai-védelmi jellegű feladatokon kívül a milícia tevékenységi körébe tartozik még a polgári lakosság megóvása természeti katasztrófa, ipari baleset, tömeges egészségügyi vészhelyzet vagy más, ehhez hasonló jellegű veszélyhelyzet idején.[17]

A Tengeri Milícia viszonylag új keletű feladatai közé tartozik Kína területi követeléseinek érvényre juttatása a Dél-kínai-tengeren.[18] Ezzel kapcsolatban 2013-ban Kuangtung tartomány katonai körzete mozgósításért felelős részlegének igazgatója három pontban foglalta össze a Tengeri Milícia szerepét. Egyfelől a kínai nemzeti akarat megtestesüléseként hivatkozott rá, amelynek célja az ország jogos tengeri követeléseinek az érvényesítése. Másfelől a milícia tagjai példaképként szolgálnak az ország halászai számára azzal, hogy hazájuk fejlődéséért és jólétéért dolgoznak,

---

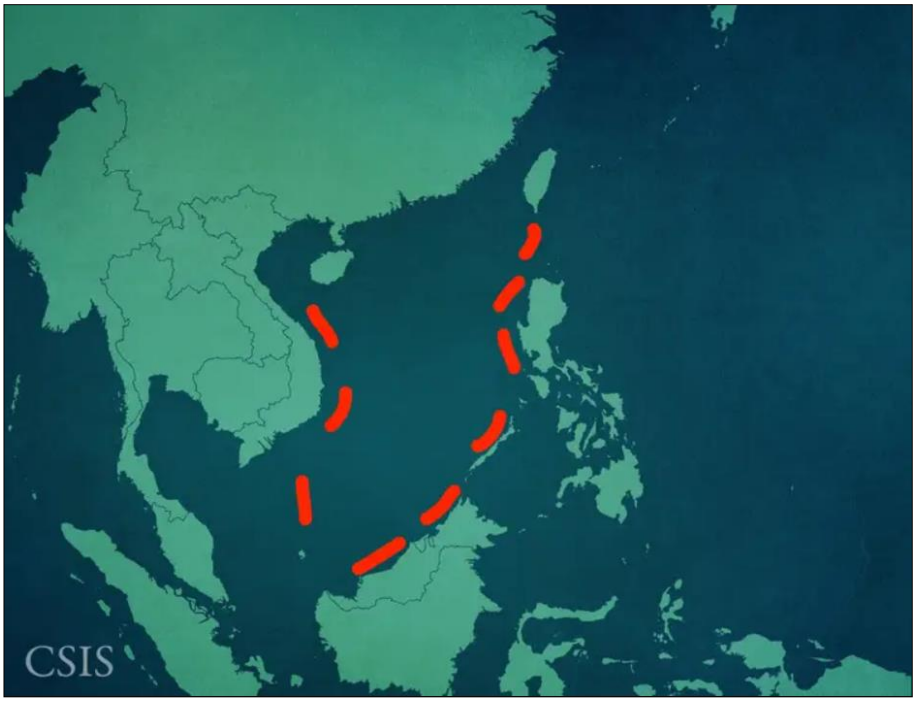
[15] KRASKA, James: China's Maritime Militia Vessels May Be Military Objectives During Armed Conflict. The Diplomat, 2020.07.07. https://thediplomat.com/2020/07/chinas-maritime-militia-vessels-may-be-military-objectives-during-armed-conflict/; letöltés: 2020.10.25.

[16] ERICKSON, Andrew S. – KENNEDY, Conor M.: China's Maritime Militia. p. 5. https://www.cna.org/cna_files/pdf/chinas-maritime-militia.pdf; letöltés: 2020.10.25.

[17] Uo.

[18] GROSSMAN, Derek – MA, Logan: A Short History of China's Fishing Militia and What It May Tell Us. The RAND Blog, 2020.04.06. https://www.rand.org/blog/2020/04/a-short-history-of-chinas-fishing-militia-and-what.html; letöltés: 2020.11.14.

kihajóznak a Kína által birtokba vett szigetekhez és zátonyokhoz, ezzel biztosítják az ország számára, hogy az kifejezhesse jogát a vitatott területek feletti ellenőrzésre. A Tengeri Milícia harmadik fontos szerepe, hogy tagjai a biztonságos hajózás letéteményesei, akik az elsők között képesek reagálni egy válsághelyzet idején, hiszen a Kínát övező tengerek minden szegletében megtalálhatók, így azonnal tudnak segíteni a bajbajutottakon.[19]



1. ábra. A kilencpontos vonal[20]

A területi követeléseket, amelyekre az igazgató az első és második pontokban utalt, a Peking által meghatározott úgynevezett kilencpontos vonalon (*nine-dash-line*) belül található vizekre és szigetekre érti, amelyek lefedik a Dél-kínai-tenger 90%-át, és amelyekre Kína történelmi okokra hivatkozva tart igényt.[21] Annak érdekében, hogy követelésének érvényt szerezzen, Kína apró szigeteket, sziklákat és zátonyokat kezdett

[19] ERICKSON, Andrew S. – KENNEDY, Conor M.: China's Maritime Militia. p. 4. https://www.cna.org/cna_files/pdf/chinas-maritime-militia.pdf; letöltés: 2020.10.25.

[20] LIU, Zhen: Here's what's behind the 'nine-dash line' that sparked the South China Sea conflict. Insider, 2016.07.12. https://www.businessinsider.com/the-nine-dash-line-at-the-heart-of-the-south-china-sea-conflict-2016-7; letöltés: 2020.10.24.

[21] CASARINI, Nicola: A Sea at the Heart of Chinese National Interest. Global Challenges, Issue no. 1, February 2017. https://globalchallenges.ch/issue/1/a-sea-at-the-heart-of-chinese-national-interest/; letöltés: 2020.11.15.

elfoglalni a Paracel- és a Spratley-szigetek térségében, és 2013–2016 között azokat feltöltve nagyobb alapterületű mesterséges szigeteket alakított ki. A rajtuk létrehozott támaszpontok felépítésében aktív szerepet vállaltak a Tengeri Milícia egységei is, elsősorban építőanyagok szállítását végezték.[22] A szigetek környékéről kínai halászhajók űzik el a más államok halászflottájához tartozó hajókat azzal, hogy tevékenységüket akadályozzák, zaklatják őket, de arra is volt példa, hogy a kínaiak szándékosan nekiütköztek a „riválisˮ hajóknak. A vitatott hovatartozású mesterséges szigetek körüli vizeken a milícia egységei persze nemcsak az idegen halászokkal szemben, hanem a térség fosszilis energiaforrásai után kutató társaságok hajóival, sőt a kereskedőhajókkal szemben is fellépnek.[23]

A Dél-kínai-tenger hajózási útvonalai a világ legforgalmasabbjai közé tartoznak, hiszen évente mintegy 3400 milliárd dollárnyi áruforgalom halad itt keresztül. Emellett azt is fontos megemlíteni, hogy jelentős még kiaknázatlan kőolaj- és földgázkészletek rejlenek a vízfelszín alatt, a térség feletti fennhatóság megszerzése ezért stratégiai jelentőségű.[24] Pekingnek azonban az is érdeke, hogy a térségben érdekelt államokkal való összetűzései ne eszkalálódjanak katonai konfliktussá, ezért inkább hibrid hadviseléssel próbálja akaratát érvényesíteni vetélytársaival szemben. A kínai pártvezetés stratégiájában a Tengeri Milíciának kulcsszerepe van Peking tengeri követeléseinek ilyen jellegű érvényre juttatásában. A milícia egységei ugyanis megkülönböztethetetlenek a ténylegesen polgári tulajdonban álló hajóktól, és így civil hajónak minősülnek, nem hadihajónak. Ebből fakadóan védi őket a nemzetközi humanitárius jog,[25] amelynek alapvető jogforrásai az 1949-es Genfi egyezmények. Így tehát más országok hadihajói még egy katonai konfliktus során sem léphetnének fel a Tengeri Milícia hajóival szemben úgy, ahogy azt egy „valódiˮ hadihajóval szemben tennék, ha nem akarják megsérteni a hatályos nemzetközi egyezményeket.

A halászhajók mindennapi gazdasági tevékenységük fenntartása mellett titokban végezhetnek felderítést és megfigyelést anélkül, hogy retorzió érné őket emiatt. Az Amerikai Egyesült Államoknak egy hadihajója például nehéz helyzetben találná magát, ha titokban kellene átkelnie a kínai halászhajóktól hemzsegő Dél-kínai-tengeren úgy, hogy közben egyik se vegye észre és jelentse a pozícióját. Amennyiben pedig egy, a milíciához tartozó hajót katonai jellegű tevékenysége miatt mégis elfogná vagy megsemmisítené egy ellenséges erő, akkor Kína bizonyára igyekezne arra irányítani a nemzetközi média figyelmét, hogy ártatlan és ártalmatlan halászait veszi célba a másik állam. Kína ezzel potenciálisan aláásná a másik fél nemzetközi diplomáciai státuszát és polgári lakosságának eltökéltségét.

---

[22] KORKMAZ, Huseyin: Hybrid warfare and maritime militia in China. Anadolu Agency, 2020.02.07. https://www.aa.com.tr/en/analysis/analysis-hybrid-warfare-and-maritime-militia-in-china/1897259; letöltés: 2020.10.18.

[23] U.S.-China Strategic Competition in South and East China Seas: Background and Issues for Congress. Congressional Research Service, 2020. p. 12. https://fas.org/sgp/crs/row/R42784.pdf; letöltés: 2020.10.23.

[24] Uo. p. 6.

[25] KRASKA, James – MONTI, Michael: The Law of Naval Warfare and China's Maritime Militia. International Law Studies, Volume 91, 2015. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1406&context=ils; letöltés: 2020.10.25.

A Tengeri Milícia azonban távolról sem lenne ártalmatlan egy katonai konfliktus során, hiszen hajóinak és tengerészeinek puszta száma is jelzi, hogy komoly fenyegetést jelenthet a térség államaira. A nagy flotta és embertömeg mellett természetesen a milícia olyan erőforrásokhoz is hozzájut, amilyenekhez közönséges halászok nem jutnának hozzá. Ilyenek például könnyűfegyverek, illetve olyan megerősített testű halászhajók, amelyek jól bírják az ütközéseket, sőt az sem elképzelhetetlen, hogy Peking halászhajónak álcázott hadihajókat von be a Tengeri Milícia műveleteibe.[26] Mindezeket figyelembe véve egyértelmű, hogy a milícia egységei esetében a jogi státusz meghatározása nagy nehézségekbe ütközik. Egy halászhajó, amely egész évben pusztán halászattal foglalkozik, viszont az év egyetlen napján katonai jellegű tevékenységet végez, az vajon katonai vagy civil hajónak minősül? Ez a dilemma Peking milíciával kapcsolatos szürkezónás stratégiájának egyik, ha nem a legmeghatározóbb eleme.

Az Amerikai Egyesült Államok erre a dilemmára a választ tavaly adhatta meg. 2019. január 28-án John Richardson tengernagy, az Egyesült Államok Haditengerészetének akkori vezérkari főnöke és Shen Jinlong altengernagy,[27] a Népi Felszabadító Hadsereg Haditengerészetének vezérkari főnöke közti megbeszélésen Richardson bejelentette, hogy egy konfliktus esetén az amerikaiak a Tengeri Milícia hajóit – és a kínai Parti Őrség hajót is – ugyanúgy kezelnék, mint a hadihajókat, mivel a halászhajókat katonai feladatokra alkalmazzák.[28] Ez a figyelmeztetés elvileg jelentősen növeli a Kína által azzal vállalt kockázatot, hogy halászhajói katonai tevékenységet folytatnak. A kijelentés mögötti elrettentés hatásosságát viszont csökkentheti, hogy az amerikai hadihajók valószínűleg nem lépnének fel agresszívan még a kínai hadihajókkal szemben sem. Emellett a jelenlegi viszonylag békés kapcsolatok fenntartása és a feszültség fokozódásának elkerülése végett sem valószínű, hogy békeidőben erőszakot alkalmaznának a milícia hajóival szemben. A jövőre nézve azonban nem lenne túl biztató, ha Washington mégis úgy döntene, hogy a milícia hajóit katonainak tekinti, mivel a Dél-kínai-tengeren rendszeresen járőröznek amerikai hadihajók, és a Tengeri Milícia is folytatja működését a régió minden szegletében, így jelentősen megnőhet egy nagyobb konfliktus esélye a két nagyhatalom között.

A Tengeri Milícia stratégiája

A Tengeri Milícia által is alkalmazott szürkezónás (azaz a béke és a háború közti, háborús küszöb alatt zajló) műveletek tipikus jellemzője a Peking által a Kelet-kínai- és Dél-kínai-tengeren alkalmazott stratégiának. A térségben zajló folyamatokat elemző szakértők ezt a stratégiát a „szalámiszeletelő” (*salami-slicing*),[29] „inkrementális”, azaz

---

[26] KRASKA, James – MONTI, Michael: The Law of Naval Warfare and China's Maritime Militia. International Law Studies, Volume 91, 2015. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1406&context=ils; letöltés: 2020.10.25.

[27] 2019 júliusa óta tengernagy.

[28] SEVASTOPULO, Demetri – HILLE, Kathrin: US warns China on aggressive acts by fishing boats and coast guard. Financial Times, 2019. https://www.ft.com/content/ab4b1602-696a-11e9-80c7-60ee53e6681d; letöltés: 2020.11.15.

[29] U.S.-China Strategic Competition in South and East China Seas: Background and Issues for Congress. Congressional Research Service, 2020. p. 71. https://fas.org/sgp/crs/row/R42784.pdf; letöltés: 2020.10.23.

fokozatosan eszkaláló (*incremental*),[30] és a „belopódzó" (*creeping*)[31] jelzőkkel illetik. Kína minden lehetőséget megragad ugyanis, hogy folytassa a térségbeli terjeszkedési tevékenységét, legfőképpen akkor, amikor a nemzetközi figyelem nem rá irányul. Peking a koronavírus-járvány időszakát is arra használja fel, hogy a stratégiájába illő műveleteket hajtson végre a dél-kínai-tengeri szomszédjai ellen, miközben a világ figyelmét a pandémiás helyzet köti le. Erről Mike Pompeo amerikai külügyminiszter a 2020. április 22-ei beszédében az ASEAN külügyminisztereivel folytatott videokonferencián számolt be:

„*Két módot szeretnék kiemelni, hogy a Kínai Kommunista Párt hogyan használja ki a világ COVID–19 válságra összpontosított figyelmét azzal, hogy folytatja provokatív magatartását. […] Láthattuk, hogy a Kínai Kommunista Párt katonai nyomást gyakorol Tajvanra, és rákényszeríti akaratát szomszédjaira a Dél-kínai-tengeren, és még olyan messzire is elment, hogy elsüllyesztett egy vietnámi halászhajót.*"[32]

A Mike Pompeo által közölt incidens során az említett vietnámi halászhajó 20 nappal korábban süllyedt el a Paracel-szigetek közelében azt követően, hogy összeütközött a kínai Parti Őrség egyik hajójával, amely korábban távozásra szólította fel. A halászokat ezután a Parti Őrség felvette, majd átszállította őket az eseményeket távolabbról figyelő két másik vietnámi halászhajóra. Az ütközés felelőseként Peking a vietnámi halászhajót, míg Hanoi a Parti Őrség hajóját nevezte meg. Az ügyet bonyolítja, hogy Vietnámnak is van tengeri milíciája, amely a kínaihoz hasonlóan az ország 1,5 milliós milíciájának része, és számítások szerint közel 46 ezer tagja van.[33] Az a flotta is halászhajókból áll, így nehéz eldönteni, hogy az említett incidens során valóban pusztán egy polgári hajó esett áldozatul, vagy a vietnámi tengeri milícia akciója sikeredett félre. Annak a lehetősége is felmerült, hogy a vietnámi tengerészek szándékosan ütköztek neki és süllyesztették el a saját hajójukat, jól tudva, hogy a közelben figyelő társaik rögzítik az eseményeket, és az esetet követően kimentik őket.[34]

---

[30] MENDIS, Patrick – WANG, Joey: China's Art of Strategic Incrementalism in the South China Sea. The National Interest, 2020.08.08. https://nationalinterest.org/feature/china%E2%80%99s-art-strategic-incrementalism-south-china-sea-166445; letöltés: 2020.11.14.

[31] DIEHL, Jackson: China's 'Creeping Invasion'. The Washington Post, 2014.09.14. https://www.washingtonpost.com/opinions/jackson-diehl-chinas-creeping-invasion-on-the-global-order/2014/09/14/91275a9e-3a60-11e4-9c9f-ebb47272e40e_story.html; letöltés: 2020.11.15.

[32] Secretary Michael R. Pompeo Remarks to the Press At a Press Availability, April 22, 2020. https://it.usembassy.gov/secretary-michael-r-pompeo-remarks-to-the-press-at-a-press-availability-april-22-2020/; letöltés: 2021.03.21.

[33] XIANGMIAO, Chen: Vietnam's Maritime Militia: A "Black Hole" of the South China Sea. SCSPI, 2020.04.30. http://www.scspi.org/en/dtfx/1588176000; letöltés: 2020.11.14.

[34] NGUYEN, The Phuong: Vietnam's Maritime Militia Is Not a Black Hole in the South China Sea. Asia Maritime Transparency Initiative, 2020.05.22. https://amti.csis.org/vietnams-maritime-militia-is-not-a-black-hole-in-the-south-china-sea/; letöltés: 2020.11.14.

Kínai halászhajók, illetve vietnámi, fülöp-szigeteki, japán és tajvani hajók közti ehhez hasonló összetűzésekre számos példát találni az elmúlt évek híradásaiban. A vietnámi halászhajó elsüllyedése mellett a 2020-as év nevezetesebb incidensei a következők voltak:

- március 16-án a Csinmen-szigetek közelében egy tíz kínai halászhajóból álló flotta a tajvani parti őrséggel keveredett összetűzésbe, amely során a tajvani parti őrség egy hajója megsérült;[35]
- március 30-án kínai halászhajók többször is nekiütköztek a *Shimakaze* japán rombolónak Sanghajtól 200 kilométerre, és az egyik ütközés a romboló oldalán egy 1 méter átmérőjű lyukat ütött;[36]
- június 14-én egy kínai halászhajó nekiütközött egy vietnámi halászhajónak a Kína által birtokba vett Paracel-szigetekhez tartozó Lincoln-szigettől 15 kilométerre, az ütközés következtében a vietnámi hajó léket kapott és kis híján elsüllyedt, a rajta tartózkodó 16 halászt a kínai legénység felvette a saját hajójára, majd segítettek a vietnámi hajó úszóképességének helyreállításában.[37]

Az incidensek számát még jobban gyarapíthatja a jövőben, hogy a térség államai a kínai – és részben a vietnámi – Tengeri Milícia hatásos tevékenységének következtében megkísérelhetik saját tengeri milíciájukat létrehozni. 2020. októberi híradások szerint a már így is több tízezres létszámú kínai és vietnámi tengeri milíciák mellett a Fülöp-szigetek is fontolgatta saját halászaiból és halászhajó-flottájából egy tengeri milícia megszervezését.[38] Rodrigo Duterte fülöp-szigeteki elnök november 5-ei tájékoztatóján azonban bejelentette, hogy országa nem kíván még több konfliktusba keveredni Kínával, így ezt a tervet egyelőre félretették.[39] Maga az ötlet viszont nyilvánvaló indikátora annak, hogy egy tengeri milícia olcsón és hatékonyan képes a nemzeti érdekek érvényesítésére, ezért megszervezése és fenntartása kifizetődő befektetés a Kelet-kínai- és a Dél-kínai-tenger feletti fennhatóságért versengő országoknak.

---

[35] PANDA, Ankit: Taiwan Coast Guard Reports Chinese Speed Boat Harassment Near Kinmen. The Diplomat, 2020. https://thediplomat.com/2020/03/taiwan-coast-guard-reports-chinese-speed-boat-harassment-near-kinmen/; letöltés: 2020.11.22.

[36] TANG, Didi: Japanese destroyer holed after collision with Chinese trawler. The Times, 2020.04.02. https://www.thetimes.co.uk/article/japanese-destroyer-holed-after-collision-with-chinese-trawler-0372zfv2m; letöltés: 2020.11.22.

[37] Chinese Vessel Rams Vietnamese Fishing Boat in S. China Sea. The Maritime Executive, 2020.06.14. https://www.maritime-executive.com/article/report-chinese-vessel-rams-vietnamese-fishing-boat-in-s-china-sea; letöltés: 2020.11.22.

[38] ROBLES, Alan: Philippines' plan for maritime militia to match China raises fears of 'shooting war'. South China Morning Post, 2020.10.16. https://www.scmp.com/week-asia/politics/article/3105687/philippines-plan-maritime-militia-match-china-raises-fears; letöltés: 2020.11.22.

[39] STRANGIO, Sebastian: Philippines Shelves Plan for South China Sea Fishing Militia. The Diplomat, 2020.11.06. https://thediplomat.com/2020/11/philippines-shelves-plan-for-south-china-sea-fishing-militia/; letöltés: 2020.11.22.

Összegzés

Egyértelműen megállapítható, hogy a Népi Fegyveres Erők Tengeri Milíciája nem pusztán egy kiegészítő elem a Népi Felszabadító Hadsereg Haditengerészete és a kínai Parti Őrség mellett. Azon túl, hogy fontos támogató szerepet tölt be e két haderőnem műveleteiben a Kelet-kínai- és a Dél-kínai-tengeren, önálló akciói is láthatóan jelentős elrettentő vagy akár kényszerítő erővel bírnak. Kína a világ legnagyobb halászflottájával rendelkezik, amelynek akciórádiusza nem korlátozódik pusztán a partközeli vizekre, hanem több száz, akár több ezer kilométernyi távolságra is elér. Létszámának köszönhetően a Tengeri Milícia megfigyelés alatt tarthatja a régió egészét, és ha kell, erőszakkal is megvédi Peking érdekeit a vitatott hovatartozású területeken. Félkatonai mivoltából fakadóan a kínai vezetésnek nem kell attól tartania, hogy egy incidens katonai konfliktussá eszkalálódik egy rivális ország (legfőképpen az Amerikai Egyesült Államok) haditengerészetével szemben.

A hibrid hadviselés részeként a Tengeri Milícia „álcázott haditengerészetként" zaklathatja és zavarhatja el a vetélytársak hajóit a Kína által saját fennhatósága alá deklarált vizekről, ezáltal korlátozva őket a szabad hajózáshoz való jogukban. Tekintetbe véve Pekingnek a Tengeri Milíciájára irányuló nagyfokú figyelmét és azt a gyakorlatot, hogy a szervezet az utóbbi években egyre gyakrabban kerül bevetésre a Kelet-kínai- és a Dél-kínai-tengeren, valószínűnek tűnik, hogy Kína a Tengeri Milíciát kulcsfontosságú elemnek látja a tengeri nagyhatalommá válása útján.

FELHASZNÁLT IRODALOM

- CASARINI, Nicola: A Sea at the Heart of Chinese National Interest. Global Challenges, Issue no. 1, February 2017. https://globalchallenges.ch/issue/1/a-sea-at-the-heart-of-chinese-national-interest/; letöltés: 2020.11.15.
- CAVAS, Christopher P.: China's 'Little Blue Men' Take Navy's Place in Disputes. Defense News, 2015.11.02. https://www.defensenews.com/naval/2015/11/03/chinas-little-blue-men-take-navys-place-in-disputes/; letöltés: 2020.10.25.
- China's National Defense in 2010. Information Office of the State Council, 2011.03.31. https://media.nti.org/pdfs/1_1a.pdf; letöltés: 2020.10.18.
- Chinese Vessel Rams Vietnamese Fishing Boat in S. China Sea. The Maritime Executive, 2020.06.14. https://www.maritime-executive.com/article/report-chinese-vessel-rams-vietnamese-fishing-boat-in-s-china-sea; letöltés: 2020.11.22.
- DIEHL, Jackson: China's 'Creeping Invasion'. The Washington Post, 2014.09.14. https://www.washingtonpost.com/opinions/jackson-diehl-chinas-creeping-invasion-on-the-global-order/2014/09/14/91275a9e-3a60-11e4-9c9f-ebb47272e40e_story.html; letöltés: 2020.11.15.

- ERICKSON, Andrew S. – KENNEDY, Conor M.: China's Maritime Militia. https://www.cna.org/cna_files/pdf/chinas-maritime-militia.pdf; letöltés: 2020.10.25.
- ERICKSON, Andrew S. – KENNEDY, Conor M.: Directing China's "Little Blue Men": Uncovering the Maritime Militia Command Structure. Asia Maritime Transparency Initiative, 2015.09.11. https://amti.csis.org/directing-chinas-little-blue-men-uncovering-the-maritime-militia-command-structure/; letöltés: 2020.10.25.
- GREEN, Michael – HICKS, Kathleen – COOPER, Zack – SCHAUS, John – DOUGLAS, Jake: Counter-Coercion Series: Harassment of the USNS Impeccable. Asia Maritime Transparency Initiative, 2017.05.09. https://amti.csis.org/counter-co-harassment-usns-impeccable/; letöltés: 2020.11.15.
- GROSSMAN, Derek – MA, Logan: A Short History of China's Fishing Militia and What It May Tell Us. The RAND Blog, 2020.04.06. https://www.rand.org/blog/2020/04/a-short-history-of-chinas-fishing-militia-and-what.html; letöltés: 2020.11.14.
- HÁDA Béla: A Kínai Népköztársaság és az Amerikai Egyesült Államok haditengerészeti erőviszonyai – tények és nézőpontok. Stratégiai Védelmi Kutatóintézet, Elemzések 2020/24, 2020.12.04. http://real.mtak.hu/120691/1/SVKI_Elemzesek_2020_24_AKinaiNepkoztarsasagesazAmerikaiEgyesultAllamokhaditengereszetieroviszonyaiHadaB..pdf; letöltés: 2020.12.12.
- KORKMAZ, Huseyin: Hybrid warfare and maritime militia in China. Anadolu Agency, 2020.02.07. https://www.aa.com.tr/en/analysis/analysis-hybrid-warfare-and-maritime-militia-in-china/1897259; letöltés: 2020.10.18.
- KRASKA, James – MONTI, Michael: The Law of Naval Warfare and China's Maritime Militia. International Law Studies, Volume 91, 2015. https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=1406&context=ils; letöltés: 2020.10.25.
- KRASKA, James: China's Maritime Militia Vessels May Be Military Objectives During Armed Conflict. The Diplomat, 2020.07.07. https://thediplomat.com/2020/07/chinas-maritime-militia-vessels-may-be-military-objectives-during-armed-conflict/; letöltés: 2020.10.25.
- LIU, Zhen: Here's what's behind the 'nine-dash line' that sparked the South China Sea conflict. Insider, 2016.07.12. https://www.businessinsider.com/the-nine-dash-line-at-the-heart-of-the-south-china-sea-conflict-2016-7; letöltés: 2020.10.24.
- MENDIS, Patrick – WANG, Joey: China's Art of Strategic Incrementalism in the South China Sea. The National Interest, 2020.08.08. https://nationalinterest.org/feature/china%E2%80%99s-art-strategic-incrementalism-south-china-sea-166445; letöltés: 2020.11.14.

- NGUYEN, The Phuong:
  Vietnam's Maritime Militia Is Not a Black Hole in the South China Sea.
  Asia Maritime Transparency Initiative, 2020.05.22.
  https://amti.csis.org/vietnams-maritime-militia-is-not-a-black-hole-in-the-south-china-sea/; letöltés: 2020.11.14.
- PANDA, Ankit: Taiwan Coast Guard Reports Chinese Speed Boat Harassment Near Kinmen. The Diplomat, 2020.
  https://thediplomat.com/2020/03/taiwan-coast-guard-reports-chinese-speed-boat-harassment-near-kinmen/; letöltés: 2020.11.22.
- ROBLES, Alan:
  Philippines' plan for maritime militia to match China raises fears of 'shooting war'.
  South China Morning Post, 2020.10.16.
  https://www.scmp.com/week-asia/politics/article/3105687/philippines-plan-maritime-militia-match-china-raises-fears; letöltés: 2020.11.22.
- Secretary Michael R. Pompeo Remarks to the Press At a Press Availability, April 22, 2020.
  https://it.usembassy.gov/secretary-michael-r-pompeo-remarks-to-the-press-at-a-press-availability-april-22-2020/; letöltés: 2021.03.21.
- SEVASTOPULO, Demetri – HILLE, Kathrin:
  US warns China on aggressive acts by fishing boats and coast guard.
  Financial Times, 2019.
  https://www.ft.com/content/ab4b1602-696a-11e9-80c7-60ee53e6681d; letöltés: 2020.11.15.
- STRANGIO, Sebastian: Philippines Shelves Plan for South China Sea Fishing Militia.
  The Diplomat, 2020.11.06.
  https://thediplomat.com/2020/11/philippines-shelves-plan-for-south-china-sea-fishing-militia/; letöltés: 2020.11.22.
- TANG, Didi: Japanese destroyer holed after collision with Chinese trawler.
  The Times, 2020.04.02.
  https://www.thetimes.co.uk/article/japanese-destroyer-holed-after-collision-with-chinese-trawler-0372zfv2m; letöltés: 2020.11.22.
- U.S.-China Strategic Competition in South and East China Seas: Background and Issues for Congress. Congressional Research Service, 2020.
  https://fas.org/sgp/crs/row/R42784.pdf; letöltés: 2020.10.23.
- XIANGMIAO, Chen:
  Vietnam's Maritime Militia: A "Black Hole" of the South China Sea.
  SCSPI, 2020.04.30.
  http://www.scspi.org/en/dtfx/1588176000; letöltés: 2020.11.14.

DR. ALBERT ÁGOTA – DR. TÓTH SÁNDOR ALEZREDES –
ÜVEGES ANDRÁS JÓZSEF SZÁZADOS – LÉVAI ZSOLT

A KÖZLEKEDÉSI RENDSZEREK ÉS AZ INFORMÁCIÓS TERRORIZMUS KAPCSOLATA

Bevezetés

A mindennapi életünkben gyakran vesszük igénybe a közlekedési eszközöket. A közlekedés, illetve a közforgalmú közlekedés életünk meghatározó eleme, ennek a rendszernek a sérülése vagy egy elemének kiesése jelentős anyagi, gazdasági és társadalmi károkat okozhat. Egy ország működéséhez elengedhetetlen a közlekedési rendszer megfelelő működése, éppen ezért a közlekedési hálózatok a terrorizmus tekintetében kiemelt célpontnak tekinthetőek, mivel alapvetően és döntően nagyszámú személy tartózkodik huzamosabb időn keresztül viszonylag szűkebb helyeken.

A terrortámadások egyik lehetséges elkövetési módja a fizikai pusztítás, a másik pedig a kibertérben elkövetett támadás, ami a fizikai térben okoz károkat vagy követel emberéleteket. Ha még pontosabban akarunk fogalmazni, akkor mindenképpen meg kell jegyezni azt is, hogy a gyors digitalizációs folyamatok miatt az információs terrorizmus nemcsak a kiberteret vagy a fizikai valóságot érinti, hanem a kettő peremterületét, a digitális ökoszisztémát is fenyegeti,[1] mivel a tömegközlekedést kiszolgáló információs infrastruktúra is ennek a része. Emellett meg kell azt is említeni, hogy a modern közforgalmú közlekedési szolgáltatók nagy mennyiségű személyes adatot[2] tárolnak és kezelnek, amely a működésükhöz elengedhetetlen.

A közlekedési infrastruktúrák az alábbi tulajdonságokkal jellemezhetők:

- hálózat- és rendszerjellegűek;
- nagy kiterjedésűek;
- többnyire állami tulajdonban vagy legalább állami felügyelet alatt működnek;
- szolgáltatásaik piaci áruk;
- jelentős fenntartási költségeik vannak.

Ezekből a tulajdonságukból az következik, hogy a közlekedési infrastruktúra egyes elemeinek kiesése jelentős anyagi és társadalmi károkat okoz.[3] Ez leginkább azokra az elemekre igaz, amelyek jelentős forgalmat bonyolítanak le, és pótlásuk, helyettesíthetőségük nehezen vagy egyáltalán nem oldható meg.[4]

---

[1] KOVÁCS László: A kibertér védelme. Dialóg Campus Kiadó, Budapest, 2018. pp. 22–23. https://www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf; letöltés: 2021.04.25.

[2] Nemcsak az utasok személyes adatait, hanem a munkavállalók és a beszállítók adatait is ide kell érteni.

[3] SZÁSZI Gábor: A vasúti közlekedési alágazat, mint kritikus infrastruktúra. In: HORVÁTH Attila – BÁNYÁSZ Péter (szerk.): Fejezetek a kritikus infrastruktúra védelemből – Kiemelten a közlekedési alrendszer. Tanulmánykötet. Magyar Hadtudományi Társaság, Budapest, 2013. pp. 167–190. http://real.mtak.hu/72510/1/KIV_tanulmanykotet.pdf; letöltés: 2021.04.25.

[4] Például a Déli összekötő vasúti híd és a Pentele híd.

Az ilyen közlekedési hálózati elemek[5] joggal sorolhatók a létfontosságú közlekedési infrastruktúrák közé. A 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről szóló mellékletében is egyértelműsíti[6] ezeket az alágazatokat. Miután a közlekedési hálózat az egész országot lefedi, sőt nemzetközi kapcsolatokkal rendelkezik, számos ilyen létfontosságú hálózati elem lehetséges.

Ha egy országnak akarunk (politikai) károkat okozni, akkor ennek egyik lehetséges módja a közlekedési rendszer támadása és rombolása. A közlekedési rendszer kiterjedése és bonyolultsága okán már a normál működés során is előfordulhatnak zavarok, amelyek jelentős fennakadásokat okozhatnak, és ha ezeket szándékos emberi cselekedet idézi elő, akkor a károk előre felbecsülhetetlenek lehetnek.[7] Fentiekből következik, hogy a közlekedési hálózat ellen sok helyen lehetséges hatásos terrorcselekmény elkövetése. A terrortámadások egyik lehetséges elkövetési módja a fizikai, a másik pedig a kibertérben elkövetett támadás. A Kovács–Krasznay szerzőpáros a közlekedési ágazatot egy Magyarország elleni lehetséges terrortámadás egyik területeként azonosítja.[8] A 2017-ben megjelent újabb tanulmányukban megállapítják, hogy a kiberhadviselés egyre nagyobb terepet és szerepet kap a konfliktusok előidézésében.[9]

A fizikai terrortámadások akkor lehetnek hatékonyak, ha megfelelően elő vannak készítve, azaz a művelet maximális áldozatszámmal és jelentős károkozással jár. A terrorcselekmények megfelelő előkészítéséhez az elkövetőknek adatokra van szükségük a tervezett célpontokról. Az adatok forrása ma már legtöbb esetben a nyílt internet, mert az infrastruktúrák üzemeltetetői és a szolgáltatók a sok esetben kötelező, máskor önszántukból közölt adatai révén a szélsőségesek rengeteg olyan adathoz és információhoz juthatnak, amelyek segítik őket támadásaik megfelelő tervezésében és végrehajtásában.

Kérdésként merül fel, hogy milyen közérdekű adatokat szükségszerű megosztani, illetve a feltett adatokat mennyire kell védeni. Cikkünkben azt vizsgáljuk, hogy milyen kritériumokat lehet azonosítani, rendszerezni és meghatározni annak érdekében, hogy ne kerülhessenek ki az internetre olyan adatok, amelyek segítséget nyújthatnak egy esetleges terrortámadás kivitelezéséhez.

---

[5] A 2012. évi CLXVI. törvény melléklete alapján a közúti közlekedés, a vasúti közlekedés, a légi közlekedés, a vízi közlekedés és a logisztikai központok.

[6] 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről.
https://net.jogtar.hu/jogszabaly?docid=a1200166.tv; letöltés: 2021.04.25.

[7] FÁBOS Róbert: A közlekedési informatikai rendszerek sérülékenysége. In: HORVÁTH Attila – BÁNYÁSZ Péter (szerk.): Fejezetek a kritikus infrastruktúra védelemből – Kiemelten a közlekedési alrendszer. Tanulmánykötet. Magyar Hadtudományi Társaság, Budapest, 2013. pp. 191–225.
http://real.mtak.hu/72510/1/KIV_tanulmanykotet.pdf; letöltés: 2021.04.25.

[8] KOVÁCS László – KRASZNAY Csaba: Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 2010/1. szám. pp. 44–56.
http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf; letöltés: 2021.04.25.

[9] KOVÁCS László – KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. Nemzet és Biztonság, 2017/1. szám. pp. 3–16.
http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf; letöltés: 2021.04.25.

Problémafelvetés

Jelenleg hazánkban a 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról (továbbiakban: Infotv.[10]), illetve a közérdekű és közérdekből nyilvános adatok nyilvánosságáról rendelkező egyéb jogszabályok határozzák meg azt, hogy a szolgáltatóknak milyen közérdekű adatot kell feltüntetni elektronikus portáljaikon.[11] Jelenleg a szolgáltatók felelőssége, hogy milyen közérdekű, illetve közérdekből nyilvános adatot hoznak nyilvánosságra, valamint mely esetekben élnek az Infotv. által biztosított mentességekkel,[12] azaz ezen adatok megismeréséhez való jog korlátozásának lehetőségével.[13]

Alágazatonként megvizsgáljuk az interneten fellelhető információk körét, illetve kitérünk a jövő fejlesztései tekintetében az autonóm közlekedés védelmi kérdéseire is. A vizsgálatot követően következtetéseket vonunk le és javaslatokat teszünk a nyitott kérdésekre. A fő probléma mellett vizsgáljuk azt is, hogy a GDPR milyen formában jelenik meg ágazatonként, valamint gyakorol-e hatást a kiberbiztonság vonatkozásban. Mielőtt a főbb kérdéseket kifejtenénk, mindenképpen tisztázni kell a közlekedéssel összefüggő adatok megjelenési formáját, valamint azt, hogy mi a terrorizmus.

Terrorizmus

A terrorizmusnak jelenleg nincs egységes definíciója, meghatározására több szakértő és nemzetközi szervezet is kísérletet tett. A NATO szerint a terrorizmus „*Félelmet vagy rettegést keltő erő vagy erőszak törvénytelen használata vagy azok használatával való fenyegetés személyek vagy tulajdon ellen, kormányok vagy társadalmak kényszerítésére vagy megfélemlítésére, vagy egy népesség felett az irányítás átvételére történő kísérlet során, politikai, vallási vagy ideológiai célok elérése érdekében.*" Fontos kiemelni azt is, hogy az információs terrorizmus eszköztára csak komplex előre tervezett módon használható, ami egyben a terrorista tevékenység egyik jellemzője, azaz a terrorizmus az erőszak szándékos és módszeres használata, általában (közvetlenül vagy közvetetten) személyek ellen. A terroristák erőszakos eszközökkel (robbantással, fegyveres erőszakkal stb.) küzdenek céljaik megvalósításáért. Mivel a célok általában nem valósulhatnak meg azonnal (pl. a fennálló politikai rend megdöntése, egy nép függetlenségének megteremtése), a terroristák általában több erőszakos cselekményt is elkövetnek előre megtervezett módon.[14]

---

[10] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. 3. § 5. és 6. pont. https://net.jogtar.hu/jogszabaly?docid=a1100112.tv; letöltés: 2021.04.25.

[11] Például MÁV-START Zrt. – Közérdekű adatok. https://www.mavcsoport.hu/mav-start/bemutatkozas/kozerdeku-adatok; letöltés: 2021.04.25.

[12] Infotv. 27. § (1)–(2).

[13] Például a minősített adatra hivatkozás, illetve a közérdekű, valamint közérdekből nyilvános adatok megismeréséhez való jog törvény általi korlátozása honvédelmi, nemzetbiztonsági érdekre, illetve bűncselekmények üldözése vagy megelőzése érdekére hivatkozással. KOVÁCS Ágnes Lilla: Rések a pajzson. Ludovika Egyetemi Kiadó, 2021.03.22. https://www.ludovika.hu/magazin/aula/2021/03/22/resek-a-pajzson/; letöltés: 2021.04.25.

[14] SERBAKOV Márton Tibor: A terrorizmus definíciójának kérdése. Büntetőjogi Szemle, 2019/2. szám. p. 94. https://ujbtk.hu/wp-content/uploads/lapszam/BJSz_201902_87-100o_SerbakovMarton.pdf; letöltés: 2021.03.24.

Függetlenül attól, hogy a terrorizmust elsősorban büntetőjogi (európai felfogás), vagy büntetőjogi és politikai kategóriaként (amerikai felfogás) értelmezzük,[15] a gyakorlati szakembereknek foglalkozniuk kell a létfontosságú rendszerelemek terrortámadások elleni védelmével. A 2021. január végén megjelent ENSZ-jelentés[16] is alátámasztja, hogy az ISIL/Daesh terrorszervezet – a közel-keleti területei veszteségei ellenére – visszanyerheti képességét a terrorcselekmények végrehajtására, amelyek közt véleményünk szerint számításba kell venni a különböző információs és közlekedési rendszerek, infrastruktúrák elleni lehetséges támadásokat is.

A terroristák akkor érik el leginkább a céljukat, ha a lehető legkisebb ráfordítással okoznak kárt, illetve váltanak ki nagy sajtóvisszhangot, politikai hatást. A terrorizmusra adott különböző definíciók azonban nem mindig adnak eligazítást a témánkat érintő veszélyekkel összefüggésben, viszont megfelelő kockázatelemzéssel rámutathatunk az adott rendszerek sebezhetőségeire.

Meg kell azonban jegyezni, hogy az utóbbi néhány év tapasztalatai azt mutatják, hogy az iszlamista terrorszervezetek egyre kevésbé képesek európai támadások közvetlen koordinálására, irányítására ezért kénytelenek megelégedni azzal, hogy a propagandájuk által inspirált elkövetők önállóan hajtják végre a támadásokat. A kiberterrorizmus napjaink egyik legfenyegetőbb tevékenysége. Sajátossága, hogy egyszerre használja az információs infrastruktúrát célpontként, valamint végrehajtási eszközként,[17] illetve közvetítő elemként az egyes lehetséges támadások elkövetéséhez szükséges adatok forrásához.

Bár a hatóságok általában kevés információt szivárogtattak ki, feltételezhetjük, hogy a nyugat-európai elkövetők többsége radikális iszlám nézeteket vallott. Másik közös tulajdonságuk az volt, hogy – a 2020. novemberi bécsi támadástól,[18] valamint a franciaországi[19] és a németországi[20] autós incidensektől eltekintve – igyekeztek egyszerű, szúró- vagy vágóeszközöket használni.

Mi a terrorizmus? Biztonságpolitikai Szemle, Corvinák, Terrorizmus – 2. Új típusú biztonsági kihívások. https://web.archive.org/web/20160417115546/http://biztpol.corvinusembassy.com/?module=corvinak&module_id=4&cid=32; letöltés: 2021.04.25.

[15] TÁLAS Péter: A nemzetközi terrorizmus és a szervezett bűnözés hatása a nemzetközi biztonságra és Magyarország biztonságára. Budapest, 2007. p. 6. http://kisebbsegkutato.tk.mta.hu/uploads/files/archive/904.pdf; letöltés: 2021.03.24.

[16] Twelfth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat. United Nations Security Council, 29 January 2021. https://undocs.org/en/S/2021/98; letöltés: 2021.03.24.

[17] PAPP Zoltán István: A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái. Doktori (PhD) értekezés. NKE, Katonai Műszaki Doktori Iskola, Budapest, 2018. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/Papp_Zoltan_PhD_ertekezes_tervezete.pdf; letöltés: 2021.04.25.

[18] November 2-án Kujtim Fejzulai, 20 éves észak-macedón–osztrák kettős állampolgár gépkarabéllyal és kézi lőfegyverekkel támadt járókelőkre Bécsben. A merényletnek négy halálos áldozata és 22 sérültje volt. A támadót a hatóságok lelőtték.
SCHUETZE, Christopher F. – EDDY, Melissa – BENNHOLD, Katrin – KOETTL, Christoph: Terrorist Shooting in Capital of Austria. The New York Times, 2020.11.03. https://www.nytimes.com/2020/11/02/world/europe/vienna-shooting.html; letöltés: 2021.04.07.

[19] Április 27-én Colombes városában a 29 éves Youssef Tihlah gépjárművel szándékosan ütött el rendőröket. A támadásban hárman megsérültek, az elkövetőt a rendőrség előállította. Az elkövető Franciaországban született, hűséget esküdött az ISIL/Daesh-nek.

Az áldozatok száma általában alacsony volt, ami egyrészt a választott eszközöknek volt köszönhető, másrészt pedig a koronavírus-járvány miatt bevezetett korlátozások miatt alkalom sem nagyon nyílhatott a tömeges méretű merényletek elkövetésére.

A nyugati – például a francia, az osztrák – kormányok kénytelenek újszerű intézkedéseket alkalmazni és a régi jogszabályokat módosítani, hogy az iszlamista fenyegetésnek elejét vegyék. Ilyen terület az információbiztonság és a létfontosságú rendszerelemek védelme is, ugyanis feltételeznünk kell, hogy a terrorszervezetek tagjai vagy követői rendelkeznek olyan mélységű technikai, távközlési, informatikai tudással, hogy anyagi kárt tudjanak okozni egyes tömegesen alkalmazott eszközökben.

Végeredményben a kibertérben elkövetett támadásoknak lehet a legtöbb kárvallottjuk vagy áldozatuk, és könnyen belátható a terrorszervezetek ilyen irányú képességek megteremtésére irányuló érdeklődése. Ami az ISIL/Daesh-t illeti, ez a terrorszervezet feltehetően rendelkezik bizonyos kiberképességekkel és olyan követői bázissal, amely igyekszik a legújabb informatikai eszközök, szoftverek megszerzésére, valamint a kellő tudás elsajátítására.

Fokozott veszélynek vannak kitéve a tömegközlekedési eszközök – így a vasúthálózat – is, amelyek megtámadása viszonylag kis ráfordítással véghez vihető, az okozott kár mértéke viszont jelentős. A 2004. márciusi madridi terrortámadások során a terroristák például négy vonatszerelvényen robbantottak, aminek következtében 191 ember meghalt és több mint 1500 megsebesült.[21]

Könnyen belátható, hogy az ismertetett sérülékenységek, illetve potenciális terrorista eljárások kockázati tényezők, mert a terrorszervezetek olyan „szakértőket" is toborozhatnak és inspirálhatnak, akik képesek és készek az egyszerű késeléseknél összetettebb, magasabb nehézségi fokú merényletek elkövetésére is. A toborzás, illetve a szélsőséges eszmék, valamint az elkövetés módja terjesztésének a legegyszerűbb és legelterjedtebb módszere a különböző közösségi médiafelületek használata, amelyek tökéletes ellenőrzésére a hatóságok még mindig nem képesek.

A közlekedéssel összefüggő adatok és megjelenésük

Az interneten gyakorlatilag számos olyan nyílt információ beszerezhető, amely segítséget nyújthat erőszakos cselekmények kivitelezéséhez. A nyugati társadalmak információszabadsága még a terrorszervezetek számára is rengeteg információt nyújt a házilag elkészíthető robbanóeszközöktől az egészen érzékeny információkig.[22]

ALLEN, Peter: 'I did it for ISIS': Terror suspect crushes two police motorcyclists with his BMW in Paris leaving one in a coma. MailOnline, 2020.04.27. https://www.dailymail.co.uk/news/article-8262853/I-did-ISIS-Terror-suspect-crushes-two-police-motorcyclists-Paris.html; letöltés: 2021.04.25.

[20] Augusztus 18-án egy 30 éves iraki férfi szándékosan hajtott bele személygépjárművel az autópályán közlekedő motoros járőrökbe. A merénylet során hat személy sebesült meg. Az elkövető az „Allah Akbar" felkiáltással szállt ki a gépjárműből. Berlin motorway crashes probed as terror attack. BBC News, 2020.08.19. https://www.bbc.com/news/world-europe-53832113; letöltés: 2021.04.12.

[21] The worst Islamist attack in European history. The Guardian, 2007.10.31. https://www.theguardian.com/world/2007/oct/31/spain; letöltés: 2021.04.12.

[22] KOVÁCS László: Az információs terrorizmus eszköztára. Robothadviselés 6. tudományos szakmai konferencia, 2006. november 22. Hadmérnök, Különszám, 2006. http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.pdf; letöltés: 2021.03.08.

Természetesen az internet nemcsak az adatszerzést könnyíti és gyorsítja meg, hanem rajta keresztül is el lehet követni műveleteket. Ez maga a klasszikus értelemben vett kiberterrorizmus vagy információs terrorizmus, amikor az elkövetők olyan számítógépes rendszereket támadnak meg, amelyek valamilyen létfontosságú rendszert irányítanak. Professzor Dr. Kovács László *A kibertér védelme* című könyvében a kiberterrorizmust és annak kérdéseit részleteiben is tárgyalja.[23]

A közlekedési rendszer ellen tervezett terrorakciók előkészítése során fontos lehet műszaki és személyes adatok megszerzése. Ezek tájékoztatást nyújthatnak egy adott infrastruktúra-elem szerkezetéről és építéséről,[24] valamint forgalmáról, amelyekből a szükséges robbanóanyag összetétele és mennyisége kiszámítható. Az említett példában szereplő Kőröshegyi völgyhíd honlapján megtalálhatók például a völgyhíd pilléreinek magasságai és távolságuk egymástól, illetve számos fotó az építményről. Ezek az adatok megfelelőek lehetnek a terroristák számára, ugyanakkor a kérdés az, hogy relevánsak-e a lakosság részére. Főleg, hogy ezek a paraméterek a laikus érdeklődőknek nem jelentenek lényegi információkat, így ezek feltüntetésének nincs is gyakorlatilag relevanciája.

A közlekedési infrastruktúrák elleni terrorakciók sikeres végrehajtásához leginkább olyan adatok megszerzése lehet fontos, amelyek alapján eldönthető, hogy egy adott infrastruktúra-elem vagy az azt használó közlekedési eszköz ellen mikor érdemes a támadást végrehajtani. Az ilyen jellegű információkat vizsgálatunk szempontjából alapvetően két csoportba érdemes sorolni:

– üzemi adatok: az infrastruktúra kezelőjének vagy az adott infrastruktúrát használó közlekedési vállalatok belső információi;

– ügyféladatok: olyan információk, amelyek az adott közlekedési alágazatot igénybe vevő ügyfelek (pl. utasok) részére adnak tájékoztatást.

A következőkben valamennyi közlekedési alágazat estében megvizsgáljuk az üzemi és az ügyféladatok megismerésének veszélyeit.

A közlekedéstervezés elve

A közlekedéstervezés egyik alapkérdése a megfelelő kapacitás biztosítása, azaz hogy a jelentkező mobilitási igényeket a közlekedési infrastruktúra és a személyközlekedési szolgáltatók ki tudják elégíteni. Ennek felmérésére általában keresztmetszeti vagy célforgalmi felméréseket használnak.

A keresztmetszeti felmérés azt mutatja meg, hogy az infrastruktúra egy adott pontján hány közlekedő[25] halad keresztül. A célforgalmi felmérés az utazások kiinduló és végpontját rögzíti, így megmondja, hogy az utazás mely körzetek között bonyolódik le, ugyanakkor nem ad felvilágosítást a használt útvonalról, pedig a

[23] KOVÁCS László: A kibertér védelme. Dialóg Campus Kiadó, Budapest, 2018. pp. 197–203. https://www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf; letöltés: 2021.04.25.

[24] Például a Kőröshegyi völgyhídnak a Wikipédián saját oldala van: Kőröshegyi völgyhíd. Wikipédia, 2021.02.24. https://hu.wikipedia.org/wiki/K%C5%91r%C3%B6shegyi_v%C3%B6lgyh%C3%ADd; letöltés: 2021.04.25.

[25] Jármű, kerékpáros vagy gyalogos stb.

kapacitástervezés során ez is legalább annyira fontos kérdés, mint a honnan-hova forgalom felvétele.

Ma már mindkét felmérés lebonyolítható a mobiltelefonok cellainformációinak felhasználásával, hiszen majdnem mindenkinek van már ilyen készüléke, és annak működéséhez szükséges, hogy a telefonközpont folyamatosan ismerje, hogy az egyes készülékek melyik körzetben vannak. Ez a tulajdonság lehetővé teszi, hogy meghatározzák az egyes készülékek útjait, amelyek természetesen azonosak a készülék birtokosának az útjaival.[26] A mozgási jellemzők alapján a közlekedési mód és az utazásra vonatkozó egyéb információk is kinyerhetők. Az teljesen egyértelmű, hogy ilyen adatok nyílt hálózaton való tárolása nem célszerű. A módszer alkalmazása véleményünk szerint további adatvédelmi kérdéseket is felvet, ezért szükségesnek tartjuk az így kinyerhető utazási információk GDPR-alapú vizsgálatát.

A szükséges adatok forrásai

Az előző pontokban vizsgáltuk, hogy milyen adatok rendelkezésre állására lehet szükség ártó szándékú cselekedetek tervezéséhez és elkövetéséhez. Ebben a pontban az vizsgáljuk, hogy ezek az adatok honnan szerezhetők be.

Elsőként említhetők az egyes közlekedési infrastruktúrák saját elektronikus felületei. Például a zürichi főpályaudvar honlapján[27] számos műszaki adat elérhető, amelyek kiindulási pontként használhatók.[28] Ugyancsak idetartoznak azok a weboldalak, amelyek ugyan nem hivatalos oldalak, nem is szakemberek írják ezeket, ugyanakkor a közölt információk elegendő tartalommal bírhatnak. Az ilyen közösségi szerkesztésű oldalak egyik hátránya, hogy nem ellenőrzött információkat is tartalmazhatnak.[29] Ugyancsak itt kell megemlíteni az olyan közösségi oldalakat, amelyek sokat tesznek a közérdekű adatok nyilvánosságáért.

Másodikként említhetők a különböző szolgáltatók saját honlapjai.[30] Ezeken az oldalakon is sok információ található, olykor olyan üzemi információk is, amelyeket véleményünk szerint nem célszerű nyilvánosságra hozni.

Harmadik nagy csoport azok halmaza, akik üzleti lehetőséget látnak a közlekedési adatok értékesítésében, például útvonaltervezési, illetve -fejlesztési célok érdekében (optimális útvonalak, multieszközös utazások, dugók elkerülése,[31] infrastruktúra-bővítési szükséglet feltérképezése stb.), és ennek érdekében építenek

---

[26] DING-BING, Lin – RONG-TERNG, Juang – HSIN-PIAO, Lin: Mobile location estimation and tracking for GSM systems. 2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications, 5-8 Sept. 2004. https://ieeexplore.ieee.org/document/1368838; letöltés: 2021.04.25.

[27] ShopVille-Zürich Hauptbahnhof – herzlich willkommen. https://www.sbb.ch/de/bahnhof-services/am-bahnhof/bahnhoefe/shopville-zuerich-hauptbahnhof.html; letöltés: 2021.04.25.

[28] A példaként hozott zürichi főpályaudvari bevásárlóközpont honlapján látható az üzletközpont kihasználtsága.

[29] Lásd a Kőröshegyi völgyhíd oldalát a Wikipédián.

[30] Például MÁV-START Zrt. – Közérdekű adatok. https://www.mavcsoport.hu/mav-start/bemutatkozas/kozerdeku-adatok; letöltés: 2021.04.25.

[31] CHAPPLE, Theo: Reducing congestion at Blackwall Tunnel with Waze. Digital Blog, 2018.01.11. https://blog.tfl.gov.uk/2018/01/11/waze-partnership-reducing-congestion-at-blackwall-tunnel/; letöltés: 2021.04.25.

nagyméretű adatbázisokat (BigData[32] adatbázisokat, például MaaS[33] szolgáltatás igénybevételéhez).

A közlekedési rendszer működését számos szakkönyv, -cikk, tanulmány, diploma- és PhD-dolgozat is vizsgálja és elemzi, bemutatva a hiányosságokat és a gyenge pontokat. Az írásművek döntő többsége felkerül az internetre, azok mindenki számára hozzáférhetővé válnak. Ezekből szintén olyan információk tudhatók meg, amelyek segíthetik az ártó szándékú műveletek előkészítését. Fel kell tenni a kérdést, hogy a kutathatóság vagy a biztonság élvez-e előnyt a fontos információk közzétételét illetően. Természetesen igaz ez a könyvtárakban elérhető szakirodalmi forrásokra is.

A közlekedéssel kapcsolatos nyilvános adatok

Az információszabadság alapvető jog, amelyről az Európa Unió Alapjogi Chartája[34] is rendelkezik. Eszerint „*mindenkinek joga van a véleménynyilvánítás szabadságához. Ez a jog magában foglalja a véleményalkotás szabadságát, valamint az információk és eszmék megismerésének és közlésének szabadságát anélkül, hogy ebbe hatósági szerv beavatkozhatna, továbbá országhatárokra való tekintet nélkül.*”[35]

Az Alaptörvény[36] szerint mindenkinek joga van közérdekű adatok megismeréséhez és terjesztéséhez, az Inftotv.[37] alapján pedig a közfeladatot ellátó szervnek lehetővé kell tennie, hogy a kezelésében lévő közérdekű adatot és közérdekből nyilvános adatot erre irányuló igény alapján bárki megismerhesse. A „bárki” ebben az esetben azt jelenti, hogy az adatigénylőnek nem szükséges igazolni személyazonosságát[38] és az adatigénylés célját, valamint a közérdekű, illetve közérdekből nyilvános adat felhasználása sem korlátozható „indokolatlanul”.

---

[32] A BigData fogalma alatt azt a bonyolult technológiai környezetet értjük, amely lehetővé teszi olyan összetett adatbázisok feldolgozását, amelyek annyira nagyméretűek és annyira komplexek, hogy feldolgozásuk a meglévő adatbázis-menedzsment eszközökkel jelenleg nehézségekbe ütközik.

[33] Mobility-as-a-Service – a koncepció célja, hogy ne az felhasználóknak kelljen igazodniuk a közlekedési szolgáltatók termékeihez, hanem a kínálat igazodjon az emberekhez, mindig az aktuális igényeket legjobban kiszolgálva.
GOODALL, Warwick – FISHMAN, Tiffany Dovey – BORNSTEIN, Justine – BONTHRON, Brett: The rise of mobility as a service – Reshaping how urbanites get around. Deloitte Review, Issue 20, 2017. pp. 113–129. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/consumer-business/deloitte-nl-cb-ths-rise-of-mobility-as-a-service.pdf; letöltés: 2021.04.25.

[34] Az Európai Unió Alapjogi Chartája. Az Európai Unió Hivatalos Lapja, 2016.06.07. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN; letöltés: 2021.04.25.

[35] Uo. 11. Cikk. C 202/396.

[36] Magyarország Alaptörvénye (2011. április 25.). VI. cikk (3) bekezdés. https://net.jogtar.hu/jogszabaly?docid=a1100425.atv; letöltés: 2021.04.25.

[37] Infotv. 26. § (1) bekezdés.

[38] Infotv. 28. § (2) bekezdés.
„Ha törvény másként nem rendelkezik, az adatigénylő személyes adatai csak annyiban kezelhetők, amennyiben az az igény teljesítéséhez, az igénynek a 29. § (1a) bekezdésében meghatározott szempont alapján való vizsgálatához, illetve az igény teljesítéséért megállapított költségtérítés megfizetéséhez szükséges. A 29. § (1a) bekezdésében meghatározott idő elteltét, illetve a költségek megfizetését követően az igénylő személyes adatait haladéktalanul törölni kell.”

Az információszabadság azonban nem abszolút jog, maga az Infotv. határozza meg a kivételeket, amelyek korlátozhatják azt.[39] A törvény azt is kimondja, hogy a nyilvánosságra hozatal nem eredményezheti a hozzáférést olyan adatokhoz – például különösen a védett ismerethez –, amelyek megismerése az üzleti tevékenység végzése szempontjából aránytalan sérelmet okozna, feltéve, hogy ez nem akadályozza meg a közérdekből nyilvános adat megismerésének lehetőségét.[40] Az előbbiekben említett elgondolás vonalán jött létre cikkünk is, mivel jelenleg csak ez az egy lehetőségünk van arra, hogy az információs terrorizmus információszerző műveleteit meg lehessen akadályozni. Azaz vizsgálni kell azt, hogy az egyes közérdekű adatok önállóan vagy valamilyen tematika alapján végrehajtott gyűjtése, elemzése is jelenthet nemzetbiztonsági kockázatot.

A közlekedéssel kapcsolatos nyilvános adatok és a GDPR

Az is az információszabadság korlátjai közé sorolható, hogy a közérdekből nyilvános adat újrafelhasználása során a GDPR szabályait figyelembe kell venni.

Jelen esetben tehát a közfeladatot ellátó szervezetek[41] feladata, hogy mérlegeljék:

– mely közérdekű és közérdekből nyilvános adatokat kell kiadniuk az információszabadság alapján;

– mely adatok esetében tudják mentességre hivatkozással az adatkiadást megtagadni; illetve

– amennyiben a nemzetközi gyakorlat azt mutatja, hogy bizonyos adatkategóriáknak a védendő adatok között kellene szerepelniük, de a hazai jogszabályi környezetben jelenleg nem tartoznak ebbe a körbe, abban az esetben a felügyeleti szervüknél kezdeményezzék az ehhez szükséges jogszabály-módosítást.

Amennyiben a közérdekű adat megismerése iránti igény teljesítését a közfeladatot ellátó szerv arra hivatkozva tagadja meg,[42] hogy a közérdekű vagy közérdekből nyilvános adat azért nem ismerhető meg, mert az a minősített adat védelméről szóló törvény szerinti minősített adat, abban az esetben az adatot igénylő jogosult bírósághoz fordulni.[43] Az eljárás során a bíróság az Adatvédelmi és Információszabadság Hatóság titokfelügyeleti hatósági eljárását[44] kezdeményezi, egyidejűleg a peres eljárást felfüggeszti.

---

[39] Például minősített adat, nemzetbiztonsági érdek stb.

[40] Infotv. 27. § (3) bekezdés.

[41] Például a közlekedést biztosító, a közlekedéssel kapcsolatban szolgáltatást nyújtó, infrastruktúrát üzemeltető.

[42] Klasszikus értelemben véve az adatok felülminősítése.

[43] Infotv. 31. § (6a) bekezdés.

[44] Intotv. 62. § (1) bekezdés.
„Ha a Hatóság vizsgálata alapján vagy egyébként valószínűsíthető, hogy a nemzeti minősített adat minősítése jogellenes, a Hatóság titokfelügyeleti hatósági eljárást indíthat."
A titokfelügyeleti eljárás részletszabályait az Infotv. 62–63. § tartalmazza.

Itt mindenképpen meg kell jegyezni azt is, hogy nem feltétlenül részeiben kell vizsgálni az egyes publikált közérdekű információdarabokat. A szolgáltatóknak mindenképpen célszerű komplex módon vizsgálni azt, hogy az interneten több helyen kipublikált adatokat együttesen milyen kockázatot jelentenek.

Személyes adatok védelme

A fentiek mellett fontos megjegyezni azt, hogy a közlekedési rendszerek fejlesztése alapvetően és meghatározóan ma már a nagy mennyiségű személyes adat felhasználására, elemzésére és értékelésére épül. A tömegközlekedési rendszerek, a légitársaságok, a gépjárműgyártók, a szállítmányozásban érdekelt hatóságok és egyéb szerveztek, a közlekedésben érdekelt nemzetközi szereplők, mint az Uber és a Lyft a fejlesztések és (szolgáltatás-) elemzések során egyértelműen kezelnek személyes adatokat, amelyek az Unióban a GDPR hatálya alá tartoznak.

Ezek az adatok a klasszikus esetekben az utazó neve, a kapcsolattartáshoz szükséges információk, mint például elektronikus levelezési cím, postacím vagy telefonszám. Ezen adatok mellett természetesen tárolnak még olyan statisztikai adatokat, amelyek a kutatásokhoz és a fejlesztésekhez szükségesek, mint például visszatérő utazók esetében az utazás gyakorisága, a jegyárak és előfizetések (bérletek), valamint a kedvezményes vásárlások statisztikai mutatói.

A személyes adatok kezelése során az adatkezelőknek (pl. a közlekedési és a telekommunikációs szolgáltatóknak) figyelembe kell venniük azt is, hogy egyes estekben a nem klasszikus értelemben vett személyes adatok is átformálódhatnak olyan adatokká, amelyekből következtethetünk személyekre,[45] azaz a személyek azonosíthatók (pl. rendszám, IP-cím, lokációs adatok stb.). Sőt, egy kutatás arra az eredményre jutott, hogy négy térbeli-időbeli pont elegendő a személyek 95%-ának egyedi azonosításához.[46]

Támadási kategóriák

Az ágazati bontás elvégzése előtt fontos rendszerezni azt, hogy milyen fenyegetettségi kategóriákat lehet azonosítani, amelyek érintik az intelligens közlekedési rendszereket.

Segítségül hívhatjuk például az ENISA[47] dokumentumait, ezek közül több is foglalkozik az intelligens közlekedési rendszerekkel és azok fenyegetettségével:

---

[45] Personal data in transport: exploring a framework for the future. Open Data Institute, 2018. https://theodi.org/wp-content/uploads/2018/06/OPEN-Personal-data-in-transport-.pdf; letöltés: 2021.04.25.

[46] DE MONTJOYE, Yves-Alexandre – HIDALGO, César A. – VERLEYSEN, Michel – BLONDEL, Vincent D.: Unique in the Crowd: The privacy boundsof human mobility. Scientific Reports, 2013.03.25. https://www.nature.com/articles/srep01376.pdf; letöltés: 2021.04.25.

[47] Európai Uniós Kiberbiztonsági Ügynökség – European Union Agency for Cybersecurity. (A 2004-es megalakulásakor kapott elnevezése European Network and Information Security Agency.) Az ENISA a hálózat- és információbiztonság európai szakértői központjaként működik. Feladata, hogy a hálózat- és információbiztonság területén jelentkező új kihívások előrejelzése és az európai országok támogatása abban, hogy – a digitális környezetben bekövetkezett fejleményeket is szem előtt tartva – sikeresen kezeljék ezeket a kihívásokat.

– intelligens közforgalmú közlekedési rendszerek;[48]
– intelligens repülőterek;[49]
– alacsonyabb szinten automatizált okosjárművek;[50]
– magas szinten automatizált okosjárművek;[51]
– okosjárművek mesterséges intelligenciával kapcsolatos kihívásai.[52]

Az ENISA[53] szerint az intelligens közforgalmú közlekedéssel (IPT[54]) kapcsolatban hét támadási kategóriát célszerű számba venni:

1. Nagyméretű és széles spektrumú támadást, amelynek célja a nagyméretű fizikai pusztítás. A teljes közlekedési IT-infrastruktúra bénítása és rombolása, amelynek következtében a szolgáltatás teljes leállása vagy megbénulása várható.
2. Olyan ember vagy természet okozta természeti katasztrófa, amely a közlekedést támogató ICT[55]-hálózat kiesését okozza, megbénítva ezzel a közlekedési rendszert.
3. Konfigurációs vagy a rendszerelemek meghibásodásából származó károk, ami miatt az ITxPT[56] rendszer megbénul.
4. Jelentős minőségromlás, ami már akadályozza az üzemszerű működést.
5. Olyan kibertámadás, amely folyamán visszaéléssel vagy káros informatikai tevékenységgel célirányosan rombolják az infrastruktúrát.
6. A nem szándékos károkozás, amely anyagi vagy személyei károkat okoz.
7. Szabotázs, amely során egy belső munkatárs – aki hozzáfér érzékeny adatokhoz – személyes ellenérdekeltségű motivációtól vezérelve rombolja vagy bénítja a közlekedési rendszer IT-infrastruktúráját (ilyen esemény magyar vonatkozásban még nem történt).

---

[48] Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations. ENISA, December 2015. https://www.enisa.europa.eu/publications/good-practices-recommendations; letöltés: 2021.04.29.
[49] Securing Smart Airports. ENISA, December 2016. https://www.enisa.europa.eu/publications/securing-smart-airports; letöltés: 2021.04.29.
[50] Cyber Security and Resilience of smart cars. Good practices and recommendations. ENISA, December 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars; letöltés: 2021.04.29.
[51] ENISA Good Practices For Security Of Smart Cars. ENISA, November 2019. https://www.enisa.europa.eu/publications/smart-cars; letöltés: 2021.04.29.
[52] Cybersecurity Challenges In The Uptake Of Artificial Intelligence in Autonomous Driving. ENISA, February 2021. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving; letöltés: 2021.04.29.
[53] Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations. ENISA, December 2015. https://www.enisa.europa.eu/publications/good-practices-recommendations; letöltés: 2021.04.29.
[54] Intelligent Public Transport.
[55] Information and Communications Technology.
[56] Information Technology for Public Transport.

Az informatikai és a kiberbiztonság vonatkozásában az ENISA az alábbi külső és belső tényezőket azonosítja.[57] Ezekből véleményünk szerint szűkítve és kiegészítve az alábbiak a legjelentősebbek:

Külső kockázat:

1. Olyan elosztott túlterheléses támadás, amely megbénítja a közlekedési eszközök vezérlő- és irányítórendszerét, valamint a közlekedésmenedzsmentet támogató informatikai infrastruktúrát.
2. Hardverek és szoftverek manipulációja, ami közvetlenül érinti a közlekedési infrastruktúrát.
3. Az utas- és közlekedésbiztonságot érintő adatok módosítása és manipulálása.
4. Illetéktelen behatolás a közlekedés során használt vezeték nélküli rendszerekbe, amelynek során az utasok személyes adatai kerülnek illetéktelenek kezébe.
5. Az utasok személyes adatait érintő adatszivárgás.
6. Közösségi médiakampány negatív manipulációja.
7. Ellenérdekeltségű szervezet vagy csoportosulás közösségi médiában indított lejáratő kampánya.
8. Ellenérdekeltségű ország vagy szervezet lejáratő kampánya, aminek célja az aktuális kormány reputációjának rombolása.
9. Visszaélés az utazók személyes adataival.

Belső kockázat:

1. Belső munkatárs sértettségből adódó adatszivárogtatása.
2. Közlekedési irányítórendszer téves konfigurációja.
3. Gondatlanság vagy vétlen emberi mulasztás.

Az ENISA az IPT-rendszerekkel kapcsolatos kihívások felsorolásában kiemelt figyelmet szentel a biztonságnak és a kiberfenyegetéseknek,[58] valamint résanalízissel is segíti a szakemberek munkáját és tanácsokat ad a jó gyakorlatokra is.[59]

Ágazati bontás

Közúti közlekedés

A Központi Statisztikai Hivatal 2013-ban publikált *A közúti közlekedés területi jellemzői* című kiadványa szerint az alsóbbrendű utak nagy sűrűségben és egyenletes lefedettséggel borítják az országot.[60] A mellékutak nagy szerepet töltenek be a

[57] Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations. ENISA, December 2015. p. 24. https://www.enisa.europa.eu/publications/good-practices-recommendations; letöltés: 2021.04.29.
[58] Uo. 3.4. Challenges, 5. Gap analysis.
[59] Uo. 4. Good practices for securing intelligent public transport.
[60] A közúti közlekedés területi jellemzői. Központi Statisztikai Hivatal, 2013. augusztus. p. 3. https://www.ksh.hu/docs/hun/xftp/idoszaki/regiok/debgyorkozutikozl.pdf; letöltés: 2021.04.25.

főúthálózat alternatívájaként, ugyanakkor az is igaz, hogy kapacitásuk jelentősen alacsonyabb a főutakénál.

Az ország útszerkezetét megvizsgálva elmondható, hogy a hazai úthálózat sűrűsége miatt egyes közúthálózati elemek kiesése nem okoz jelentős problémát, így a közúti infrastruktúra támadása önmagában nem hozhat jelentős eredményt, mert a legtöbb út és útvonal rendelkezik redundáns megoldással, ugyanakkor az infrastruktúrát igénybe vevőkről szerzett információk már hasznosak lehetnek. Ilyen lehet például az adott infrastruktúra-elem csúcsidei igénybevétele. A tervezett támadás akkor érhet el megfelelő hatást, ha a lehető legtöbb áldozatot szedi, vagyis amikor adott infrastruktúra-elemet egy időben a legtöbben használják. Az ilyen forgalmi adatok interneten történő megjelenítése ebből a szempontból veszélyes lehet, ugyanakkor ez terepszemlével is kitapasztalható. Az viszont már komoly „segítséget" jelenthet, hogy az adatokból leszűrhetők azok a helyszínek, ahol érdemes lehet terepszemlét tartani. Ezek az adatok alapvetően a felhasználók személyes adatai, mint például geolokációs adatok, valamint az ezen alapuló forgalmi statisztikai adatok.

Forgalmi adatok

A forgalmi adatoknál sokkal fontosabbak lehetnek a közúti forgalomirányítás adatai. A számítógép által vezérelt forgalomirányítás[61] biztosítja a közúti infrastruktúra működőképességét, a forgalomirányítás feletti hatalomátvétel pedig kiváltképp alkalmas lehet tömegbalesetek előidézésére és ezáltal jelentős méretű károkozásra. Általában elmondható, hogy a közúti közlekedési rendszernek képesnek kell lennie forgalomirányító lámpák nélküli működésre is. Minden esetben van olyan ismeretanyag,[62] amelyet alkalmazva a balesetek elkerülhetők, ugyanakkor a mai forgalomnagyság mellett ez állandó torlódásokhoz és így a közlekedési folyamatok jelentős lassulásához vezethet. A közúti áruszállítás során különösen a veszélyes anyagot vagy éppen katonai eszközöket szállító tehergépjárművek adatai lehetnek fontosak.

A közúti közforgalmú közlekedés témánk szempontjából releváns üzemi adatai az autóbuszok jármű-fordulóterve vagy a közlekedési jegyzék,[63] továbbá a terhelési és az operatív forgalomirányítás adatai.

A fordatervből megtudható, hogy adott jármű (ez minden nap másik lehet) a nap adott időpontjában melyik járatot teljesíti. Ez fontos lehet abból a szempontból, hogy a járművek a nap folyamán nemcsak egy viszonylaton közlekednek, hanem több járatot is kiszolgálnak.[64] Amennyiben a cél az, hogy a leginkább zsúfolt járat ellen történjen az akció, akkor a fordaadatok megszerzése feltétlenül szükséges.

---

[61] Például a közlekedési lámpák fázisprogramjai.

[62] 1/1975. (II. 5.) KPM-BM együttes rendelet a közúti közlekedés szabályairól (KRESZ). https://net.jogtar.hu/jogszabaly?docid=97500001.kpm; letöltés: 2021.04.25.

[63] Fordaterv – A forda a menetrendi járatokat autóbuszokra lebontva tartalmazza, a járatokat a járművekhez rendeli hozzá. Egy forda egy autóbusz egy napi programja, az autóbusz által ellátandó feladatokat tartalmazza.

[64] Ez leginkább kisebb városokban van így, de Budapesten is előfordul.

A terhelési adatok megmutatják, hogy adott járművön adott időben mennyien tartózkodnak. Az adatok megszerzése szintén az áldozatszám maximalizálása miatt fontos.

Látható tehát, hogy e két adat birtokában a városi és a helyközi közúti közösségi közlekedés ellen megfelelő „eredményű" terrorakció tervezhető.

A távolsági buszközlekedés esetén a terhelési adatok helyett az adott járatra eladott menetjegyek is sokatmondóak lehetnek, miután távolsági buszon álló utas nem lehet, így az eladott menetjegyek száma mutatják a járat terhelését.

Az operatív menetirányítás adatai a mindenkori aktuális forgalmi helyzetet tükrözik, így ezekből megállapítható, hogy adott jármű az útvonalán éppen hol tartózkodik. Ez az adat távirányítású robbantások esetén fontos, hogy a detonáció éppen a megfelelő helyen következzen be.

Az ügyféladatok tekintetében leginkább az utasinformációkat kell kiemelni. A menetrendi tervadatok megjelenítése az utazástervezés során nélkülözhetetlen, egy városi utazást is ma már meg kell tudni tervezni. A jelenkor utasát már nem az érdekli, hogy a busz 5–7 percenként közlekedik, hanem az, hogy mikor jön a következő járat, az utazástervező szoftverek és alkalmazások pedig már a mobiltelefon helykoordinátái alapján azonnal megmondják, hogy mikor jön a következő olyan járat, amelyikkel utazni szeretnénk.

A városi közlekedés sajátossága azonban, hogy nem egy kiemelt járat lehet zsúfolt (kivétel lehet egy műszakváltáskor adott üzembe közlekedő járat), hanem a csúcsidő több járata is, így nincs kiemelt szerepe egy adott viszonylat egy járatának. A valós idejű online adatok leginkább arra szolgálhatnak, hogy a robbanószerkezet működésbe hozatala a megfelelő helyen történjen meg.

A C-ITS[65] rendszerek, a kapcsolódó és az önvezető járművek

A gépjárműgyártás és -fejlesztés egyértelműen előnyben részesíti a kapcsolódó, illetve az önvezető járműveket. Az önvezető járművek elterjedéséhez elengedhetetlen a közlekedés résztvevői és az infrastruktúra közötti folyamatos és megfelelő sávszélességű, kis késleltetésű és biztonságos kommunikáció.

A kapcsolódó járműveken túlmutató önvezetőgépjármű-technológia már teljes egészében az informatikai megoldásokra épül a klasszikus értelemben vett gépjárműtechnológiai megoldások mellett. Alapvető különbség a kötött pályás közlekedéssel szemben, hogy a jármű kerekeit a vezető kormányozza, így a balesetek bekövetkezésének egy részéért ő a felelős. Az informatikai megoldásoknak ezt a felelősséget kell átvenniük, valamint tudniuk kell megakadályozni, hogy a jármű irányításához illetéktelenek hozzáférjenek.

C-ITS rendszerek

A közúti közlekedés területén soha nem látott forradalom előtt állunk, az intelligens közlekedési rendszerek egyre nagyobb teret hódítanak. A járművek nemcsak önmaguk okosodnak, hanem egymással és a közúti infrastruktúrával is interakcióba lépnek.

[65] Cooperative Intelligent Transport Systems.

Ez az együttműködő, intelligens közlekedési rendszerek világa, amely lehetővé teszi az úthasználók és a forgalomirányítók számára olyan információk megosztását és felhasználását, amelyek korábban még nem álltak rendelkezésre, és amelyek segítik a tevékenységük koordinálását is.

A C-ITS a hozzá fűzött remények alapján nemcsak ugrásszerűen javítja majd a közúti közlekedés biztonságát és a forgalomszervezés hatékonyságát, hanem a vezetési élményt is jelentősen növelheti, hiszen aktívan segíteni fogja a járművek vezetőit a döntéshozatalban és a forgalmi szituációkhoz történő gyors alkalmazkodásban.

A C-ITS-technológia lehetővé teszi a valós idejű információcserét a járművek,[66] illetve a járművek és az infrastruktúra[67] között, ez utóbbiba beletartozik a járművek kommunikációja a gyalogosokkal[68] és a hálózattal[69] is. A V2X-kommunikáció magában foglalja a V2V- és a V2I-kommunikációt is, ezáltal – elviekben – pontos és megbízható adatokat tud szolgáltatni az útviszonyokról, a gépjárművekről és azok helyzetéről. A rendszer előnye, hogy nemcsak a vezetőket tájékoztatja a forgalmi körülményekről, hanem a forgalomszervezés hatékonyságát is segíti, ez pedig akár a környezetterhelés (károsanyag-kibocsátás) drasztikus csökkentéséhez is vezethet.

A C-ITS lényege, hogy a gépjárművekbe telepített szenzorok és vezérlők adatokat gyűjtenek és elemeznek,[70] és ezek összesítése alapján képesek előre jelezni a forgalmi viszonyokat és a vészhelyzeteket. A járművek üzeneteket továbbítanak, azaz figyelmeztetést küldenek egymásnak a potenciális veszélyekről,[71] valamint kommunikálnak a közúti intelligens infrastruktúrával.[72] A gépjárművek és a forgalomirányító központok közötti kétirányú kommunikáció lehetővé teszi a gyors reagálást a problémákra – például forgalmi torlódásra vagy jeges útszakaszokra –, ezáltal mérsékli azok negatív hatását.

A jövő már elkezdődött. A Volkswagen például a Golf 8 modelljében a V2I már alapfelszerelés, több uniós tagállamban pedig megkezdték a C-ITS valós feltételek melletti kiépítését stratégiai szövetségek keretében – példa erre a Rotterdamot Frankfurttal és Béccsel összekötő uniós együttműködési folyosó, illetve az Amsterdam Group.[73] Az Európai Űrstratégia[74] is hangsúlyozza annak szükségességét, hogy az űrtechnológiákat az összekapcsolt személygépjárművekre vonatkozó stratégiákba integrálják, kiaknázva ezzel a Galileo és az EGNOS[75] navigációs rendszerek igénybevételének előnyeit.

---

66 Vehicle-to-Vehicle – V2V.
67 Vehicle-to-Infrastructure – V2I.
68 Vehicle-to-Pedestrian – V2P.
69 Vehicle-to-Network – V2N.
70 Sebesség, gumi tapadása, ablaktörlő sebessége.
71 Például vészfékezés, torlódások eleje és vége.
72 Például jelzőlámpákkal az optimális sebesség megválasztásához.
73 Amsterdam Group – A közúti közlekedési hatóságok (Díjas Autópályák, Hidak és Alagutak Koncessziós Társaságainak Európai Szövetsége [ASECAP]), a POLIS-ban (európai régiók és városok hálózata) részt vevő városok és a Car2Car kommunikációs konzorciumba szerveződött gépjárműipar.
74 Space Strategy for Europe, COM (2016) 705 final. https://stip.oecd.org/stip/policy-initiatives/2019%2Fdata%2FpolicyInitiatives%2F26561; letöltés: 2021.04.25.
75 European Geostationary Navigation Overlay Service.

Hazai szinten az M86-os út csornai elkerülő szakaszán a Budapesti Műszaki és Gazdaságtudományi Egyetem szakemberei osztrák közreműködéssel tesztelték a kooperatív közlekedés előnyeit 2020 júniusában, illetve a Magyar Közút Nonprofit Zrt. is belevágott a CROCODILE[76] korridorprojektbe, amelynek második szakaszában 13 helyszínen telepítettek C-ITS rádiós adó-vevő berendezéseket.

A hazai közútfejlesztések célja, hogy 2022-ig letegyék az alapjait egy olyan kétszintű forgalmimenedzsment-központnak, amely adatvezérelt döntéstámogatói rendszereinek köszönhetően proaktív módon lesz képes működni, és a Nemzeti Adathozzáférési Ponton (NAP) keresztül megosztott adatok segítségével a digitális térképeket és utastájékoztatókat készítő szolgáltatók is magasabb színvonalon lesznek képesek szolgáltatni.

Az új technológia azonban új kihívások elé állítja nemcsak az adatvédelmet, hanem a biztonsági szakértőket is.

A C-ITS folyamatos adatszóráson alapul, *ad-hoc* kommunikációkat hoz létre és nem igényli a felhasználók közötti állandó kommunikáció vagy kapcsolatok meglétét. A rendszer keretében kétfajta üzenet továbbítására kerül sor:

– kooperatív figyelemfelhívó üzenetek (CAM[77]), amelyek szórása folyamatos, és kinematikai, valamint a jármű méretére vonatkozó adatokat tartalmaznak;

– decentralizált környezeti értesítő üzenetek (DENM[78]), amelyek a CAM kiegészítéseként csak speciális, vészhelyzetnek számító események (pl. balesetek) esetén kerülnek továbbításra, és ezen esemény helyszínére vonatkozó helymeghatározó adatokat tartalmaznak.

Ezek az üzenetek titkosított aláírásokat tartalmaznak, így garantálva a fogadó fél számára, hogy az üzenetek megbízható forrásból származnak. A tanúsítványok felhasználók közötti kiosztása egy nyilvános kulcsokra épülő infrastruktúra-alapú architektúrával történik, ez alapján adott időben minden egyes tanúsítvány egyetlen gépjárműhöz van hozzárendelve.[79]

A járművek között továbbított üzenetek személyes adatok, mivel:

– a PKI[80] által kibocsátott engedélyezési tanúsítványokat tartalmaznak, amelyek kizárólag a feladóhoz vannak társítva;

– fejlécet, időbélyeget, helymeghatározó adatokat és a járműre vonatkozó méretadatokat rögzítenek.[81]

---

[76] Cooperation of Road Operators for Consistent and Dynamic Information Level – útkezelők együttműködése a következetes és dinamikus információáramlás érdekében.

[77] Cooperative Awareness Message.

[78] Decentralized Environmental Notification Message.

[79] SANTAA, José – PEREÑÍGUEZA, Fernando – MORAGÓNA, Antonio– SKARMETAA, Antonio F.: Experimental Evaluation of CAM and DENM Messaging Services in Vehicular Communications. Transportation Research Part C: Emerging Technologies, Volume 46, September 2014. pp. 98–120.

[80] Public Key Infrastructure – nyilvános kulcsú infrastruktúra.

[81] 03/2017. számú vélemény a személyes adatok kooperatív intelligens közlekedési rendszerek (C-ITS) keretében történő kezeléséről. WP 252. A 29. cikk szerinti Adatvédelmi Munkacsoport, 2017.10.04. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171; letöltés: 2021.04.25.

Ezek az adatok álnevesített adatoknak tekinthetők, mivel az azonosításhoz szükséges információk az adatok felhasználójához nem kerülnek továbbításra, ezeket a tanúsító hatóságok tárolják.

Az Európa Bizottság 2016-ban kifejezte aggodalmát az intelligens rendszerek biztonsága tekintetében: „*a közlekedési rendszerek digitalizálódásának fokozódásával a feltörésekkel és a kibertámadásokkal szembeni kiszolgáltatottságuk is nő. A C-ITS kommunikációk kiberbiztonsága ezért kritikus fontosságú, és európai szintű fellépést igényel. (…) Emellett a biztonsági megoldások egységességének hiánya kockázatot jelent az interoperabilitás és a végfelhasználók biztonsága szempontjából. A Bizottság véleménye szerint ezért a C-ITS európai kiépítése érdekében közös biztonsági és tanúsítási politikát kell kidolgozni.*”[82]

A 29. cikk szerinti Adatvédelmi Munkacsoport 2017. októberi véleményében[83] fogalmazta meg a legalapvetőbb védelmi követelményeit a személyes adatok C-ITS keretében történő kezelésével kapcsolatban, ezek többsége a magánélet védelmén keresztül a rosszindulatú felhasználás (mint kockázat) elleni védelmet hangsúlyozza.

A testület szükségesnek tartja:

– adatvédelmi hatásvizsgálatok elvégzését annak érdekében, hogy már a kezdetektől ismertek legyenek az érintettek jogait és szabadságait érintő kockázatok (pl. adatvédelmi incidensek miatti kockázatok), valamint legyen lehetőség e kockázatok tudatos és szisztematikus csökkentésére;

– a telepített C-ITS-funkciók mindegyikének az alapértelmezés szerinti kikapcsolását, azaz a vezetőknek ne legyen kötelező adatokat szolgáltatni önmagukról akkor is, ha nem szívesen tennék ezt;

– a magánélet védelmét szolgáló egyéb megoldások alkalmazását a rendszer tervezése során, például a rendszer generalizálását vagy zajhozzáadással történő kiegészítését úgy, hogy ezek ne befolyásolják negatívan a környezetről alkotott képet és a veszélyek felismerésének esélyét, ezzel egyidejűleg azonban korlátozzák a gépjárművezető felesleges terhelését vagy hosszú távú nyomon követését;

– beépített és alapértelmezett adatvédelem előírásainak következetes végrehajtását, ezzel téve lehetővé a felhasználók számára az igényeiknek leginkább megfelelő nyomon követési opciók kiválasztását (időzítés, gyakoriság, helyek stb.), illetve hogy ezen adatok biztonsága meg legyen őrizve a rosszindulatú támadókkal szemben (pl. egy esetleges terrortámadásban célszemély követése stb.);

---

[82] A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az együttműködő, intelligens közlekedési rendszerek európai stratégiája – mérföldkő az együttműködő, összekapcsolt és automatizált mobilitás megvalósítása felé. COM(2016) 766 final. Európai Bizottság, Brüsszel, 2016.11.30. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52016DC0766&from=EN; letöltés: 2021.04.25.

[83] 03/2017. számú vélemény a személyes adatok kooperatív intelligens közlekedési rendszerek (C-ITS) keretében történő kezeléséről. WP 252. A 29. cikk szerinti Adatvédelmi Munkacsoport, 2017.10.04. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171; letöltés: 2021.04.25.

– a biztonság megerősítését, hogy a C-ITS-adatok törvényes célokon túlmutatóan ne legyenek felhasználva, és a szereplők, illetve „külsősök” ne manipulálhassák az adatokat (pl. mesterségesen előidézzenek tereléseket, ne történhessenek rosszindulatú beavatkozások stb.);

– fokozott figyelem fordítását a tanúsítványok cseréjének gyakoriságára a kiválasztott gyakoriság és a hosszú távú nyomon követés kockázata közötti optimális egyensúly kialakítása érdekében;

– a tanúsítványok kiosztására szolgáló PKI-mechanizmusról részletes nyilvános dokumentáció készítését és a mechanizmus szigorú ellenőrzését annak érdekében, hogy a tanúsító szervezetek közötti összejátszásokból és a rosszindulatú szereplők megjelenéséből származó kockázatok csökkenthetők legyenek;

– az adatok minőségének körültekintő értékelését az intelligens rendszer nem semleges felhasználásából, a hamis riasztások („farkaskiáltások”) generálásából és a valós vészhelyzetek félreértelmezéséből származó kockázatok csökkentése érdekében;

– az adatmegőrzési határidők egyértelmű meghatározását minden C-ITS-platformban részt vevő fél vonatkozásában, illetve javasolja a részt vevők számára a központosított adatbázisok létrehozásának megtiltását.

A GDPR és a C-ITS

A felhasználók szempontjából az általános adatvédelmi rendelet (továbbiakban: GDPR) az, ami a legerősebb biztosíték arra vonatkozóan, hogy az adataik, illetve jogaik és szabadságaik védelme biztosított legyen, a rendszert fenntartókat pedig ugyanezen jogszabály rendelkezései kényszerítik az adatbiztonság követelményeinek szigorú betartására, legyen az logikai, fizikai vagy adminisztratív védelem. A GDPR előírásainak szándékos vagy gondatlan megszegése, illetve egy esetleges adatvédelmi incidens miatt kiszabott adatvédelmi hatósági büntetés a szereplőket éves árbevételük akár 2–4 százalékától is megszabadíthatja.

Az érintettek (a közlekedésben részt vevők, illetve a környéken tartózkodók vagy egyéb módon érintett személyek) számára súlyos, akár katasztrofális következményekkel járhat az információbiztonság (a bizalmasság, a sértetlenség és a rendelkezésre állás[84]) sérülése, például:

– közlekedési baleset következtében megsérülhetnek, vagy akár az életüket is veszthetik;

– az incidens jelentős kihatással lehet az ökológiai lábnyomra;[85]

– a C-ITS felhasználható zaklatásra, célszemélyek privát szférájának megtámadására;[86]

[84] CIA (Confidentiality – Integrity – Availability) követelményrendszer.
[85] Például veszélyes anyagot érintő baleset miatti környezetszennyezés, manipulációval eltérített forgalom miatt bekövetkezett környezetrongálás stb.

– a C-ITS felhasználható (szervezett) bűnözés céljaira, pl. terrorcselekmények elkövetése, csempészet, emberkereskedelem érdekében stb.;

– adatok manipulálhatók bűncselekmény elkövetése céljából, például anyagi haszonszerzés céljából tanúsítványok hamisítása, gazdasági érdek miatt adatok eltérítése (nem engedélyezett értékesítése) marketing vagy profilozási célból stb.;

– irányítás átvétele távolról, információmanipulálás (pl. felhasználás gerillamarketingre, a közlekedésben részt vevők „megviccelése", terrorcselekmény végrehajtása), információeltérítés vagy -megsemmisítés;

– jelentős közvetlen vagy közvetett anyagi kár okozása (infrastruktúra, ingó és ingatlan vagyontárgyak, különösen járművek sérülése stb.);

– a C-ITS üzemeltetői jó hírnevének sérelmét okozhatja, a rendszerbe vetett közbizalmat sértheti (negatív sajtó, nemzeti vagy nemzetközi politikai nyomás stb.) és az ügyfelek elpártolását eredményezheti (pl. a vezetők kikapcsolják az okos eszközöket);

– a GDPR megsértése miatt (pl. adatvédelmi incidens okozása) jelentősen sérül az érintettek privát szférája, vagy az esemény akár komoly pénzügyi nehézségeket, kárt okozhat számukra.

A nagyadat korszakában még felmérni is nehéz azt az adatmennyiséget, amely az C-ITS-adatközpontokban koncentrálódni fog, és amely adatoknak nemcsak a léte lehet ismeretlen, hanem a felhasználási célja is.

A Tesla által forgalmazott gépjárművek példája már megnyomta a vészcsengőt – az Európai Unió adatvédelemre szakosodott hatóságai egyelőre szkeptikusak a cég legújabb innovációit illetően, a leendő németországi „gigaautógyár" pedig a Baden-Württenbergi adatvédelmi hatóság célkeresztjébe került a GDPR előírásainak feltételezett megsértése miatt.[87]

A Tesla fejlesztései tekintetében ráadásul nem sokat tesz az átláthatóság érdekében, például legendák keringenek arról, hogy az autók nyolc fedélzeti kamerával folyamatos felvételeket készítenek a gépjármű környezetéről, és ezek a felvételek vajon hova jutnak el, ki szervezi őket világméretű adatbázisba és ki kontrollálhatja azt. A probléma jelentőségét növeli az, hogy a járművekben nemcsak kép-, hanem hangfelvételek is készülhetnek, illetve a Tesla autóit jellemzően a gazdasági, a politikai és a művészeti élet domináns szereplői (a „tehetősek") vásárolják.

---

[86] Például közéleti személyek, celebek tevékenységének nyomon követése, az adatok alapján magánéletük feltérképezése, sajtóban történő megszellőztetése stb.

[87] GDPR-t sért(het)nek a Tesla fedélzeti kamerái. GDPR.News.hu, 2020.10.25. https://gdpr.news.hu/cikkek/gdpr-t-serthetnek-a-tesla-fedelzeti-kamerai/; letöltés: 2021.04.25. HESSEL, Stefan: The Tesla Sentry Mode – ideas for more data protection and GDPR compliance. LinkedIn, 2020.02.23. https://www.linkedin.com/pulse/tesla-sentry-mode-ideas-more-data-protection-gdpr-stefan-hessel; letöltés: 2021.04.25.

E személyek nyomon követésével, lehallgatásával nemcsak a terrorcselekmények kockázata nagy, hanem nemzetgazdasági vagy akár globális válságok is okozhatók (tőzsdemanipuláció, bizalmatlanság keltése, politikai feszültség szítása, kormányválság előidézése stb.) Ha pedig belegondolunk abba, hogy évente félmillió okosgépjármű kerülhet Európa közterületeire csak ebből az egy Tesla-gyárból, az már komoly nemzetbiztonsági problémafelvetéseket is eredményezhet. Ilyen feszítő kérdések lehetnek – többek között:

- jogosulatlan adattovábbítás harmadik országba (pl. olyan joghatóságba, ahol ellenérdekelt titkosszolgálatok működnek);
- védett területek és személyek kontrolálhatatlan megfigyelése, a megszerzett adatok rosszindulatú felhasználásának lehetőségei (pl. pszichológiai manipuláció, terrortámadás stb.);
- egy szervezetnél koncentrálódó nagyadat mint a hekkertevékenység és a kiberterrorizmus szempontjából csalogató „*honey pot*” stb.

A privát szféra igen súlyos sérelmét eredményezheti, hogy a sofőrnek, illetve a gépjárműben tartózkodó egyéb személyeknek adott esetben semmilyen beleszólásuk sem lehet a belső, nemcsak képet, hanem akár hangot is rögzítő kamerák működésébe, ez pedig zsaroláshoz (pl. pszichológiai manipuláció), jó hírnév sérelméhez, anyagi kárhoz és magánéleti válsághoz is vezethet.

A GDPR és a kapcsolódó járművek

Az Európai Adatvédelmi Testület (EDPB[88]) kapcsolódó gépjárművekkel foglalkozó iránymutatása[89] behatóan tárgyalja az adatbiztonságot, és kiemeli azt az ökoszisztémát, amelybe ezek a – többségében személyes – adatok bekerülnek.

Ez a környezet már nem korlátozódik az autóipar hagyományos szereplőire, hanem annak részesei:

- az új típusú digitális gazdaság szereplői is, például informatikai alapú szolgáltatások nyújtói (online zenét és közlekedési információt szolgáltatók, vezetést segítő rendszerek, felhasználáson alapuló biztosítást kínáló biztosítók, dinamikus térképezők, felhőszolgáltatók stb.);
- a közúti infrastruktúra üzemeltetői;
- a távközlési szolgáltatók;
- az autóipari beszállítók, gyártók és forgalmazók, az autójavítók;
- a flottamenedzserek és
- maguk a gépjárművezetők is.

[88] European Data Protection Board.

[89] Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 2.0. Adopted on 9 March 2021. European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf; letöltés: 2021.04.25.

Figyelembe kell venni azt is, hogy nemcsak a járművek és az infrastruktúrák kapcsolódnak (V2V, V2I), hanem a kapcsolódó járművekben számtalan elektronikai vezérlőeszköz, illetve IoT-eszköz[90] is található, amelyek mind járművön belül, mind a járművön kívülre is kommunikálnak, felbecsülhetetlen mennyiségű adatvédelmi és adatbiztonsági problémát generálva.

A funkciók, szolgáltatások és interfészek összetettsége jelentősen növeli a sérülékenységet és a támadási kockázatot, valamint a legtöbb IoT-eszközzel ellentétben a csatlakoztatott járművek olyan kritikus rendszerek, ahol fokozott annak az veszélye, hogy hekkerek (kiberterroristák) megpróbálják kihasználni e rendszerek sebezhetőségét. Az illetéktelen hozzáférés területén tovább növeli a kockázatot az, hogy az adatok járművön belül és kívül is (pl. felhőszolgáltatóknál) tárolhatók, és az is, hogy a sofőrnek időnként meg kell válnia az autójától, és ilyenkor az adatok egy részéhez harmadik félnek (pl. szervizek) is hozzáférést kell biztosítania.

Az iránymutatás különösen fontosnak tartja a lokációs, a biometrikus és a bűnügyi adatok védelmét, valamint azt, hogy ezen adatkategóriák a fokozatosság elvét figyelembe véve a lehető legkisebb mértékben legyenek kezelve, továbbá javaslatokat ad ezen adatok kezelésének elkerülésére, illetve a biztonságuk megőrzésére, például:

- biometrikus adat helyett biometrikus sablon, és csakis az autóban használva-tárolva titkosított formában;
- a lokációs adatgyűjtés alapértelmezett állapotban kikapcsolt legyen, illetve a bekapcsolt eszköz bármikor kikapcsolható legyen, valamint a sofőrnek legyen lehetősége kiválasztani, hogy melyik alkalmazást működteti, mikor törli akár véglegesen az adatait, a tájékoztatást pedig az általa értett nyelven kapja;
- korlátozott mennyiségű autentikációs lehetőség;
- beépített és alapértelmezett adatvédelem maximális érvényesítése;
- a lehető legkevesebb adat kerüljön ki a gépjárműből (az adatoknak csak kis része legyen továbbítva másik autók, egyéb fogadók, illetve felhők felé, ezzel is csökkentve a kockázatot);
- az autó biztonsági funkciói fizikailag legyenek elkülönítve az autóba beépített applikációktól annak érdekében, hogy a hozzáférés az autó adataihoz ne függjön a felhők kapacitásától;
- a továbbítás előtt az adatok lehetőleg legyenek anonimizálva vagy álnevesítve;
- az adatkezelők folytassanak le hatásvizsgálatot a kockázatok csökkentése érdekében, és lehetőleg többszintű tájékoztatást alkalmazzanak stb.

[90] Internet of Things (IoT). https://www.internetsociety.org/iot/?gclid=Cj0KCQjwgtWDBhDZARIsADEKwgO6IOoVMEWceFmYEMMQVjHRQhXjbcSvwqJD4tfBx7zxBpXGlZfk7gIaAiigEALw_wcB; letöltés: 2021.04.25.

Az EDPB olyan biztonsági követelményeket javasol, amelyek – bár hatalmas feladatot rónak a szereplőkre a GDPR-megfelelőség biztosítása terén, de – jelentősen csökkentik a kibertámadások kockázatát is, például a következő megoldások segítségével:

- a kommunikációs csatornák és az autón kívüli adattárolás titkosítása a legmodernebb algoritmus segítségével;
- minden jármű esetében egyedi titkosítási kulcsmenedzsment alkalmazása;
- titkosítási kulcsok rendszeres megújítása és védelme;
- adatfogadó eszközök autentikációja;
- a fedélzeti szolgáltatáskészlet-azonosító (SSID[91]) kikapcsolhatósága (a nyomon követhetőség csökkentése érdekében);
- adatok integritásának biztosítása (pl. *hashing*);
- a személyes adatokhoz történő hozzáférés megbízható felhasználói hitelesítési technikák (jelszó, elektronikus tanúsítvány stb.) függvényében;
- az autógyártók részéről a biztonsági rések gyors kijavítása a jármű teljes élettartama alatt;
- támadásjelzés üzemeltetése azzal a lehetőséggel, hogy szükség esetén a jármű alacsonyabb funkciókkal üzemeltethető legyen;
- hozzáférés naplózása annak érdekében, hogy az esetleges anomáliák és támadások visszakövethetők és elemezhetők legyenek.

Önvezető járművek kockázatai

Az útjainkon már hozzászoktunk az okos eszközökkel felszerelt, illetve kapcsolódó járművekhez, amelyek képesek például összehangolni a sofőr online üzleti naptárját az autó fedélzeti számítógépében lévő útvonaladatokkal,[92] jelzik, ha a vezető túllépte a megengedett sebességet, baleset esetén automatikusan hívják a segítséget, de a jövő ezen jelentősen túlmutat, a fejlődés egyértelműen az önvezető járművek térnyerésének irányába halad.

Elengedhetetlen feltétel a közlekedés résztvevői közötti és az infrastruktúrával folytatott megfelelő és teljes egészében az informatikai megoldásokra épül kommunikáció (lásd a már említett C-ITS) ahhoz, hogy ne a gépjárművet vezetők uralják a járművezetés folyamatát. Alapvető különbség a kötött pályás közlekedéssel szemben, hogy a jármű kerekeit a vezető kormányozza, így a balesetek bekövetkezésének jelentős részéért a gépjárművet vezető a felelős. Ezt a felelősséget kell átvennie az informatikának, amelynek nemcsak az a feladata, hogy a jármű és

[91] Service Set Identifier.
[92] Például a Volvo Call On rendszere.

utasai (rakománya) A-ból B-be biztonságosan eljussanak, hanem a rendszernek képesnek kell lennie arra is, hogy megakadályozza illetéktelen személyek hozzáférését a jármű irányításához.

Az első feladat V2X-kommunikáció megfelelő biztosítása, amely csak olyan rendszereken keresztül lehetséges, amelyekbe kívülről nem lehet behatolni és nem lehet a járművek irányításába jogosulatlanul beleavatkozni. A biztonság szempontjából az is fontos eldöntendő kérdés, hogy a járműben ülők beleavatkozhatnak-e a biztonság szempontjait szem előtt tartó irányítási folyamatokba. Amennyiben igen, ez lehetőséget teremthet az olyan öngyilkos merényletekre, amikor a járműben ülő szándékosan okoz balesetet, ez pedig felveti annak szükségességét, hogy a védelmi rendszereknek meg kell tudni akadályozniuk az ilyen cselekedeteket. Ez természetesen a tervezés során a kockázatokat előre figyelembe vevő, tökéletesen működő V2X-kommunikáció esetén lehetséges.

A második feladat a jármű irányítása távoli átvételének a megakadályozása. Ez a távirányítású autók kérdését veti fel.

Járműfedélzeti hálózatok kiberbiztonsági kérdései[93]

Az önvezető technológia számos egyéb kockázatot is magában hordoz. Ilyen tényező az időjárás is, mivel a rossz látási viszonyok nagyban befolyásolják a gépjárműre szerelt szenzorok működését.

A lézeres rendszerek esetében ez azt jelenti, hogy köd és eső esetén a mért eredmények tévesek vagy pontatlanok lehetnek. Emellett sok más kockázati tényező is fennáll, mint például a kommunikációs infrastruktúra, a mesterséges intelligencia kockázatai, a hagyományos és az önvezető járművek viszonya.

Ezekről a problémákról és kockázatokról részletesebb útmutatást találunk Dr. Kiss Gábor, Berecz Csilla Éva és Tóth László cikkében,[94] ahol a szerzők felsorolják és röviden rendszerezik ezeket a kockázati tényezőket. De ezek mellé napjainkban már mindenképpen meg kell említeni és meg kell vizsgálni az önvezető autók kiberbiztonságát egy másik aspektusból, mégpedig nem a technológia szemszögéből, hanem az információs terrorizmus vonatkozásában.

Az önvezető gépjárművek részben emberi beavatkozás nélkül vesznek részt a közúti forgalomban. A gépjárművet nagyrészt vagy szinte teljesen számítógép (esetleg mesterséges intelligencia) felügyeli. Egy ilyen gépjármű-irányítási rendszer szándékos manipulációjával – a minimálisan szükséges kibervédelmi rendszerek nélkül – komoly közúti baleseteket lehet okozni.

---

[93] TOKODY Dániel – ALBINI Attila – ADY László – TEMESVÁRI Zsolt Marcell – RAJNAI Zoltán: Kiberbiztonság az autóiparban. Bánki Közlemények, 1. évfolyam 3. szám, 2018. pp. 71–77. http://bk.bgk.uni-obuda.hu/index.php/BK/article/download/79/47/; letöltés: 2021.04.25.

[94] KISS Gábor – BERECZ Csilla Éva – TÓTH László: A jövő közlekedése vagy sebezhető eszköz az önvezető autó? Bánki Közlemények, 2. évfolyam 1. szám, 2019. pp. 5–10. http://bk.bgk.uni-obuda.hu/index.php/BK/article/download/105/54/; letöltés: 2021.04.25.

Erre sajnos már a kiberbűnözői csoportok is felfigyeltek, a hekkerek – mint akár más informatikai rendszer esetében – valamilyen sérülékenység kihasználásával beléphetnek a gépjármű informatikai rendszerébe, majd kisebb módosítások (szenzorok paramétereinek átállításával) elvégzésével komolyabb baleseteket tudnak előidézni.

A 2020. évi *Black Hat* konferencián egy csapat informatikai szakember bemutatta azt, hogy milyen módon lehet távoli eléréssel illetéktelenül belépni egy E-osztályú Mercedes Benz személygépjármű rendszerébe, majd ezt követően elindítani a motort és kinyitni a gépjármű ajtajait.[95]

A probléma sajnos nem új keletű, 2015-ben már volt rá példa, amikor azt szimulálták, hogy hekkerek egy Jeep típusú személygépjárműbe illetéktelenül beléptek és módosították a személygépjármű egyes elemeinek paramétereit, ezzel aktívan zavarva a forgalomban részt vevő gépjármű vezetőjét.[96]

Természetesen az előbbiekben említett támadási lehetőségeken kívül még számos más kockázat rejlik az okosautók működésében. Az ENISA 2016-ban részletesen elemezte a kockázatokat az alacsonyabb szinten automatizált,[97] 2019-ben pedig a magas szinten automatizált (autonóm) járművek esetében.[98] A dokumentumok fontos intézkedési javaslatokat adnak a lehetséges támadások kivédéséhez,[99] ám az ártó szándékú személyek számára is kiváló ötleteket adnak a legsebezhetőbb pontok megtalálásához. A kiberbiztonsággal kapcsolatos jó gyakorlatok keretében három olyan nagy témakört vizsgálnak, amelyekre összpontosítani kell:

– eljárások: beépített biztonság, beépített adatvédelem, eszközmenedzsment, kockázat- és fenyegetésmenedzsment;
– szervezeti intézkedések: kapcsolat a beszállítókkal, oktatás és tudatosság, biztonság- és incidensmenedzsment;
– technikai intézkedések: detektálás, hálózat- és protokollvédelem, szoftverbiztonság, felhőbiztonság, titkosítás, hozzáférés-menedzsment, önvédelem és kiberellenálló-képesség, a (fél)önvezető autók önvédelme és kiberellenálló-képessége, működésfolytonosság.

---

[95] WHITTAKER, Zack: Security bugs let these car hackers remotely control a Mercedes-Benz. Tech Crunch, 2020.08.07. https://techcrunch.com/2020/08/06/security-bugs-mercedes-benz-hack/; letöltés: 2021.03.11. Creating Safer Interconnected Vehicles. IEEE. https://innovationatwork.ieee.org/creating-safer-interconnected-vehicles/; letöltés: 2021.04.25.

[96] Hackers Remotely Kill a Jeep on the Highway – With Me in It. Wired, 2015.07.21. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; letöltés: 2021.04.21. 'Jeep hack' dismissed on the basis of speculation. Automotive World, 2020.05.06. https://www.automotiveworld.com/articles/jeep-hack-dismissed-on-the-basis-of-speculation/; letöltés: 2021.04.21.

[97] Cyber Security and Resilience of smart cars. Good practices and recommendations. ENISA, December 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars; letöltés: 2021.04.29.

[98] ENISA Good Practices For Security Of Smart Cars. ENISA, November 2019. https://www.enisa.europa.eu/publications/smart-cars; letöltés: 2021.04.29.

[99] Uo. 3. Threats and Attack Scenarios, Annex B: Threat Taxonomy, Annex C: Security Measures Mapping.

A mesterséges intelligenciával (MI) kapcsolatos lehetséges támadásokat külön ENISA-kiadvány taglalja[100] különös tekintettel a kiberbiztonságra, a kihívásokra és a legjobb gyakorlatokra, valamint néhány lehetséges támadás forgatókönyvét is felvázolja. Számtalan javaslatot megfogalmaz az MI és a biztonság kapcsán, ám a javaslatoknak korlátja az, hogy az MI kiberbiztonságával foglalkozó fejlesztők és rendszertervezők még nem rendelkeznek megfelelő biztonsági ismeretekkel és szakértelemmel a témában, ez pedig olyan jelentős akadály, amely jelenleg még hátráltatja a biztonság integrációját az autóiparban.

Vasúti közlekedés

A vasúti közlekedés a nagy tömeg és nagy sebesség miatt már eleve veszélyes üzem, így rendkívül szigorú szabályok vonatkoznak a forgalom lebonyolítására. Az internetre felkerülő anyagokat szintén szétbontva, üzemi és utasadatokként vizsgáljuk.

A vasúti közlekedés üzemi adatai

A vasúti infrastruktúra kiterjedése a közútinál általában kisebb, így az útvonalak koncentráltak, és ennél az alágazatnál nem beszélhetünk egyéni közlekedésről. A vasúti közlekedés alapfilozófiájából következően[101] az alágazati szereplők leginkább a jól kihasznált vonatok közlekedésében érdekeltek. Ez adott esetben akár 1000 utast is jelenthet egy vonaton, és ez a szám már a terroristák figyelmét is felkeltheti.

Az autóbuszoknál már tárgyalt fordatervek a vasút esetében többletinformációt is hordozhatnak. A vonatok esetében a fordulók a szerelvények összeállítását is tartalmazzák, azaz megismerhető, hogy egy adott vonat hány kocsival közlekedik. Miért lehet ez fontos adat? Szigorúan kiberbiztonsági oldalról vizsgálva a kérdést megállapíthatjuk, hogy az interneten közzétett szerelvényfordulók alapján és az összeállításokat ismerve eldönthető, hogy melyik vonat ellen érdemes robbantásos terrorakciót végrehajtani. Az teljesen egyértelműnek tűnik, hogy a sok kocsival közlekedő vonatokon sok utas is tartózkodik, így a terroristáknak a merényletet célszerű ezek ellen szervezni a számukra kívánatos eredmény elérése érdekében.

A közlekedési vállalatok az utóbbi idők civil nyomásra már közzéteszik fordáikat az interneten,[102] sőt olyan belső tervek is megtalálhatók a világhálón, amelyekből kifejezetten érzékeny adatok is megszerezhetők.[103]

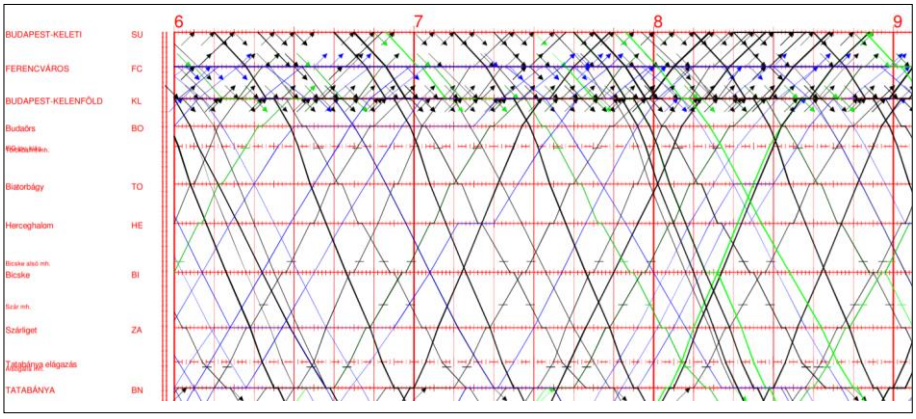
---

[100] Cybersecurity Challenges In The Uptake Of Artificial Intelligence in Autonomous Driving. ENISA, February 2021. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving; letöltés: 2021.04.29.

[101] Nagy tömegű áruk és jelentős számú utas szállítása. MÁNDOKI Péter (szerk.): Közlekedés és társadalom. Budapest, 2010. pp. 39–40. https://dtk.tankonyvtar.hu/xmlui/bitstream/handle/123456789/3251/Mandoki_Kozlekedes_es_tarsadalom.pdf?sequence=1&isAllowed=y; letöltés: 2021.04.25.

[102] MÁV-START Zrt. – Vonatösszeállítás (SzVÖR). https://www.mavcsoport.hu/mav-start/bemutatkozas/belfoldi-utazas/vonatosszeallitas-szvor; letöltés: 2021.04.25.

A vasúti infrastruktúra szűkössége miatt annak kapacitásával gazdálkodni kell, ami azt jelenti, hogy a vasúti infrastruktúrát csak meghatározott feltételekkel lehet igénybe venni. A vasútvonalakon közlekedő szinte valamennyi vonatnak menetrendet szerkesztenek,[104] amely az igénylő számára úgynevezett menetvonalban testesül meg. A menetvonalakat a kapacitásgazdálkodó szervezet a menetrendábrában jeleníti meg.



1. ábra. Menetrendábra (részlet)[105]

Az ábrából kiolvashatók az egyes vonatok menetvonalai (menetrendjei). Az ábra egy út-idő grafikon, amelynek függőleges tengelye az út (vasútvonal), vízszintes tengelye pedig az idő. Teljesen világos, hogy a grafikonról leolvasható, hogy adott vonat melyik időpontban hol tartózkodik vagy halad, vagyis az, hogy hol érdemes a robbantást végrehajtani.

A magyarországi vasútvonalak menetrendábráit a kapacitáselosztó szervezet az interneten közzéteszi.[106] A kapacitáselosztó szervezetet erre az 55/2015. (IX. 30.) NFM-rendelet 2019. évi módosítása kötelezi. Ez kiberbiztonsági szempontból nem szerencsés, ugyanis így az egyes vonalakon közlekedő vonatok pontos időadatai minden probléma nélkül kiolvashatók és a terrorakciók megtervezhetők.[107]

---

103 Például a kocsik ajtóinak reteszelhetőségéről.
Tableau européen des services directs.
https://viaggiandoavapore.files.wordpress.com/2019/12/ewp-2013-1.pdf; letöltés: 2021.04.25.

104 Kivételt képeznek egyes munkamenetek és segélyvonatok.

105 Menetrendi ábrák 2019-2020 éves.
https://www2.vpe.hu/menetrendi_abrak/2019_2020; letöltés: 2021.04.25.

106 VPE Vasúti Pályakapacitás-elosztó Kft. – Menetrend Ábrák 2020/2021 éves kiutalások.
https://www2.vpe.hu/menetrendi_abrak/2020_2021; letöltés: 2021.04.25.

107 LÉVAI Zsolt – ÜVEGES András József: A vasúti közlekedés informatikai adatvédelme. Felderítő Szemle, XIX. évfolyam 2. szám, 2020. pp. 103–139.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-2.pdf; letöltés: 2021.04.25.

Az ábrán nincsenek számok, csak az egyes menetvonalak láthatók, amelyek különböző színűek. Az alkalmazott háromféle színkód azonban könnyen megfejthető. A legtöbb a különböző vastagságú fekete, majd a kék, végül pedig a zöld színű menetvonal.

Logikusan kikövetkeztethető,[108] hogy a fekete a személyvonatok színe (valószínűleg egy vasúthálózaton abból közlekedik a legtöbb).

Állomások adatai

Külön kell foglalkozni a nagyállomások üzemi adataival. A vasútállomások üzemi folyamatainak bonyolultsága megkívánja, hogy egyes nagyobb állomásokon ezeket a folyamatokat megtervezzék. Ezt a tervet üzemi technológiának nevezzük. A technológia része egy másik grafikon, amelyen egy adott állomás berendezéseinek (pl. vágányainak) igénybevételét ábrázolják. Ebből megtudható, hogy adott állomáson egy vonat melyik vágányra jár be, így egy állomási terrorakció ezen adatok birtokában megtervezhető. Természetesen ezek az adatok nem nyilvánosak, és nem is tárolják azokat nyílt hálózaton, így jelenleg ezzel kockázati tényezőként kevésbé kell számolni.

Forgalomirányítás

A vasúti forgalomirányítási adatok a vonatok közlekedési információit és a biztosítóberendezések kezelésének adatait jelentik.

A vonatok közlekedési adatai szintén egy út-idő grafikonon jelennek meg. Ez a menetgrafikon, amely nem más, mint egy valós idejű menetrendábra. Az adatok az üzemirányító központokban jelennek meg, ahol a forgalomirányítást végző munkatársak felügyelik a vonatok közlekedését és szükség esetén beavatkoznak. A fő kérdés a beavatkozás, illetve annak a lehetősége a terroristák számára.

Itt az üzemirányítást ketté kell választani aszerint, hogy a központban dolgozó munkavállaló csak ellenőrző vagy irányító szerepkört tölt-e be. Az ellenőrzés csak az állomási, helyben végzett munka megfigyelésén alapul, és a hibás döntéseket van hivatott javítani, az irányítói szerep az állomások távkezelését jelenti. Az ellenőrző szerep leginkább kimerül az irányító és az állomási személyzet közti telefonos párbeszédben, míg az utóbbi esetben már működési parancsok kiadása is történik (pl. váltóállítás).

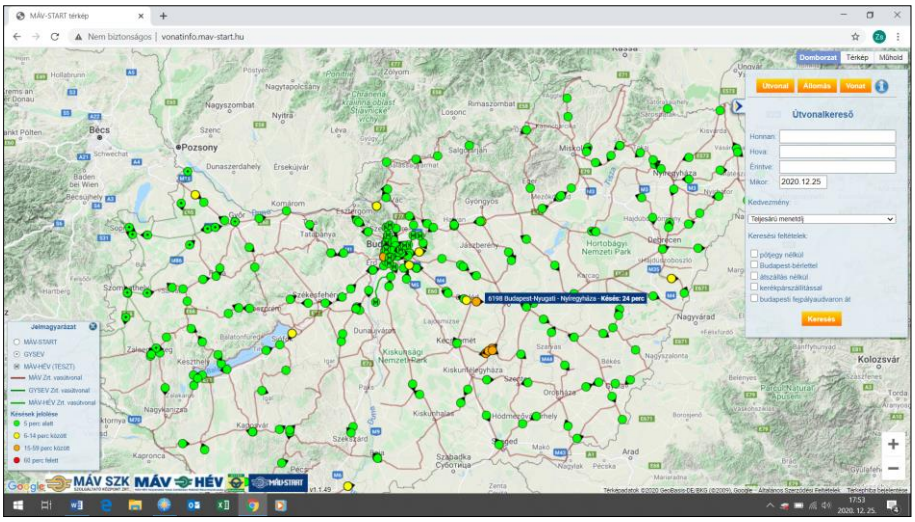
Minden körülmények között el kell érni, hogy a kiadott parancsok megfelelőek legyenek (pl. az előbb említett váltó megfelelő vágányra vezessen), és hogy adott menet (vonat) közlekedésének ideje alatt újabb parancsot ne lehessen kiadni (pl. a váltó átállítása a vonat alatt). Könnyen belátható, hogy egy ilyen parancs végrehajtása súlyos következménnyel járhat (pl. kisiklás). A kibervédelem itt leginkább abban áll, hogy megakadályozzuk ellentétes értelmű parancsok kiadását

[108] A Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar logisztika szakos hallgatói körében végzett kutatási eredmények alapján.

(pl. hogy egy adott váltón egyszerre két vonat is közlekedhessen), illetve a már beállított berendezések átállítását egy bizonyos időponttól addig, amíg a vonat az adott berendezést használja. Egyértelműen tilos ilyen esetekben nyílt hálózat használata, hogy kizárhassuk a külső beavatkozásokat.

Ügyféladatok

Információkat a vonatok közlekedéséről az ügyféladatokon keresztül is lehet szerezni. A valós idejű közlekedési adatok nyilvánosak, és a mai korban már elvártak. A rendelkezésre álló idő értéke annyira megnőtt, hogy gyakorlatilag a ma embere már perceket sem hajlandó elvesztegetni, hanem a vonat tényleges érkezésére kíván kiérni az állomásra. Természetesen ez fordítva is igaz, egy szolgáltatónak elemi érdeke, hogy ügyfelei részére percre pontos információt adjon a vonatok közlekedéséről. Ma már csak így lehet megfelelő utasforgalmat elérni. A különböző vonatinfóoldalak tehát mutatják a vonatok percre pontos közlekedését és késését (2. ábra).



2. ábra. A MÁV-START egy térképe[109]

Ezen kívül vannak olyan vasúttársaságok, ahol a vonatok kihasználtságára is találunk adatokat (3. ábra *Auslastung* oszlop). Mint már említettük, ezek az adatok szemrevételezéssel is megszerezhetők, ugyanakkor megkönnyítik az ártó szándékú cselekedeteket elkövetni szándékozókat műveleteik tervezésében és előkészítésében.

[109] A MÁV-START térképe. http://vonatinfo.mav-start.hu/; letöltés: 2020.12.25.

3. ábra. Kihasználtsági adatok[110]

Tehervonatok közlekedési adatai

A tehervonatok esetében magának a vonatnak a robbantása elegendő lehet az infrastruktúra rombolásához is. A nagy tömeg miatt a kisiklás a pályában is jelentős kárt okozhat, nem beszélve a jármű- és árukárról. Szintén a menetrendábrából tudható meg, hogy mikor és merre közlekedik tehervonat. Természetesen itt is kiemelt jelentőségű a veszélyes árut szállító tehervonatok közlekedési és ügyféladatainak védelme. Vannak olyan tehervonatok, amelyek menetrendjét nem jelenítik meg a menetrendábrában, sőt még elektronikus formában sem továbbítják, nehogy bárki illetéktelen is hozzáférjen az adatokhoz.

A vasúti közlekedés esetében is a jövő az intelligens rendszereké,[111] ami hasonló kiberbiztonsági problémákat vet fel, mint más intelligens rendszerek esetében.

Vízi közlekedés

A vízi közlekedés pályája olyan közeg, amelyben egy robbantás nem, vagy csak kismértékben tesz kárt, így leginkább a kikötők és a szállítóeszközök védelme lehet indokolt. Ugyanakkor hajózási útvonalakon található műtárgyak (pl. hidak) rombolása blokkolhatja az útvonalakat.

A Google térképén a rotterdami kikötő berendezései[112] teljes mértékben kivehetők (4. ábra), így könnyen meghatározhatók azok a helyszínek, ahol lehetséges hatásos terrorakció elkövetését tervezni, mert a bekövetkező károk jelentősek lehetnek.

---

110 A svájci állami vasúttársaság utastájékoztató honlapja. https://sbb.ch/de/kaufen/pages/fahrplan/fahrplan.xhtml; letöltés: 2020.12.25.

111 BRANNER, Ricky – VARELA, Catalina: Intel: On Track to the Future – With Smart Railways. Intel Corporation, 2020. https://www.intel.com/content/www/us/en/transportation/resources/smart-railways-ebook.html; letöltés: 2021.04.25.

112 Például az ásványolaj-tárolók.

Erre példát láttunk 2020 nyarán Bejrútban, ahol egy nem felügyelt kikötői raktárépületben jelentős mennyiségű ammónium-nitrát robbant fel,[113] aminek következtében több százan meghaltak és több ezren megsérültek. A közúti és a vasúti szállításhoz hasonlóan itt is ki kell emelni, hogy a veszélyes anyagok szállításának és tárolásának megfelelő védelme a közlekedési infrastruktúra védelmének egyik legfőbb kérdése.

4. ábra. A rotterdami kikötő részlete a Google térképén[114]

A vízi járművek sebessége viszonylag kicsi, ugyanakkor az ütközések során keletkezett sérülések következtében a jármű elsüllyedhet, ami áldozatokkal járhat. Ennek a veszélye a nyílt vízen a legnagyobb, a kikötőkben leginkább a nem megfelelő navigáció okozhat baleseteket. A kikötői berendezésekkel történő ütközés során a hajó szállítmánya vízbe kerülhet, ami szerencsés esetben csak anyagi kárt, súlyosabb esetben (pl. veszélyes anyag esetén) emberáldozatot is eredményezhet. A fő veszélyt nem is annyira az adott vízi jármű balesete, hanem az e miatt szükségessé váló korlátozások jelenthetik. Dokkok, rosszabb esetben az egész kikötő hosszabb idejű lezárása már érezteti hatását a gazdaságban, ezért a kikötői navigáció informatikai rendszereit mindenképpen védeni kell külső kibertámadásokkal szemben.

Ugyan nem terrorakció volt, de mindenképpen szemléletes példa a Szuezi-csatornában 2021 márciusában elakadt konténerszállító hajó esete. A rossz navigáció következtében a hajó megfeneklett, elzárva az útvonalat a többi hajótól, így a csatornát nem lehetett használni. A leállás következtében körülbelül napi 14–15 millió USD

[113] MANSOUR Elie – SLEIMAN, Georges Abi: Beirut Municipality Rapid Building-level Damage Assessment. Municipality of Beirut and UN-Habitat. Working Version, October 2020. https://unhabitat.org/sites/default/files/2020/10/municipality_of_beirut_-_beirut_explosion_rapid_assessment_report.pdf; letöltés: 2021.04.25.

[114] Port of Rotterdam. https://www.google.com/maps/place/Port+of+Rotterdam/@51.8925899,4.3544751,1110m/data=!3m1!1e3!4m5!3m4!1s0x47c43364d44f9f39:0xc5831d410339551e!8m2!3d51.9047712!4d4.4845515; letöltés: 2021.04.29.

veszteség érte a világgazdaságot.[115] A példa is mutatja, hogy a hajók navigációs berendezései feletti esetleges terrorista hatalomátvétel milyen hatásokkal járhat.

A hajók esetében az alábbi veszélyhelyzetek fordulhatnak elő:[116]

- összeütközés;
- zátonyra futás;
- tűzesetek;
- stabilitás és úszóképesség elvesztése.

A vízi járművek informatikai védelme a veszélyhelyzetek elkerülésére szolgáló berendezések védelmét jelenti,[117] illetve itt már felmerülhet a szállított áru ellenőrzését végző informatika védelme is. A hajó rakterében szükséges hőmérsékletet felügyelő rendszer elektronikai támadása esetén elképzelhető, hogy az elállított hőmérséklet miatt a szállított anyag tekintetében spontán reakció indul meg, és ez a veszélyes anyag önrobbanásához vezethet.

Légi közlekedés

A légi közlekedés infrastruktúrája olyan közeg, amely nem reagál a robbantásokra, ezért ebben az esetben a kulcskérdés a repülőterek és a légi járművek védelme, valamint a légi forgalom irányítása.

A repülőterek informatikai védelme a repülőtéri irányítás, valamint a fel- és leszállást segítő berendezések (fénytechnikai berendezések) védelmét jelenti. A jelzőberendezések használhatatlansága vagy azok adatainak szándékos megváltoztatása esetén a repülőgépek közlekedése nem lesz biztonságos, és légi balesetek következhetnek be.[118]

A légi forgalom valós idejű alakulását mutató honlapról információk nyerhetők egy adott járat pontos helyzetéről, repülési magasságáról (lábban és méterben), sebességéről (csomóban és km/h-ban). Az adatok egy része díj ellenében hozzáférhető, de az árak nem olyan magasak (10–40 USD), hogy azok ne férjenek bele egy terrortámadás költségvetésébe. A repülési helyzet valós idejű adatai nagy segítséget nyújthatnak a terrorakciók elkövetőinek a támadás pontos idejének meghatározásakor. Ezek a honlapok ma már szinte valós idejű információkat szolgáltatnak.[119] A repülés esetén az időjárási viszonyok nagymértékben befolyásolhatják az út időtartamát, ezért ezek az adatok nem általánosíthatók, mert az időjárás naponta változik.

---

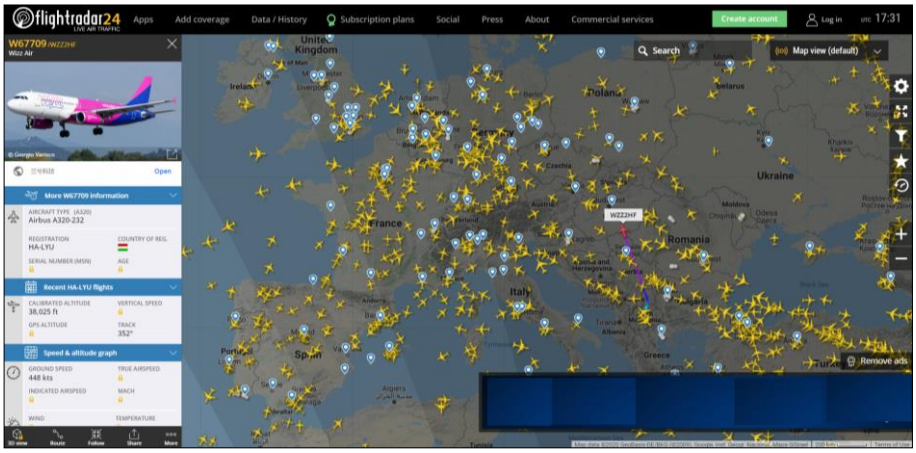
115 RUSSON, Mary-Ann: The cost of the Suez Canal blockage. BBC News, 2021.03.29. https://www.bbc.com/news/business-56559073; letöltés: 2021.04.25.

116 LÉVAI Zsolt: Közlekedésbiztonság. Dialóg Campus Kiadó, Budapest, 2019. https://nkerepo.uni-nke.hu/xmlui/bitstream/123456789/15740/1/670_HHK_Kozelekedesbiztonsag.pdf; letöltés: 2021.04.25.

117 Ilyenek lehetnek a navigációs berendezések.

118 LÉVAI Zsolt: Közlekedésbiztonság. Dialóg Campus Kiadó, Budapest, 2019. https://nkerepo.uni-nke.hu/xmlui/bitstream/123456789/15740/1/670_HHK_Kozelekedesbiztonsag.pdf; letöltés: 2021.04.25.

119 Real-time Flight Status and Radar for All US/Canada Flights. FlightAware, 2016.04.06. https://flightaware.com/news/article/Realtime-Flight-Status-And-Radar-For-All-USCanada-Flights/223; letöltés: 2021.04.25.



5. ábra. A légi forgalom valós idejű alakulását mutató honlap[120]

A repülés esetében a járművek elleni műveletek megakadályozásának fő kérdése a robbanószerkezet gépre juttatásának megakadályozása. Az informatikának itt elsősorban a minél korszerűbb detektorok alkalmazásában van szerepe.

A légi forgalom irányítása lehet:[121]

– távolkörzeti irányítás;
– közelkörzeti irányítás (a repülőterek 50–100 kilométeres körzetében);
– repülőtéri irányítás (a repülőterek 5–10 kilométeres körzetében).

A légi közlekedésben minden irányításnak megvan a maga feladatköre annak érdekében, hogy a közlekedés biztonságos legyen. Az informatika szerepe itt elsődlegesen a megfelelő kommunikáció biztosítása mind a műszerek, mind pedig az értekezőberendezések (rádiók) segítségével.

A légi balesetek súlyossága megköveteli, hogy a légiforgalmi irányítás a legmegfelelőbben működjön, azaz a hibák száma minimális legyen. Ezért kiemelten fontos, hogy az irányítóberendezések fölötti hatalmat ne lehessen kívülről átvenni, a berendezéseket csak az kezelhesse, akinek erre jogosultsága van. A megfelelő hozzáférés-jogosultsági rendszerek alkalmazásával az elvárt védelem kialakítható. Természetesen az irányítási információk nem kerülhetnek fel az internetre, ugyanakkor készülnek ismeretterjesztő videók ilyen helyeken, amelyek szabadon megtekinthetők.[122]

---

120 Flightradar24: Live Flight Tracker. https://flightradar24.com/WZZ2HF/2657fc95; letöltés: 2020.12.25.

121 LÉVAI Zsolt: Közlekedésbiztonság. Dialóg Campus Kiadó, Budapest, 2019. https://nkerepo.uni-nke.hu/xmlui/bitstream/123456789/15740/1/670_HHK_Kozelekedesbiztonsag.pdf; letöltés: 2021.04.25.

122 101. Radar előtt: így dolgoznak a Hungarocontrol légiforgalmi irányítói. Aeropark Budapest, 2019.11.13. https://www.youtube.com/watch?v=xP_qtbMryl0); letöltés: 2021.04.25.

Okosrepülőterek

Az „okos” repülőterek új kihívások elé állítják a biztonsági szakembereket.[123] Az intelligens repülőterek olyan repülőterek, amelyek olyan hálózati, adatközpontú válaszadási lehetőségeket használnak, amelyek egyrészt jobb és zökkenőmentesebb utazási élményt nyújtanak az utasoknak, másrészt pedig garantálják a magasabb szintű biztonságot mind az utasok, mind az üzemeltetők, mind a lakosság biztonsága érdekében. Ezekre a hálózatba kapcsolt adatvezérelt reagálási képességekre általában intelligens komponensekként utalnak, és ezeket az intelligens összetevőket integrált tárgyak internete (IoT) komponenseként definiálják. Ezek olyan hozzáadott értékű szolgáltatásokat hoznak létre, amelyek adatfeldolgozási képességgel rendelkeznek, az egyszerű adatok összesítésétől kezdve az emberi döntések támogatásáig vagy automatizált válaszig.

Az ENISA tanulmánya[124] részletesen tárgyalja a fenyegetéseket, amelyek egy okos repülőteret érhetnek:

– rosszindulatú cselekmények:
  - szolgáltatásmegtagadással járó támadás (DOS[125]) és elosztott szolgáltatásmegtagadással járó támadás (DDOS[126]);
  - támadások, amelyek eredménye lehet a hálózat kimaradása, a biztonsági ellenőrzések lelassulása, az utasok késése, a járatok törlése, a bizalom elvesztése, a jó hírnév károsodása és pénzügyi kár;
  - szoftverek sebezhetőségének (biztonsági rések) kihasználása;
  - visszaélés hatáskörrel/autorizációval (pl. pszichológiai manipuláció[127] vagy adathalászat[128] segítségével megszerzett hozzáférési információk használata);
  - hálózati/intercepciós támadások (lehallgatás, fizikai manipuláció);
  - repülőtéri eszközök engedély nélküli módosítása (pl. adatok átírása repülőtéri rendszerekben stb.);
  - fizikai hozzáférések vagy adminisztratív kontrollok megsértése (személy- vagy felhatalmazásazonosítás támadása);

---

123 Securing Smart Airports. ENISA, December 2016. https://www.enisa.europa.eu/publications/securing-smart-airports; letöltés: 2021.04.29.

124 Securing Smart Airports. ENISA, December 2016. 4.2.1. Threat taxanomy. https://www.enisa.europa.eu/publications/securing-smart-airports; letöltés: 2021.04.29.

125 Denial of Service – A szolgáltatásmegtagadású támadás egy alkalmazás vagy operációs rendszer ismert gyengeségeit vagy valamilyen speciális protokoll tulajdonságait veszi célba. Az alkalmazás vagy rendszer elérésére feljogosított felhasználókat megakadályozza a számukra fontos információk, a számítógép-rendszer vagy akár a számítógép-hálózat elérésében.

126 Distributed Denial of Service.

127 Social engineering – Amikor egy jogosultsággal rendelkező felhasználó jogosulatlan személy számára bizalmas adatokat ad át, vagy lehetőséget biztosít a rendszerbe történő belépésre a másik személy megtévesztő viselkedése miatt.

128 Phishing – Olyan tevékenység, amikor egy internetes csaló oldal egy népszerű cég hivatalos oldalának mutatja magát, és megpróbál bizonyos személyes adatokat, például azonosítót, jelszót, bankkártyaszámot illetéktelenül megszerezni.

- rosszindulatú szoftver IT-rendszerbe juttatása;
- repülőtéri eszközök fizikai támadása (szabotázs, robbantás, vandalizmus stb.);

– emberi hiba (pl. konfigurációs hiba, eszközök elvesztése, előírások megsértése stb.);

– rendszerhiba (eszközelemek, eszközök, rendszerek meghibásodása, kommunikációs, áramellátási vagy szolgáltatási problémák, hardver meghibásodása, szoftverproblémák stb.);

– természeti katasztrófák (földrengés, szélsőséges időjárás, vulkánkitörés stb.) és társadalmi események (terroristatámadás, instabil politikai viszonyok, zavargások, pandémia stb.), amelyek például üzemanyag-hiányt, fizikai károkat stb. okozhatnak;

– harmadik fél hibái (felhőszolgáltatók, internetszolgáltatók, közművek szolgáltatáskiesései stb.).

A tanulmány részletesen taglalja a támadható felületeket, valamint konkrét támadási szituációkat is elemez (pl. hálózati támadás a poggyászkezelő rendszer ellen) jó gyakorlatok nevesítésével, segítséget nyújtva ezzel mind a biztonsági szakembereknek, mind az ötleteket kereső ártó szándékú személyeknek.

Következtetéseink és megállapításaink az alábbiak:

– az infrastruktúra-elemek műszaki és szervezési adatai sok esetben megtalálhatók az interneten, ezek bizonyos esetekben a terroristák számára hasznosak lehetnek;

– a veszélyes árut szállító jármű elleni támadás következményei sokkal súlyosabbak lehetnek, ezért ezeknek a közlekedési adatoknak a védelme kiemelt fontosságú;

– az egyes terminálok, vasútállomások, dokkok, repülőterek üzemi berendezései az internetes térképekről könnyen azonosíthatók;

– az ártó szándékú cselekmények elkövetéséhez szükséges adatokat tartalmazó szakirodalmak jelentős része az interneten szabadon hozzáférhető;

– a közlekedési szolgáltatók üzemi adatai szintén fontos információkat szolgáltathatnak a terrorcselekmények elkövetői számára, ugyanakkor a közösségi közlekedés esetében ma már elvárt a valós idejű utastájékoztatás;

– egyre nagyobb jelentősége van a harmadik felek általi adatmegosztásnak (pl. forgalomfigyelés stb.);

– a hagyományos, illetve C-ITS-infrastruktúra tekintetében fontos a vezérlő programokhoz, adatbázisokhoz történő illetéktelen hozzáférés megakadályozása, hogy az infrastruktúra-elem betölthesse funkcióját és ne történjenek balesetek;

– az intelligens rendszerek biztonságának kialakításához és fenntartásához jelentős segítséget nyújthatnak az ENISA kiadványai;

– a személyes adatok védelmére rendelkezésre állnak a GDPR adatvédelemre vonatkozó – igen szigorú – előírásai, különös tekintettel az önvezető autókra és a C-ITS-ekre;

– az önvezető járművek tekintetében a jármű irányításának és kommunikációjának védelme az elsőrendű feladat (öngyilkos merényletek elkövetésének lehetősége illetve megakadályozhatósága, az adatvédelem eszközei, *social engineering* stb.).

Megállapításaink alapján a kiberbiztonság minél nagyobb mérvű elérése érdekében a következő javaslatokat tesszük:

– Az intelligens rendszerek (okosrepülőtér, okosvasút, C-ITS), a kapcsolódó járművek és az önvezető járművek tekintetében javasolt olyan biztonsági rendszer kiépítése, amely a lehető legkörültekintőbben veszi figyelembe a kockázatokat, illetve az elérhető technikai színvonalat felhasználva a legkörültekintőbb védelmi rendszert alkalmazza. E védelmi rendszer kialakításakor a GDPR követelményeinek a teljesítése prioritást kell kapjon, mivel a beépített és az alapértelmezett adatvédelem következetes érvényesítése jelentősen megnehezíti a rosszindulatú hozzáférést ezekhez a rendszerekhez.

– Nem javasoljuk a közlekedési üzemi adatok kontrollálatlan közzétételét az interneten. Javasoljuk ugyanakkor meghatározni, hogy ebben a tekintetben mi számít közérdekű és közérdekből nyilvános adatnak, valamint melyek azok az adatkörök, amelyek a nyilvánosságra hozás tekintetében mentességet kell élvezzenek.

– A különleges (veszélyes) szállítási feladatok adatait nem javasoljuk megjeleníteni, illetve a feladat elvégzése után javasoljuk azok azonnali megsemmisítését.

– Fontosnak tartjuk a kutatási szabadság fenntartását, ugyanakkor megfontolásra javasoljuk az érzékeny adatokat tartalmazó szakirodalmak esetében a szerzők megfelelő körültekintését az ilyen adatok nyilvánosságra hozása során (pl. a szakirodalomban található információk minősítése), illetve szükség esetén a kutatási helyek korlátozását könyvtárakra, akár még online formában is.

Az ártó szándékú cselekmények megfelelő végrehajtása csak precíz tervezés után lehetséges. A közlekedési rendszereket bonyolultságuk mellett a szakértők „puha” célpontoknak tartják,[129] mert könnyen hozzáférhetők, és a támadások kivitelezése sem okoz rendkívüli nehézségeket. Mindez persze csak akkor igaz,

[129] HORVÁTH Attila: A vasúti közlekedés terrorfenyegetettségének jellemzői a városokban. Hadmérnök, IV. évfolyam 3. szám, 2009. szeptember. pp. 180–189. http://www.hadmernok.hu/2009_3_horvatha.pdf; letöltés: 2021.04.25.

ha az előkészületek és a tervezés megfelelő szintű. Ehhez megfelelő szaktudás szükséges, amelyhez az információk leginkább a világhálóról, illetve kisebb részben a könyvtárakból beszerezhetők. Az alaposabb szaktudás pénzért (akár ismeretlen eredetűként is, lásd bitcoin) is megszerezhető.

Cikkünkben azt vizsgáltuk, hogy a közlekedési ágazat elleni terrorcselekmények tervezéséhez szükséges információk közül melyek találhatók meg az interneten, és hogy az információs terrorizmus hogyan érvényesülhet a nyílt hálózatokon keresztül.

Vizsgálatunkat mindegyik alágazatban lefolytattuk, valamint röviden kitértünk az önvezető autók kiberbiztonsági problémájára is.

A terrorizmus napjainkban is jelen van, és egyik egyre szélesebb körben elterjedő formája a kiberterrorizmus, amely rohamos terjedésével potenciálisan nagy károkat képes okozni. A kiberterrorizmus a közlekedés területén egyrészt jelenti a közlekedési rendszerek informatikai támadását, illetve a fizikai terrortámadások előkészítéseként a releváns információk megszerzését. Cikkünk vizsgálatai, megállapításai és azok alapján tett javaslataink hozzájárulhatnak ahhoz, hogy a közlekedési ágazatot ténylegesen a gazdaság és a társadalom szolgálatába tudjuk állítani, és ne kelljen tartani terrortámadások miatt a rendszer összeomlásától. Reményeink szerint a javaslatokkal elősegítjük az ENISA 2015-ös dokumentumában[130] megfogalmazott kockázatelemzési hiány csökkentését.

Jelenleg az Info. tv. ad jogszabályi lehetőséget arra, hogy a fellelhető adatokat minősítsük és azokat az internetről eltávolítsák.

A cikkben említett és nyíltan fellelhető közérdekű adatokat komplex módon kell vizsgálni, nem pedig külön álló módon. Nemzetbiztonsági kockázatukat ennek függvényében szükséges vizsgálni.

FELHASZNÁLT IRODALOM

- ‘Jeep hack’ dismissed on the basis of speculation. Automotive World, 2020.05.06. https://www.automotiveworld.com/articles/jeep-hack-dismissed-on-the-basis-of-speculation/; letöltés: 2021.04.21.
- 03/2017. számú vélemény a személyes adatok kooperatív intelligens közlekedési rendszerek (C-ITS) keretében történő kezeléséről. WP 252. A 29. cikk szerinti Adatvédelmi Munkacsoport, 2017.10.04. https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=610171; letöltés: 2021.04.25.
- 1/1975. (II. 5.) KPM-BM együttes rendelet a közúti közlekedés szabályairól (KRESZ). https://net.jogtar.hu/jogszabaly?docid=97500001.kpm; letöltés: 2021.04.25.

[130] Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations. ENISA, December 2015. https://www.enisa.europa.eu/publications/good-practices-recommendations; letöltés: 2021.04.29.

- 101. Radar előtt: így dolgoznak a Hungarocontrol légiforgalmi irányítói. Aeropark Budapest, 2019.11.13. https://www.youtube.com/watch?v=xP_qtbMryl0); letöltés: 2021.04.25.
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. https://net.jogtar.hu/jogszabaly?docid=a1100112.tv; letöltés: 2021.04.25.
- 2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről. https://net.jogtar.hu/jogszabaly?docid=a1200166.tv; letöltés: 2021.04.25.
- A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának. Az együttműködő, intelligens közlekedési rendszerek európai stratégiája – mérföldkő az együttműködő, összekapcsolt és automatizált mobilitás megvalósítása felé. COM(2016) 766 final. Európai Bizottság, Brüsszel, 2016.11.30. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52016DC0766&from=EN; letöltés: 2021.04.25.
- A MÁV-START térképe. http://vonatinfo.mav-start.hu/; letöltés: 2020.12.25.
- A közúti közlekedés területi jellemzői. Központi Statisztikai Hivatal, 2013. augusztus. https://www.ksh.hu/docs/hun/xftp/idoszaki/regiok/debgyorkozutikozl.pdf; letöltés: 2021.04.25.
- A svájci állami vasúttársaság utastájékoztató honlapja. https://sbb.ch/de/kaufen/pages/fahrplan/fahrplan.xhtml; letöltés: 2020.12.25.
- ALLEN, Peter: 'I did it for ISIS': Terror suspect crushes two police motorcyclists with his BMW in Paris leaving one in a coma. MailOnline, 2020.04.27. https://www.dailymail.co.uk/news/article-8262853/I-did-ISIS-Terror-suspect-crushes-two-police-motorcyclists-Paris.html; letöltés: 2021.04.25.
- Az Európai Unió Alapjogi Chartája. Az Európai Unió Hivatalos Lapja, 2016.06.07. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:12016P/TXT&from=EN; letöltés: 2021.04.25.
- Berlin motorway crashes probed as terror attack. BBC News, 2020.08.19. https://www.bbc.com/news/world-europe-53832113; letöltés: 2021.04.12.
- BRANNER, Ricky – VARELA, Catalina: Intel: On Track to the Future – With Smart Railways. Intel Corporation, 2020. https://www.intel.com/content/www/us/en/transportation/resources/smart-railways-ebook.html; letöltés: 2021.04.25.
- CHAPPLE, Theo: Reducing congestion at Blackwall Tunnel with Waze. Digital Blog, 2018.01.11. https://blog.tfl.gov.uk/2018/01/11/waze-partnership-reducing-congestion-at-blackwall-tunnel/; letöltés: 2021.04.25.
- Creating Safer Interconnected Vehicles. IEEE. https://innovationatwork.ieee.org/creating-safer-interconnected-vehicles/; letöltés: 2021.04.25.

- Cyber Security and Resilience of Intelligent Public Transport. Good practices and recommendations. ENISA, December 2015. https://www.enisa.europa.eu/publications/good-practices-recommendations; letöltés: 2021.04.29.
- Cyber Security and Resilience of smart cars. Good practices and recommendations. ENISA, December 2016. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-of-smart-cars; letöltés: 2021.04.29.
- Cybersecurity Challenges In The Uptake Of Artificial Intelligence in Autonomous Driving. ENISA, February 2021. https://www.enisa.europa.eu/news/enisa-news/cybersecurity-challenges-in-the-uptake-of-artificial-intelligence-in-autonomous-driving; letöltés: 2021.04.29.
- DE MONTJOYE, Yves-Alexandre – HIDALGO, César A. – VERLEYSEN, Michel – BLONDEL, Vincent D.: Unique in the Crowd: The privacy boundsof human mobility. Scientific Reports, 2013.03.25. https://www.nature.com/articles/srep01376.pdf; letöltés: 2021.04.25.
- DING-BING, Lin – RONG-TERNG, Juang – HSIN-PIAO, Lin: Mobile location estimation and tracking for GSM systems. 2004 IEEE 15th International Symposium on Personal, Indoor and Mobile Radio Communications, 5-8 Sept. 2004. https://ieeexplore.ieee.org/document/1368838; letöltés: 2021.04.25.
- ENISA Good Practices For Security Of Smart Cars. ENISA, November 2019. https://www.enisa.europa.eu/publications/smart-cars; letöltés: 2021.04.29.
- FÁBOS Róbert: A közlekedési informatikai rendszerek sérülékenysége. In: HORVÁTH Attila – BÁNYÁSZ Péter (szerk.): Fejezetek a kritikus infrastruktúra védelemből – Kiemelten a közlekedési alrendszer. Tanulmánykötet. Magyar Hadtudományi Társaság, Budapest, 2013. pp. 191–225. http://real.mtak.hu/72510/1/KIV_tanulmanykotet.pdf; letöltés: 2021.04.25.
- Flightradar24: Live Flight Tracker. https://flightradar24.com/WZZ2HF/2657fc95; letöltés: 2020.12.25.
- GDPR-t sért(het)nek a Tesla fedélzeti kamerái. GDPR.News.hu, 2020.10.25. https://gdpr.news.hu/cikkek/gdpr-t-serthetnek-a-tesla-fedelzeti-kamerai/; letöltés: 2021.04.25.
- GOODALL, Warwick – FISHMAN, Tiffany Dovey – BORNSTEIN, Justine – BONTHRON, Brett: The rise of mobility as a service – Reshaping how urbanites get around. Deloitte Review, Issue 20, 2017. pp. 113–129. https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/consumer-business/deloitte-nl-cb-ths-rise-of-mobility-as-a-service.pdf; letöltés: 2021.04.25.
- Guidelines 01/2020 on processing personal data in the context of connected vehicles and mobility related applications. Version 2.0. Adopted on 9 March 2021. European Data Protection Board. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202001_connected_vehicles_v2.0_adopted_en.pdf; letöltés: 2021.04.25.
- Hackers Remotely Kill a Jeep on the Highway – With Me in It. Wired, 2015.07.21. https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/; letöltés: 2021.04.21.

- HESSEL, Stefan: The Tesla Sentry Mode – ideas for more data protection and GDPR compliance. LinkedIn, 2020.02.23. https://www.linkedin.com/pulse/tesla-sentry-mode-ideas-more-data-protection-gdpr-stefan-hessel; letöltés: 2021.04.25.
- HORVÁTH Attila: A vasúti közlekedés terrorfenyegetettségének jellemzői a városokban. Hadmérnök, IV. évfolyam 3. szám, 2009. szeptember. pp. 180–189. http://www.hadmernok.hu/2009_3_horvatha.pdf; letöltés: 2021.04.25.
- Internet of Things (IoT). https://www.internetsociety.org/iot/?gclid=Cj0KCQjwgtWDBhDZARIsADEKwgO6IOoVMEWceFmYEMMQVjHRQhXjbcSvwqJD4tfBx7zxBpXGlZfk7gIaAiigEALw_wcB; letöltés: 2021.04.25.
- KISS Gábor – BERECZ Csilla Éva – TÓTH László: A jövő közlekedése vagy sebezhető eszköz az önvezető autó? Bánki Közlemények, 2. évfolyam 1. szám, 2019. pp. 5–10. http://bk.bgk.uni-obuda.hu/index.php/BK/article/download/105/54/; letöltés: 2021.04.25.
- KOVÁCS Ágnes Lilla: Rések a pajzson. Ludovika Egyetemi Kiadó, 2021.03.22. https://www.ludovika.hu/magazin/aula/2021/03/22/resek-a-pajzson/; letöltés: 2021.04.25.
- KOVÁCS László – KRASZNAY Csaba: Digitális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. Nemzet és Biztonság, 2010/1. szám. pp. 44–56. http://www.nemzetesbiztonsag.hu/cikkek/kovacs_laszlo__krasznay_csaba-digitalis_mohacs_.pdf; letöltés: 2021.04.25.
- KOVÁCS László – KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint. Nemzet és Biztonság, 2017/1. szám. pp. 3–16. http://www.nemzetesbiztonsag.hu/cikkek/nb_2017_1_03_kovacs_laszlo-krasznay_csaba_-_digitalis_ mohacs_2.0_kibertamadasok_es_kibervedelem_a_szakertok_szerint.pdf; letöltés: 2021.04.25.
- KOVÁCS László: A kibertér védelme. Dialóg Campus Kiadó, Budapest, 2018. https://www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf; letöltés: 2021.04.25.
- KOVÁCS László: Az információs terrorizmus eszköztára. Robothadviselés 6. tudományos szakmai konferencia, 2006. november 22. Hadmérnök, Különszám, 2006. http://hadmernok.hu/kulonszamok/robothadviseles6/kovacs_rw6.pdf; letöltés: 2021.03.08.
- Kőröshegyi völgyhíd. Wikipédia, 2021.02.24. https://hu.wikipedia.org/wiki/K%C5%91r%C3%B6shegyi_v%C3%B6lgyh%C3%ADd; letöltés: 2021.04.25.
- LÉVAI Zsolt – ÜVEGES András József: A vasúti közlekedés informatikai adatvédelme. Felderítő Szemle, XIX. évfolyam 2. szám, 2020. pp. 103–139. https://www.knbsz.gov.hu/hu/letoltes/fsz/2020-2.pdf; letöltés: 2021.04.25.
- LÉVAI Zsolt: Közlekedésbiztonság. Dialóg Campus Kiadó, Budapest, 2019. https://nkerepo.uni-nke.hu/xmlui/bitstream/123456789/15740/1/670_HHK_Kozelekedesbiztonsag.pdf; letöltés: 2021.04.25.

- Magyarország Alaptörvénye (2011. április 25.). VI. cikk (3) bekezdés. https://net.jogtar.hu/jogszabaly?docid=a1100425.atv; letöltés: 2021.04.25.
- MÁNDOKI Péter (szerk.): Közlekedés és társadalom. Budapest, 2010. pp. 39–40. https://dtk.tankonyvtar.hu/xmlui/bitstream/handle/123456789/3251/Mandoki_Kozlekedes_es_tarsadalom.pdf?sequence=1&isAllowed=y; letöltés: 2021.04.25.
- MANSOUR Elie – SLEIMAN, Georges Abi: Beirut Municipality Rapid Building-level Damage Assessment. Municipality of Beirut and UN-Habitat. Working Version, October 2020. https://unhabitat.org/sites/default/files/2020/10/municipality_of_beirut_-_beirut_explosion_rapid_ assessment_report.pdf; letöltés: 2021.04.25.
- MÁV-START Zrt. – Közérdekű adatok. https://www.mavcsoport.hu/mav-start/bemutatkozas/kozerdeku-adatok; letöltés: 2021.04.25.
- MÁV-START Zrt. – Vonatösszeállítás (SzVÖR). https://www.mavcsoport.hu/mav-start/bemutatkozas/belfoldi-utazas/vonatosszeallitas-szvor; letöltés: 2021.04.25.
- Menetrendi ábrák 2019-2020 éves. https://www2.vpe.hu/menetrendi_abrak/2019_2020; letöltés: 2021.04.25.
- Mi a terrorizmus? Biztonságpolitikai Szemle, Corvinák, Terrorizmus – 2. Új típusú biztonsági kihívások. https://web.archive.org/web/20160417115546/http://biztpol.corvinusembassy.com/?module=corvinak&module_id=4&cid=32; letöltés: 2021.04.25.
- PAPP Zoltán István: A kiberterrorizmus módszerei, lehetséges eszközei és az ezek ellen történő védekezés alternatívái. Doktori (PhD) értekezés. NKE, Katonai Műszaki Doktori Iskola, Budapest, 2018. https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/Papp_Zoltan_PhD_ertekezes_tervezete.pdf; letöltés: 2021.04.25.
- Personal data in transport: exploring a framework for the future. Open Data Institute, 2018. https://theodi.org/wp-content/uploads/2018/06/OPEN-Personal-data-in-transport-.pdf; letöltés: 2021.04.25.
- Port of Rotterdam. https://www.google.com/maps/place/Port+of+Rotterdam/@51.8925899,4.3544751,1110m/data=!3m1!1e3!4m5!3m4!1s0x47c43364d44f9f39:0xc5831d410339551e!8m2!3d51.9047712!4d4.4845515; letöltés: 2021.04.29.
- Real-time Flight Status and Radar for All US/Canada Flights. FlightAware, 2016.04.06. https://flightaware.com/news/article/Realtime-Flight-Status-And-Radar-For-All-USCanada-Flights/223; letöltés: 2021.04.25.
- RUSSON, Mary-Ann: The cost of the Suez Canal blockage. BBC News, 2021.03.29. https://www.bbc.com/news/business-56559073; letöltés: 2021.04.25.
- SANTAA, José – PEREÑÍGUEZA, Fernando – MORAGÓNA, Antonio– SKARMETAA, Antonio F.: Experimental Evaluation of CAM and DENM Messaging Services in Vehicular Communications. Transportation Research Part C: Emerging Technologies, Volume 46, September 2014. pp. 98–120.

- SCHUETZE, Christopher F. – EDDY, Melissa – BENNHOLD, Katrin – KOETTL, Christoph: Terrorist Shooting in Capital of Austria. The New York Times, 2020.11.03. https://www.nytimes.com/2020/11/02/world/europe/vienna-shooting.html; letöltés: 2021.04.07.
- Securing Smart Airports. ENISA, December 2016. https://www.enisa.europa.eu/publications/securing-smart-airports; letöltés: 2021.04.29.
- SERBAKOV Márton Tibor: A terrorizmus definíciójának kérdése. Büntetőjogi Szemle, 2019/2. szám. pp. 87–100. https://ujbtk.hu/wp-content/uploads/lapszam/BJSz_201902_87-100o_SerbakovMarton.pdf; letöltés: 2021.03.24.
- ShopVille-Zürich Hauptbahnhof – herzlich willkommen. https://www.sbb.ch/de/bahnhof-services/am-bahnhof/bahnhoefe/shopville-zuerich-hauptbahnhof.html; letöltés: 2021.04.25.
- Space Strategy for Europe, COM (2016) 705 final. https://stip.oecd.org/stip/policy-initiatives/2019%2Fdata%2FpolicyInitiatives%2F26561; letöltés: 2021.04.25.
- SZÁSZI Gábor: A vasúti közlekedési alágazat, mint kritikus infrastruktúra. In: HORVÁTH Attila – BÁNYÁSZ Péter (szerk.): Fejezetek a kritikus infrastruktúra védelemből – Kiemelten a közlekedési alrendszer. Tanulmánykötet. Magyar Hadtudományi Társaság, Budapest, 2013. pp. 167–190. http://real.mtak.hu/72510/1/KIV_tanulmanykotet.pdf; letöltés: 2021.04.25.
- Tableau européen des services directs. https://viaggiandoavapore.files.wordpress.com/2019/12/ewp-2013-1.pdf; letöltés: 2021.04.25.
- TÁLAS Péter: A nemzetközi terrorizmus és a szervezett bűnözés hatása a nemzetközi biztonságra és Magyarország biztonságára. Budapest, 2007. http://kisebbsegkutato.tk.mta.hu/uploads/files/archive/904.pdf; letöltés: 2021.03.24.
- The worst Islamist attack in European history. The Guardian, 2007.10.31. https://www.theguardian.com/world/2007/oct/31/spain; letöltés: 2021.04.12.
- TOKODY Dániel – ALBINI Attila – ADY László – TEMESVÁRI Zsolt Marcell – RAJNAI Zoltán: Kiberbiztonság az autóiparban. Bánki Közlemények, 1. évfolyam 3. szám, 2018. pp. 71–77. http://bk.bgk.uni-obuda.hu/index.php/BK/article/download/79/47/; letöltés: 2021.04.25.
- Twelfth report of the Secretary-General on the threat posed by ISIL (Da'esh) to international peace and security and the range of United Nations efforts in support of Member States in countering the threat. United Nations Security Council, 29 January 2021. https://undocs.org/en/S/2021/98; letöltés: 2021.03.24.
- VPE Vasúti Pályakapacitás-elosztó Kft. – Menetrend Ábrák 2020/2021 éves kiutalások. https://www2.vpe.hu/menetrendi_abrak/2020_2021; letöltés: 2021.04.25.
- WHITTAKER, Zack: Security bugs let these car hackers remotely control a Mercedes-Benz. Tech Crunch, 2020.08.07. https://techcrunch.com/2020/08/06/security-bugs-mercedes-benz-hack/; letöltés: 2021.03.11.

KÁROLY LÁSZLÓ ALEZREDES

EGYSÉGES FELDERÍTŐRENDSZER KIALAKÍTÁSA A VÁLSÁGKEZELŐ MŰVELET MEGINDÍTÁSA ELŐTT

Bevezetés

A 21. században a konfliktusok jellege és természete gyökeresen megváltozott. Új fogalmakat kellett megismernünk és megtanulnunk az értelmezésüket. Ehhez egy teljesen újfajta gondolkodás kell, amely folyamatos rugalmasságot és az újhoz történő alkalmazkodást igényel. Véleményem szerint a változás fontosságának a felismerése és a megváltozott környezethez történő minél gyorsabb alkalmazkodási képesség a legfontosabb katonai tulajdonságok közé került.

A világban teljesen újfajta válságokkal nézünk szembe. Ilyenek a migráció, a járványok, az ivóvízhiány, az élettérért folyó harc, a klímaváltozás, a bukott államok, a terrorizmus stb. E válságok megoldásában szinte minden alkalommal részt vesznek a fegyveres erők – akár vezető, akár támogató szerepkörben. Ezekben a műveletekben a fegyveres erők vezetői gyakran újfajta kihívásokkal néznek szembe, olyanokkal, amelyekkel korábban nem találkoztak. Itt nem működik az, hogy nézzük meg, mit csináltak elődeink az előző háborúban, és kövessük az ő műveleti elveiket, mert a korábbi tapasztalatok valószínűleg nem alkalmazhatók az adott műveletben. Nem léteznek szabályzatok és műveleti utasítások, amelyek alapján végre lehet hajtani a feladatot. Ezekben a válságokban és konfliktusokban szinte minden esetben elölről kell kezdeni a műveleti eljárások kialakítását, a parancsnokoknak a saját kreativitásuk és rugalmasságuk adja a feladatok megoldásának az alapját.

Az új típusú fenyegetések kezelésére létrehozott válságkezelő műveletek új elemként jelentek meg a modern kor hadviselésében. A válságkezelő műveleteknek számos fogalma létezik. Ebben az elemzésben minden olyan nemzetközi műveletet annak tekintek, amely az adott válság nemzetközi normák szerinti rendezésére irányul, és célját katonai, politikai, gazdasági, információs és társadalmi eszközökkel kívánja elérni. ***Válságkezelő (reagáló) műveletek:*** *ide tartozik minden olyan katonai művelet, amely nem köthető a NATO-alapszerződés 5. cikkéhez. A konfliktus területén a békefolyamat támogatása érdekében alkalmazott műveleteket nevezik béketámogató műveleteknek. A béketámogató műveletek közé tartoznak a békefenntartó és a béketeremtő, valamint a konfliktusmegelőző, illetve a humanitárius műveletek.*[1]

A válságkezelő műveleteknek több fajtája van, de jelen tanulmányban azokat az aszimmetrikus konfliktusok vonatkozásában fogom vizsgálni. „*Az aszimmetrikus hadviselés pontosan körvonalazott, politikai célok érdekében folytatott, gyakran több szervezet ideológiai, vallási, etnikai közösségen alapuló katonai és nem katonai*

[1] VASTAGH László: NATO: válságkezelés és missziók. honvédelem.hu, 2010.11.23. https://honvedelem.hu/hirek/nato-valsagkezeles-es-missziok.html; letöltés: 2019.08.12.

műveleteket, eljárásokat és módszereket alkalmazó közvetlen és közvetett hatásokra építő és egymás hatásait felerősítő, a biztonság különböző dimenzióinak területét veszélyeztető harcmodor, főként harcászati eljárás, amelyek együttes hatásával kényszeríthetjük akaratunkat az ellenségre."[2]

Jelen tanulmányban nem részletezem az aszimmetrikus konfliktusok sajátosságait, mindössze a jobb érthetőség miatt mutatom be röviden. Az aszimmetrikus konfliktusokban a szemben álló felek technikailag és – általában – létszámukat tekintve nem egyenlők. Megkülönböztetünk „erősebb" és „gyengébb" felet. Jellemzői, hogy az „erősebb" fél hagyományos hadviselési elveket, míg a „gyengébb" fél nem hagyományos hadviselési elveket alkalmazva igyekszik a céljait megvalósítani. A hagyományos oldalról történő megközelítés során reguláris erők alkalmazása, klasszikus katonai manőverek, tűzvezetés és vezetés-irányítási rendszerek jelennek meg. Ezzel szemben a konfliktus nem hagyományos megközelítése terrorcselekmények elkövetését, lakosság befolyásolását, pszichológiai műveleteket és gerilla-hadviselést jelent.[3]

Ahhoz, hogy a parancsnokok ilyen újfajta műveleti környezetben eredményesen tevékenykedhessenek megfelelő minőségű, mennyiségű és időszerű információra van szükségük. Ez nem új keletű gondolat, mert amióta létezik hadviselés, mindig is szükség volt rá. A 21. század műveleteiben ezek jellege azonban megváltozott. Az egyik legfontosabb tényezővé a műveleti tempó miatt a gyorsaság vált. A felderítési információigény már nemcsak katonai jellegű lehet, hanem a biztonság valamennyi – politikai, gazdasági, kulturális, társadalmi, információs stb. – szegmensét érintheti. Ilyen információkat csak összadatforrású felderítésben gondolkodó és egységes felderítőrendszer tudja biztosítani számukra.

Ebben a tanulmányban röviden bemutatom az összadatforrású felderítést és az egységes felderítőrendszert. Igyekszem rámutatni, hogy mennyire fontos a felderítőrendszert már a kontingens műveleti készenlétét megelőzően kialakítani, mert a parancsnokoknak már a műveleti készenléthez is pontos információkra van szükségük. Emiatt a kialakítást már a hazai bázison meg kell kezdeni, közvetlenül a kontingens összeállítása után. A műveleti területre történő kiérkezés után már nincsen idő, ott csak a helyi sajátosságoknak megfelelően kell a felderítőrendszert pontosítani, illetve a nemzetközi együttműködésre kell a hangsúlyt helyezni. Fontos már az elején leszögezni, hogy a felderítési készenlét nem egyenlő a kontingens műveleti készenlétével. A felderítést hamarabb be kell vezetni, hogy az érdemben hozzá tudjon járulni a kontingens feladatainak a megkezdéséhez.

A téma megértésének elősegítése céljából csak röviden mutatom be egy válságkezelő műveletben részt vevő kontingens szerepvállalásának fázisait. A részletes ismertetés egy külön publikáció témája lehetne.

---

[2] RESPERGER István – KISS Álmos Péter – SOMKÚTI Bálint: Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással. Zrínyi Kiadó, Budapest, 2013. p. 23.

[3] ARREGUIN-TOFT, Ivan: How The Weak Win Wars – A Theory Of Asymmetric Conflict. International Security, Volume 26, Issue 1, July 2001. pp. 93–128. https://web.stanford.edu/class/polisci211z/2.2/Arreguin-Toft%20IS%202001.pdf; letöltés: 2015.02.08.

Írásomban az egységes felderítőrendszer elméleti felépítését mutatom be. Nem célom, hogy a Magyar Honvédség, más nemzet, vagy külföldön szolgálatot teljesítő kontingens felderítőrendszerét elemezzem. Munkám aktualitásának azt tekintem, hogy a Magyar Honvédség bármikor kaphat feladatot egy új nemzetközi válságkezelő műveletben történő részvételre. Ebben az esetben ki kell alakítani a kontingens vonatkozásában az egységes felderítőrendszert. Ehhez kívánok hozzájárulni.

Összadatforrású felderítés[4]

A kontingens felderítésének a műveleti környezet valamennyi szegmenséről információkat kell gyűjtenie, ehhez pedig minden adatszerzési módot alkalmaznia kell. Ezek kiegészítik egymást, és egyik sem élvezhet prioritást. Az adatgyűjtési tervet ennek megfelelően kell elkészíteni, eközben minden lehetőséget figyelembe kell venni.[5] Az információszerzési lehetőségeket négy csoportra oszthatjuk:

- az adott hadszíntéren a nemzetközi erők által üzemeltett, minden szövetséges partner részére hozzáférhető, informatikai hálózaton létrehozott adatbázisok;
- külön igénylésre a szakemberek által készített anyagok (például kapcsolati háló, incidenslista stb.);
- a nemzeti hírszerzés által biztosított információk;
- saját erőforrásból megszerzett információk (pl. járőrök, forráshálózat működtetése, lehallgatóberendezések stb.).

Az összadatforrású felderítésnél fontos, hogy minden felderítési ág lehetőségeit ki kell használni. Az adatok megszerzése céljából a kontingensek és a nemzetközi művelet felderítőszervezetei emberi erővel folytatott felderítést (Human Intelligence – HUMINT), rádióelektronikai felderítést (Signals Intelligence – SIGINT), képfelderítést (Imagery Intelligence – IMINT), nyílt forrású információszerzést (Open Source Intelligence – OSINT), kiberhírszerzést (Cyber Intelligence – CYBINT) folytathatnak, valamint egyéb adatszerzési módokat is alkalmazhatnak.

A válságkezelő műveletekben fontos információszerző lehetőség lehet egy merénylet, egy ellenálló elfogása és egy kutató-felszámoló művelet után végzett helyszínelés is.[6] Az itt megtalált számítástechnikai eszközök, fegyverzeti anyagok, ujjlenyomatok stb. információkat rejthetnek. Véleményem szerint ezeket nem lehet egy adott adatszerzési módba besorolni, mert lehet IMINT (fényképek vizsgálata), vagy számítástechnikai eszközökön tárolt adatok lementése (CYBINT) stb.

---

[4] KÁROLY László: Az összadatforrású felderítés az aszimmetrikus konfliktusokban. Felderítő Szemle, XIV. évfolyam 3. szám, 2015. szeptember. p. 92. https://www.knbsz.gov.hu/hu/letoltes/fsz/2015-3.pdf; letöltés: 2017.04.11.

[5] CONNABLE, Ben: Military Intelligence Fusion for Complex Operation – A New Paradigm. RAND National Defence Research Institute, 2012. pp. 20–21. https://www.rand.org/content/dam/rand/pubs/occasional_papers/2012/RAND_OP377.pdf; letöltés: 2015.02.08.

[6] Tactical Site Exploitation and Cache Search Operations. Tactics, Techniques, and Procedures. Center for Army Lessons Learned (CALL), Handbook, No. 07-26, May 2007. p. 31. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB410/docs/Tactical%20Site%20Exploitation.pdf; letöltés: 2015.02.08.

A modern kori hadviselésben egyre nagyobb szerepet tölt be a magánszektor szerepe, különösen a hírszerzés és a logisztika területén. Ezek a cégek kiváló információszerző lehetőségekkel és elemzői képességekkel rendelkeznek, emiatt létfontosságú velük az együttműködés kialakítása. A műveleti területen potenciális információforrásként kezelendők a felderítőrendszer számára.[7]

Megállapítható, hogy a 21. század válságkezelő műveleteiben tevékenykedő kontingensparancsnokok információigényeit csak olyan felderítőrendszer tudja kielégíteni, amely minden szóba jöhető adatszerző lehetőséget kihasznál, és azokat kombinálva, az előnyös tulajdonságaikat figyelembe véve alkalmazza.

Egységes felderítőrendszer[8]

A 21. század válságkezelési műveletei komplexitása miatt fontos az egységes rendszerek használat, mint például kommunikációs/informatikai rendszer, logisztikai szabványrendszer, egészségügyi kiürítési rendszer, személyi azonosító okmányok, biztonsági tanúsítványrendszer és természetesen a felderítőrendszer. Ezzel lehet az adott rendszerben működő részelemeket és képességeket térben és időben összehangoltan alkalmazni. Egy adott rendszer elemei önállóan is jelentős képességekkel bírnak, de szoros együttműködésben és közös alkalmazásban sokkal hatékonyabbak. Egy adott rendszer elemei kiegészítik egymást, támogatják a másik működését. Alfred Rolington gondolata: „*egy rendszer működésének hatékonyságát a részegységek tevékenységének megfelelő koordinálása növeli*.”[9] Ez a koordináció pedig az egységes vezetés feladata.

Az egységes felderítőrendszernek is egységes irányítás alatt kell működnie, és így az információszerzésbe bevont erők és képességek tevékenységét össze lehet hangolni. A cél, hogy elkerüljük a duplikációt és a képességek felhasználása optimális legyen. Az egységes felderítőrendszer irányítása és működtetése az adott kontingens felderítőfőnökének a feladata. A rendszer magában foglalja az irányító és az adatszerző (szervezetszerű és nem szervezetszerű), feldolgozó, elemző-értékelő és tájékoztató elemeket.

Az egységes felderítőrendszer **horizontálisan** három nagy területet és egyéb kiegészítő elemeket foglal magában:

- katonai felderítés;
- nemzeti hírszerzés;[10]

---

[7] SZALAI Gábor: A nemzeti hírszerzés és a magánszektor kapcsolatának alapkérdései az USA-ban. Hadtudományi Szemle, 1. évfolyam 2. szám, 2008. pp. 22–29. http://epa.oszk.hu/02400/02463/00002/pdf/EPA02463_hadtudomanyi_szemle_2008_2_022-029.pdf; letöltés: 2015.02.15.

[8] KÁROLY László: Az egységes felderítőrendszer bemutatása az aszimmetrikus konfliktusokban. Felderítő Szemle, XV. évfolyam 4. szám, 2016. december. pp. 42–61. https://www.knbsz.gov.hu/hu/letoltes/fsz/2016-4.pdf; letöltés: 2017. 04.11.

[9] ROLINGTON, Alfred: Hírszerzés a 21. században – A mozaikmódszer. Antall József Tudásközpont, Budapest, 2015. p. 170.

[10] Alapszervezete a Nemzeti Hírszerző Elem (National Intelligence Cell – NIC) és az alárendelt szervezete a Nemzeti Hírszerző Támogató Elem (National Intelligence Support Team – NIST).

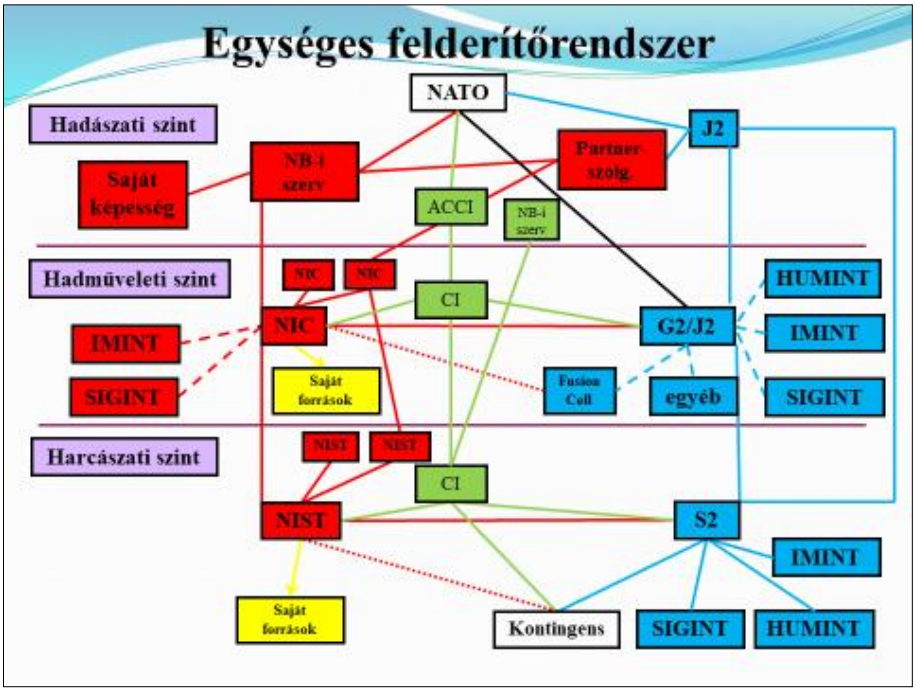
– elhárítás;[11]

– egyéb kiegészítő elemek.

Továbbá az egységes felderítőrendszer is katonai **vertikális** formát követ, vagyis beszélhetünk harcászati, hadműveleti és hadászati szinten lévő szervezeti elemekről.

Az egységes felderítőrendszerben a vertikális és a horizontális részeket együttesen kell értelmezni.

Egy adott válságkörzetben megjelennek a korábban már említett civil szervezetek és vállalatok is, amelyek rendelkezhetnek adatszerző képességgel. Ilyenek például a nemzetközi elemző vállalatok (Stratfor), magán biztonsági vállalatok, diplomáciai képviseletek és segélyszervezetek. Véleményem szerint megközelítés kérdése, hogy ezeket a felderítőrendszer részeinek vagy adatforrásoknak tekintjük. A velük való együttműködést ki kell alakítani.



1. ábra. Az egységes felderítőrendszer elvi felépítésének vázlata[12]
(piros = nemzeti hírszerzés, zöld = elhárítás, kék = katonai felderítés)
Szerkesztette: Károly László

[11] Az elhárítás feladatai közül az egységes felderítőrendszerben a biztonsági helyzettel kapcsolatosakat kell érteni, és nem része a kontingens személyi állományának nemzetbiztonsági védelme és ellenőrzése.

[12] Az egységes felderítőrendszer elvi felépítésének ábráját legelőször Müller Zsolt őrnagy dolgozta ki a Magyar Honvédség afganisztáni szerepvállalásának kezdetén, 2006-ban.

Az egységes felderítőrendszer katonai szervezet, tehát a vertikális alá- és fölérendeltségi viszonyt be kell tartani. Fontossága abban rejlik, hogy a rendszer bármelyik pontján keletkező információigényt és a megszerzett információt képes eljuttatni a rendszer egy adott vagy valamennyi szegmenséhez, mert a vertikális és a horizontális kapcsolat is rendelkezésre áll. Így a rendszer megsokszorozza a saját képességét, ezzel a hatékonyságát is jelentősen megnöveli. Az adott válságkezelő műveletben valamennyi nemzeti kontingens kialakít hasonló rendszert, amelyeknek több közös pontjuk van. Ezzel az egész műveleti terület le van fedve, és megvalósul a hálózatközpontú felderítés.[13]

Egy katonai művelet fázisainak rövid bemutatása

Egy válságkezelő műveletben a katonai kontingens szerepvállalásának négy jelentős fázisa van:

a) honi területen történő felkészülés;

b) felkészülés folytatása a műveleti területen, készenlét elérése;

c) feladatok végrehajtása a műveleti területen;

d) felkészülés a kivonásra és kivonás.

a) Először egy állam politikai vezetőiben megfogalmazódik az elgondolás a részvételről egy adott műveletben. Megkezdődik az információk összegyűjtése annak jellegéről, a várható kockázatokról, a politikai előnyökről és hátrányokról, az érdekek érvényesítésének lehetőségeiről stb. A politikai döntés megszületése után kezdődik meg a konkrét felkészülés a feladat végrehajtására, megalakul a kontingens, megkezdődik a speciális kiképzés, amely rengeteg személyügyi, felderítési, hadműveleti, logisztikai, híradó/informatikai stb. feladatokkal jár. A felkészülés után történik a kontingens kitelepítése a műveleti területre.

b) A műveleti területen folytatódik a kontingens olyan speciális felkészítése, amelyet hazai területen nem lehet végrehajtani. Ekkor kerülnek kialakításra az élet- és munkafeltételek, a parancsnokok megszervezik a még specifikusabb kiképzési foglalkozásokat, megszervezik a nemzetközi együttműködés részleteit stb. Ezeket a feladatokat vagy már a műveleti területen, vagy egy műveleti területen kívüli felvonulási területen hajtják végre. Ennek a fázisnak a végén éri el a kontingens a műveleti készenlétet.

c) Ebben a fázisban az adott kontingens végrehajtja a rendeltetésszerű feladatait a nemzetközi kötelék részeként. Fontosnak tartom megjegyezni, hogy a feladatrendszer a folyamatosan változó műveleti helyzet függvényében változhat, ami folyamatos kiképzést és alkalmazkodási képességét követel meg. Időtartama a politikai döntéstől függ.

---

[13] CORDESMAN, Anthony H.: The Intelligence lessons of the Iraqi Wars(s). Center for Strategic and International Studies, Washington, 2004. pp. 11–12. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/iraq_intelligenceiraqiwar.pdf; letöltés: 2015.03.21.

d) A válságkezelő művelet végéhez közeledve a kontingens megkezdi a felkészülést a feladatok befejezésére vagy átadására, majd a kivonulásra. Ez történhet azért, mert a válságkezelő művelet elérte célját, vagy valamilyen ok miatt a kontingenst kivonják az adott műveleti területről. Mindkét esetet szintén politikai döntés előz meg.

Ezekhez a fázisokhoz kapcsolódik az egységes felderítőrendszer kialakítása, működtetése és felszámolása is. Mindegyik fázisban meghatározott jellegű feladatrendszert kell végrehajtania, ugyanis részfeladatok már az első fázisban is megjelennek. Ez azt jelenti, hogy olyan speciális eset áll elő, hogy a megalakításnak és az egyes elemei működésének párhuzamosan már mennie kell.

Az egységes felderítőrendszert a honi területen történő felkészülés, illetve a műveleti területen lévő felkészülés fázisaiban kell kialakítani. Arra kell törekedni, hogy az első fázisban a lehető legtöbb munkát el kell végezni, mert a műveleti területre történő megérkezés után már nagyon kevés idő fog rendelkezésre állni. Nem győzöm eleget hangsúlyozni, hogy a felderítési készenlétet az adott kontingens műveleti készenléténél megelőzően el kell érni.

Az egységes felderítőrendszer kialakítása

A politikai döntés után megkezdődik a kontingens összeállítása, amelynek állománytáblája, feladatrendszere, létszáma stb. követi a mandátumban meghatározott tényezőket. A feladatrendszer adja az egységes felderítőrendszer alapját is, mert a mandátum ismeretében derül ki, hogy milyen szervezetszerű felderítőerőket, milyen jellegű felderítőtörzset és milyen nemzeti hírszerző támogatást kell megszervezni. Az adott állam nemzetbiztonsági szolgálata(i) – egyeztetve a megalakításért felelős katonai szervezettel – fog(nak) döntést hozni a nemzeti hírszerző és elhárító elemekről. Vagyis az első és talán a legfontosabb lépés az egységes felderítőrendszer kialakításához tisztázni a kontingens feladatrendszeréhez kapcsolódó felderítő- és nemzetbiztonsági elemek összetételét.

A különböző feladatrendszerű kontingenseknek gyökeresen eltérő információigényei lehetnek. Fontos meghatározni, hogy a kontingensnek azért kellenek a biztonsági helyzetről információk, mert támadó jellegű feladatokat fog végrehajtani, és a kezdeményezés megragadása a cél (különleges műveleti csoportok kinetikus műveletei), vagy pedig azért kellenek az információk, hogy elkerüljék a konfrontációt az ellenállókkal/terroristákkal/felkelőkkel (MH Tartományi Újjáépítési Csoport). Ez a kettősség merőben más követelményeket fog az egységes felderítőrendszer elé is állítani.

A következő lépésben kijelölésre kerül a személyi állomány. Fontossága abban rejlik, hogy megtudjuk ki lesz a felderítőfőnök – mert ő a legfontosabb, legmeghatározóbb személy –, illetve kiderül, kik lesznek a hírszerző és az elhárító elemek vezetői, illetve kiket válogatnak be a személyi állományukba.

Megjegyzés: az államok többségében egy adott kontingens hírszerző és elhárító állománya nem a haderőből, hanem egy nemzetbiztonsági szolgálattól kerül ki. Személyükre a kontingenst megalakító szervezetnek és a kontingensparancsnoknak nincsen befolyása. A közös felkészülés végrehajtása érdekében előnyös, ha minél hamarabb kiderül a személyük és csatlakoznak a kontingenshez. Ez kulcsfontosságú az egységes felderítőrendszer hatékony kialakítása érdekében is.

Az egységes felderítőrendszer kialakítását megelőzően tisztázni kell, hogy melyik nemzetközi szervezet „szárnya" alatt jött létre a válságkezelő művelet, vagy pedig egy koalíciós műveletről beszélünk. Ez utóbbi történt az Amerikai Egyesült Államok vezette koalíciónak az ENSZ BT határozata nélküli, az Iszlám Állam ellen folytatott tevékenysége során Irakban és Szíriában 2014-től. Fontossága abban rejlik, hogy az adott nemzetközi szervezet korlátozásokat vezethet be, így például ENSZ-műveletben nem lehet NIC-et telepíteni.

A felderítőrendszer kialakítása előtt a kijelölt felderítőfőnök feladata, hogy a kontingensparancsnokkal tisztázza szándékát és értesse meg vele ennek fontosságát. Magyarázza el, hogy ez nem öncélú tevékenység, hanem a kontingens támogatása érdekében történik. A parancsnok pedig értse meg, hogy ez egy rendszer, amelynek irányítója a felderítőfőnök. A felderítési doktrínák szerint mindig az adott szintű parancsnok felel a felderítés megszervezéséért, tehát a parancsnoknak előnyére válik egy agilis, produktív és jól felkészült felderítőfőnök támogatása. A parancsnoknak folyamatos támogatást kell nyújtania a felderítőfőnök számára abban, hogy utasítást ad az alegységparancsnokoknak a felderítőfőnök támogatása érdekében. Ennek oka, hogy minden alegység képes valamilyen szintű információgyűjtésre, aminek a koordinálását a felderítőfőnök hajtja végre. Az alegységparancsnokoknak ebben együttműködést kell mutatniuk, mert ők a munkájuk során is erre az egységes felderítőrendszerre támaszkodhatnak. Ezért nekik is segíteniük kell a rendszer működését. Sajnos az elmúlt évek tapasztalatai azt mutatták, hogy ez nem minden esetben volt evidencia, és a felderítőfőnöknek komoly „harcot" kellett vívnia néhány alegységparancsnokkal az együttműködés érdekében. Ennek az együttműködésnek a gördülékenységét tudják támogatni a kontingensparancsnoknak az egységes felderítőrendszert támogató feladatszabásai. A vezető beosztású személyeknek – kiemelten a felderítőfőnöknek – kiemelkedő menedzseri tulajdonságokkal kell rendelkezniük.[14]

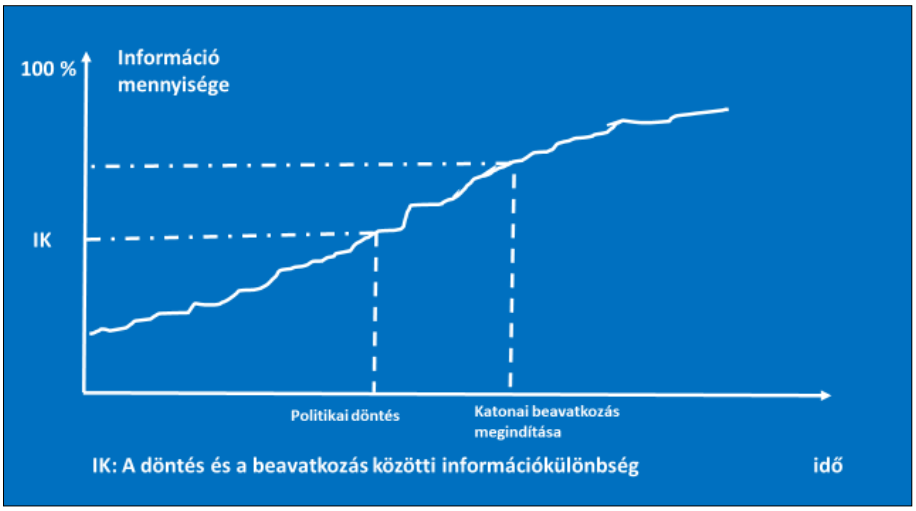
Az egységes felderítőrendszer kialakítása természetesen nagymértékben függ a rendelkezésre álló képességektől és technikai eszközöktől. Általános elv, hogy az adott haderőben rendelkezésre álló legmodernebb eszközöket szokták kiküldeni a műveleti területre. Abban az esetben, ha a konkrét technikai eszközök beszerzése a művelettel kapcsolatban történik, akkor figyelembe kell venni a rendszerbe állítás folyamatát és a kiképzés időigényét is.

[14] LAHNEMAN, William J.: The Future of Intelligence Analysis. Final Report, Volume 1. Department of Security Studies and International Affairs, Daytona Beach, 2006. pp. 14–16. https://commons.erau.edu/cgi/viewcontent.cgi?article=1000&context=db-security-studies; letöltés: 2015.02.16.

Az egységes rendszer kialakítása során úgy kell gondolkodni, hogy először a kontingens és az egyéni beosztásokban szolgáló saját katonáink, illetve a hazai politikai és katonai vezetők és nemzetbiztonsági szervezetek információigényét legyen képes kielégíteni. Utána legyen képes minél több saját forrásból származó információt átadni a nemzetközi művelet felderítőrendszerébe. Legvégül legyen képes elemzett információkat küldeni a NATO és az EU adott szervezeti elemeinek is.[15] Sajnos a kapacitás hiánya miatt gyakran előfordul, hogy a felderítőfőnöknek prioritási sorrendet kell felállítania. Ebben az esetben az előbbiekben bemutatott sorrendet kell követnie. Az első mindig a saját nemzet katonája!

Az egységes felderítőrendszer kialakítása honi területen

Miután az előző alfejezetben bemutatott tényezők tisztázásra kerültek, akkor a felderítőfőnök irányításával megkezdődhet az egységes felderítőrendszer kialakítása. A folyamat során figyelembe kell venni egy fontos tényezőt. A felkészülés előrehaladtával egyre több információval fogunk rendelkezni a műveleti terület sajátosságairól, az ellenség képességeiről, a műveleti környezetről, a lakosságról, a veszélytényezőkről stb. A műveleti környezet szélesebb ismeretét és a rendelkezésre álló információkat minden esetben figyelembe kell venni, és képesnek kell lenni a felderítőrendszer kialakítását menet közben módosítani, amennyiben az szükséges. Az alábbi ábra mutatja, hogyan változik a rendelkezésre álló információ mennyisége az idő előrehaladtával.



2. ábra. A rendelkezésre álló információ mennyiségének alakulása[16]
Szerkesztette: Károly László

[15] Afganisztánban a NATO Hírszerzési Információegyesítő Központnak (NATO Intelligence Fusion Centre) küldtünk és kaptunk is információkat.

[16] HORVÁTH Csongor: Adatgyűjtést koordináló és felderítési követelmények menedzsment. Szakmai előadás, KNBSZ, Budapest, 2015. április 16.

Az egységes felderítőrendszer kialakításának – szerintem – első és legfontosabb lépése a személyügyi kérdések tisztázása, a megfelelő jelöltek kiválasztása. Ki kell választani a vezető beosztású és a kulcsfontosságú, illetve speciális szaktudást igénylő katonákat. Természetesen nagyon fontos szempont a megfelelő szaktudás, képzettség és tapasztalat, de legalább ennyire mértékadó a kollégák rendszerben való gondolkodási képessége.

A felderítőrendszer vezetőinek kiemelt feladata, hogy megértessék szándékaikat a kontingens teljes személyi állományával. Mindenkinek szerepe van a rendszerben, mert minden tábort elhagyó, vagy a helyiekkel bármilyen módon kapcsolatba kerülő katona képes adatgyűjtésre. Fontos, hogy már a felkészítés során minden katonában kialakuljon a közös munka iránti igény és szándék. A kiképzési feladatokat már úgy kell megszervezni, hogy a részt vevő alegységek – amelyek nem szervezetszerű felderítő-alegységek – képesek legyenek adatokat gyűjteni, valamint megértésék ennek fontosságát.

A következő fontos lépés a munkafolyamatok kialakítása. Ekkor kell letenni a felderítőrendszer alapjait, figyelembe véve a haderő által biztosított képességeket és a műveleti környezet sajátosságait. Ezek közül a legfontosabbak:

- adatgyűjtési tervek elkészítése;
- felelősségi területek kijelölése;
- információáramlás rendje;
- információigénylés folyamata;
- kontingensen belüli együttműködés kialakítása;
- jelentőrendszer (*egy képességgel bíró szervezet, s nem egy aktuális cselekvés*) kialakítása;
- adattárak és adatbázisok létrehozása;[17]
- saját alegységek beszámoltatásának rendje.

Ezeket a szervezési feladatokat már honi bázison is el lehet végezni, amivel idő spórolható meg a műveletre történő kiutazás után.

A szervezetszerű alegységek felkészítésére is külön hangsúlyt kell helyezni. Számukra is – mint minden alegységnek – a valóságot megközelítő helyzeteket kell megteremteni és begyakorolni az egységes rendszer működését és működtetését. Mindenkinek meg kell értenie a rendszer működését és az abban betöltött szerepét.

Megjegyzés: a felderítőknek kell megértetniük a kontingens teljes személyi állományával az egységes felderítőrendszert, amihez elengedhetetlen, hogy ők kiválóan ismerjék azt. Ennek hiányában a rendszer és saját maguk hitelességét veszélyeztetik.

---

[17] TEAMEY, Kyle – SWEET, Jonathan E.: Organizing Intelligence for Counterinsurgency. Military Review, September-October 2006. pp. 24–29. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20061031_art007.pdf; letöltés: 2015.02.08.

A felkészítés során az alegységparancsnokoknak is meg kell ismerniük a rendszer képességét, mert ennek megfelelően tudnak információigényeket küldeni. Ha mindenki ismeri a képességeket és a lehetőségeket, akkor el lehet kerülni a félreértésekből eredő feszültségeket.

A felderítőrendszer kialakításának befejezése a műveleti területen

Az adott kontingens érkezhet közvetlenül a műveleti területre. Ez abban az esetben valósul meg, ha a válságkezelő művelet már folyamatban van, és a nemzeti kontingens csatlakozik az ott lévő erőkhöz. Erre példa a magyar részvétel a 2003-as *Iraki Szabadság* műveletben, amikor az amerikai és egyéb koalíciós erők már Irakban voltak, így az MH Szállítózászlóalj közvetlenül a műveleti területre érkezhetett. Másik esetben a kontingens egy felvonulási területre érkezhet (szomszédos ország, illetve olyan országrész, amely nem része a műveleti területnek), ahonnan kiindulva kezdik meg a feladatok végrehajtását. Ez abban az esetben valósul meg, ha a nemzeti kontingens a válságkezelő művelet megindításától részt vesz benne.

A műveleti vagy felvonulási területretörténő megérkezés után folytatni kell az egységes felderítőrendszer kiépítését.

Fontos feladat a megfelelő jogi környezet kialakítása. Ahogyan korábban már volt róla szó, a műveleti szerepvállalás alapját az engedélyező ENSZ Biztonsági Tanács, a NATO vagy az Európai Unió határozata adja. A felderítőerők alkalmazásához ez már elegendő. A felderítőtevékenység végrehajtásának alapjait a nemzetközi művelet vezetése által jóváhagyott egységes műveleti eljárás (SOP[18]) és az erő alkalmazásának elvei (ROE[19]) képezik. Azért fontosak, mert valamennyi részt vevő nemzet egységesen fogja értelmezni a feladatok végrehajtásának rendjét. Ezeket az okmányokat alapul véve minden nemzet elkészíti a hatályos műveleti eljárást, amelyben a saját kontingens egészének a tevékenységét szabályozzák a nemzeti korlátozásokkal együtt. Ebből készül el az adott szervezeti egységre vonatkozó szervezeti és működési szabályzat, majd minden egyes katona munkaköri leírása.

Megjegyzés: joggal merül fel a kérdés, hogy ezeket az okmányokat a kontingens vezetése miért nem a honi területen készíti el. Azért, mert egyszerűen nem áll elegendő információ a rendelkezésre a felkészülés otthoni szakaszában.

A nemzeti hírszerzés és elhárítás esetében az őket delegáló nemzetbiztonsági szervezet vezetője hagyja jóvá a tevékenységükre vonatkozó, a nemzetbiztonsággal foglalkozó törvény által szabályozott utasításokat. Ezek az esetek túlnyomó többségében minősítettek. Ugyanakkor rájuk is vonatkoznak a ROE, a SOP és a hatályos műveleti eljárás előírásai. Amennyiben ellentmondás van ezekben az előírásokban, akkor a szinkronizálásukra ebben a fázisban kell lépéseket tenni.

A műveleti területre történő megérkezés után a legfontosabb feladat a munkafeltételek és a nemzetközi együttműködés kialakítása. A munkafolyamatokat a helyi sajátosságoknak megfelelően alakítani, módosítani és pontosítani szükséges.

[18] Standard Operating Procedure – SOP.
[19] Rules of Engagement – ROE.

A munkafeltételek során ki kell alakítani az informatikai (minősített hálózatok) és a logisztikai feltételeket. Ennek célja, hogy a zavartalan munkavégzés biztosítva legyen.

A válságkezelő műveletek nemzetközi jellegűek. Emiatt a nemzetközi együttműködés kulcsfontosságú. A felderítőfőnöknek és a kijelölt kollégáinak fel kell venniük a kapcsolatot a művelet minden olyan személyével és szervezeti egységével, akikkel/amelyekkel együttműködés várható vagy elengedhetetlen. A kapcsolatfelvételt lehetőség szerint személyesen kell végrehajtani, mert az sokkal hatékonyabb együttműködést vetít előre, mintha az csak az informatikai eszközökön keresztül valósult volna meg. Ha személyesen nincsen erre lehetőség, akkor maradnak a számítógépek és telefonok. A kapcsolatfelvétel után le kell fektetni az együttműködés alapjait, és meg kell beszélni annak részleteit. Ezek összefüggésben vannak a munkafolyamatok kialakításával is, mert az információigénylés és információáramlás rendjét a nemzetközi közösséggel is ki kell alakítani, nem csak a saját kontingens tagjaival. Fontos, hogy a két rendszer minél közelebb álljon egymáshoz (pl. igénylőlapok), mert az meggyorsítja a munkát.

Megjegyzés: mind a kontingensen belüli, mind a nemzetközi együttműködés során a gyorsaság létfontosságú. A gyorsan változó műveleti környezetben az információ hamar idejét múlttá válik, ezért azt minél hamarabb el kell juttatni a felhasználóhoz. Ehhez járulnak hozzá a hatékonyan kialakított munkafolyamatok.

A nemzetközi együttműködés másik sarokpontja az adatszerzési képességek tisztázása. Ez azért fontos, hogy a megfelelő helyekre küldjünk információigényeket, és ne várjunk válaszokat olyanoktól, akiknek nincsen megfelelő képességük. Végül pontosítani kell az elérhetőségeket.

A HUMINT-feladatok végrehajtása érdekében meg kell kezdeni a forráshálózat kiépítését. Ennek során meg kell ismerni a helyi jogi szabályokat, amelyek alkalmazása a források kutatásának és foglalkoztatásának a feltétele. A SIGINT- és az IMINT-alegységek megkezdik az eszközeik telepítését és alkalmazásuk előkészítését.

A felderítőtörzs folytatja a „*harcmező felderítő előkészítését*”.[20] „*Az IPB a szemben álló fél, a terep, az időjárás, valamint a civil környezet módszeres elemzésének és megjelenítésének a folyamata, egy meghatározott érdekeltségi területen belül, meghatározott küldetés végrehajtása során*”.[21] Folytatják az adattárak feltöltését, pontosítják a korábban megszerzett adatokat. A meglevő adatokból olyan információkat készítenek, amelyek támogatják a kontingens valamennyi részének munkáját. Mindenkinek tisztában kell lennie azzal, hogy ezek az információs jelentések még nem tökéletesek. Idő kell a felderítőrendszernek is a felkészüléshez és a műveleti környezet megismeréséhez.

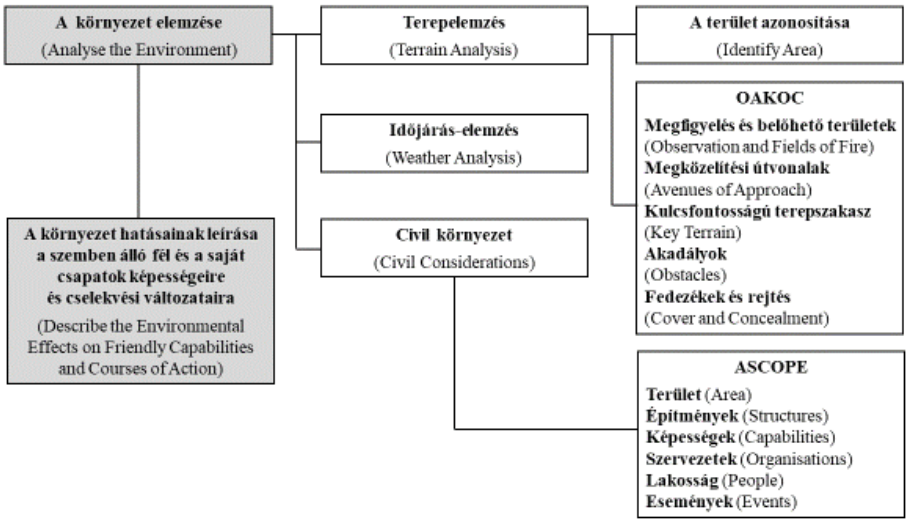
Ekkor kell a felderítőtörzsnek véglegesítenie a környezet műveletre gyakorolt hatásainak az elemzését. Ez nagyon fontos lesz a parancsnokok számára, mert ebből látják, hogy milyen környezetben fognak tevékenykedni.

---

[20] Intelligence Preparation of Battlefield – IPB.

[21] CSATÓ Attila: A harcmező felderítő előkészítésének (IPB) aktuális értelmezése. Diplomamunka, NKE, Budapest, 2013. p. 13.

Ennek részleteit az alábbi ábra szemlélteti:



3. ábra. A környezet műveletre gyakorolt hatásainak elemzése[22]

Következő fontos feladat az adatgyűjtést koordináló és a felderítésikövetelmények-menedzsment[23] kialakítása. Amennyiben a személyügyi feltételek megengedik, a felderítőtörzs elkülönített részlege foglalkozik ezzel a folyamattal. Munkája során irányítja az adatgyűjtést és kapcsolatot tart fenn valamennyi szervezeti egységgel. Két része van: adatgyűjtés-koordinációs és felderítési követelményekkel foglalkozó.

A műveleti területen a kontingensparancsnokkal és az alegységparancsnokokkal újból pontosítani kell az információigényeket. Ez azért fontos, mert a kiérkezés után ők is rengeteg új információhoz jutottak, megismerkedtek a helyi sajátosságokkal, ami módosítja a hazai bázison kialakított elképzeléseiket. Ezért a felderítőfőnöknek is esetleg módosítania kell az adatgyűjtési tervet, és új információigényeket kell megfogalmaznia a szervezetszerű és a nem szervezetszerű adatszerzők részére.

A felderítőtörzs nagyon fontos feladata az IPB-n belül a fenyegetések értékelése (pl. a szemben álló fél harceljárásai/fegyverzeti eszközei, képességei, szándékai, illetve fontos célpontok meghatározása stb.), valamint a szemben álló fél legveszélyesebb és legvalószínűbb cselekvési változatainak a meghatározása. A felderítőfőnök ezek ismeretében tudja azonosítani a kezdeti felderítési követelményeket.

[22] CSATÓ Attila: A harcmező felderítő előkészítésének (IPB) aktuális értelmezése. Diplomamunka, NKE, Budapest, 2013. p. 31.
[23] Collection Coordination and Information Requirement Management – CCIRM.

Az egységes felderítőrendszer akkor tekinthető késznek, ha elérte a műveleti készenlétet (nem azonos a kontingens műveleti készenlétével), az erők és a képességek szétbontakoztak, valamint megkezdődött felderítés. Meg kell azonban jegyezni, hogy „hátradőlni" nem szabad, mert a folyamatosan változó műveleti környezet megköveteli a felderítőrendszer változtatását is.

Speciális eset: együttműködés a fogadó ország[24] felderítő-, hírszerző és elhárító elemeivel

A 21. század válságkezelő műveleteire az a jellemző, hogy valamilyen formában szoros együttműködés alakul ki a fogadó ország felderítő-, hírszerző és elhárító elemeivel. Szakmai vitákat szokott eredményezni, hogy a fogadó ország e szervezeteiben dolgozókat HUMINT-forrásoknak vagy együttműködőknek kell-e tekinteni.

Figyelembe kell venni azonban, hogy e személyek megbízhatóságáról kevés információ áll a rendelkezésre. Emiatt kétirányú információáramlás csak nagyon korlátozott és ellenőrzött módon valósulhat meg. Az átadott információk komoly szűrésen mennek keresztül, aminek célja a forrásvédelem és az információk kiszivárgásának a megakadályozása. A nemzetközi művelet adatszerzői viszont folyamatosan gyűjtenek információt a helyi szervezetekről és szervezetektől.

A helyi nemzetbiztonsági szervezetek kiváló információforrások, mert ők vannak otthon, ismerik a helyi viszonyokat és megvannak a kapcsolataik. Az általuk megszerzett információk egy részét hivatalosan átadhatják a nemzetközi erőknek, míg a fennmaradó részt titkos együttműködés keretében osztják meg.

Ezen kettősség miatt nehéz megállapítani, hogy együttműködésről vagy foglalkoztatásról beszélünk. Véleményem szerint mind a kettő.

Befejezés

A jelenkor aszimmetrikus konfliktusaiban máshogyan kell gondolkodni, mint a múlt század háborúiban. Ez kiemelten igaz a felderítésre és a hírszerzésre is. Emiatt jelentős paradigmaváltáson mentünk/megyünk keresztül. Az egyik legfontosabb változás, hogy az információszerzést nem állami szereplők ellen kell végrehajtani, ami miatt a felderítés jelentősen felértékelődött. A hagyományos háborúkban támogató szerepet, de a nem hagyományosakban vezető szerepet tölt be a felderítés.[25]

---

[24] Fogadó országon azt értem, amelyben a válságkezelő művelet végrehajtásra kerül. Ennek az országnak a hivatalos kormánya, adminisztrációja és fegyveres/rendvédelmi/nemzetbiztonsági ereje a válságkezelő műveletben részt vevő erők támogatását élvezik. Ennek célja, hogy a művelet befejezése után a helyi hivatalos szervek képesek legyenek átvenni a feladatokat és önállóan – a válságkezelő művelet céljával összhangban – működtetni az államot.

[25] ZEYTOONIAN, Dan: Intelligence Design: COIN Operation and Intelligence Collection and Analysis. Military Review, September-October 2006. pp. 30–37. https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20061031_art008.pdf; letöltés: 2015.02.08.

Az elmúlt néhány évben új fogalmakkal kellett megismerkednünk, mint például: a felderítés lakosságközpontúsága, valós idejű információk fontossága, hálózatközpontú felderítés, hatásalapú célkiváltás, információs fölény stb. Mindegyik esetben központi szerepet tölt be az egységes felderítőrendszer.

Az egységes felderítőrendszer sem új keletű dolog. A korábbi évszázadok hadvezérei is ennek megfelelően képzelték el az információk megszerzését. A jelenkor válságkezelő műveleteiben azonban ez a rendszer sokkal összetettebb lett, és sokkal nagyobb kihívásokkal néz szembe. Korábban többnyire a katonai jellegű információkat kellett gyűjteni, de a jelenben a műveleti környezet minden területével foglalkozni kell. Például előfordulhat, hogy a felderítőfőnöknek egy tartomány demográfiai térképét kell a parancsnok asztalára letennie, vagy javaslatot tennie egy iskola felépítésének a helyszínére.

Ezek miatt fontos, hogy az egységes felderítőrendszert minél előbb fel kell építeni, a kontingens teljes személyi állományával megértetni a működését, valamint bemutatni a benne elfoglalt helyüket és a szerepüket.

A műveleti környezet és emiatt a válságkezelő erők feladatai folyamatosan változnak. Ez megköveteli a felderítőrendszertől is a változás fontosságának a felismerését és a szükséges változtatás végrehajtását. Ez nagy fokú rugalmasságot vár el a felderítőfőnöktől és a teljes személyi állománytól. Külön kihívást jelent a váltások miatti helyzet, amikor az átadás-átvétel után az újonnan kiérkezett személyi állománynak kell folytatnia a munkát.

Összefoglalva, egy egységes felderítőrendszer működése meghatározó egy kontingens életében és fontossága felbecsülhetetlen. Minden tagjának büszkének kell lennie arra, hogy része lehetett a tevékenységében, mert azzal rendkívüli tapasztalatot és egy életre szóló élményt szerzett.

FELHASZNÁLT IRODALOM

- ARREGUIN-TOFT, Ivan: How The Weak Win Wars – A Theory Of Asymmetric Conflict. International Security, Volume 26, Issue 1, July 2001. pp. 93–128. https://web.stanford.edu/class/polisci211z/2.2/Arreguin-Toft%20IS%202001.pdf; letöltés: 2015.02.08.
- CONNABLE, Ben: Military Intelligence Fusion for Complex Operation – A New Paradigm. RAND National Defence Research Institute, 2012. pp. 20–21. https://www.rand.org/content/dam/rand/pubs/occasional_papers/2012/RAND_OP377.pdf; letöltés: 2015.02.08.
- CORDESMAN, Anthony H.: The Intelligence lessons of the Iraqi Wars(s). Center for Strategic and International Studies, Washington, 2004. pp. 11–12. https://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/iraq_intelligenceiraqiwar.pdf; letöltés: 2015.03.21.
- CSATÓ Attila: A harcmező felderítő előkészítésének (IPB) aktuális értelmezése. Diplomamunka, NKE, Budapest, 2013.

- HORVÁTH Csongor: Adatgyűjtést koordináló és felderítési követelmények menedzsment. Szakmai előadás, KNBSZ, Budapest, 2015. április 16.
- KÁROLY László:
  Az egységes felderítőrendszer bemutatása az aszimmetrikus konfliktusokban.
  Felderítő Szemle, XV. évfolyam 4. szám, 2016. december. pp. 42–61.
  https://www.knbsz.gov.hu/hu/letoltes/fsz/2016-4.pdf; letöltés: 2017. 04.11.
- KÁROLY László:
  Az összadatforrású felderítés az aszimmetrikus konfliktusokban.
  Felderítő Szemle, XIV. évfolyam 3. szám, 2015. szeptember. pp. 91–104.
  https://www.knbsz.gov.hu/hu/letoltes/fsz/2015-3.pdf; letöltés: 2017.04.11.
- LAHNEMAN, William J.: The Future of Intelligence Analysis.
  Final Report, Volume 1. Department of Security Studies and International Affairs,
  Daytona Beach, 2006. pp. 14–16.
  https://commons.erau.edu/cgi/viewcontent.cgi?article=1000&context=db-security-studies; letöltés: 2015.02.16.
- RESPERGER István – KISS Álmos Péter – SOMKÚTI Bálint:
  Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.
  Zrínyi Kiadó, Budapest, 2013.
- ROLINGTON, Alfred: Hírszerzés a 21. században – A mozaikmódszer.
  Antall József Tudásközpont, Budapest, 2015.
- SZALAI Gábor:
  A nemzeti hírszerzés és a magánszektor kapcsolatának alapkérdései az USA-ban.
  Hadtudományi Szemle, 1. évfolyam 2. szám, 2008. pp. 22–29.
  http://epa.oszk.hu/02400/02463/00002/pdf/EPA02463_hadtudomanyi_szemle_2008_2_022-029.pdf; letöltés: 2015.02.15.
- Tactical Site Exploitation and Cache Search Operations. Tactics, Techniques, and Procedures.
  Center for Army Lessons Learned (CALL), Handbook, No. 07-26, May 2007.
  https://nsarchive2.gwu.edu/NSAEBB/NSAEBB410/docs/Tactical%20Site%20Exploitation.pdf; letöltés: 2015.02.08.
- TEAMEY, Kyle – SWEET, Jonathan E.: Organizing Intelligence for Counterinsurgency.
  Military Review, September-October 2006. pp. 24–29.
  https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20061031_art007.pdf; letöltés: 2015.02.08.
- VASTAGH László: NATO: válságkezelés és missziók.
  honvédelem.hu, 2010.11.23.
  https://honvedelem.hu/hirek/nato-valsagkezeles-es-missziok.html; letöltés: 2019.08.12.
- ZEYTOONIAN, Dan:
  Intelligence Design: COIN Operation and Intelligence Collection and Analysis.
  Military Review, September-October 2006. pp. 30–37.
  https://www.armyupress.army.mil/Portals/7/military-review/Archives/English/MilitaryReview_20061031_art008.pdf; letöltés: 2015.02.08.

ERDÉSZ VIKTOR FŐHADNAGY

AZ IDGA KONFERENCIÁJA A MESTERSÉGES INTELLIGENCIA SZEREPÉRŐL A HÍRSZERZŐ ELEMZÉS-ÉRTÉKELÉSBEN

Az amerikai nemzeti biztonsági szféra fejlesztéséért tevékenykedő IDGA[1] kutatóintézet 2020. október 29–30-án a nemzetbiztonsági hírszerző elemzés-értélés témakörében rendezett online konferenciát.[2] Az eredetileg áprilisban Washingtonban tervezett esemény a koronavírus-járvány következtében az online térbe szorult, de így is érdekfeszítő előadásokat hallhattunk a mesterséges intelligenciának (MI) az elemzés-értékelésben betöltött szerepéről.

Dr. Lilian Alessa, az Idahói Egyetem CRC kutatóközpontjának[3] igazgatója

Dr. Alessa „*Emberekre támaszkodva: A mesterséges intelligencia sikere vagy bukása az emberi tényezőn múlik*”[4] című előadásának alapvetése, hogy az amerikai Hírszerző Közösség[5] mára fulladozik a rendelkezésére álló adatok tengerében. Ennek fő haszonélvezői az Amerikai Egyesült Államok – az előadásban meg nem nevezett – ellenségei, mert a tevékenységükre utaló jelek elvesznek az adattömegben.

Az amerikai hírszerzés rendszere napainkban is a hírszerző elemzés-értékelés atyjaként számon tartott Sherman Kent[6] által kidolgozott hírszerzési cikluson[7] alapszik. A ciklus középpontjában az elemzők állnak, ezért az elemzőkre nehezedő nyomás a hírszerzés teljes rendszerére kihat. A hírszerzési ciklus elméletének megalkotásakor Kent nem láthatta előre az információs korszak eljövetelét, amelynek hatására a hírszerző elemző-értékelők egyre kevésbé képesek elvégezni a rendelkezésre álló információ feldolgozását.[8] A kihívás hatványozottan jelentkezik az anomáliák és a mintázatok detektálása tekintetében.

---

1 Institute for Defense and Government Advancement.
2 Intelligence Analytics Summit.
3 A 2014-ben alapított Center for Resilient Communities társadalmi-ökológiai interdiszciplináris kutatásokat végez. Az amerikai Hírszerző Közösség figyelmét elsősorban a rendszertudomány gyakorlati alkalmazásában elért eredmények kelthették fel.
4 Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors.
5 Intelligence Community – IC.
6 A történész végzettségű Kent 1942-től a második világháborúban létrehozott Stratégiai Szolgálatok Hivatalánál (Office of Strategic Services – OSS), majd annak utódszervezeténél, a Központi Hírszerző Ügynökségnél (Central Intelligence Agency – CIA) szolgált különböző elemzői beosztásokban. A hírszerzési ciklus mellett a Hírszerző Közösség konszenzusos álláspontját tartalmazó Nemzeti Hírszerzési Értékelések (National Intelligence Estimate – NIE) módszertanának kidolgozása is Kent érdeme. A CIA a 2000-ben alapított elemző-értékelő akadémiáját Sherman Kentről nevezte el.
7 Intelligence Cycle.
8 Az emberi erőforrás feldolgozóképessége mára elégtelenné vált ahhoz, hogy az adat–információ–tudás–bölcsesség folyamat a kellő időben végbemenjen.

1. ábra. A Sherman Kent által kidolgozott hírszerzési ciklus jelenleg alkalmazott változata[9, 10]

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

[9] ALESSA, Lilian: Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors. Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.

[10] A ciklus elemei: Planning and Direction (az információigények fogadása és a hírszerzés folyamatának megtervezése és megszervezése); Collection (adatszerzés); Processing and Exploitation (az információk feldolgozása és rendszerezése); Analysis and Production (az információk elemzése és értékelése, valamint a tájékoztatók készítése); Dissemination and Integration (a döntéshozók/felhasználók tájékoztatása, más megközelítésben a hírszerzési információk eljuttatása a rendeltetési helyükre, azok integrációja). A körfolyamat fontos eleme a visszacsatolások (Feedback) rendszere, mert minden egyes szakasz között vannak visszautalások az előző szakaszokra. Végül az ellenőrzés (Evaluation) járul hozzá a ciklus komplex működéséhez.
A ciklus elemei magyar elnevezésének forrása:
VIDA Csaba: A hírszerzési ciklus. In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban. Dialóg Campus Kiadó, Budapest, 2018. pp. 114–132.
http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11004/web_PDF_EKM_Nemzetbiztonsag_elmelete_a_kozszolgalatban.pdf?sequence=1&isAllowed=y; letöltés: 2021.03.07.

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

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

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

Az MI nemzetbiztonsági alkalmazásával szemben támasztott reményeknek elsősorban a rádióelektronikai felderítés (SIGINT[11]), a képi hírszerzés (IMINT[12]), valamint a geoinformációs/térinformatikai hírszerzés (GEOINT[13]) terén elért eredmények adnak alapot. A komplex, strukturálatlan adatvagyonon alapuló területeken ugyanakkor – ami a védelmi és biztonsági területek nagyobb részét lefedi – az MI-eszközök felhasználása kevésbé volt sikeres. Ennek fő oka az emberi tényezőben keresendő. Az egyetlen megoldást az elemzők gépi kiegészítése (augmentációja) jelenti, vagyis olyan szoftveres környezetet kell biztosítani a számukra, amely hatékonyan és integráltan támogatja a tevékenységüket.

Az új megközelítés alapfeltételeként olyan keretrendszerre van szükség, amelyben a hírszerzési ciklus valamennyi résztvevője: műveleti tisztek, elemző-értékelők, témaszakértők, vezetők és döntéshozók részt vesznek a kulcsfontosságú indikátorok (a veszélytényezők kialakulására vagy erősödésére utaló jelek) meghatározásában és a fontossági sorrendek felállításában. Az indikátorlista folyamatos karbantartása ahhoz is hozzájárul, hogy az emberek a mesterséges intelligencián alapuló, egyre inkább az automatizálás irányába elmozduló hírszerzési folyamatok középpontjában maradhassanak, azok fő hajtóerejeként.

A hírszerzés adat-ökoszisztémájának menedzselésére új szakértői csoport, az úgynevezett „*rule manager*ek" kialakítása szükséges. Az ilyen, a hírszerzés rendszerében is jártas adatmenedzserek[14] feladata az adatforrások (adatbázisok), valamint a döntéshozók és az elemző-értékelők információigényének számon

[11] SIGnals INTelligence.
[12] IMagery INTelligence.
[13] GEOspatial INTelligence.
[14] Dr. Alessa szerint valamennyi, a hírszerzés által foglalkoztatott szakértő vonatkozásában kiemelten fontos, hogy szorosan a hírszerzés rendszeréhez kapcsolódjanak, mert másképpen tudásukat nem tudják hasznosítani.

tartása, az indikátorlisták karbantartása. Az adatmenedzserek képesek közvetítőként is fellépni az elemző-értékelők és a technikai adatszerzők között az adatszerzők számára testreszabott információigények (gyűjtési igények) megfogalmazásával. Emellett részt vehetnek az elemző-értékelő forgatókönyvek felvázolásában, az új, kialakulóban lévő fenyegetések felfedésében, valamint az adat és az információ vizualizációjában.

Dr. Alessa mondandójának alátámasztására bemutatta az általa vezetett kutatócsoport fejlesztésében létrehozott nagyadatalapú (*big data based*) Stratégiai Hírszerző Keretrendszer[15] elnevezésű adatfúziós rendszer vizualizációs modulját, a MOSAIC-ot.[16] A 2017 óta 400 szakértő bevonásával fejlesztett MOSAIC a rendelkezésre álló adat térben és időben történő megjelenítésére szolgáló GEOINT-rendszer, amelynek segítségével a vizsgált entitás, jelenség vagy folyamat vizuális (térképes) megjelenítése térben és időben tetszés szerint változtatható. Az időfaktor bizonyos határokon belül a jövőbe is kitolható, lehetővé téve előrejelzések és forgatókönyvek készítését. A MOSAIC fő erőssége éppen a rejtett trendek felfedésében, az előrejelző hírszerzés hatékony támogatásában áll.

A hírszerző szolgálatok és a szervezeti egységek egymástól elkülönített adatbázisai,[17] illetve a betekintési jogosultsági csoportok és szintek jelentette nehézséget azzal küszöbölik ki, hogy a keretrendszer algoritmusainak több verziója fut párhuzamosan az adatbázisokban. A megfelelő betekintési jogosultsággal rendelkező szervezeti egységek információigényeire az algoritmusok által összegyűjtött válaszok a kormányzati felhőben valós időben mozognak.

A MOSAIC három, egymással párhuzamosan futtatott úgynevezett genetikus algoritmuson alapul.[18] A nyílt információk és rendvédelmi adatbázisok feldolgozásán alapuló projektek egyikének eredményeképpen sikerült eddig nem detektált, alacsony láthatóságú illegális tevékenységeket felderíteni az alaszkai határszakaszon, majd azok ellen hatósági intézkedéseket kezdeményezni. Egy másik projekt olyan indikátorokat detektált amerikai belterületen, amelyek a hadszíntér ellenséges műveleti előkészítésére[19] utalnak. A kutatás által biztosított információk (nem részletezett területeken) megváltoztatták az amerikai vezetés egyes politikáit.

Dr. Alessa megjegyezte, hogy a hatalmas adatmennyiség miatt a nyílt adatbázisokban futtatott algoritmusok sokkal pontosabb és szélesebb körű eredményeket hoznak, mint a minősített rendszereken kereső társaik.

---

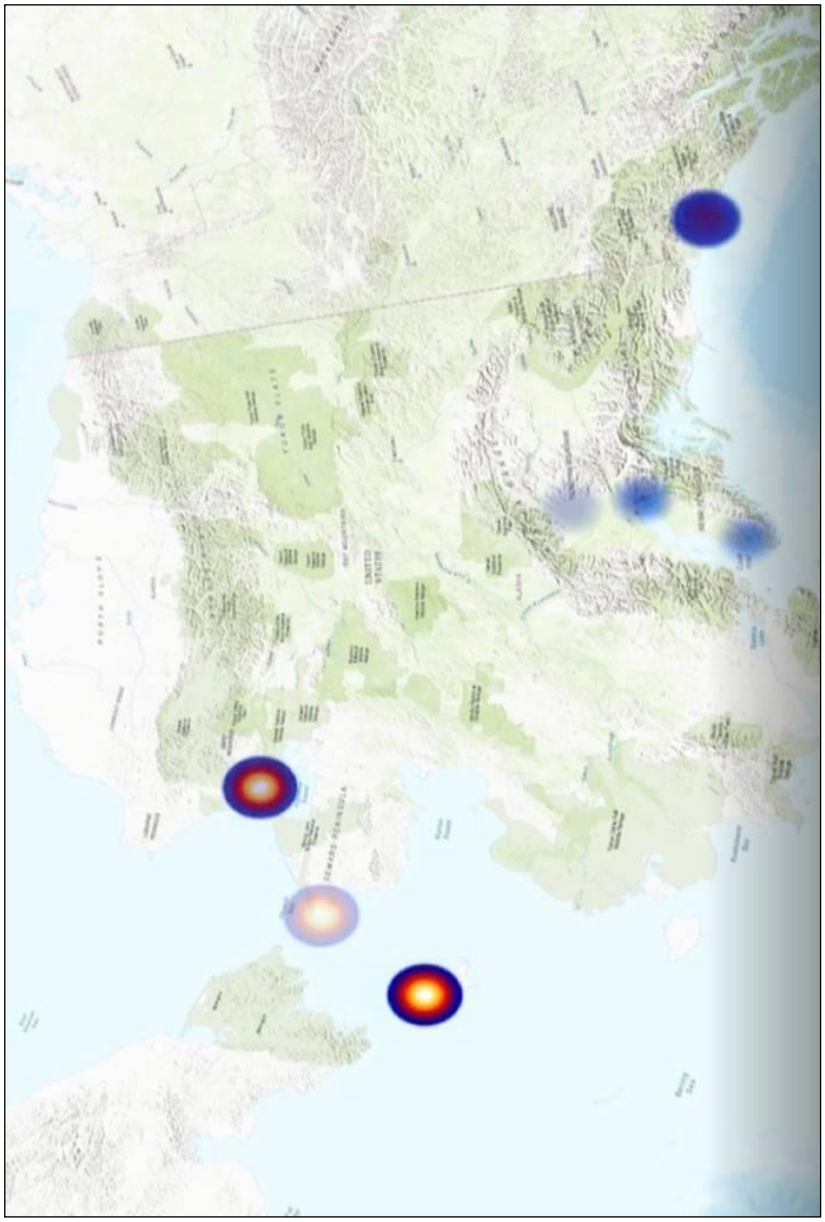
[15] Strategic Intelligence Framework.

[16] Massive-scale Operational Structural Awareness Intelligence Composite.

[17] Az előadó érzékletesen „adatbörtönnek” nevezi az ilyen adatbázisokat.

[18] Ezek a keresőszoftverek képesek a biológiai evolúcióhoz hasonló kiválasztódással fejlődni a feladatok végrehajtása során. Az ilyen algoritmusok speciális verziója, az úgynevezett „Evolutionary Generative Adversarial Networks” esetében a fejlesztők egymással versengő algoritmusokat hoznak létre. Erre példa két algoritmus, amelyek egyikének feladata nem létező személyekről fotókat hamisítani, a másiké pedig a hamisítványokat felfedezni. A számítástechnikai adatfeldolgozó képesség a 2010-es évtized közepére jutott el arra a szintre, hogy az 1960-as évek óta fejlesztett genetikus algoritmusok gyakorlati feladatok megoldásához is felhasználhatók legyenek.

[19] Operational Preparation of the Battlespace – OPIB.



2. ábra. A MOSAIC adatvizualizációs felülete

ALESSA, Lilian: Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors.

Az adatbázisok tekintetében elmondta, hogy azok mozgatása nem tanácsos. Az adatok másolása költséges, lassú, sérülékenységet és veszteségeket okoz. E helyett a kereső algoritmusokat kell „az adatokhoz mozgatni”, tehát olyan megoldásokra van szükség, amelyek a meglévő szervereken alkalmazhatóak. Az adatok tisztítását, ezáltal megbízhatóságuk növelését szintén erre specializált algoritmusokkal célszerű megoldani. Nem létezik „elavult adat”, tehát mindent tárolni kell, de az archiválást ellenzi, mert az archivált adatokat valójában nem lehet felhasználni.

Az elemzés-értékeléshez használt szoftverek esetében kizárólag a keretrendszer egységesíthető, míg a különböző részfeladatok összessége célszoftverek sokaságával hajtható végre.

Az elemzés-értékelés MI általi fejlesztéséhez elengedhetetlen a bőséges számítógépes kapacitás és a magas szintű algoritmusok megléte, de a kulcs a képzett munkaerőben és a nemzetbiztonsági szolgálatok szervezeti kultúrájának megváltoztatásában keresendő. Dr. Alessa megfogalmazásában a nemzetbiztonsági kultúra változtatása ahhoz hasonlatos, mintha megpróbálnánk egy vízcseppet rávenni, hogy „*felfelé folyjék a hegyen*”. Ez csak a hegy dőlésszögének megváltoztatásával lehetséges!

Dr. Alessa elmondta, hogy a MOSAIC fejlesztésében részt vevő szakértők többsége olyan nemzetbiztonsági munkatárs, akik új megoldásokat keresnek, és arra jutottak, hogy erre csak a tudományos életben van lehetőségük, a szolgálatoknál nem. A különböző szolgálatok munkatársainak együttműködésére szintén csak így nyílik valós lehetőség.

Susan W. Kalweit, a Nemzeti Térinformatikai Ügynökség (NGA) elemző-értékelő igazgatója

Susan W. Kalweit elemző-értékelő igazgató *Műveleti tempó: a gyors és megbízható elemzés biztosításának egyenlete*[20] című előadásában bemutatta a Nemzeti Térinformatikai Ügynökség (NGA[21]) megközelítését a mesterséges intelligencia által nyújtott lehetőségek elemző-értékelő szempontú kiaknázására. Elmondta, hogy a szervezet tevékenységének alapját kiterjedt adatbázisa adja. Az adatbázisban 12 millió földrajzi név, 125 millió gravitációs mérési eredmény, 4 milliárd légiforgalmi adatelem, 118 millió négyzetkilométernyi pontos

[20] KALWEIT, Susan W.: Mission Intensity: Thriving in the Smart Machine Age. Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.

[21] National Geospatial-Intelligence Agency. Az NGA a nemzeti hírszerző főigazgató (Director of National Intelligence – DNI) és a védelmi miniszter alárendeltségében működik. Központja Springfieldben (Virginia állam) található, 14 500 fős személyi állománnyal végzi a feladatait. A munkatársak 66%-a civil, 31%-a szerződéses és 3%-a katona. A személyi állomány 52%-a a központban, további 26%-a a St. Louis és Arnold városokban (Missouri) található alközpontokban, 22%-a pedig több mint 20 ország mintegy 200 telephelyén végzi feladatait.

sztereografikus[22] képfelvétel, valamint 70 millió hidrográfiai tereptárgyra vonatkozó adat található. Az NGA termékei között repülési, szárazföldi, tengeri és tengeralatti navigációs térképek, repülési információs jelentések, tengeri határok térképei és tengerészeti navigációs veszélyfigyelmeztetések szerepelnek. Az NGA emellett saját és kereskedelmi műholdfelvételek elemzés-értékelésével, valamint földrajzi, politikai földrajzi, humán földrajzi és katonai térképek készítésével is foglalkozik. Az NGA 90 külföldi partnerrel kötött képfelvételek és térképek megosztására vonatkozó megállapodást.

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

- az 1940-es évek legvégétől alakították ki a nagy magasságból készült analóg (manuálisan előhívott) képfelvételek elkészítésének és elemzés-értékelésének módszertanát, ilyen képfelvételeket egészen 2005-ig készítettek;
- az 1970-es évek végétől kezdték meg a térképészet, a georeferált[23] digitális információ és a képelemzés integrálását;
- a 2000-es évek elejétől kezdődött a térinformatikai nagyadat felhasználása előrejelző elemző-értékelő modellekhez;
- 2008-tól alkalmaznak MI-t az elemzés-értékelésben.

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

Új gondolkodásmódot kellett meghonosítani a technológia alkalmazásában és a humánmunkaerő-menedzsmentben is. Az új munkakörnyezet alapja az adatba, vagyis az NGA fő erőforrásába, valamint az adat feldolgozásához használt szoftverekbe vetett bizalom kialakítása. Ennek érdekében adatmenedzsmenttel foglalkozó szakértői csoportokat alkalmaznak, amelyek feladatai közé tartozik az adat hitelesítése is. Ezek a csoportok végzik az úgynevezett „*deep fake*” – a valóságosnak tűnő hamisított – információ (pl. kép, videofelvétel) kiszűrését is.

---

[22] A sztereográfiai vetület a gömb síkként történő ábrázolásának módja.
Sztereográfiai vetítés – Stereographic projection.
https://hu.qaz.wiki/wiki/Stereographic_projection; letöltés: 2021.03.14.

[23] A georeferálás során a digitálisan készített térkép pixeleihez földrajzi koordinátákat rendelnek.

A humán munkaerő kialakításánál inkluzív, a szaktudás széles körét magában foglaló szemléletet követnek. Az elemző-értékelő munkához IMINT- és GEOINT-szakértőkből, adattudósokból, adatmenedzserekből, adatgondozókból[24] és adatgyűjtő szakemberekből álló multidiszciplináris csoportokat hoznak létre. A területi szakértők tekintetében a fókuszt Kínára helyezték.

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

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

Barnil Bhattacharjee és James Tirbaso, Altair vállalat

Az amerikai Altair informatikai vállalat munkatársai előadásukban[25] bemutatták a Védelmi Minisztérium 2020-ban elfogadott adatstratégiájában kulcsszerepet beöltő VAULTIS adattárház-rendszert. A VAULTIS segítségével az érintett szervezetek akár több terrabájtnyi adat menedzsmentjét is képesek saját rendszereiken elvégezni. Az ajánlott szoftvercsomagok megoldást nyújtanak a túlszabályozott és a valóságban nem alkalmazott adatkezelési szabályok jelentette nehézségekre is.

Az Altair az adatot stratégiai eszközként kezeli, amely alapján felső vezetői szintű döntések is hozhatóak. Az egyes adatelemek könnyen visszakereshetőek, azonosíthatóak, növelve azok megbízhatóságát.

A vállalat könnyen telepíthető, a felhasználó által igényre szabható megoldásokat nyújt. Az adatmenedzsment-rendszer képes a strukturálatlan adattömeget strukturálni (*scraping*) és azt a saját adatbázissal összevetni (pl. híváslista összevetése nemzetbiztonsági adatbázissal). Az elemzés felhasználóbarát (*drag and drop* rendszerű), az elemzés eredményéről a rendszer összefoglalót készít.

A VAULTIS rendszert a Védelmi Minisztérium 2020 szeptemberében közzétett adatstratégiája[26] is nevesíti.

---

[24] Data Steward.

[25] BHATTACHARJEE, Barnil – TIRBASO, James: Activate VAULTIS: Self-Service Data Analytics to Kickstart 2020 DoD Data Strategy Implementation Recording. Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.

[26] Executive Summary: DoD Data Strategy. Unleashing Data to Advance the National Defense Strategy. Department of Defence of United States of America, 2020.09.30. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF; letöltés: 2020.12.16.

A rendszer elnevezésére szolgáló betűszó kibontása:

- az adat láthatósága (Visible): a felhasználók legyenek képesek arra, hogy a számukra szükséges adatot megtalálják;
- az adat hozzáférhetősége (Accessible);
- az adat érthetősége (Understandable): a felhasználók legyenek képesek az adat tartalmának, környezetének és felhasználhatóságának felismerésére;
- az adatok összekapcsolása (Linked): az adatok közötti kapcsolatok felfedezése;
- az adatok megbízhatósága (Trustworthy);
- interoperabilitás (Interoperable);
- biztonság (Secure): a felhatalmazás nélküli használat és a manipulálás lehetőségének kizárása.

Travis Pittman, az East View Information Services tartalomszolgáltató vállalat munkatársa

Travis Pittman néhány perces előadásában[27] elmondta, hogy a minneapolisi East View Information Services az amerikai védelmi szféra nyílt forrású tartalomszolgáltatója. Egyik fő termékük a legnagyobb kínai akadémiai adatbázis, a Kínai Nemzeti Tudás Infrastruktúra (CNKI[28]) licencelt változata. A CNKI-n évente több mint 5000 kutatás-fejlesztési és innovációs tudományos folyóiratban 1,1 millió kutató mintegy hatmillió tudományos publikációt tesz közzé. Az adatbázis cikkei .pdf és .xml formátumban érhetőek el, az adatbázisban a keresés több mint száz kategóriában (kulcsszavak, absztrakt, teljes szöveg, kutatóhely, pénzügyi támogató, szerzők, források) lehetséges.

A CNKI egyik fő előnye a cikkek, a kutatók és az intézmények kontextusának, egymás közötti kapcsolatának feltérképezhetőségében áll. Az adatbázis felhasználásával az East View munkatársai is készítenek elemzéseket a kínai védelmi jellegű kutatásokról. Az elemzéseikben kiemelt szektoroknak a hajógyártás, a rakétatechnológia, a műholdas kommunikáció, a kibervédelem és az egészségügy számítanak. A megjelent tudományos cikkek alapján elemzéseket készítenek a Kínai Népi Felszabadító Hadsereg (PLA[29]) szervezeti felépítéséről, tartalékos és félkatonai erőiről, katonai stratégiájáról és doktrínájáról, valamint a közrend fenntartásában betöltött szerepéről is. Elemzik továbbá a PLA jelentette új fenyegetéseket, az alkalmazott új technológiákat és a fejlesztések trendjeit.

[27] PITTMAN, Travis: Az East View tartalomszolgáltató vállalat bemutatása. Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.
[28] China National Knowledge Infrastructure.
[29] People's Liberation Army – PLA.

Az East View a CNKI mellett más nyílt adatbázisokat is szolgáltat az amerikai védelmi szféra részére. 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 pozícionálja magát. Mindemellett kiterjedt GEOINT-adatbázissal is rendelkezik.

Dewey Murdick, a Georgetown Egyetem CSET központjának adattudományi igazgatója

A washingtoni egyetem kialakulóban lévő technológiákkal és azok biztonsági vonatkozásaival foglalkozó kutatóközpontjának (CSET[30]) adattudományi igazgatója az előadásában[31] bemutatta a kutatóhely kínai védelmi célú fejlesztések feltérképezésére irányuló tevékenységét.

A CSET összesen 17 tartalomszolgáltatóval, köztük az East View-val áll szerződésben. A szolgáltatók összesen 28 terrabájt szöveges adatot biztosítanak, ami mintegy 14 milliárd oldalnak felel meg. A szövegcorpus többségét 215 millió, elsősorban angol, kínai és orosz nyelvű tudományos publikáció; több mint ötmillió szervezeti ábra; vállalati és kormányzati pénzügyi tranzakciókra vonatkozó adatok; 250 millió álláshirdetés; 450 millió szakmai életrajz; illetve sajtóadatbázisok és üzleti hírszerzési információk teszik ki. A CSET az adatbázisokból a szervezeti adatok, a hivatkozások, a szóhasználat stb. alapján hálózati kapcsolatokat készít, amelyek alapján jelenleg 678, összesen több mint 207 milliárd sornyi relációs adatot tartalmazó adattáblát üzemeltet. A jól strukturált, megbízható és kifinomult módszerekkel elemzett nagyadat alapján jól megalapozott, mély elemzéseket és értékeléseket képesek készíteni szervezetekről és személyekről. Az évtizedekre visszanyúló adattömeg trendelemzést is lehetővé tesz. Az adattárház karbantartását dedikált szakemberek végzik gépi tanuláson (GT) alapuló algoritmusok segítségével. A több ezer virtuális processzornyi számítástechnikai kapacitást a Google számítási felhőszolgáltatása[32] biztosítja.

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

Az első kutatás során a CNKI adatbázisából kiszűrték azokat a tudományos publikációkat, amelyek az MI-nek a hadászati stabilitásra gyakorolt hatásait vizsgálták. A keresés során 58 ilyen, 2016 és 2020 között megjelent cikket találtak.

---

[30] Center for Security and Emerging Technology.

[31] MURDICK, Dewey: CSET's Data Science Efforts and Open Source Analysis on China's Emerging Technologies. Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.

[32] Google Cloud Computing.

Az írások elemzése alapján a személyzet nélküli repülőgépek (UAV[33]) és tengeralattjárók (UUV[34]), az intelligens lövedékek, a műholdak, az elektronikus hadviselési eszközök,[35] a hírszerző-, megfigyelő és felderítőeszközök (ISR[36]), illetve az automatizált kibervédelem tekinthetők kulcstechnológiáknak. A publikációk közül negyven foglalkozott a haderő csapásmérő képességének fokozásával, 28 az MI felhasználási lehetőségeivel az ellenséges hadászati erők felderítésére, 11 az erőalkalmazás költségvonzatának csökkentésével, hét pedig a vezetés-irányítási rendszer sebezhetőségének csökkentésével. Az MI-eszközök elterjedése ugyanakkor kihívásokat is jelenthet a korszerű haderőknek. Az 58 kínai publikáció közül kilenc állítja, hogy növekedhet a technikai meghibásodások valószínűsége, nyolc szerint növekedhet a vezetés-irányítási rendszerek sérülékenysége, ugyancsak nyolc cikk foglalkozik a légvédelem hatékonyságának csökkenésével, hat a támadásokra rendelkezésre álló válaszidő csökkenésével, négy pedig a csapásmérési képesség csökkenésével. A publikációkból a CSET arra a következtetésre jutott, hogy a kínai katonai gondolkodók túlbecsülik az amerikai haderő – nyílt forrásokból felmérhető[37] – MI-képességeit.[38]

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

A harmadik kutatás a kínai biztonsági erők 2010–2019 közötti kutatási igényeivel foglalkozott. A vizsgált szervezetek a PLA, a Közbiztonsági Minisztérium[39] és a belbiztonsági rendőrség[40] voltak.[41] A CSET a globális tudományos adatbázisok alapján 121 ezerre becsüli a világ tudományos klasztereinek[42] számát, amelyek a vizsgált időszakban összesen mintegy 105 millió publikációt tettek közzé. A klaszterek közül 14 500 köthető a kínai biztonsági erőkhöz. E kutatói közösségek összesen 28 387 publikációt készítettek el az MI témakörében, amelyek közül 26 538-at a PLA, 1452-t a Közbiztonsági Minisztérium, 757-et pedig a belbiztonsági rendőrség klaszterei tettek közzé. A publikációk az MI vegyes felhasználási lehetőségein belül útvonaltervezéssel, célpontkiválasztással, több célpont egyidejű követésével,[43]

---

[33] Unmanned Aerial Vehicle.
[34] Unmanned Underwater Vehicle.
[35] Az MI-alapú elektronikai hadviselés angol szakirodalmi elnevezése: Cognitive Electronic Warfare.
[36] Intelligence, Surveillance, Reconnaisance.
[37] A CSET akadémiai szervezetként nem fér hozzá minősített információkhoz.
[38] FEDASIUK, Ryan: Chinese Perspectives on AI and Future Military Capabilities. CSET, August 2020. https://cset.georgetown.edu/research/chinese-perspectives-on-ai-and-future-military-capabilities/; letöltés: 2021.03.16.
[39] Ministry of Public Security – MPS.
[40] People's Armed Police – PAP.
[41] A CNKI adatbázisában minimális számú publikáció köthető az Állambiztonsági Minisztériumhoz (Ministry of State Security – MSS), ezért ezt a szervezetet nem vizsgálták.
[42] Klaszter alatt az egyazon tudományos problémával foglalkozó, egymás kutatásaira építő tudományos közösséget értik.
[43] Dewey Murdick hangsúlyozta, hogy a PLA klaszterei 348 publikációt jelentettek meg a ballisztikus célpontok megkülönböztetésével és a ballisztikus lövedékek útvonaltervezésével kapcsolatban.

behatolásérzékeléssel,[44] szteganográfiával,[45] adatelemzéssel, egészségüggyel, illetve mérnöki és anyagtudományokkal voltak kapcsolatosak. A számítógépes látás fő felhasználási lehetőségei közül a célpontazonosítással és -követéssel, a hiperspektrális képszenzorokkal,[46] az arc- és ujjlenyomat felismerésével, a testtartás elemzésével, a járművek felismerésével, valamint a hamisítványok kiszűrésével foglalkoztak. A természetes nyelvek feldolgozása[47] területén a kutatások a közösségi média felderítésére, az online hangulatelemzésre[48] és a szövegek kategorizálására összpontosítottak. A robotika területén pedig a vezérlőrendszerek, a személyzet nélküli járművek, az exoszkeletonok (mesterséges külső vázak) és a humanoid robotok jelentették a kutatások fő irányait.

Összegzés

A konferencia kiváló betekintést engedett az amerikai nemzetbiztonsági hírszerző elemzés-értékelés jelenlegi helyzetébe, eljárásaiba és problémáiba. Az előadások alapján egyértelmű, hogy a szolgálatok széleskörűen alkalmazzák az MI-alapú elemző-értékelő szoftverrendszereket. és mind a nyílt, mind a minősített rendszereiken nagyadattal dolgoznak. Számukra a fő kihívást az új technológiához illő eljárások, szervezeti felépítés és az emberi munkaerő képzése, összességében a nemzetbiztonsági szervezeti kultúra újraszabása jelenti.[49]

Az MI hírszerzésben történő alkalmazásának legfontosabb hozadéka a hírszerzési folyamatok, vagyis végeredményben a döntéshozók tájékoztatásának felgyorsulása a tájékoztatás minőségének számottevő javítása mellett. Ennek jelenlegi fő gátja már nem a technológia, hanem az eredendően absztrakt hírszerzési ciklus elemeinek merev, bürokratikus értelmezése.[50] A komplex problémakör gyökerében az áll, hogy a ciklus különböző elemeit végző szervezeti elemek között adminisztratív, a *need to know* elvére hivatkozó falak emelkednek. Amerikai

---

[44] Intrusion Detection.

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

[46] A több mint húsz diszkrét spektrális sávval rendelkező szenzorokat hiperspektrális képszenzoroként is említik.
A Tanács 6/2012/EU álláspontja első olvasatban a kettős felhasználású termékek kivitelére, transzferjére, brókertevékenységére és tranzitjára vonatkozó közösségi ellenőrzési rendszer kialakításáról szóló 428/2009/EK tanácsi rendelet módosításáról. Az Európai Unió Hivatalos lapja, 2012.04.13. p. 17.
https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:107E:0001:0273:HU:PDF; letöltés: 2021.03.14.

[47] Natural Language Processing – NLP.

[48] Akár a lakosság privát elektronikus levelezésében is.

[49] ERDÉSZ Viktor: Az amerikai hírszerzési reform és tanulságai. Felderítő Szemle, XVIII. évfolyam 3. szám, 2019. pp. 111–128.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2019-3.pdf; letöltés: 2021.03.05.

[50] Vida Csaba a hírszerzési ciklust érő kritikákat elemezve amellett érvel, hogy „a ciklus a hírszerzési folyamat elméleti letükröződése és nem a gyakorlati megvalósulása”, valamint „az elmélet egy keretet biztosít annak érdekében, hogy az adott hírszerző szolgálat hatékonyan és eredményesen működjön, de a gyakorlat során figyelembe kell venni a szolgálat lehetőségeit, képességeit és helyzetét.”
VIDA Csaba: Létezik-e még a hírszerzési ciklus? (Miről szól a hírszerzés?) Felderítő Szemle, XII. évfolyam 1. szám, 2013. szeptember–október. pp. 43–57.
https://www.knbsz.gov.hu/hu/letoltes/fsz/2013-1.pdf; letöltés: 2021.03.05.

felfogás szerint az akadály ledöntésének vagy megkerülésének legjobb módja a feladat-, illetve küldetésorientált, több terület képviselőiből álló csoportok alakítása és azok önálló szervezeti egységként történő kezelése.

A témában felszólaló előadók a mellett érveltek, hogy a szervezeti kultúra megváltoztatásának fő eszköze és az új típusú gondolkodásmód minél szélesebb körű meghonosítása a toborzás kiterjesztése a szolgálatok számára eddig ismeretlen szakterületekre. E téren különösen nagy hangsúlyt kaptak az adattudósok, az adatmenedzserek és az adatgondozók, akik kulcsfontosságú szerepet töltenek be nemcsak az MI-alapú elemző-értékelő rendszerek üzemeltetésében, hanem a hírszerzés rendszerének adatvezéreltté tételében is. Az előadók fontosnak tartották hangsúlyozni, hogy a speciális tudással rendelkező szakértők csak abban az esetben lehetnek hasznosak a nemzetbiztonsági rendszerben, ha a szolgálatok a tevékenységüket integrálják, vagyis kiterjedt nemzetbiztonsági háttértudást adnak nekik, és csapattagként kezelik őket. Ennek velejárója annak elfogadása is, hogy ezek az elhivatott, de nem a nemzetbiztonsági rendszerben szocializálódott szakemberek maguk is formálják a szervezeti kultúrát. A nemzetbiztonsági rendszerbe integrált szakértőkkel sem lehetséges ugyanakkor a szolgálatok rendkívül szerteágazó feladatkörének teljes lefedése, ezért elkerülhetetlen az aktív együttműködés kialakítása az akadémiai szférával és a kutatóintézetekkel, a technológiai vállalatokkal, valamint a kereskedelemi tartalomszolgáltatókkal. Az együttműködésben a szolgálatoknak kell a vezető szerepet betölteniük, hiszen ők képesek összefogni a saját és a partnerszervezetek tevékenységét.

Az amerikai nemzetbiztonsági szféra elsőrendű területi fókusza már egyértelműen Kína. A Kínával folytatott szuperhatalmi versengés egyes nemzetbiztonsági elemző-értékelő vonatkozásainak bemutatása demonstrálta a témában jártas kutatóhelyekkel és tartalomszolgáltatókkal megvalósuló hírszerző együttműködés kiterjedtségét és az ebben rejlő lehetőségeket. Egyértelmű, hogy lehetetlen a szükséges szaktudás és az adatbázisok felhalmozása a szolgálatok falain belül, ezért a nemzetbiztonsági szféra kénytelen nyitni a lehetséges partnerek felé.[51] Ennek az Amerikai Egyesült Államokban jelentős hagyományai vannak, amelyekre építve a korszerű informatikai megoldások birtokában új fejezetet nyithattak.

Nem kétséges, hogy a kiterjedt együttműködés számos és súlyos biztonságvédelmi, elhárítási kockázatot rejt magában, de az amerikai megközelítés egyértelműen a kockázatok csökkentését és menedzselését, nem elkerülésüket pártolja.[52] Emögött nyilvánvalóan az amerikai üzleti szemlélet áll, amelyben az elmaradt nyereség is veszteségnek számít, és amelyben olyan nyereségre törekszenek, amely minden, a

---

[51] ERDÉSZ Viktor: Az irányítás és az elemzés-értékelés rendszere az amerikai Hírszerző Közösségben. Nemzetbiztonsági Szemle, 8. évfolyam 2. szám, 2020. pp. 3–17. https://folyoirat.ludovika.hu/index.php/nbsz/issue/view/313/44; letöltés: 2021.03.10.

[52] Emellett érvelt az amerikai nemzeti mesterségesintelligencia-stratégia bemutatása során Katharina McFarland volt védelmi beszerzésekért felelős államtitkár, a Nemzeti Biztonsági Bizottság a Mesterséges Intelligenciáért (National Commission on Artificial Intelligence) tagja 2021. március 10-ei előadásán. MCFARLAND, Katharina: Mission Focused: The Mission to Integrate Artificial Intelligence into the Military's Future Battle Rhythm. The Cipher Brief, 2021.03.10. https://www.thecipherbrief.com/column_article/the-mission-to-integrate-artificial-intelligence-into-the-militarys-future-battle-rhythm; letöltés: 2021.03.15.

műveleti tempóból adódó potenciális veszteséget bőségesen ellensúlyoz. Természetesen nem elhanyagolható tényező a kihívás nagysága sem, hiszen a kínai tudományos szakirodalom önmagában is nagyadatot generál, amelynek feldolgozása elképzelhetetlen a hagyományos módszereket alkalmazó elszigetelt szolgálatok számára.

FELHASZNÁLT IRODALOM

- A Tanács 6/2012/EU álláspontja első olvasatban a kettős felhasználású termékek kivitelére, transzferjére, brókertevékenységére és tranzitjára vonatkozó közösségi ellenőrzési rendszer kialakításáról szóló 428/2009/EK tanácsi rendelet módosításáról. Az Európai Unió Hivatalos lapja, 2012.04.13. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2012:107E:0001:0273:HU:PDF; letöltés: 2021.03.14.
- ALESSA, Lilian: Relying on Humans: How Artificial Intelligence Succeeds or Fails on Human Factors. Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.
- BHATTACHARJEE, Barnil – TIRBASO, James: Activate VAULTIS: Self-Service Data Analytics to Kickstart 2020 DoD Data Strategy Implementation Recording. Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.
- ERDÉSZ Viktor: Az amerikai hírszerzési reform és tanulságai. Felderítő Szemle, XVIII. évfolyam 3. szám, 2019. pp. 111–128. https://www.knbsz.gov.hu/hu/letoltes/fsz/2019-3.pdf; letöltés: 2021.03.05.
- ERDÉSZ Viktor: Az irányítás és az elemzés-értékelés rendszere az amerikai Hírszerző Közösségben. Nemzetbiztonsági Szemle, 8. évfolyam 2. szám, 2020. pp. 3–17. https://folyoirat.ludovika.hu/index.php/nbsz/issue/view/313/44; letöltés: 2021.03.10.
- Executive Summary: DoD Data Strategy. Unleashing Data to Advance the National Defense Strategy. Department of Defence of United States of America, 2020.09.30. https://media.defense.gov/2020/Oct/08/2002514180/-1/-1/0/DOD-DATA-STRATEGY.PDF; letöltés: 2020.12.16.
- FEDASIUK, Ryan: Chinese Perspectives on AI and Future Military Capabilities. CSET, August 2020. https://cset.georgetown.edu/research/chinese-perspectives-on-ai-and-future-military-capabilities/; letöltés: 2021.03.16.
- KALWEIT, Susan W.: Mission Intensity: Thriving in the Smart Machine Age. Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.
- MCFARLAND, Katharina: Mission Focused: The Mission to Integrate Artificial Intelligence into the Military's Future Battle Rhythm. The Cipher Brief, 2021.03.10. https://www.thecipherbrief.com/column_article/the-mission-to-integrate-artificial-intelligence-into-the-militarys-future-battle-rhythm; letöltés: 2021.03.15.

- MURDICK, Dewey: CSET's Data Science Efforts and Open Source Analysis on China's Emerging Technologies.
  Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.
- PITTMAN, Travis: Az East View tartalomszolgáltató vállalat bemutatása.
  Előadás. Intelligence Analytics Online Summit 2020 konferencia, 2020.10.29–30.
- Sztereográfiai vetítés – Stereographic projection.
  https://hu.qaz.wiki/wiki/Stereographic_projection; letöltés: 2021.03.14.
- VIDA Csaba: A hírszerzési ciklus.
  In: RESPERGER István (szerk.): A nemzetbiztonság elmélete a közszolgálatban.
  Dialóg Campus Kiadó, Budapest, 2018. pp. 114–132.
  http://m.ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/11004/web_PDF_EKM_Nemzetbiztonsag_elmelete_a_kozszolgalatban.pdf?sequence=1&isAllowed=y;
  letöltés: 2021.03.07.
- VIDA Csaba: Létezik-e még a hírszerzési ciklus? (Miről szól a hírszerzés?)
  Felderítő Szemle, XII. évfolyam 1. szám, 2013. szeptember–október. pp. 43–57.
  https://www.knbsz.gov.hu/hu/letoltes/fsz/2013-1.pdf; letöltés: 2021.03.05.

KISVÁRI TAMÁS EZREDES

A KÍNAI KIBERTÉR ÉS A KÍNAI HADERŐ KIBERMŰVELETI ERŐINEK ÉS TEVÉKENYSÉGÉNEK BEMUTATÁSA

Bevezetés

Kína kapcsán szinte napi rendszerességgel lehet olvasni a nemzetközi és a magyar sajtóban, hogy Kínában milyen szigorú szabályozás alatt van az internet, illetve Kína mekkora veszélyt jelent a nemzetközi kibertérben. Az alábbi tanulmányban ezt a két témakört szeretném jobban bemutatni, és reményeim szerint sikerül is majd eloszlatni Kínával kapcsolatos néhány tévhitet ezen a területen is.

A kínai kibertér

A kínai kibertér valóban jelentős korlátozások mellett működik, de legnagyobb meglepetésre a kínai internetet a lakosság sokkalta szélesebb körben használja, mint azt az európai országokban feltételezzük. Ez különösen igaz a mobilalkalmazásokra és a mobiltelefonon elérhető szolgáltatásokra. Jelenleg Kínában valójában nem létezik és nem is tud létezni az, akinek nincs okostelefonja, mobilinternete és Wechat-elérhetősége. Ezt a folyamatot a Covid–19 világjárvány csak erősítette és gyorsította.

De először is nézzük meg a kibertér korlátozásait. Kínában a pártállami rendszer mindent elkövet, hogy az interneten csak olyan tartalom, szolgáltatás jelenhessen meg, amely összhangban van a Kínai Kommunista Párt ideológiájával és az általa elrendelt szabályozással, de ezt Kínában inkább úgy fogalmazzák meg, hogy ami összhangban van az ország alkotmányával. Az alkotmány első cikke így fogalmaz: „*a Kínai Népköztársaság olyan szocialista állam, amelyet a munkás-paraszt szövetségre alapozott népi demokratikus diktatúra kormányoz. A szocialista berendezkedés alapvető államforma a Kínai Népköztársaság számára. Az ország vezetését a Kínai Kommunista Párt gyakorolja a szocializmus kínai sajátosságai alapján. Tilos a szocialista rendszer rombolása vagy megkérdőjelezése bármely természetes vagy jogi személyek részéről.*”[1]

A kibertér és az internet is ennek megfelelően működik, vagyis minden olyan hangot elhallgattatnak, amely káros a Kínai Kommunista Párt hatalmára nézve. Ennek eszköze az Aranypajzs[2] – az internet-ellenőrzés Közbiztonsági Minisztérium[3] által működtetett keretrendszere – és az azon belül működő Nagy Kínai Tűzfal,[4] amelyek

[1] Constitution of the People's Republic of China. A Kínai Népköztársaság Alkotmánya. The State Council the People's Republic Of China, 2019.11.20. http://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html; letöltés: 2021.04.14.

[2] Golden Shield Project (Chinese: 金盾工程; pinyin: jīndùn gōngchéng).

[3] Ministry of Public Security (MPS).

[4] The Great Firewall of China (GFW; Chinese: 防火长城; pinyin: Fánghuǒ Chángchéng).

külföldről nézve intranetté alakítják a kínai internetet egy kis kapukijárattal a nagyvilágban működő globális internetre.

A Nagy Kínai Tűzfal jelenleg tiltja a teljes Google szolgáltatási csomagot, a nyugati közösségi média szolgáltatásait (Facebook, Twitter, Instagram, Whatsapp, Youtube) és minden olyan weboldalt, amely valószínűleg kritikus hangon írhatna Kínáról és a kínai vezetésről (BBC, South China Morning Post, CNN, The New York Times stb.).

Egy példával szeretném bemutatni a rendszer működését. 2012-ben – amikor először voltam külszolgálaton Kínában – a nyugati híroldalak még elérhetők voltak az országban. A New York Times 2012. október 25-én megjelentetett egy cikket, amelyben arról írt, hogy Ven Csiabao (Wen Jiabao) akkori miniszterelnök, a kommunista párt legfelsőbb vezetése tagjának családja 2,7 Mrd USD értékű vagyon felett rendelkezik.[5] A cikk hatására a nyugati híroldalak szinte kivétel nélkül elérhetetlenné váltak Kínában. Ekkor még működött a Google keresőoldala, de az amerikai vállalat csak úgy tudott működni Kínában, hogy együttműködött a kínai hatóságokkal. Ez azt jelentette, hogy ha valaki rákeresett a Nagy Kínai Tűzfalra, akkor szép képtalálatokat kapott a Kínai Nagyfalról, de semmit sem olvashatott a tűzfalról, mint ahogy a pekingi Tienanmen téren 1989-ben történt véres eseményekről sem. A Google keresőszolgáltatás kínai megfelelője, a Baidu sem hozott fel olyan találatokat, amelyek problémát jelentenének Kínában, vagy amit a kínai vezetés nem kíván publikálni. Az 1. ábrán látható az a kép, amelyet a Baidu keresőoldal felhozott a Nagy Kínai Tűzfalra végrehajtott keresésem után.

Az első, a második és a negyedik találat arról ír, hogy miként szolgálja az amerikai média által Nagy Kínai Tűzfalnak hívott rendszer a kínai internet biztonságát, míg a harmadik Észak-Korea internetkorlátozásáról ír.

Az ellenőrzőrendszer működéséről egy másik érdekesség, hogy a Kínában az említett közösségi médiaszolgáltatások többségét helyettesítő Wechat applikáció komoly állami ellenőrzés alatt áll, amit jól mutatnak a kanadai Citizenlab jelentései, amelyek a Wechat rendszert tesztelik.[6] Eszerint ha a Wechat üzenetküldőjébe bizonyos érzékeny szavakat beírunk, akkor azok már nem jelennek meg a partner képernyőjén, de ha valahogyan mégis sikerül kijátszani az automatikus ellenőrzést, akkor is az államra vagy a vezetőkre tett kritikus megjegyzések döntő többsége 30 percen belül törlődik a rendszerből, de 24 órán túl már egyetlen kritikus hang sem maradhat elérhető a neten. Akiket pedig az ellenőrzőrendszer veszélyesnek minősít, azoknak felfüggesztik vagy egyszerűen törlik a fiókját és a Wechat szolgáltatáshoz való hozzáférését, a Kommunista Pártra veszélyt jelentő személyek viszont valószínűleg nem úszhatják meg ennyivel a dolgot.

---

[5] BARBOZA, David: Billions in Hidden Riches for Family of Chinese Leader. The New York Times, 2012.10.25. https://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html; letöltés: 2021.04.14.

[6] KENYON, Miles: WeChat Surveillance Explained. The Citizen Lab, 2020.05.07. https://citizenlab.ca/2020/05/wechat-surveillance-explained/; letöltés: 2021.04.14.

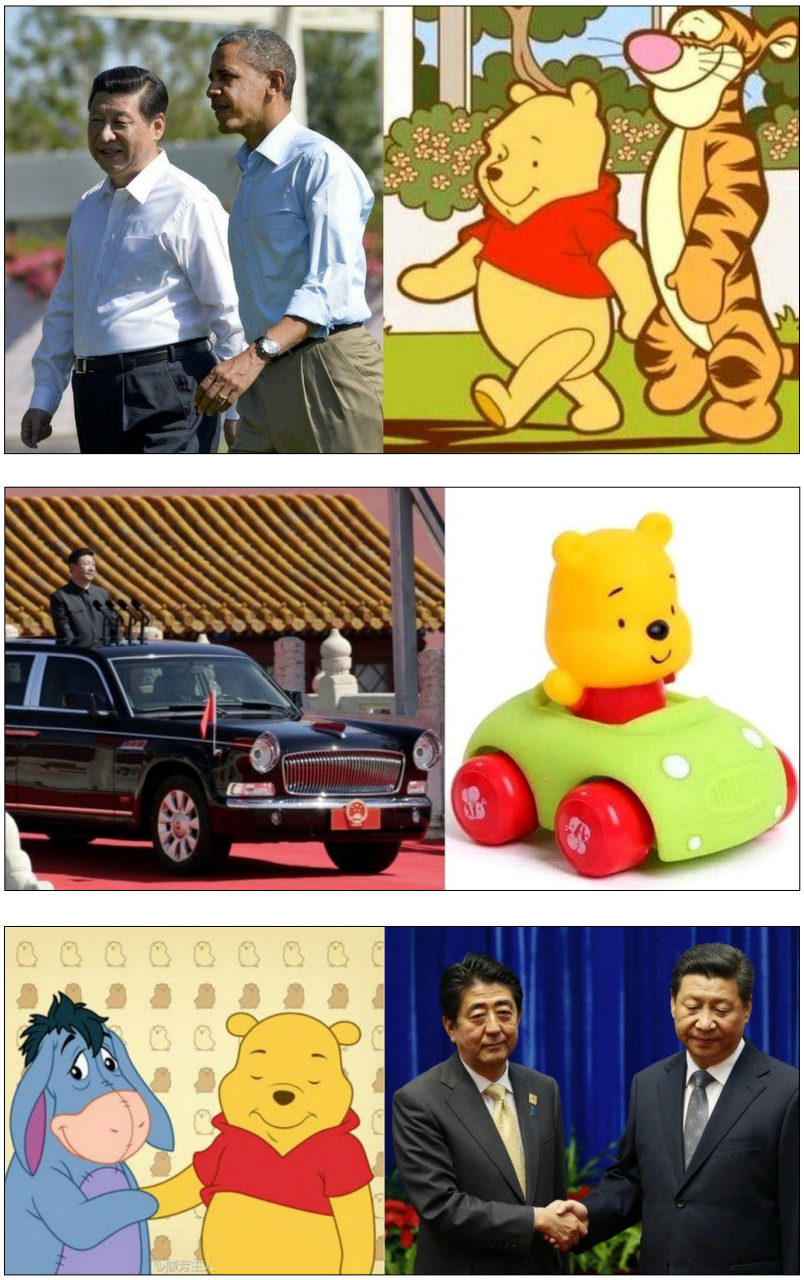
1. ábra. Baidu-keresés a Nagy Kínai Tűzfalról

A legdurvább példával a nyugat-kínai Ujgur Autonóm Területen 2009-ben történt lázadás mutatja a korlátozó rendszer kiterjedését. A 197 áldozatot és 1700 sérültet követelő 2009. július 5-i ujgur felkelés a kínai han lakosság ellen arra kényszerítette a kínai hatóságokat, hogy lekapcsolják a teljes telekommunikációs rendszert az Ujgur Autonóm Területen, mivel az internet és a telekommunikációs szolgáltatások jó lehetőséget biztosítottak a felkelés szervezőinek. A China Daily kínai napilap 2010. január 18-án tudósított arról, hogy az autonóm területen újra engedélyezték az SMS szolgáltatást – napi 20 üzenetben korlátozva annak használatát.[7]

Egy másik, akár nevetségesnek is tekinthető eset, amikor 2015-ben Kínában a cenzorok letiltották a Micimackót mint filmet és témát. Ennek egyik oka az volt, hogy az ötletes kommentelők Micimackó kínai nevével (Weini Xiong – 威尼熊) próbálták kijátszani a cenzorokat, amikor a kínai pártfőtitkárról vagy államfőről akartak írni, akinek a megszólítása – Hszi elvtárs (Xi tongzhi – 习同志) – valamennyire hasonlít a mackó szó (Xiong – 熊) kiejtésére. A másik ok, hogy az internetes mémek készítői előszeretettel ábrázolták Hszi Csinping kínai elnököt Micimackóként, amikor Obama amerikai elnökkel és Abe Sinzó japán miniszterelnökkel találkozott, vagy amikor megtekintette a 2015-ös díszszemlét (2. ábra).[8]

[7] JIA, Cui: SMS returns to Xinjiang. China Daily, 2010.01.18. https://www.chinadaily.com.cn/china/2010-01/18/content_9332764.htm; letöltés: 2021.04.14.

[8] MCDONELL, Stephen: Why China censors banned Winnie the Pooh. BBC News; 2017.07.17. https://www.bbc.com/news/blogs-china-blog-40627855; letöltés: 2021.04.14.



2. ábra. A kínai államfő Micimackóként történő ábrázolása

A Baidu keresőoldal a korlátozásoknak megfelelően nem dobja fel a Google szolgáltatás által megtalált képeket, ami jól mutatja a kínai rendszer működését.

Az említett korlátozások természetesen sok bosszúságot és nehézséget okoznak a Kínában élő külföldieknek. A korlátozások azonban részben megkerülhetők VPN-szolgáltatással,[9] bár pártkongresszusok, fontosabb találkozók és ülések, továbbá jelentősebb évfordulók esetén érzékelhető, hogy az internet külföldi irányban még jobban lelassul, és a VPN-szolgáltatások is akadoznak. Ennek az az oka, hogy a kínai internet valójában intranet – korlátozott kijárattal a nemzetközi szerverek felé. Ezért tekinthető komoly küzdelemnek az internet használata a külföldiek számára Kínában, mert bár egy 300 Mbit/sec sebességű ADSL-előfizetés a kínai szerverek irányában adja is az ígért sebességet, de a külföldi szerverek irányában sokszor nem éri el az 1 Mbit/sec sebességet – még a VPN bekapcsolása mellett sem.

Felmerülhet a kérdés, hogy a kínai lakosság hogyan tudja elfogadni az ilyen fokú hálózati ellenőrzést és korlátozásokat a 21. században, a globális internet világában. Tapasztalatom alapján nagyon jól, és még az európai szolgáltatásoktól is fejlettebb módon úgy, hogy ők ebből nem sokat érzékelnek a nyelvi és a kulturális különbségek okán. Egyfelől minden nyugati szolgáltatásnak megvan a kínai megfelelője[10] (Google–Baidu; Amazon, Ebay – JD, Taobao; Instagram, Facebook, Twitter – Wechat; Youtube – Youkou, QIY). A Wechat ugyanakkor Kínában sokkal több, mint a három nyugati közösségi alkalmazás ötvözése, mert ennél jelentősebb, több funkciója van, amit a következő bekezdésben mutatok majd be. Másfelől a Wechat alkalmazást Kínában közel egymilliárd ember használja a mindennapokban, így az azon futó szolgáltatások mindenki számára elérhetőek az egész országban, ami óriási kényelmet és nagy fokú online jelenlétet ad mindenki számára. Nincs az, mint Európában, hogy egyes országokban – amelyek lakosságszáma egyébiránt összevethető a közepes méretű kínai városok lakosságszámával – elérhető az Uber vagy az AirB&B-szolgáltatás, míg más országokban nem, ennek következtében pedig nem alakítható ki egy egységes rendszer az Európai Unió 448 millió lakosának.[11] Kínában a teljes lakosság számára ugyanolyan korlátozások és lehetőségek mellett érhető el az internet minden szolgáltatása.

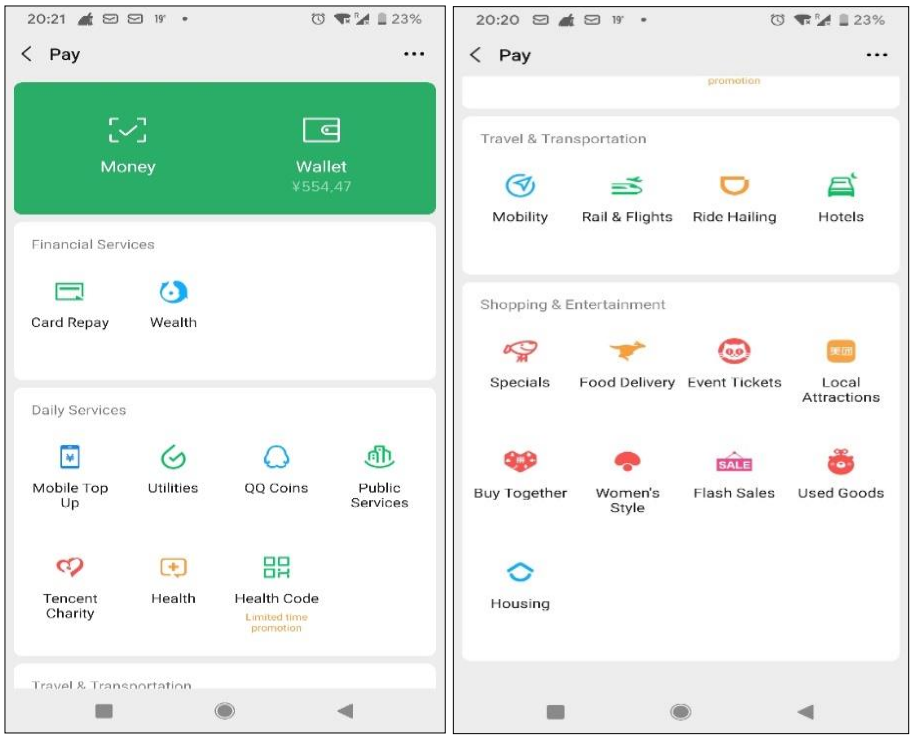
E szolgáltatások közül Kínában szerintem kiemelkedik a készpénz nélküli fizetési szolgáltatás, amely akár a Tencent által működtetett WechatPay, vagy az Alibaba vállalat által üzemeltetett legnagyobb webáruház, a Taobao bázisán még 2004-ben létrehozott Alipay applikáció. Ez lehetővé teszi a kínai állampolgároknak, hogy a telefonjukkal fizessenek mindent, beleértve a piacon vásárolt élelmiszert, a közértben, a plázákban vásárolt termékeket, a biciklibérlést, az ételfutárt, az elektronikus vásárlást és a közüzemi szolgáltatások költségeit. A WechatPay platformon működő szolgáltatások között van repülőjegy- és vonatjegyvásárlás, szállásfoglalás, jegyrendelés, ételfutár, közösségi vásárlás, használt cikk eladása szolgáltatás, de nem is sorolom tovább, a képek jobban megmutatják a rendszer kiterjedtségét.

---

[9] VPN – Virtual Private Network, magyarul virtuális magánhálózat.

[10] VANCE, Ashlee: The People's Republic of The Future. Youtube, 2019.05.23. https://www.youtube.com/watch?v=taZJblMAuko; letöltés: 2021.04.14.

[11] EU population in 2020: almost 448 million. Eurostat, 2020.07.10. https://ec.europa.eu/eurostat/documents/2995521/11081093/3-10072020-AP-EN.pdf/d2f799bf-4412-05cc-a357-7b49b93615f1; letöltés: 2021.04.27.



3. ábra. A WechatPay szolgáltatásai

A WechatPay szolgáltatás Kínán belüli használói képesek egymásnak pénzt küldeni. Természetesen az összes online fizetést igénylő szolgáltatás csak akkor működik, ha valaki rendelkezik kínai bankkártyával és azzal regisztrál a WechatPay szolgáltatásra, így az megfelel a pénzmosás elleni szabályoknak is, mert a bankrendszerben és a pénzügyi szolgáltató rendszerében a pénzmozgás teljes mértékben nyomon követhető. Mind az Alipay, mind a WechatPay szolgáltatás biztosítja az online fizetést bármilyen kínai platformon, beleértve az internetes vásárlást, a közüzemi vagy a parkolási díjak kifizetését is. A rendszer elterjedtségét mutatja, hogy van olyan parkoló, amelyből Alipay vagy WechatPay szolgáltatás nélkül már nem lehet kiállni, mivel nincs parkolási díjat szedő személy a kapunál. A parkolás egyébként Pekingben már sok esetben a kamerarendszereken keresztül automatikusan kerül kiszámlázásra, amit az online applikációval lehet kifizetni a fenti pénzügyi szolgáltatásokon keresztül. Ehhez rendelkezésre állnak a megfelelő rendszámfelismerő rendszerek.

A Covid–19 világjárvány minden online szolgáltatás elterjedését jelentősen elősegítette Kínában is, mint talán mindenhol a világon, és elengedhetetlenné tette a Wechat és az Alipay szolgáltatások, valamint a mobilinternet használatát minden kínai állampolgár számára, mivel ezeken a platformokon fut az egész országban egységes Health Kit egészségügyi szolgáltatás is.

Ez annyit jelent, hogy a magyarországi ügyfélkapu-rendszer részeként működő Elektronikus Egészségügyi Szolgáltatási Tér szolgáltatáshoz hasonlóan a Health Kit applikációban jelennek meg az elvégzett Covid-tesztek eredményei, de itt kapott helyet az oltási igazolvány elektronikus változata is. A Health Kit egyúttal a kontaktkutatás és a karanténszabályozás legfőbb eszköze is, mivel az applikáció automatikusan színkódot (piros-sárga-zöld) vált, ha az illető olyan helyen tartózkodott, ahol igazolt fertőző személy volt. Ez a gyakorlatban úgy működik, hogy addig nem lehet bemenni egy étterembe, boltba vagy bankba, amíg le nem húztuk az adott hely QR-kódját a Health Kit applikációval, amely hanggal és a képernyőn is jelzi, hogy az adott személy nem áll egészségügyi korlátozás alatt, így bemehet az adott intézménybe. Csak zöld kóddal lehet közösségbe menni, a sárga karanténkorlátozást jelent, míg a piros igazolt fertőzöttséget. Mivel az adatokat tárolják, ezért amikor egy személyről utólag kiderül, hogy fertőzött, a Health Kit számítógépes rendszerében könnyű megállapítani, hogy kikkel tartózkodott hosszabb ideig egy légtérben, akik szintén vírushordozók lehetnek. Ebből is látszik, hogy a Health Kit szolgáltatás használata Kínában nem opcionális, azt kötelező használni, vagyis aki nem használja, az nem tud vásárolni még alapélelmiszert sem.

A Health Kit applikáció használatának hatásosságát jelzi a következő példa. 2020 novemberében a 15 millió lakosú Tiencsin (Tianjin) városban azonosítottak öt új Covid-fertőzöttet, majd az applikáció segítségével találtak mintegy 500 közeli kontaktszemélyt. Őket és a lakóépületeikből további több száz családot egy napon belül kényszerkaranténoztak, majd letesztelték a városrész mintegy 2,2 millió lakóját.[12] Az intézkedés következtében néhány hét alatt megszűnt a fertőzés a városban. Az említett gyakorlat az alapja a kínai járvány elleni védekezés sikerének, annak, hogy a járvány csak néhány ezer áldozatot követelt az 1,4 milliárd lakosú országban, ha lehet hinni a kínai híradásoknak. Ugyanakkor a fentihez hasonló intézkedések egy demokratikus országban végrehajthatatlan feladatot jelentenének, mivel azok sértik a lakosság személyiségi jogait. Senki sem viselné el, ha kötelező lenne a nyomon követő applikáció használata, de valószínűleg azt sem, ha a hatóságok lezárnák a lakóháza bejáratát éjszakára, hogy a lakást biztosan senki se hagyhassa el, ami általános volt Kínában a járvány kezdetekor, de még most is előfordulhat, ha új gócpont alakul ki egy lakókörzetben.

Ezzel el is érkeztem ahhoz a megállapításhoz, hogy a kínai lakosság széles körű internethasználata hatékonyan hozzájárul ahhoz is, hogy a kínai vezetés szoros ellenőrzés alatt tartsa az embereket. A WechatPay vagy az AliPay rendszerek kapcsolódnak a bankok rendszereihez, így valós időben ellenőrzik a bankkártya-adatokat és az egyéb banki adatokat a regisztráció során. Minden ilyen szolgáltatás együttműködik az arcfelismerő rendszerrel is. Ez azt jelenti, hogy a banki regisztrációnál, a WechatPay és az AliPay szolgáltatások igénylésénél, de minden banki tranzakciónál, mobiltelefonos ügyintézésnél is kötelező az arckép és a személyi igazolvány – külföldiek esetén az útlevél – adatainak a fotózása, ami automatikusan megtörténik minden határátlépésnél is. Ez a közterületeken működő kiterjedt kamerarendszerrel és a megfelelő szoftverekkel összekapcsolva óriási

[12] LIU, Caiyu – FAN, Anqi: Local outbreak resurfaces in several Chinese cities as winter comes. Global Times, 2020.11.22.
https://www.globaltimes.cn/content/1207677.shtml; letöltés: 2021.04.14.

lehetőséget ad a rendfenntartó szerveknek azon személyek kiszűrésére, akik bűncselekményt követnek el, veszélyt jelentenek a társadalomra vagy a rendszerre, de akár a közlekedési jogviták rendezésére is.

Az AliPay és a WechatPay rendszerek használatának kiterjedtségét jól mutatja a napokban született bírósági ítélet, amely 2,8 Mrd USD (kb. 850 Mrd HUF) összegre büntette az Alipay üzemeltetőjét – az Ant Csoportot –, amely a Kínában és nemzetközileg is ismert kínai milliárdos, Jack Ma érdekeltségébe tartozik. Azt Ant Csoport Alipay szolgáltatásában – amely már a teljes pénzügyi területet felöleli a megtakarítástól a hitelekig – Kínában évente több tízmilliárd tranzakció történik, ami a világ legnagyobb „pénzintézetévé" tette a kínai piacon is 55%-os részesedéssel piacvezető vállalatot. Mindez a cég túlzott megerősödését eredményezte, amit a Kínai Kommunista Párt csak úgy tud elfogadni, ha a vállalat teljes mértékben együttműködik a kínai hatóságokkal. Ezzel szemben Jack Ma még 2020 őszén komoly kritikát fogalmazott meg a pénzügyi felügyelet ellen, amely korlátozta a cég kötvénykibocsátási terveit. A Kínai Kommunista Párt által vezetett rendszer már nem tudta a Nyugat által is csodált különc kínai milliárdostól érkező kritikát megemészteni, így megbüntette az Ant Csoportot. Ezzel azt is biztosította, hogy Jack Ma minél jobban eltávolodjon a vállalattól, és egyidejűleg az állam nagyobb részesedést szerezzen Kína legnagyobb pénzügyi vállalkozásában.[13]

Összességében a leírtakból könnyen kikövetkeztethető, hogy Kínában a fent említett korlátozásokon túl az 5G rendszer bevezetése már nem okozhatott további biztonsági problémákat a lakosság számára, mert Kínában az új rendszer bevezetése csak annyiban növeli az ellenőrzés lehetőségét, hogy egyre több háztartási és egyéb eszköz csatlakozik majd az internetre, ami természetszerűleg még több adatot biztosít a felhasználó mindennapi életéről. Az 5G kapcsán a nyugati társadalmakban óriási félelem van főképp a kínai Huawei telekommunikációs vállalat által kifejlesztett rendszert illetően, de nehéz megítélni, hogy a valós félelem a kínai gyártó rendszerétől van-e, vagy azt az internetre kötött eszközök számának gyors növekedésétől való tartózkodás okozza, esetleg ez csak egy politikai kérdés és a befolyásért folyó harc része az Amerikai Egyesült Államok és a Kínai Népköztársaság között.

Jelenleg Pekingben és a legtöbb kelet-kínai nagyvárosban mindhárom kínai mobilszolgáltatónak van kereskedelmi 5G szolgáltatása. 2020. decemberi adatok szerint Kínában 700 ezer darab 5G-bázisállomás működik – ami a világ 5G-bázisállomásainak 80%-a –, míg Kínában 160 millió 5G-előfizető van, amely a világ előfizetőnek 70%-a. Kínában mindhárom szolgáltató működtet már tisztán 5G-bázisállomásokra épülő rendszert is több nagyvárosban.[14] Ennek köszönhető, hogy a

[13] VASWANI, Karishma: Is Alibaba's fate a warning to China's tech giants? BBC News, 2021.04.15. https://www.bbc.com/news/business-56741551; letöltés: 2021.04.20.

[14] WEISSBERGER, Alan: China tops 200M 5G subs while operators move to 5G SA. IEEE Communication Society, 2020.12.22. https://techblog.comsoc.org/2020/12/22/china-tops-200m-5g-subs-while-operators-move-to-5g-sa/; letöltés: 2021.04.14.

világon minden második 5G-képes okostelefont jelenleg Kínában értékesítik,[15] és az országban minden harmadik eladott telefon 5G-technológiát használ.[16] 2020 szeptemberében kínai gyártók állították elő az 5G-képes mobilkészülékek 80%-át, és akkor még nem volt 5G-képes iPhone mobiltelefon az Apple kínálatában,[17] mert az első ilyen iPhone, az iPhone 12 csak 2020 októberében jelent meg.

Az 5G szolgáltatás körüli viták kapcsán – mint egykor rádiófelderítő szakon végzett és az új technológia iránt mindig nagy érdeklődést mutató tiszt – szeretném megosztani saját véleményemet és tapasztalataimat. Egyfelől nem nehéz belátni – különösen az Edward Snowdenhez kapcsolódó botrány óta –, hogy minden, ami az internetre kerül és ott történik, az nem marad magánügy, és a világháló jelenléte egyre inkább az életünk minden területét érinti. Az 5G-vel ez még inkább így lesz, így egyre kiszolgáltatottabbá válunk majd az internetet ellenőrizni képes, a főbb szervereket működtető szervezeteknek és országoknak. Természetes, hogy jobb ilyen területen is egy szövetséges országnak kiszolgáltatottnak lenni, mint egy nem szövetséges vagy esetleg ellenséges országnak, ha nincs mód a kiszolgáltatottság kivédésére. Végső megoldást csak az jelenthetne, ha a területen nagyhatalmi státusszal rendelkezők, mint az Amerikai Egyesült Államok, a Kínai Népköztársaság és az Oroszországi Föderáció felállítanának egy normarendszert, amely megvédene mindenkit. Erre azonban – a nagyhatalmak közötti feszült viszonyt ismerve – jelenleg nem látszik reális lehetőség, ráadásul éppen az említett országok azok a szereplők, amelyek leginkább képesek a kitettségből adódóan az adatok gyűjtésére és feldolgozására.

Az 5G problémakörének másik olvasata a nagyhatalmak közötti gazdasági és technológiai versenyfutás, amelyben – a korábbi bekezdésben ismertetett számok alapján – úgy tűnik, hogy a Nyugat jelenleg lemaradásban van. A technológiai versenyfutás kapcsán az alábbi tapasztalatokat szereztem. Először 2009-ben érkeztem Kínába, amikor a saját káromon szembesültem azzal, hogy a legnagyobb kínai szolgáltató, a kb. 800 millió előfizetővel rendelkező China Mobile egy Európában ismeretlen 3G rendszert, a TD-CDMA rendszerre épülő hálózatot alakított ki, ezért a Magyarországon beszerzett 3G-képes mobiltelefon nem tudta használni azt a szolgáltatást, amíg nem váltottam szolgáltatót. Mivel Kína elkésett a 3G fejlesztésével, ezért a világon a China Mobile és a China Telecom szolgáltatón kívül más nem alkalmazta a TD-CDMA rendszert, bár a kettő akkor valószínűleg felölelte a világ mobil-előfizetőinek ötödét. A harmadik kínai szolgáltató, a China Unicom az Európában is elterjedt WCDMA rendszert alkalmazta. A China Mobile és a China Unicom az Európában elterjedt GSM rendszerre építette még a 2G hálózatát, míg a China Telecom a többek között az Amerikai Egyesült Államokban, Japánban és Dél-Koreában is alkalmazott CDMA rendszert használta 2G gyanánt.

---

[15] DAYARAM, Sareena: China is buying most of the world's 5G phones, report finds. CNET, 2020.02.21. https://www.cnet.com/news/china-is-buying-most-of-the-worlds-5g-phones-report-finds/; letöltés: 2021.04.14.

[16] RANGER, Steve: 5G smartphone sales in China are rocketing. That could be a big deal for the rest of the world. ZDNET, 2020.07.28. https://www.zdnet.com/article/5g-smartphone-sales-in-china-are-absolutely-rocketing/; letöltés: 2021.04.14.

[17] WANG, Junwei: China's 5G smartphone sales set to reach 140m units in 2020. China Daily, 2020.09.29. https://global.chinadaily.com.cn/a/202009/29/WS5f72ca36a31024ad0ba7c9ba.html; letöltés: 2021.04.14.

Az áttérés a 4G szolgáltatásra már a 2012–2016 között teljesített első kínai külszolgálatom idején történt, és ott a LTE-FDD nyugati és az LTE-TDD kínai rendszer már minden modern telefonban egyidejűleg elérhető volt, mert Kína ekkor már fel tudta venni a lépést a nyugat-európai fejlesztőkkel.

Kínában ugyanakkor a fejlődés sebessége minden területen nagyobb, mint a nyugat-európai és az észak-amerikai térségben, így az 5G szolgáltatásban a kínai Huawei már jelentős lépéselőnyre tett szert a nyugati fejlesztőkkel szemben. Félő volt, hogy ha az 5G területén nem sikerül megállítani a Huawei terjeszkedését, akkor a nyugat-európai és az észak-amerikai gyártók végleg vereséget szenvednek, hosszabb távon eltűnhetnek a piacról. Ráadásul itt van még a 6G szolgáltatás is, amelynek a fejlesztése már megkezdődött Kínában. Ennek megfelelően a Huawei és az 5G körüli vita inkább a két nagyhatalom, az Amerikai Egyesült Államok és a Kínai Népköztársaság közötti technológiai versenyfutás része, ahol jelenleg a kínai fél vezet. Washington – hogy behozhassa lemaradását – adminisztratív korlátozással akar időt nyerni, és azokat biztonsági megfontolásokkal próbálja elfogadhatóvá tenni nyugat-európai partnerei számára. Ez azért is nehéz, mert a Snowden-botrány óta ismert, hogy az Amerikai Egyesült Államok nem csak az „ellenséges" országokban folytatott adatgyűjtést, vagyis nem tekinthető ártatlannak a számítógépes kémkedés világában. Az amerikai fél által megfogalmazott biztonsági megfontolásokat a Huawei-jel szemben bizonyos országok elfogadják, és ezzel lelassítják saját fejlődésüket is, míg más országok nem teszik ezt meg. A kérdés másik vetülete azon információk hiánya, hogy az igazi biztonsági problémát a Huawei 5G rendszerének hardverelemei vagy a hozzájuk tartozó szoftverek okozzák-e, amire amerikai részről nincs egyértelmű magyarázat vagy bizonyíték.

A kínai haderő kiberműveleti erői

Mielőtt rátérnék a kínai haderő kiberműveleti erőire és azok kialakításának hátterére, nézzük meg, hogy a Kínai Népköztársaságban milyen szervezetek rendelkeznek még ilyen képességekkel.

A Kínai Népköztársaság a nyugati országokhoz viszonyítva nagyon korlátozottan biztosít információt a különböző állami szervek működéséről, azok költségvetéséről. A kínai kiberműveleti erőkről és tevékenységükről ezért leginkább csak nyugati elemzések adnak korlátozott képet és mutatnak be olyan eseteket, amikor egyértelművé vált, hogy mely ország állhat a kibertámadás mögött, még ha ezt a legtöbb esetben nem is lehet egyértelműen bizonyítani.

Kínában az elemzések azt mutatják, hogy a kiberműveleti képességek területén a legnagyobb képességekkel a Kínai Népi Felszabadító Hadsereg rendelkezik, megelőzi az Állambiztonsági Minisztériumot. Az e témában készült tanulmányok megemlítik a Kínai Népi Felszabadító Hadsereghez kötődő Népi Milíciák ilyen irányú képességeit is, illetve a kínai technológiai vállalatok együttműködését ezen a területen.[18]

[18] MORGUS, Robert – FONSECA, Brian – GREEN, Kieran: Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? New America Cybersecurity Initiative, 2019.07.26. https://www.newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/china-and-cyberspace/; letöltés: 2021.04.20.

A Népi Milíciák a haderő második tartalékát képezik. Minden 18–35 év közötti kínai állampolgárnak részt kell vennie a tevékenységében az érvényben lévő honvédelmi törvény alapján. A technológiai szektorban dolgozók természetesen valószínűleg az ott megszerzett tudásukat kamatoztathatják a kínai haderő érdekében a Népi Milíciák szervezetében, míg a tenger mellett élők a Haditengerészeti Milíciához csatlakoznak.

A technológiai cégek kapcsán érdemes figyelembe venni, hogy Kínában az állam és az azt irányító Kínai Kommunista Párt mindent képes a felügyelete alatt tartani, ellentétben a liberális demokráciákkal, ahol a cégek működésének legnagyobb mozgató ereje a profit. A Kínai Népköztársaság ezt a helyzetet is jól kihasználja minden területen. Egy aktuális példa: Kína annak az országnak ad el oltóanyagot, amelyik nem kritizálja őt, hajlandó teljes körű együttműködésre a kínai vezetéssel, és ennek megfelelően a kínai állami és magánvállalatok csak azon országokkal köthetnek a szerződéseket, amely országok irányában a kínai állami vezetés támogatja a vakcina eladását. Minden vakcinaexporthoz a kínai Külügyminisztériumban adják ki az engedélyt. Példaként említhetném a Fülöp-szigetek oltóanyag-ellátásának helyzetét. Az ország elnöke 2020 decemberében azt javasolta az amerikai kormányzatnak, hogy ha utóbbi szeretne továbbra is amerikai bázisokat az országban, akkor biztosítson oltóanyagot a Fülöp-szigetek lakosságának.[19] Nem kapott választ, Kína viszont azonnal biztosított vakcinát az ország részére.[20] Ha a külpolitikai vonatkozásokat nézzük, akkor a Fülöp-szigetek kulcsszerepet játszik a Kínai Népköztársaság és az Amerikai Egyesült Államok közötti vetélkedésben a Dél-kínai-tengeren. A Fülöp-szigetek az egyik azon országok között, amelyek legközelebb fekszenek a Spratly-szigetcsoporthoz, amelyen belül Kína több mesterséges szigetet épített, továbbá a szigetcsoport több szigete a Fülöp-szigetek kizárólagos gazdasági övezetében található.[21]

A kínai haderő képességeit illetően a vezetés először 1997-ben hozott létre egy 100 fős csoportot a legfelsőbb katonai felsővezetés alárendeltségében, amely a számítógépes rendszerek biztonságáért, illetve azok elterjesztéséért volt felelős. Ez a csoport adta a később létrehozott kiberműveleti erők alapját. Ezt követően a kiber- és elektronikaiharc-erők az Általános Vezérkar 3. és 4. csoportfőnökségeként működtek 2015-ig, majd Kína a katonai reform részeként létrehozta a kiber- és az űrhadviselésért felelős Hadászati Támogató Erőt (SSF[22]).[23]

---

[19] VENZON, Cliff: Duterte threatens to end US military pact if no vaccines. Nikkei Asia, 2020.12.27. https://asia.nikkei.com/Politics/International-relations/Duterte-threatens-to-end-US-military-pact-if-no-vaccines; letöltés: 2021.04.27.

[20] Philippine President Duterte receives first dose of China's Sinopharm Covid-19 vaccine. South China Morning Post, 2021.05.04. https://www.scmp.com/video/asia/3132144/philippine-president-duterte-receives-first-dose-chinas-sinopharm-covid-19; letöltés: 2021.04.27.

[21] WINGFIELD-HAYES, Rupert: China's Island Factory. BBC News, 2014.09.09. https://www.bbc.co.uk/news/resources/idt-1446c419-fc55-4a07-9527-a6199f5dc0e2; letöltés: 2021.04.27.

[22] Strategic Support Force (SSF).

[23] KANNAN, Saikiran: Inside China's cyber war room: How PLA is plotting global attacks. India Today, 2020.08.06. https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06; letöltés: 2021.04.20.

A 2015-ös katonai reform két jelentős változást hozott. Egyfelől megalakították a Szárazföldi Vezérkart azzal a céllal, hogy a korábban szárazföldi súlypontú haderőt átalakítsák összhaderőnemi erővé, vagyis a szárazföldi erőket azonos szintre hozzák vissza, mint a légierő, a haditengerészet és a hadászati csapásmérő erők. A szárazföldi haderőnem korábbi hét területi parancsnokságát egyidejűleg a légierő és a haditengerészet bevonásával öt összhaderőnemi parancsnoksággá alakították, aminek célja szintén a szárazföldi erők túlsúlyának a megszüntetése volt.

A másik lépés összhangban van a 2015-ben kiadott Katonai Stratégiával, amely megnevezte a világűrt és a kiberteret a hadviselés új területeiként, az új hadszíntereken szükséges képességeket (elektronikai hadviselés, pszichológiai hadviselés, űrhadviselés, kiberhadviselés) egy új haderőnembe egyesítette, amelyet Stratégiai Támogató Erők néven hozott létre, és az a másik négy haderőnemmel (szárazföldi, légierő, haditengerészet, rakétacsapatok) azonos szintű parancsnokságként alakult meg 2015 végén. A reform kapcsán fontos megemlíteni, hogy a Kínai Népi Felszabadító Hadseregnek 2020-ig kellett elérnie a teljes gépesítettséget, 2035-ig a teljes körű informatizáltság elérése a cél annak érdekében, hogy 2049-re – a Kínai Népköztársaság centenáriumára, egyidejűleg az ország teljes újraegyesítésével – a kínai haderő a világ egyik legerősebb hadereje legyen.[24]

A koncepciót a kínai kiberműveleti erőkre a kínai haderő még 2013-ban alkotta meg, neve Hármas Hadviselés,[25] amely a közvélemény és a média befolyásolásával, a pszichológiai hadviseléssel, valamint a nemzeti és a nemzetközi joghézagok kihasználásával teremt kedvező feltételeket a stratégiai célok eléréséhez.

4. ábra: A kínai Hármas Hadviselés[26]

[24] China's Military Strategy (full text). Kína Katonai Stratégiája. The State Council the People's Republic Of China, 2015.05.27. http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm; letöltés: 2021.04.20.

[25] Three Warfares.

[26] KANIA, Elsa; The PLA's Latest Strategic Thinking on the Three Warfares. The Jamestown Foundation, 2016.08.22. https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/; letöltés: 2021.04.20.

Ezek – az elektronikai hadviseléssel és a hírszerzéssel kiegészülve – testesítik meg a nem hagyományos és a kiberhadviselés teljes spektrumát.

Kína – miután 2015-ben a katonai reform részeként jelentős átalakításokat hajtott végre a haderő szervezetében, majd 2016-ban egy új haderőnemként létrehozta az összhaderőnemi logisztikai parancsnokságot is (egyelőre a haderőnemeknél eggyel alacsonyabb, hadszíntérparancsnokság-helyettesi szinten) –, 2021. január 1-jei hatállyal új védelmi törvényt fogadott el, amely 30. cikkelyében megjeleníti a hadviselés új területeit: a világűrt, az elektromágneses teret és a kiberteret.[27]

A koncepciókat illetően a japán NIDS biztonságpolitikai kutatóintézet a technológiai fejlettség és a hadviselés összefüggései kapcsán úgy véli, hogy Kína egyre inkább támaszkodik majd a tömeges adatokra támaszkodó hírszerzői elemzésekre és a mesterséges intelligenciára a modern hadviselésben.[28]

A kínai Központi Katonai Bizottság[29] döntése alapján 2016. január 1-jei hatállyal létrehozták a Hadászati Támogató Erőt, amelynek szervezete az 5. ábrán látható.

A Hadászati Támogató Erő (SSF) szervezetében – mint minden kínai egységnél és parancsnokságon – megtalálható a négy funkcionális csoportfőnökség: a törzs, a politikai munka főnöksége, a logisztikai és a fegyverzeti főnökség. A szervezetet az SSF parancsnoka és a vele azonos szinten lévő politikai biztosa együttesen vezeti. A kettős vezetés a kínai haderőben teljes mértékben működő modell, századszinttől minden alakulatnak két vezetője van: a parancsnoka és a politikai biztosa. Előbbi nagyobb felelősséggel tartozik a szakmai feladatok vonatkozásában, míg utóbbi a politikai nevelés és a humánpolitikai munka területén rendelkezik nagyobb hatáskörrel, de a rendszer arra kötelezi őket, hogy helyetteseik bevonásával bizottsági döntéshozatalt valósítsanak meg, mint ahogy ez így működik a kínai politikai vezetés minden szintjén. Ezért is nevezhető Kína egy autokratikus országnak kínai sajátosságokkal, mint ahogy az ország politikai rendszere is a szocializmus kínai sajátossággal nevet kapta.

Az SSF két fő műveleti részre osztható: az űrhadviselés erőire, valamint a kiber-, elektronikai és pszichológiai hadviselés erőire. Az űrhadviselési erők legfőbb eleme a Kínai Népi Felszabadító Hadsereg által üzemeltetett négy űrrakéta-kilövő állomás (Csiucsüan – Jiuquan, Tajjüan – Taiyuan, Hszicsang – Xichang, Vencsang – Wenchang[30]), a pekingi űrrepülő-irányító központ, a Hszian (Xian) városában működő műholdirányító központ és tengeri űrmegfigyelő központ.

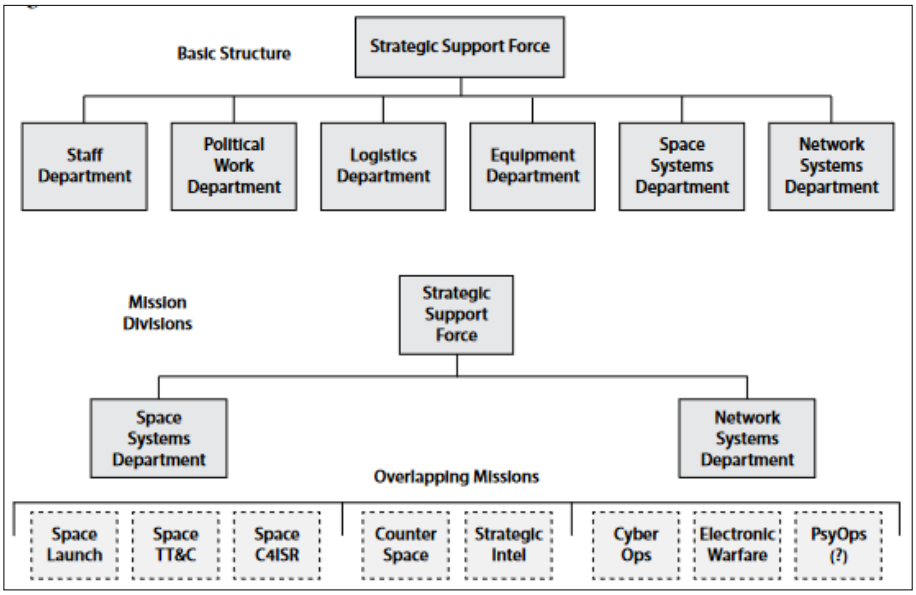
---

[27] 中华人民共和国国防法. A Kínai Népköztársaság Honvédelmi törvénye. A Védelmi Minisztérium honlapja, 2020.12.27. http://www.mod.gov.cn/regulatory/2020-12/27/content_4876050.htm; letöltés: 2021.04.20.

[28] NIDS China Security Report 2021 – China's Military Strategy in the New Era. National Institute for Defense Studies, Japan, 2020. p. 17. http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2021_A01.pdf; letöltés: 2021.04.20.

[29] Central Military Commission (CMC).

[30] A kínai települések neveit a magyar átírás szerint jelenítettem meg, de zárójelben vagy kötőjellel szerepel az angol kiejtés szerinti pinyin átírás a könnyebb kereshetőség érdekében.



5. ábra. A Hadászati Támogató Erő szervezete[31]

A kiber- és elektronikaiharc-erők magukban foglalják a korábban az Általános Vezérkar 3. csoportfőnöksége által felügyelt kiberműveleti és elektronikai felderítőerőket, valamint a 4. főcsoportfőnökség által felügyelt rádiótechnikai felderítő- és zavaróerőket, továbbá ez a terület felügyeli a Politikai Főcsoportfőnökség állományából átvett pszichológiai hadviselési erőket is. A rádiótechnikai erők egy jelentős része azonban az Összhaderőnemi Vezérkar alárendeltségében maradt, mert Kínában továbbra is a haderő felel a légtérvédelem mellett a teljes légi irányításért is.

A korábbi 3. főcsoportfőnökség állományából az új szervezethez kerültek a 12 kiberműveleti és elektronikai hírszerzési iroda, a pekingi számítógépközpont és az 57., 58., 59. kutatóintézetek. A korábbi 3. csoportfőnökség alá tartozott, Luojang (Luoyang) városban működő Kínai Népi Felszabadító Hadsereg Idegen Nyelvi Egyetemét integrálták a korábban a 4. csoportfőnökség alatt működő Információtechnológiai Egyetem állományába.[32]

[31] COSTELLO, John – MCREYNOLDS, Joe: China's Strategic Support Force: A Force for a New Era. INSS, October 2018. p. 21. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf; letöltés: 2021.04.20.

[32] Uo. p. 34.

Az SSF fő kiberműveleti erőit az említett 12 iroda jelenti, közülük az amerikai nyomozóhatóságoknak a Sanghajban működő irodát sikerült egyértelműen azonosítaniuk,[33] azt a FireEye internetbiztonsági szervezet ATP1 hekkercsoportként tartja nyilván.[34] Egy tanulmány 130 ezer főre becsüli a kínai haderő azon állományát, amely az amerikai Nemzetbiztonsági Ügynökséghez[35] hasonlóan elektronikai és kiberműveletekben vesz részt,[36] de a pontos számadat nem áll rendelkezésre.

A 4. csoportfőnökség állományából Langfang (Langfang), Jintan (Yingtan), Pejdajho (Beidaihe), Nicseng (Nicheng) városokban működő elektronikaiharc-dandárok átkerültek az SSF állományába, majd onnan a létrehozott hadszíntér-parancsnokságok felügyelete alá, mert ezek inkább harcászati, hadműveleti képességet képviselnek, a szakmai felügyeletüket azonban az SSF látja el. A pekingi űrközpont is – a négy kilövőállomással együtt – az SSF állományába került, de nem a hálózati szervezethez, hanem az űrhadviselést felügyelő részleghez. A hálózati részleghez került az 54. kutatóintézet is, amely korábban a 4. csoportfőnökség alá tartozott.[37]

A SSF és az új katonai körzetek megalakításával a kínai katonai vezetés jelentősen átalakította a katonai hírszerzés rendszerét is: a korábbi 2. csoportfőnökség bázisán egy hadászati felderítőhivatalt hoztak létre az Összhaderőnemi Vezérkar alárendeltségében, míg a hadműveleti-harcászati felderítőerők felügyeletét teljes egészében átadták az öt hadszíntér-parancsnokságnak, valamint a felderítő csoportfőnökség egy része átkerült az SSF állományába.[38]

A pszichológiai hadviselés erőit illetően az SSF szervezetébe került át a 311. bázis, amely korábban a Politikai Főcsoportfőnökség állományába tartozott.[39] Ez a kínai haderő egyetlen Tajvanra irányuló PsyOps egysége, amely a Fucsian (Fujian) tartomány székhelyén, Fucsou (Fuzhou) városában települ, és legalább hat alárendelt ezred bevonásával folytat propagandaháborút Tajvan ellen.[40] Emellett a kínai haderő működtet újságot, TV-csatornát, művészegyüttest, de ezek továbbra is a jelenleg Politikai Munka Főcsoportfőnökségének hívott szervezet alárendeltségében működnek, és feladatuk alapvetően a kínai közvélemény befolyásolása és a haderő moráljának fenntartása.

---

[33] Five Chinese Military Hackers Charged – Indicted in Connection with Cyber Espionage Offenses Against U.S. FBI, 2014.05.19. https://www.fbi.gov/news/stories/five-chinese-military-hackers-charged-with-cyber-espionage-against-us; letöltés: 2021.04.20.

[34] Advanced Persistent Threat Groups – Who's who of cyber threat actors: APT1. https://www.fireeye.com/current-threats/apt-groups.html#china; letöltés: 2021.04.20.

[35] National Security Agency (NSA).

[36] KOZŁOWSKI, Andrzej: The "Cyber Weapons Gap." The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan. University of Lodz, p. 4. https://core.ac.uk/download/pdf/71981805.pdf; letöltés: 2021.04.20.

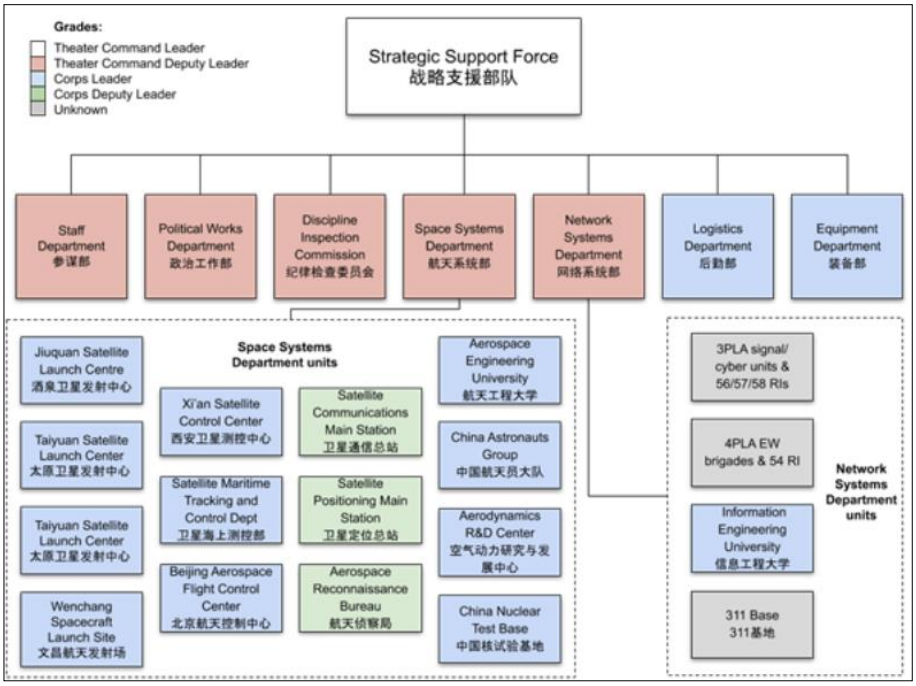
[37] COSTELLO, John – MCREYNOLDS, Joe: China's Strategic Support Force: A Force for a New Era. INSS, October 2018. p. 37. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf; letöltés: 2021.04.20.

[38] Uo. p. 42.

[39] Uo. p. 38.

[40] KANIA, Elsa B.: The Role of PLA Base 311 in Political Warfare against Taiwan (Part 3). Global Taiwan Brief, Volume 2, Issue 7, 2017.02.15. https://globaltaiwan.org/2017/02/15-gtb-2-7/#ElsaKania021517; letöltés: 2021.04.20.

Az SSF szervezetéről a 2015-ös megalapítása óta folyamatosan jelennek meg információk – főképpen amerikai kutatóintézetektől. Ezek közül a legfrissebb és legrészletesebb struktúrát az SSF szervezetéről a 2019. május 29-én frissített jelentés tartalmazza a Jamestown biztonsági kutatóintézet kiadásában.



6. ábra. Az SSF szervezete (2019.09.)[41]

Sajnos ez sem részletezi jobban a kiberműveleti erők szerkezetét, bár jelzi, hogy a 12 iroda és a három kutatóközpont – amelyek korábban a Vezérkar 3. csoportfőnökségéhez tartoztak – most biztosan az SSF részét képezik.

Ennél részletesebb információk a Project 2049 Institute elnevezésű kutatóintézet 2011-es jelentésében vannak, amely részleteiben bemutatja a kiberműveletekkel és kiberkémkedéssel foglalkozó 12 iroda célirányait és tevékenységét.[42] Sajnos az információk már elég régiek, de ennél részletesebb bemutatás azóta sem jelent meg a kínai haderőt tanulmányozó kutatóintézetek kiadványaiban.

[41] NI, Adam – GILL, Bates: The People's Liberation Army Strategic Support Force: Update 2019. The Jamestown Foundation, 2019.05.29. https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/; letöltés: 2021.04.20.

[42] STOKES, Mark A. – LIN, Jenny – HSIAO, Russell: The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure. Project 2049 Institute, 2011.11.11. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf; letöltés: 2021.04.20.

Az SSF valós tevékenységéről nagyon kevés információ áll rendelkezésre, nem úgy, mint a Kínai Népköztársaság által feltételezetten elkövetett kibertámadásokról. Ezek közül megemlítek néhány nagy vihart kavart esetet, melyekhez hasonlókról a nemzetközi sajtóban szinte napi rendszerességgel jelennek meg írások.

De először nézzük meg, hogy mire is használta és a jövőben mire használhatja a kínai haderő a kibertámadó képességeit, melyeket egy az ausztrál védelmi tárcához kapcsolódó honlap nagyon jól összefoglalt:

– kiberkémkedés;
– az információs fölény kialakítása egy konfliktust megelőző helyzetben vagy egy konfliktus kezdeti szakaszában;
– a harcoló erők tevékenységének támogatása, ezáltal a képességek növelése.[43]

Kína eddig a legnagyobb sikereit a kibertérben a kiberkémkedés területén érte el főképpen észak-amerikai és nyugat-európai hadiipari vállalatok szervereibe való behatolásokkal és nagy mennyiségű adat letöltésével. Ilyen volt például az F–35 típusú ötödik generációs repülőgép tervrajzainak és leírásainak 2009-es megszerzése.[44]

Az FBI vezetője, Christopher Wray egy 2020-ban adott interjúban arról beszélt, hogy Kína évente kb. 300–600 Mrd USD kárt okoz amerikai vállalatoknak és a kormányzatnak az általa végrehajtott kiberkémkedéssel.[45]

Szintén nagy vihart kavart az Amerikai Egyesült Államokban az, amikor 2015-ben kiderült, hogy valószínűsíthetően kínai hekkerek megszerezték 4,2 millió amerikai közalkalmazott teljes személyzeti anyagát, beleértve a biztonsági kérdőíveket is.[46]

2018 decemberében került napvilágra, hogy kínai hekkerek sikeresen támadtak meg 45 amerikai technológiai vállalatot és állami intézményt, ahonnan nagy mennyiségű adatot töltöttek le, többek között a haditengerészethez tartozó 100 ezer fő adatait.[47] Ezek csak ízelítők, mert lehetetlen a teljesség igényével bemutatni a kínai hekkerek és a kínai hírszerzés által elkövetett sikeres műveletek teljes körét.

---

[43] POMERLEAU, Mark: 3 ways China's military could use cyber in war. Fifth Domain, 2019.01.16. https://www.fifthdomain.com/dod/2019/01/16/3-ways-chinas-military-could-use-cyber-in-war/; letöltés: 2021.04.20.

[44] ALEXANDER, David: Theft of F-35 design data is helping U.S. adversaries – Pentagon. Reuters, 2013.06.19. https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619; letöltés: 2021.04.20.

[45] China theft of technology is biggest law enforcement threat to US, FBI says. The Guardian, 2020.02.06. https://www.theguardian.com/world/2020/feb/06/china-technology-theft-fbi-biggest-threat; letöltés: 2021.04.20.

[46] FINKLEA, Kristin – CHRISTENSEN, Michelle D. – FISCHER, Eric A. – LAWRENCE, Susan V. – THEOHARY, Catherine A.: Cyber Intrusion into U.S. Office of Personnel Management: In Brief. Congressional Research Service, 2015.07.17. https://fas.org/sgp/crs/natsec/R44111.pdf; letöltés: 2021.04.21.

[47] BURKE, Evan – SERRONE, Matthew – THOMAS, Khristal – NELSON, Arthur – HAIMOWITZ, Ian: Survey of Chinese-linked Espionage in the United States Since 2000. Center for Strategic and International Studies. https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000; letöltés: 2021.04.20.

Egy nemzetközi tanulmány szerint a világban végrehajtott kibertámadások közel 30%-áért bizonyítottan Kína tehető felelőssé. Az ország 2009 és 2019 között 79 dokumentált kibertámadást hajtott végre a világ 20 országában. Kínát kis lemaradással Oroszország követi, amely az adott időszakban bizonyítottan 75 támadást indított 19 ország ellen.[48]

Vannak példák arra is, hogy amikor Kína kisebb konfliktusba kerül egy másik országgal, akkor előszeretettel nyúl a kiberfegyvertárhoz, hogy elterelje a figyelmet a konfliktusról, illetve a saját oldalára próbálja állítani a közvéleményt. Erre a legutóbbi példát a 2020 júniusában Kína és Indiai között kiújult határkonfliktus szolgáltatta, amelyben sajnálatos módon 20 indiai és négy kínai katona is életét vesztette. A kínai médiában a konfliktus idején jelentősen nőtt a témában bemutatott dokumentumfilmek száma, és az érintett vitatott hovatartozású területet kínaiként mutatták be. A konfliktus kialakulásakor az India elleni kibertámadások száma megsokszorozódott, öt nap leforgása alatt 40 ezer támadás ért különböző indiai intézményeket.[49] Valószínűsíthetően Kína felelős azért a 2020 októberében végrehajtott kibertámadásért is, amely az ország áramellátó rendszerét érte, komoly nehézségeket okozva Indiában.[50]

Szerencsére még nincs tapasztalat arról, hogy Kína milyen módon alkalmazná a kibererőit egy esetleges háborús konfliktus esetén, de feltételezhetően egy Tajvan szigete elleni invázió azzal kezdődne, hogy minden erővel akadályoznák Tajvan informatikai rendszereinek működését, és valószínűleg megpróbálnák leválasztani a szigetet a globális internetről, mint ahogy tennék ezt a kínai szárazfölddel is. Utóbbi a nagy Kínai Tűzfallal könnyen megoldható. A kínai támadás lehetősége óriási félelemmel tölti el a tajvani hadműveleti tervezőket,[51] mivel egy olyan területről beszélünk, ahol világviszonylatban a leggyorsabb internettel rendelkeznek, így feltehetően sok szolgáltatás épül a világhálóra.

Sajnos napjainkban az amerikai–kínai szembenállás közelebb hozta egy Tajvan és a Kínai Népköztársaság, illetve a Kínai Népköztársaság és az Amerikai Egyesült Államok közötti konfliktus lehetőségét. Egyfelől Washington az elmúlt években több olyan lépést is tett Tajpej irányában, amilyeneket a korábbi amerikai adminisztrációk óvatosságból nem tettek meg, másfelől Kína erősödésével a pekingi vezetés egyre inkább sürgetni fogja majd Tajvan és a szárazföldi Kína egyesülését, még ha Tajvan lakossága békés úton nem is mutat erre hajlandóságot.

---

[48] ROBINSON, Joe; Cyberwarfare statistics: A decade of geopolitical attacks. Privacy Affairs, 2021.02.25. https://www.privacyaffairs.com/geopolitical-attacks/; letöltés: 2021.04.20.

[49] Chinese hackers attempted 40,000 cyber attacks on Indian web, banking sector in 5 days. India Today, 2020.06.24. https://www.indiatoday.in/india/story/chinese-hackers-attempted-40-000-cyber-attacks-on-india-1692088-2020-06-24; letöltés: 2020.04.21.

[50] ADLER, Seth: IOTW: China Possibly To Blame For India's 2020 Power Outage As Cyber Warfare Increases Globally. Cyber Security Hub, 2021.03.05. https://www.cshub.com/attacks/articles/iotw-china-possibly-to-blame-for-indias-2020-power-outage-as-cyber-warfare-increases-globally; letöltés: 2021.04.20.

[51] Taiwan Fears China Could Cut Undersea Cables. Asia Sentinel, 2019.02.01. https://www.asiasentinel.com/p/taiwan-fears-china-cut-undersea-cables; letöltés: 2021.04.20.

A kínai stratégiai tervek Hszi Csinping kínai pártfőtitkár és államfő „Kínai Álom” elnevezésű koncepciója szerint 2049-ig – a Kínai Népköztársaság centenáriumáig – Tajvannak is vissza kell térnie Kínához, mint ahogy az elmúlt időszakban felgyorsították a demokratikus Hongkong és Makaó integrálását az autokratikus, egy pártra épülő kínai rendszerbe, miközben korlátozták a két különleges közigazgatási terület lakossága számára az „Egy ország két rendszer” szisztéma alapján biztosított demokratikus jogokat. Kína elsősorban Tajvan békés integrációjában érdekelt, de nem zárja ki erő alkalmazását sem, különösen akkor, ha a tajvani vagy az amerikai vezetés további lépéseket tesz a sziget függetlenedése érdekében.

Összességében a kínai internet továbbra is komoly korlátozások mellett működik, mely korlátozások célja a kínai rendszer és a Kommunista Párt vezető szerepének megőrzése, de emellett a lakosság sokkal szélesebb körben alkalmazza az internet adta lehetőségeket, mint a nyugati demokráciákban tesszük ezt. Ez az egységes kínai internetszolgáltatásnak köszönhető, vagyis az 1,4 milliárdos kínai lakosság teljes egésze ugyanazon szolgáltatásokat használja, ami óriás kínai technológiai cégek kialakulását eredményezte, amelyek gazdasági erejüknek köszönhetően terjeszkednek más kontinensekre is.

A kínai katonai vezetés a 2015-ös katonai reformmal új erőt hozott létre a Hadászati Támogató Erő megalapításával az új hadviselési területekre, ami előremutató lépésnek tekinthető. Az erők tevékenységéről és szervezetéről a külföldi tanulmányokon túl csak nagyon korlátozottan állnak rendelkezésre megbízható információk, mert Kína a lehető legkevesebb információt adja ki magáról, hogy ezzel ne gyengítse önmagát. A kibertámadó erők működése része a Kínai Kommunista Párt által előszeretettel alkalmazott hibrid hadviselésnek, amelynek az elvei még Szun-Ce idejéből származnak, aki a hadviselés törvényeiben azt írta meg, hogy a legszebb győzelem az, amit harc nélkül érhetünk el. Erre a célra a kiberhadviselés – benne a kiberkémkedés és a kibertámadások – rendszere ideális a kínai vezetés számára, mert úgy lehet sikereket elérni, hogy nagyon nehezen bizonyítható az állami szervek szerepvállalása a támadásokban. A napokban mind Japánban,[52] mind az Amerikai Egyesült Államokban[53] újabb vádak fogalmazódtak meg Kínával szemben kiberkémkedés miatt, de a hivatalos kínai kommunikáció szerint az ország maga is áldozata a kibertámadásoknak, és a kínai kormányzat nem követ el kibertámadásokat egyetlen ország ellen sem. Nem könnyű ennek az ellenkezőjét bizonyítani, de néha azért sikerül, bár Kína kormányzata ekkor sem ismeri el azt.

[52] YAMAGUCHI, Mari: Japan says Chinese military likely behind cyberattacks. Japan Today, 2021.04.21. https://japantoday.com/category/crime/japan-says-chinese-military-likely-behind-cyberattacks; letöltés: 2021.04.22.

[53] China-linked hackers used VPN flaw to target US defence industry, researchers say. South China Morning Post, 2021.04.21. https://www.scmp.com/tech/tech-war/article/3130375/china-linked-hackers-used-vpn-flaw-target-us-defence-industry; letöltés: 2021.04.22.

FELHASZNÁLT IRODALOM

- ADLER, Seth: IOTW: China Possibly To Blame For India's 2020 Power Outage As Cyber Warfare Increases Globally. Cyber Security Hub, 2021.03.05. https://www.cshub.com/attacks/articles/iotw-china-possibly-to-blame-for-indias-2020-power-outage-as-cyber-warfare-increases-globally; letöltés: 2021.04.20.
- Advanced Persistent Threat Groups – Who's who of cyber threat actors: APT1. https://www.fireeye.com/current-threats/apt-groups.html#china; letöltés: 2021.04.20.
- ALEXANDER, David: Theft of F-35 design data is helping U.S. adversaries – Pentagon. Reuters, 2013.06.19. https://www.reuters.com/article/usa-fighter-hacking/theft-of-f-35-design-data-is-helping-u-s-adversaries-pentagon-idUSL2N0EV0T320130619; letöltés: 2021.04.20.
- BARBOZA, David: Billions in Hidden Riches for Family of Chinese Leader. The New York Times, 2012.10.25. https://www.nytimes.com/2012/10/26/business/global/family-of-wen-jiabao-holds-a-hidden-fortune-in-china.html; letöltés: 2021.04.14.
- BURKE, Evan – SERRONE, Matthew – THOMAS, Khristal – NELSON, Arthur – HAIMOWITZ, Ian: Survey of Chinese-linked Espionage in the United States Since 2000. Center for Strategic and International Studies. https://www.csis.org/programs/technology-policy-program/survey-chinese-linked-espionage-united-states-2000; letöltés: 2021.04.20.
- China theft of technology is biggest law enforcement threat to US, FBI says. The Guardian, 2020.02.06. https://www.theguardian.com/world/2020/feb/06/china-technology-theft-fbi-biggest-threat; letöltés: 2021.04.20.
- China's Military Strategy (full text). Kína Katonai Stratégiája. The State Council the People's Republic Of China, 2015.05.27. http://english.www.gov.cn/archive/white_paper/2015/05/27/content_281475115610833.htm; letöltés: 2021.04.20.
- China-linked hackers used VPN flaw to target US defence industry, researchers say. South China Morning Post, 2021.04.21. https://www.scmp.com/tech/tech-war/article/3130375/china-linked-hackers-used-vpn-flaw-target-us-defence-industry; letöltés: 2021.04.22.
- Chinese hackers attempted 40,000 cyber attacks on Indian web, banking sector in 5 days. India Today, 2020.06.24. https://www.indiatoday.in/india/story/chinese-hackers-attempted-40-000-cyber-attacks-on-india-1692088-2020-06-24; letöltés: 2020.04.21.
- Constitution of the People's Republic of China. A Kínai Népköztársaság Alkotmánya. The State Council the People's Republic Of China, 2019.11.20. http://english.www.gov.cn/archive/lawsregulations/201911/20/content_WS5ed8856ec6d0b3f0e9499913.html; letöltés: 2021.04.14.

- COSTELLO, John – MCREYNOLDS, Joe: China's Strategic Support Force: A Force for a New Era. INSS, October 2018. https://ndupress.ndu.edu/Portals/68/Documents/stratperspective/china/china-perspectives_13.pdf; letöltés: 2021.04.20.
- DAYARAM, Sareena: China is buying most of the world's 5G phones, report finds. CNET, 2020.02.21. https://www.cnet.com/news/china-is-buying-most-of-the-worlds-5g-phones-report-finds/; letöltés: 2021.04.14.
- EU population in 2020: almost 448 million. Eurostat, 2020.07.10. https://ec.europa.eu/eurostat/documents/2995521/11081093/3-10072020-AP-EN.pdf/d2f799bf-4412-05cc-a357-7b49b93615f1; letöltés: 2021.04.27.
- FINKLEA, Kristin – CHRISTENSEN, Michelle D. – FISCHER, Eric A. – LAWRENCE, Susan V. – THEOHARY, Catherine A.: Cyber Intrusion into U.S. Office of Personnel Management: In Brief. Congressional Research Service, 2015.07.17. https://fas.org/sgp/crs/natsec/R44111.pdf; letöltés: 2021.04.21.
- Five Chinese Military Hackers Charged – Indicted in Connection with Cyber Espionage Offenses Against U.S. FBI, 2014.05.19. https://www.fbi.gov/news/stories/five-chinese-military-hackers-charged-with-cyber-espionage-against-us; letöltés: 2021.04.20.
- JIA, Cui: SMS returns to Xinjiang. China Daily, 2010.01.18. https://www.chinadaily.com.cn/china/2010-01/18/content_9332764.htm; letöltés: 2021.04.14.
- KANIA, Elsa B.: The Role of PLA Base 311 in Political Warfare against Taiwan (Part 3). Global Taiwan Brief, Volume 2, Issue 7, 2017.02.15. https://globaltaiwan.org/2017/02/15-gtb-2-7/#ElsaKania021517; letöltés: 2021.04.20.
- KANIA, Elsa; The PLA's Latest Strategic Thinking on the Three Warfares. The Jamestown Foundation, 2016.08.22. https://jamestown.org/program/the-plas-latest-strategic-thinking-on-the-three-warfares/; letöltés: 2021.04.20.
- KANNAN, Saikiran: Inside China's cyber war room: How PLA is plotting global attacks. India Today, 2020.08.06. https://www.indiatoday.in/world/story/inside-china-s-cyber-war-room-how-pla-is-plotting-global-attacks-1708292-2020-08-06; letöltés: 2021.04.20.
- KENYON, Miles: WeChat Surveillance Explained. The Citizen Lab, 2020.05.07. https://citizenlab.ca/2020/05/wechat-surveillance-explained/; letöltés: 2021.04.14.
- KOZŁOWSKI, Andrzej: The "Cyber Weapons Gap." The Assessment of the China's Cyber Warfare Capabilities and Its Consequences for Potential Conflict over Taiwan. University of Lodz. https://core.ac.uk/download/pdf/71981805.pdf; letöltés: 2021.04.20.
- LIU, Caiyu – FAN, Anqi: Local outbreak resurfaces in several Chinese cities as winter comes. Global Times, 2020.11.22. https://www.globaltimes.cn/content/1207677.shtml; letöltés: 2021.04.14.

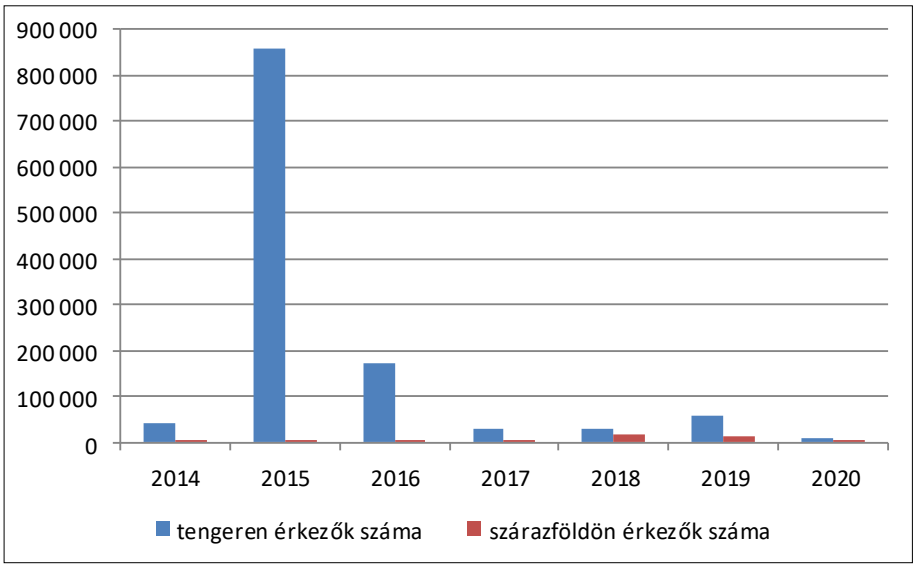
- McDonell, Stephen: Why China censors banned Winnie the Pooh. BBC News, 2017.07.17. https://www.bbc.com/news/blogs-china-blog-40627855; letöltés: 2021.04.14.
- Morgus, Robert – Fonseca, Brian – Green, Kieran: Are China and Russia on the Cyber Offensive in Latin America and the Caribbean? New America Cybersecurity Initiative, 2019.07.26. https://www.newamerica.org/cybersecurity-initiative/reports/russia-china-cyber-offensive-latam-caribbean/china-and-cyberspace/; letöltés: 2021.04.20.
- Ni, Adam – Gill, Bates: The People's Liberation Army Strategic Support Force: Update 2019. The Jamestown Foundation, 2019.05.29. https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/; letöltés: 2021.04.20.
- NIDS China Security Report 2021 – China's Military Strategy in the New Era. National Institute for Defense Studies, Japan, 2020. http://www.nids.mod.go.jp/publication/chinareport/pdf/china_report_EN_web_2021_A01.pdf; letöltés: 2021.04.20.
- Philippine President Duterte receives first dose of China's Sinopharm Covid-19 vaccine. South China Morning Post, 2021.05.04. https://www.scmp.com/video/asia/3132144/philippine-president-duterte-receives-first-dose-chinas-sinopharm-covid-19; letöltés: 2021.04.27.
- Pomerleau, Mark: 3 ways China's military could use cyber in war. Fifth Domain, 2019.01.16. https://www.fifthdomain.com/dod/2019/01/16/3-ways-chinas-military-could-use-cyber-in-war/; letöltés: 2021.04.20.
- Ranger, Steve: 5G smartphone sales in China are rocketing. That could be a big deal for the rest of the world. ZDNET, 2020.07.28. https://www.zdnet.com/article/5g-smartphone-sales-in-china-are-absolutely-rocketing/; letöltés: 2021.04.14.
- Robinson, Joe; Cyberwarfare statistics: A decade of geopolitical attacks. Privacy Affairs, 2021.02.25. https://www.privacyaffairs.com/geopolitical-attacks/; letöltés: 2021.04.20.
- Stokes, Mark A. – Lin, Jenny – Hsiao, Russell: The Chinese People's Liberation Army Signals Intelligence and Cyber Reconnaissance Infrastructure. Project 2049 Institute, 2011.11.11. https://project2049.net/wp-content/uploads/2018/05/pla_third_department_sigint_cyber_stokes_lin_hsiao.pdf; letöltés: 2021.04.20.
- Taiwan Fears China Could Cut Undersea Cables. Asia Sentinel, 2019.02.01. https://www.asiasentinel.com/p/taiwan-fears-china-cut-undersea-cables; letöltés: 2021.04.20.
- Vance, Ashlee: The People's Republic of The Future. Youtube, 2019.05.23. https://www.youtube.com/watch?v=taZJblMAuko; letöltés: 2021.04.14.

- VASWANI, Karishma: Is Alibaba's fate a warning to China’s tech giants? BBC News, 2021.04.15. https://www.bbc.com/news/business-56741551; letöltés: 2021.04.20.
- VENZON, Cliff: Duterte threatens to end US military pact if no vaccines. Nikkei Asia, 2020.12.27. https://asia.nikkei.com/Politics/International-relations/Duterte-threatens-to-end-US-military-pact-if-no-vaccines; letöltés: 2021.04.27.
- WANG, Junwei: China's 5G smartphone sales set to reach 140m units in 2020. China Daily, 2020.09.29. https://global.chinadaily.com.cn/a/202009/29/WS5f72ca36a31024ad0ba7c9ba.html; letöltés: 2021.04.14.
- WEISSBERGER, Alan: China tops 200M 5G subs while operators move to 5G SA. IEEE Communication Society, 2020.12.22. https://techblog.comsoc.org/2020/12/22/china-tops-200m-5g-subs-while-operators-move-to-5g-sa/; letöltés: 2021.04.14.
- WINGFIELD-HAYES, Rupert: China's Island Factory. BBC News, 2014.09.09. https://www.bbc.co.uk/news/resources/idt-1446c419-fc55-4a07-9527-a6199f5dc0e2; letöltés: 2021.04.27.
- YAMAGUCHI, Mari: Japan says Chinese military likely behind cyberattacks. Japan Today, 2021.04.21. https://japantoday.com/category/crime/japan-says-chinese-military-likely-behind-cyberattacks; letöltés: 2021.04.22.
- 中华人民共和国国防法. A Kínai Népköztársaság Honvédelmi törvénye. A Védelmi Minisztérium honlapja, 2020.12.27. http://www.mod.gov.cn/regulatory/2020-12/27/content_4876050.htm; letöltés: 2021.04.20.

FELEGYI JÚLIA

GÖRÖGORSZÁG MIGRÁCIÓS POLITIKÁJA

Görögország földrajzi elhelyezkedése miatt egyike az Európába irányuló illegális migrációnak leginkább kitett tranzitországoknak. A jellemzően Törökország irányából érkező ázsiai és afrikai bevándorlók a balkáni migrációs útvonalon itt léptek be az Európai Unió területére és haladtak tovább célországaik felé. Az elmúlt évtizedben több hullámban nagyszámú illegális bevándorló érkezett a görög szigetekre, ami jelentős gazdasági, humanitárius és biztonsági kihívások elé állította az amúgy is gyenge gazdasági lehetőségekkel bíró országot. A tavalyi évben egyrészt a pandémia miatt, másrészt a határozottabb védelmi intézkedések (lásd az évroszi eseményeket[1]) következtében csökkent a Görögországba érkező illegális migránsok száma, és a Törökországból induló migrációs útvonal inkább Ciprus felé tolódott el. Ugyanakkor fontosnak tartom megvizsgálni az eddig történteket, és a 2020-as év eseményei alapján néhány következtetést levonni.



1. ábra. A Görögországba érkezett illegális bevándorlók statisztikája[2]

[1] 2020. februárban Törökország elnöke bejelentette, hogy nem tartóztatja tovább az illegális migránsokat, így több ezer bevándorló próbált Görögország, és ezzel az EU területére jutni a tavaszi hónapokban, jellemzően az Évrosz határfolyó közelében.

[2] Mediterranean situation – Greece. UNHCR, Operational Portal, Refugee Situations. https://data2.unhcr.org/en/situations/mediterranean/location/5179; letöltés: 2021.01.25.

A migráció történeti előzménye és törvényi szabályozása

Görögország migrációs szabályozásának alapját az 1951-es genfi egyezmény és az Európai Uniós alapelvek képezik. Az 1990-es éveket megelőzően – Spanyolországhoz és Olaszországhoz hasonlóan – Görögország is inkább kibocsátó, mintsem célország volt. Az emigráció első hullámát az 1893-as gazdasági válság indította el: 1890–1920 között félmillió görög állampolgár keresett új életet jellemzően az Amerikai Egyesült Államokban és Egyiptomban.[3] 1950–1974 között a görög kivándorlók – egyes források szerint több mint egymillió fő – nagy része az Amerikai Egyesült Államokba, Kanadába és Ausztráliába, később pedig Nyugat-Európába távozott.[4] A Nyugat-Németországba történő kivándorlás 1974-et követően is jellemző maradt, ám kisebb mértékben.[5] Ezzel párhuzamosan visszatért mintegy 492 ezer görög állampolgár, köztük az 1946–49-es polgárháború amnesztiát kapott résztvevői is. Az 1970-es és az 1980-as években ugyan érkeztek menekültek a volt Szovjetunió és a balkáni államok területéről, ám számuk nem volt jelentős. Újabb kutatások alapján azonban elmondható, hogy 1973 körül már közel 40 ezer – jellemzően pakisztáni és egyiptomi – illegális bevándorló tartózkodott az ország területén.[6] 1986-ban viszont már 90 ezer külföldi tartózkodott az országban, bár harmaduk más európai államból származott, és ebbe a számba a legálisan és az illegálisan ott tartózkodók is beletartoztak. Az egy évvel későbbi népszámlálás szerint 165 ezer fő vallotta magát külföldinek az akkor 10,26 milliós országban.[7]

Az 1990-es évek elején a hirtelen drasztikusan emelkedő illegális migráció okai közt szerepel a kelet-közép-európai rendszerek átalakulása, ezek biztonságpolitikai folyamatai. Albánia, Jugoszlávia és a Szovjetunió összeomlása migrációt generáló tényező volt, amely Görögországot (is) célországgá tette. Ehhez hozzájárul, hogy bár az 1990-es évek Európájában Görögország a─legkevésbé fejlett országok közé tartozott, földrajzi elhelyezkedése miatt mégis ideérkezett az illegális migránsok nagy része. Már ebben az időszakban megfigyelhető volt, hogy a bevándorlók jelentős része az úgynevezett 3D[8] munkákat végezte. Az 1990 után érkezett bevándorlók döntő többsége illegálisan érkezett, és az 1998-as szabályozási program ellenére több mint felük nem kívánt sem munkavállalási, sem tartózkodási engedély iránti kérelmet benyújtani. Ennek oka egyrészt a legális kereseti lehetőségek csekély vonzereje (alacsony fizetés) volt, valamint az, hogy a többség csupán rövidebb, bizonytalan ideig kívánt az országban maradni.[9]

---

[3] KASIMIS, Charalambos: Greece, migration 1830s to present. In: Ness Immanuel (edit.): The Encyclopedia of Human Migration. Wiley-Blackwell, Chicester, United Kingdom, 2013. p. 1. https://www.researchgate.net/publication/236650301_Greece_migration_1830s_to_present; letöltés: 2021.01.28.

[4] LIANOS, Theodore P.: Report on immigration to Greece (Pilot Study). European Migration Network, Greek National Contact Point, Center for Planning and Economic Research, Athens, September 2004. pp. 6–7. https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/reports/docs/emn-studies/illegally-resident/gr-finalstudy_en.pdf; letöltés: 2021.01.03.

[5] 1975 és 1989 között mintegy 215 ezer fő.

[6] LIANOS, Theodore P.: Report on immigration to Greece (Pilot Study). p. 7.

[7] KASIMIS, Charalambos: Greece, migration 1830s to present. p. 2.

[8] Dirty, dangerous, demeaning – piszkos, veszélyes, megalázó.

[9] LIANOS, Theodore P.: Report on immigration to Greece (Pilot Study). p. 21.

A beutazási és a tartózkodási feltételeket 1991-ben az 1975-ös számú törvényben szabályozták először, amelyet 2001-ben a 2910. számú törvény követte.[10] Itt a fő fókusz a beutazás feltételeinek lefektetésén és a munkavállalási feltételek szabályozásán volt. Ez a tendencia folytatódott a 2005. évi 3386. számú törvénnyel, amely megkísérelte a hosszú távú ott-tartózkodás tisztázását, és hangsúlyt fektetett az integrációra is. A fentiek azonban csupán a törvényi háttér kialakításának kezdetét jelentették, így az érkező bevándorlók még számos jogi hiányosságba és ezáltal adminisztratív akadályokba ütköztek. A tapasztalatok tükrében 1997–2007 között négy szabályozási programot hajtottak végre a további joghézagok lefedésére. 1996-ban hozták az első, kifejezetten a menekültek védelmét szolgáló törvényt, amely a menekültügyi eljáráson kívül lehetőséget biztosított gyorsított eljárásra is, definiálta a megalapozatlan kérelmeket, valamint kitért a biztonságos harmadik ország fogalmára. A jogszabály figyelembe vette az EU ajánlásait is, és a 2000-es évek végén alkalmazkodott a 2003-as dublini rendelethez, a 2007-es befogadásról szóló irányelvhez, és a 2008-as eljárásokról és képesítésekről szóló irányelvekhez is. Ezt követően, 2010-ben a 3838-as törvény megkönnyítette az állampolgárság megszerzését a migránsoknak, valamint szavazati joggal is felruházta őket a helyközi választásokon.[11] A menekültügyi rendszert ért kritikák következtében a 2011. évi 3907-es törvény jelentős reformokat tartalmazott a menedékkérők fogadásával kapcsolatban. A 2005. évi 3386. számú Rendelkezési Törvényt követően az EU-direktívákat átültető módosítások – például a családegyesítés és a hosszú távú tartózkodási engedélyek helyzetét – a 2014. évi 4251-es törvény kodifikálta.[12]

A 2012-es év is változást hozott a migrációs folyamatokban. Görögország – a megnövekedett illegális migráció kezelése érdekében – mintegy 12 kilométer hosszúságban határkerítést épített a Törökországgal határos szárazföldi területein, az Évrosz folyó mentén. A négyméteres szögesdrót-kerítés megépítése több mint hárommillió euróba került, célja a török szárazföldről érkező migránsok EU-ba történő illegális átjutásának megakadályozása. A Kastanies és Nea Vyssa települések közti kerítés lezárta a gyalogos átjutási lehetőséget a két ország között, így átmenetileg más migrációs útvonalak erősödtek meg.[13]

A 2015-ös migrációs hullám nagyrészt Görögországon keresztül érkezett Európa területére. A görög szigeteken a migránsok jelentős többsége nem nyújtott be menedékkérelmet, hanem ahogy lehetőségük adódott, továbbutaztak a görög szárazföldre, majd a nyugat-balkáni útvonalon haladtak tovább célországaik felé. Az Európai Bizottság bírálta Görögországot a hiányos határellenőrzés miatt, valamint aggodalmát fejezte ki a dokumentumok ellenőrzésének és az ujjlenyomatvételek rendszeres elmulasztása miatt. Jóllehet a migránsok nagy része csak rövid ideig tartózkodott a szigeteken, a folyamatosan érkező nagy tömegek miatt azonban

[10] CECCORULLI, Michela: National Case Studies: Terms, definitions and concepts on migration. In: FASSI, Enrico and LUCARELLI, Sonia (edit.): The European Migration System and Global Justice. A First Appraisal. p. 117. https://core.ac.uk/download/pdf/85260111.pdf; letöltés: 2020.12.30.

[11] CECCORULLI, Michela: National Case Studies: Terms, definitions and concepts on migration. p. 120.

[12] CECCORULLI, Michela: National Case Studies: Terms, definitions and concepts on migration. pp. 117–118.

[13] Greece completes anti-migrant fence at Turkish border. ekathimerini-com, 2012.12.17. https://www.ekathimerini.com/147035/article/ekathimerini/news/greece-completes-anti-migrant-fence-at-turkish-border; letöltés: 2021.02.08.

elszállásolásuk így is jelentős kihívás elé állította a görög államot. Az Égei-tenger szigetein (Lészvosz, Híosz, Számosz, Lérosz és Kósz) öt uniós fogadóállomást (hotspotot) építettek a görög haderő bevonásával, elsőként a lészvoszit nyitva meg. A Frontex parti járőrözést indított Lészvosz, Híosz és Számosz közelében.[14]

2015 szeptembere és 2016 januárja között az ujjnyomatvételen átesett migránsok aránya 70 százalékponttal[15] emelkedett. A görögországi uniós fogadóállomások naponta összesen mintegy 11 ezer személy ujjnyomatának rögzítésére képesek, a Frontex pedig okmányszakértőket küldött a szigetekre a hamis okmányok azonosítása érdekében.[16] A súlyos anyagi problémákkal küzdő országnak az Európai Bizottság 192 millió eurós[17] pénzügyi segítséget nyújtott a migrációs válság kezelésére és a határvédelem erősítésére.[18] 2016-ban a 4375. számú törvény szabályozta a befogadási feltételek módosítását, amelyre az EU–Törökország megállapodás végrehajtása érdekében volt szükség.[19]

Kevés nyílt információ áll rendelkezésre az illegális migráció görög nemzeti biztonságra gyakorolt hatásáról. Egy tanulmány szerint már az 1990-es évek óta magasabb a külföldi származásúak által elkövetett bűncselekmények száma, mint a görög állampolgárok által elkövetetteké.[20] Alapvetően a kisebb súlyú, például lopással kapcsolatos bűncselekményekre kell elsősorban gondolnunk, összességében ez azonban a görög közbiztonság romlását jelentette. A 2015-ös migrációs hullám idején felmerült, hogy szélsőséges eszmékkel szimpatizálók, terroristák, súlyos bűncselekményeket elkövetők is érkezhettek a menekültek közé vegyülve. Ezt erősítette meg Hassan F. esete, akire a belga titkosszolgálat hívta fel a figyelmet 2018-ban. A görög Országos Hírszerző Szolgálat (EYP[21]) beazonosította az ISIL/DAESH[22] feltételezett aktivistáját, aki oltalmazotti státuszt is kapott, az európai társszervezetek azonban nem rendelkeztek terhelő információval róla, akit végül 2019-ben hazánkban tartóztattak le.[23] Az eset ugyan nem sikertörténet, de felhívja a figyelmet az érintett államok nemzetbiztonsági szolgálatainak többletfeladataira, és jól alátámasztja a szorosabb együttműködés és információmegosztás szükségességét.

---

[14] Az európai migrációs stratégia végrehajtása: a Bizottság jelentése a Görögországban, Olaszországban és a Nyugat-Balkánon elért eredményekről. Európai Bizottság, 2016.02.10. https://ec.europa.eu/commission/presscorner/detail/hu/IP_16_269; letöltés: 2021.02.17.

[15] 8%-ról 78%-ra.

[16] Az európai migrációs stratégia végrehajtása: a Bizottság jelentése a Görögországban, Olaszországban és a Nyugat-Balkánon elért eredményekről.

[17] Az EU a görögországi menekültek beilleszkedését és lakhatását elősegítő új humanitárius programot indít. Európai Bizottság, 2017.07.27. https://ec.europa.eu/commission/presscorner/detail/hu/IP_17_2121; letöltés: 2021.01.24.

[18] KOCSIS Máté: A görög migrációs válság és az EU-török együttműködés. biztonságpolitika.hu, 2020.04.19. https://biztonsagpolitika.hu/egyeb/a-gorog-migracios-valsag-es-az-eu-torok-egyuttmukodes; letöltés: 2020.12.22.

[19] CECCORULLI, Michela: National Case Studies: Terms, definitions and concepts on migration. pp. 117–118.

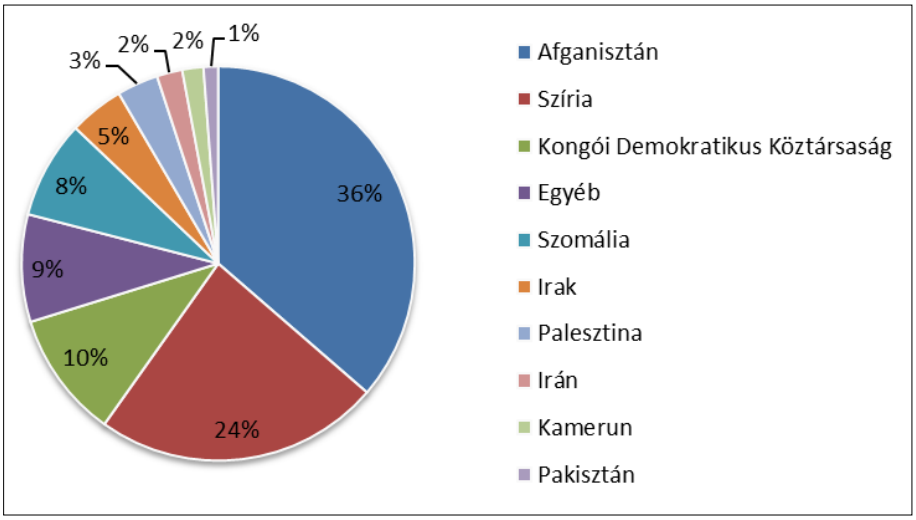
[20] LIANOS, Theodore P.: Report on immigration to Greece (Pilot Study). pp. 16–17.

[21] Ethniki Ypiresia Plirophorion.

[22] ISIL – Islamic State of Iraq and Levant, magyarul Iszlám Állam. DAESH – Dawlat al-Islamiyah f'al-Iraq wa al-Sham.

[23] Kommandósok hozták a bíróságra az Iszlám Állam tagját, elrendelték a letartóztatást. hvg.hu, 2019.03.24. https://hvg.hu/itthon/20190324_Kommandosok_hoztak_a_birosagra_az_Iszlam_Allam_tagjat_a_birosag_letartoztatta; letöltés: 2021.02.20.

2019 júliusában Kiriákosz Micotákiszt választották meg miniszterelnöknek, aki kampánya során szigorú, de igazságos reformokat ígért a migrációs politikával kapcsolatban. A menedékkérők részére hatékonyabb, a túlzsúfolt táborokat elkerülő rendszer kiépítésére tett ígéretet, ez azonban napjainkig nem valósult meg. 2019 második felében tovább emelkedett a görög szigetekre érkezők létszáma, ugyanakkor valóban számos intézkedés történt a migráció kontrollálása érdekében. Az első intézkedések közt szerepelt a menedékkérők társadalombiztosítási számának visszavonása, helyette ideiglenes rendszert dolgoztak ki. A migrációs politika 2019-es jellemzésekor több szakértő is arra hívta fel a figyelmet, hogy ugyan az állam csökkentette a migránsok és a menedékkérők jogait és jogosultságait, de ezzel párhuzamosan elmulasztotta az intézményi rendszer reformját, és az illegális migrációt csökkentő intézkedések kidolgozását.[24] A változások közé tartozott az is, hogy nyáron – az addig a migrációs ügyekért felelős minisztérium helyett – a befogadóközpontok felügyelete átkerült a polgári védelemért felelős minisztériumhoz. A kormány emellett bejelentette, hogy az Égei-tenger keleti részén található hotspotokat bezárják, és új, zárt fogvatartási központok létrehozását, valamint a szárazföldön működő nyílt menekülttáborok zárttá tételét tervezik.[25]



2. ábra. A 2020-ban Görögországba érkezett illegális migránsok etnikai megoszlása[26]

[24] HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands. Migration Policy Institute, 2020.09.25. https://www.migrationpolicy.org/article/greece-struggles-balance-competing-migration-demands; letöltés: 2020.12.27.

[25] STAMATOUKOU, Eleni: How the Greek policy on migration is changing. The European Data Journalism Network. 2019.12.27. https://www.europeandatajournalism.eu/eng/News/Data-news/How-the-Greek-policy-on-migration-is-changing; letöltés: 2021.02.13.

[26] Mediterranean situation – Greece. UNHCR, Operational Portal, Refugee Situations. https://data2.unhcr.org/en/situations/mediterranean/location/5179; letöltés: 2021.01.25.

A kormány prioritásai között szerepelt a hazatoloncolások hatékonyabbá tétele, ennek ellenére az előző években jellemző évenkénti 16 ezer repatriáláshoz képest 2019-ben csupán 9700 hazatoloncolás történt. 2019 őszén a görög parlament jóváhagyta a nemzetközi védelemről szóló törvényt, amely felgyorsította a menekültügyi eljárásokat, mivel 20 napban maximalizálva annak lefutási idejét. A kormány e döntését emberjogi szervezetek azzal támadták, hogy így nehezítik az eljárásban részt vevők számára a jogi segítségnyújtás lehetőségét. Olyan esetről is beszámolt a Migrationpolicy hírportál, hogy novemberben 28 szubszaharai migráns kérelmét azért utasították el, mert azok nem válaszoltak a feltett kérdésekre, amikor tolmács nem volt jelen.[27]

2020

2020-ban több, a migrációs helyzetet jelentősen befolyásoló esemény történt. Január 22-én közel 10 ezer lakos tüntetett Lészvosz szigetén az illegális migráció hatékonyabb kezeléséért, és követelték, hogy a szigeteken elszállásolt migránsokat szállítsák el. Két héttel később a Moria tábor lakói is demonstráltak a jobb életkörülményekért és a gyorsabb menekültügyi eljárásért. A kormány zárt menekültügyi központok építésének terveivel reagált, ez azonban kiváltotta a helyi lakosság éles tiltakozását, akik a hatóságokkal is összecsaptak az építkezések megakadályozása érdekében.[28]

Micotákisz miniszterelnök februárban 220 fővel emelte a bevándorlási hivatal munkatársainak létszámát, hogy az ügyhátralék csökkenthető legyen. Ezzel egy időben megállapodást írt alá az Európai Menekültügyi Támogatási Hivatallal,[29] így az több mint 1000 fővel megduplázta jelenlétét az országban. Ez azért is volt indokolt, mert míg 2019 szeptemberében a feldolgozatlan kérelmek száma 72 ezer volt, a számuk 2020 februárjára 97 ezerre nőt. Az említett időszak alatt a szigetek tehermentesítése céljából közel 30 ezer menedékkérőt szállítottak a szárazföldre, ám ennek majdnem a kétszerese, 55 ezer újabb bevándorló érkezett. A szigeteken található hotspotok befogadóképességét ezért 17 ezerről 40 ezerre emelték.[30]

Február 29-én Recep Tayyip Erdoğan, Törökország elnöke bejelentette, hogy nem tartóztatja tovább az Európai Unió irányába induló migránsokat. Ez az intézkedés leginkább Görögországot érintette, hiszen több tízezer migráns próbált átjutni a török–görög szárazföldi és tengeri határokon.[31] Csak március elsején 736 fő migráns érkezett vízi úton a görög szigetekhez. Athén Ankarát vádolta a szervezett migrációs nyomás miatt, ezzel egy időben pedig – a Frontex erőinek segítségével – igyekezett a tömeges határáttörési kísérleteket megakadályozni a szárazföldi határainál. Az összecsapásokról mindkét ország és a civil szervezetek is másként számoltak be. Törökország szerint több migráns is életét vesztette, de ezt

[27] HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands.
[28] Uo.
[29] European Asylum Support Office – EASO.
[30] HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands.
[31] KOCSIS Máté: A görög migrációs válság és az EU-török együttműködés.

Görögország tagadta.[32] A görög titkosszolgálat tevékenysége ebben az időszakban is hasznos volt, többek között az ő információira is támaszkodtak az érkezésekkel kapcsolatban. Az Évrosz határfolyó mentén felgyűlt több ezer illegális migráns naponta próbált átjutni görög területre, így a határvédelmi erők megkezdték a terület megerősítését. A konfliktuszónába látogatott többek közt Ursula von der Leyen, az Európai Bizottság elnöke is, aki Görögországot Európa pajzsának nevezte, és támogatásáról biztosította az államot.[33]

Márciustól a kormány egy hónapra szűkítette az integrációt támogató ESTIA-programot,[34] amely többek között mintegy 20 ezer migráns számára bérelt apartmanokat. A júniusban indult HELIOS átmeneti segélyprogram ezzel szemben csupán 8000 személynek biztosított segítséget, így a civil szervezetek több ezer utcára került migráns család miatt bírálták az intézkedéseket.[35] Az UNHCR adatai alapján nem számottevő a menekültek munkaerőpiaci integrációja, amelyet részben a nyelvtudás hiánya, részben a szükséges engedélyek megszerzésének nehézségei indokolnak.[36] Az oktatásban is jelentős visszaesés mutatkozott: 2019 és 2020 áprilisa között a menekült gyermekek száma 29 ezerről 45 ezer főre nőtt, ám az oktatásban részt vevők száma 11 500 főről csupán 13 000 főre emelkedett. Ez a gyakorlatban azt jelenti, hogy a szárazföldön tartózkodó gyermekek 61%-a, míg a szigeteken lévőknek csupán 6%-a iratkozott csak be az iskolába. Természetesen a szigeteken jelen lévő civil szervezetek is folytatnak képzéseket, ám ők is csak a gyermekek 28%-át érték el.[37]

Az évroszi konfliktussal egy időben az EU a pénzügyi segítségen kívül azzal is támogatni próbálta Görögországot, hogy a görög szigeteken tartózkodó minden migránsnak felajánlott 2000 eurót, ha önként hazatér a származási országába. A felajánlással azonban – vélhetően részben a koronavírus-helyzet eszkalálódása miatt is – a vártnál jóval kevesebben éltek.[38] A kormány 2020. április 14-én elfogadta a 3063-as törvényt, amely a menekültügy, a migráció és a társadalmi integráció területén működő görög és külföldi NGO-k nyilvántartásának és működésének szabályait szigorította. Lényeges, hogy az új rendeleteket a görögországi menekültügyi és migrációs törvények legutóbbi, 2019 novemberében és 2020 májusában elfogadott reformjaival összefüggésben hajtották végre, amelyek jelentősen korlátozták a menedékkérők és a migránsok jogait, valamint korlátozásokat vezettek be a nem kormányzati szervezetekre is, többek között a regisztrációs

[32] HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands.
[33] Uo.
[34] ESTIA – Emergency Support to Integration and Accommodation – Segítség az integrációban és az ellátásban.
[35] HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands.
[36] Míg 2019-ben a menekültek és a menedékkérők 95%-a rendelkezett társadalombiztosítási számmal, ez 2020 nyarára 66%-ra csökkent, a vizsgált időszakban az adószámmal rendelkezők aránya pedig 68%-ról 57%-ra esett vissza.
[37] HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands.
[38] EU to give migrants in Greece 2000 euro to go home. BBC News, 2020.03.12. https://www.bbc.com/news/world-europe-51859007; letöltés: 2021.02.19.

követelmények tekintetében.[39] Az év elején indult az új, 4636/2019-es számú menekültügyi törvény elfogadtatási folyamata, amelyet a parlament végül májusban fogadott el. A törvényt számos kritika érte a civil szervezetek részéről, bírálták a menekültügyi őrizet intézményét, valamint a kormány elrettentésre és az önkéntes hazatérések növelésének céljára irányuló erőfeszítéseit is.[40]

Athén az égei-tengeri szigetek felé tartó migránsok feltartóztatására egyedi ötlettel állt elő: úszó kerítés megvalósítására írtak ki pályázatot január végén. A 2,7 kilométer hosszú, 1,1 méteres úszó akadály kiépítése júliusban kezdődött, és közel félmillió euróba került.[41] Szeptember 9-én a Moria tábor kigyulladt, aminek következtében több mint 13 ezer migráns maradt fedél nélkül. A szándékos gyújtogatókat a hatóság előállította. A tábor lakói a tűzesetet követően több tüntetést is szerveztek azt követelve, hogy engedjék őket útjukra Európa felé. Az esettel kapcsolatban egy német tartomány felajánlotta, hogy befogad ezer migránst, valamint tárgybeli és anyagi felajánlások is érkeztek a tagországoktól.[42]

2020-ban ezernél is több menedékkérőt telepítettek át más uniós országokba, többek közt Belgiumba, Finnországba, Németországba, Franciaországba, Írországba, Luxemburgba és Portugáliába. A Moria tábor leégését követően majdnem ugyanennyi kísérő nélküli kiskorút vállaltak még át a tagországok, az átszállításuk nagy része meg is valósult még 2020-ban.[43]

A nyár folyamán számos kritika érte mind a görög parti őrséget, mind a Frontex munkatársait, hogy erőszakkal kényszerítik vissza török felségvizekre a csónakokkal érkező migránsokat, működésképtelenné teszik vízi járműveiket, így azok csak a török parti őrség segítségében bízhatnak.[44] A média hatására a Frontex belső vizsgálatot indított, ám az nem tárt fel terhelő bizonyítékokat.[45] 2021 januárjában két szervezet, a Front-Lex és a Legal Centre Lesvos egy 34 oldalas vádiratot tett közzé, amelyben felszólítják a Frontexet, hogy hagyjon fel jogsértő műveleteikkel és szüntesse be tevékenységét az Égei-tenger körzetében.[46]

---

[39] Greece: Regulation of NGOs working on migration and asylum threatens civic space. reliefweb, 2020.08.02. https://reliefweb.int/report/greece/greece-regulation-ngos-working-migration-and-asylum-threatens-civic-space; letöltés: 2021.02.08.

[40] STAMATOUKOU, Eleni: How the Greek policy on migration is changing.

[41] Greece to deploy floating barrier in Aegean to block migrants. Daily Sabah, 2020.07.01. https://www.dailysabah.com/politics/greece-to-deploy-floating-barrier-in-aegean-to-block-migrants/news; letöltés: 2021.02.15.

[42] Moria migrants: Fire destroys Greek camp leaving 13,000 without shelter. BBC News, 2020.09.09. https://www.bbc.com/news/world-europe-54082201; letöltés: 2021.02.18.

[43] Over 1,000 migrants relocated from Greece in 2020. InfoMigrants, 2020.10.02. https://www.infomigrants.net/en/post/27697/over-1-000-migrants-relocated-from-greece-in-2020; letöltés: 2021.02.15.

[44] KINGSLEY, PATRICK – SHOUMALI, Karam: Taking Hard Line, Greece Turns Back Migrants by Abandoning Them at Sea. The New York Times, 2020.08.14. https://www.nytimes.com/2020/08/14/world/europe/greece-migrants-abandoning-sea.html; letöltés: 2020.12.28.

[45] HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands.

[46] DOBOZI Gergely: Jogvédők kritizálják a Frontexet. Mandiner, 2021.02.17. https://precedens.mandiner.hu/cikk/20210217_ngo_frontex_csoportos_kiutasitas_migracio_jogellenes; letöltés: 2021.02.19.

Mihalisz Krohidisz, a polgárvédelmi miniszter szerint Görögország számára 2021 a biztonság éve lesz, a koronavírus elleni vakcinákra és az épülő görög határkerítésre utalva ezzel. A tavalyi év során kezdődött a török–görög határkerítés megerősítése, amelyről január elején már képeket is publikáltak. A 27 kilométer hosszú, 4,3 méter magas kerítésszakasz megépítése 62,9 millió euró, ennek során nyolc katonai megfigyelőpontot is kiépítenek.[47]

Az Európai Unió és Törökország együttműködése

Az ENSZ Menekültügyi Főbiztosságának adatai szerint Törökországban kb. négymillió migráns tartózkodik, közülük 3,6 millió Szíriából érkezett. Ez a tömeg megfelelő alkupozíciót jelent Erdoğan elnök számára, amikor Brüsszellel tárgyal.

Az EU és Törökország 2015 októberében megállapodást írt alá, amely alapján az Európai Unió rendszeres pénzbeli támogatást biztosít a Törökországban élő szíriai menekültek helyzetének javítására – összesen 6 milliárd euró értékben –, Ankara viszonzásul keményebben fellép az embercsempészek ellen, és szorosabban együttműködik a görög és a bolgár hatóságokkal az illegális migráció visszaszorítása érdekében. 2016 tavaszán az EU és Törökország aláírta azt a nyilatkozatot is, amely szerint a görög szigetekre Törökországból illegálisan belépő, illetve nemzetközi védelemre nem jogosult migránst Ankarának vissza kell fogadnia, továbbá minden visszaküldött szíriai migráns után egy másik szíriait telepítenének át Törökországból az Európai Unió területére. A felek rögzítették a törökök kötelezettségvállalását az újabb szárazföldi és vízi migrációs útvonalak megnyílásának megakadályozására, az EU pedig ígéretet tett a pénzügyi támogatás gyorsabb folyósítására. A nyilatkozat gyenge pontja azonban annak kötelező érvényének hiánya volt, végrehajtása csupán kölcsönös bizalmi elven alapult. Ezen kívül a nyilatkozat említette a török csatlakozási tárgyalások felgyorsítását az EU-val, tárgyalásokat vámunió létrehozásáról, illetve a vízumkötelezettség eltörlésének végrehajtását, ám érdemleges előrelépés e területeken eddig nem történt.[48]

Törökország az egyezség megkötése óta többször fenyegetőzött annak felbontásával, a migránsok szabad átengedésével, jellemzően az EU-hoz fűződő elhidegülő viszonya következtében, de a határ megnyitására nem került sor. A bejelentés gyorsan terjedt a Törökországban tartózkodó több millió migráns közt, és több ezren indultak el a görög–török szárazföldi határ felé szervezett buszjáratokkal is. A görög hatóságok azonnal lezárták a Pazurkale közelében fekvő átkelőket, és a kormány bejelentette, hogy felfüggesztik a menedékkérelmek benyújtásának lehetőségét. Fizikai konfliktus alakult ki a migránsok, a görög határvédelmi erők és a migránsokat segítő török haderő között is. Márciusban végül a pandémia oldotta meg ideiglenesen a helyzetet, és a török haderő a migránsok egy részét visszaszállította ázsiai török területekre.[49]

[47] Construction of Evros border fence to be completed within months. Greek City Times, 2020.12.30. https://greekcitytimes.com/2020/12/30/evros-border-to-be-completed-soon/; letöltés: 2021.02.20.
[48] KOCSIS Máté. A görög migrációs válság és az EU-török együttműködés.
[49] Uo.

Nemzetközi szervezetek és nem kormányzati szervezetek (NGO-k) jelenléte és tevékenysége

Az ENSZ Menekültügyi Főbiztossága (UNHCR[50]) 1952 óta van jelen az országban, de a 2015-ös eseményekig a szervezet jellemzően csak jogsegéllyel foglalkozott. A 2015-ös menekülthullámot követően azonban prioritásai között szerepelt a helyzetelemzés és a jogi segítségnyújtás a görög kormány részére.[51]

Több, jelentősebb EU-valamint tagországi finanszírozású program is segítette a migrációs helyzet kezelését. Ezek közül kiemelném a már említett ESTIA-programot, amelyet 2017. július 27-én indítottak. A finanszírozás az EU 192 millió eurós úgynevezett szükséghelyzeti támogatási eszközök keretében 2016-ban nyújtott támogatást egészíti ki, amely így összesen 401 millió eurót tett ki. Az Európai Unió 2020-ig összesen 1,3 milliárd eurót meghaladó összegű támogatást nyújtott a görög kormánynak a migrációs és a határigazgatási kihívások koordinálására. Az ESTIA program 151 millió eurós költségvetéssel rendelkezett, amely az alábbiak szerint oszlott meg.

1. Lakásbérlés közel 30 ezer fő részére. Az ESTIA keretében az UNHCR segítségével 93,5 millió euró értékben 22 ezer városi szálláshelyet biztosítottak a menekültek életkörülményeinek javítása érdekében. 2017 végére közel 30 ezer főnek béreltek lakásokat Görögországban.

2. Készpénztámogatás a menekültek részére. Az 57,6 millió eurós keretből havonta juttattak készpénzt a menedékkérőknek és a menekülteknek egy új kártyarendszer alkalmazásával. A támogatás célja a kérelmezők emberi méltóságának megőrzése volt, és ebből a fejenként 90 vagy 150 eurós összegből[52] alapvető szükségleteiket[53] tudták fedezni. A program ezzel egyúttal a helyi kisvállalkozások fellendítését is célozta, hiszen azt feltételezte, hogy a rászorulók helyben költik el az összeget.[54] A 2019. márciusi adatok szerint közel 69 ezer ilyen kártya volt használatban. A szállásokhoz hasonlóan ezt is a menekültstátusz megállapítását követő hat hónapig biztosították.[55]

3. A fennmaradó keretet pedig olyan NGO[56]-k közt osztják meg, amelyek szállások és az egészségügyi alapellátás biztosítására, oktatásra vagy mentálhigiénés támogatásra használnák azt.[57]

---

[50] UNHCR – United Nations High Commissioner for Refugees.

[51] Görögországi migrációs helyzetkép. A Migrációkutató Intézet terepkutatása, 2019. április 9-11. Útibeszámoló. p. 1. https://www.migraciokutato.hu/wp-content/uploads/2019/05/G%C3%B6r%C3%B6g-%C3%BAtibesz%C3%A1mol%C3%B3_MKI_20190516.pdf; letöltés: 2021.01.14.

[52] Az összeget az étkezést nem biztosító, vagy étkezést is magában foglaló ellátórendszertől függően határozták meg.

[53] Például élelmiszerek, gyógyszerek, tömegközlekedés finanszírozása.

[54] Az EU a görögországi menekültek beilleszkedését és lakhatását elősegítő új humanitárius programot indít.

[55] Görögországi migrációs helyzetkép. A Migrációkutató Intézet terepkutatása, 2019. április 9-11. p. 1.

[56] NGO – Non-Governmental Organization, vagyis nem kormányzati szervezet.

[57] Az EU a görögországi menekültek beilleszkedését és lakhatását elősegítő új humanitárius programot indít.

Ezen felül az Európai Bizottság extrém helyzetek esetére – például migránsok tömeges Európába áramlásakor – a szükséghelyzeti támogatási eszköz révén humanitárius segítségnyújtásként 2018-ig 700 millió euró összegig terjedő uniós támogatást különített el. Az összeg partnerszervezetek által elérhető, például az ENSZ, a Vöröskereszt és az NGO-k ügynökségei segítségével.[58]

A Menekültügyi, Migrációs és Integrációs Alap, a Belső Biztonsági Alap, a leginkább rászoruló menekülteket támogató Európai Segítségnyújtási Alap és az EU egészségügyi programja már eddig is jelentős pénzügyi forrásokat biztosított Görögország számára. Szót kell ejteni még az uniós polgári védelmi mechanizmusban részt vevő államoknak az anyagi segítségnyújtásra vonatkozó felajánlásairól, amelyek keretében 2015-ben 15 ország ajándékozott a görög táboroknak sátrakat, hálózsákokat, ágyfelszerelést, fűtő- és világítóberendezéseket, valamint generátorokat.[59]

Az NGO-k szerepe sokat vitatott. Számos szervezet a tengeren utazó illegális migránsok „mentésére" szakosodott, amely több kutatás szerint is migrációt erősítő tényező. Jelen publikációnak nem célja azt vizsgálni, hogy a fenti csoportba tartozó szervezetek ténylegesen menekülteket vagy illegális migránsokat mentenek-e, ki van valóban életveszélyben, és összejátszanak-e az embercsempészekkel. Az NGO-k más csoportja továbbképzéssel, alapvető szükségletek támogatásával foglalkozik, és jelentős szerepet kapnak a kialakult helyzet kezelésében.

Az első példa a számosz-szigeti Vathy településen található, ez a Samos Volunteers[60] által üzemeltetett Alpha Center. A központnak saját honlapja is van, ahol várják az önkéntesek jelentkezését, akik a helyszínen nyelveket oktatnak, és olyan hasznos szabadidős elfoglaltságot nyújtanak, mint hangszeres oktatás, sportfoglalkozások, mentálhigiénés tanácsadás. A központot igénybe vevők nagy része muszlim, így szombatonként csak nőknek tartanak tanfolyamokat. A foglalkozásokon kívül a migránsok társasjátékozhatnak, fénymásolhatnak, segítséget kérhetnek hivatalos ügyek intézésében, ezért a létesítmény népszerű és szinte mindig teltházas. A szervezet számos másik NGO-val együttműködik, 2016 óta szakosodott az alapvető ellátások helyett a képzések biztosítására.[61]

Az Aegean Boats Report[62] szervezetet a norvég Tommy Olsen alapította azzal a céllal, hogy segítséget nyújtson a görög szigetekre érkező migránsoknak. A szervezet célja, hogy részletesebben tájékoztasson az égei-tengeri migrációs helyzetről, mint azt a kormányzat és az UNHCR teszi. Honlapján nyilvántartás található a már partot ért és a visszafordított vízi járművekről is, ezekről heti, havi és éves jelentéseket tesz elérhetővé.[63] A görög kormány megvádolta a szervezetet,

[58] Az európai migrációs stratégia végrehajtása: a Bizottság jelentése a Görögországban, Olaszországban és a Nyugat-Balkánon elért eredményekről.
[59] Uo.
[60] Számoszi Önkéntesek.
[61] Samos Volunteers. https://www.samosvolunteers.org/; letöltés: 2021.01.25.
[62] Jelentés az égei-tengeri hajókról.
[63] Aegean Boat Report. https://aegeanboatreport.com/; letöltés: 2021.02.06.

hogy az segíti a szomáliai illegális migránsokat, akikből az elmúlt hónapokban egyre többen érkeznek a görög szigetekre.[64]

A fenti példákon kívül a nagyobb szervezetek közül a Hellén Vöröskereszt, az Orvosok Határok Nélkül, és az SOS Gyermekfalu is jelen van az országban. A migránsok számos görög helyre is fordulhatnak segítségért, például az ARSIS-hoz,[65] a Görög Tanács a Menekültekért szervezethez, a The Orange House pedig a fent említett Alpha Centerhez hasonló elven működik, csak itt még az LGBTI-csoporthoz[66] tartozókat is kiemelten kezelik. A fentieken kívül sok, kifejezetten kiskorú menekültekre szakosodott alapítványt is találhatunk. Természetesen a vallási szervezetek is jelen vannak, közülük az Apostoli alapítvány, a görög Karitász és az Ökomenikus Menekültprogram a legjelentősebbek. A görög kormány az ilyen szervezeteket az átláthatóság és a hatékony segítség érdekében egy honlapon[67] tartja nyilván, ahol a rászoruló menekültek könnyen eligazodhatnak.[68]

A görögországi befogadóközpontok koronavírus-helyzete

Az országban 2020. február 26-án regisztrálták az első hivatalos koronavírus-fertőzöttet. Ezt követően utazási korlátozásokat léptettek életbe és lezárták a határokat, így a gyors intézkedéseknek köszönhetően (a nyáron újraindult turizmusig) viszonylag alacsony maradt a fertőzöttség. Szeptember elején kevesebb, mint 12 ezer fertőzést mutattak ki a hatóságok.[69] Nemzetközi segélyszervezetek és orvosok is figyelmeztettek a járvány veszélyeire a túlzsúfolt görög menekülttáborokban, és talán ennek is köszönhető, hogy súlyosabb fertőzéshullám nélkül zajlott le a pandémia a táborokban. A ritsonai és a malakasai táborban találtak fertőzötteket, de tömeges járványhullám nélkül sikerült izolálni a kiszűrt koronavírusos lakókat.[70]

Következtetések, konklúzió

A turizmus jelentős visszaesése több okra is visszavezethető. A pandémiás helyzeten kívül tavaly februárban és márciusban a nagyszámú migráns jelenléte, de a még feszültebbé vált török–görög politikai viszony miatt az egyébként jelentős török nyaralóközönség sem jelent meg Görögországban. Tovább súlyosbítja a problémát, hogy a migránsok a turizmus elriasztásán és a humanitárius igények kielégítésén kívül is többletköltséget jelentenek a szigeteknek. Jorgosz Karamanisz, Híosz alpolgármestere szerint egy migráns átlagosan nyolc kilogramm szemetet hagy hátra érkezéskor (mentőmellények, mentőcsónak, vizes ruhák, palackok), amelyek rendszeres elszállítása

---

64 NGO in Greece reacts to migrant trafficking accusations. InfoMigrants, 2020.12.11. https://www.infomigrants.net/en/post/29045/ngo-in-greece-reacts-to-migrant-trafficking-accusations; letöltés: 2021.02.06.

65 Association for the Social Support of Youth – Egyesület a fiatalság szociális támogatásáért.

66 LGBTI – Lesbian, Gay, Bisexual, Transgender, Intersexed.

67 Study in Greece – Refugees. https://refugees.studyingreece.edu.gr/; letöltés: 2021.02.09.

68 Contact information - NGOs helping refugees and migrants in Greece. May 2019. https://griechenland.diplo.de/blob/1338134/c36b39f79f40d5a56452021d2f510ad2/merkblatt-hilfsorganisationen-hilfe-fuer-fluechtlinge-in-griechenland-en-data.pdf; letöltés: 2021.02.09.

69 HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands.

70 KOCSIS Máté: A görög migrációs válság és az EU-török együttműködés.

nélkül a turizmusból élő szigetek jelentős anyagi hátrányt szenvednek.[71] Több, migrációs krízisben érintett görög sziget polgármestere is felismerte, hogy az illegális migráció megfékezésére nem megoldás a menekülttáborok kiépítése, helyette a kibocsátó országok rekonstrukciója lenne a célravezető.[72]

A nemzetbiztonsági kockázatot, valamint az integrációs kísérletek kudarcának esélyét növeli, hogy a szigeteken – az európai átvállalások ellenére – még mindig magas a kiskorúak száma, akik éveket töltenek, töltöttek ott, és nagy részük nem vett részt oktatásban. Ez kilátástalan, vesztenivaló nélküli generációt szül, amely melegágya lehet a vallási szélsőségeknek. Egy részüket elszállították vagy elszöktek más európai országokba, ami a többi országnak – köztük Magyarországnak mint alternatív tranzitországnak – is komoly kockázatokat jelent.

Az EU 2000 eurós felajánlása – hogy a görög szigetekről a bevándorlók hazatérjenek – nem rossz kezdeményezés, érdemes azonban megvizsgálni, kik éltek ezzel a lehetőséggel, ők honnan származtak, és felmérni azt is, hogy akik nem éltek vele, miért döntöttek így. A válaszok elemzése alapján lehetne kidolgozni további intézkedéseket. Ugyanakkor természetesen ez nem oldja meg a kibocsátó országok problémáit, ahogy a *push* faktorok sem fognak csökkenni ettől, ám véleményem szerint a tüneti kezeléseket is mind figyelembe kell vennünk.

A 2020. februárban kezdődött évroszi konfliktus esetében szomorú tény, hogy mind a török, mind a görög fél ferdített és valótlan dolgokat állított/tagadott a krízissel és a migránsok tengeren való kezelésével kapcsolatban, így a bevándorlók ismét a politika eszközévé váltak. Ez egyben ismét felhívta a figyelmet Törökország migrációs folyamatokkal kapcsolatos jelentős szerepére is. Erdoğan elnök kezében a közel hárommillió szíriai menekült olyan tényező, amelyet komolyan kell vennie Európának.

Az NGO-knak a kérdéskörben játszott szerepe nem fekete vagy fehér. Igenis vannak szükséges és hasznos szervezetek, tudni kell azonban megkülönböztetni őket a migrációból és az emberek nyomorából politikai és/vagy gazdasági hasznot húzó társaságoktól, és természetesen ők sem jelentenek megoldást a migrációs válságra. Sajnos még az alapvetően pozitív szerepet betöltő szervezetek esetében is sokszor politikai folyamatok és célok is megjelenhetnek a háttérben, illetve az eredeti, valós segítő szándék idővel torzulhat.

Bár jelenleg a pandémiás helyzet, valamint a népszerűbbé vált spanyolországi és olaszországi útvonalak miatt Görögország tekintetében nem beszélhetünk migrációs válságról, Athénnak mégis számos megoldatlan problémával kell szembenéznie. Értékelésem szerint a 2020-as évből rengeteget tanult az ország, de még jobban fel kell készülnie egy esetleges, az évroszi eseményekre hasonlító tömeges áttörési kísérlet kezelésére. Az országnak hatékonyabb megoldást kell kidolgoznia mind a tengeren érkező illegális migránsok távoltartására, mind a már táborokban tartózkodók ellátására. A fentieket az EU migrációs alapelveivel, az alapvető emberi jogokkal és a lakosság érdekeivel összeegyeztetni – a meglehetősen szűkös anyagi lehetőségekkel és politikával átszőve – egy igazán komplex kihívás.

[71] Görögországi migrációs helyzetkép. A Migrációkutató Intézet terepkutatása, 2019. április 9-11. p. 5.
[72] Görögországi migrációs helyzetkép. A Migrációkutató Intézet terepkutatása, 2019. április 9-11. p. 7.

FELHASZNÁLT IRODALOM

- Aegean Boat Report.
  https://aegeanboatreport.com/; letöltés: 2021.02.06.
- Az EU a görögországi menekültek beilleszkedését és lakhatását elősegítő új humanitárius programot indít. Európai Bizottság, 2017.07.27.
  https://ec.europa.eu/commission/presscorner/detail/hu/IP_17_2121; letöltés: 2021.01.24.
- Az európai migrációs stratégia végrehajtása: a Bizottság jelentése a Görögországban, Olaszországban és a Nyugat-Balkánon elért eredményekről.
  Európai Bizottság, 2016.02.10.
  https://ec.europa.eu/commission/presscorner/detail/hu/IP_16_269; letöltés: 2021.02.17.
- CECCORULLI, Michela: National Case Studies: Terms, definitions and concepts on migration. In: FASSI, Enrico and LUCARELLI, Sonia (edit.):
  The European Migration System and Global Justice. A First Appraisal. pp. 87–138.
  https://core.ac.uk/download/pdf/85260111.pdf; letöltés: 2020.12.30.
- Construction of Evros border fence to be completed within months.
  Greek City Times, 2020.12.30.
  https://greekcitytimes.com/2020/12/30/evros-border-to-be-completed-soon/;
  letöltés: 2021.02.20.
- Contact information - NGOs helping refugees and migrants in Greece. May 2019.
  https://griechenland.diplo.de/blob/1338134/c36b39f79f40d5a56452021d2f510ad2/merkblatt-hilfsorganisationen-hilfe-fuer-fluechtlinge-in-griechenland-en-data.pdf; letöltés: 2021.02.09.
- DOBOZI Gergely: Jogvédők kritizálják a Frontexet. Mandiner, 2021.02.17.
  https://precedens.mandiner.hu/cikk/20210217_ngo_frontex_csoportos_kiutasitas_migracio_jogellenes; letöltés: 2021.02.19.
- EU to give migrants in Greece 2000 euro to go home. BBC News, 2020.03.12.
  https://www.bbc.com/news/world-europe-51859007; letöltés: 2021.02.19.
- Görögországi migrációs helyzetkép.
  A Migrációkutató Intézet terepkutatása, 2019. április 9-11. Útibeszámoló.
  https://www.migraciokutato.hu/wp-content/uploads/2019/05/G%C3%B6r%C3%B6g-%C3%BAtibesz%C3%A1mol%C3%B3_MKI_20190516.pdf; letöltés: 2021.01.14.
- Greece completes anti-migrant fence at Turkish border.
  ekathimerini-com, 2012.12.17.
  https://www.ekathimerini.com/147035/article/ekathimerini/news/greece-completes-anti-migrant-fence-at-turkish-border; letöltés: 2021.02.08.
- Greece to deploy floating barrier in Aegean to block migrants.
  Daily Sabah, 2020.07.01.
  https://www.dailysabah.com/politics/greece-to-deploy-floating-barrier-in-aegean-to-block-migrants/news; letöltés: 2021.02.15.
- Greece: Regulation of NGOs working on migration and asylum threatens civic space.
  eliefweb, 2020.08.02.
  https://reliefweb.int/report/greece/greece-regulation-ngos-working-migration-and-asylum-threatens-civic-space; letöltés: 2021.02.08.
- HERNÁNDEZ, Joel: Greece Struggles to Balance Competing Migration Demands.
  Migration Policy Institute, 2020.09.25.
  https://www.migrationpolicy.org/article/greece-struggles-balance-competing-migration-demands; letöltés: 2020.12.27.

- KASIMIS, Charalambos: Greece, migration 1830s to present.
  In: Ness Immanuel (edit.): The Encyclopedia of Human Migration.
  Wiley-Blackwell, Chicester, United Kingdom, 2013.
  https://www.researchgate.net/publication/236650301_Greece_migration_1830s_to_present;
  letöltés: 2021.01.28.
- KINGSLEY, PATRICK – SHOUMALI, Karam:
  Taking Hard Line, Greece Turns Back Migrants by Abandoning Them at Sea.
  The New York Times, 2020.08.14.
  https://www.nytimes.com/2020/08/14/world/europe/greece-migrants-abandoning-sea.html;
  letöltés: 2020.12.28.
- KOCSIS Máté: A görög migrációs válság és az EU-török együttműködés.
  biztonságpolitika.hu, 2020.04.19.
  https://biztonsagpolitika.hu/egyeb/a-gorog-migracios-valsag-es-az-eu-torok-egyuttmukodes**;**
  letöltés: 2020.12.22.
- Kommandósok hozták a bíróságra az Iszlám Állam tagját, elrendelték a letartóztatást.
  hvg.hu, 2019.03.24.
  https://hvg.hu/itthon/20190324_Kommandosok_hoztak_a_birosagra_az_Iszlam_Allam_tagjat_a_birosag_letartoztatta; letöltés: 2021.02.20.
- LIANOS, Theodore P.: Report on immigration to Greece (Pilot Study).
  European Migration Network, Greek National Contact Point, Center for Planning and Economic Research, Athens, September 2004. pp. 6–7.
  https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/networks/european_migration_network/ reports/docs/emn-studies/illegally-resident/gr-finalstudy_en.pdf; letöltés: 2021.01.03.
- Mediterranean situation – Greece. UNHCR, Operational Portal, Refugee Situations.
  https://data2.unhcr.org/en/situations/mediterranean/location/5179; letöltés: 2021.01.25.
- Moria migrants: Fire destroys Greek camp leaving 13,000 without shelter.
  BBC News, 2020.09.09.
  https://www.bbc.com/news/world-europe-54082201; letöltés: 2021.02.18.
- NGO in Greece reacts to migrant trafficking accusations.
  InfoMigrants, 2020.12.11.
  https://www.infomigrants.net/en/post/29045/ngo-in-greece-reacts-to-migrant-trafficking-accusations; letöltés: 2021.02.06.
- Over 1,000 migrants relocated from Greece in 2020.
  InfoMigrants, 2020.10.02.
  https://www.infomigrants.net/en/post/27697/over-1-000-migrants-relocated-from-greece-in-2020; letöltés: 2021.02.15.
- Samos Volunteers.
  https://www.samosvolunteers.org/; letöltés: 2021.01.25.
- STAMATOUKOU, Eleni: How the Greek policy on migration is changing.
  The European Data Journalism Network. 2019.12.27.
  https://www.europeandatajournalism.eu/eng/News/Data-news/How-the-Greek-policy-on-migration-is-changing; letöltés: 2021.02.13.
- Study in Greece – Refugees.
  https://refugees.studyingreece.edu.gr/; letöltés: 2021.02.09.

CSUTAK ZSOLT

A KIBERMÁTRIX KIHÍVÁSAI ÉS LEHETŐSÉGEI A 21. SZÁZAD TÁRSADALMÁBAN

Bevezető gondolatok

„A képzelet fontosabb, mint az ismeret."
Albert Einstein

Albert Einstein elhíresült gondolatával indítva eszmefuttatásunkat a 21. század elején a biológiai és a kibertéri vírusjárványok korában érdemes a tudományos-fantasztikus írók, jövőkutatók elképzeléseit is megvizsgálni akár még a múlt század elejéről is, hiszen kísérteties hasonlóságokra, megfelelésekre és megvalósult disztópikus jelenségekre bukkanhatunk napjaink globalizált társadalmaiban. Elég, hacsak a brit H. G. Wells, Arthur C. Clarke, William Gibson vagy az amerikai sci-fi nagymesterének számító Isaac Asimov megvalósult elképzelésire gondolunk, mint a világméretű számítógép-alapú könyvtárra, lakható űrállomásra vagy épp okos beszélő gépek és emberek összekapcsolódott hálózatára.[1]

Az emberiség létét fenyegető vírustámadásról, sőt másodlagos virtuális valóságkettőzésről (mátrix) is olvashatunk ezekben a tudományos-fantasztikus művekben, amelyek révén – ha megfogadjuk Einstein fent említett bölcsességét – tulajdonképpen könnyebben értelmezhetjük jelen valóságunk kihívásait is. Az emberiség írott történelmének körülbelül hét évezrede során még nem tapasztalhattunk olyan szintű gyors technológiai és életmódbeli változásokat, mint amilyenek az utóbbi évtizedekben meghatározzák hétköznapjainkat.

Elöljáróban, mintegy tézisszerűen megállapíthatjuk, hogy a teljesen új digitális technológiák, illetve a mesterséges intelligencia beláthatatlan fejlődési horizontja és perspektívái reális kockázati tényezőhalmazt hordoznak magukban. Továbbá – e technológiák immanens fejlődési potenciálját tekintve és a történelmi tapasztalatok alapján az emberiség pusztításra és építésre egyaránt hajlamos orientációját figyelembe véve – az új technológiák számos és jelentős veszélyforrást hordoznak a demokratikus társadalmak működését és az emberi kapcsolatok alakulását illetően.

Tanulmányunkban a következő oldalakon arra az alapkérdésre keresünk választ, hogy milyen jellemző vonásokkal írhatjuk le a posztmodern társadalmak és az új digitális technológiák komplex kapcsolatát, összefüggéseit. Elsődlegesen a téma kevésbé vizsgált társadalmi vetületeit és tudományetikai problémáit, illetve az ehhez kapcsolódó potenciális biztonságpolitikai veszélyforrásokat fogjuk áttekinteni és feltáró módon elemezni. Hipotézisszerű megállapításunk, hogy a 21. századi

[1] Több mint beszédes Isaac Asimov a The New York Timesnak adott jövőbelátó interjúja 1964-ből, a „2014-es világkiállítás" technikai csodáiról beszélve.
ASIMOV, Isaac: Visit to the World Fair of 2014. The New York Times, 1964.08.16. https://archive.nytimes.com/www.nytimes.com/books/97/03/23/lifetimes/asi-v-fair.html?src=longreads; letöltés: 2020.01.15.

társadalmakra és a demokrácia általános állapotára talán a legnagyobb veszélyt a kiberbűnözés, az online közösségi médiaplatformok befolyása és az előzmény nélküli számítógép-alapú technológiák forradalma jelenti. Erre a feltevésre keresünk támogató érveket a következő oldalakon.

Emberi létünk és egyre jobban összefonódó globalizált társadalmaink egészét vizsgáló holisztikus szemléletű filozófusok szerint napjainkban a számítógépek vezérelte digitális rendszerek és a mesterséges intelligencia (MI) fejlődésének korában olyan drasztikus átalakulásnak és paradigma-szintlépésnek lehetünk tanúi, mint amilyen fél évezreddel ezelőtt a könyvnyomtatás megjelenése, illetve a 19. század végén az elektromos áram elterjedése jelenthetett.[2] A McLuhan által csak Gutenberg-galaxisnak[3] is nevezett könyv- és papíralapú tudásmegosztáson alapuló civilizációs korszak érzékelhető módon élettartamának végéhez közelít, helyesebben szólva gyökeresen átalakul, digitalizálódik, virtualizálódik, és ami talán a legjellemzőbb új vonása: mediatizálódva hálózatosodik. Az emberiség történetében soha nem voltak az emberi és a gépi hálózatok olyan fontosak és befolyásosak, mint napjainkban a legnagyobb ember alkotta mesterséges hálózat, az internet korában, amely – amint látni fogjuk – már túlságosan is meghatározza a 21. század „poszt-posztmodern" társadalmakat, azok minden szegmensével együtt.

Felmérések szerint[4] 2018 óta az emberiség nagyobbik fele (több mint négymilliárd ember) már napi rendszerességgel használ valamilyen digitális online eszközt, és az összekapcsolódott globális okoseszköz-állomány (*smart devices*) mérete, az úgynevezett IoT (*internet of things*), vagyis a világhálóra kapcsolódott készülékek száma ma már 25 milliárdra tehető, 2025-re pedig elérheti a döbbenetes 75 milliárdos számot is.[5] Ez az új, tulajdonképpen önálló életet élő gigászi eszközállomány (az okosóráktól az önjáró mini tengeralattjárókon és a katonai robotokon keresztül a teljesen automata budapesti 4-es metróig) már részben mesterséges intelligencia felügyelete alatt dolgozik, amely már önmagában biztonsági kockázati tényezőt jelent még a rosszindulatú külső behatások nélkül is.

A továbbiakban rövid betekintést nyújtunk az új digitális, pontosabban szólva kibertérbeli eszközállomány és milliónyi alkalmazástípus jelentette új paradigma fő jellemvonásaiba, és különösképpen az új világjelenség biztonságpolitikai vetületeibe, amelyek nemcsak az egyéni végfelhasználók, hanem a multinacionális társaságok és nemzetállamok biztonságát is jelentősen meghatározzák, illetve befolyásolják. Kérdés, hogy az emberi természet és hagyományos interperszonális együttműködésen alapuló társadalmaink felkészültek-e a forradalmian új és radikális digitális átállásra, életmódra, és mindez milyen kulturális, társadalmi és következésképp politikai következményekkel járhat. Ahogy számos világhírű gondolkodó, mint Albert Einstein, Neumann János, Stephen Hawking vagy Yuwal Harari és technológiai forradalmár nagyvállalkozó, mint Elon Musk is feltette már a kényelmetlen kérdést: foglalkozunk-e eleget az új, gyakran embert helyettesítő okos technológiai megoldások (például a

[2] FORD, Martin: Robotok kora. HVG Könyvek, Budapest, 2017. pp. 10–13.
[3] MCLUHAN, Marshall: The Gutenberg Galaxy. University of Toronto Press, Toronto, 2011.
[4] CLEMENT, J.: Internet usage worldwide – statistics & facts. Statista, 2020.10.26. https://www.statista.com/topics/1145/internet-usage-worldwide/; letöltés: 2021.01.15.
[5] Internet of Things – number of connected devices worldwide 2015-2025. Statista, 2016.11.27. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide; letöltés: 2020.01.28.

mesterséges intelligencia és a robotika) erkölcsi és emberi vonatkozásaival, vagy a kényes kérdések megválaszolását a jövő generációira hagyjuk?[6]

A világháló biztosította globális virtuális összekapcsolódás (*global interconnectedness*) előzmény nélküli az emberiség történetében, és sajnálatos módon az ezzel járó álhírek, áltudományos fórumok és összeesküvés-elméletek viharos terjedése is komoly társadalmi és biztonságpolitikai kockázatot jelent egyéni, közösségi és állami szinten egyaránt.

A növekvő biztonságpolitikai aggodalmakon és potenciális kiber veszélyforrásokon túl fontosnak tarjuk megvizsgálni az új digitális technológia alapú társadalmaink szociálpszichológiai, kulturális átalakulási folyamatát és kulcsfontosságú tényezőit, amelyek még a biztonsági kihívásoknál is drasztikusabb változásokat és radikális jelenségeket tartogatnak az elemzők számára. Társadalomtudósok és kritikus elemzők véleménye szerint[7] a digitális információs technológiák tervezői és előállítói rendszerszerűen elfeledkeznek új megoldásaik közvetett egyéni és társadalmi hatásáról, vagy csak évekkel később felemás érzésekkel szembesülnek azokkal, mint ahogy – lentebb látni fogjuk – az internet tervezésekor is történt.

Általánosítással élve, a közép-, illetve hosszú távú társadalmi, kulturális egyéb emberi következmények vizsgálata, figyelembevétele nem tartozik a programozók, szoftverfejlesztő mérnökök prioritásai közé, és természetesen ezért nem szeretnénk őket kárhoztatni, hiszen egy digitális termék, szolgáltatás megtervezéséhez és előállításához teljesen más képességekre és ismeretekre van szükség, mint azok későbbi biztonságpolitikai vagy össztársadalmi hatásának elemzéséhez. Ugyanakkor mindezen technológiák hatáselemzése újszerűségük, egy-két évtizedes vagy csupán pár éves múltjuk miatt nem kis szellemi kihívást jelent. Olyan kutatókat, elemzőket kell találni, akik egyrészt behatóan ismerik az új digitális technológiákat, másrészt a társadalmi vonatkozásokra és az emberi rezgésekre is fogékonyak, valamint a tágabb társadalomtudományi összefüggések feltárására is képesek.

Feltehetőleg ebből az okból kifolyólag e puhább technológiai vonatkozások kevésbé kutatott és feltárt területnek számítanak a jelen pillanatig, mondhatnánk egészen addig, amikor számos negatív hatásuk már a laikusok számára is nyilvánvalóvá válik. Ezzel kapcsolatban érdemes megjegyeznünk két kiragadott és elgondolkodtató példát, amelyek már igencsak meghatározzák hétköznapjainkat a kiberkorban. Egyrészt Norton A. Schwartz, az amerikai légierő tábornokának és kibervédelmi parancsnokának *bon mot*-vá vált megjegyzése sokatmondó, miszerint napjainkban „*egy áramszünet lehet, hogy csupán áramszünet, ellenben a kiberhadviselésben már lehet, hogy egy előzetes katonai csapás része*.”[8]

---

[6] CLIFFORD, Catherine: Elon Musk: ‘Mark my words — A.I. is far more dangerous than nukes’. CNBC, 2018.03.13. https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html; letöltés: 2020.03.19.

[7] HARARI, Yuwal Noah: Homo Deus – A holnap rövid története. Animus Kiadó, Budapest, 2017. pp. 195–200.

[8] CLARKE, Richard A. – KNAKE, Robert K.: Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins, New York, 2010. p. 25.

Másrészt érdemes felidéznünk az internet két alapító atyjának is tartott Vinton Cerf és Sir Tim Berners-Lee keserű hangvételű interjúját a *The Guardian*ben az általuk kifejlesztett világhálózat átalakulásáról, sorsáról.[9] A két világhíres szakember meglátása szerint a számítógép-alapú világhálózat (*internet*) eredeti elképzelésük helyett – mint globális digitális tudáspiactér – az 1991 óta eltelt három évtized alatt valami teljesen más képződménnyé alakult a közösségi média és a tömeges online játékok uralta korban. Elég, ha csak arra az elszomorító adatra gondolunk, miszerint a mély internet (*deep web*) alvilági bugyrait uraló sötét web (*dark web*) körülbelül 80%-a gyomorforgató gyermek pornográfiával és egyéb illegális tartalommal van feltöltve,[10] amely óriási veszélyforrást jelent mind az egyének, mind a társadalom számára. Nem beszélve arról az elszomorító tényről, hogy a nemzetközi bűnüldöző szervezetek és internetes biztonsági cégek kutatásai szerint az internetalapú kiberbűnözés már 2016 óta globálisan átvette a vezetést a kábítószer-, illetve illegális fegyver- és emberkereskedelemtől. Megdöbbentő adat, miszerint az új típusú láthatatlan és névtelen kiberbűnözök által okozott kár mértéke a világon eléri az évi 5000 milliárd dollárt, ami az Amerikai Egyesült Államok közel másfél éves szövetségi költségvetésének megfelelő összeg.[11]

A szándékosan károkozó internetes szereplőkön a világháló, és különösképpen a közösségi hálózatok világa szélsőségesen demokratizálta az információáramlást és az eszmék, gondolatok cseréjét, terjedését a világban, és a fent említett realista-pesszimista emberi alapvonások révén inkább negatív előjellel. Az utóbbi évtizedekben jelentős mértékben erodálódott és megroppant a hagyományos társadalmi, politikai és akadémiai elitbe vetett hit és bizalom mértéke, ezzel fordítottan arányosan pedig az internetes valláspótlék-szerű összeesküvés-elméletek, babonaságok, hamis ezoterikus tanok népszerűsége, valamint a képzetlen megmondóemberek, önjelölt szakértő videobloggerek (*vlogger influenszerek*) befolyása immár az egekbe szökött.[12]

A felhasználók millióinak, különösképpen a fiatal generáció jelentős részének a digitalizált, virtuális, (avagy kibertéri) másodlagos valóság már az elsődleges fizikai valóságunk kiterjesztésévé vált, sőt sokuk esetében a világháló inkább elsődleges információ és élményforrásnak, megélt valóságnak tekinthető annak minden személyiségtorzító és akár tudatmódosító veszélyforrásaival.

---

[9] SOLON, Olivia: Tim Berners-Lee on the future of the web: 'The system is failing'. The Guardian, 2017.11.16. https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality; letöltés: 2019.12.29.

[10] CHEN, Hsinchun: Dark Web: Exploring and Data Mining the Dark Side of the Web. Springer, New York, 2012.

[11] MORGAN, Steve: Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine, 2020.11.13. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/; letöltés: 2021.01.15.

[12] KREKÓ Péter: A vírusnál még a tömeggyilkos háttérhatalom is jobb. Index, 2020.04.12. https://index.hu/techtud/2020/04/12/tnt_osszeeskuves_kreko_peter_podcast/; letöltés: 2020.04.12.

Fogalmak útvesztőjében

Az alábbiakban arra keresünk választ, hogy milyen tudományos paradigmák és percepciók jellemzik digitális világunkat, illetve milyen fogalmi keretrendszerben ragadhatjuk meg leginkább a világban zajló folyamatokat.

Manapság a köznyelvben gyakran szinonimaszerűen, jelentésbeli átfedésben használják a *digitális* és a *kiber* szavakat, habár az utóbbi lenne inkább helytállóbb és a valóságot jobban leképező fogalom a sokkal szűkebb értelmezési dimenziójú digitálissal ellentétben. Természetesen mindkét fogalomnak van létjogosultsága, akárcsak magyar tudományos vonatkozása is, főleg a második világháború elől Amerikába menekült magyar atomfizikusok, elméleti matematikusok kimagasló kutatói munkássága révén. A második világháború idején az ifjú amerikai John W. Tukey princetoni matematikus zseni és magyar származású professzortársa, Neumann János kidolgozta és megalapozta a 0 és az 1, kettes számrendszerbeli számjegy (*binary digit*), vagyis egy egységnyi, bitalapú (0 vagy 1, igaz/hamis) algoritmusrendszert, amely a 20. század úttörő digitális számítástechnikai paradigmájává vált.[13] Tehát a digitális kifejezés elsősorban az elektronikus számítástechnikai folyamatokhoz és bináris rendszerű algoritmusokhoz kapcsolódik. Ezzel ellentétben felettébb sok félreértésre ad okot és alkalmat a *kiber* kifejezés és a *kibernetika* tudományterület összemosása, önkéntelen és félrevezető felcserélése.

A kibernetika az információszerzés és a dinamikus rendszerek irányításának, vezérlésének, majd számítástechnikai modellezésének és programozásának új tudománya 1946 óta Norbert Wiener nevéhez fűződik, és a ma használatos *kiber* kifejezéstől teljességgel eltérő tudományos kontextusban volt használatos. Wiener, aki a görög kormányos (*kübernétész*) kifejezésből kölcsönözte új tudományágának elnevezését, az állatok és az ember alkotta mesterséges gépek dinamizmusát és irányítását hasonlónak vélte. Ezt később a játékelmélet és egyéb forradalmian új oldalági tudományos diszciplínák révén Neumann János és Harsányi János, Nobel-díjas amerikai magyar tudósok a számítástechnikában, valamint a társadalmi folyamatok (különösképpen háborús konfliktusok) lemodellezésére is kiterjesztettek, hiszen többségükben az amerikai védelmi kutatások szolgálatában működtek.[14] Ezzel kapcsolatban helytállónak bizonyult Bertrand Russell híres brit matematikus és pacifista filozófus megjegyzése, miszerint háborús időszakban nem lehet tudományt művelni, ha annak nincs valamiféle hadászati kapcsolódása vagy jelentősége.[15]

---

[13] Father of digital computer János Neumann was born 114 years ago. About Hungary, 2017.12.28. http://abouthungary.hu/news-in-brief/father-of-digital-computer-janos-neumann-was-born-114-years-ago/; letöltés: 2020.03.20.

[14] Norbert Wiener, American mathematician. Britannica. https://www.britannica.com/biography/Norbert-Wiener; letöltés: 2020.03.10.

[15] ESTEVES, Olivier: Bertrand Russell: the utilitarian pacifist. French Journal of British Studies, XX-1/2015. https://journals.openedition.org/rfcb/308; letöltés: 2020.03.25.

A sokat használt *kiber* (*cyber*) kifejezés a szó napjainkban is használt értelmében elsősorban William Gibson kanadai fizikus, sci-fi íróhoz kapcsolódik, aki a *Burning Chrome* című novellájában 1982-ben használta először ezt a kifejezést a számítógép és az ember kölcsönhatásán alapuló rendszer metaforájaként. Ugyanakkor a teljesség igényével meg kell említenünk a sci-fi brit nagymesterének, Arthur C. Clarke-nak *A város és a csillagok* című remekművét 1956-ból, amelyben már használta a virtuális mátrix és virtuális valóság fogalmakat teljesen hasonló kontextusban.[16]

Napjaink szakszerű alkalmazási módja és kontextusa szerint – elsősorban a hadtudományban és biztonsági tanulmányokban használatos fogalomtár alapján – a kibertér a teljes elektromágneses spektrumon belül működő elektronikus eszközök, információs hálózatok rendszerére utal,[17] tehát jóval szélesebb dimenziójú és tartalmú kifejezés, mint a rokon értelmű szóként is használt és jóval régebbi *digitális* fogalma. A 2000-ben kidolgozott *Joint Vision 2020* címet viselő amerikai összhaderőnemi stratégiai dokumentumban nevesítették először a különféle katonai hadviselési tartományokat (*warfighting domain)* és működési környezetet (*operational environment*), valamint területeket (*terrain*), amelyek közé bekerült az információs környezeten belül a kibertér is. Az Észtország elleni 2007. áprilisi kibertámadás, a híres *web war one*[18] drámai eseményei után 2008-tól a NATO új kibervédelmi stratégiájában szintén megjelent a kibertér mint a dinamikus katonai és civil információs környezet része, és egyben mint potenciális új hadszíntér.[19] Sőt, az egyre szaporodó és komoly aggodalomra okot adó burkolt és nyílt kibertámadások, zsarolóvírusok 2014-be arra késztették a NATO legfőbb döntéshozó szervét, az Észak-atlanti Tanácsot, hogy a jövőben egy tagállamuk ellen elkövetett bizonyítható és visszakövethető kibertámadást valódi háborús indoknak és támadásnak *(casus belli)* nyilvánítsanak, és ezt beemelték a kollektív védelmet nyújtó Washingtoni Szerződés híres 5. cikkelyének rendelkezései közé.[20]

A NATO ez irányú stratégiai megközelítéséhez és definíciójához hasonló módon a hazai hadtudományos kibertér fogalmi tisztázásában élen jár Haig Zsolt ezredes és Kovács László tábornok iránymutató szakirányú munkásságuk révén. Az információs műveletek és a kiberhadviselés magyar szakértői szerint a kibertér nem más, mint „*a harctéren a különböző hálózatba kapcsolt elektronikai rendszerek az információs színtérnek azt a részét használják, amelyben a különféle elektronikus*

---

[16] GIBSON, William: Cyberspace. Technovelgy, 1982. http://www.technovelgy.com/ct/content.asp?Bnum=53; letöltés: 2019.12.25.

[17] HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus, Budapest, 2019. pp. 22–26.

[18] BLANK, Stephen: Web War I: Is Europe's First Information War a New Kind of War? Comparative Strategy, Volume 27, Issue 3, 2008. pp. 227–247. https://www.tandfonline.com/doi/full/10.1080/01495930802185312; letöltés: 2020.01.12.

[19] HÄUßLER, Ulf: Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty. International Cyber Security Legal & Policy Proceedings, 2010. 104-5. Cooperative Cyber Defence Center of Excellence, Tallinn, Estonia, 2010. https://infosec-journal.com/article/cyber-security-and-defence-perspective-articles-4-and-5-nato-treaty; letöltés: 2020.01.10.

[20] BRENT, Laura: NATO's role in cyberspace. NATO Review, 2019.02.12. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html; letöltés: 2020.01.12.

információs folyamatok (elektronikai úton végrehajtott adatszerzés, adatfeldolgozás, kommunikáció stb.) realizálódnak, illetve az elektronikai rendszerek elleni tevékenység és a védelem megvalósul. Az információs színtér e tartományát gyakran cybertérnek is nevezzük."[21] Tehát a tisztánlátás végett és a fogalmi, szemantikai zűrzavar elkerülése érdekében a szűkebb számítástechnikai dimenzióra szorítkozó digitális ökoszisztéma kifejezés helyett érdemes és javasolt a kiberdimenzió, avagy kibertér kifejezés használata, amely lefedi az adatközvetítő és -feldolgozó fizikai hálózatot (*internet hardware*), az okos eszközök rendszerét (*Internet of Things*) és a rajtuk futó alkalmazások és programcsomagok (*software*) tömkelegét egyaránt az elektromágneses spektrum teljes skáláján.

A rekordgyorsasággal lezajló forradalmi technológiai paradigmaváltással valójában sem az átlagemberek milliói, sem számos állami szereplő nem tudnak mit kezdeni, főleg akkor, ha berögzült 20. századi mentalitás és szokásrendszer rabjaiként közelítenek az új kihívások felé.

Adat és információ: új hadviselés új fegyverekkel

„*Az adat a 21. század olaja.*"[22]

Az alábbiakban arra a problémakörre, illetve jelenségre keresünk választ, hogy a világunkban észlelhető egyre növekvő mennyiségű digitális adattömeg és információállomány milyen általános tulajdonságokkal rendelkezik, mire használható és milyen kiberbiztonsági veszélyeket hordozhat a felhasználók széles spektrumára.

Az információ – fogalomtisztázás végett: a feldolgozott adat(halmaz) – már évszázadok óta hatalmi tényező, katonai, politikai vagy gazdasági előnyszerzés szempontjából kulcsfontosságú eszköz a döntéshozók kezében. Ez a megállapítás még hangsúlyosabban igaz napjainkban, amikor az emberi elme számára már felfoghatatlan mennyiségben termelődik virtuális elektronikus adat a világhálón. A humán felhasználók (plusz az IoT és az MI) által generált átlagos napi adatforgalom az interneten 2019-ben kb. 8000 petabyte-nyi[23] volt, ami az arányosítás és az érzékelhetőség kedvéért megfelel a washingtoni Kongresszusi Könyvtár 40 millió kötetes könyvállománya kétszeresének. Nyilvánvaló, hogy a folyamatosan növekvő és többnyire értelmezhetetlen adatmennyiség egyrészt leterheli az adathordozó digitális rendszert, másrészt komoly mentális kihívást jelent az embereknek, hiszen az emberi elme nem képes ilyen mennyiségű és ilyen radikálisan gyorsan változó méretű és minőségű adattenger, külső benyomás (*input*) feldolgozására.

---

[21] HAIG Zsolt – KOVÁCS László: Fenyegetések a cybertérből. Nemzet és Biztonság, 2008. május. p. 63. https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/1010/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf?sequence=2; letöltés: 2019.12.20.

[22] Humby Clive brit matematikus, nagyvállalati marketingmenedzsernek tulajdonított mondás 2006-ból. Who should get credit for the quote "data is the new oil"? https://www.quora.com/Who-should-get-credit-for-the-quote-data-is-the-new-oil; letöltés: 2020.01.30.

[23] Data volume of global consumer IP traffic from 2017 to 2022 (in exabytes per month). Statista, 2020.02.28. https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic; letöltés: 2019.12.26.

Internetbiztonsági szakemberek és társadalomtudósok megállapításai szerint aggasztó és komoly biztonsági kockázatot jelent a kibertérben kibontakozó korlátlan információs szabadosság és kontrollálatlan demokratizmus, amint azt R. Waltzman professzor, az amerikai RAND Corporation és védelmi technológiák kutatója is megállapította. A professzor szerint az utóbbi három évtized során az emberiség történetében egyedülálló és példátlan módon keletkezett és vált hozzáférhetővé óriási tudásbázis, és ezzel párhuzamosan még nagyobb mennyiségű rosszindulatú, káros információs tartalom is.[24] Az információ, illetve digitális tartalmak vagy kártevő programok előállításához és terjesztéséhez ma már csupán két dologra van szükség: egy hálózatra kapcsolható számítástechnikai eszközre és némi infokommunikációs ismeretre, illetve szoftverkezelési vagy programozási készségekre.

A *Z*, illetve az *Alfa* generáció több százmilliónyi tagja világszerte már az internet avagy kiberkor szülötte, és jelentős részük rendelkezik mindkét alapfeltétellel. A RAND kutatói szerint az elmúlt évtized botrányos kibertéri eseményei megmutatták, hogy az információs tartomány túlságosan demokratizálódott és az információ új típusú, kiberfegyverré alakult.[25]

Mindemellett a rendszerrengető WikiLeaks[26] és az Edward Snowden-féle[27] szivárogtatási és hírszerzési kémbotrányok óta sokan nagyon túlzóan úgy gondolják, hogy az internetes virtuális világot és kommunikációt komoly kormányzati felügyelet és ellenőrzés jellemzi, de ez csak részben helytálló megállapítás. Az Amerikai Egyesült Államok és Kína – valamint kisebb mértékben Oroszország is – rendelkezik a legnagyobb, legkorszerűbb és legátfogóbb digitális adatforgalmat felügyelő és azt akár korlátozó személyi, tárgyi eszközökkel és képességekkel a világon, de még a technológiailag legfejlettebb nagyhatalmak sem képesek totális kontrollra a kibertér gigászi adatmennyisége és az internetes fizikai hálózat több csomópontos sejthálózatszerű felépítése miatt.

A 2016-os amerikai elnökválasztásra is árnyakat vető külső befolyásolási botrányok, illetve az Európát megrendítő brit brexit-népszavazás kimenetelét is kardinálisan befolyásoló kis adatelemző IT-cég, a Cambridge Analytica[28] esete rávilágított a közösségi hálózatok kontrolálatlan működési kockázatára és igencsak aggályos adathasználati gyakorlataira. Az ilyen hálózatok „puha" fegyverként, egyfajta hatalmi politikai és kommunikációs eszközként (*soft power tools*) is használhatók[29]. A digitális írástudás és kultúra többszintű és -típusú szakadékokkal szabdalt sajátosságokkal rendelkezik a világ lakossága körében. Egyrészt létezik a

---

[24] WALTZMAN, Rand: The Weaponization of Information – The Need for Cognitive Security. RAND Corporation, Santa Monica, CA, 2017.

[25] Uo. p. 24.

[26] LEIGH, David – HARDING, Luke: WikiLeaks-akták – Julian Assange háborúja a titkosítás ellen. Geopen, Budapest, 2011.

[27] GREENWALD, Glen: A Snowden-ügy. HVG Könyvek, Budapest, 2014.

[28] WERNER, Tom: The Cambridge Analytica Scandal. The Verge, 2018.04.10. https://www.theverge.com/2018/4/10/17165130/facebook-cambridge-analytica-scandal; letöltés: 2019.12.10.

[29] Joseph S. Nye hatalmi tipológiája szerint a kultúra, a kommunikáció is a hatalmi erőkivetítés összetevője lehet.
GOMICHON, Maxime: Joseph Nye on Soft Power. E-International Relations, 2013.03.08. https://www.e-ir.info/2013/03/08/joseph-nye-on-soft-power/; letöltés: 2020.02.15.

közismert digitális generációs szakadék, másrészt a világgazdaság széttöredezettségét is tükröző északi–déli vagy fejlett–fejlődő/fejletlen tengely mentén megfigyelhető Európa, Észak-Amerika és a Távol-Kelet szembenállása Afrikával, Dél-Amerikával, Dél-Ázsiával, ami tulajdonképpen párhuzamos világok, társadalmak egymásmellettiségét is jelenti.[30]

Mark Zuckerberg Canossa-járásszerű kongresszusi megjelenése és önkritikája nyomán az állami törvényi szigorítás igényléséhez nemrég csatlakoztak brit és amerikai polgárok széles tömegei is. Egyrészt a közismert 2016-os brexit-népszavazás és amerikai elnökválasztás körüli botrányok miatt, és aztán különösképpen 2020 elején a koronavírus-világjárvány révén elszaporodó internetes trollok (fizetett online kommentezők), konteók és álhírdömping miatt a britek és az amerikaiak többsége szigorúbb adatkezelési, információmegosztási és internetes szolgáltatásokat ellenőrző és felügyelő jogszabályokat szeretnének, ha nem is globális joghatállyal, de legalább saját országaik kiberterében.[31]

A fent említett felfoghatatlan mennyiségű és gyakran ellentmondó információdömping, valamint a tudományos szűrők, úgynevezett kapuőrök visszahúzódása, az elektronikus médiumok szerkesztőbizottságainak drasztikus csökkenése, illetve gyakran MI-alapú alkalmazásokkal történő helyettesítése együttesen megteszik negatív hatásukat a felhasználók és online médiafogyasztók tömegeire.

Ez a sajnálatos világtendencia jól kimutatható és megfigyelhető az utóbbi évtizedekben elvégzett médiatudatossági és szociálpszichológiai vizsgálatokban[32] az összeesküvés-elméletek és áltudományos hírportálok, különféle *influenszerek, vloggere*k befolyásának és a közösségi média tartalommegosztásainak vizsgálatakor. Olyan új, mondhatni kiberpszichológiai kifejezések, mint visszhangkamra (*echo chamber*), véleménybuborék és kognitív disszonancia, vagyis saját magunk igazába és kényelmes, önigazoló előítéleteink valóságába vetett hit, a kibertérben élő és tevékenykedő felhasználók milliárdjainak alapvonásává vált napjainkra. A kibertérben terjedő kifejezetten rosszindulatú és károkozó programokkal, zsarolóvírusokkal párhuzamosan a 21. század eddigi legnagyobb globális egészségügyi és társadalmi kihívását jelentő koronavírus-járvánnyal kapcsolatban is az egekbe szöktek a változatos összeesküvés-elméletek és víruseredet-mítoszok, amelyekben például a vizsgált amerikai lakosság közel harmada hisz.[33]

---

[30] KHANNA, Parag: Konnegtográfia – A globális civilizáció jövőjének feltérképezése. HVG Könyvek, Budapest, 2017. pp. 28–32.

[31] TAPPER, James: Social media giants must tackle trolls or face charges – poll. The Guardian, 2020.04.04. https://www.theguardian.com/technology/2020/apr/04/social-media-giants-must-tackle-trolls-or-face-charges-poll; letöltés: 2020.04.15.

[32] KREKÓ Péter: Tömegparanoia – Az összeesküvés-elméletek és álhírek szociálpszichológiája. Athaeneum, Budapest, 2018.

[33] SCHAEFFER, Katherine: Nearly three-in-ten Americans believe COVID-19 was made in a lab. Pew Research Center, 2020.04.08. https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab/; letöltés: 2020.04.12.

Az alternatív valóságba és torz, áltudományos magyarázatokba vetett hit az online közösségi média globális elterjedésével soha nem tapasztalt lendületet kapott – természetesen mint fentebb is olvashattuk – a világháló megálmodóinak eredeti magasztos elképzelésivel gyökeres ellentétben. A világhírű amerikai író és újságíró Mark Twainnek tulajdonított bölcsesség szerint „*amíg az igazság felveszi a csizmáját, addig a hazugság már kétszer megkerülte a földet*”.[34] A 19. század végén, a távíró, a telefon és a bulvársajtó kezdeti korszakában – és a világunkat átszövő kibertér előtt több mint egy évszázaddal – ez a szellemes kijelentés különösen kifinomult ember- és társadalomismeretre vallott, és sajnálatos módon napjainkban még hatványozottan érvényes. Mondanunk sem kell, hogy ez a globális jelenség és felvett emberi tulajdonság igen súlyos társadalmi és politikai biztonsági kockázatot jelent az államok kormányzatai és az emberi közösségek fennmaradása, illetve szétforgácsolódása szempontjából. A szabadjára engedett adatforgalom és a kontrolálatlan információmegosztás tekintetében – erkölcsfilozófiai szempontból – olyan dilemma előtt állunk, mint amihez hasonlóval az amerikai atomfizikusok is szembesültek 1945 júliusában. A világháború során szupertitkos amerikai Manhattan-terv több vezető tudósa – a magyar Szilárd Leó vezetésével – az atombomba első bevetésének küszöbén tudományetikai és általános erkölcsi aggályainak és fenntartásainak adott hangot F. D. Roosevelt elnöknek címzett petíciójában. A világ legjobb tudósai ugyanis még nem tartották az emberiséget mentálisan és morálisan felkészültnek az atomenergia használatára, főleg nem háborús pusztító szándékból polgári célpontok ellen.[35]

Napjaink radikálisan átalakuló digitális ökoszisztémája, avagy kiberuniverzuma is ehhez hasonló, ha nem nagyobb volumenű és még mélyrehatóbb tudományos-technológiai és szociálpszichológiai kihívást jelent az emberiség számára. Hiszen az atomenergia (és az atomfegyverek) felhasználásának célja és módja mindössze pár tucatnyi csúcsdöntéshozó és -szakember köré összpontosult a második világháború utolsó évében, akárcsak a hidegháború fél évszázada során is, miközben napjaink másodlagos virtuális univerzuma bárki számára hozzáférhető és valós biztonsági szelepek, illetve korlátok nélküli alkalmazásmódot kínál jó és rossz célokra egyaránt. Gondoljunk csak a hozzáférhető milliónyi digitális alkalmazás vagy a mesterséges intelligencia még feltáratlan lehetőségeire, illetve az emberi társadalmaink alapszükségleteit, biztonságát és fizikai létét meghatározó, számítógépek vezérelte kritikus infrastruktúrák sebezhetőségére (*cyber vulnerability of critical infrastructure*), egyre növekvő mértékű kiberhadviselési kitettségére.

Ma már egyáltalán nem a valóságtól elrugaszkodott fantazmagóriák körébe tartoznak az alábbi esetek: például egy fiatal erdélyi magyar hacker narcisztikus kivagyiságtól vezérelve – avagy az orosz katonai titkosszolgálat jutalma fejében – pusztán egy notebook és középszintű informatikai szaktudás segítségével Aradról

[34] Directory of Mark Twain's maxims, quotations, and various opinions. http://www.twainquotes.com/Lies.html; letöltés: 2020.04.12.

[35] SZILÁRD Leó: A Petition to the President of the United States. 1945.07.17. http://www.dannen.com/decision/45-07-17.html; letöltés: 2020.04.12.

feltöri az amerikai külügyminiszter magánlevelezését és mobiltelefonját,[36] behatol egy hőerőmű vezérlőrendszerébe, amely több százezer ember energiaellátásáért felelős; vagy egy 13 éves fiúnak az esete, aki a világhálón egy észtországi szigetről szélsőjobboldali terroristasejtet szervezett az Amerikai Egyesült Államokban.[37]

A legendás H. N. Schwarzkopf Jr., az amerikai hadsereg tábornoka 1991-ben az öbölháború előestéjén még mondhatta kissé ingerülten, hogy „*egy istenverte laptoppal nem lehet háborúzni, csak golyókkal és bombákkal,*"[38] ma már ez a kijelentés – mint tapasztalhatjuk – egyáltalán nem tartható, de már a 2003-as második öbölháború során sem bizonyult annak.

A szingularitás kapujában

A kibertér hálózata és a mesterséges intelligencia jelentette biztonsági kihívások és nem utolsósorban társadalmi problémák, morális aggályok egyre inkább meghatározzák a 21. század modern társadalmainak hétköznapjait.

Az alábbi oldalakon áttekintjük az önjáró okoseszközök, robotok és a mesterséges intelligencia lehetséges kiteljesedési potenciálját, védelmi technológiai fejlesztési dimenzióit. Továbbá választ próbálunk találni arra a komplex tudományfilozófiai kérdésre, hogy mennyire lehet hasznos, illetve káros az emberiség számára a technológiai forradalom e szegmense.

A 21. század generációi az internetalapú gyors, instant digitális megoldások világában élnek és szocializálódnak, illetve a szinte minden számítási és előjelzési problémára választ adó forradalmi kvantum-számítástechnika és az öntanuló mesterséges intelligencia bűvkörében nőnek fel. Nyilvánvalóan a technológiai varázslat kezdeti időszakában – ami napjainkat is jellemzi – a felhasználók nem az árnyoldalakról és negatív tényezőkről fognak elsősorban gondolkodni, hiszen ez inkább az elemzők és a társadalmi, biztonsági vonatkozásokra fogékonyabb szakértők feladata. A történelmi tapasztalat alapján azonban kijelenthetjük, hogy minden eszköz vagy alkalmazás, amely alkalmas lehet akár destruktív célokra is, azt az emberek (államok) jelentős része gátlástalanul fel fogja használni klasszikus *hobbesiánus,* avagy önérdekvezérelt céljai elérése érdekében. Mint Waltzman professzor és tudóstársai megállapították, az információ és a digitális megoldások militarizálása, fegyverré alakítása már évtizedek óta tartó jelenség, és ennek hatása alól nem lehet kivétel sem a kibertér (mint hadszíntér), sem az emberszerű robot (android kiborg), sem az őket irányító mesterséges intelligencia. Különösképpen ez utóbbi igen sok nemzetközi vitának és aggodalmaskodó hangnak adott okot megnyilvánulásra, bár az elméleti vita és az erről való futurológus gondolkodás jóval régebbi, mint gondolnánk.

---

[36] CIMPANU, Catalin: Hacker Guccifer, who exposed Clinton private email server, ready for US prison sentence. ZNet, 2018.10.24. https://www.zdnet.com/article/hacker-guccifer-who-exposed-clinton-private-email-server-ready-for-us-prison-sentence/; letöltés: 2020.04.14.

[37] GONZALEZ, Jenipher Camino: Far-right terrorist ringleader found to be teenager in Estonia. Deutsche Welle. 2020.04.10. https://www.dw.com/en/far-right-terrorist-ringleader-found-to-be-teenager-in-estonia/a-53085442; letöltés: 2020.04.15.

[38] CLARKE, Richard A. – KNAKE, Robert K.: Cyber War: The Next Threat to National Security and What to Do About It. Harper Collins, New York, 2010. pp. 19–21.

A modern digitális számítástechnika megszületésével párhuzamosan a második világháború vége felé néhány tudóst, különösképpen az angol Alan Turingot és a magyar-amerikai Neumann Jánost már a mesterséges (gépi) intelligencia kifejlesztésének gondolata kezdte foglalkoztatni. Azok az elméleti problémák (és fenntartások), amikről közel egy évszázaddal ezelőtt ők már elgondolkodtak, napjainkra egyre égetőbb és válaszra váró technológiai és tudományfilozófiai kérdésekké váltak. Vajon a gépi vagy mesterséges intelligencia – amely 2020-ban már gépi tanulásra is képes – elérheti-e (esetleg akár túlszárnyalhatja-e) az emberi elme komplexitását és működési szintjét? Ha igen (és miért ne történhetne ez meg?), akkor kérdés, hogy mikor következik be a forradalmi „szingularitás pillanata" az emberiség történetében. Vajon igaza lesz a számítógép-tervező Neumann Jánosnak és a sci-fi írással is foglalkozó amerikai matematikus kollégájának, Vernor Vinge-nek, akik már az 1950-es években a technológiai és az informatikai paradigmaváltásról – a bizonyos technológiai szingularitásról – értekeztek, ami ha bekövetkezik, akkor szerintük az általunk ismert és megszokott történelem véget érhet.[39]

Ray Kurzweil népszerű amerikai jövőkutató mérnök szerint – aki nem mellesleg a Google első műszaki fejlesztési vezérigazgató-helyettese volt, és a Szilícium-völgyi Szingularitás Kutatóegyetem társalapítója – a sokat emlegetett szingularitás, sőt akár az emberi és gépi elme összekapcsolódása (*HMI – human machine interface/interaction*) megállíthatatlanul közeledik, és várhatóan 2045 körül bekövetezik.[40] Meglátása szerint – amivel számos kutató egyetért – abban a történelmi momentumban bekövetkezik majd a MI nagy pillanata, felnőtté válása is, és elkezdődhet az „emberiség 2.0." időszaka. Hogy ez az esemény jó vagy rossz lesz számunkra, nos, az már más kérdés, arról sokat kell és fogunk még tárgyalni, de Kurzweil egyértelműen az optimista, emberbarát MI-forgatókönyv elkötelezett híve.

Közismertek és igen nagy visszhangra leltek az utóbbi években neves tudósok és technológiai újítók nyilvános kritikai észrevételei az úgynevezett emberhelyettesítő okostechnológiák, elsősorban a mesterséges intelligencia és a robotika szédületes fejlődése vonatkozásában. Néhai Stephen Hawking világhíres brit fizikus és kozmológus, Martin Ford amerikai MI-kutató szociológus, illetve Elon Musk nagyvállalkozó technológiai forradalmár szerint nem ajánlott, illetve kifejezetten veszélyes olyan technológiai megoldásokkal kísérletezgetni, amelyek egyrészt fegyverként is használhatóak és feltáratlan biztonsági kockázatokat rejtenek, másrészt tömeges alkalmazásukkal embermilliók munkáját vehetik el. Musk – az önjáró autók (és űrrakéták) világszerte elismert gyártója – meglehetősen kritikusan és ellenségesen viszonyul az önálló döntésekre is képes mesterséges intelligencia által vezérelt gépekhez, egyenesen veszélyesebbnek tartja őket az emberiség biztonságára nézve, mint a tömegpusztító nukleáris fegyvereket.[41]

---

[39] VINGE, Vernor: Technological Singularity. Whole Earth Review, January 2003. http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf ; letöltés: 2020.04.05.

[40] REEDY, Christianna: Kurzweil Claims That the Singularity Will Happen by 2045. Futurism, 2017.10.05. https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045; letöltés: 2020.04.15.

[41] CLIFFORD, Catherine: Elon Musk: 'Mark my words — A.I. is far more dangerous than nukes'. CNBC, 2018.03.14. https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html; letöltés: 2020.04.15.

Hawking professzor is hasonló, bár akadémikusan kifinomultabb véleményt fogalmazott meg már jóval korábban, amikor rávilágított arra az evolúciós ellentmondásra, miszerint egy törékeny, halandó testű ember korlátolt mentális képességeivel hogyan lesz képes vetélkedni egy „fémszövetű" és sokkal gyorsabb elméjű és tanulékonyabb mesterséges intelligenciájú robottal, még akkor is, ha saját alkotása, teremtménye elméletileg még akár tökéletesebbé is válhat emberi alkotójánál?[42] Hawking ugyancsak osztotta a brit állami kommunikációs és hírszerzési szervezet (*GCHQ*) vezetőjének véleményét, illetve Sir Berners Lee és Vinton Cerf „internetalapítók" aggodalmait a világháló biztonsági kockázatairól, amely kiber bűnözők globális fórumává alakult, és akár eltörpülhet majd az elszabaduló vagy rosszra fordítható MI disztópikus világához képest.

A sci-fi amerikai nagymestere, Isaac Asimov és barátja, John W. Campbell által már 1940-ben megálmodott és megszövegezett humanista robotika törvényei[43] – miszerint a robot nem árthat embernek, illetve nem fordulhat az alkotója ellen – sajnálatosan csak könyvben létező szabályok, a valóságban teljességgel használhatatlanok és érvénytelenek. Az okos, önjáró katonai (harci) eszközök és robotok is – a legtöbb forradalmi műszaki tudományos újításhoz hasonlóan – elsődlegesen a katonai védelmi technológiai szektor termékei, amelyeket az amerikai, orosz, kínai vagy izraeli hadmérnökök már évtizedek óta nem békés célokra terveznek.

Putyin orosz elnöknek a 2017-es tudományos diákkonferencián tett futurisztikus kijelentése bejárta a világot, miszerint „*a 21. században a mesterséges intelligencia előtt óriási lehetőségek és veszélyforrások is állnak: ez a jövő nemcsak Oroszország, hanem minden állam számára (…) mindenesetre az az ország, amelynek sikerül uralnia az MI-t, uralhatja majd a nemzetközi kapcsolatok rendszerét is*."[44] Természetesen erre a kijelentésre sok államfő és kutató felkapta a fejét, figyelembe véve azokat a tényeket, hogy az Oroszországi Föderáció védelmi kiadásainak tételei között több különleges katonai projekt foglalkozik a robotika és a mesterséges intelligencia szakirányú felhasználási módjaival, habár a titkosítások miatt nincsenek megbízható adatok az orosz védelmi kutatások mibenlétéről és fejlettségéről. Ugyanakkor sokatmondó volt a FEDOR nevű, az űrhajózásban alkalmazandó emberszerű orosz robot bemutatása a sajtónak 2017-ben – revolverrel a kezében.[45]

---

[42] CELLAN-JONES, Rory: Stephen Hawking warns artificial intelligence could end mankind. BBC News, 2014.12.02. https://www.bbc.com/news/technology-30290540; letöltés: 2020.04.15.

[43] ASIMOV, Isaac: Én, a robot. Móra Ferenc Ifjúsági Könyvkiadó, Budapest, 1991.

[44] VINCENT, James: Putin says the nation that leads in AI 'will be the ruler of the world'. The Verge, 2017.09.04. https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world; letöltés: 2019.12.11.

[45] HART, Matthew: Russia's FEDOR Robot Can Dual Wield Pistols and May Be Going to Space. Nerdist, 2017.06.22. https://nerdist.com/article/russias-fedor-robot-can-dual-wield-pistols-and-may-be-going-to-space/; letöltés: 2019.03.08.

Az orosz MI- és robotikakutatásokhoz képest az amerikai és a kínai erőfeszítések valószínűleg jóval előrébb tartanak és magasabb szinten működnek, elsősorban a nyilvános eredmények és a befektetett anyagi erőforrások gigantikus mértékét tekintve. A kínai katonai technológiai és a tudományos ambíciók nem kisebb célra törnek, mint hogy 2030-ra Kína legyen a világ első számú és legfejlettebb MI-gyártója és -használója, megelőzve az Amerikai Egyesült Államokat. E grandiózus cél elérésére a kínaiak évente mintegy 7–10 milliárd dollárt költenek, és Peking mellett felépült a világ legnagyobb, 55 hektáros MI-kutatóközpontja több mint kétmilliárd dollárból, ahol több tízezer tudós, mérnök, informatikus a gépi tanulás (*deep/machine learning*) folyamatait, a mesterséges intelligencia, a felhőszolgáltatások (*cloud computing services*) és a nagybani adatelemzés (*big data*) alkalmazási módjait kutatja.[46] A kínai diktatórikus egypártrendszer politikai viszonyainak ismeretében komoly emberjogi és erkölcsi aggodalmakra ad okot az orwelli disztópiánál is durvább kínai egyéni értékelési, úgynevezett társadalmi kreditrendszer (*Social Credit System*) bevezetése 2014-ben.

A több mint fél milliárd köztéri kamera segítségével és MI-alapú *big data*-elemző algoritmusok felhasználásával az eddig elvégzett 450 millió egyéni értékelés alapján a rendszer 2020-ig már több mint 5 millió megbízhatatlan állam- és párthűségű kínai polgárt szűrt ki a Kínai Kommunista Párt érdekei és torz biztonsági megfontolásai mentén.[47] Az ő sorsuk igencsak kérdéses, illetve nehezen követhető, hiszen jogfosztott állampolgárokká váltak a világ legnépesebb és legnagyobb digitális kontroll alatt élő országában.

Teljességgel érthető, hogy az amerikai védelmi és nemzeti biztonsági stratégiában megfogalmazott célkitűzéseknek megfelelően nevesítik mind a kiberhadviselés és a mesterséges intelligencia alkalmazási módjainak fontosságát, mind az ellenséges állami és nem állami szintű szereplők törekvéseinek visszaszorítását és ellensúlyozását.[48] Az Amerikai Egyesült Államok – amely évente összességében mintegy 100 milliárd dollár körüli rekordnagyságú összegben folytat kiterjedt kutatásokat ebben a vonatkozásban[49] – Kínát tartja első számú gazdasági és katonai riválisának a szuperhatalmi státusért folytatott harcban, így a kiberhadviselés és a MI-kutatás terén is. Ezért az amerikai kormányzat minden lehetséges szövetségesével, elsősorban a NATO keretein belül keresi és elvárja a védelmi, kutatási együttműködést elsősorban Kína és másodsorban Oroszország, továbbá egyéb kisebb, de veszélyes állami tényezők, mint Irán vagy Észak-Korea kibertéri

---

[46] CYRANOVSKI, David: China enters the batte for AI talent. Nature, 2018.01.15. https://www.nature.com/articles/d41586-018-00604-6; letöltés: 2019.03.07.

[47] KOBIE, Nicole: The complicated Truth about China's credit system. Wired, 2019.06.07. https://www.wired.co.uk/article/china-social-credit-system-explained; letöltés: 2020.04.11.

[48] National Security Strategy of the United States of America. December 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; letöltés: 2020.03.07.
MATTIS, Jim: Summary of the 2018 National Defense Strategy of the United States of America. https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf; letöltés: 2020.03.07.

[49] The National Artificial Intelligence Research and Development Strategic Plan. NSTC NITRDS, October 2016. https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf; letöltés: 2020.02.28.

feltartóztatása (*cyber containment*) érdekében.[50] Chuck Hagel egykori amerikai védelmi miniszter a *Third Offset Strategy* című stratégiai védelmi dokumentumról szóló előadásában 2014-ben kifejtette, hogy a 21. század meghatározó védelmi technológiái között első helyen állnak az okoseszközös megoldások, különösképpen a mesterséges intelligenciát felölelő alkalmazások.[51] Értékelése szerint az Amerikai Egyesült Államok a világ legnagyobb tudományos technológiai kutatási szervezetén keresztül – amely nem más, mint a Pentagon intézményrendszere – pénzt és energiát nem kímélve folytat kutatásokat, hogy ezen a téren is megőrizze az amerikai stratégiai elsőséget és dominanciát.

A nagyhatalmi érdekérvényesítés területe természetesen kiterjed az új hadszíntérnek számító kibertérre, sőt 2019 óta immár a világűrre is,[52] akárcsak az ezekkel szoros összefüggésben alkalmazandó robotikai és mesterséges intelligenciát használó megoldások, eszközök vonatkozásában egyaránt.

Az új idők új gyakorlatának beszédes adata, hogy közel egy évtized alatt már több önjáró légi harci jármű (*Unmanned Combat Aerial Vehicle*), vagyis harci drón irányító „pilótája" (*Remotely Piloted Aircraft pilot*) van az amerikai légierőnek (közel 2000), mint valódi aktív állományú harci pilótája (1700).[53] A nevadai sivatag konténeres irányító központjaiból vezérelt amerikai „égi figyelő szemek" (*eyes in the sky*), mint az ikonikus *MQ–1 Predator, MQ–4 Global Hawk* vagy a rettegett *MQ–9 Reaper* önjáró repülőgépek a világ bármelyik pontján képesek megfigyelést vagy halálos (precíziós csapásmérő) beavatkozó akciókat végrehajtani. Az Obama és Trump elnök kormányzatainak 12 éve alatt ugyanis pontosan ez történt több mint kétezer alkalommal Jemen, Szomália, Pakisztán, Afganisztán, Irak és Szíria célpontjai felett.[54]

A légi és vízi drónok fejlődési trendjét, illetve az MI egyre erőteljesebb befolyását és komplexitását követve számos katonai elemző felveti annak a potenciális forgatókönyvnek a biztonsági és morális kockázatát, amikor egy felderítődrón gépi elméje által talált és kielemzett (emberi vagy tárgyi) célpontot a szintén „önjáró" csapásmérő légi vagy vízi drón megsemmisíti, tulajdonképpen emberi beavatkozás nélkül.[55] A vezetési-irányítási és a kommunikációs rendszer

---

[50] TADJDEH, Yasmin: DoD seeks alliance to counter China and Russia. National Defense, 2020.03.03. https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia; letöltés: 2020.04.16.

[51] HAGEL, Chuck: A Game-changing third offset strategy. War ont he Rocks, 2014.11.17. https://warontherocks.com/2014/11/a-game-changing-third-offset-strategy/; letöltés: 2019.11.15.

[52] 2019. december 20-án létrejött az űrhadszíntérért felelős US Space Force mint a hatodik önálló amerikai haderőnem.
About the United States Space Force.
https://www.spaceforce.mil/About-Us/Fact-Sheet; letöltés: 2020.04.15.

[53] PAWLYK, Oriana: Drone Milestone: More RPA Jobs Than Any Other Pilot Position. Military, 2017.03.08. https://www.military.com/daily-news/2017/03/08/drone-milestone-more-rpa-jobs-any-other-pilot-position.html; letöltés: 2019.11.25.

[54] PURKISS, Jessica – SERLE, Jack: Obama's covert drone war in numbers: ten times more strikes than Bush. The Bureau of Investigative Journalism, 2017.01.17.
https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush; letöltés: 2019.12.29.

[55] PORKOLÁB Imre: Digitális katona. TEDx Győr, 2019.
https://www.youtube.com/watch?v=jBWPTBjnZPI; letöltés: 2020.04.16.

(*command-control, communication*) jelenlegi felépítése révén és a parancsnoki lánc hierarchiáját ismerve ez napjainkban még elképzelhetetlen lenne, de a tendenciákat követve a közeljövőben már ezt egyáltalán nem lehet kizárni, ami jelentős paradigmaváltást eredményezhet a jogi és az erkölcsi rendszerekben egyaránt.

A tisztán katonai vonatkozásoktól eltekintve a robotok és az „önjáró" MI-alapú technológiai megoldások nyilvánvalóan társadalmi nyugtalanságot, ellenérzéseket és egyben politikai felfordulást is eredményezhetnek. Az első számú komoly aggodalomra okot adó tényező a gépi intelligencia és az emberszerű okosrobotok embert helyettesítő szerepe lehet. Amerikai munkaerőpiaci felmérések és szociológiai számítások szerint a fejlett világban (elsősorban az Amerikai Egyesült Államokban és Kanadában) a mai munkahelyek és szakmák harmadát fenyegeti megszűnés, illetve a csak középfokú végzettséggel rendelkező felnőtt munkavállalók közel 60%-át az állásvesztés a gépi kihelyettesítés, automatizálás miatt a közeljövőben, ami soha nem látott feszültségeket, konfliktusokat, gazdasági és politikai válságot is előidézhet majd.[56]

Nem meglepő módon az 19. század eleji híres-hírhedt angol gépromboló luddíták[57] követői két évszázad múltán újra népszerűségnek örvendenek, hiszen a neoluddita „*le az (energia)hálózatról, ki a modern társadalomból*" (*off-the-grid, into the woods*) mozgalom követői több százezer főt számlálhatnak, elsősorban az Amerikai Egyesült Államokban és Kanadában.[58]

A gyorsan változó és válságidőszakokkal tarkított világunkban az erőszakos technológiaellenes, akár anarcho-terrorista jellegű fellépések egyáltalán nem kizárható események és jelenségek lesznek a jövőben, ha a fenti pesszimista munkaerőpiaci és technológiai előrejelzések bekövetkeznek, továbbá ha nem születnek ezekre kielégítő válaszok a vezetők részéről.

A kockázatokról és a negatív vonatkozásokról nem elfeledkezve a modern technológiák és a MI-alapú alkalmazások azonban egyáltalán nem ördögtől való találmányok, hiszen optimista és technológiabarát értelmezésben – mint amit többek között a világhíres Michio Kaku amerikai japán asztrofizikus is képvisel – ezek a megoldások jelentősen jobbá és könnyebbé teszik életünket, segítenek az univerzum titkainak tudományos feltárásában, a nanotechnológiás gyógyászat és a számítástechnika egyéb vívmányairól már nem is beszélve.[59]

---

[56] WEBB, Michael: The Impact of Artificial Intelligence on the Labor Market. Stanford University, January 2020. pp. 21–25.
https://www.michaelwebb.co/webb_ai.pdf; letöltés: 2020.04.02.

[57] Ned Ludd (vagy Ludlam) példáját követve (ha valóban létezett?) 1811 és 1817 között álarcos férfiak csoportjai rendszeresen szétverték a textilipari fonó- és szövőgépeket Angliában.
ANDREWS, Evan: Who Were the Luddites? History, 2019.06.26.
https://www.history.com/news/who-were-the-luddites; letöltés: 2020.04.02.

[58] BARTLETT, John: Will 2018 be the year of the neo-luddite? The Guardian, 2018.03.04.
https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite; letöltés: 2020.04.16.

[59] KAKU, Michio: Az emberiség jövője. Akkord Kiadó, Budapest, 2019. pp. 110–126.

Összegzés

Összegzésképp megállapíthatjuk, hogy a 21. században a számítógépes rendszerek és az okoseszközök által uralt kibertér hadszíntérré alakult, valamint a digitális információk ugyancsak fegyverként alkalmazhatók állami és nem állami szereplők kezében politikai és egyéb célok érdekében. Az emberi elme számára felfoghatatlan mennyiségben és komplexitásban keletkező digitális információáradat a globális véleményformáló erővel rendelkező online közösségi médiaplatformokkal kiegészülve immár a társadalmi békét és a demokráciák működését is veszélyeztethetik. A könyv- és papíralapú írásos kommunikáció és tudásközvetítés világa egy új paradigmaváltás keretében elektronikussá, digitálissá és virtuálissá vált, ahogy azt Neumann János és Isaac Asimov is elképzelte. Az utóbbi három évtizedben az internetes tudáspiactér világa azonban nem igazán úgy alakult, ahogyan azt a tudós megálmodói jó szándékú, idealista módon elképzelték. A történelmi tapasztalat és az antropológiai pesszimizmus alapján kijelenthetjük, hogy az emberi alapvonásnak megfelelően szinte minden kimagasló technológiai találmányt védelmi, illetve támadó, pusztító célra is felhasználnak. Ebből a megfontolásból az értelmes robotok katonai, támadó célra történő felhasználása ellen több mint száz hírneves tudós, globális technológiai vállalkozó közös kiáltványban is felemelte szavát és aggodalmának adott hangot Elon Musk vezetésével.[60]

A fent említett tudós szakértők véleménye alapján és Hawking professzor aggodalmaiban osztozva kijelenthetjük, hogy az emberiség nincs felkészülve a „túlfejlett mesterséges intelligencia" jelentette kihívásokra, és főleg nem annak katonai célra történő alkalmazására, mert az még a nukleáris fegyvereknél is nagyobb, beláthatatlan kockázatokat hordozhat. Ezért szükség lenne arra, hogy az ENSZ közgyűlése is elítélő állásfoglalást hozzon a gyilkos robotok (*killbot)* rendszerbe állítása ellen. Ugyancsak ebben a vonatkozásban nagy sajtóvisszhangot kapott az amerikai védelmi minisztérium és a Google közös MI-alapú robottechnológia kutatási botránya a „gyilkos okos eszközök, robotok" morális és biztonsági kockázatai miatt.[61]

Amint az internet fentebb említett „alapítóatyái" is keserűen megjegyezték, az információs szupersztráda és a rá települő kibertér sajnálatosan többnyire negatív, káros és destruktív tartalmakkal töltődött fel, és a kiberbűnözés néhány év alatt az első számú és a legnagyobb kárt okozó bűncselekménytípussá vált a világon. Úgy tűnik, hogy a bűnözői csoportok még a pusztító koronavírus-járvány idején sem pihennek, még ebben az emberpróbáló időszakban is hihetetlen módon zsarolóvírus-programokkal támadják a biológiai kutatólaboratóriumokat és a kiemelt kórházakat.

---

[60] GIBBS, Samuel: Elon Musk leads 116 experts calling for outright ban of killer robots. The Guardian, 2017.08.20. https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war; letöltés: 2019.03.11.

[61] MCDONALD, Henry: Ex-Google worker fears 'killer robots' could cause mass atrocities. The Guardian, 2019.09.15. https://www.theguardian.com/technology/2019/sep/15/ex-google-worker-fears-killer-robots-cause-mass-atrocities; letöltés: 2019.12.04.

A digitális mediatizáció világméretű tendenciáját tekintve ugyancsak ellentmondásos a közösségi médiafelületek, a multimédiás információmegosztó alkalmazások dominanciája és az influenszerek befolyása, amelyek elsődleges információforrásokká váltak, akár az iskola és a családi közeg ellenében, a kiberkor szülöttei, a *Z* és *Alfa* generációk millióri számára.[62] A 2020-as amerikai elnökválasztást övező politikai botránysorozat is jelentős mértékben a kibertérben zajlott, és látványosan megmutatta a *bigtech,* vagyis a nagy információs technológiai cégóriások és a virtuális közösségi médiaplatformok hihetetlen mértékű befolyásoló erejét. Az IT-szféra és a különféle platformokat működtető cégek még 1996-ból származó laza, jelképes jogi szabályozása és önjáró hatalmi potenciálja valószínűleg még sokáig feszült jogi, politikai és társadalmi vitákat fog generálni nemcsak a szélsőségesen polarizálódott Amerikai Egyesült Államokban, hanem már világszerte is.

A kibertéri alkalmazások és a gépi intelligencia fejlődése megállíthatatlannak tűnik, amelyek *per se* már önmagukban hordoznak biztonsági kockázatokat, nem beszélve az eleve rossz szándékú technológiahasználókról, akiknek a számarányáról csak becslések, pontos adatok, kimutatások viszont nem igazán állnak rendelkezésre.

Nassim Taleb amerikai filozófusprofesszor és kockázatelemző értékelése szerint a technológiai komplexitás és a számtalan társadalmi és természeti változó, ismeretlen tényező következtében a jövőben egyre több ismeretlen, előre nem jelezhető világméretű válsággal (úgynevezett „fekete hattyú" jelenséggel), vagy lekicsinyelt és valószerűtlennek tartott biztonsági kihívással, problémával („szürke hattyú") kell majd megbirkóznunk.[63] Legyen az biológiai eredetű világjárvány (koronavírus), kisbolygó becsapódása, egy átfogó regionális vagy kontinentális áramszünet (amely mindössze három hét alatt középkori szintre vetné vissza világunkat), nem beszélve a pusztító kiberbűncselekmények sokkal valószerűbb elszaporodásáról vagy a mesterséges intelligencia közelgő szingularitásáról, illetve annak ma még beláthatatlan következményeiről.

Az egyik legnehezebb kihívás az emberiség számára a tanulmányban felvázolt technológiai csapdából való kiút és a felhasználóbarát megoldás megtalálása. Erre leegyszerűsítve két fő opció létezik. Egyrészt a technológiai hozzáférés korlátozása vagy teljes tiltása, ami diktatórikus és kontraproduktív rossz megoldási mód. A másik megoldás egy letisztult és szigorú jogi keretrendszer kidolgozása a kibertérben működő digitális médiaszolgáltatókra és a gépi intelligencia alkalmazásaira a felhasználók és az univerzális emberi értékek és érdekek védelmében. Ezt kiegészíthetné a kiberbiztonsági felvilágosítás a médiatudatos és a kritikai gondolkodásra, illetve felkészítés a netetikettre a formális iskolai és digitális oktatás keretei között.

---

[62] JARBOE, Greg: No Matter How You Define It, Generation Z Can't Live Without YouTube. Tubular, 2017.06.02.
https://tubularinsights.com/generation-z-youtube/; letöltés: 2020.04.16.

[63] TALEB, Nassim Nicholas: The Black Swan – The Impact of the Highly Improbable. Random House, New York, 2010. pp. 189–195.

Mindazonáltal megállapíthatjuk, hogy a kritikai és az analitikus gondolkodás oktatásával és gyakorlati alkalmazásával számos kiberbiztonsági és társadalmi probléma könnyen és hatékonyan orvosolható lehet a társadalom széles tömegei körében. Mindehhez szükséges a mértéktartó racionalitás alkalmazása a döntéshozók és a felhasználók részéről, valamint a célok (például humánus társadalmi, tudományos fejlődés) elkülönítése és nem felcserélése az eszközökkel (digitális technológiák, robotika, MI), hogy elkerülhetővé váljon Einstein és Bertrand Russell profetikus megállapítása, miszerint az okos technológia világa elbutult, elkényelmesedett emberiséghez vezethet.

FELHASZNÁLT IRODALOM

- About the United States Space Force. https://www.spaceforce.mil/About-Us/Fact-Sheet; letöltés: 2020.04.15.
- ANDREWS, Evan: Who Were the Luddites? History, 2019.06.26. https://www.history.com/news/who-were-the-luddites; letöltés: 2020.04.02.
- ASIMOV, Isaac: Én, a robot. Móra Ferenc Ifjúsági Könyvkiadó, Budapest, 1991.
- ASIMOV, Isaac: Visit to the World Fair of 2014. The New York Times, 1964.08.16. https://archive.nytimes.com/www.nytimes.com/books/97/03/23/lifetimes/asi-v-fair.html?src=longreads; letöltés: 2020.01.15.
- BARTLETT, John: Will 2018 be the year of the neo-luddite? The Guardian, 2018.03.04. https://www.theguardian.com/technology/2018/mar/04/will-2018-be-the-year-of-the-neo-luddite; letöltés: 2020.04.16.
- BLANK, Stephen: Web War I: Is Europe's First Information War a New Kind of War? Comparative Strategy, Volume 27, Issue 3, 2008. pp. 227–247. https://www.tandfonline.com/doi/full/10.1080/01495930802185312; letöltés: 2020.01.12.
- BRENT, Laura: NATO's role in cyberspace. NATO Review, 2019.02.12. https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html; letöltés: 2020.01.12.
- CELLAN-JONES, Rory: Stephen Hawking warns artificial intelligence could end mankind. BBC News, 2014.12.02. https://www.bbc.com/news/technology-30290540; letöltés: 2020.04.15.
- CHEN, Hsinchun: Dark Web: Exploring and Data Mining the Dark Side of the Web. Springer, New York, 2012.
- CIMPANU, Catalin: Hacker Guccifer, who exposed Clinton private email server, ready for US prison sentence. ZNet, 2018.10.24. https://www.zdnet.com/article/hacker-guccifer-who-exposed-clinton-private-email-server-ready-for-us-prison-sentence/; letöltés: 2020.04.14.

- CLARKE, Richard A. – KNAKE, Robert K.:
  Cyber War: The Next Threat to National Security and What to Do About It.
  Harper Collins, New York, 2010.
- CLEMENT, J.: Internet usage worldwide – statistics & facts. Statista, 2020.10.26.
  https://www.statista.com/topics/1145/internet-usage-worldwide/; letöltés: 2021.01.15.
- CLIFFORD, Catherine: Elon Musk: 'Mark my words — A.I. is far more dangerous than nukes'.
  CNBC, 2018.03.13.
  https://www.cnbc.com/2018/03/13/elon-musk-at-sxsw-a-i-is-more-dangerous-than-nuclear-weapons.html; letöltés: 2020.03.19.
- CYRANOVSKI, David: China enters the batte for AI talent. Nature, 2018.01.15.
  https://www.nature.com/articles/d41586-018-00604-6; letöltés: 2019.03.07.
- Data volume of global consumer IP traffic from 2017 to 2022 (in exabytes per month).
  Statista, 2020.02.28.
  https://www.statista.com/statistics/267202/global-data-volume-of-consumer-ip-traffic;
  letöltés: 2019.12.26.
- Directory of Mark Twain's maxims, quotations, and various opinions.
  http://www.twainquotes.com/Lies.html; letöltés: 2020.04.12.
- ESTEVES, Olivier: Bertrand Russell: the utilitarian pacifist.
  French Journal of British Studies, XX-1/2015.
  https://journals.openedition.org/rfcb/308; letöltés: 2020.03.25.
- Father of digital computer János Neumann was born 114 years ago.
  About Hungary, 2017.12.28.
  http://abouthungary.hu/news-in-brief/father-of-digital-computer-janos-neumann-was-born-114-years-ago/; letöltés: 2020.03.20.
- FORD, Martin: Robotok kora.
  HVG Könyvek, Budapest, 2017.
- GIBBS, Samuel: Elon Musk leads 116 experts calling for outright ban of killer robots.
  The Guardian, 2017.08.20.
  https://www.theguardian.com/technology/2017/aug/20/elon-musk-killer-robots-experts-outright-ban-lethal-autonomous-weapons-war; letöltés: 2019.03.11.
- GIBSON, William: Cyberspace. Technovelgy, 1982.
  http://www.technovelgy.com/ct/content.asp?Bnum=53; letöltés: 2019.12.25.
- GOMICHON, Maxime: Joseph Nye on Soft Power. E-International Relations, 2013.03.08.
  https://www.e-ir.info/2013/03/08/joseph-nye-on-soft-power/; letöltés: 2020.02.15.
- GONZALEZ, Jenipher Camino: Far-right terrorist ringleader found to be teenager in Estonia.
  Deutsche Welle. 2020.04.10.
  https://www.dw.com/en/far-right-terrorist-ringleader-found-to-be-teenager-in-estonia/a-53085442; letöltés: 2020.04.15.
- GREENWALD, Glen: A Snowden-ügy. HVG Könyvek, Budapest, 2014.
- HAGEL, Chuck: A Game-changing third offset strategy. War ont he Rocks, 2014.11.17.
  https://warontherocks.com/2014/11/a-game-changing-third-offset-strategy/;
  letöltés: 2019.11.15.

- HAIG Zsolt – KOVÁCS László: Fenyegetések a cybertérből.
  Nemzet és Biztonság, 2008. május. pp. 61–69.
  https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/1010/haig_zsolt__kovacs_laszlo-fenyegetesek_a_cyberterb__l.pdf?sequence=2;
  letöltés: 2019.12.20.
- HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus, Budapest, 2019.
- HARARI, Yuwal Noah: Homo Deus – A holnap rövid története.
  Animus Kiadó, Budapest, 2017.
- HART, Matthew:
  Russia's FEDOR Robot Can Dual Wield Pistols and May Be Going to Space.
  Nerdist, 2017.06.22.
  https://nerdist.com/article/russias-fedor-robot-can-dual-wield-pistols-and-may-be-going-to-space/; letöltés: 2019.03.08.
- HÄUßLER, Ulf:
  Cyber Security and Defence from the Perspective of Articles 4 and 5 of the NATO Treaty.
  International Cyber Security Legal & Policy Proceedings, 2010. 104-5.
  Cooperative Cyber Defence Center of Excellence, Tallinn, Estonia, 2010.
  https://infosec-journal.com/article/cyber-security-and-defence-perspective-articles-4-and-5-nato-treaty; letöltés: 2020.01.10.
- Internet of Things – number of connected devices worldwide 2015-2025.
  Statista, 2016.11.27.
  https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide;
  letöltés: 2020.01.28.
- JARBOE, Greg: No Matter How You Define It, Generation Z Can't Live Without YouTube.
  Tubular, 2017.06.02.
  https://tubularinsights.com/generation-z-youtube/; letöltés: 2020.04.16.
- KAKU, Michio: Az emberiség jövője. Akkord Kiadó, Budapest, 2019.
- KHANNA, Parag: Konnegtográfia – A globális civilizáció jövőjének feltérképezése.
  HVG Könyvek, Budapest, 2017.
- KOBIE, Nicole: The complicated Truth about China's credit system. Wired, 2019.06.07.
  https://www.wired.co.uk/article/china-social-credit-system-explained; letöltés: 2020.04.11.
- KREKÓ Péter: A vírusnál még a tömeggyilkos háttérhatalom is jobb. Index, 2020.04.12.
  https://index.hu/techtud/2020/04/12/tnt_osszeeskuves_kreko_peter_podcast/;
  letöltés: 2020.04.12.
- KREKÓ Péter: Tömegparanoia – Az összeesküvés-elméletek és álhírek szociálpszichológiája.
  Athaeneum, Budapest, 2018.
- LEIGH, David – HARDING, Luke:
  WikiLeaks-akták – Julian Assange háborúja a titkosítás ellen. Geopen, Budapest, 2011.
- MATTIS, Jim:
  Summary of the 2018 National Defense Strategy of the United States of America.
  https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf; letöltés: 2020.03.07.

- McDonald, Henry: Ex-Google worker fears ’killer robots’ could cause mass atrocities. The Guardian, 2019.09.15. https://www.theguardian.com/technology/2019/sep/15/ex-google-worker-fears-killer-robots-cause-mass-atrocities; letöltés: 2019.12.04.
- McLuhan, Marshall: The Gutenberg Galaxy. University of Toronto Press, Toronto, 2011.
- Morgan, Steve: Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Cybercrime Magazine, 2020.11.13. https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/; letöltés: 2021.01.15.
- National Security Strategy of the United States of America. December 2017. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf; letöltés: 2020.03.07.
- Norbert Wiener, American mathematician. Britannica. https://www.britannica.com/biography/Norbert-Wiener; letöltés: 2020.03.10.
- Pawlyk, Oriana: Drone Milestone: More RPA Jobs Than Any Other Pilot Position. Military, 2017.03.08. https://www.military.com/daily-news/2017/03/08/drone-milestone-more-rpa-jobs-any-other-pilot-position.html; letöltés: 2019.11.25.
- Porkoláb Imre: Digitális katona. TEDx Győr, 2019. https://www.youtube.com/watch?v=jBWPTBjnZPI; letöltés: 2020.04.16.
- Purkiss, Jessica – Serle, Jack: Obama’s covert drone war in numbers: ten times more strikes than Bush. The Bureau of Investigative Journalism, 2017.01.17. https://www.thebureauinvestigates.com/stories/2017-01-17/obamas-covert-drone-war-in-numbers-ten-times-more-strikes-than-bush; letöltés: 2019.12.29.
- Reedy, Christianna: Kurzweil Claims That the Singularity Will Happen by 2045. Futurism, 2017.10.05. https://futurism.com/kurzweil-claims-that-the-singularity-will-happen-by-2045; letöltés: 2020.04.15.
- Schaeffer, Katherine: Nearly three-in-ten Americans believe COVID-19 was made in a lab. Pew Research Center, 2020.04.08. https://www.pewresearch.org/fact-tank/2020/04/08/nearly-three-in-ten-americans-believe-covid-19-was-made-in-a-lab/; letöltés: 2020.04.12.
- Solon, Olivia: Tim Berners-Lee on the future of the web: ’The system is failing’. The Guardian, 2017.11.16. https://www.theguardian.com/technology/2017/nov/15/tim-berners-lee-world-wide-web-net-neutrality; letöltés: 2019.12.29.
- Szilárd Leó: A Petition to the President of the United States. 1945.07.17. http://www.dannen.com/decision/45-07-17.html; letöltés: 2020.04.12.
- Tadjdeh, Yasmin: DoD seeks alliance to counter China and Russia. National Defense, 2020.03.03. https://www.nationaldefensemagazine.org/articles/2020/3/3/algorithmic-warfare-dod-seeks-ai-alliance-to-counter-china-russia; letöltés: 2020.04.16.

- TALEB, Nassim Nicholas: The Black Swan – The Impact of the Highly Improbable. Random House, New York, 2010.
- TAPPER, James: Social media giants must tackle trolls or face charges – poll. The Guardian, 2020.04.04. https://www.theguardian.com/technology/2020/apr/04/social-media-giants-must-tackle-trolls-or-face-charges-poll; letöltés: 2020.04.15.
- The National Artificial Intelligence Research and Development Strategic Plan. NSTC NITRDS, October 2016. https://www.nitrd.gov/PUBS/national_ai_rd_strategic_plan.pdf; letöltés: 2020.02.28.
- VINCENT, James: Putin says the nation that leads in AI 'will be the ruler of the world'. The Verge, 2017.09.04. https://www.theverge.com/2017/9/4/16251226/russia-ai-putin-rule-the-world; letöltés: 2019.12.11.
- VINGE, Vernor: Technological Singularity. Whole Earth Review, January 2003. http://cmm.cenart.gob.mx/delanda/textos/tech_sing.pdf; letöltés: 2020.04.05.
- WALTZMAN, Rand: The Weaponization of Information – The Need for Cognitive Security. RAND Corporation, Santa Monica, CA, 2017.
- WEBB, Michael: The Impact of Artificial Intelligence on the Labor Market. Stanford University, January 2020. https://www.michaelwebb.co/webb_ai.pdf; letöltés: 2020.04.02.
- WERNER, Tom: The Cambridge Analytica Scandal. The Verge, 2018.04.10. https://www.theverge.com/2018/4/10/17165130/facebook-cambridge-analytica-scandal; letöltés: 2019.12.10.
- Who should get credit for the quote "data is the new oil"? https://www.quora.com/Who-should-get-credit-for-the-quote-data-is-the-new-oil; letöltés: 2020.01.30.

DR. NÉGYESI IMRE EZREDES – DR. ALBERT ÁGOTA – ÜVEGES ANDRÁS JÓZSEF SZÁZADOS

A FELHŐALKALMAZÁSOK ADATVÉDELMI KÉRDÉSEI A GDPR TÜKRÉBEN

Előszó

A GDPR – teljes nevén *Az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről*[1] – közvetlenül alkalmazandó uniós rendelet, amely deklarálja, hogy „*a természetes személyek személyes adataik kezelésével összefüggő védelme alapvető jog*”.[2] A gyors technológiai fejlődés és a globalizáció új kihívások elé állította a személyes adatok védelmét. A személyes adatok gyűjtése és megosztása jelentős mértékben megnőtt. A technológia a vállalkozások és a közhatalmi szervek számára tevékenységük folytatásához a személyes adatok felhasználását minden eddiginél nagyobb mértékben lehetővé teszi.

E fejlemények egy olyan szilárd és az eddiginél következetesebb uniós adatvédelmi keretet igényelnek, amelyet erős kikényszeríthetőség támogat, hiszen a bizalom megteremtése fontos a digitális gazdaság belső piaci fejlődéséhez.[3] „*A természetes személyek személyes adataik kezelésével összefüggő védelméhez kapcsolódó elvek és szabályok a természetes személyek állampolgárságától és lakóhelyétől függetlenül tiszteletben tartják e természetes személyek alapvető jogait és szabadságait, különösen, ami a személyes adataik védelméhez való jogukat illeti*”,[4] ennek keretrendszere először a 95/46/EK európai parlamenti és tanácsi irányelv[5] („adatvédelmi irányelv”) volt.

Az irányelv célja az volt, hogy „*harmonizálja az adatkezelési tevékenységek tekintetében a természetes személyek alapvető jogainak és szabadságainak védelmét, valamint, hogy biztosítsa a személyes adatok tagállamok közötti szabad áramlását*”,[6] az uniós tagállamok ezen irányelv rendelkezéseit implementálták saját jogrendszerünkbe.

---

1 Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679; letöltés: 2021.03.02.

2 GDPR (1) preambulumbekezdés.

3 GDPR (6)–(7) preambulumbekezdés.

4 GDPR (2) preambulumbekezdés.

5 Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Az Európai Unió Hivatalos Lapja, 1995.11.23. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:31995L0046&from=HU; letöltés: 2021.05.01.

6 GDPR (3) preambulumbekezdés.

Magyarországon ez a jogszabály az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (továbbiakban: Infotv.)[7] volt.

A GDPR az adatvédelmi irányelv utódaként 2016. május 24-én lépett hatályba, majd ezt követően egy kétéves felkészülési ciklus után, 2018. május 25-től már minden uniós tagállamban közvetlenül alkalmazandó rendelet. A GDPR-t kell alkalmazni:

- a személyes adatok Unióban tevékenységi hellyel rendelkező adatkezelők vagy adatfeldolgozók tevékenységeivel összefüggésben végzett kezelésére, függetlenül attól, hogy az adatkezelés az Unió területén történik vagy nem;
- az Unióban tartózkodó érintettek személyes adatainak az Unióban tevékenységi hellyel nem rendelkező adatkezelő vagy adatfeldolgozó által végzett kezelésére, ha az adatkezelési tevékenységek:
  - áruknak vagy szolgáltatásoknak az Unióban tartózkodó érintettek számára történő nyújtásához kapcsolódnak, függetlenül attól, hogy az érintettnek fizetnie kell-e azokért; vagy
  - az érintettek viselkedésének megfigyeléséhez kapcsolódnak, feltéve, hogy az Unió területén belül tanúsított viselkedésükről van szó;
- a személyes adatoknak nem az Unióban, hanem olyan helyen tevékenységi hellyel rendelkező adatkezelő által végzett kezelésére, ahol a nemzetközi közjog értelmében valamely tagállam joga alkalmazandó.[8]

Összegezve, ha az előbb említett elveket és célokat le akarjuk írni, akkor elmondható, hogy „*a GDPR felváltja a korábbi és a már meglehetősen idejét múlt 95/46/EK adatvédelmi irányelvet, és egy olyan összehangolt adatvédelmi jogszabályt jelent az uniós tagországoknak, amelynek alapvető célja az uniós polgárok személyes és magánadatainak védelme*”.[9]

Cikkünkben meg kívánjuk vizsgálni azt, hogy a felhőszolgáltatások esetében milyen követelményeket kell teljesíteniük a szereplőknek a GDPR-megfelelőség érdekében, illetve azt, hogy a GDPR milyen módon hatott a felhőszolgáltatók adatvédelmi gyakorlatára. A téma nagysága és komplexitása miatt a publikációban alapvetően a felhőtárhelyeken tárolt adatok kezelésének GDPR-megfelelőségét, valamint a felhőszolgáltatás (*cloud computing*) és a GDPR összefüggését vizsgáljuk. A cikkben kitérünk a jelenlegi felhőszolgáltatások adatbiztonsági, adatkezelési és adminisztrációs kérdéseire is.

---

[7] 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. https://net.jogtar.hu/jogszabaly?docid=a1100112.tv; letöltés: 2021.03.17.

[8] GDPR 3. cikk (1)–(3) bekezdés.

[9] KOVÁCS László: A kibertér védelme. Dialóg Campus Kiadó, Budapest, 2018. p. 257. https://www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf; letöltés: 2021.03.11.

Összefoglalva: a cikk célja, hogy megvizsgáljuk, a felhőszolgáltatás különböző adatkezelési tevékenységei (pl. az adattárolás és -felhasználás, valamint az adattörlés) milyen kihívásokkal szembesülnek a GDPR alapelveinek történő megfelelés során, továbbá kitekintésként megvizsgáljuk a jelenleg ismert problémákat és nyitott kérdéseket is.

A cikk esettanulmányokat és interjúkat, valamint elemzéseket is felhasznál, amelyben a kezelt adatok felhőben történő tárolásának problémáit, valamint a jelenlegi felhőszolgáltatások általános problémáit tárgyaljuk a GDPR tükrében. Emellett jelentősebb felhőszolgáltatók adatkezelési tájékoztatóit elemezve tárgyaljuk az ezekben a tájékoztatókban megfogalmazott garanciákat és biztosítékokat, illetve az esetlegesen felmerülő egyedi megoldásokat is.

Célunk, hogy az egyre gyorsabban terjedő felhőszolgáltatás biztonsági kockázatait a GDPR tükrében bemutassuk, valamint rámutassunk azokra a nyitott kérdésekre, amelyek az adatkezelők, adatfeldolgozók, valamint az érintettek oldaláról felmerülhetnek.

Probléma felvetése

Már GDPR előtt, azaz az adatvédelmi irányelv korszakában, a felhőszolgáltatások „hőskorában" is számos kérdés merült fel az informatikai végzettségű mérnökökben, illetve az adatvédelemmel foglalkozó jogászokban azzal kapcsolatban, hogy az adatvédelemre vonatkozó rendelkezéseket hogyan kell alkalmazni az egyes modern technológiák esetében. Véleményünk szerint napjainkban a GDPR egy olyan jogszabály, amely az érintettek jogait védi az adataikon keresztül, így nem várható el, hogy konkrét műszaki elgondolásokat tartalmazzon és konkrét „*to do*" listát bocsásson rendelkezésre. Az érintettek érdekei, valamint a technológiai újdonságok megkövetelik, hogy a rendelet alapvetően informatikai rendszerek tekintetében is tartalmazzon keretszabályokat. Ami azt jelenti, hogy legalább részlegesen kitöltve az 5. cikkben megfogalmazott alapelveket tartalmazza, és ezen kereteket értelmezze a 29. cikk szerinti Adatvédelmi Munkacsoport, illetve az Európai Adatvédelmi Testület iránymutatásai szerint. A felhőszolgáltatások esetében ilyen iránymutatás a 05/2012. számú vélemény a számítási felhőről (WP 196),[10] amely rögzíti az ilyen típusú szolgáltatások alapkövetelményeit, és amelynek javaslatai a GDPR rendelkezéseiben fellelhetők.

Bevezetés

Uniós keretek között először a 95/46/EK európai parlamenti és tanácsi irányelv („adatvédelmi irányelv") volt az a jogi aktus, amelynek célja az volt, hogy „*harmonizálja az adatkezelési tevékenységek tekintetében a természetes személyek alapvető jogainak és szabadságainak védelmét, valamint, hogy biztosítsa a személyes adatok tagállamok közötti szabad áramlását*".[11] Ezt az irányelvet helyezte hatályon kívül az Európai Parlament és a Tanács (EU) 2016/679 rendelete a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen

[10] Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing (WP 196). https://www.gpdp.gov.mo/uploadfile/others/wp196_en.pdf; letöltés: 2021.03.14.

[11] GDPR (3) preambulumbekezdés.

adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről. A rendelet 2016. május 24-én lépett hatályba, és kétéves türelmi időszak után 2018. május 25-től alkalmazandó közvetlenül minden uniós tagállamban. Hazánkban a GDPR rendelkezéseit az Infotv. 2. § (2) bekezdésében sorolja fel azokat a szakaszokat, amelyek az előbbiekben említett rendelettel együtt alkalmazandók.

A GDPR jelentősége, hogy a felhőszolgáltatásokat (vagyis az azokkal kapcsolatos adatvédelmi követelményeket) az Európai Unió szintjén immáron egységesen szabályozza, illetve az EGT-tagállamokon kívüli harmadik országba adattovábbítást csak abban az esetben minősíti jogszerűnek, ha e harmadik országban az adatkezelő, illetve a megbízása alapján eljáró adatfeldolgozó, azaz a felhőszolgáltató az uniós védelemmel „egyenszilárdságú" védelmet biztosít. Az adatkezelésekben érintettek érdekeit hangsúlyozó „harmadik ország" biztosította GDPR-ral egyenértékű adatvédelem követelménye azonban a felhőszolgáltatások dinamikus fejlődésének akadályát is jelenthetik, különös tekintettel az Európai Unió Bírósága által 2020 júliusában hozott ítéletre, amely megsemmisítette az Európa Unió és az Amerikai Egyesült Államok közötti GDPR-megfelelőségű adatáramlást biztosító adatvédelmi pajzsot.[12]

Nem közvetlenül ehhez csatlakozik, de mégis érinti ezt a kérdéskört Erdős Gabriella egyetemi adjunktus *Néhány gondolat az adatbiztonságról és adatkezelésről az okos alkalmazások területén* című cikke. A cikk 6. pontja a GDPR, a PSD2[13,14] és az e-Privacy irányelv viszonyát vizsgálja röviden.[15] Ebben a tanulmányban a szerző jól láthatóan leírja azt, hogy van két olyan terület is, amely szorosan összefügg és látszólag akár akadályozhatja is az adatvédelemi törekvéseket. „*Az egyik a digitális közös piac megteremtése, amely többek között a digitális tartalmakhoz való könnyebb hozzáférést, a geo-blokkolás megakadályozását tűzi ki célul*", valamint a „*másik olyan terület, amely szorosan kapcsolódik az adatvédelemhez, a magánélet tiszteletben tartása*".[16]

Fontos megvizsgálni azt is, hogy alapvetően a felhőszolgáltatások mely típusaival foglalkozunk a cikkben, különös tekintettel a felhőszolgáltatók felelősségére.

---

[12] 91/20. sz. Sajtóközlemény. Európai Unió Bírósága, Luxembourg, 2020. július 16. – A C-311/18. sz. ügyben hozott ítélet. Data Protection Commissioner kontra Facebook Ireland és Schrems. A Bíróság érvénytelennek nyilvánítja az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló 2016/1250 határozatot.
https://naih.hu/kozlemenyek/EUB_sajtokozlemeny_cp200091hu.pdf; letöltés: 2021.03.15.

[13] Payment Service Directive – A PSD2 az Európai Unió második pénzforgalmi irányelve, amelynek célja, hogy optimális környezetet teremtsen a digitális pénzügyi szolgáltatások fejlődéséhez és támogassa új szolgáltatók belépését a pénzügyi szektorba (PSD, 2007/64/EC).

[14] MOZDZYNSKI, Daniel: The Conceptions of new payment methods based on revised payment services directive (PSD2), Information Systems in Management, Volume 6, Number 1, 2017. p. 51.
https://www.researchgate.net/publication/317841044_THE_CONCEPTIONS_OF_NEW_PAYMENT_METHODS_BASED_ON_REVISED_PAYMENT_SERVICES_DIRECTIVE_PSD2; letöltés: 2021.03.17.

[15] e-Privacy Regulation. Statement 03/2021 on the ePrivacy Regulation, European Data Protection Board, 2021.03.09.
https://edpb.europa.eu/our-work-tools/our-documents/topic/e-privacy-regulation_hu; letöltés: 2021.03.15.

[16] ERDŐS Gabriella: Néhány gondolat az adatbiztonságról és adatkezelésről az okos alkalmazások területén. Corvinus Law Papers, CLP 2/2020. p. 6.
http://unipub.lib.uni-corvinus.hu/5685/1/CLP_202002.pdf; letöltés: 2021.03.11.

A felhőszolgáltatásokat a tartalmuk (kategóriája) alapján több csoportra osztjuk: szoftver mint szolgáltatás,[17] platform mint szolgáltatás,[18] infrastruktúra (kiszervezett kapacitás[19]) mint szolgáltatás, tárolás mint szolgáltatás.[20] De ezek mellett akár projekt (művelet vagy küldetés[21]) szintjén is lehet már felhőszolgáltatásokat alkalmazni, például felhőalapú pilóta nélküli repülőrendszer (UAS[22]) megvalósítása vonatkozásában. Ez utóbbi témában Vránics Dávid Ferenc és Palik Mátyás készített egy összefoglaló művet, amelyben már a megvalósítás gyakorlati kérdéskörét is tárgyalják.[23]

Más rendszer alapján csoportosítva a felhőszolgáltatásokat feloszthatjuk publikus és privát felhőszolgáltatásra is. A publikus ez esetben nem azt jelenti, hogy adataink nyilvánosak lesznek bárki számára, hanem az erőforrásokat és adott szolgáltatásokat bárki elérheti, illetve megrendelheti, míg a privát felhőrendszer esetében egy szervezet több telephelyéről (gyárából, irodájából stb.) csatlakoznak egy egységesített központi architektúrába.[24] A gyakorlatban ez egy olyan adatközpont, amelyet az adott vállalat üzemeltet. Természetesen mindkét rendszer alapvetően hálózatfüggő.[25]

Sok felhőszolgáltatást igénybe vevő szereplő úgy gondolja, az „ő felhője" nem tartalmaz személyes adatot, ezért nem vonatkozik rá a GDPR, figyelmen kívül hagyva azt a tényt, hogy a jogosultságokkal, a hozzáféréssel, valamint a naplózással kapcsolatos adatok már önmagukban személyes adatok lehetnek.

A GDPR szerint személyes adat az azonosított vagy azonosítható természetes személyre („érintettre") vonatkozó bármely információ. Azonosítható az a természetes személy, aki közvetlen vagy közvetett módon, különösen valamely azonosító, például név, szám, helymeghatározó adat,[26] online azonosító[27] alapján beazonosítható.[28]

---

[17] A felhőszolgáltató a szoftvert nyújtja interneten keresztül („SaaS").

[18] A felhőszolgáltató az alkalmazás üzemeltetéséhez szükséges környezetet biztosítja („PaaS").

[19] A felhőszolgáltató az infrastruktúrát (virtuális gépet és más erőforrásokat) biztosítja, az operációs rendszert és az alkalmazásokat a felhasználó működteti („IaaS").

[20] Storage as a Service (STaaS).

[21] Mission as a Service.

[22] Unmanned Aircraft Systems.

[23] VRÁNICS Dávid Ferenc – PALIK Mátyás: Mission as a Service – Egy felhőalapú UAS megvalósítása. Repüléstudományi Közlemények, 31. évfolyam 3. szám, 2019. pp. 153–167. https://folyoirat.ludovika.hu/index.php/reptudkoz/article/view/265/2801; letöltés: 2021.03.10.

[24] What is a private cloud? Microsoft Azure. https://azure.microsoft.com/en-us/overview/what-is-a-private-cloud/; letöltés: 2021.03.04.

[25] Mi a nyilvános, magán- és hibrid felhő? Bevezetés a felhőszolgáltatások üzembe helyezési lehetőségeibe. https://azure.microsoft.com/hu-hu/overview/what-are-private-public-hybrid-clouds/#faq; letöltés: 2021.01.19.

[26] Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv"). Official Journal L 201, 31/07/2002. pp. 0037–0047. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32002L0058&from=ES; letöltés: 2021.03.04.
Az Európai Parlament és a Tanács 2006/2004/EK rendelete (2004. október 27.) a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről („Rendelet a fogyasztóvédelmi együttműködésről"). Az Európai Unió Hivatalos Lapja, 2004.12.09. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32004R2006&from=ES; letöltés: 2021.03.12.

[27] Például vezetéknév.utónév@szervezet.com típusú e-mail-címek, sütiazonosító, IP-cím.

[28] GDPR 4. cikk 1. pont.

A természetes személyek összefüggésbe hozhatók az általuk használt alkalmazások, eszközök és protokollok által rendelkezésre bocsátott online azonosítókkal, például IP-címekkel[29] és sütiazonosítókkal,[30] ezáltal olyan nyomok keletkezhetnek, amelyek egyedi azonosítókkal és a szerverek által fogadott egyéb információkkal összekapcsolva felhasználhatók a természetes személyes profiljának létrehozására és az adott személy azonosítására.[31] Az adatok tárolásának, módosításának vagy törlésének ellenőrzését megkönnyítő naplóadatok szintén személyes adatnak minősülhetnek az adott adatkezelési műveletet kezdeményező személy vonatkozásában.[32]

„*Az adatvédelem elveit minden azonosított vagy azonosítható természetes személyre vonatkozó információ esetében alkalmazni kell. Az álnevesített személyes adatok, amelyeket további információ felhasználásával valamely természetes személlyel kapcsolatba lehet hozni, azonosítható természetes személyre vonatkozó adatnak kell tekinteni. Valamely természetes személy azonosíthatóságának meghatározásakor minden olyan módszert figyelembe kell venni – ideértve például a megjelölést –, amelyről észszerűen feltételezhető, hogy az adatkezelő vagy más személy a természetes személy közvetlen vagy közvetett azonosítására felhasználhatja. Annak meghatározásakor, hogy mely eszközökről feltételezhető észszerűen, hogy egy adott természetes személy azonosítására fogják felhasználni, az összes objektív tényezőt figyelembe kell venni, így például az azonosítás költségeit és időigényét, számításba véve az adatkezeléskor rendelkezésre álló technológiákat, és a technológia fejlődését. Az adatvédelem elveit ennek megfelelően az anonim információkra nem kell alkalmazni, nevezetesen olyan információkra, amelyek nem azonosított vagy azonosítható természetes személyre vonatkoznak, valamint az olyan személyes adatokra, amelyeket olyan módon anonimizáltak, amelynek következtében az érintett nem vagy többé nem azonosítható.*”[33]

Sok szereplő nincs tisztában az adatkezelés sokrétűségével, ezért úgy gondolják, hogy valójában nem részesei az adatkezelési folyamatoknak („nem látnak bele az adatokba”). A GDPR azonban felsorolja az adatkezelési műveleteket, miszerint adatkezelés a személyes adatokon vagy adatállományokon automatizált vagy nem automatizált módon végzett bármely művelet vagy műveletek összessége, így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés, továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés.[34] E felsorolás alapján egy felhőszolgáltató már azzal megvalósítja az adatkezelést, ha semmi mást nem csinál, csak adatot tárol.

---

[29] Egyedi hálózati azonosító, amelyet az internetprotokoll segítségével kommunikáló számítógépek egymás azonosítására használnak.

[30] Ha a böngésző visszaküld egy sütit, akkor a kiszolgálónak lehetősége van összekapcsolni az aktuális kérést a korábbiakkal. Leggyakrabban egy adott weboldal regisztrált felhasználóinak azonosítására, „bevásárlókosár” nyilvántartására vagy látogatók nyomon követésére használják.

[31] GDPR (30) preambulumbekezdés.

[32] WP 196, 2. pont.

[33] GDPR (26) preambulumbekezdés.

[34] GDPR 4. cikk 2. pont.

A cikkben megpróbálunk fókuszálni a felhőszolgáltatás kihívásaival, így például az adatok tárolásával és az adattörléssel kapcsolatos kérdéskörökre, valamint a felmerülő problémákra. A cikkben felhasznált információk egy része olyan szakemberektől származik, akik alapvetően a felhőszolgáltatások informatikai adatbiztonságával és GDPR-megfelelőséggel foglalkoznak. Az interjúk alanyai között adminisztrátor, általános értelemben vett felhasználó, valamint technológiai igazgató is szerepel, de a levont következtetések nem reprezentatív értékűek.

Korábbi kutatások

A felhőszolgáltatás témában számos nemzetközi és hazai publikáció készült, amelyek – többségében – arra összpontosítanak, hogy a felhőszolgáltatásnak milyen kritériumoknak kell megfelelnie.

A felhőszolgáltatások és a GDPR vonatkozásában is készült már egy tanulmány, amely részletesen tárgyalja a felhasználók adatainak felhőszolgáltatás alatti mozgatását. Ebben a tanulmányban nemcsak kizárólag az adatmozgatással kapcsolatos kérdéseket vizsgálják, hanem azt is, hogy a felhőszolgáltatásnak a GDPR alapján milyen kritériumoknak kell megfelelnie. A jelentés konklúziója, hogy ha a felhőszolgáltatók továbbra is versenyképes termékeket kívánnak nyújtani mind az egyéni, mind a vállalati ügyfeleiknek, akkor az adatok hordozhatóságához adatkezelőként és adatfeldolgozóként is meg kell felelniük a GDPR követelményeinek. Emellett valamilyen új követelmény teljesítése érdekében a szolgáltatásnak rugalmasnak kell lennie. Mivel maga a tanulmány az adathordozhatóságot vizsgálja, így a cikk fókuszában a GDPR 20 cikke áll.[35]

A blokklánc-rendszerek viszonylatában egy forradalmian új koncepció is felmerült Simon Farshid, Andreas Reitz és Peter Roßbach cikkében. A cikk szerint az új blokklánc-koncepcióban a blokkokon belüli régi adatok törölhetőek. Ennek következtében a blokklánc segítségével lehetőség nyílna olyan okosszerződést készíteni, amely műszakilag is szavatolja a törlést például a felhőszolgáltatás igénybevétele során magából a felhőből. Azaz a felhasználó, aki a szerződő fél, egy beküldött kódsor vagy parancssor segítségével a blokkokból kitörli régi adatait. A cikk alapján egy ilyen blokkláncprototípus-algoritmus segítségével feloldanák a felhőszolgáltatás és a GDPR-megfelelőség egyik fontosabb kérdését is. Véleményünk szerint az elgondolás új megvilágításba helyezi a blokklánc felhasználhatóságát, viszont szembemegy a blokklánc egyik alapelvével, mégpedig azzal, hogy a rendszerben visszamenőleg (függetlenül az adatfajtától) nem lehet törölni.[36]

Dr. Frivaldszky Gáspár ügyvéd, az Informatikai Vállalkozások Szövetsége és az International Association of Privacy Professionals tagja internetes cikkében már rávilágít a GDPR és a felhőszolgáltatás tágabb értelemben vett problémáira, illetve az

[35] EU általános adatvédelmi rendelet: Az adathordozhatósághoz való jog. https://www.privacy-regulation.eu/hu/20.htm; letöltés: 2021.01.19.

[36] FARSHID, Simon – REITZ, Andreas – ROßBACH, Peter: Design of a forgetting blockchain – A possible way to accomplish GDPR compatibility. Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019. p. 7088. https://core.ac.uk/download/pdf/211327966.pdf; letöltés: 2021.03.04.

ágazat szempontjából a jogi és a technológiai viszonyt is említi. A cikkben jól megfogalmazza azt a problémát, amivel napjainkban találkozhatunk, miszerint „*Az informatikusoknak a felhőszolgáltatásokkal kapcsolatos kérdések túl jogiak, a jogászoknak túl informatikaiak. Az átlag cégvezető meg mind a jogi, mind az informatikai problémáktól idegenkedik. Ez a szakadék a rohamos ütemű technikai fejlődéssel csak nőni látszik*.”[37] A fentiek mellett tanulmány készült a könyvtárak és a levéltárak vonatkozásában is.[38]

Az előbbiekben említett problémát alátámasztja az, hogy az interjúk során a műszaki területen dolgozó felhőszolgáltatási adminisztrátorok inkább látták adminisztrációs tehernek a GDPR-szabályozást, mint tényleges olyan jogi anyagnak, amely az adatok és ezen keresztül az érintettek védelmét biztosítja.

A felhő a GDPR előtt

A felhőszolgáltatásokkal kapcsolatos adatvédelmi elvárások

A 95/46/EK európai parlamenti és tanácsi irányelv 29. cikke szerinti Adatvédelmi Munkacsoport 2012 júliusában elfogadott, már említett 05/2012. sz. véleményében (WP 196) fektette le a felhőszolgáltatásokkal kapcsolatos adatvédelmi elvárások sarokpontjait. Eszerint a felhőszolgáltató igénybe vevője és a felhőszolgáltatás biztosítójának kapcsolata alapvetően adatkezelő–adatfeldolgozó kapcsolat, amelyben a szolgáltatást igénybe vevő határozza meg az adatkezelés célját, és ő viseli a felelősséget is az adatkezelés tekintetében. Természetesen előfordulhatnak olyan esetek, amikor a szolgáltatást igénybe vevő már maga is adatfeldolgozó, valamint a felhőszolgáltató is adatkezelővé válhat, amennyiben ő határozza meg az adatkezelés célját.

A vélemény kiemelt fontossággal kezeli a felhőszolgáltatásokkal kapcsolatos kockázatokat, amely kockázatok többsége két kategóriába sorolhatók: egyrészt az adatok feletti ellenőrzés hiányából fakadnak, másrészt magával az adatkezelési műveletekkel kapcsolatos elégtelen információk (azaz az átláthatóság hiánya) miatt számottevőek.

A felhőszolgáltatás igénybe vevője – a szolgáltatás természetéből adódóan – úgy bocsátja az általa kezelt adatokat a szolgáltató által kezelt rendszerek rendelkezésére, hogy többé már nem gyakorol kizárólagos ellenőrzést felettük, „*és nem tudja megtenni az adatok rendelkezésre állása, sértetlensége és bizalmas természete, átláthatósága, elkülönítése, az azokba történő beavatkozási lehetősége és az adatok hordozhatósága érdekében szükséges technikai és szervezési intézkedéseket*”.[39]

---

[37] FRIVALDSZKY Gáspár: A felhőszolgáltatások adatvédelmi kérdései – Az uniós adatvédelmi rendelet (GDPR) fényében. https://adatvedelmi.hu/felhoszolgaltatasok-adatvedelmi-kerdesei-az-unios-adatvedelmi-rendelet-gdpr-fenyeben/; letöltés: 2020.12.23.

[38] TÓTH Fanni: A GDPR-ról – különös tekintettel a könyvtárakra és levéltárakra. Debreceni Jogi Műhely, XV. évfolyam, 1–2. szám, 2018.07.08. pp. 63–75. https://ojs.lib.unideb.hu/DJM/article/view/6911/6360; letöltés: 2021.01.17.

[39] WP 196, 2. pont.

A rendelkezésre állás hiánya bekövetkezhet például a különböző felhőalapú rendszerek közötti átjárhatóság hiánya miatt (*vendor lock-in*[40]), a bizalmasság pedig sérülhet például a közvetlenül a szolgáltatóhoz intézett bűnüldözési megkeresések következtében. Ez utóbbi esetben az is előfordulhat, hogy a felhőben tárolt személyes adatokat úgy hozhatja a szolgáltató (akár harmadik országbeli) bűnüldöző szervek tudomására, hogy annak nincs uniós jogalapja. A beavatkozási lehetőség hiánya is hordozhat kockázatot, mivel gyakran olyan dinamikusak, bonyolultak a szolgáltatási láncok (pl. a felhőszolgáltató az általa kínált szolgáltatást más szolgáltatóktól igénybe vett szolgáltatások időben változó kombinálásával hozza létre), hogy azok folyamatosan módosulhatnak a szolgáltatásra vonatkozó szerződés során. Az ilyen folyamatosan változó környezetben az érintettek jogainak érvényesítése nem mindig maradéktalan (pl. törlési igény), és az elkülönítés hiánya is hordozhat kockázatokat, aminek eredményeként a szolgáltató (illetve annak rendszergazdái) különböző igénybe vevőktől származó adatokat kapcsolhat össze.

Az átláthatóság hiánya azt eredményezheti, hogy az adatkezelők nincsenek tisztában azzal, hogy nem egy adatfeldolgozóval, hanem akár az adatfeldolgozók többszintű, egymásnak alárendelt láncolatával állnak szemben, és az sem mindig világos, az adatokat a világ mely pontján és milyen joghatóság alatt tárolják.

A vélemény konkrét ajánlásokat fogalmaz meg, amelyek már előrevetítik a GDPR későbbi rendelkezéseit is, például:

– A felhőszolgáltatást igénybe vevő felelősséggel tartozik a felhőszolgáltató tevékenységéért, ezért olyan szolgáltatót kell választani, amely megfelel az uniós jogszabályi követelményeknek.

– A szolgáltató és a szolgáltatást igénybe vevő közötti kapcsolatot – különös tekintettel az általuk viselt felelősségekre – írásba kell foglalni, valamint a szolgáltatónak az alvállalkozóival kötött szerződéseiben ugyanezen felelősségeknek meg kell jelennie.

– Alapvető követelmény az adatvédelem alapelveinek betartása, így különösen az átláthatóság elvének való megfelelés. A szolgáltatóknak „*a szerződés megtárgyalása során tájékoztatniuk kell az igénybevevőket szolgáltatásuk valamennyi (adatvédelmi szempontból) releváns tényezőjéről; az igénybevevőknek különösen az alábbiakról kell tájékoztatást kapniuk: a megfelelő számításifelhő-szolgáltatás nyújtásához hozzájáruló összes alvállalkozó, valamint az összes olyan helyszín, ahol a szolgáltató és/vagy az alvállalkozói adatokat tárolhatnak vagy dolgozhatnak fel (…); érdemi tájékoztatást kell nyújtani az igénybevevő számára a szolgáltató által foganatosított technikai és szervezési intézkedésekről; az igénybevevőnek helyes módszerként tájékoztatnia kell az érintetteket a számításifelhő-szolgáltatóról és (adott esetben) az összes alvállalkozóról, valamint az olyan helyszínekről, ahol a szolgáltató és/vagy az alvállalkozói adatokat tárolhatnak vagy dolgozhatnak fel.*”[41]

---

[40] Terjesztőtől való függés – Amikor a felhasználó függ egy gyártó vagy szolgáltató termékeitől vagy szolgáltatásoktól. Ezt csak nagyobb költségek árán tudja a későbbiekben kiváltani. A monopóliumhelyzettel szembeni bizalom elvesztését okozhatják azok a költségek, amelyek akadályt hoznak létre egy új termékkel bevezetésével szemben.

[41] WP 196, 4.1. pont.

– Követelmény a célhoz kötöttség elve: „*az igénybevevőnek gondoskodnia kell a célmeghatározás és -korlátozás elveinek betartásáról, valamint arról, hogy a szolgáltató és az alvállalkozók további célokból ne dolgozzanak fel adatokat. Az erre vonatkozó kötelezettségvállalásokat bele kell foglalni a megfelelő szerződéses intézkedésekbe (a technikai és szervezési biztosítékokat is beleértve).*”[42]

– A felhőszolgáltatás igénybe vevője felel azért, hogy a szolgáltató (és adott esetben az alvállalkozói) töröljék a tárolt személyes adatokat akkor, amikor a konkrét célok érdekében már nincs azokra szükség. Ennek teljesítése érdekében a feleknek az általuk kötött szerződésben biztonságos törlési mechanizmusokat (megsemmisítés, demagnetizáció, felülírás) kell előírni.

– Olyan biztosítékok kikötése, mint például az adatokhoz hozzáférési jogosultságok szigorú korlátozása, titoktartás, a szolgáltatás igénybe vevője részéről a felhőszolgáltató alvállalkozók igénybevételéhez előzetes írásbeli hozzájárulás.

– A szerződésnek azt is elő kell írnia a felhőszolgáltató számára, hogy „*küldjön értesítést a személyes adatok közlésére vonatkozó, bűnüldöző hatóságoktól érkező, jogilag kötelező megkeresésekről, kivéve, amennyiben az ilyen közlés egyéb okból tilos*”,[43] valamint azt, hogy a szolgáltatást igénybe vevő jogi biztosítékot kapjon arra, hogy a felhőszolgáltató el fogja utasítani a jogilag nem kötelező közlés iránti kérelmeket.

– A szolgáltatás igénybe vevőjének gondoskodnia kell arról, hogy a szolgáltató köteles legyen együttműködni az alábbiak tekintetében: az adatkezelési műveletek nyomon követése, az érintett adat-hozzáférési/kiigazítási/törlési jogának gyakorlása, valamint (adott esetben) a szolgáltatás igénybe vevőjének értesítése az adatait érintő adatsértésekről.

– A határon átnyúló adattovábbítások során a felhőszolgáltatás igénybe vevőjének ellenőriznie kell, hogy a szolgáltató garantálni tudja-e a határon átnyúló adattovábbítások jogszerűségét (pl. adekvát határozat, általános szerződéses feltételek, kötelező erejű vállalati szabályok), és lehetőség szerint korlátozhatja-e az igénybe vevő által kiválasztott országokba irányuló adattovábbításokat.

– A felhőszolgáltatás igénybe vevőjének elő kell írnia, hogy a felhőszolgáltató és alvállalkozói végezzék el az adatfeldolgozási műveletek naplózását és az igénybe vevőt fel kell jogosítani az ilyen adatfeldolgozási műveletek ellenőrzésére. A vélemény szerint az adatkezelő által választott külső ellenőrzés és tanúsítás is elfogadható lehet, amennyiben az garantálja a teljes átláthatóságot.

– A technikai és a szervezési intézkedéseknek arra kell irányulniuk, hogy orvosolják a felhőalapú számítástechnikai környezet egyik jellegzetességét, az ellenőrzés és az információk hiánya miatt fellépő kockázatokat. A technikai intézkedések közé olyan intézkedések tartoznak, amelyek célja a rendelkezésre állás, sértetlenség, bizalmas jelleg, elkülönítés, beavatkozási lehetőség és hordozhatóság biztosítása, a szervezeti intézkedések pedig az átláthatóság érvényre juttatására összpontosítanak.

---

[42] WP 196, 4.1. pont.
[43] WP 196, 4.1. pont.

Kockázatelemzés mint követelmény

Kiemelendő, hogy a vélemény szerint a felhőszolgáltatást igénybe venni tervező szervezeteknek (szektortól függetlenül) első lépésként átfogó és alapos kockázatelemzést kell végezniük, a szolgáltatóknak pedig minden olyan információt rendelkezésre kell bocsátaniuk, amelyek segítségével ezt a kockázatelemzést el lehet végezni. A 29. cikk szerinti Adatvédelmi Munkacsoport szerint a szolgáltatást igénybe vevő csak úgy vehet igénybe felhőszolgáltatást, hogy annak igénybevétele előtt megfelelő kockázatelemzést végzett, amely kiterjedt az adatfeldolgozást végző szervezetek földrajzi helyére, az adatvédelmi kockázatok, valamint a szolgáltatás igénybevételéből fakadó előnyök elemzésére. A vélemény idézi a berlini Nemzetközi Távközlési Adatvédelmi Munkacsoport 2012 áprilisában elfogadott Sopoti Nyilatkozatát,[44] amely kimondja, hogy a felhőszolgáltatás „*nem eredményezheti az adatvédelmi normák csökkentését a hagyományos adatfeldolgozáshoz képest*”.[45]

A felhőszolgáltatások piacán gyakori, hogy a szolgáltatás igénybe vevőjének piaci súlya elhanyagolható, és nem rendelkezik valódi mozgástérrel ahhoz, hogy ráhatása legyen a szolgáltatási szerződés lényegi tartalmára, de mivel ő mint adatkezelő dönt egyes adatkezeléseinek felhőszolgáltatóhoz történő kihelyezéséről, ezért teljes mértékben felelős a szolgáltató jogszerű működéséért. A 29. cikk szerinti Adatvédelmi Munkacsoport az 1/2010. számú véleményében is kifejtette, hogy „*egy kis adatkezelő és a nagy szolgáltatók alkupozíciójának egyenlőtlensége nem indokolhatja, hogy az adatkezelő olyan kikötéseket és szerződési feltételeket fogadjon el, amelyek nem felelnek meg az adatvédelmi jognak*”[46] – azaz az adatkezelőnek (a szervezetnek) olyan felhőszolgáltatót kell választania,[47] amely garantálja az adatvédelemre vonatkozó jogszabályok betartását.

A kockázatértékeléshez az EU Kiberbiztonsági Ügynöksége (ENISA)[48] 2009-ben megjelent kiadványa[49] nyújt segítséget a szervezetek számára. Emellett a kis- és középméretű vállalkozások (kkv) részére 2015-ben adtak ki hasonló iránymutatást segítségként a témában.[50] A 2009-es dokumentum ellenőrzőlistái abban kívánnak segítséget nyújtani, hogy a felhőszolgáltatást igénybe venni kívánók értékelni tudják a szolgáltatás bevezetésének kockázatát, össze tudják hasonlítani a

---

[44] Working Paper on Cloud Computing – Privacy and data protection issues – „Sopot Memorandum”. International Working Group on Data Protection in Telecommunications, 51st meeting, 23-24 April 2012, Sopot (Poland).
http://germanitlaw.com/wp-content/uploads/2012/04/Sopot-Memorandum1.pdf; letöltés: 2021.03.15.
https://naih.hu/files/IWGDPT---Sopot-Memorandum--HUN.pdf; letöltés: 2021.03.15.

[45] WP 196, 2. pont.

[46] 1/2010. számú vélemény az „adatkezelő” és az „adatfeldolgozó” fogalmáról (WP 169). A 29. cikk szerinti Adatvédelmi Munkacsoport, 2010.02.16.
http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_hu.pdf; letöltés: 2021.03.15.

[47] Ilyen szolgáltatókat tömörít például a CISPE.
CISPE.cloud: Public Register.
https://cispe.cloud/publicregister/; letöltés: 2021.03.15.

[48] European Union Agency for Cybersecurity (ENISA).
https://europa.eu/european-union/about-eu/agencies/enisa_en; letöltés: 2021.03.08.

[49] Cloud Computing Security Risk Assessment. ENISA, 2009.11.20.
https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment; letöltés: 2021.03.15.

[50] Cloud Security Guide for SMEs. ENISA, 2015.04.10.
https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes; letöltés: 2021.03.15.

különböző felhőszolgáltatók kínálatát és képesek legyenek biztosítékokat szerezni a szolgáltatóktól, valamint csökkenteni tudják a kockázatokat. A kiadvány a felhőszolgáltatás előnyei mellett számba veszi a legfőbb kockázatokat is, többek között az adatok feletti felügyelet elvesztését, az adathordozhatóság hiányát (*vendor lock-in*), az elkülönülés sérelmét, a megfelelőség hiányát, az adatvédelmi hiányosságokat és a rossz szándékú „bérlőtársat". A kkv-k számára készült 2015-ös kiadvány a felhőszolgáltatásnak mint számtalan előnyt biztosító szolgáltatásnak az igazi marketinganyaga. A kockázatok felsorolásában pedig nemcsak a „hagyományos" kockázatok szerepelnek (fizikai veszélyek, a szoftverek sérülékenysége, a hálózati támadások, joghatósági problémák stb.), hanem már megjelenik a pszichológiai manipuláció[51] és a váratlan költségek rizikója is. A dokumentum nemcsak a kockázatokat írja le részletesen az informatikában és az adatvédelmi jogban járatlanok számára, hanem a felhő- és a hagyományos IT-megoldások közötti különbségeket is, valamint esettanulmányokkal és kérdéssorokkal mutatja be a kockázatelemzés folyamatát.

Összességében megállapítható, a felhőszolgáltatókkal kapcsolatos elvárások és jogi követelmények nem a GDPR vívmánya, a GDPR „csak" az eltérő tagállami jogalkotásokat egységesítette és egyes kérdések esetében szigorította. A 29. cikk szerinti Adatvédelmi Munkacsoport véleménye (WP 196) már 2012-ben utal a készülő adatvédelmi rendeletre, amelyben:

- az adatkezelő és az adatfeldolgozó felelősségi köre kiegyensúlyozottabbá válik az elszámoltathatóság elvének megfelelve, illetve az adatbiztonság területén a technikai és a szervezeti intézkedések jogi kötelezettsége is kiemelt szerepet kap;
- egyértelművé válik, hogy az adatkezelő utasításait megszegő adatfeldolgozó (így a felhőszolgáltató is) adatkezelőnek minősül, adatkezelői felelősséggel.

CISPE[52] magatartási kódex

A felhőszolgáltatók már a GDPR hatályba lépése előtt megkezdték a felkészülést a megfelelőségi kritériumok teljesítése érdekében. Az európai felhőinfrastruktúra-szolgáltatók szakmai szövetsége, a CISPE ezért kidolgozott egy magatartáskódexet. A szövetség minősíti, majd ellenőrzi a csatlakozó szolgáltatókat a kritériumok megvalósítását követően.[53,54]

---

[51] Social engineering – Amikor egy jogosultsággal rendelkező felhasználó jogosulatlan személy számára bizalmas adatokat átad, illetve lehetőséget biztosít illetéktelen belépésre a másik személy megtévesztő viselkedése miatt.

[52] Az európai felhőinfrastruktúra-szolgáltatók szakmai szövetsége: Cloud Infrastructure Services Providers in Europe – CISPE.
Cloud Infrastructure Services Providers in Europe. https://cispe.cloud/; letöltés: 2021.02.26.

[53] Data Protection Code of Conduct Task Force. CISPE.cloud.
https://cispe.cloud/cctf/; letöltés: 2021.02.13.

[54] A CISPE magatartási kódex verifikációját a szolgáltatók egy logóval jelezhetik.

A magatartási kódex meghatározza, hogy a felhőszolgáltatónak minden európai ügyfele[55] adatait az európai gazdasági térségen belül kell tárolnia és feldolgoznia. Emellett a tagoknak garanciát kell vállalniuk arra vonatkozóan is, hogy a letárolt adatokat nem használják fel egyéb célra (pl. valamilyen direktmarketing-cél vagy profilozás).[56]

A kódex azt is meghatározza, hogy az adatok kezelésével kapcsolatos felelősségek hogyan oszlanak meg, valamint részletesen leírja a követelményeket a szolgáltató által végzett adatfeldolgozás vonatkozásában. A kódex a CISPE-tagokat kötelezi a teljes transzparenciára a követelmények teljesítésével kapcsolatban.[57] A kódex tervezetét a 29. cikk szerinti Adatvédelmi Munkacsoport is véleményezte.[58]

A GDPR újdonságai

Adatvédelmi hatásvizsgálat

A GDPR előírja, hogy abban az esetben, amikor az adatkezelés természetes személyek jogaira és szabadságaira nézve magas kockázattal jár (pl. új technológia alkalmazása esetén), akkor az adatkezelőnek – annak érdekében, hogy az adatkezelés jellegét, hatókörét, körülményeit és céljait, valamint a kockázat forrásait figyelembe véve felmérje a magas kockázat különös valószínűségét és súlyosságát – az adatkezelés megkezdése előtt adatvédelmi hatásvizsgálatot kell végeznie. Ez a hatásvizsgálat magában foglalja különösen az említett kockázat mérséklését, a személyes adatok védelmét, valamint az e rendeletnek való megfelelés bizonyítását célzó tervezett intézkedéseket, garanciákat és mechanizmusokat.[59] Az adatvédelmi hatásvizsgálat elvégzéséért az adatkezelő felel.[60] A hatásvizsgálatnak ki kell terjednie legalább:[61]

- a tervezett adatkezelési műveletek módszeres leírására és az adatkezelés céljainak ismertetésére, beleértve adott esetben az adatkezelő által érvényesíteni kívánt jogos érdeket;
- az adatkezelés céljaira figyelemmel az adatkezelési műveletek szükségességi és arányossági vizsgálatára;
- az érintettek jogait és szabadságait érintő kockázatok vizsgálatára;

---

[55] A kódex nem tesz különbséget a vállalatok és magánszemélyek között.
[56] What EU institutions and Europe need to do to succeed in the digital economy. CISPE.cloud. https://cispe.cloud/cispe-manifesto/; letöltés: 2021.02.13.
[57] Data Protection Code of Conduct for Cloud Infrastructure Service Providers. CISPE.cloud, 2017.01.27. https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf; letöltés: 2021.03.15.
[58] Article 29 Data Protection Working Party. Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (WP 232). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf; letöltés: 2021.02.13.
[59] GDPR (90) preambulumbekezdés.
[60] GDPR (84) preambulumbekezdés.
[61] GDPR 35. cikk (7) bekezdés.

– a kockázatok kezelését célzó intézkedések bemutatására, ideértve a személyes adatok védelmét és az e rendelettel való összhang igazolását szolgáló, az érintettek és más személyek jogait és jogos érdekeit figyelembe vevő garanciákat, biztonsági intézkedéseket és mechanizmusokat.

Az adatvédelmi hatásvizsgálatok lefolytatására a felhőszolgáltatást igénybe venni kívánók számára a 29. cikk szerinti Adatvédelmi Munkacsoport e tárgyban készült iránymutatása[62] tud segítséget nyújtani, illetve a francia adatvédelmi hatóság (CNIL[63]) nyílt forráskódú szoftverét[64,65] hívhatják segítségül.

Az adathordozhatóság joga

A GDPR az érintetti jogok között nevesíti az adathordozhatóság jogát,[66] vagyis az érintett (azaz a természetes személy) jogosult arra, hogy a rá vonatkozó és általa egy adatkezelő rendelkezésére bocsátott személyes adatokat tagolt, széles körben használt, géppel olvasható formátumban megkapja, továbbá jogosult arra, hogy ezeket az adatokat egy másik adatkezelőnek továbbítsa anélkül, hogy ezt akadályozná az az adatkezelő, amelynek a személyes adatokat a rendelkezésére bocsátotta, amennyiben az adatkezelés hozzájáruláson vagy szerződésen alapul és az automatizált módon történik. Az érintett jogosult arra is – amennyiben ez technikailag megvalósítható –, hogy kérje a személyes adatok adatkezelők közötti közvetlen továbbítását. Az adathordozhatóság jogának korlátja, hogy a jog nem érintheti hátrányosan mások jogait és szabadságait.

Meg kell jegyezni, hogy az adathordozhatóság joga a GDPR alapján csak a természetes személyt illeti meg, így a szervezeteknek más jogi megoldást kell találniuk az adataik hordozhatóságának megvalósítására, illetve a hordozhatóság kockázatainak csökkentésére.

Az adatkezelő és az adatfeldolgozó kapcsolata (adatfeldolgozási megállapodások)

A GDPR IV. fejezetének 1. szakasza tartalmaz rendelkezéseket az adatkezelő és az adatfeldolgozó, azaz a felhőszolgáltatást igénybe vevő és a felhőszolgáltatást nyújtó szolgáltató általános kötelezettségeiről, így többek között a 26. cikk rendelkezik arról, hogy:

---

[62] Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e. https://www.naih.hu/files/WP248_rev01_hu.pdf; letöltés: 2021.03.15.

[63] Commission Nationale de l'Informatique et des Libertés.

[64] A hatásvizsgálati szoftver célja segítséget nyújtani az adatkezelők részére a természetes személyek személyes adatainak védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK irányelv hatályon kívül helyezéséről szóló Európai Parlament és a Tanács (EU) 2016/679 rendelet rendelkezéseivel összhangban álló adatkezelés kialakításában és az annak történő megfelelés bizonyításában.

[65] Adatvédelmi hatásvizsgálati szoftver (PIA software). https://naih.hu/hatasvizsgalati-szoftver; letöltés: 2021.03.15.

[66] GDPR 20. cikk.

– Ha az adatkezelést az adatkezelő nevében más végzi, akkor az adatkezelő (azaz jelen esetben a felhőszolgáltató) kizárólag olyan adatfeldolgozókat vehet igénybe, akik vagy amelyek megfelelő garanciákat nyújtanak az adatkezelés GDPR-követelményeinek való megfelelésére és az érintettek jogainak védelmét biztosító megfelelő technikai és szervezési intézkedések végrehajtására.

– Az adatfeldolgozó (azaz a felhőszolgáltató) az adatkezelő előzetesen írásban tett eseti vagy általános felhatalmazása nélkül további adatfeldolgozót (alvállalkozót) nem vehet igénybe. Az általános írásbeli felhatalmazás esetén az adatfeldolgozó tájékoztatja az adatkezelőt minden olyan tervezett változásról, amely további adatfeldolgozók igénybevételét vagy azok cseréjét érinti, ezzel biztosítva lehetőséget az adatkezelőnek arra, hogy ezekkel a változtatásokkal szemben kifogást emeljen.

– Az adatfeldolgozó által végzett adatkezelést az uniós jog vagy tagállami jog alapján létrejött olyan – az adatkezelés tárgyát, időtartamát, jellegét és célját, a személyes adatok típusát, az érintettek kategóriáit, valamint az adatkezelő kötelezettségeit és jogait meghatározó – szerződésnek vagy más jogi aktusnak kell szabályoznia, amely köti az adatfeldolgozót az adatkezelővel szemben. A 26. cikk (3) bekezdése részletesen felsorolja a szerződésbe kötelezően belefogalmazandó követelményeket (pl. utasításnak megfelelően történő eljárás, titoktartási kötelezettség, adatbiztonság biztosítása, adatfeldolgozó alvállalkozók igénybevétele, személyes adatok harmadik országba továbbítása, szerződés esetén az adatok sorsa, adatvédelmi incidens esetén az adatkezelő értesítésének kötelezettsége, érintetti jogok biztosításában közreműködési kötelezettség, audit lefolytatása stb.).

– Amennyiben az adatfeldolgozó (azaz a felhőszolgáltató) bizonyos, az adatkezelő nevében végzett konkrét adatkezelési tevékenységekhez további adatfeldolgozók szolgáltatásait is igénybe veszi, akkor azokra is ugyanazokat az adatvédelmi kötelezettségeket kell telepíteni, mint amelyek az adatkezelő és az adatfeldolgozó között fennállnak. Ha a felhőszolgáltató alvállalkozója nem teljesíti az adatvédelmi kötelezettségeit, akkor az őt megbízó adatfeldolgozó teljes felelősséggel tartozik az adatkezelő felé a másik adatfeldolgozó kötelezettségeinek a teljesítéséért.

– Amennyiben egy adatfeldolgozó (azaz a felhőszolgáltató) a GDPR rendelkezéseit megsértve maga határozza meg az adatkezelés céljait és eszközeit, akkor őt az adott adatkezelés tekintetében adatkezelőnek kell tekinteni.

Minden adatfeldolgozónak (azaz felhőszolgáltatónak) nyilvántartást kell vezetnie az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról, ennek minimális tartalmát[67] a GDPR szintén előírja.

[67] GDPR 30. cikk (2) bekezdés.

Az elfeledtetéshez való jog és az adattörlés problémái

A GDPR nevesíti minden adatkezelő és adatfeldolgozó „rémálmát", a törléshez való jogot („az elfeledtetéshez való jog"),[68] miszerint az érintett – bizonyos feltételek megléte esetén – jogosult arra, hogy kérésére az adatkezelő indokolatlan késedelem nélkül törölje a rá vonatkozó személyes adatokat, az adatkezelő pedig köteles arra, hogy az érintettre vonatkozó személyes adatokat indokolatlan késedelem nélkül törölje.

A törléshez való jogot nem szabad összekeverni a törlési kötelezettséggel, amely a GDPR alapelveiből (célhoz kötöttség, korlátozott tárolhatóság, adattakarékosság elve) következő kötelezettség. Függetlenül azonban attól, hogy alapelv betartása miatt (pl. megszűnt az adatkezelés célja, elvesztette „szavatosságát" az adat stb.) vagy érintetti kérelemre történik a törlés, az adatkezelőnek a törléssel kapcsolatos követelményeket maradéktalanul be kell tartania, akár hagyományos módon kezeli az adatokat, akár felhőszolgáltatót vesz igénybe.

A törléssel kapcsolatos adatkezelői problémákkal kapcsolatban a Nemzeti Adatvédelmi és Információszabadság Hatóság egy GDPR előtti, 2015. évi határozatában – szakértői véleményre hivatkozva – fejtette ki a véleményét, miszerint „*kétféle adattörlés történik, logikai és fizikai. A logikai adattörlés a vizsgált rendszeren azt jelenti, hogy az adatrekordot töröltként megjelölik, és a továbbiakban töröltként kezeli a rendszer, viszont az adatok valódi fizikai törlése nem történik meg, a törölt rekord adatai fizikailag nincsenek törölve. A fizikai adattörlés a logikai adattörléssel szemben az adatok fizikai törlését jelenti, a rekord tényleges törlésével, vagy a törlendő adat fizikai felülírásával, például a vizsgálat során elmondottak szerint „X" karaktereknek a megfelelő mezőbe beírásával. A vizsgált rendszernél látható volt, hogy a logikailag törölt adatok halványan, de egyértelműen olvashatóan megjelentek a felületen, ami a szakértő véleménye szerint nem tekinthető logikai törlésnek sem, hiszen a logikai törlés az adatokat kezelő szoftver útján bármelyik felhasználó részére elérhetetlenné (töröltté) kell, hogy tegye az adatot, az adat csupán adatbázis szinten található meg. A logikai törlés jelen esetben nem akadályozza meg a törlendő adat elérését, mert egyrészt a használt informatikai rendszerben is megjelenik a törölt adat, másrészt az adatbázisban akkor is elérhető marad, ha a program módosítását követően ott már nem jelenne meg. A logikai törlésnek van olyan megoldása a szakértői vélemény szerint, amely mindkét célt megvalósítja, az adat felismerhetetlenségének biztosítását is, és az ismételt felhasználás megakadályozását is. Ha a törlendő adatot tartalmazó mezőket például annak az MD5 algoritmussal elkészített hash lenyomatára cserélnék, akkor az adat is felismerhetetlenné válna, és az újonnan érkezett adatra ugyanezen algoritmussal generált hash kulcs használatával a duplikálás is elkerülhető lenne.*"[69]

[68] GDPR 17. cikk.

[69] NAIH/2015/21/20/H. (NAIH-17/2014/H.) személyes adatok kezelése az Intrum Justitia Zrt. és az Intrum Justitia Kft. követeléskezelési tevékenysége során (határozat). https://naih.hu/files/21_2015_hatarozat.pdf; letöltés: 2021.03.15.

Az említett NAIH-határozat a 95/46/EK irányelv 6. cikke (1) bekezdés e) pontjának szemléletét tükrözi, amely szerint a személyes adatok tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak az adatok gyűjtése vagy további feldolgozása céljainak eléréséhez szükséges ideig teszi lehetővé. A rendelkezés lényege, hogy a már nem szükséges személyes adatokat törölni kell, vagy valóban anonimmá kell tenni azokat. A 29. cikk szerinti Adatvédelmi Munkacsoport véleménye szerint[70] a felhőszolgáltatások esetén a szolgáltatás igénybe vevője felel annak biztosításáért, hogy töröljék a személyes adatokat, amint a fenti értelemben már nincs rájuk szükség. A Munkacsoport leszögezi, hogy az adatok törlésével kapcsolatos elv érvényesítési kötelezettsége független attól, hogy a személyes adatok tárolása merevlemezes meghajtón vagy egyéb adathordozón (pl. biztonsági másolatok) történik, illetve azt is biztosítani kell, hogy minden (másolati) példány is visszavonhatatlanul törölve legyen, így a korábbi verziók, az ideiglenes fájlok és fájltöredékek is. Sőt, a törlés során nem szabad elfelejtkezni arról sem, hogy az adatok tárolásának, módosításának vagy törlésének ellenőrzését megkönnyítő naplóadatok szintén személyes adatnak minősülhetnek, tehát a törlési kötelezettség ezekre is vonatkozhat.

A Munkacsoport véleménye szerint „*a személyes adatok biztonságos törlése szükségessé teszi az adathordozó megsemmisítését vagy demagnetizálását, illetve a tárolt személyes adatok tényleges törlését azok felülírásával. A személyes adatok felülírására olyan speciális szoftvereszközöket kell alkalmazni, amelyek egy elismert specifikációnak megfelelően többször felülírják az adatokat.*”[71] A törlési kötelezettség teljesítése során a felhőszolgáltatás igénybe vevőjének meg kell bizonyosodnia arról, hogy a szolgáltató biztosítja a követelményeknek megfelelő törlést.

A már említett 2009-es ENISA-kiadvány[72] a nem biztonságos, illetve hatástalan törlések (*insecure or ineffective deletion of data*) előfordulási valószínűségét és a kockázatot önmagát közepesre értékeli, a szervezetre gyakorolt hatását azonban nagyon magasra. Az értékeléshez fűzött magyarázat szerint amikor valamilyen szolgáltatót megváltoztatunk és esetleg a hardware-t áthelyezik, az adatok a biztonsági előírásokban megjelölt időn túl is hozzáférhetővé válnak. Emiatt kivitelezhetetlen is lehet a biztonsági irányelvekben megjelölt folyamatok végrehajtása, ugyanis az adatok teljes körű törlése csak a lemez megsemmisítésével lenne lehetséges, a lemezen azonban más felhasználók adatait is tárolják normál esetben. Ezáltal – még ha a kérés egy felhőalapú szolgáltatás során igénybe vett adatcsomag törlésére vonatkozik is – valójában ezzel nem törölhetők teljesen az adatok a legtöbb operációs rendszerben. Ha az adatok valós, teljes körű törlésére van szükség, akkor különleges folyamatokat/ procedúrákat kell végrehajtani, amelyeket a klasszikus értelembe vett alkalmazások nem feltétlenül (vagy egyáltalán nem) támogatnak.

A törléssel kapcsolatos elvárások a GDPR után sem módosultak, az Európai Adatvédelmi Testület (EDPB[73]) beépített adatvédelemről szóló 04/2019 iránymutatásában a Testület – többek között – a korlátozott tárolhatóság elvének

[70] WP 196, 3.4.1.3. pont.
[71] WP 196, 3.4.1.3. pont.
[72] Cloud Computing Security Risk Assessment. ENISA, 2009. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment; letöltés: 2021.03.15.
[73] European Data Protection Board, 2018. május 25-től a 29. cikk szerinti Adatvédelmi Munkacsoport utódja.

teljesítésével kapcsolatban fejti ki a véleményét, miszerint ha már nincs szükség a személyes adatok kezelésére, akkor azokat törölni vagy anonimizálni szükséges. Az adatok bármilyen megtartásának objektíven igazolhatónak kell lennie az elszámoltathatóság elvének figyelembevételével. A törlés alternatív megoldása lehet az anonimizálás, feltéve, hogy az adatkezelő tekintettel van az összes releváns körülményre, valamint rendszeresen újraértékeli a kockázatok valószínűségét és súlyosságát, ideértve az újraazonosítás kockázatát is. Az adatkezelőnek figyelembe kell vennie a korlátozott tárolhatóság elvének követelményét is, hogy olyan szisztematikus eljárásokkal rendelkezzen az adattörlések tekintetében, melyek segítségével meg tud felelni ennek a követelménynek.

Természetesen adott esetben az adatkezelőnek nemcsak a személyes adatok, hanem egyéb adatok törléséhez is érdeke fűződhet, a nem személyes adatok törlése kapcsán azonban nem kell magát tartania a GDPR előírásaihoz, és a felhőszolgáltatót is más jogi eszközökkel tudja rászorítani az adatok törlésére.

Mit ajánlanak az adatvédelmi hatóságok a felhőszolgáltatások igénybe vevőinek?

Az adatvédelmi hatóságok gyakran adnak ki tájékoztatókat különféle adatvédelmi témákban, az egyik ilyen a *cloud computing*, azaz a felhőszolgáltatás. Ezekben a kiadványokban segítséget nyújtanak a szakértelemmel nem rendelkező leendő felhőhasználóknak annak érdekében, hogy egyrészt tisztában legyenek azzal, mi is az a felhőszolgáltatás és milyen kockázatokat kell felvállalniuk, ha ilyet kívánnak igénybe venni, másrészt a lehető legkörültekintőbben tudjanak választani a számukra elérhető szolgáltatók közül.

A brit hatóság 2012-ben olyan tájékoztató anyagot[74] adott ki a felhőszolgáltatások témájában, amely mind a mai napig hasznos tanácsokat nyújt az érdeklődőknek a tekintetben, hogy hogyan válasszanak felhőszolgáltatót és mit tegyenek annak érdekében, hogy csökkentsék a kockázatukat.

Az ír hatóság a kiadványában[75] a hangsúlyt a biztonságra, illetve az adatfeldolgozási megállapodásra helyezi, valamint azokra az alapelvekre, amelyek teljesítését a GDPR elvárja a felhőszolgáltatóktól, míg egy másik útmutatója[76] a felhőszolgáltatások technikai kockázataira hívja fel a figyelmet (adatvédelmi incidens, adatokhoz jogosulatlan hozzáférés, felhasználói fiókok „eltérítése”[77]).

---

[74] Guidance on the use of cloud computing. Information Commissioner’s Office, Data Protection Act, 1998. https://ico.org.uk/media/about-the-ico/documents/1042330/cloud-computing-guidance-for-organisations.pdf; letöltés: 2021.03.15.

[75] Guidance for Organisations Engaging Cloud Service Providers. Data Protection Commission, 2019. https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guidance%20for%20Engaging%20Cloud%20Service%20Providers_Oct19.pdf; letöltés: 2021.03.15.

[76] Five Steps to Secure Cloud-based Environments. Data Protection Commission, 2019. https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190606%20Five%20Steps%20to%20Secure%20Cloud-based%20Environments.pdf; letöltés: 2021.03.15.

[77] Hijacking of accounts.

A felhőszolgáltatást igénybe vevők részéről az adatbiztonságnak két aspektusa van:

– a felhőszolgáltatónak mint adatfeldolgozónak bizonyságot kell adnia arról, hogy az adatokat csakis a felhasználó utasításai alapján kezeli (írásbeli megállapodás alapján);

– a felhőszolgáltatónak bizonyságot kell adnia arról, hogy a tevékenysége során figyelembe vette a továbbított, tárolt vagy más módon kezelt személyes adatok véletlen vagy jogellenes megsemmisítéséből, elvesztéséből, megváltoztatásából, jogosulatlan közléséből vagy az azokhoz való jogosulatlan hozzáférésből eredő kockázatokat.

A szolgáltatást igénybe vevőnek még az adatok felhőszolgáltatóra bízása előtt meg kell győződnie arról, hogy a szolgáltató biztonsági előírásai elegendőek és megfelelőek a GDPR-nak, illetve annak, hogy a (szolgáltatást igénybe vevő) adatkezelő nevében megfelelően tudjon eljárni. Ilyen előírások, intézkedések lehetnek például:

– szükség esetén a személyes adatok álnevesítése és/vagy titkosítása;

– a szolgáltatást igénybe vevő ügyfelek személyes adatainak elkülönítése vagy szétválasztása más ügyfelek adataitól;

– a bizalmasság, sértetlenség és elérhetőség biztosítása a szolgáltatás teljes időtartama alatt, ezt elősegíthetik technikai és szervezeti intézkedések:

  - hozzáféréskontroll: erős jelszavak megkövetelése, kétfaktoros autentikáció, felhasználói jogosultságok beállítása (*need to know* elvének következetes érvényesítése) és rendszeres felülvizsgálata;

  - a szolgáltatás igénybe vevője számára az alapértelmezett biztonsági beállítások személyre szabása lehetőségének biztosítása, például adatvesztés megelőzése, mobil eszközök menedzsmentje, központosított adminisztrációs eszközök, aktivitás figyelés és riasztás, *malware* védelem, loginriasztás, spam, hamisítás (*spoofing*) és adathalász (*phishing*) védelem, üzenetküldés és -kapás titkosítása, üzenet tartalmának titkosítása stb., valamint figyelmeztetés e beállítások rendszeres felülvizsgálatára;

  - tűzfalak, vírusirtók;

  - személyzet oktatása, a hozzáférés-menedzsmentben a fluktuáció nyomon követése;

  - belső szabályzatok, titoktartási követelmények stb.)

  előírása és teljesítése (GDPR 32. cikk);

– annak képessége, hogy nem várt fizikai sérülések vagy technikai hibák után a személyes adatok elérhetősége és hozzáférhetősége időben helyreállítható legyen;

– a technikai és a szervezeti intézkedések rendszeres tesztelése, hatékonyságuk felmérése és értékelése;

– adatvédelmi incidens esetére reagálási terv és intézkedési protokoll a szolgáltatást igénybe vevők minél gyorsabb értesítésére, hogy a lehető legkisebbre lehessen csökkenteni az érintettek jogait és szabadságait érintő kockázatokat;

– képesség arra, hogy a szerződés teljesülése után az adatok vissza legyenek juttatva a szolgáltatás igénybe vevőjének vagy (helyreállíthatatlanul) törölve legyenek.

Európai uniós törekvések – GAIA-X projekt

Az Európai Bizottság 2020 februárjában tette közzé az adatokkal kapcsolatos stratégiáját.[78] Az elgondolás szerint az európai „adatökoszisztéma" kereteit tovább kell fejleszteni és versenyképességé kell tenni, de kiemeli és hangsúlyozza az adatok védelmét is. Részletezi a főbb problémákat és kihívásokat, ezek között pedig kiemelt szerepet kapnak az adatok hozzáférhetősége, a kiegyensúlyozatlanság a piacokon, az interoperabilitás hiánya, az adatok minőségével kapcsolatos problémák, valamint az EU jelenlegi technológiai függősége az amerikai és a kínai felhőszolgáltató óriásoktól.

Ennek a függőségnek a leküzdése érdekében német–francia kezdeményezésre életre hívták a GAIA-X projektet, amelynek célja Európa saját digitális ökoszisztémája létrehozása. A projekt nem akar saját szabályozási rendszert kialakítani, hanem a már meglévő uniós jogalkotásra kíván támaszkodni. Bármelyik felhőszolgáltató csatlakozhat hozzá – beleértve az Amazont, a Google-t és a Microsoftot is – amennyiben betartja az alapelveket:

– európai adatvédelem (ideértve a GDPR, a nem személyes adatok Európai Unióban való szabad áramlásának keretéről szóló rendelet[79] és a kiberbiztonsági jogszabály[80] rendelkezéseit);

– nyitottság és átláthatóság (nyíltadat-infrastruktúra, szabványosított szerződések és eljárások a komplexitás és a költségek csökkentése érdekében);

[78] A European Strategy for Data. European Commission, 2021.03.09. https://ec.europa.eu/digital-single-market/en/european-strategy-data; letöltés: 2021.03.15.

[79] Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete (2018. november 14.) a nem személyes adatok Európai Unióban való szabad áramlásának keretéről. Az Európai Unió Hivatalos Lapja, 2018.11.28. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R1807&from=EN; letöltés: 2021.03.15.

[80] Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). Az Európai Unió Hivatalos Lapja, 2019.06.07. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0881&from=EN; letöltés: 2021.03.15.

– hitelesség és bizalom (mechanizmusok biztosítása annak érdekében, hogy a projektben részt vevők betartsák az informatikai biztonságra, az adatok szuverenitására, a szolgáltatási szintekre és keretrendszerekre vonatkozó szabályokat, valamint az együttműködés és a vállalatközi autentikáció és hozzáférés menedzsment feltételeit;

– digitális szuverenitás és önrendelkezés (minden résztvevő eldöntheti, hogy hol, hogyan és milyen célból kezeli a saját adatait);

– szabad hozzáférés a piachoz és európai értékteremtés, lehetőség a szervezetek közötti adatcserére, együttműködésre, felhőszolgáltatások összekapcsolására;

– modularitás és interoperabilitás (a különböző felhőplatformok adatainak összekapcsolása és integrálása, a hozzáférés akadályainak megszüntetése, a kisebb, speciális felhőszolgáltatók versenybe lépésének lehetővé tétele, ami jelentősen segítheti az adathordozhatóságot nemcsak a természetes személyek, hanem a szervezetek tekintetében is);

– felhasználóbarátság (központosított szolgáltatáson alapuló ismert interfészek alkalmazása annak érdekében, hogy a rendszer átfogó know-how nélkül is használható legyen).

A projekt nem önálló felhőszolgáltatást akar létrehozni, hanem alapvetően az adat és az infrastruktúra összekapcsolásáról van szó úgy, hogy a résztvevők számára nagyobb mozgásszabadságot biztosítson a szolgáltatások igénybevétele és adott esetben a szolgáltatások vagy szolgáltatók közötti adathordozhatóság vonatkozásában.

Ebben a projektben már a gyakorlatban is megjelenik az igény olyan szabványok kidolgozására, amelyek lehetővé teszik (biztosítják) az adatmozgást a különböző szolgáltatók között. A koncepció szerint a GAIA-X architektúrája felhasználható bármely adatvédelmi[81] szabvány betartásának biztosítására, mint ahogy a GDPR-ra is. A GAIA-X egyik meghatározó eleme a „dinamizmus", amely lehetővé teszi a felhasználók számára, hogy könnyen válthassanak szolgáltatót. A szolgáltatás várhatóan már 2021-ben elérhető lesz.

Felhő a gyakorlatban

A felhőszolgáltatók adatkezelési tájékoztatói

Problémafelvetésünk aktualitását alátámasztja az is, hogy a felhőszolgáltatók – annak ellenére, hogy feltehetően alapvetően teljesítik a GDPR adatkezelésre vonatkozó szabályait – az adatkezelési tájékoztatóikban[82] (adatfeldolgozói kódexeikben, adatkezelési szabályzataikban, ki hogyan nevezi) jellemzően bizalmi alapra építik a szerződő felek közötti adatkezelést, és így az adatok törlését is. A problémafelvetés alátámasztása érdekében megvizsgáltunk Magyarországon üzemelő tíz nagyobb felhőszolgáltató adatkezelési tájékoztatóját.

[81] A leírás egyes eseteiben az adatvédelmet és az információbiztonságot együtt értelmezi.

[82] Ebben az esetben most nem teszünk különbséget a privacy és az adatvédelem fogalma között, mert a vizsgált esetekben ritkán szinonimaként használják őket.

Megállapításunk szerint a vizsgált adatvédelmi tájékoztatók alapvetően tartalmazzák a GDPR ide vonatkozó pontjait (érintetti jogok felsorolása, adattovábbítás garanciái stb.), illetve tökéletesen idézik a GDPR definíciótárát is. Általános probléma, hogy a tájékoztatók keverik a GDPR, illetve az Infotv. rendelkezéseit, valamint nem követték le a GDPR bevezetése utáni hazai korrekciós jogszabály-módosításokat.

Szerepkör, illetve az adatfeldolgozók beazonosítása

Kiemelkedő hiányosságnak számít, hogy a szervezetek csak elvétve azonosítják be saját szerepkörüket (mikor adatkezelők és mikor adatfeldolgozók, illetve amennyiben ez utóbbiak, akkor milyen felelősségeik vannak), valamint az általuk igénybe vett adatfeldolgozók és adatfeldolgozó alvállalkozók tekintetében sem biztosítják a megfelelő minőségű és mennyiségű információt az érintettek számára, pedig ez létfontosságú lenne a szolgáltatások igénybe vevőinek bizalma megszerzéséhez, illetve megtartásához. A szolgáltatók által megadott információk alapján szinte semmilyen információt sem kapunk a „kevert" szolgáltatásokról (pl. amikor más felhőszolgáltatók szolgáltatásaival vegyítik a sajátjukat), ahogy arról sem, milyen joghatóságok alatt tárolhatják az érintettek adatait (szolgáltatók által bérlelt tárhelyek, redundáns szerverek geolokációja stb.).

Az egyik szolgáltató tájékoztatójában az adatfeldolgozókról a következők szerint tájékoztat: „*Az adatkezelő az adatkezelés során a szerződés teljesítéséhez vele szerződött adatfeldolgozó(k) számára továbbítja az adatokat. A címzettek kategóriái: domain regisztrátor, hosting szolgáltatók, könyvelési/számviteli szolgáltató, elektronikus számlázási szolgáltató*". Hasonlóképpen jár el egy másik szolgáltató is: „*Az Adatkezelő az adatkezelés során a szerződés teljesítéséhez vele szerződött Adatfeldolgozó(k) számára továbbítja az adatokat. A címzettek kategóriái: IT-üzemeltetők, hírlevél rendszer üzemeltetők, webtárhely szolgáltatók, webtartalom fejlesztő, szerződött viszonteladó partnerek, rendezvényszervező, fotó-videó szolgáltató, hosztesz szolgáltató, vagyonvédelmi szolgáltató, rendezvény szponzorai.*"

Van azonban olyan szolgáltató is, amely a tájékoztatójában összesen egyetlen mondatot áldoz az adatfeldolgozóira: „*Az Adatkezelő a harmadik fél saját beszállítóit és adatfeldolgozóit kötelezi az elfogadott biztonsági intézkedések alkalmazására, korlátozva az adatfeldolgozó cselekvési szabadságát kizárólag az igénybe vett szolgáltatásra.*"

Ezekben és a hasonló esetekben a szolgáltató igen nagyvonalúan kezeli a GDPR 13. és 14. cikkeiben foglalt tájékoztatási kötelezettséget, amely szerint az érintett rendelkezésére kell bocsátani – többek között és adott esetben – a személyes adatok címzettjeit, illetve a címzettek kategóriáit, ha van ilyen. A 29. cikk szerinti Adatvédelmi Munkacsoport az átláthatóság követelményeiről szóló iránymutatása[83] alapján „*a „címzett" kifejezést a 4. cikk (9) bekezdése az alábbiak szerint definiálja:*

[83] Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról. WP260 rev.01. A 29. cikk szerinti Adatvédelmi Munkacsoport, 2017.11.29. https://naih.hu/files/wp260rev01_hu.pdf; letöltés: 2021.03.04.

„*az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik,* ***függetlenül attól, hogy harmadik fél-e***" [utólagos kiemelés]. *(…) Ennek következtében az egyéb adatkezelők, közös adatkezelők és adatfeldolgozók, akik vagy amelyek részére az adatokat továbbítják, szintén* „*címzettnek*" *minősülnek, és a harmadik fél címzettekre vonatkozó tájékoztatás mellett az ilyen címzettekről is tájékoztatást kell nyújtani.*

A személyes adatok tényleges (megnevezett) címzettjeit vagy a címzettek kategóriáit kell megadni. A tisztességes eljárás elvével összhangban az adatkezelőknek az érintettek számára leginkább releváns információkat kell rendelkezésre bocsátaniuk a címzettekkel kapcsolatban. A gyakorlatban ez általában a megnevezett címzetteket jelenti, hogy az érintettek pontosan tudják, ki rendelkezik a személyes adataikkal. Ha az adatkezelők úgy döntenek, hogy a címzettek kategóriáit adják meg, az információnak a lehető legkonkrétabbnak kell lennie, és magában kell foglalnia a címzett típusát (pl. az általa végzett tevékenységekre való utalással), az érintett szakmát, az ágazatot és alágazatot, valamint a címzettek tartózkodási helyét."

Nemzetközi adattovábbítás

Harmadik országba adattovábbítás megemlítése leggyakrabban a domain regisztrációjával kapcsolatban merül fel, amennyiben a regisztráció nem EGT-tagállam területén történik, illetve van olyan szolgáltató is, amelyik bevállalja a nemzetközi adattovábbítást úgy, hogy garanciaként általános adatvédelmi kikötéseket, illetve adatfeldolgozói megállapodást jelöl meg, az érintettek számára érthetetlen mozaikszavakkal (*SSC + DPA*). A hanyag tájékoztatás tipikus példája az, amikor a szolgáltató ugyan ad meg cégneveket az adattovábbítással kapcsolatban, de Magyarországot, Romániát és Csehországot is a GDPR szempontjából harmadik országok közé sorolja.

Adatbiztonság

Az adatbiztonság tekintetében a felhőszolgáltatók – többségében – felületes és igen általános jellegű műszaki információkat közölnek a tájékoztatóikban arról, hogy az adatokat mily módon védik, valamint milyen módszerrel törlik, illetve anonimizálják szükség szerint. Elmondható, hogy a tájékoztatás leginkább adatvédelmi szabályok és garanciák általános jellegű közlésében merül ki, de például azzal kapcsolatban az érintett nem kap információt, hogy az adatok végleges törlését – azaz az adatok felismerhetetlenné tételét oly módon, hogy a helyreállításuk többé nem lehetséges – milyen módszerrel végzi az adattárolásra szakosodott.

A felhőszolgáltatások esetében az adatkezelési tájékoztatók külön szakaszban tárgyalják a domain regisztrációjával kapcsolatos kérdést,[84] mivel egyes esetekben, olyan harmadik országba is elküldik az adatokat, amelyek nem tartoznak a GDPR hatálya alá.

[84] A Forpsi Domain Regisztráció és hosting szolgáltatása – Kommunikáció harmadik feleknek és a címzettek kategóriáinak.

A személyes adatok a szolgáltatás nyújtásával szigorúan összefüggő célokra továbbításra kerülnek olyan harmadik személynek vagy szervezetnek (regisztrációs hatóságoknak és akkreditált szolgáltatóknak), amelyek olyan országokban találhatók, ahol nem alkalmazzák a GDPR-t (EU-n kívüli országok), de amelyekre vonatkozóan az Európai Bizottság rendelkezése alapján a személyes adatok megfelelő szintű védelme biztosított. Természetesen ilyen esetben az érintett felet tájékoztatják arról, hogy a domain név bejegyzése magában foglalja a személyes adatoknak a nyilvánosan hozzáférhető nyilvántartásba (*Whois*) történő bejegyzését, amelyet a választott kiterjesztésért felelős regisztrációs hatóság tart fenn, kivéve azokat az eseteket, amikor az érintett fél az illetékes nyilvántartó hatóság által meghatározott módon vagy a szolgáltatással kapcsolatos szerződéses feltételeknek megfelelően a személyes adatok elrejtését kérte.[85]

A harmadik félnek küldött adatok esetében egyes nyilatkozatok részletesen tájékoztatják a felhasználót arról, hogy ki pontosan a harmadik fél (név, telephely, adószám), míg más esetekben csak gyűjtőfogalomként említik ezeket az entitásokat.

Egy esetben külön kiemelték azt a lehetőséget, hogy ha a felhasználók nem saját személyes adataikat adják meg, akkor az adatközlő kötelessége az érintett hozzájárulásának a beszerzése.

A felhőszolgáltatások adatkezelése esetén másik sarkalatos kérdés a domain regisztrációja. A domainszolgáltatás során, amely alatt általában a szolgáltatók a domainnév regisztrációját értik, a regisztrációhoz szorosan kötődő személyes adatok átadásra kerülnek harmadik feleknek,[86] amelyek olyan országokban találhatók, ahol nem alkalmazzák a GDPR-t (EU-n kívüli országok), de amelyekre vonatkozóan az Európai Bizottság rendelkezése alapján a személyes adatok megfelelő szintű védelme biztosított.

A felhőszolgáltatásokhoz köthető adatkezelési tájékoztatókban érintve megjelenik a felhasználók lehetősége arra, hogy személyes adataik vonatkozásában saját maguk járjanak el. Ilyen szolgáltatás például a webmail is, vagyis a webmail szolgáltatással a megrendelő, aki egyben az érintett is, közvetlenül menedzselheti e-mail-fiókját és beállításait.[87]

Jogszabályi hivatkozások

A szolgáltatók a leggyakrabban az alábbi jogszabályokra hivatkoznak:

– Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) – a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet, GDPR);

[85] Az ilyen adatkezelés jogi alapja a meglévő szerződéshez kapcsolódó szolgáltatások nyújtása, a jogi előírások betartása, valamint a szolgáltató jogos érdekeinek érvényesítése a célokhoz szükséges adatkezelés elvégzése érdekében.

[86] Regisztrációs hatóságoknak és akkreditált szolgáltatóknak.

[87] Az adatkezelés jogalapja a megkötött szerződés vagy a megrendelés teljesítése (GDPR 6. cikk (1) bekezdés b pont). A kezelt személyes adatok köre az e-mail-címe (mint felhasználónév) és a belépéshez szükséges jelszó. Az adatkezelés időtartama: a szerződés fennállásáig vagy a felhasználói profil érintetett általi törléséig. Az adatok megadása alapfelétele a szolgáltatás igénybevételének.

– az információs önrendelkezési jogról és az információszabadságról szóló 2011. évi CXII. törvény (Infotv.);

– a Polgári Törvénykönyvről szóló 2013. évi V. törvény (Ptk.);

– a számvitelről szóló 2000. évi C. törvény (Számv. tv.);

– a gazdasági reklámtevékenység alapvető feltételeiről és egyes korlátairól szóló 2008. évi XLVIII. törvény (Grt.);

– az elektronikus kereskedelmi szolgáltatások, valamint az információs társadalommal összefüggő szolgáltatások egyes kérdéseiről szóló 2001. évi CVIII. törvény (Ekertv.).

A jogszabályt mint fogalmat sajátosan értelmezi az a szolgáltató, aki az irányadó jogszabályok között utolsó pontként az alábbit szerepelteti: „*a fentiekkel kapcsolatos bármely bírósági vagy hatósági értelmezés, illetve bármely illetékes felügyeleti hatóság által kiadott iránymutatás, útmutató, gyakorlati szabályzat, jóváhagyott etikai kódex vagy jóváhagyott tanúsítási mechanizmus*”, meglehetősen összezavarva ezzel az átlagos szolgáltatást igénybe vevőt, különösen a természetes személyeket.

A tájékoztatókban csak elvétve szerepel utalás a GDPR 8. cikkére, mely szerint az információs társadalommal összefüggő szolgáltatások esetében – a többi szolgáltatás 18 éves korhatárához képest – GDPR alapján a nemzeti korhatár 16 év.

Hipotézis igazolása

A cikkhez kérdőíves kutatást is felhasználtunk, ami megerősítette, hogy maguk a felhasználók (nem vállalati) is csak a jogszabályok maradéktalan betartásában bíznak, a gyakorlatban viszont nem rendelkeznek irányítással személyes adataik felett a felhőszolgáltatóknál. Emellett a GDPR-nak nyilván van áttételes hatása az adatszivárgások vonatkozásában, mivel az érvényesíthető büntetések mértéke jelentősen növelte az üzemeltetési kockázatokból származó potenciális költségeket.

A GDPR további hatása az, hogy az egyes szolgáltatók a saját belső audit mellett igénybe vesznek külső auditszolgáltatást is. Így végeztethet független auditot, amelynek az eredményét nyilvánosságra hozza, ezzel növelve a szolgáltatás kiberbiztonságát. A GDPR-megfelelőség sok vállalkozás esetében az IT-rendszerekben korábban elhanyagolt fejlesztéseket kényszerített ki, amelyek során esetleges sérülékenységeket is kijavíthattak, vagy legalábbis csökkenthettek.

A GDPR tekintetében megállapítható, hogy a rendelet hatályba lépésétől a szolgáltatók várhatóan több forrást fognak ráfordítani a törlést és az anonimizálást végrehajtó speciális célszoftverekre.

Az interjúk és az adatkezelési nyilatkozatok elemzése és értékelése során megállapítottuk, hogy ezek a tájékoztatók még jelenleg is hiányosak vagy elnagyoltak. Emellett közös jellemzőik, hogy laikus felhasználók vagy ügyfelek részére nehezen olvashatók vagy értelmezhetők, bár a GDPR meghatározza, hogy a tájékoztatóknak közérthetőknek kell lenniük.

Megállapítható az is, hogy a felhőszolgáltatások esetében külön kutatást igényel azon egészségügyi rendszerek vizsgálata, amelyek felhőszolgáltatásokat vesznek igénybe, mert a koronavírus-járvány során az egészségügyi informatikai rendszerek kiemelt kiberbiztonsági kockázatoknak vannak kitéve.

A GDPR egy másik fontos kérdése a kiberbiztonság tükrében az, hogy a felhőszolgáltatók mennyire veszik figyelembe a rendeletet. A magas bírságok következtében az elkövetkező időszakban várhatóan egyre nagyobb forrásokat fordítanak majd a felhőinfrastruktúra védelmére. A GDPR alkalmazásának első évében a hatóságok kisebb összegű bírságokat szabtak ki. A CNIL Google-lal szemben kiszabott 50 millió eurós bírsága volt az első precedens arra, hogy a GDPR által jelentősen megemelt bírságlimitek előbb-utóbb jelentős összegű bírságokat is eredményezhetnek. A jelentős hatósági bírságok nagy figyelmet érdemelnek, hiszen ráirányítják a figyelmet az adatbiztonság és a kiberbiztonság kérdésére. Emellett felhívják a figyelmet az incidensek kezelésére és arra is, hogy a bírságon kívül egy incidens milyen egyéb jelentős hatásokkal járhat az érintett adatkezelőkre nézve.[88]

FELHASZNÁLT IRODALOM

- 1/2010. számú vélemény az „adatkezelő” és az „adatfeldolgozó” fogalmáról (WP 169). A 29. cikk szerinti Adatvédelmi Munkacsoport, 2010.02.16. http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp169_hu.pdf; letöltés: 2021.03.15.
- 2011. évi CXII. törvény az információs önrendelkezési jogról és az információszabadságról. https://net.jogtar.hu/jogszabaly?docid=a1100112.tv; letöltés: 2021.03.17.
- 91/20. sz. Sajtóközlemény. Európai Unió Bírósága, Luxembourg, 2020. július 16. – A C-311/18. sz. ügyben hozott ítélet. Data Protection Commissioner kontra Facebook Ireland és Schrems. A Bíróság érvénytelennek nyilvánítja az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről szóló 2016/1250 határozatot. https://naih.hu/kozlemenyek/EUB_sajtokozlemeny_cp200091hu.pdf; letöltés: 2021.03.15.
- A European Strategy for Data. European Commission, 2021.03.09. https://ec.europa.eu/digital-single-market/en/european-strategy-data; letöltés: 2021.03.15.
- Adatvédelmi hatásvizsgálati szoftver („PIA software”). https://naih.hu/hatasvizsgalati-szoftver; letöltés: 2021.03.15.
- Article 29 Data Protection Working Party. Opinion 02/2015 on C-SIG Code of Conduct on Cloud Computing (WP 232). https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2015/wp232_en.pdf; letöltés: 2021.02.13.
- Article 29 Data Protection Working Party. Opinion 05/2012 on Cloud Computing (WP 196). https://www.gpdp.gov.mo/uploadfile/others/wp196_en.pdf; letöltés: 2021.03.14.

[88] Részvényárfolyamok esése, cégértéket érintő azonnali hatások, reputációs veszteség, valamint az egyéni kártérítési igények megjelenése.

- Az Európai Parlament és a Tanács (EU) 2016/679 rendelete (2016. április 27.) a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet). https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri=CELEX:32016R0679; letöltés: 2021.03.02.
- Az Európai Parlament és a Tanács (EU) 2018/1807 rendelete (2018. november 14.) a nem személyes adatok Európai Unióban való szabad áramlásának keretéről. Az Európai Unió Hivatalos Lapja, 2018.11.28. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32018R1807&from=EN; letöltés: 2021.03.15.
- Az Európai Parlament és a Tanács (EU) 2019/881 rendelete (2019. április 17.) az ENISA-ról (az Európai Uniós Kiberbiztonsági Ügynökségről) és az információs és kommunikációs technológiák kiberbiztonsági tanúsításáról, valamint az 526/2013/EU rendelet hatályon kívül helyezéséről (kiberbiztonsági jogszabály). Az Európai Unió Hivatalos Lapja, 2019.06.07. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32019R0881&from=EN; letöltés: 2021.03.15.
- Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről („Elektronikus hírközlési adatvédelmi irányelv”). Official Journal L 201, 31/07/2002. pp. 0037– 0047. https://eur-lex.europa.eu/legal-content/HU/TXT/HTML/?uri= CELEX:32002L0058&from=ES; letöltés: 2021.03.04.
- Az Európai Parlament és a Tanács 2006/2004/EK rendelete (2004. október 27.) a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről („Rendelet a fogyasztóvédelmi együttműködésről”). Az Európai Unió Hivatalos Lapja, 2004.12.09. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:32004R2006&from=ES; letöltés: 2021.03.12.
- Az Európai Parlament és a Tanács 95/46/EK irányelve (1995. október 24.) a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról. Az Európai Unió Hivatalos Lapja, 1995.11.23. https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:31995L0046&from=HU; letöltés: 2021.05.01.
- CISPE.cloud: Public Register. https://cispe.cloud/publicregister/; letöltés: 2021.03.15.
- Cloud Computing Security Risk Assessment. ENISA, 2009. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment; letöltés: 2021.03.15.
- Cloud Computing Security Risk Assessment. ENISA, 2009.11.20. https://www.enisa.europa.eu/publications/cloud-computing-risk-assessment; letöltés: 2021.03.15.
- Cloud Infrastructure Services Providers in Europe. https://cispe.cloud/; letöltés: 2021.02.26.

- Cloud Security Guide for SMEs. ENISA, 2015.04.10. https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes; letöltés: 2021.03.15.
- Data Protection Code of Conduct for Cloud Infrastructure Service Providers. CISPE.cloud, 2017.01.27. https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf; letöltés: 2021.03.15.
- Data Protection Code of Conduct Task Force. CISPE.cloud. https://cispe.cloud/cctf/; letöltés: 2021.02.13.
- e-Privacy Regulation. Statement 03/2021 on the ePrivacy Regulation, European Data Protection Board, 2021.03.09. https://edpb.europa.eu/our-work-tools/our-documents/topic/e-privacy-regulation_hu; letöltés: 2021.03.15.
- ERDŐS Gabriella: Néhány gondolat az adatbiztonságról és adatkezelésről az okos alkalmazások területén. Corvinus Law Papers, CLP 2/2020. http://unipub.lib.uni-corvinus.hu/5685/1/CLP_202002.pdf; letöltés: 2021.03.11.
- EU általános adatvédelmi rendelet: Az adathordozhatósághoz való jog. https://www.privacy-regulation.eu/hu/20.htm; letöltés: 2021.01.19.
- European Union Agency for Cybersecurity (ENISA). https://europa.eu/european-union/about-eu/agencies/enisa_en; letöltés: 2021.03.08.
- FARSHID, Simon – REITZ, Andreas – ROßBACH, Peter: Design of a forgetting blockchain – A possible way to accomplish GDPR compatibility. Proceedings of the 52nd Hawaii International Conference on System Sciences, 2019. pp. 7087–7095. https://core.ac.uk/download/pdf/211327966.pdf; letöltés: 2021.03.04.
- Five Steps to Secure Cloud-based Environments. Data Protection Commission, 2019. https://www.dataprotection.ie/sites/default/files/uploads/2019-06/190606%20Five%20Steps%20to%20 Secure%20Cloud-based%20Environments.pdf; letöltés: 2021.03.15.
- FRIVALDSZKY Gáspár: A felhőszolgáltatások adatvédelmi kérdései – Az uniós adatvédelmi rendelet (GDPR) fényében. https://adatvedelmi.hu/felhoszolgaltatasok-adatvedelmi-kerdesei-az-unios-adatvedelmi-rendelet-gdpr-fenyeben/; letöltés: 2020.12.23.
- Guidance for Organisations Engaging Cloud Service Providers. Data Protection Commission, 2019. https://www.dataprotection.ie/sites/default/files/uploads/2019-10/Guidance%20for%20Engaging%20 Cloud%20Service%20Providers_Oct19.pdf; letöltés: 2021.03.15.
- Guidance on the use of cloud computing. Information Commissioner's Office, Data Protection Act, 1998. https://ico.org.uk/media/about-the-ico/documents/1042330/cloud-computing-guidance-for-organisations.pdf; letöltés: 2021.03.15.
- Iránymutatás az (EU) 2016/679 rendelet szerinti átláthatóságról. WP260 rev.01. A 29. cikk szerinti Adatvédelmi Munkacsoport, 2017.11.29. https://naih.hu/files/wp260rev01_hu.pdf; letöltés: 2021.03.04.

- Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e. https://www.naih.hu/files/WP248_rev01_hu.pdf; letöltés: 2021.03.15.
- KOVÁCS László: A kibertér védelme. Dialóg Campus Kiadó, Budapest, 2018. https://www.uni-nke.hu/document/uni-nke-hu/Kov%C3%A1cs%20L%C3%A1szl%C3%B3.pdf; letöltés: 2021.03.11.
- Mi a nyilvános, magán- és hibrid felhő? Bevezetés a felhőszolgáltatások üzembe helyezési lehetőségeibe. https://azure.microsoft.com/hu-hu/overview/what-are-private-public-hybrid-clouds/#faq; letöltés: 2021.01.19.
- MOZDZYNSKI, Daniel: The Conceptions of new payment methods based on revised payment services directive (PSD2), Information Systems in Management, Volume 6, Number 1, 2017. pp. 50–60. https://www.researchgate.net/publication/317841044_THE_CONCEPTIONS_OF_NEW_PAYMENT_METHODS_BASED_ON_REVISED_PAYMENT_SERVICES_DIRECTIVE_PSD2; letöltés: 2021.03.17.
- NAIH/2015/21/20/H. (NAIH-17/2014/H.) személyes adatok kezelése az Intrum Justitia Zrt. és az Intrum Justitia Kft. követeléskezelési tevékenysége során (határozat). https://naih.hu/files/21_2015_hatarozat.pdf; letöltés: 2021.03.15.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). https://eur-lex.europa.eu/eli/reg/2016/679/oj; letöltés: 2021.01.19.
- TÓTH Fanni: A GDPR-ról – különös tekintettel a könyvtárakra és levéltárakra. Debreceni Jogi Műhely, XV. évfolyam, 1-2. szám, 2018.07.08. pp. 63–75. https://ojs.lib.unideb.hu/DJM/article/view/6911/6360; letöltés: 2021.01.17.
- VRÁNICS Dávid Ferenc – PALIK Mátyás: Mission as a Service – Egy felhőalapú UAS megvalósítása. Repüléstudományi Közlemények, 31. évfolyam 3. szám, 2019. pp. 153–167. https://folyoirat.ludovika.hu/index.php/reptudkoz/article/view/265/2801; letöltés: 2021.03.10.
- What EU institutions and Europe need to do to succeed in the digital economy. CISPE.cloud. https://cispe.cloud/cispe-manifesto/; letöltés: 2021.02.13.
- What is a private cloud? Microsoft Azure. https://azure.microsoft.com/en-us/overview/what-is-a-private-cloud/; letöltés: 2021.03.04.
- Working Paper on Cloud Computing – Privacy and data protection issues – „Sopot Memorandum”. International Working Group on Data Protection in Telecommunications, 51st meeting, 23-24 April 2012, Sopot (Poland). http://germanitlaw.com/wp-content/uploads/2012/04/Sopot-Memorandum1.pdf; letöltés: 2021.03.15. https://naih.hu/files/IWGDPT---Sopot-Memorandum--HUN.pdf; letöltés: 2021.03.15.

DR. FÓRIZS SÁNDOR NY. R. DANDÁRTÁBORNOK

A HATÁRŐRSÉG FELDERÍTŐSZOLGÁLATÁNAK TEVÉKENYSÉGE 1951–1952-BEN

Bevezetés

A határőrség felderítőszolgálata 1950–1956 közötti helyzetét, tevékenységét több színvonalas, adatokban gazdag publikáció is feldolgozta.[1] A szerzők többéves időszakot vizsgálnak átfogóan és a nagy összefüggéseket, a jelentős adatokat mutatják be. Az én célom az apró eseményeken keresztül érzékeltetni az 1950–1952-es időszakban kialakult rendkívüli helyzetet és a bekövetkezett különleges eseményeket.

Az adatokat a Magyar Nemzeti Levéltár Országos Levéltára Lángliliom utcai anyagából merítettem. Itt az érdeklődő megtalálja a határőrség dokumentumait évek szerint dobozokba sorolva. Alapvetően a „HOP XIX-B-10" jelzésű (HOP, Határőrség Országos Parancsnokság) 1951–1952. évi anyagaira támaszkodtam. A parancsokon és jelentéseken kívül rendkívüli adatgazdagságuk miatt külön megemlítem a naponta készült parancsnoksági ügyeleti jelentéseket. A napi összefoglaló tájékoztatókat megküldték az elöljárónak és a társszervek vezetőinek. Mivel 1951-ben a határőrizet főiránya, súlypontja már a jugoszláv államhatár volt, a napi jelentések belső tartalmi sorrendje is a jugoszláv, majd az osztrák, ezt követően az úgynevezett „baráti viszonylatok" történéseit tartalmazza.

A befejező fejezet a saját alakulaton belüli események, balesetek, szökések, rendkívüli események, amelyek magukban is nagyon érdekesek. A felderítőmunka számtalan mozzanatára is találunk itt információt. A határ mellett történt elfogást vagy éppen büntetlen határsértést – ez bekövetkezhetett kifelé vagy befelé is – másnap már jelenti az ügyeletes tiszt. Amennyiben az elfogott személyt később ellenséges ügynöknek minősítették, ezt utólag ceruzával beírták a jelentésbe UDB,[2] esetleg CIC,[3] ritkábban FSS[4] jelzéssel. A felderítőtisztek egyik feladata volt az elfogottak kihallgatása, az események „visszagöngyölítése", kapcsolatok, személyek, okok és helyszín keresése. Így számtalanszor előfordul, hogy az anyag egy kifelé vagy befelé

[1] ORGOVÁNYI István: Az Államvédelmi Hatóság Határőrség felderítő osztályának megszervezése és tevékenysége 1950 és 1956 között. I–II. rész. Betekintő, 2015/1. és 2015/2. szám.
https://betekinto.hu/sites/default/files/betekinto-szamok/2015_1_orgovanyi.pdf; letöltés: 2021.03.10.
https://betekinto.hu/sites/default/files/betekinto-szamok/2015_2_orgovanyi.pdf; letöltés: 2021.03.10.
JAKUS János: Titkos háború a déli államhatár mentén az '50-es évek elején. Közép-Európai Közlemények, V. évfolyam 1. szám, 2012/1. No. 16. pp. 42–54.
http://vikek.eu/wp-content/uploads/2014/02/KEK-16.pdf; letöltés: 2021.03.14.

[2] UDB – Uprava Državne Bezbednosti– Állambiztonsági Igazgatóság, jugoszláv katonai felderítési és hírszerzési szervezet.

[3] CIC (levéltári anyagokban C.I.C.) – Counter Intelligence Corps – az Amerikai Egyesült Államok hadseregének hírszerző szolgálata. Ebben az időben a szövetséges hatalmak által megszállt Ausztriában is működött. Rendszeresen kihallgatták a kiszökött személyeket, illetve különböző feladattal illegálisan visszaküldtek egyeseket.

[4] FSS – Field Security Section – Tábori Biztonsági Részleg, brit katonai hírszerző szervezet. Ebben az időben Ausztria brit megszállási övezetében is tevékenykedett.

bekövetkezett büntetlen határsértést tartalmaz, azaz az ismeretlen személy átjutott az államhatáron, majd talán öt hónappal később megjelenik a ceruzás bejegyzés, például „Elfogva 10.12-én.”, „UDB ügynök”.

A határőrség részéről külföldön, délen és nyugaton folytatott úgynevezett „külső”, azaz a szomszédos ország területén folytatott felderítést csupán áttételesen érintem, az általam feldolgozott anyagok konkrét eseteket nem tartalmaznak. Ilyen jellegű tevékenység a „baráti viszonylatokban” a határőrség részéről nem folyt. Egy év napi jelentései, vagyis több száz oldalnyi anyag, a levéltárban egy nyilvántartási számon fut,[5] ezért a pontos hivatkozásoknál esetenként a hónap és a nap megjelölését lehet alkalmazni.

A határőr felderítőszolgálat működésének sajátosságai, feladatai

Miután a Tájékoztató Iroda 1948. június 19. és 23. között tartott bukaresti értekezletén határozatban ítélte el a Jugoszláv Kommunista Pártot, a magyar politikai vezetés rendkívüli agresszivitással lépett fel Jugoszláviával szemben, „fasisztának”, az „imperialisták ügynökének” bélyegezve minden alap nélkül a szomszédos országot. A határőrizeti erők zömét ezt követően a jugoszláv államhatárra csoportosították, az osztrák irány másodlagossá vált.

Ha az 1950-es évet, az ÁVH Határőrség és felderítőszolgálata alapítási évét nézzük, az alábbi adatokat lehet megemlíteni: a 4071 nyilvántartott határsértőből 3616 főt fogtak el. Az osztrák és a jugoszláv szakaszon 395 fő büntetlen határsértés következett be, ebből kifelé 194 esetben 322 fő, befelé 66 esetben 73 fő. 1950 januárjában alakult a felderítőosztály, a zászlóaljaknál április 30-tól működtek felderítőcsoportok. Hálózati úton 896 főt fogtak el.

A felderítőszervek 1014 hálózati személyt foglalkoztattak, 50 esetben tettek át személyt az államhatáron felderítési céllal. Politikai megbízhatatlanság miatt 504 tisztet/tiszthelyettest eltávolítottak, 20 magasabb beosztású vezetőt leváltottak. Hazaárulás, azaz határőr külföldre szökése 38 fő részéről következett be, főleg Jugoszláviába.[6] 1951-ben 14 esetben 21 határőr szökött ki külföldre.

Fontosabb intézkedések, körülmények, melyek a felderítőmunkát befolyásolták:

– Műszaki zárat, aknamezőt és nyomsávot építettek ki a déli és a nyugati határon. Az aknamező olyan mértékben veszélyes volt – részben a szabálytalan telepítések és a gyenge minőségű anyagok miatt –, hogy a szökni szándékozók mellett a határőrök is nagy számban sérültek, illetve haltak meg miatta.[7] Még a nagyatádi kerület parancsnoka is felrobbant egy helyszíni bejárás alkalmával.

---

[5] MNL HOP XIX-B-10 1952. év 3., 4., 5. sz. doboz I/3. tárgykör 6. folyószám. Ügyeleti jelentések.
MNL HOP XIX-B-10 1951. év 2., 3., 4., 5. sz. doboz I/3. tárgykör 139. folyószám. Ügyeleti jelentések.

[6] MNL HOP XIX-B-10 1950. év 39. sz. doboz I/5. tárgykör 3. folyószám. Jelentés, 1950.12.12. „Tárgy: Évi beszámoló a Határőrség és Belső Karhatalom 1950. évben végzett munkájáról.”

[7] VARGA János: A határportyázó századoktól a határrendészeti kirendeltségekig. Magyar Rendészet, XV. évfolyam 6. szám, 2015. pp. 133–146.
https://folyoirat.ludovika.hu/index.php/magyrend/article/view/3569/2852; letöltés: 2021.03.09.

– Határövezetet (15 kilométer mélységben) és azon belül egy 50, valamint egy 500 méteres határsávot hoztak létre, ahová a beutazás, belépés engedélyhez volt kötve. Ezzel a mélységből a szükséges engedély nélkül jövőket már a vonatokon ki lehetett szűrni.

– Ausztriában az államhatár túlsó oldalán szovjet megszállási zóna húzódott 1955-ig. A szovjetek visszaadtak minden elfogott személyt. A kifelé igyekvő határsértőknek ezen az övezeten is át kellett haladniuk az angol zónáig, hogy biztonságban legyenek, ebben általában támaszkodhattak a helyi osztrák lakosság segítségére. A güssingi szovjet parancsnokság által visszaadott személyeket a felderítőszolgálat hallgatta ki, tudni szerették volna, hol, mikor, kinek a segítségével és milyen módszerrel sikerült átlépniük az államhatárt. A nyugati felderítőszervek gyakran küldték be ügynökeiket az országba. A magyar oldal határközeli településein nagy számban embercsempészek működtek.

– A nyugati és a déli államhatáron a szolgálati utak kivételével jelentősen lecsökkent a határforgalom, és megszűnt a kishatárforgalom. A kettősbirtokosok tevékenysége ellehetetlenült. 1951. november 17-én feloszlatták a murakeresztúri forgalomellenőrző pontot, mert a Közlekedési és Postaügyi Minisztérium leállította a Murakeresztúr–Kotor közötti vasúti forgalmat.

– A két oldalon élő rokonok legálisan nem érintkezhettek egymással. A jugoszlávok a Dráván két hidat is felrobbantottak a saját oldalukon. Információt, adatokat beszerezni a túloldali területekről korlátozottan lehetett. A magyar határőrség összefüggő csapatfigyelési rendszert működtetett. Ez az optikai eszközökkel belátható mélységig, maximum öt kilométerig – amennyiben nem esett az irányba erdő stb. – jelentette az eseményeket, amelyeknek azonban különösebb felderítési értéke nem volt. A napi feljegyzésekben általában az alábbiak szerepelnek: műszaki és gazdasági munkálatok, jugoszlávok járőrözése, gyakorlatok, aknatelepítés, katonai és polgári személyek mozgása stb. Mindezek miatt mindkét fél erőltette ügynökök átküldését az államhatáron adatgyűjtés, propagandaanyagok beküldése és a jugoszlávok részéről a Magyarországon élő szerb nemzetiségű lakosokkal történő kapcsolattartás céljából.

A határőr felderítőszolgálat az adott viszonyokhoz és saját létszámához mérten feladataiban túl lett terhelve, a központi elvárásokat teljes egészében nem volt képes teljesíteni. A szolgálat fontosabb feladatai voltak:

– Az elfogott határsértők kihallgatása, ezzel a tevékenységgel adatok szerzése, a kihallgatás befejezéséig a személyek fogdában történő őrzése (ezt külön őrszemélyzet végezte), majd a határsértők átadása az ÁVH megyei osztályainak.

– Az ország mélységéből államhatár irányába utazó és a járőrök által előállított személyek ügyének vizsgálata. Annak megállapítása, hogy volt-e kiszökési szándékuk.

– A sikeres kiszökések esetében operatív eszközökkel az elkövető személyének megállapítása, menetvonalának, esetleges segítőinek azonosítása.

– A befelé történt határsértések esetében tipikus mozzanat volt, hogy a nyomsávellenőrző járőr fedte fel a történteket, és a zászlóalj a mélység lezárásával, csapatkutatással razziát vezetett be. Ehhez kapcsolódott a felderítőszolgálat operatív kutatással a személy kilétének megállapítására.

– A felderítőszolgálatnak úgynevezett hálózatot, hálózati személyeket kellett működtetnie, fenntartania. A magyar területen élő hálózati személyek olyan helyi lakosok voltak, akik önként, meggyőződésből, esetleg kényszerítés, zsarolás, fenyegetés hatására vállalták az együttműködést a felderítőtiszttel. Adatokat szolgáltattak ismeretlenek megjelenéséről, a határőrség által érdekeltek tevékenységéről, embercsempészetre vagy kiszökési szándékra utaló jelekről. Megfigyelték a rájuk bízott egyéneket, családokat, szükség esetén riasztották a megbízójukat.

– Az embercsempészet elleni fellépés a szolgálat egyik legfontosabb feladata lett. A jól megszervezett, jelentős létszámú járőrszolgálat szinte biztosan elfogta a szökni szándékozókat, de alapvetően tehetetlen volt a helyi lakosok által vezetett határsértőkkel szemben. A kialakult rendszerben külön személyek hozták le a fizetős ügyfeleket a távoli városokból (pl. Budapest), határközeli településeken házakban rejtve pihentek, majd az éjszakai órákban már más csempészek levitték őket az államhatárig. Nem volt ritka a fegyveres kísérés sem. Természetesen maradtak nyomok a nyomsávon, gyakran látni lehetett, hol fordult vissza az embercsempész, melyik településig lehetett visszakövetni a nyomokat. Ismét a felderítőtisztek kerültek előtérbe, ha a katonai eszközök már nem hoztak eredményt. A tevékenység határőrségre nézve különösen veszélyes változata volt a fegyveres kisérő, illetve amikor az államhatár túloldalán fegyveresek várták a kiszökőket, esetleg már átjárót is nyitottak a műszaki záron.

– A határőrség ebben az időben nem nézte jó szemmel, ha az őrsi katonák a helyi lakossággal barátkoztak, szorosabb kapcsolatot építettek ki. Állandóan a civilek és a katonák közös kiszökésétől rettegtek, ami egyébként többször is bekövetkezett. Ezért elvárták, hogy a felderítőtisztek az ilyen kialakuló barátságról, esetleges szerelmi kapcsolatokról is személyes vagy hálózati úton adatokhoz jussanak. Bár szorosan véve a katonák hasonló jellegű ügyei, esetleges szökési szándékai a határőrségnél is működő elhárító szolgálat hatáskörébe tartoztak, itt a két szolgálat közösen volt érintve. A szolgálat hatáskörébe 1950. december közepén összesen 9 kerület, 13 zászlóalj, 39 század, 192 őrs, 32 határforgalom ellenőrzési kapitányság – majd forgalomellenőrző pont (FEP) az új megnevezéssel – és 1 tiszti és tiszthelyettesi iskola tartozott.

– 1950–1955 között valóságos ügynökháború dúlt a magyar és a jugoszláv felderítőszervek között egészen addig a pillanatig, amíg a két ország politikai viszonyai nem rendeződtek. A feladatok e területéről részletesebben jelentőségük miatt külön pontban írok.

– Az árucsempészet és az államhatár jogtalan átlépésének felderítése is a szolgálat hatáskörébe tartozott, különösen csehszlovák és román viszonylatban. Az árucsempészet – jellemzően lábbeli és ruhafélék, tűzkő, technikai eszközök – gazdaságilag lényegében jelentéktelen értéket képviselt. A tiltott határátlépések – ha nem csempészetről volt szó – általában rokonlátogatáshoz, temetéshez, születéshez, családi eseményekhez kapcsolódtak. Normális utazási, látogatási, határátlépési lehetőségek megléte esetén a szolgálatnak és az egész határőrségnek lényegesen kevesebb feladata lett volna. Az okmányok gyakran tartalmazzák, hogy csehszlovák viszonylatban az elfogás hálózati adat alapján történt, valaki jelentette. Ennek, mivel a legtöbbször csempészethez vagy az említett családi rendezvények valamelyikéhez kapcsolódott, egészen más volt a súlya, mint a déli és a nyugati államhatáron.

– A felderítőtisztektől elvárták, hogy a helyi tanácsok, pártszervezetek, rendőrség vezetőivel, beosztottjaival szoros kapcsolatot tartsanak fenn, tőlük adatokat, információkat szerezzenek, amelyeket a határőrizet megszervezése területén lehetett felhasználni.

– A szolgálat és az egyes tisztek működéséhez meghatározott, igen bürokratikus, irodai, nyilvántartási előírások kapcsolódtak a meghallgatási jegyzőkönyvek vezetésétől az ügynöki dossziék felfektetéséig. Mindezeket a munkákat az akkori viszonyok között gyakran gépkocsi nélkül, kerékpárral, kevés írógéppel, rossz telefonos összeköttetési viszonyok között és a munkatársak gyenge szakmai felkészültsége mellett kellett végezni.

– Külön feladatrendszert képezett a terepen folyó munka, a helyszínek megtekintése, szemrevételezés az eseményeket követően vagy ügynöki átdobások előtt, részvétel kivizsgálásokban. Korántsem veszélytelen tevékenységről van szó. Egy aknán felderítőtiszt robbant fel a letenye-szigeti szemrevételezéskor, valószínűleg az előző nap Jugoszláviába kiszökött határőr ügyének kivizsgálása közben.

A határőrség felderítőszolgálata

A magyar határőrség 1949. december 31-éig a honvédség állományába tartozott Honvéd Határőrség néven. A szervezetnek már akkor volt felderítőapparátusa.[8] A felállítására vonatkozó információkat az Állambiztonsági Szolgálatok Történeti Levéltára őrzi.[9] 1950. január 1-jével a határőrség átkerült az Államvédelmi Hatóság ekkor felállított IV. főosztálya (Határőrség és Belső Karhatalom) kötelékébe, a Minisztertanács alárendeltségébe, és ekkor jelentős szervezeti módosításokat hajtottak végre, valamint nagyszámú személyzeti elbocsátás, illetve felvétel történt. Az átszervezés lényegében 1952-ig eltartott.

A lényegesen több feladatot kapott felderítőszerveket át-, illetve újraszervezték. 1950 januárjában alakult meg az ÁVH Határőrség Főparancsnokság Felderítő Osztálya. A határőrségnél ennek osztályvezetője lett a felderítőtevékenység csúcs szakmai képviselője. A rendszerben lefelé a kerületeknél felderítőalosztályokat, a zászlóaljaknál felderítőcsoportokat állítottak fel. A zászlóaljak alárendeltségében működő határőrőrsöket felelősség vonatkozásában szétosztották a felderítőcsoportok tisztjei és tiszthelyettesei között (iránytartók). A frissen felállított struktúrát nem tudták a felderítőmunka végzésében tapasztalt munkatársakkal feltölteni. A szintén az ÁVH-hoz került határrendőrség hivatásos állományából csoportosítottak át embereket, de ezek jó része – bár rendőr néven futott – eddig határforgalom-ellenőrzéssel foglalkozott, így szintén nem értett az új típusú feladatokhoz. Magától az állami rendőrségtől sem tudtak elegendő szakembert átirányítani. Mindezek miatt a kezdéskor 1950–1953 között teljesen tapasztalatlan, felkészületlen gárdával indultak neki a növekvő feladatoknak. A személyi állomány 90%-a mindössze rövidebb-hosszabb idejű operatív iskolát végzett, és 1951 márciusáig semmilyen katonai vagy szakmai továbbképzésben nem részesült.

---

[8] VARGA János: A magyar határőrizeti szervek reagáló képessége (1867-1989). Rendőrtiszti Főiskola Rendvédelmi füzetek, 1999/26. szám. pp. 1–23.

[9] ÁBTL 1.11. 7-436/6/31. 23. d. A Honvéd Határőrség elhárító-felderítő szolgálatának megszervezése és felépítése, 1945–1948.

1950 novemberében 116 operatív beosztott volt állományban, így a határőrség felderítése 40 tiszttel és 76 tiszthelyettessel rendelkezett az állam öt országhoz kapcsolódó 2215 kilométeres határán. A déli és a nyugati viszonylatú zászlóaljaknál összesen 88 felderítő, közülük 27 tiszt és 61 tiszthelyettes dolgozott. 1953-ban a felderítőapparátus operatív állományának szervezetszerű létszáma már 225 fő, de csak 194 hely volt betöltve, 31 fő hiányzott az állományból. A felderítőszervek létszáma 1954 szeptemberében 183 fő.[10] A létszám elégtelenségét a feladatokhoz mérve azonnal beláthatjuk, amennyiben az állandóan változó szervezettel összehasonlítjuk. 1951-ben a 618 kilométer hosszúságú jugoszláv államhatáron 3 határőrkerület, 11 zászlóalj, 81 őrs és 3 forgalomellenőrző pont (FEP) működött.

Mivel nem volt elég szakember, ezért a felderítőerőket 1951 januárjában kerületek közötti átcsoportosítással megerősítették, a külső és a belső felderítés céljára 4-4 főt vesznek el az egyéb irányú kerületektől. „*Figyelembe véve a jugoszláv határszakaszt, mint súlyterületet*”[11] szól az indoklás a 2., 3., 4., 5. kerületeknél (dél és nyugat), az állománytábla feletti létszámemelést kívánnak elérni a 6., 8., 9. kerületektől elvett munkatársakkal. Kerületenként kettő fővel a külső és egy fővel a belső felderítést kell megerősíteni.

A helyzeten nem sokat segített, hogy befejeződött az öthetes felderítőtanfolyam. „*A tanfolyam hallgatói fiatal gyakorlati tapasztalattal nem rendelkező bajtársak, akik a felderítő munka elvégzéséhez szükséges* [ide a parancsba tollal kézírással betoldva „minimális”] *elméleti alapot elsajátították.*”[12] Szabályozták a végzettek fogadásának rendjét, a tartásra átadandó hálózati személyek anyagának tanulmányozását, kivitelüket találkozóra, az érvényben lévő utasítások bemutatását.

Hivatalosan az egyik legnagyobb problémának a magyarországi délszláv lakosság támogatásának hiányát látják.[13] Közülük többen szolgáltak a jugoszláv partizánok sorában, rendelkeznek az államhatáron átnyúló rokoni kapcsolatokkal, vagy szenvedtek el üldöztetést 1941-től nemzetiségi hovatartozásuk miatt. Őket tekintik a jugoszláv felderítőszervek lehetséges belső ügynökeinek. Támogatásuk megnyerésére külön parancsban intézkedett az országos parancsnok,[14] de annak belső fogalmazása kizárja az eredményt, hiszen nem tudják a fő problémákat, az országos politika hibáit ellensúlyozni. Látják, „*a délszláv lakosság még sok helyen nem segíti elő a határőrzés feladatainak, célkitűzéseinek valóra váltását*, *… sőt többször előfordul, hogy erkölcsileg és anyagilag támogatják a határsértőt.*” A határőrök „*a délszláv lakosságot egyes helyeken egészében ellenségnek tekintik*”.

---

[10] ORGOVÁNYI István: Az Államvédelmi Hatóság Határőrség felderítő osztályának megszervezése és tevékenysége 1950 és 1956 között. I–II. rész. Betekintő, 2015/1. és 2015/2. szám. https://betekinto.hu/sites/default/files/betekinto-szamok/2015_1_orgovanyi.pdf; letöltés: 2021.03.10. https://betekinto.hu/sites/default/files/betekinto-szamok/2015_2_orgovanyi.pdf; letöltés: 2021.03.10.

[11] MNL HOP XIX-B-10 1951. év 1. sz. doboz I./1, I./2 tárgykör 1-18. folyószám. 09. sz. parancs. 1951.01.09.

[12] MNL HOP XIX-B-10 1951. év 1. sz. doboz I./1, I./2 tárgykör 1-18. folyószám. 045. sz. parancs. 1951.05.23.

[13] DEÁK József: A rendészettudomány kialakulása és gondozásának nemzetbiztonsági, határőrizeti példái a Belügyi Szemlében a rendszerváltásig. Nemzetbiztonsági Szemle, IV. évfolyam 4. szám, 2016. pp. 43–75. https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1883/1172; letöltés: 2021.03.12.

[14] MNL HOP XIX-B-10 1951. év 1. sz. doboz I./1, I./2 tárgykör 1-18. folyószám. 028. sz. parancs. 1951.03.22. „Tartalom: Délszláv lakosság között végzett politikai munka és a délszláv lakosság fokozottabb megnyerése a határőrzés és honvédelem érdekeinek.”

A politikai munka hiányosságaira vezették vissza a nehézségeket, „*nem konkrét, nem fogja át a Tító- banda kegyetlenkedéseit, a jugoszláv dolgozók nyomorát, nem nevel eléggé a Tító- ellenes és imperialista-ellenes gyűlöletre*”, lényegében saját nemzete ellen akarja fordítani az érintett lakosságot, „*le kell leplezni az imperialisták és titóista fasiszták háborús készülődését, a titóista fasiszta terrort*”.[15] A feladatok megoldását a parancs a kerületek politikai alosztályai vezetőire bízza. Megoldási eszközök: havonta a falvakban előadást tartani, fellépni a katonák lakossággal szembeni durvasága ellen.[16]

A felderítőmunka végzéséhez kiadták az *Instrukció a felderítő szervek munkájáról*[17] megnevezésű anyagot, amely 1951. április 23-án lépett érvénybe. Természetesen szigorúan titkos minősítésű, a kerület felderítő-alosztályvezetője tárolja, az operatív állománynak oktatják, havonta jelenteni kell, hogy megvan(!), lemásolni, abból jegyzetet készíteni tilos. Júniusban nagy átfogó parancsban szabályozták országos szinten a felderítőmunka végzését.[18]

A parancs kifogásolja, hogy nincsenek összefoglaló nyilvántartások, elemzések a kerületeknél az ellenséges elemekről, „*ennek eredményeképpen nem mutatható ki az ellenséges erő valódi helyzete… ami megnehezíti megfelelő intézkedések kidolgozását az ellenük folytatandó harcban.*” Részletes napi és havi jelentési rendszert alakítottak ki.

A kerület felderítő-alosztályvezetője összesíti a zászlóaljaktól beérkező jelenéseket, „*csatolja az osztályellenség tevékenységének fontosabb eseteiről készült jelentést*”, a fogalmazás már jelzi a felderítőtevékenység egyik félrecsúszott feladatát, mert „*számszerűen ki kell mutatni a megállapított bűntettesek szociális összetételét*”. Egyébként a határterületről származó elkövetők jelentős része földműves volt, esetenként lehetett beírni, hogy kulákszármazású.

Az előírt havi jelentés tételei között szerepeltek a következő pontok:

„*a) Terrorista akciók /politikai okokból elkövetett gyilkosságok vagy támadás párt és állami funkcionáriusok ellen, úgyszintén az ilyen irányú szándék/.*

b) Diverzáns akció /gyújtogatás, tömegmérgezés, robbanás stb., úgyszintén külön diverzió gyanús esetek/.

c) Szabotázs és szabotázsgyanús cselekmények /munka tudatos akadályozása, kötelezettség nem teljesítése, vagy hanyag teljesítése/.

d) Tömeges demokrácia ellenes megmozdulások és erre való felbujtások.”[19]

---

[15] Uo.

[16] DEÁK József: Az állambiztonsági propaganda, annak kialakulása és fejlődése – nemzetbiztonság és civil kapcsolatok. Társadalom és Honvédelem, 17. évfolyam 3–4. szám. NKE Szolgáltató Nonprofit Kft., Budapest, 2013. pp. 408–417.

[17] MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám. 035. sz. parancs. 1951.04.23.

[18] MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám. 054. sz. parancs. 1951.06.29. „Az Államvédelmi Hatóság Határőrség felderítő szervei operatív beszámolásának módjáról és határidejéről.”

[19] Uo.

Ezeknek a jelentési szempontoknak nincs sok közük a határőrizethez, azokban keverednek a határőrizeti szakmai és az állambiztonsági feladatok.

A negyedik határőrkerület (akkor Pécs) felderítőmunkájának ellenőrzésénél típushibákat állapítottak meg:

- „*Nem veszik figyelembe, hogy a kerület határszakaszával szemben dolgozó népünk legelvetemültebb ellensége Tító és bandája áll*";[20]
- kevés a hálózati úton elfogott személy;
- nem épülnek be a határsávba beépített UDB-rezidentúrákba;
- a hálózatok összetétele nem kielégítő, a hálózati egyének sok esetben dekonspirálódnak;
- ellenőrzési és oktatási hibák tapasztalhatók;
- az operatív munkatársak sok esetben indokolatlanul éjszaka is bent maradnak a munkahelyen;
- „*A vezető bajtársak liberálisan bánnak beosztottjaikkal. Nem követelik meg a katonai vasfegyelmet.*"[21]

Ügynökháború

Mind a déli, mind pedig a nyugati államhatáron valóságos ügynökháború dúlt, súlyponttal Jugoszlávia irányába. Az ügynökök jugoszláv részről az államhatáron átküldött személyek voltak, akiknek a legkülönbözőbb adatokat kellett beszerezniük a szovjet és a magyar csapatok helyzetéről, a lakosság hangulatáról, a magyar határ mellett épülő erődvonalról. Gyakran hoztak át magyar nyelvű kiadványokat. Feladatuk volt hálózat kiépítése, személyek beszervezése, a határsértések segítése helyismeretük révén. A Jugoszláviából érkezők jórészt magyar nemzetiségű magyar vagy jugoszláv állampolgárok voltak, hiszen elengedhetetlennek bizonyult a magyar nyelv használata az ország mélységében. A magyarországi szerbeket az UDB előszeretettel vette igénybe (kényszerítette) ilyen tevékenységre. Sokan rendelkeztek rokoni kapcsolatokkal a határ menti településeken, ami lehetőséget adott az elrejtőzésre. Az ügynökök – mivel lényegében nem volt határforgalom – talán az egyetlen eszköznek bizonyultak a felderítés számára, hogy a mélységi területekről információkat szerezzenek, de a legtöbb esetben ezeknek a beszerzett adatoknak az értéke igen kétséges volt.

Az átdobásoknak – vagy ellenkezőleg, az átküldött személyek elfogásának – szabályos forgatókönyvei alakultak ki, és a jugoszláv, valamint a magyar fél váltakozó sikerrel alkalmazta ezeket. A hazánkba történő beküldésnek általában még éjfél előtt meg kellett történnie, hogy a határsértő világosodásig valamelyik lakott települést, tanyát, a belső segítséget, busz- és vasútállomásokat elérje. Az akció kezdetét rendszerint szemrevételezés előzte meg UDB-tisztek és a jövőbeni ügynök részvételével, kiválasztották a műszaki záron történő áthaladás helyét, a mélységbe

[20] MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám. 067. sz. parancs. 1951.08.03.
[21] Uo.

vezető optimális menetvonalat, tanulmányozták a magyar járőrrendszert, különös tekintettel az éjszakai nyomsávellenőrzés rendjére. A Dráván csónakkal hozták át a személyeket. A szemrevételező csoportok esetleges felfedése magyar részről fogadási előkészületekhez vezethetett, ezért gyakran alkalmaztak látszatszemrevételezéseket az erők bizonyos irányokból történő elvonása érdekében. Ugyanezt a célt szolgálta az átdobás idején a helyszíntől távolabb lövöldözés kezdése, határsértés imitálása, rakétázás stb. Az ügynököt biztosító csoport kísérte le az államhatárig, esetleg azt átlépve egészen a műszaki zárig, átjárót nyitva számára drótvágással, akna felszedésével. Géppisztolyos, golyószórós katonák fedezték a tevékenységet, a magyar részről történt észlelés esetén figyelmeztető lövésekkel tartották távol a magyar járőreinket a beavatkozástól a csoport visszavonásáig. Természetesen az volt számukra a legkedvezőbb változat, ha az átdobásnak nem maradt nyoma a műszaki záron, azt a nyomsávellenőrző járőr nem fedte fel, és a személy titokban bejutott a mélységbe. A határsértések látenciája igen magas volt, többnyire egy elfogást követően derült fény a megelőző esetekre.

Az ellenintézkedések rendszerében a túloldali terület és a műszaki zár folyamatos figyelése volt az első feladat. Ha a nyomsávon befelé irányuló nyomokat észleltek, és még nem telt el hosszú idő a bejöveteltől, esély nyílt a személy elfogására. A csapaterő területeket zárt le, az üldözők nyomozó kutyával próbálták követni a nyomokat. A felderítőtisztek a településeken aktivizálták kapcsolataikat, ellenőrizték a közforgalmú járműveket. A kifelé igyekvő ügynökök fogadásánál a jugoszlávok szintén alkalmaztak megtévesztő tevékenységet a figyelem elterelése céljából, fény- és rakétajelzésekkel mutatták az éjszakában az optimális vagy éppen a veszélyes irányokat, a magyar járőrök helyét.

Az elfogott ügynökök számára vonatkozóan megbízható adatokkal feltehetően nem fogunk rendelkezni. Az egyik publikáció szerint „*1951. január 1-je és december 10-e között déli viszonylatban 66 ügynököt fogtak el a határőrség szervei.*" Az ÁVH által készített egyik összefoglaló szerint 1950-ben a magyar határőrizeti szervek 31 titóista ügynököt vettek őrizetbe. „*1951-ben kémkedés miatt 321 főt vettek őrizetbe az ország területén, és ebből 106 főt titóista kémkedés miatt tartóztattak le.*"[22] Az előző adatok országosan érvényesek, magam csak a határőrség dokumentumait vizsgáltam. Az 1951. évi ügyeleti jelentések 17 fő CIC és 69 fő UDB-ügynök elfogását tartalmazzák. 1952-ben tíz hónap alatt az ügyeleti jelentések szerint 65 fő UDB-, 17 fő CIC-, 2 fő FSS- és 2 fő MHBK-ügynököt[23] fogtak el, az UDB-ügynököket többnyire a déli, a többieket a nyugati államhatáron.

A számadatokban bizonyos mértékig kételkednünk szükséges. Azon elfogott személyek esetében látom lehetségesnek az ügynöki minősítést, akiknél propagandaanyagokat, hamis személyi okmányokat, hamis határsáv- és határövezeti engedélyeket, ügynöki jelentéseket, Budapest területére szóló hamis bejelentőlapot, méregkapszulát, speciális eszközöket, fegyvereket találtak, magyar határőr egyenruhát

[22] ORGOVÁNYI István: Az Államvédelmi Hatóság Határőrség felderítő osztályának megszervezése és tevékenysége 1950 és 1956 között. I–II. rész. Betekintő, 2015/1. és 2015/2. szám. https://betekinto.hu/sites/default/files/betekinto-szamok/2015_1_orgovanyi.pdf; letöltés: 2021.03.10. https://betekinto.hu/sites/default/files/betekinto-szamok/2015_2_orgovanyi.pdf; letöltés: 2021.03.10.

[23] MHBK – Magyar Harcosok Bajtársi Közössége, szélsőjobboldali, katonai jelleggel felépített magyar emigráns szervezet.

viseltek, vagy fegyverhasználattal kísérelték meg a kijutást az országból. Sokszor túlzásnak találom azonban az ilyen megjelölést, amolyan „pontvadászatnak" ítélem a határőrség részéről. A felderítőszolgálat saját eredményei felturbózásaként indokolatlanul alkalmazta ezt a besorolást. Néhány az általam vitatott UDB-ügynökként besorolt esetek közül:

– 1951.09.05. Péterhida őrs, Milanovics Sztepan szerb nemzetiségű katona jött át, géppisztoly, 2 db kézigránát volt a fegyverzete. Nyilván nem fog egy ügynök jugoszláv katonai egyenruhában tevékenykedni.

– 1951.08.07. horvát nemzetiségű jugoszláv katona szökött át, pisztollyal, 4170 dinárral.

– 1952.05.09-én UDB-elfogásként szerepel Zalatkovics Milán szerb nemzetiségű jugoszláv határőr szakaszvezető, egyenruhában, géppisztollyal és két tár tölténnyel jött át. Az illető a szemben lévő határőrőrs (*karola*) parancsnoka volt, és reggel 06.20-kor fogták el, amint biciklivel átkerékpározott az államhatáron. Nyilvánvalóan áttévedésről van szó. Ebben az időszakban egy másik *karola* parancsnok is áttévedt, szintén ügynökminősítést kapott.

Találhatunk vitathatatlan eseteket is:

– 1952.10.23. UDB-ügynökjelzést viseli az esemény, ahol Szalafőn október 23-án 0.30-kor kifelé irányuló határsértéskor három fő vívott tűzharcot a járőrrel. Kettőt közülük a határőrök agyonlőttek, egy sebesülten kijutott, amit vérnyomok mutattak. Az agyonlőtt Oravecz Gyula és Oravecz Imre farkasfai lakosoknál egy-egy géppisztoly volt, és határőr egyenruhát viseltek. A túloldal figyelésekor észlelték, hogy a személyeket a túloldalon várták, a sebesültet gépkocsival elszállították.

– 1952.02.14-én a Hegykő őrs járőre elfogott két főt (egy férfit és egy nőt), akiknél fegyver is volt – Mauser puska 102 db lőszerrel, egy Király géppisztoly 6 tárral, 208 db lőszerrel, két pisztoly– valamint robbanóanyag és egy a határőrség tulajdonát képező zseblámpa. Lehetséges, hogy ez a határőrségi lámpa indította be azt az operatív munkát, amelynek során elfogtak még három személyt, egyikük Kiss Bertalan határőr a Hegykő őrsről. Az öt személy együtt akart kiszökni.

Említsünk meg egy példát a sikertelen átdobások közül:

– 1952.10.01. Dedecskecskés őrsön 20.00–21.00 között aknarobbanás történt, a magyar járőr 200 méterre volt a helyszíntől. Reggel kivizsgáláskor a műszaki zár és a nyomsáv között „*egy magyar legénységi mintájú téli katonasapkát /jugó csillaggal/, egy hátizsákot, egy 48 M géppisztolyt 70 db tölténnyel és egy magyar katonazubbony aknaszilánktól szétszaggatott ujját találták.*" A talaj, a hátizsák és a zubbonyujj vérrel volt szennyezve.[24] A földön a nyomok mutatták, amint a sérültet visszahúzták a műszaki zárról. Napokkal később egy jugoszláv földmunkás átszólt a magyar járőrnek és elmondta, hogy a felrobbant tisztet ő vitte lovaskocsin az orvoshoz. Az esetet külön publikáció is feldolgozta.[25]

[24] MNL HOP XIX-B-10 1952. év 3., 4., 5. sz. doboz I/3. tárgykör 6. folyószám. Ügyeleti jelentések. 1952.10.01.

[25] FÓRIZS Sándor: Rejtélyes határesemény a műszaki záron. Új Honvédségi Szemle, 1997/6. szám. pp. 39–42. http://www.forizs-sandor.hu/pdf/18.pdf; letöltés: 2021.03.11.

– Az UDB gyakran erőszakkal kényszerítette a jugoszláviai magyarokat ügynöki tevékenységre. Ezt egy feljegyzett átbeszélés esete is mutatja az ügyeleti jelentésekben. 1952.07.10-én egy asszony Jugoszláviából átbeszélt a magyar járőrnek, Nagyatád kerület Rédics őrsén. A göntérházai nő a fia, Gál Péter után érdeklődött, akit kollégájával, Varga Józseffel együtt „*1950 decemberében a jugoszlávok mindkettőt elvitték és a határon átdobták. A jugoszláv rádió bemondta, hogy Magyarországon mindkettőt felakasztották.*”[26] Ez a vissza- vagy átkényszerítés különösen veszélyes volt a kiszökött katonákra nézve. Steindl Tibor határőr Somogyudvarhely őrsön 1949-ben átszökött Jugoszláviába több társával együtt, miután az őrsön erőszakkal megszerzett fegyverekkel tartották sakkban a katonákat. Az UDB visszaküldte Magyarországra, ahol nem folytatott semmilyen tevékenységet. Két évig bujkált, szülei lakásán fogták el, és „katonai zendülés, szökés és kémkedés”[27] miatt kötél általi halálra ítélték, kivégezték. Elrendelték az esetről szóló parancs felolvasását minden köteléknél.[28]

Személyek visszaadása 1956-ban

A Jugoszlávia és Magyarország között hosszabb időn keresztül folytatott tárgyalások eredményeként 1956. december 7-én és 9-én hazatért 141 fő olyan személy, akik az októberi események során menekültek déli szomszédunkhoz. Az átadásra a röszkei és a murakeresztúri átkelőhelyeken hivatalosan, névjegyzék alapján került sor. Ugyanakkor a jugoszláv szervek átadtak 18 olyan személyt is, akikről a levéltár semmilyen adatot sem tartalmaz. Vélhetően kapcsolódnak az előző évek jugoszláv–magyar ügynökháborújához.[29]

Erről a 18 személyről – akiket a jugoszlávok decemberben külön adtak át Röszkén és a halasi határőrkerületnek jegyzőkönyvet kellett róluk készíteni – nem szerepel információ az iratgyűjtőben. Kilétükhöz egyik kapaszkodó az a megállapítás, hogy amnesztiában részesültek Jugoszláviában. A két ország ebben az időben kezd felülemelkedni mindazokon a sérelmeken, melyek 1941–1953 között felhalmozódtak. Talán ez az esemény is ezt jelzi. Rendelkezünk a halasi kerületparancsnok országos törzsfőnökhöz felterjesztett jelentésével 1956. szeptember 10-ei dátummal. Az írásban a parancsnok egy, a jugoszláv szervekkel folytatott helyi vegyesbizottsági ülésen elhangzottakról tájékoztat:

„*Május hónapban … a jugoszláv hatóságok 18 főt adtak át, köztük olyanokat is, akik mint ügynökök lettek kiküldve a Jugoszláv Szövetségi Népköztársaság területére. Május hónapban kerületünk szakaszán a jugoszláv szerveknek 9 fő átszökött személy lett visszaadva.*”

---

[26] MNL HOP XIX-B-10 1952. év 3., 4., 5. sz. doboz I/3. tárgykör 6. folyószám. Ügyeleti jelentések. 1952.07.10.

[27] MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám. 0114. sz. parancs. 1951.11.23.

[28] Az esetről részletesebben lásd a következő publikációt:
FÓRIZS Sándor: Külföldre szökések a határőrségtől 1951-ben. Belügyi Szemle, 62. évfolyam, 2014/6. szám. pp. 48–62.
http://www.forizs-sandor.hu/pdf/38.pdf; letöltés: 2021.03.04.

[29] FÓRIZS Sándor: Menekültek Jugoszláviában 1956. novemberben. Hadtudomány, XXX. évfolyam, 2020/1. szám. pp. 42–52.
http://real.mtak.hu/109492/1/042-052_Forizs.pdf; letöltés: 2021.03.11.

„Közölték a tárgyaláson, hogy szeretnék visszakapni Ursák Istvánt /: szül.: 1919.4.29. Szabadka :/, aki 1951-ben jött át, és tudomásuk szerint le van zárva. Továbbá Nagy László volt zentai lakost, aki 1953-év végén jött át, 1954-évben írt levelet feleségének a fogházból. Címe: Budapest, B.V.-volt….

Amennyiben a jugoszláv szervek által kért 2-fő átadása megtörténne, úgy a mi részünkről is volnának olyan személyek, akik visszaadását kérnénk, így Csapó Béla /: 1923. Bácskismonostor :/ volt jánoshalmi lakost, akit 1953 április 11-én feladatának végrehajtása közben a jugoszláv szervek elfogtak és 14-évi börtönbüntetést kapott. Nevezett felesége munkaképtelen, egy 3 éves gyermeke van, általunk havonta részesül anyagi támogatásban."[30]

Ez előzőekből kitűnik, hogy az elfogott ügynökök sorsának rendezése legalább 1957-ig eltartott.

Zárógondolatok

Publikációmban különleges viszonyokkal foglalkozom, a határőrség felderítőszolgálata 1951–1952. évi tevékenységével. Szinte minősített időszaki körülmények között, kimondatlanul, de rendkívüli jogrend feltételei alatt kellett a szolgálatnak az erejét, lehetőségeit meghaladó feladatokat teljesítenie. A Jugoszláviával megromlott kapcsolatok egyetlen oka a Szovjetunió rossz jugoszlávellenes politikájának túlhajszolt másolása, egy szolgai megfelelni vágyás, ami nem vette figyelembe az ország érdekeit. Ennek igazságtartalmát mutatja, hogy a szovjet politika változásával – 1956-ra időben eltolódva – a magyar hozzáállás is teljes fordulatot vett.

A felderítőszolgálat a határőrség nyílt csapattevékenysége, a járőrrendszerű határőrizet fontos kiegészítő elemévé vált.[31] Különösen az embercsempészek és az ügynökök elfogásában, az események „visszagöngyölítésében", a határsértőket segítő helyi lakosok felkutatásában és őrizetbe vételében – ahol a nyílt katonai eszközök nem vezethettek eredményre – lett a szolgálatnak kiemelt szerepe. Sajnos az országos politika elvárásai miatt az alkalmazott módszerek sújtották a magyarországi nemzetiségeket, különösen a szerbeket, akikre a határőrség vezetése is gyanakodva tekintett, de az átlagos határ menti lakosokat is, akiket elzártak az államhatár másik oldalán élő rokonaiktól. A felderítőmunka kibontakozását lassította a szakmailag felkészült munkatársak hiánya, a viszonylag alacsony létszám, és különösen a nyugati államhatáron a lakossági támogatás csekély mértéke. Nem kevésbé lett zavaró a szakmai határőrizeti felderítőtevékenység és az állambiztonsági feladatok folyamatos keveredése.

---

[30] MNL HOP XIX-B-10 1956. év 17. sz. doboz VI/1-7. tárgykör 86. folyószám. „Tárgy: Jugoszláv szervek felvetése."

[31] Erre a fontos kiegészítő elemre még sokáig szükség volt (és van) a határellenőrzési feladatok során. Ezt jelzi az is, hogy a határőrség hazánk EU-csatlakozása után is több mint 600 fős felderítőszervezetet működtetett, amely létszám a rendőrségbe integrálódás során sajnálatosan a huszadára csökkent.
RITECZ György: Határőrizet a rendszerváltástól napjainkig. In: PÓSÁN László – VESZPRÉMY László – BODA József – ISASZEGI János (szerk.): Őrzők, vigyázzatok a határra! Határvédelem, határőrizet, határvadászok a középkortól napjainkig. Zrínyi Kiadó, Budapest, 2017. p. 667.

FELHASZNÁLT IRODALOM

- DEÁK József: A rendészettudomány kialakulása és gondozásának nemzetbiztonsági, határőrizeti példái a Belügyi Szemlében a rendszerváltásig. Nemzetbiztonsági Szemle, IV. évfolyam 4. szám, 2016. pp. 43–75. https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1883/1172; letöltés: 2021.03.12.
- DEÁK József: Az állambiztonsági propaganda, annak kialakulása és fejlődése – nemzetbiztonság és civil kapcsolatok. Társadalom és Honvédelem, 17. évfolyam 3–4. szám. NKE Szolgáltató Nonprofit Kft., Budapest, 2013. pp. 408–417.
- FÓRIZS Sándor: Külföldre szökések a határőrségtől 1951-ben. Belügyi Szemle, 62. évfolyam, 2014/6. szám. pp. 48–62. http://www.forizs-sandor.hu/pdf/38.pdf; letöltés: 2021.03.04.
- FÓRIZS Sándor: Menekültek Jugoszláviában 1956. novemberben. Hadtudomány, XXX. évfolyam, 2020/1. szám. pp. 42–52. http://real.mtak.hu/109492/1/042-052_Forizs.pdf; letöltés: 2021.03.11.
- FÓRIZS Sándor: Rejtélyes határesemény a műszaki záron. Új Honvédségi Szemle, 1997/6. szám. pp. 39–42. http://www.forizs-sandor.hu/pdf/18.pdf; letöltés: 2021.03.11.
- JAKUS János: Titkos háború a déli államhatár mentén az ’50-es évek elején. Közép-Európai Közlemények, V. évfolyam 1. szám, 2012/1. No. 16. pp. 42–54. http://vikek.eu/wp-content/uploads/2014/02/KEK-16.pdf; letöltés: 2021.03.14.
- ORGOVÁNYI István: Az Államvédelmi Hatóság Határőrség felderítő osztályának megszervezése és tevékenysége 1950 és 1956 között. I–II. rész. Betekintő, 2015/1. és 2015/2. szám. https://betekinto.hu/sites/default/files/betekinto-szamok/2015_1_orgovanyi.pdf; letöltés: 2021.03.10. https://betekinto.hu/sites/default/files/betekinto-szamok/2015_2_orgovanyi.pdf; letöltés: 2021.03.10.
- RITECZ György: Határőrizet a rendszerváltástól napjainkig. In: PÓSÁN László – VESZPRÉMY László – BODA József – ISASZEGI János (szerk.): Őrzők, vigyázzatok a határra! Határvédelem, határőrizet, határvadászok a középkortól napjainkig. Zrínyi Kiadó, Budapest, 2017. pp. 642–673.
- VARGA János: A határportyázó századoktól a határrendészeti kirendeltségekig. Magyar Rendészet, XV. évfolyam 6. szám, 2015. pp. 133–146. https://folyoirat.ludovika.hu/index.php/magyrend/article/view/3569/2852; letöltés: 2021.03.09.
- VARGA János: A magyar határőrizeti szervek reagáló képessége (1867-1989). Rendőrtiszti Főiskola Rendvédelmi füzetek, 1999/26. szám. pp. 1–23.

- ÁBTL 1.11. 7-436/6/31. 23. d. A Honvéd Határőrség elhárító-felderítő szolgálatának megszervezése és felépítése, 1945–1948.
- MNL HOP XIX-B-10 1950. év 39. sz. doboz I/5. tárgykör 3. folyószám.
  Jelentés, 1950.12.12.
  „Tárgy: Évi beszámoló a Határőrség és Belső Karhatalom 1950. évben végzett munkájáról.”
- MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám.
  09. sz. parancs. 1951.01.09.
- MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám.
  028. sz. parancs. 1951.03.22.
  „Tartalom: Délszláv lakosság között végzett politikai munka és a délszláv lakosság fokozottabb megnyerése a határőrzés és honvédelem érdekeinek.”
- MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám.
  035. sz. parancs. 1951.04.23.
- MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám.
  045. sz. parancs. 1951.05.23.
- MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám.
  054. sz. parancs. 1951.06.29.
  „Az Államvédelmi Hatóság Határőrség felderítő szervei operatív beszámolásának módjáról és határidejéről.”
- MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám.
  067. sz. parancs. 1951.08.03.
- MNL HOP XIX-B-10 1951. év 1. sz. doboz I/1-2. tárgykör 1-18. folyószám.
  0114. sz. parancs. 1951.11.23.
- MNL HOP XIX-B-10 1951. év 2., 3., 4., 5. sz. doboz I/3. tárgykör 139. folyószám.
  Ügyeleti jelentések.
- MNL HOP XIX-B-10 1952. év 3., 4., 5. sz. doboz I/3. tárgykör 6. folyószám.
  Ügyeleti jelentések.
- MNL HOP XIX-B-10 1952. év 3., 4., 5. sz. doboz I/3. tárgykör 6. folyószám.
  Ügyeleti jelentések. 1952.07.10.
- MNL HOP XIX-B-10 1952. év 3., 4., 5. sz. doboz I/3. tárgykör 6. folyószám.
  Ügyeleti jelentések. 1952.10.01.
- MNL HOP XIX-B-10 1956. év 17. sz. doboz VI/1-7. tárgykör 86. folyószám.
  „Tárgy: Jugoszláv szervek felvetése.”

DR. GERENCSÉR ÁRPÁD –
SIPOSNÉ DR. KECSKEMÉTHY KLÁRA

AZ AMUR TÉRSÉG VÁLTOZÓ GEOSTRATÉGIAI JELENTŐSÉGE

Az Amur térség földrajzi elhelyezkedése

Az Amur térség Oroszország távol-keleti részén található, a távol-keleti gazdasági makrorégió részei alkotják. A nevét az Amur folyóról kapta. Az Amur térséget az Amuri terület (Амурская область, 363 700 km²), a Zsidó autonóm terület (Еврейская автономная область, 36 266 km²), a Bajkálontúli határterület (Забайкальский край, 431 500 km²) és a Habarovszki határterület (Хабаровский край) déli része alkotja (1. ábra).

1. ábra. Az Amur térség az orosz Távol-Keleten
Szerkesztette: Siposné dr. Kecskeméthy Klára
Megjegyzés: 1. Bajkálontúli határterület; 2. Amuri terület; 3. Habarovszki határterület; 4. Zsidó autonóm terület

Az Amur térség lakossága a terület nagyságához képest csekély, és a fiatalság jelentős elvándorlása miatt folyamatosan csökken. A négy közigazgatási egység összlakossága 2016. január 1-jén 3 389 373 fő, ebből a városi lakosság 2 483 480 fő volt, négy év alatt egy közepes nagyságú város (36 595 fő) lakosságszámával tovább csökkent a térség lakossága (1. táblázat).[1]

[1] ОЦЕНКА ЧИСЛЕННОСТИ НАСЕЛЕНИЯ на 1 января 2016 года и в среднем за 2015 год. http://www.gks.ru/free_doc/new_site/population/demo/Popul2016.xls; letöltés: 2020.11.01.

	Lakosság összesen (fő)	Városi (fő, %)	Vidéki (fő, %)
Zsidó autonóm terület	158 381	108 743 68,7%	49 638 31,3%
Amuri terület	790 676	535 760 67,7%	254 916 32,3%
Bajkálontúli határterület	1 059 657	722 656 68,2%	337 001 31,8%
Habarovszki határterület	1 315 310	1 079 726 82,1%	235 584 17,9%
Összesen	**3 324 024**	**73,6%**	**26,4%**

1. táblázat. Az Amur térség lakosságának száma
(2020. január 1.)[2]

2. ábra. Transzszibériai, Transzmandzsúriai és Bajkál–Amur vasútvonalak[3]

ОЦЕНКА ЧИСЛЕННОСТИ НАСЕЛЕНИЯ на 1 января 2020 года и в среднем за 2019 год. https://www.gks.ru/storage/mediabank/PrPopul2020.xls; letöltés: 2021.01.10.
A tanulmány az Amur térség vizsgálatakor a Habarovszki határterület déli részét, területének mintegy egyharmadát és a lakosság részéről mintegy 800 ezer főt vett alapul.

[2] ОЦЕНКА ЧИСЛЕННОСТИ НАСЕЛЕНИЯ на 1 января 2020 года и в среднем за 2019 год. https://www.gks.ru/storage/mediabank/PrPopul2020.xls; letöltés: 2021.01.10.

[3] The Trans-Siberian Railroad. https://www.trans-siberian-travel.com; letöltés: 2020.10.28.

A térségen halad keresztül a Transzszibériai vasútvonal a Tulun–Irkutszk–Ulan-Ude–Csita–Habarovszk–Nahodka/Vlagyivosztok vonalon, valamint a Bajkál–Amur (Tajset–Komszomolszk-na-Amure) vasútvonal. A távol-keleti kereskedelmi forgalom fő ütőere ez a vasútvonal. Csitából Harbinon keresztül Pekingbe tart a mandzsúriai vasútvonal (2. ábra). Egyelőre meghatározó szerepet játszik a teherszállítás területén, de Kína a közeljövőben be akarja fejezni az *Új Selyemút*, avagy *Egy övezet egy út* program részeként a Kína–Pakisztán–Irán–Törökország vasútvonal építését. Ez jelentős konkurenciát jelent majd az oroszországi Transzszibériai vasút számára.

A térség nyersanyagokban rendkívül gazdag. Jelentős arany-, wolfram-, ólom-, ezüst-, molibdén-, mangán- és rézkészletek állnak rendelkezésre, valamint ritka ásványok is előfordulnak, amelyek rendkívül értékesek és keresettek. Két szénmező (Dél-Jakutföld, Habarovszk) található itt, mindkettő művelés alatt áll. Mezőgazdasági szempontból az erdőgazdálkodás a húzóágazat. Gabonatermesztésre csak az Amur folyó mentén van lehetőség, azon belül is a Habarovszktól nyugatra fekvő területen és a mongol−kínai−orosz hármashatár térségében.

A térség változó geostratégiai jelentősége

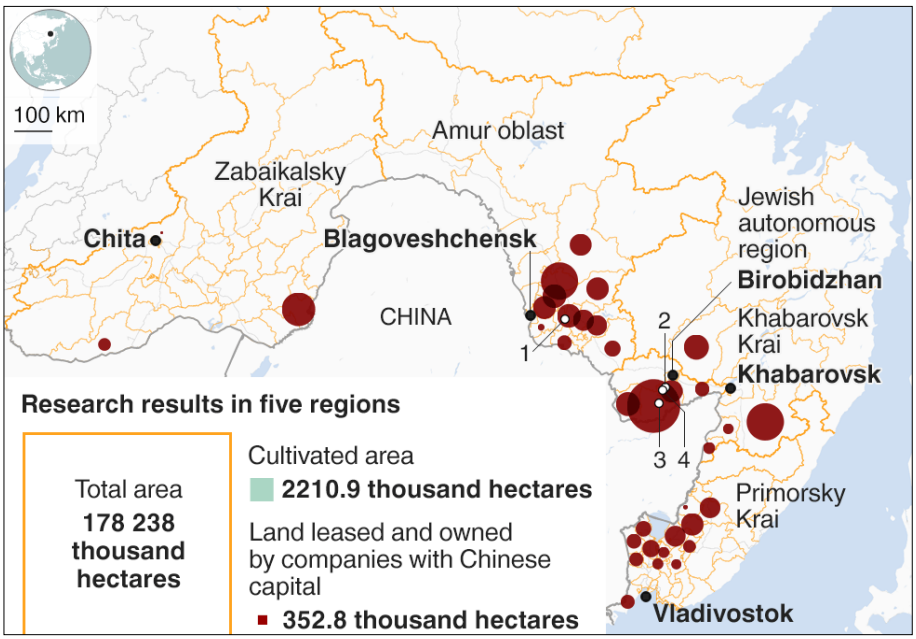
Az Amur térség két geopolitikai szereplő, regionális hatalom ütköző-, illetve határzónájában helyezkedik el. A térség stratégiai jelentősége folyamatosan változott a történelem során. A cári időkben a száműzöttek egyik célállomása volt. Sztálin az Amur mellett „álmodta" meg a szovjet „Siont", Birobidzsánt. Ez ma a Zsidó autonóm terület nevet viseli. Ez lett volna a Szovjetunió területén szétszórtan élő zsidók „autonóm" területe, ide akarta a Lavrentyij Pavlovics Berija vezetése alatt álló NKVD-vel (Belügyi Népbiztosság, НКВД – Народный комиссариат внутренних дел) összegyűjteni a zsidókat. Az 1928-ban alapított terület fővárosa Birobidzsán, a zsidó lakosság nagy része nem költözött a területre, jelentős részük az országot is elhagyta, Izraelbe és az Amerikai Egyesült Államokba vándorolt ki. A legutóbbi rendelkezésre álló 2010. évi népszámlálási adatok szerint a Zsidó autonóm terület lakossága 171 726 fő, ebből 160 185 fő (92,8%) orosz és csak 1628 fő (0,94%) volt zsidó.[4]

A térség miatt már volt fegyveres konfliktus, ezért érdemes megvizsgálni, hogy ez a terület miként jelenik meg az orosz és a kínai geopolitikai gondolkodásban.

Napjainkban az Amur térség geostratégiai jelentőségét meghatározza, hogy közvetlenül határos Kínával, Észak-Koreával és a vitatott hovatartozású Kuril-szigetekkel, a térség nyugati része a mongol–kínai–orosz határtérségre esik, valamint Vlagyivosztok a terület legnagyobb és meghatározó – katonai szempontból kiemelt – fontosságú kikötővárosa. Mivel Szibéria déli területei egyre jobban felértékelődnek Kína számára, így az energetikai szektoron, a térségen áthaladó kőolaj-és földgázvezetékeken, az energetikai infrastrukturális fejlesztéseken kívül is egyre nagyobb jelentősége lesz az Amur térségnek. Az Amur térség a kínai

[4] Az Oroszországi Föderáció Statisztika Hivatala 2010. évi népszámlálás részletes adatai. Владение языками населением наиболее многочисленных национальностей по субъектам Российской Федерации. https://www.gks.ru/free_doc/new_site/perepis2010/croc/Documents/Vol4/pub-04-07.pdf; 2021.01.15.

terjeszkedés egyik célterülete, ahol többek között a mezőgazdaságban is jelentős pozíciókat szereztek meg. 2018-ban 352,8 ezer hektár nagyságú mezőgazdasági területet műveltek kínaiak a határ menti közigazgatási egységekben. Ez a teljes művelésre alkalmas terület (2 210 900 hektár) 16%-a. A 3. ábra az orosz Távol-Keleten található kínai gazdaságokat szemlélteti, így az általunk definiált Amur térség mellett a Tengermelléki határterület (Primorszkij kraj) adatai is szerepelnek a térképen.[5]



3. ábra. A kínai gazdaságok által művelt mezőgazdasági területek az orosz Távol-Keleten[6]
Jelmagyarázat: a kínaiak által művelt mezőgazdasági területek, települések:
1. Makszimovka, 2. Opitnoje Polje, 3. Babsztovo, 4. Dimitrovo

A térség szerepe azért is nő, mert Kína túlnépesedett, az Amur térség ivóvízkészlete hatalmas, az orosz ajkú lakossága pedig drasztikusan csökken. Összességében nagy a belakható tér, jó a terület eltartóképessége, sőt a klímaváltozás hatására az egyre növekszik.

Az Amur térség iránti érdeklődés a kétezres években megnövekedett, különösen a 2008. évi pénzügyi világválság következményeként. A térségben egyre több a kínai gazdálkodó, arányuk különösen a Zsidó autonóm területen nagy.

[5] ZAKHAROV, Andrei – NAPALKOVA, Anastasia: Why Chinese farmers have crossed border into Russia's Far East. BBC News, 2019.11.01. https://www.bbc.com/news/world-europe-50185006; letöltés: 2021.01.09.
[6] Uo.

A Szovjetunió felbomlását követően felerősödött a kínai betelepedés az Amur térségbe. Az új kínai bevándorlók kérdése központi téma volt az orosz vezetés számára, de a kínai kérdés a lakosság tájékoztatásában is fontos elem volt.[7] A „munkavállaló" kínaiak jelentősége már 1992-ben megmutatkozott a munkaerőhiánnyal küszködő orosz agráriumban, a városokból is sok helyi lakos elvándorolt Oroszország más térségeibe, így a bevándorló kínaiak szerepe itt jelentősen felértékelődött. Igaz, nagyon sok kínai illegálisan érkezett, és a feketepiacon szereztek meg ingatlanokat.[8] A kínai–orosz határt az 1858. évi Aiguni Szerződés határozta meg. A kínai bevándorlás az 1860-as évektől szezonális jelleget öltött.[9] Sokan ma is csak a vegetációs időszakban tartózkodnak a térségben, aztán hazamennek Kínába. Az 1880-as évekig az orosz hatóságok 20 éves adókedvezményt adtak azoknak, akik földet vásároltak és letelepedtek a térségben.

A két nemzet – a kínai és az orosz – között számos konfliktus alakult már ki, éppen ezért nagyon vegyes a megítélés mindkét oldalon. A kínaiak jobban szeretnek kínaiakkal dolgozni, mivel megbízhatóbbak és nagyobb a teljesítőképességük. Az orosz lakosság majdnem fele egyértelműen az orosz állam területi integritása elleni cselekedetnek tekinti a kínaiak egyre növekvő jelenlétét és befolyását, míg egyharmaduk szerint Kína az orosz gazdasági fejlődést veszélyezteti.[10] Sajátos egybeesés volt, hogy a bűncselekmények száma 1992-ben érte el csúcsát, amikor nagyon sok kínai érkezett a térségbe. Ám a kínaiak is elszenvedői voltak a romló közbiztonsági helyzetnek.[11]

A kínaiak bevándorlása már a 19. század közepén, az 1860-as évektől jelentős volt. Már abban az időben is „sárga veszedelemnek" nevezték a kínaiak betelepülését.[12] Az orosz expanzió a 19. század második felében a térségben lezárult. Ebben az időszakban 500 ezer kínai élhetett az orosz Távol-Keleten (a térség teljes lakossága 2 millió fő volt ebben az időszakban). A kínaiak a mezőgazdaságban, a kereskedelemben és a szolgáltatási szektorban dolgoztak.[13] A bolsevikok hatalomra kerülésekor szövetségesként tekintettek a kínaiakra az imperializmus elleni harcban.

---

[7] SHIAU-SHYANG, Liou: Chinese Immigration to Russia and Its Non-traditional Security Impact. East Asia, Volume 34, Issue 4, December 2017. pp. 275–276. https://www.researchgate.net/publication/322092741_Chinese_Immigration_to_Russia_and_Its_Non-traditional_Security_Impact; letöltés: 2021.01.20.

[8] MINAKIR, Pavel A.: Chinese Immigration in the Russian Far East: Regional, National, and International Dimensions. In: AZRAEL, Jeremy R. – PAYIN, Emil A. (edit.): Cooperation and Conflict in the Former Soviet Union: Implications for Migration. Rand, Santa Monica, 1996. pp. 92–94. https://www.rand.org/pubs/conf_proceedings/CF130.html; letöltés: 2021.01.26.

[9] ALEXEEVA, Olga: Chinese Migration in the Russian Far East – A Historical and Sociodemographic Aanalysis. China Perspectives, 2008/3, December 2008. pp. 21–22. https://www.researchgate.net/publication/301896718_Chinese_Migration_in_the_Russian_Far_East_A_Historical_and_Sociodemographic_Aanalysis; letöltés: 2021.01.27.

[10] ZAKHAROV, Andrei – NAPALKOVA, Anastasia: Why Chinese farmers have crossed border into Russia's Far East. BBC News, 2019.11.01. https://www.bbc.com/news/world-europe-50185006; letöltés: 2021.01.09.

[11] MINAKIR, Pavel A.: Chinese Immigration in the Russian Far East: Regional, National, and International Dimensions. p. 93.

[12] SHIAU-SHYANG, Liou: Chinese Immigration to Russia and Its Non-traditional Security Impact. pp. 275–276.

[13] MINAKIR, Pavel A.: Chinese Immigration in the Russian Far East: Regional, National, and International Dimensions. p. 86.

A polgárháború után, a bolsevik hatalom megszilárdulását követően az oroszok még pozitívan tekintettek a kínaiakra, és ez még az 1930-as évekre is igaz volt. 1938-ban a térségben a kínaiak aránya az akkori lakosság kevesebb mint 1%-a volt. A két nemzet még nem tekintett ellenségesen egymásra, és ez egészen az 1950-es évekig volt így.[14]

A két nemzet közötti feszültség 1956 után kezdődött, az 1960-as években felerősödött, majd 1969-ben az Usszuri folyó konfliktusában csúcsosodott ki. A kínai kisebbség helyzete ebben az időben nem volt irigylésre méltó, mivel a két ország közötti határzónából elsősorban kínaiakat telepítették ki, a helyüket pedig oroszokkal töltötték fel.[15] Nyikita Hruscsov úgy nyilatkozott, hogy „*a kínaiak el akarják foglalni Szibériát. Be akarnak hatolni és átvenni a helyi gazdaság vezetését, úgy hogy a kínai lakosok számbeli fölényt szereznek az oroszok és más nemzetiségek fölött. Így a kínaiak meggyökereznek az orosz Távol-Keleten.*"[16]

Az orosz Távol-Kelet problémáját Gorbacsovék is érzékelték. A szovjet gazdasági reform nem hozta a tervezett eredményeket. A Szovjetunió Kommunista Pártja Központi Bizottsága és a Minisztertanács 1987 szeptemberében meghirdette *A Távol-Kelet és a Bajkál régió társadalmi és gazdasági fejlődésének hosszú távú állami programját 2000-ig*. Ez is mutatja, hogy a moszkvai vezetés érzékelte a térség problematikáját. Az ugyanebben az időben meghirdetett kínai gazdasági reform sikertörténetként vonult be a történelembe, a Szovjetunió felbomlása viszont soha nem látott visszaesést hozott. Az ipari termelés és a beruházások volumene az 1970-es évek szintjére esett vissza. 1986–1987-ben még 4,4%-os növekedés jellemezte a térség gazdaságát, de utána jelentős csökkenés volt tapasztalható.[17] Az oroszok hozzáállása a kérdéshez kettős: egyrészt szükség van a kínaiakra, mivel a megüresedett munkahelyeket ők töltik ki a jelentős orosz elvándorlás miatt, másrészt a nagy tömegű bevándorlótól való félelem egyre nagyobb.

Vlagyimir Putyin 2000-ben így fogalmazott az orosz Távol-Kelettel kapcsolatban: „*Ha Moszkva nem fejleszti aktívan az orosz Távol-Keletet, akkor a helyi lakosok egy nap japánul, koreaiul vagy kínaiul fognak beszélni*".[18] Az orosz Távol-Keleten a nagyszámú bevándorló okozza a kínaiaktól való félelmet. Sokan félnek attól, még vezetői szinten is, hogy kínai autonómiatörekvések merülnek fel, esetleg enkláve alakul ki. Moszkva felismerte, hogy bilaterális megállapodásokon keresztül kell a térséget fejlesztenie, hogy azt befolyása alatt tartsa, és ezzel a kínai bevándorlás okozta nemzetbiztonsági kihívást is csökkenteni tudja. Az együttműködésekből fakadó előnyök felhasználásával akarja Moszkva az orosz ajkú lakosságot is visszacsábítani a Távol-Keletre.[19]

---

[14] SHIAU-SHYANG, Liou: Chinese Immigration to Russia and Its Non-traditional Security Impact. p. 274.
[15] MINAKIR, Pavel A.: Chinese Immigration in the Russian Far East: Regional, National, and International Dimensions. p. 87.
[16] SHIAU-SHYANG, Liou: Chinese Immigration to Russia and Its Non-traditional Security Impact. p. 275.
[17] MINAKIR, Pavel A.: Chinese Immigration in the Russian Far East: Regional, National, and International Dimensions. p. 89.
[18] SHIAU-SHYANG, Liou: Chinese Immigration to Russia and Its Non-traditional Security Impact. p. 276.
[19] Uo. pp. 282–284.

A Szovjetunió felbomlását követő időszakban a térség egyre jobban elszigetelődött az orosz központi térségektől és a FÁK-tagországoktól. Az orosz Távol-Kelet azonban egyre jobban felértékelődött Kína, Japán és Dél-Korea számára, azaz egyre jobban beintegrálódott az ázsiai pacifikus államok kereskedelmi rendszerébe. A kínai működő tőke beáramlásának kedvelt célpontja volt az Amur térség. Kínának a térség exportjából 1992-ben 27,3%-os részesedése volt, 1993-ban már 33,6%. Azt fontos azonban megjegyezni, hogy bármennyire is kedvelt befektetési területévé vált a kínaiaknak az orosz Távol-Kelet, területi igényekkel nem léptek fel.[20]

A kínai–szovjet/orosz határ az Usszuri folyónál történt konfliktus után egészen 1988-ig zárva volt. Az enyhülés 1988-ban kezdődött a határok megnyitásával. A félelem alapja az 1990-es évektől az volt – amire az orosz média jelentősen rá is játszott –, hogy a Tengermelléki határterület 2,2 millió fős orosz lakosságával szemben a szomszédos Heilongjiang határterületen 38 millió fős kínai lakosság él. Ezt tetézendő néhány orosz tanulmány ebben az időben a kínai tartomány lakosságát 70 millió főre becsülte, amivel a félelmet tovább növelte. Az eltérő demográfiai adottságokat sok orosz elemző nem tekinti másnak, mint „*Kína demográfiai nyomását Oroszországra*”.[21] Az orosz–kínai kapcsolatokra jellemző volt a hullámzás. Ezt nagyon jól mutatja Vlagyimir Stegnyij nyilatkozata, aki korábban a Tengermelléki határterület helyettes kormányzója volt: „*... jelenleg a katonai képességünk akkora, hogy egyes becslések szerint Kínát harmincháromszor tudnánk elpusztítani. De a katonai erőegyensúly jövője bizonytalan. A jövőben a katonai erőegyensúly romlani fog számunkra. Kína rengeteg pénzt költ a hadseregére. Mi nem tudjuk megtenni ugyanilyen mértékben*.”[22]

Az Usszuri folyónál kialakult konfliktus (Damanszkij-sziget)

Oroszország és Kína közös határa 4133 km.[23] Az első határviták a 17. században alakultak ki a keletre terjeszkedő cári felfedezők, kereskedők és a kínai szervek között. Az 1860-as Pekingi Szerződés kijelölte ugyan az Usszurit határfolyónak, de a szigeteket egyik félnek sem adta.[24] A nemzetközi jog szerint a határfolyókon a vízi határ többféle módon értelmezhető: a fősodor vonalát, a folyó középvonalát vagy a legmélyebb pontokat összekötő vonal tekinthető államközi határnak. Az Usszurihoz hasonló folyók esetében azonban – melyek gyakran változtatják medrüket, és az év jelentős részében elárasztják a part menti területeket – ez komoly problémát okozhat. A Kínai Népköztársaság és a Szovjetunió 1950. február 14-én barátsági, szövetségi és kölcsönös segítségnyújtási szerződést írt alá. 1951 januárjában szovjet–kínai egyezmény szabályozta a hajózás rendjét az Amur, az Usszuri és más határfolyókon.

---

[20] MINAKIR, Pavel A.: Chinese Immigration in the Russian Far East: Regional, National, and International Dimensions. pp. 90–92.

[21] ALEXSEEV, Mikhail A. – HOFSTETTER, C. Richard: Russia, China, and the Immigration Security Dilemma. Political Science Quarterly, Volume 121, Number 1, Spring 2006. p. 8. http://www.jstor.org/stable/20202643; letöltés: 2021.01.25.

[22] Uo. p. 11.

[23] The World Factbook: China. https://www.cia.gov/the-world-factbook/countries/china/#geography; letöltés: 2021.01.11.

[24] USSR/China: Soviet and Chinese Forces Clash on the Ussuri River. U.S. Department of State, 1969.03.04. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB49/sino.sov.1.pdf; letöltés: 2021.01.11.

Kína és a Szovjetunió egyik konfliktusa 1968 augusztusában elsődlegesen az atomfegyver technológiájának át nem adása miatt robbant ki, de a szakirodalom határvitaként jellemezi.[25] A konfliktus provokációk formájában már 1964 októberében elkezdődött. Abban szinte lehetetlen igazságot tenni, hogy ki kezdte és milyen provokációt követett el. 1968 közepétől az Usszuri folyó sorozatos határincidensek színhelye lett. A szovjet határőrség 1969. március 2-án keveredett újabb, több halálos áldozatot követelő fegyveres összetűzésbe a kínai beszivárgó alakulatokkal.[26] 1969-re már mindkét ország több százezer fős fegyveres erőt állomásoztatott a térségben, 25–30 szovjet hadosztály diszlokált a határ térségében, a kínaiak pedig Mandzsúriában összpontosították az erőiket (két határőrhadosztály, 24 lövészhadosztály, két páncéloshadosztály, hat tüzérhadosztály), összesen 34 hadosztályt.[27] A két ország közötti legismertebb és a legnagyobb nemzetközi visszhangot kiváltó újabb fegyveres összetűzés 1969. március 15-én történt. A kínai haderő egy ezrede előbb beszivárgással, majd harckocsik, tüzérség és aknavetők támogatásával megkísérelte elfoglalni az Usszuri határfolyón található Damanszkij-szigetet. Az első összecsapás a szovjet határőrökkel folyt, a sziget a következő órákban többször cserélt gazdát. Az összecsapás kimenetelét szovjet reguláris gépesített lövészkötelékek bevetése döntötte el: egy önálló rakéta-sorozatvető osztály (BM–21 Grad típusú eszközökkel) több órán át tartó csapást mért a rohamozó kínai gyalogságra. A kínaiak visszavonultak az állásaikba, de az egész folyószakaszt elaknásították.[28] A hivatalos szovjet adatok szerint 1969 márciusában 58 halott (közöttük 14 tiszt) és 94 sebesült (kilenc tiszt) volt a veszteség. A kínai veszteségek nem ismertek.[29]

A Szovjetunió kínai határprovokációról, az ország területe és határai sérthetetlenségéről és megsemmisítő válaszcsapás lehetőségéről beszélt. A kínai nyilatkozatok a szigetet – kínai nevén Csenpao – Kína részének nyilvánították. Bár a nemzetközi sajtó már a szovjet–kínai háborút vizionálta, a feszült időszak után enyhülés következett, 1969. szeptember 11-én a két fél tárgyalóasztalhoz ült. 1969 szeptemberétől 2004-ig csak diplomáciai csörte zajlott a két hatalom között. Az Argun folyó 413 kis szigetéről is folyt a vita, 1996-ban 204 sziget orosz, 209 pedig kínai fennhatóság alá került, egy 5 km²-es terület sorsáról azonban csak 2004-ben döntöttek.

A két ország közötti határvita Mihail Gorbacsov hatalomra kerülésével mozdult ki a holtpontról, 1991-ben már több száz sziget hovatartozásáról, a Habarovszk melletti két nagy szigetről pedig 2004-ben állapodtak meg. A Tarabarov- (Yinlong) és a Nagy-Usszuri-szigettel (Heixiazi) kapcsolatban csak 2008-ban született megállapodás, ekkor Kína 170 km² területet kapott.[30]

---

[25] ZENTAI László: Kína területi vitái. Lázár Kollokvium, 2011.04.29. p. 12. http://lazarus.elte.hu/hun/lk/110429/2011-04-29-zl.pdf; letöltés: 2021.01.11.

[26] 1969 – A Damanszkij incidens. Ritkán látható történelem, 2016.10.04. https://ritkanlathatotortenelem.blog.hu/2016/10/04/1969_a_damanszkij-incidens; letöltés: 2021.01.11.

[27] USSR/China: Soviet and Chinese Forces Clash on the Ussuri River. U.S. Department of State, 1969.03.04. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB49/sino.sov.1.pdf; letöltés: 2021.01.11.

[28] A szovjet-kínai határincidens évfordulója. Múlt-Kor, 2004.03.16. https://mult-kor.hu/cikk.php?id=878; letöltés:2021.01.11.

[29] 1969 – A Damanszkij incidens. Ritkán látható történelem, 2016.10.04. https://ritkanlathatotortenelem.blog.hu/2016/10/04/1969_a_damanszkij-incidens; letöltés: 2021.01.11.

[30] China, Russia hail end of border dispute. WordPress, 2008.10.16. https://jzobk.wordpress.com/tag/tarabarov-island/; letöltés:2021.01.11.

A térség gazdasági jelentősége

Az Amur térség gazdasága

A térség a Távol-Keleti Szövetségi Körzet része. A térség aranykészletei a legjelentősebbek Oroszországban. Az Amur térség második az orosz aranybányászat rangsorában, itt 206 aranybánya található. A térségben az aranybányászat 1867-ben kezdődött. A legfontosabb aranybányák: Szolovjevszkij, Pionyer, Pokrovszkij, Tokur, Albin, Oszipkan és Malomir, az itteni bányákból évente közel 30 tonna aranyat termelnek ki.[31] Garinszkoje és Kuranah környékén vasércbányák találhatók. Oroszországban először ebben a térségben gépesítették az aranybányászatot.[32] Egyre nagyobb jelentősége lesz a megújuló energiaforrásoknak és az őket kiszolgáló iparágaknak (pl. hulladékfeldolgozás). Ennek központja Szvobodnij városa.

A térség sajátos geológiai adottságai miatt földjében sok értékes anyag megtalálható: urán, titán, wolfram, ólom, molibdén, nikkel, ezüst, réz, apatit, grafit, szén, féldrágakövek stb.[33] A térségben jelen van a villamosipar, a mezőgazdasági és a vasúti gépgyártás, a bányászati és a bányagépipar. Közlekedése fejlett, itt halad át a Bajkál–Amur vasútvonal, és az Amur folyó is jelentős közlekedési folyosó. A térség híres a szójabab termesztéséről. Az erdészet és az azt kiszolgáló iparágak fejlettek, jelentős bevételt hoznak a szövetségi kormánynak.

Szibéria Ereje

Oroszország a hosszú távú elképzelések ellenére az európai szénhidrogén-piacon pozícióvesztéssel és az export visszaesésével kénytelen szembesülni. A költségvetés számára meghatározó fontosságú exportbevételek biztosítása érdekében nagyszabású projekteket indított el a Távol-Keleten. A Szibéria Ereje (Сила Сибири) gázvezeték egy grandiózus fejlesztés, amely 2014-ben kezdődött a Gazprom irányításával. Megvalósulásával a jakutföldi földgáz jut el a kínai piacra, a gázvezeték orosz területen 3000 km, a kínai szakaszon 5111 km hosszú. A vezeték Blagovescsenszk határvárosnál lép át a kínai oldalra.

A gázvezeték a két legfontosabb távol-keleti földgázmező (Csajanda–Csajandinszkoje és Kovikta–Koviktinszkoje) földgázát továbbítja a felhasználókhoz. A projekt első szakasza, a 2200 km hosszú vezeték a csajandai gázmező és Blagovescsenszk városa között már elkészült. Jelenleg a fejlesztés második szakasza van folyamatban, amikor a két gázmező (Csajanda és Kovikta) összekötése történik egy 800 km hosszú vezetékkel.[34] 2014 májusában a Gazprom és a kínai CNPC (**China National Petroleum** Corp.) egy 30 éves szerződést írt alá 1300 Mrd m^3

[31] Russia Gold Mining: Amur Region. CEIC. https://www.ceicdata.com/en/russia/mining-and-quarrying-volume-gold-annual/gold-mining-amur-region; letöltés: 2021.03.22.

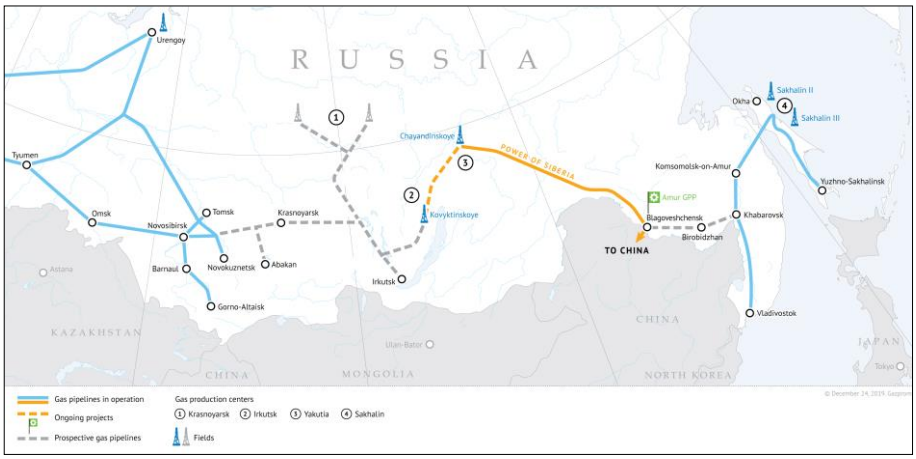
[32] Building a Russian Far East mining Champion. Petropavlovsk PLC, Annual Report & Accounts 2009. https://www.petropavlovsk.net/wp-content/uploads/2018/05/Petropavlovsk_AR09_Final.pdf; letöltés: 2021.01.26.

[33] Characteristics of the Regional Economy. Government of the Amur Region, 2018.12.20. https://www.amurobl.ru/en/pages/economy/characteristics-of-the-regional-economy/; letöltés: 2021.01.26.

[34] Power of Siberia – The largest gas transmission system in Russia's East. Gazprom. https://www.gazprom.com/projects/power-of-siberia/; letöltés: 2020.10.31.

földgáz szállítására.[35] A Szibéria Ereje gázvezetéken a Kínába történő gázszállítás 2019. december 2-án megkezdődött.[36]

A térség gazdasági erejét mutatja, hogy a Gazprom a Szvobodnij járásban építi az Amur Gázfeldolgozó Üzemet. Az üzem a világ egyik legnagyobb földgázfeldolgozó üzeme lesz, 2015 októbere óta tart az építkezés, várhatóan 2021-ben üzemelik be, a kapacitása 49 Mrd m^3/év lesz.[37] Az üzem a Szibéria Ereje gázvezetéken keresztül érkező csajandai és 2022-től a koviktai mezőkön kitermelt földgázt dolgozza fel (4. ábra). A két mezőn az együttes földgáztartalékok elérik a 3900 Mrd m^3-t.[38]



4. ábra. A Szibéria Ereje gázvezeték nyomvonala és további jövőbeni tervezett vezetékek[39]

Jelmagyarázat: Gázkitermelő központok: 1. Krasznojarszki, 2. Irkutszki, 3. Jakutföldi 4. Szahalini
Szibéria Ereje gázvezeték

Keleti Gázprogram

A Gazprom egy nagy volumenű fejlesztést hajt végre a Keleti Gázprogram (Восточная газовая программа) keretében. A program lényege, hogy a nagy földgázmezőket egy rendszerbe kösse össze, és egy nagy kapacitású gázátadó és

[35] Amur Gas Processing Plant, Amur Region. Hydrocarbons Technology. https://www.hydrocarbons-technology.com/projects/amur-gas-processing-plant-amur-region/; letöltés: 2020.10.31.

[36] China-Russia east-route natural gas pipeline in operation. XinhuaNet, 2019.12.02. http://www.xinhuanet.com/english/2019-12/02/c_138600270.htm; letöltés: 2020.10.31.

[37] Progress of Amur GPP construction project reaches 70.5 per cent. Gazprom, 2020.12.17. https://www.gazprom.com/press/news/2020/december/article521180/; letöltés: 2021.01.12.

[38] Chayandinskoje Field – A resource base for the Power of Siberia gas pipeline. Gazprom. https://www.gazprom.com/projects/chayandinskoye/, letöltés: 2020.10.31.
Kovyktinskoje Field – The most prolific gas field in eastern Russia. Gazprom. https://www.gazprom.com/projects/kovyktinskoye/; letöltés: 2020.10.31.

[39] Power of Siberia – The largest gas transmission system in Russia's East. Gazprom. https://www.gazprom.com/projects/power-of-siberia/; letöltés: 2020.10.31.

-továbbító rendszeren keresztül eljuttassa a kitermelt földgázt Oroszország kelet-szibériai és távol-keleti térségeiben lévő felhasználók számára, valamint hosszú távon előkészítse annak exportját. A Kínába, valamint a csendes-óceáni térség más országaiba irányuló gázexport érdekében Kelet-Szibériában és a Távol-Keleten integrált gáztermelési, szállítási és ellátási rendszer állami fejlesztési programját (Keleti Gázprogram) 2007 szeptemberében fogadták el. Az Oroszországi Föderáció kormánya a Gazpromot nevezte ki a program fő koordinátorának. Öt nagy gázmezőt kapcsolnak össze a megaprojekt keretében: a krasznojarkszkit, az irkutszkit, a jakutföldit, a szahalinit és a kamcsatkait.[40]

A szahalini part menti területek hatalmas készletei (600 millió tonna kőolaj, 700 Mrd m^3 földgáz) lehetővé tették a Gazprom számára, hogy földgázkitermelő központot hozzon létre a térségben, és megkezdhesse a földgáz szállítását Oroszország távol-keleti és ázsiai fogyasztói számára. A Gazprom két nagyszabású projektet vezet a régióban, a Szahalin II[41] (Piltun-Asztohszkoje és Lunszkoje part menti mezők) és a Szahalin III elnevezésűket, ezen belül három tengeri platformot: Kirinszkij (Kirinszkoje, Juzsno-Kirinszkoje és Minginszkoje mezők), az Ajasszkij és a Vosztocsno-Odoptyinszkij. A szahalini gázkitermelő központ fejlesztése szempontjából a Szahalin III kulcsfontosságú. Az innen származó gáz képezi a Szahalin–Habarovszk–Vlagyivosztok gázszállító rendszer erőforrását.[42]

A Jakutföldön lévő és 1200 Mrd m^3 készlettel rendelkező csajandai gázmező a kitermelőközpont bázisa. A Gazprom fejlesztési/kutatási engedélyekkel rendelkezik további helyi területekre is. Az irkutszki jelenleg a legnagyobb kelet-oroszországi kitermelőközpont, amely a 2700 Mrd m^3 gázkészletű Koviktai/Koviktinszkoje mezőre épül. A Kamcsatkai terület gázellátását biztosító projekt részeként a Gazprom a Kamcsatkai-félsziget nyugati partján fekvő Ksukszkoje és Nyizsnye-Kvakcsikszkoje mezőket kiaknázva szállít gázt a fogyasztóknak Petropavlovszk-Kamcsatszkijba és más településekre.

A keleti régiókban a földgázszállítási kapacitások fejlesztése a földgázkitermelő szektor fejlődésével párhuzamosan folyik. A kelet-oroszországi gázszállítási rendszer integrálását tervezik az országos egységes gázellátó rendszerbe, így létrehozva a világ legnagyobb egységes technológiai komplexumát. A régióban a Gazprom kiépítette a Szahalin–Habarovszk–Vlagyivosztok földgázvezetéket, amely a Szahalini területen, valamint a Habarovszki és a Tengermelléki határterületeken halad keresztül. Emellett üzembe helyezte a Szibéria Ereje földgázvezetéket, amely az Irkutszki területen, Jakutföldön és az Amuri területen halad keresztül.

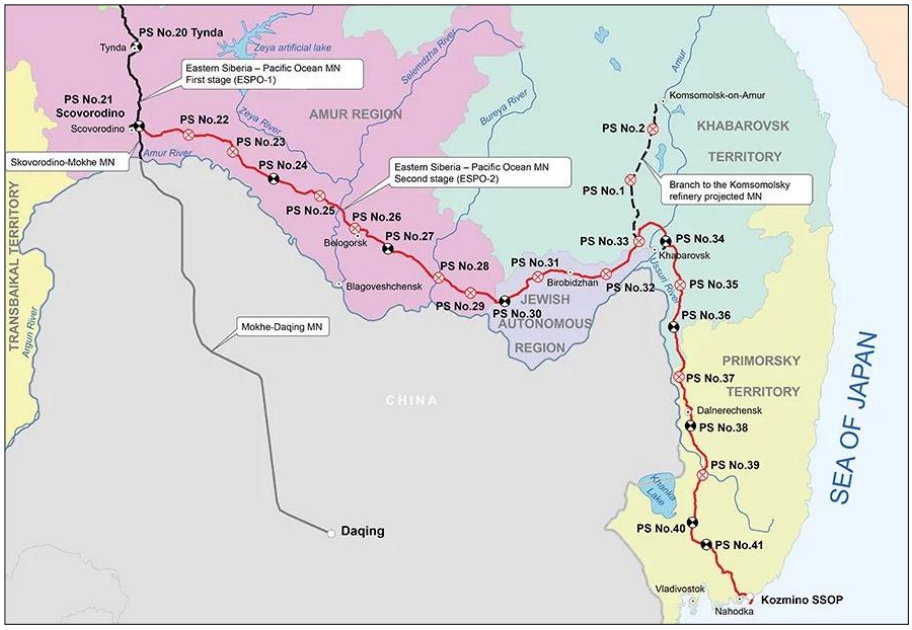
[40] WEINER Csaba: Az orosz gázipar helyzete a világgazdaságban és hatása a nemzetközi együttműködésre. Doktori disszertáció. Széchenyi István Egyetem, Győr, 2010. p. 314. http://www.kodolanyi.hu/oroszcivilizacio/doc/hasznos/weiner_orosz_gazipar.pdf; letöltés:2020.11.03.

[41] Sakhalin II – Russia's first liquefied natural gas plant. Gazprom. https://www.gazprom.com/projects/sakhalin2/; letöltés: 2021.03.23.

[42] Sakhalin III – Cutting-edge technologies for subsea hydrocarbon production. Gazprom. https://www.gazprom.com/projects/sakhalin3/; letöltés:2020.11.03.

Kelet-Szibéria–Csendes-óceán kőolajvezeték[43]

A szibériai olaj a Transznyeftyegaz által épített Kelet-Szibéria–Csendes-óceán (Восточная Сибирь – Тихий океан, ВСТО) kőolajvezetéken jut el a kínai piacra és egyben ellátja Habarovszk és Vlagyivosztok városokat is.



5. ábra. A távol-keleti orosz (Kelet-Szibéria–Csendes-óceán) kőolajvezeték[44]

A vezetéket a Transznyeftyegaz két fázisban valósította meg. Az elsőben a Tajset és Szkovorogyino közötti szakasz épült meg, hossza 2757 km, és 2009 óta üzemel.[45] A második szakasz Szkovorogyino és Kozmino (Nahodka) között épült meg, hossza 1963 km (5. ábra). Szkovorogyinoból kiépítettek egy 64 km-es elágazást a Kína határ (Mohe) felé, ahonnan további 992 km-es vezeték halad Daqingig.[46] 2012 decemberében helyezték üzembe, évente 30 millió tonna kőolaj továbbítására képes.

[43] Transneft Brings Eastern Siberia – Pacific Ocean Oil Pipeline to Maximum Capacity. Transneft, 2019.11.27. https://en.transneft.ru/newsPress/view/id/25213; letöltés: 2020.11.05.

[44] Нефтепровод Восточная Сибирь - Тихий Океан (ВСТО). Neftegaz.RU, 2013.03.19. https://neftegaz.ru/tech-library/transportirovka-i-khranenie/141847-vostochnyy-nefteprovod-vsto/; letöltés: 2021.04.27.

[45] The ESPO (Eastern Siberia Pacific Ocean) Oil Pipeline, Siberia, Russia. Hydrocarbons Technology. https://www.hydrocarbons-technology.com/projects/espopipeline/; letöltés: 2020.11.05.

[46] Uo.

A vezeték teljes hossza 4720 km, Kozmino kikötőjében még tengeri töltőberendezést is építettek a tankerek számára.[47]

Oroszország stratégiai célkitűzése a közép-szibériai szénhidrogénmezők összekapcsolása a kelet-szibériai mezőkkel. Így egy egységes rendszeren keresztül akarja elérni nemcsak az európai, hanem a sokkal nagyobb és növekvő ázsiai piacot. Ehhez az egyik út az Amur térségen keresztül vezet. A kelet-ázsiai piacok eléréséhez a Gazprom és a Transznyeftyegaz jelentős fejlesztéseket hajt végre a Szibéria Ereje, a Keleti Gázprogram és a Kelet-Szibéria–Csendes-óceán kőolajvezeték-programok keretében.

Oroszország Kínába irányuló szénhidrogénexportjának volumene az elkövetkező években tovább fog növekedni, de a 2030 utáni időszakban a Kína által előzetesen meghirdetett új energiapolitika következtében jelentős mértékű visszaeséssel kell majd számolnia.

Űrrepülőterek

A térség jelentőségét tovább növeli az, hogy Oroszországban három űrkikötő – Pleszeck, Szvobodnij és Vosztocsnij – alkalmas űrjárművek indítására, ezekből kettő az Amuri területen található. Az Oroszországi Föderáció Védelmi Minisztériumának 1. számú Állami Kísérleti Űrrepülőtere az Arhangelszki terület Pleszeck települése mellett helyezkedik el. A bázist ma is elsősorban a haderő használja. A 2. számú kísérleti űrrepülőtér (Szvobodnij) Bajkonurral egy szélességi körön, az Amuri területen helyezkedik el, jelenleg használaton kívül van. A bázist a hadászati rakétacsapatok használták 1961 és 1994 között.[48] Az Amuri terület kiemelt jelentőségét az orosz űrkutatás szempontjából az adja, hogy a térségben Ciolkovszkij (korábban Uglegorszk) településen építették fel a harmadik, Vosztocsnij elnevezésű űrkikötőt. A bázisról az első kísérleti rakétaindítást 2015 végére tervezték, de csak 2016 áprilisában indítottak űreszközt. A bázist Bajkonur pótlása[49] érdekében építette az orosz kormány megbízásából az űrkutatásokért felelős Roszkoszmosz Állami Vállalat (2015-ig Orosz Szövetségi Űrügynökség).[50] A bázist az Angara modulrendszerű legújabb hordozórakéták indításához fogják használni, amelyek a Szojuz hordozórakétákat váltják fel.[51] 2016 óta hét indítást végeztek a bázisról, amelyből egy volt sikertelen (2. táblázat).

---

[47] Transneft Brings Eastern Siberia – Pacific Ocean Oil Pipeline to Maximum Capacity. Transneft, 2019.11.27. https://en.transneft.ru/newsPress/view/id/25213; letöltés: 2020.11.05.

[48] Svobodny. European Space Agency. http://www.esa.int/About_Us/ESA_Permanent_Mission_in_Russia/Svobodny; letöltés: 2020.10.31. A bázis Blagovescsenszktől 120 km-re északra található, területe 780 km^2. A 1966. március 1-jén kiadott 305. számú elnöki rendelet alapján kezdték el a bázis kialakítását. Az űrrepülőteret 2007 februárjában elnöki rendeletre bezárták, annak ellenére, hogy szinte teljesen kiépítették.

[49] Bajkonur használatáért Oroszország évente 115 millió dollárt fizet Kazahsztánnak.

[50] LADÁNYI László: Oroszország új űrközpontot épít. National Geographic, 2010.07.29. http://www.ng.hu/Fold/2010/07/Oroszorszag_uj_urkozpontot_epit; letöltés: 2020.10.31.

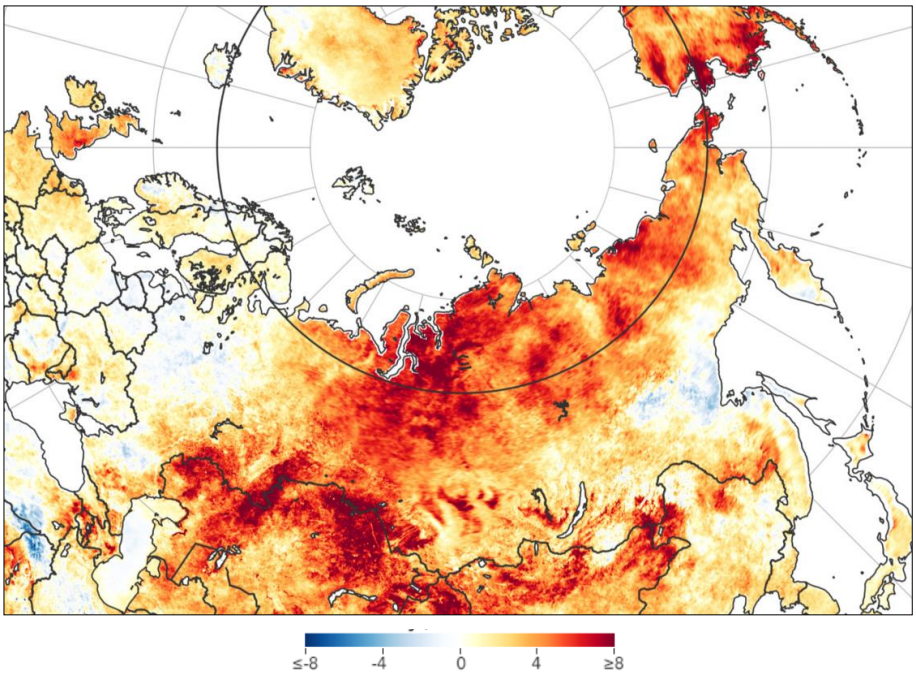
[51] ZAK, Anatoly: Soyuz launch pad in Vostochny – The launch pad location. RussianSpaceWeb. http://www.russianspaceweb.com/vostochny_soyuz.html; letöltés: 2021.01.20.

	Indítás időpontja	Indítóeszköz	Státusz
1.	2016.04.28.	Szojuz–2–1a/Volga	sikeres
2.	2017.11.27.	Szojuz–2–1b/Fregat	sikertelen
3.	2018.02.01.	Szojuz–2–1a/Fregat	sikeres
4.	2018.12.27.	Szojuz–2–1a/Fregat–M	sikeres
5.	2019.07.05.	Szojuz–2–1b/Fregat	sikeres
6.	2020.12.18.	Szojuz–2–1b/Fregat	sikeres
7.	2021.03.21.	Szojuz–2–1b/Fregat	sikeres

2. táblázat. Rakétaindítások a Vosztocsnij űrkikötőből 2016 és 2021 között[52]

A klímaváltozás hatása az Amur térségben

A globális klímaváltozás nagy változást hozott a Földön, jelentősen felértékelte az Északi-sarkvidék régiójának geostratégiai, geopolitikai, gazdasági és katonai jelentőségét. Fontos kiemelni, hogy Oroszország szibériai területein, az Amur térségben is jelentős éghajlati változások mennek végbe (6. ábra).



6. ábra. Szibéria, a földfelszín hőmérsékleti anomália-térképe[53]

[52] ZAK, Anatoly: Soyuz launch pad in Vostochny – Missions orignated from the Soyuz launch facility in Vostochny. RussianSpaceWeb. http://www.russianspaceweb.com/vostochny_soyuz.html; letöltés: 2021.04.28.

[53] Heat and Fire Scorches Siberia. Earth Observatory, March 19 – June 20, 2020. https://earthobservatory.nasa.gov/images/146879/heat-and-fire-scorches-siberia; letöltés: 2020.11.05.

Az Északi-sarkvidéki Tanács (Arctic Council)[54] megfigyelői tagságára 2013-ban Dél-Korea, Japán és Szingapúr mellett Kína is jelentkezett. A 2018. januári kínai geopolitikai nyilatkozat és megközelítés, miszerint Kína magát „közel-arktiszi" országként határozta meg, érdekes és figyelemre méltó jelentőségű, hiszen ennek már rövid távú következményei is vannak. Ez alapján nagy az esély arra, hogy Kína a Jeges-tenger menti hajózási és kereskedelmi útvonalakhoz történő hozzáférésével részt vegyen a nyersanyagok, különösen az energiakészletek feltárásában és kiaknázásában, azok kitermelésére is igényt formáljon, részt vegyen a kereskedelemben és az ezekhez szükséges infrastrukturális fejlesztésekben, amihez megfelelő erőforrással és technológiával rendelkezik.[55] Az *Új Selyemút*, avagy *Egy övezet, egy út* program a szibériai térséget, az Amur térséget is bekapcsolja, és szárazföldi útvonalat építenek ki. A Transzszibériai vasútvonal is fontos részét képezi ennek a 2011-ben bejelentett új kínai projektnek, amely szárazföldi összeköttetéseket tervez létrehozni Európa és Ázsia között.[56]

A klímaváltozás hatására az Amur térségben a mezőgazdasági termelés volumene is jelentősen növekedni fog. A nagyobb eltartóképesség miatt a túlnépesedett kínai területekről tömegek bevándorlása várható. Szibériában a modernkori történelem során először a kukorica is megterem, ami a drasztikus éghajlati változásokat mutatja.

Illegális és legális migráció

Az Amur fontos határszakasz Kína és Oroszország között. Kína északkeleti része (Mandzsúria) sűrűn lakott terület, és a folyó kínai oldalán jelentős mezőgazdasági tevékenység zajlik. A kínai kormány mindig is ösztönözte, hogy akár illegálisan is vegyék birtokba az Amur folyótól északra fekvő orosz területeket. A két ország lakosságszámát összehasonlítva látható, hogy jelenleg az arány az orosz és a kínai népesség között 1:10 a kínai javára. Nehéz pontosan megmondani, mennyi kínai él jelenleg Szibériában. Kína Mandzsúria tartományában 70 millió ember él, kevesebb mint 25 év alatt 13%-kal növekedett a terület népessége. Oroszország távol-keleti részén összesen 7,4 millió ember él, a népsűrűség kevesebb, mint 1,3 fő/km^2, ami óriási feszültséget jelent a két ország között (7. ábra).[57]

Oroszországnak óriási gondja, hogy az orosz ajkú lakosság elhagyja Szibériát, a helyükre pedig a legtöbb esetben illegális bevándorlók érkeznek. 1999 januárja és 2000 júniusa között 1 millió fő illegálisan, 1,5 millió fő pedig legálisan lépett Kínából Oroszország területére. Az illegálisan Oroszországba érkezők legnagyobb része a Távol-Keleten marad és dolgozik. A kínai–orosz határon zajló migrációval

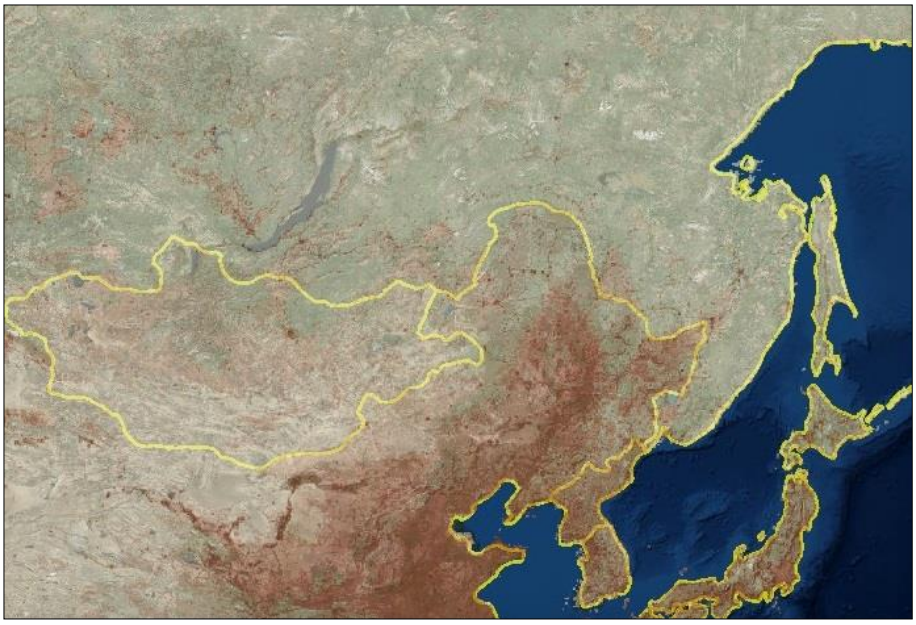
[54] DODDS, Klaus – NUTTALL, Mark: The Arctic – What Everyone Needs to Know. Oxford University Press, New York, 2019. p. 152.

[55] DODDS, Klaus – NUTTALL, Mark: The Arctic – What Everyone Needs to Know. pp. 215–216.

[56] BANDARZSEVSZKIJ, Anton: A Transzszibériai vasútvonal 100 éve. PAGEO, 2017.02.01. http://www.geopolitika.hu/hu/2017/02/01/a-transzsziberiai-vasutvonal-100-eve/; letöltés: 2020.10.17. Az Új Selyemút részeként felmerült a Polar Route tengeri útvonal kérdése is, amely az ázsiai térséget kötné össze az Északi-útvonalon keresztül Európával. The Polar Route and the Belt and Road Initiative. OBOReurope. https://www.oboreurope.com/en/polar-route/; letöltés:2020.10.20.

[57] ZEIHAN, Peter: Analysis: Russia's Far East Turning Chinese. ABC News, 2006.01.06. http://abcnews.go.com/International/story?id=82969&page=1; letöltés:2020.10.31.

kapcsolatban Alekszandr Sajkin[58] 2000. július 29. napján adott tájékoztatást arról, hogy 18 hónap alatt megközelítőleg 1,5 millió ember érkezett illegálisan Kínából Oroszországba.[59] A növekvő kínai bevándorlás a kínai hatalom növekedését jelzi, és egyben előrevetíti a Kína és Oroszország között a jövőben a határok miatt kialakuló feszültséget.[60]



7. ábra. Kína és Oroszország népsűrűsége a térségben[61]
Szerkesztette: Siposné dr. Kecskeméthy Klára

Azt világosan kell látni, hogy a két ország viszonya sajátos. Kína túlnépesedett, sok az olcsó munkaerő és olcsó termékekkel tudja ellátni az orosz piacot. Oroszországban a gazdasági szankciók és az ukrán válság miatt az egyes termékek beszerzése nehézkessé és drágává vált. Szibériának kell az olcsó munkaerő, amit a kínaiak biztosítani tudnak. Az orosz lakosok félnek a sok odaérkező kínaitól és a nyomukban megjelenő jelentős szervezett bűnözői csoportoktól. A hivatalos orosz

[58] Az Oroszország Szövetségi Határszolgálat Határellenőrzési Osztály akkori vezetőjeként nyilatkozott, korábban a kínai–orosz határrendészet vezetője is volt.

[59] TIRNOVEANU, Dragos: Russia, China and the Far East Question – Are there any Chinese 49ers around? The Diplomat, 2016.01.20. https://thediplomat.com/2016/01/russia-china-and-the-far-east-question/; letöltés: 2021.02.25.

[60] KLEIMENOV, Mihail – SAMKOV, Stanislav: Criminal Transportation of Persons: Trends and Recommendations. In: STOECKER, Sally – SHELLEY, Louise (edit.): Human Traffic and Transnational Crime: Eurasian and American Perspectives. Rowman & Littlefield, Oxford, 2002. p. 34.

[61] A térkép a National Geography MapMaker Interactive segítségével készült. MapMaker Interactive. National Geography. https://mapmaker.nationalgeographic.org/; letöltés:2020.02.17.

belügyi és egyéb kormányzati források 2 és 5 millió fő közötti számot adnak meg.[62] Amíg Oroszország európai része több termék beszállításának problémájától szenved, addig a Távol-Keletet olcsó, kétes minőségű kínai termékekkel látják el. Lehetséges, hogy Kína az Orosz Birodalom terjeszkedése során elvesztett Távol-Keletet akarja visszaszerezni? Az Amur térség igazából csak 150 éve tartozik orosz fennhatóság alá. Ennek ellenére Moszkva nagyon ragaszkodik a területhez, minden esetben kijelenti, hogy „*Az Amur orosz volt, most is az, és mindig az is marad.*"[63]

Összegzés

Az Amur térség mind Oroszország, mind Kína számára stratégiai fontosságú terület, amely a két regionális hatalom ütközőzónájában található. Az elmúlt évszázadokban Kína és az Orosz Birodalom, majd a Szovjetunió között számos alkalommal robbant ki határvita a térségért, 1969. március 15-én fegyveres összetűzésre is sor került. Hosszú évtizedek teltek el, mire a mindkét fél által vitatott határ az Amur, az Usszuri és az Argun folyók mentén megnyugtatóan rendeződött.

A térség rendkívül gazdag ásványi nyersanyagokban, energiahordozókban, ritka és nemesfémekben. A térség gazdasági erejét mutatja a Gazprom (Szibéria Ereje gázvezeték, Keleti Gázprogram) és a Transznyeftyegaz (Kelet-Szibéria–Csendes-óceán kőolajvezeték) energiaforrások kiaknázására irányuló erőfeszítései. Az Amur térség stratégiai jelentőségét növelik a térségben található űrrepülőterek (Szvobodnij, Vosztocsnij) is.

A térség napjainkban is jelentősen befolyásolja Oroszország és Kína viszonyát. A határterület lakosságának számában és népsűrűségében hatalmas különbségek mutatkoznak a két ország között. Az Amur térség a kínai legális és illegális bevándorlás célterülete, és a bevándorlás iránya és nagysága nem csökken. Kína napjainkban is vitában áll Oroszországgal az illegális bevándorlás miatt, a két hatalom között emiatt a jövőben elmérgesedhet a vita. Az Amur térség geostratégiai fontosságú terület Oroszország számára. Ehhez kapcsolódóan ki kell emelni azt is, hogy a Japán (Keleti)-tenger és az Ohotszki-tenger stratégiai jelentőségénél fogva az Amur térség fontossága is jelentősen növekedni fog.

FELHASZNÁLT IRODALOM

- 1969 – A Damanszkij incidens. Ritkán látható történelem, 2016.10.04. https://ritkanlathatotortenelem.blog.hu/2016/10/04/1969_a_damanszkij-incidens; letöltés: 2021.01.11.
- A szovjet-kínai határincidens évfordulója. Múlt-Kor, 2004.03.16. https://mult-kor.hu/cikk.php?id=878; letöltés:2021.01.11.

[62] ALEXEEVA, Olga: Chinese Migration in the Russian Far East – A Historical and Sociodemographic Aanalysis. p. 28.

[63] JACOBS, Frank: Why China Will Reclaim Siberia. The New York Times, 2015.01.13. https://www.nytimes.com/roomfordebate/2014/07/03/where-do-borders-need-to-be-redrawn/why-china-will-reclaim-siberia; letöltés: 2020.10.31.

- ALEXEEVA, Olga:
  Chinese Migration in the Russian Far East – A Historical and Sociodemographic Aanalysis.
  China Perspectives, 2008/3, December 2008. pp. 20–32.
  https://www.researchgate.net/publication/301896718_Chinese_Migration_in_the_Russian_Far_East_A_Historical_and_Sociodemographic_Aanalysis; letöltés: 2021.01.27.
- ALEXSEEV, Mikhail A. – HOFSTETTER, C. Richard:
  Russia, China, and the Immigration Security Dilemma.
  Political Science Quarterly, Volume 121, Number 1, Spring 2006. pp. 1–32.
  http://www.jstor.org/stable/20202643; letöltés: 2021.01.25.
- Amur Gas Processing Plant, Amur Region. Hydrocarbons Technology.
  https://www.hydrocarbons-technology.com/projects/amur-gas-processing-plant-amur-region/; letöltés: 2020.10.31.
- BANDARZSEVSZKIJ, Anton: A Transzszibériai vasútvonal 100 éve. PAGEO, 2017.02.01.
  http://www.geopolitika.hu/hu/2017/02/01/a-transzsziberiai-vasutvonal-100-eve/; letöltés: 2020.10.17.
- Building a Russian Far East mining Champion.
  Petropavlovsk PLC, Annual Report & Accounts 2009.
  https://www.petropavlovsk.net/wp-content/uploads/2018/05/Petropavlovsk_AR09_Final.pdf; letöltés: 2021.01.26.
- Characteristics of the Regional Economy. Government of the Amur Region, 2018.12.20.
  https://www.amurobl.ru/en/pages/economy/characteristics-of-the-regional-economy/; letöltés: 2021.01.26.
- Chayandinskoje Field – A resource base for the Power of Siberia gas pipeline. Gazprom.
  https://www.gazprom.com/projects/chayandinskoye/, letöltés: 2020.10.31.
- China, Russia hail end of border dispute. WordPress, 2008.10.16.
  https://jzobk.wordpress.com/tag/tarabarov-island/; letöltés:2021.01.11.
- China-Russia east-route natural gas pipeline in operation. XinhuaNet, 2019.12.02.
  http://www.xinhuanet.com/english/2019-12/02/c_138600270.htm; letöltés: 2020.10.31.
- DODDS, Klaus – NUTTALL, Mark: The Arctic – What Everyone Needs to Know.
  Oxford University Press, New York, 2019.
- Heat and Fire Scorches Siberia. Earth Observatory, March 19 – June 20, 2020.
  https://earthobservatory.nasa.gov/images/146879/heat-and-fire-scorches-siberia; letöltés: 2020.11.05.
- JACOBS, Frank: Why China Will Reclaim Siberia. The New York Times, 2015.01.13.
  https://www.nytimes.com/roomfordebate/2014/07/03/where-do-borders-need-to-be-redrawn/why-china-will-reclaim-siberia; letöltés: 2020.10.31.
- KLEIMENOV, Mihail – SAMKOV, Stanislav:
  Criminal Transportation of Persons: Trends and Recommendations.
  In: STOECKER, Sally – SHELLEY, Louise (edit.): Human Traffic and Transnational Crime: Eurasian and American Perspectives. Rowman & Littlefield, Oxford, 2002. pp. 29–46.
- Kovyktinskoje Field – The most prolific gas field in eastern Russia. Gazprom.
  https://www.gazprom.com/projects/kovyktinskoye/; letöltés: 2020.10.31.

- LADÁNYI László: Oroszország új űrközpontot épít. National Geographic, 2010.07.29. http://www.ng.hu/Fold/2010/07/Oroszorszag_uj_urkozpontot_epit; letöltés: 2020.10.31.
- MapMaker Interactive. National Geography. https://mapmaker.nationalgeographic.org/; letöltés:2020.02.17.
- MINAKIR, Pavel A.: Chinese Immigration in the Russian Far East: Regional, National, and International Dimensions. In: AZRAEL, Jeremy R. – PAYIN, Emil A. (edit.): Cooperation and Conflict in the Former Soviet Union: Implications for Migration. Rand, Santa Monica, 1996. pp. 85–97. https://www.rand.org/pubs/conf_proceedings/CF130.html; letöltés: 2021.01.26.
- Power of Siberia – The largest gas transmission system in Russia's East. Gazprom. https://www.gazprom.com/projects/power-of-siberia/; letöltés: 2020.10.31.
- Progress of Amur GPP construction project reaches 70.5 per cent. Gazprom, 2020.12.17. https://www.gazprom.com/press/news/2020/december/article521180/; letöltés: 2021.01.12.
- Russia Gold Mining: Amur Region. CEIC. https://www.ceicdata.com/en/russia/mining-and-quarrying-volume-gold-annual/gold-mining-amur-region; letöltés: 2021.03.22.
- Sakhalin II – Russia's first liquefied natural gas plant. Gazprom. https://www.gazprom.com/projects/sakhalin2/; letöltés: 2021.03.23.
- Sakhalin-III – Cutting-edge technologies for subsea hydrocarbon production. Gazprom. https://www.gazprom.com/projects/sakhalin3/; letöltés:2020.11.03.
- SHIAU-SHYANG, Liou: Chinese Immigration to Russia and Its Non-traditional Security Impact. East Asia, Volume 34, Issue 4, December 2017. pp. 271–286. https://www.researchgate.net/publication/322092741_Chinese_Immigration_to_Russia_and_Its_Non-traditional_Security_Impact; letöltés: 2021.01.20.
- Svobodny. European Space Agency. http://www.esa.int/About_Us/ESA_Permanent_Mission_in_Russia/Svobodny; letöltés: 2020.10.31.
- The ESPO (Eastern Siberia Pacific Ocean) Oil Pipeline, Siberia, Russia. Hydrocarbons Technology. https://www.hydrocarbons-technology.com/projects/espopipeline/; letöltés: 2020.11.05.
- The Polar Route and the Belt and Road Initiative. OBOReurope. https://www.oboreurope.com/en/polar-route/; letöltés:2020.10.20.
- The Trans-Siberian Railroad. https://www.trans-siberian-travel.com; letöltés: 2020.10.28.
- The World Factbook: China. https://www.cia.gov/the-world-factbook/countries/china/#geography; letöltés: 2021.01.11.
- TIRNOVEANU, Dragos: Russia, China and the Far East Question – Are there any Chinese 49ers around? The Diplomat, 2016.01.20. https://thediplomat.com/2016/01/russia-china-and-the-far-east-question/; letöltés: 2021.02.25.

- Transneft Brings Eastern Siberia – Pacific Ocean Oil Pipeline to Maximum Capacity. Transneft, 2019.11.27. https://en.transneft.ru/newsPress/view/id/25213; letöltés: 2020.11.05.
- USSR/China: Soviet and Chinese Forces Clash on the Ussuri River. U.S. Department of State, 1969.03.04. https://nsarchive2.gwu.edu/NSAEBB/NSAEBB49/sino.sov.1.pdf; letöltés: 2021.01.11.
- WEINER Csaba: Az orosz gázipar helyzete a világgazdaságban és hatása a nemzetközi együttműködésre. Doktori disszertáció. Széchenyi István Egyetem, Győr, 2010. p. 314. http://www.kodolanyi.hu/oroszcivilizacio/doc/hasznos/weiner_orosz_gazipar.pdf; letöltés:2020.11.03.
- ZAK, Anatoly: Soyuz launch pad in Vostochny – Missions origniated from the Soyuz launch facility in Vostochny. RussianSpaceWeb. http://www.russianspaceweb.com/vostochny_soyuz.html; letöltés: 2021.04.28.
- ZAK, Anatoly: Soyuz launch pad in Vostochny – The launch pad location. RussianSpaceWeb. http://www.russianspaceweb.com/vostochny_soyuz.html; letöltés: 2021.01.20.
- ZAKHAROV, Andrei – NAPALKOVA, Anastasia: Why Chinese farmers have crossed border into Russia's Far East. BBC News, 2019.11.01. https://www.bbc.com/news/world-europe-50185006; letöltés: 2021.01.09.
- ZEIHAN, Peter: Analysis: Russia's Far East Turning Chinese. ABC News, 2006.01.06. http://abcnews.go.com/International/story?id=82969&page=1; letöltés:2020.10.31.
- ZENTAI László: Kína területi vitái. Lázár Kollokvium, 2011.04.29. http://lazarus.elte.hu/hun/lk/110429/2011-04-29-zl.pdf; letöltés: 2021.01.11.
- Владение языками населением наиболее многочисленных национальностей по субъектам Российской Федерации. https://www.gks.ru/free_doc/new_site/perepis2010/croc/Documents/Vol4/pub-04-07.pdf; 2021.01.15.
- Нефтепровод Восточная Сибирь - Тихий Океан (ВСТО). Neftegaz.RU, 2013.03.19. https://neftegaz.ru/tech-library/transportirovka-i-khranenie/141847-vostochnyy-nefteprovod-vsto/; letöltés: 2021.04.27.
- ОЦЕНКА ЧИСЛЕННОСТИ НАСЕЛЕНИЯ на 1 января 2016 года и в среднем за 2015 год. http://www.gks.ru/free_doc/new_site/population/demo/Popul2016.xls; letöltés: 2020.11.01.
- ОЦЕНКА ЧИСЛЕННОСТИ НАСЕЛЕНИЯ на 1 января 2020 года и в среднем за 2019 год. https://www.gks.ru/storage/mediabank/PrPopul2020.xls; letöltés: 2021.01.10.

E SZÁMUNK TARTALMA

POMOGÁCS PÉTER

A „KIS KÉK EMBEREK” – A KÍNAI NÉPKÖZTÁRSASÁG TENGERI MILÍCIÁJÁNAK TEVÉKENYSÉGE A KELET-KÍNAI- ÉS A DÉL-KÍNAI-TENGEREN

A tanulmány célja a kínai Népi Fegyveres Erők Tengeri Milíciája Kelet-kínai- és a Dél-kínai-tengeren folytatott tevékenységének bemutatása. Kína a Tengeri Milíciáját a hibrid hadviselés keretein belül arra használja, hogy kiterjessze befolyását a térségre. Méretéből és félkatonai jellegből adódóan a szervezet ideális eszköz Kína kezében kelet-ázsiai riválisaival, vagy akár az Amerika Egyesült Államokkal szembeni fellépésre, miközben a konfliktusok intenzitása végig a háborús küszöb alatt marad. A Tengeri Milícia vélhetően nagy hangsúlyt kap Peking stratégiai jövőképében, miszerint Kínának belátható időn belül tengeri nagyhatalommá kell válnia.

Kulcsszavak: Kína, Tengeri Milícia, Kelet-kínai-tenger, Dél-kínai-tenger, hibrid hadviselés, halászat.

DR. ALBERT ÁGOTA –
DR. TÓTH SÁNDOR ALEZREDES
ÜVEGES ANDRÁS JÓZSEF SZÁZADOS –
LÉVAI ZSOLT

A KÖZLEKEDÉSI RENDSZER ÉS AZ INFORMÁCIÓS TERRORIZMUS KAPCSOLATRENDSZERE

A terrorizmus nemcsak mindennapi biztonságunkat, hanem demokratikus társadalmaink alapértékeit, valamint az európai polgárok jogait és szabadságát is fenyegeti. A terrorizmus elleni küzdelem elsődleges prioritást jelent az Európai Unió és tagállamai, valamint nemzetközi partnerei számára. Mára ezt nemcsak a fizikai térben kell értelmezni, hanem a kibertérben is. A kibertérből érkező fenyegetések már a fizikai térben is rombolást vagy pusztítást okozhatnak. Az információs terrorizmus során végrehajtott műveletek érinthetik a közlekedési rendszereket. Ezek a közlekedési rendszerek a működésükhöz szükséges nagy mennyiségű személyes adatot is tárolnak, amelyekre az információs terrorizmus szintén hatással lehet.

Kulcsszavak: információs terrorizmus, közforgalmi közlekedés, GDPR, adatvédelem.

CONTENTS

KÁROLY LÁSZLÓ ALEZREDES

EGYSÉGES FELDERÍTŐRENDSZER KIALAKÍTÁSA A VÁLSÁGKEZELŐ MŰVELET MEGINDÍTÁSA ELŐTT

Az egységes felderítőrendszer kialakítását a válságkezelő műveletet megelőzően kell végrehajtani. A felderítőrendszernek a készenlétet a kontingens műveleti készenlétét megelőzően el kell érnie. A rendszer kialakítása a kontingens felderítőfőnökének a feladata.

Kulcsszavak: aszimmetrikus hadviselés, egységes felderítőrendszer, elhárítás, katonai felderítés, nemzeti hírszerzés, összadatforrású felderítés.

ERDÉSZ VIKTOR FŐHADNAGY

AZ IDGA KONFERENCIÁJA A MESTERSÉGES INTELLIGENCIA SZEREPÉRŐL A HÍRSZERZŐ ELEMZÉS-ÉRTÉKELÉSBEN

Az IDGA online konferenciája kiváló betekintést engedett az amerikai nemzetbiztonsági hírszerző elemzés-értékelés jelenlegi helyzetébe, eljárásaiba és problémáiba. Az előadások alapján az amerikai szolgálatok széleskörűen alkalmazzák az MI-alapú elemző-értékelő szoftverrendszereket és a nagyadatot. A fejlődés fő gátja már nem a technológia kiforratlansága, hanem a Hírszerző Közösség bürokratikus megközelítése és az emberi munkaerő egy részének hozzáállása. Az előadások bemutatták az akadémiai szférával, a technológiai vállalatokkal, valamint a kereskedelmi tartalomszolgáltatókkal megvalósuló szoros nemzetbiztonsági együttműködés egyes Kínával kapcsolatos eredményeit is.

Kulcsszavak: mesterséges intelligencia, hírszerzés, elemzés-értékelés, Amerikai Egyesült Államok, Kína.

KISVÁRI TAMÁS EZREDES

A KÍNAI KIBERTÉR ÉS A KÍNAI HADERŐ KIBERMŰVELETI ERŐINEK ÉS TEVÉKENYSÉGÉNEK BEMUTATÁSA

Kínában a kibertér igen komoly korlátozásokkal működik, aminek alapvetően belpolitikai okai vannak. Ennek ellenére a kínai lakosság az európai lakosságnál kiterjedtebben használja az internet adta lehetőségeket. Kína az 5G területén már jelentősen meghaladta a világot, és ez a tendencia valószínűleg csak erősödni fog.

Kína a 2015-ben végrehajtott katonai reform részeként egy új haderőnemet alkotott az elektronikai harc, a pszichológiai és kiberhadviselés, illetve az űrhadviselés folytatására. Kína egyre szélesebb körben tervezi alkalmazni az új területek adta lehetőségeket, hogy harc nélkül nyerje meg háborúit, és a hibrid hadviselés eszközeivel érje el külpolitikai céljait. A kiberterületen Kína eddig leginkább a kiberkémkedésre koncentrált, de a példák azt mutatják, hogy a kiberképességeik alkalmasak az ellenség rendszereinek pusztítására is, ha erre lenne szükség.

Kulcsszavak: internet, kibertér, kiberkémkedés, Hadászati Támogató Erő.

LIEUTENANT COLONEL LÁSZLÓ KÁROLY

ORGANIZING OF INTEGRATED INTELLIGENCE SYSTEM BEFORE THE CRISES RESPONSE OPERATION

The integrated intelligence system has to be organized prior to the crises response operation. The integrated intelligence system has to achieve the standby before the operational readiness of the contingent. The Intelligence Chief of the contingent has to organize the integrated intelligence system.

Keywords: asymmetric warfare, integrated intelligence system, counterintelligence, military intelligence, national intelligence, all source intelligence.

FIRST LIEUTENANT VIKTOR ERDÉSZ

IDGA CONFERENCE ON THE ROLE OF ARTIFICIAL INTELLIGENCE IN INTELLIGENCE ANALYSIS

IDGA's online conference granted excellent insight into the current situation, procedures and problems of American intelligence analysis. According to the presentations, US intelligence and security services widely utilize artificial intelligence-based software systems and big data. Technological maturity is no longer a substantial obstacle of progress; it is now the bureaucratic approach of the Intelligence Community and the attitude of some of the human workforce. The presentations also highlighted some China-related outcome of intelligence cooperation realized with the academic sphere, technological companies and commercial content providers.

Keywords: artificial intelligence, intelligence, analysis, USA, China.

COLONEL TAMÁS KISVÁRI

OVERVIEW OF THE CHINESE CYBERSPACE AND PEOPLE'S LIBERATION ARMY'S CYBER OPERATION FORCES AND THEIR ACTIVITY

In the People's Republic of China cyber space has long been operating within the strict boundaries set by internal politics. Nonetheless, internet usage is significantly more widespread amongst China's population compared to its European counterparts. Today, China has a significant lead in the global 5G domain and remains in a strong position to inevitably continue widening the gap.

As part of the 2015 military reform, China established a new force comprising of electronic, psychological and cyber warfare capabilities as well as space warfare capability. China seeks to use its new capabilities to enable it to win wars without combat and achieve its foreign policy objectives using the hybrid warfare capabilities. In the cyber domain China has so far focused its efforts in cyber espionage, but recent examples show that the cyber capabilities of China are suitable for destroying enemy networks if required.

Keywords: internet, cyberspace, cyber domain, cyber-espionage, SSF.

FELEGYI JÚLIA

GÖRÖGORSZÁG MIGRÁCIÓS POLITIKÁJA

A publikáció célja a görög migrációs politika bemutatása, annak kezdeteitől egészen napjainkig. A szerző a történelmi bevezetést követően a migrációval kapcsolatos események kronologikus bemutatására törekszik.

Görögország földrajzi elhelyezkedése miatt a kezdeti kibocsátó országból cél- és tranzitországgá vált. Az elmúlt évtizedekben egyre gyakoribbá váltak az illegális átjutási kísérletek mind az égei-tengeri szigetekre, mind Törökország felől a szárazföldre. Az illegális migráció enyhítésére a görög kormány a határok megerősítésével, a tengeri és a szárazföldi ellenőrzések fokozott intenzitásával, vízi akadályokkal és jogszabályokkal is keresi a megoldást. A legtöbb célországhoz hasonlóan az elmúlt időszakban az újonnan érkező illegális bevándorlók és a velük kapcsolatos intézmények és bűncselekmények az illegális migrációnak leginkább kitett területeken a turizmus csökkenése és a pandémia miatt egyébként is feszült lakosság tiltakozását váltották ki.

2020-ban a koronavírus, a török–görög konfliktus újraéledése és a tavaszi török–görög szárazföldi határra nehezedő migrációs nyomás is próbára tette a görög kormányt. A pandémia és a megváltozott migrációs útvonalak következtében ugyan az elmúlt hónapokban kevesebben érkeztek, de a fennálló problémákkal a vezetésnek továbbra is számolnia kell. Az égei-tengeri táboroknál történt gyújtogatások, az ott tartózkodók elszállásolása, a bevándorlók integrációja és a turizmus több okból történt kiesése mind csapást mértek az új kormányra, amely a publikáció megjelenésének idején is keresi a működőképes megoldást.

Kulcsszavak: Görögország, migráció, migrációs politika.

CSUTAK ZSOLT

A KIBERMÁTRIX KIHÍVÁSAI ÉS LEHETŐSÉGEI A 21. SZÁZAD TÁRSADALMÁBAN

A 21. században az emberiség korábban még soha nem tapasztalt technológiai változásokkal, forradalmian új megoldásokkal szembesül, amelyek teljesen új társadalmi, lélektani kihívásokat jelentenek és nyilvánvaló módon jelentős biztonsági kockázatokat is hordoznak. Ebben a virtuális, digitális ökoszisztémában állami és nem állami szereplők versengenek és konfliktusokat gerjesztenek, bűncselekményeket követnek el, ami napjainkban már első számú globális problémává fejlődött. A társadalmak működését meghatározó online médiaszolgáltatók befolyása, a kiberfegyverek, harci robotok és mesterséges intelligencia vezérelte összekapcsolódó okosgépek és -rendszerek hálózata és várható fejlődése már nem csupán a sci-fi irodalom érdekes jelenségei, hanem a jelen és a közeljövő világának aggodalomra is okot adó trendjei. Mindezen új technológiai tényezők emberi, társadalmi vonatkozásairól és veszélyforrásairól már nem lehet eltekinteni, habár a problémákat könnyebb beazonosítani, mint megfelelő válaszokat találni rájuk.

Kulcsszavak: kibertér, kiberbiztonság, mesterséges intelligencia, digitális alkalmazások, jövőkutatás.

JÚLIA FELEGYI

GREECE'S MIGRATION POLICY

The aim of this publication is to present the Greek migration policy, from its beginnings to nowadays. Following the historical introduction, the author seeks to present events related to migration in chronological order.

Due to its geographical location, Greece has moved from an initial issuing country to a destination and transit country. Attempts at illegal transit both to the Aegean islands and from Turkey to the mainland have become increasingly common in recent decades. To alleviate illegal migration, the Greek government is also looking for a solution through the strengthening of borders, the fortified intensity of sea and land border controls, water barriers and legislation. As in most destination countries, recent arrivals of illegal immigrants and related institutions and crimes have provoked protests from the already tense population in the areas most exposed to illegal migration. This situation was even worsened by the pandemic and declining tourism.

In 2020, the coronavirus, the resurgence of the Turkish-Greek conflict, and the migratory pressure on the Turkish-Greek land border in the spring also put the Greek government to the test. Although fewer people have arrived in recent months as a result of the pandemic and changed migration routes, management still has to deal with the problems that exist. The arson attacks in the Aegean camps, the accommodation of those there, the integration of immigrants and the dropping of tourism for several reasons have all dealt a blow to the new government, which is also looking for a workable solution at the time of publication.

Keywords: Greece, migration, migration policy.

ZSOLT CSUTAK

CHALLENGES OF THE CYBER MATRIX IN THE 21ST CENTURY SOCIETY

In the 21st century, the human race must face and cope with such new revolutionary technological challenges and trends that had never been encountered before in history. These factors feature brand new psychologic, social challenges and evidently pose serious security risks, as well. In this inter-connected global digital ecosystem, state and non-state actors commit various acts simultaneously, which altogether constitute major global security risks. Crucial issues, such as cyber warfare, weaponization of digital information and the influential effects of social media platforms upon society cannot be neglected anymore. Nevertheless, finding proper solutions proves to be even a bigger intellectual and political challenge than identifying the emerging problems.

Keywords: cyber warfare and security, digital applications, artificial intelligence, futurology.

DR. NÉGYESI IMRE EZREDES –
DR. ALBERT ÁGOTA –
ÜVEGES ANDRÁS JÓZSEF SZÁZADOS

A FELHŐALKALMAZÁSOK ADATVÉDELMI KÉRDÉSEI A GDPR TÜKRÉBEN

Napjaink szinte elválaszthatatlan része a felhőszolgáltatás. A felhőszolgáltatások lehetővé teszik az igény szerinti hálózati hozzáférést megosztott, konfigurálható számítástechnikai erőforrásokhoz, amelyeket gyorsan lehet allokálni és használatukat lezárni minimális menedzsment-ráfordítással vagy szolgáltatói közreműködéssel. Emellett a felhőszolgáltatások túlnyomó többsége már globálisan is hozzáférhető bárhonnan, és viszonylag kis anyagi ráfordítással nagyméretű tárhelyeket tudunk bérelni személyes vagy üzleti adataink tárolására. A felhőszolgáltatásnak azonban árnyoldala is van, mivel előfordulhat, hogy a szolgáltatást igénybe vevők egyáltalán nem rendelkeznek kontrollal saját adataik felett, és még az is elképzelhető, hogy azzal sincsenek tisztában, hogy éppen egy felhőszolgáltatást vesznek igénybe.

A személyes és az üzleti adatok felhőben tárolása számos kockázatot hordoz, ezek egy részét pedig a szereplők a GDPR segítségével tudják csökkenteni, ideértve például az érintetti jogok érvényesíthetőségét, az alapelveknek való megfelelőséget, valamint a beépített adatvédelem követelményét, amelyek mind erősíthetik a felhasználók bizalmát a felhőszolgáltatásokban.

Kulcsszavak: GDPR, adatvédelem, felhőszolgáltatás, információbiztonság.

DR. FÓRIZS SÁNDOR NY. R. DANDÁRTÁBORNOK

A HATÁRŐRSÉG FELDERÍTŐSZOLGÁLATÁNAK TEVÉKENYSÉGE 1951–1952-BEN

A publikáció a határőrség felderítőszolgálata 1951–1952. évi tevékenységét ismerteti levéltári dokumentumok alapján. Az olvasó megismerheti a jugoszláv és az osztrák államhatáron bekövetkezett, a felderítőmunka szempontjából fontos eseményeket, megtett intézkedéseket, a megjelent jelentősebb dokumentumokat, az abban az évben kialakult sajátos biztonsági helyzetet. A szerző bemutat néhány egyéni történést, melyeken keresztül betekintést nyerhetünk a határőrségi felderítőmunka rendkívüli körülményeibe.

Kulcsszavak: átdobás, felderítőszolgálat, határőrség, hálózati munka, ügynök.

COLONEL IMRE NÉGYESI, PhD –
ÁGOTA ALBERT LL. M. –
CAPTAIN ANDRÁS JÓZSEF ÜVEGES

DATA PROTECTION ISSUES OF THE CLOUD SERVICE IN THE LIGHT OF THE GDPR

Nowadays, cloud computing and services are becoming more and more part of us. Cloud services provide on-demand network access to shared, configurable computing resources that can be quickly allocated and finished with minimal management effort or provider intervention. In addition, most cloud services are now available globally from anywhere, with relatively small financial sources we can rent large storage space for our personal or business data. Sensitive personal and business data stored in the cloud holds a number of risks. It is also important to emphasize that data stored in the European Union and in the EU Member States on cloud services should also be examined in the light of the GDPR. In our article, we systematize and identify the risks that cloud service poses to GDPR compliance. What methods are currently used by service providers to protect personal and business data stored in the cloud, as well as the impact of GDPR on cybersecurity of cloud services.

Keywords: GDPR, data protection, cloud service, information security.

BRIGADIER GENERAL (RET.) SÁNDOR FÓRIZS, CSc

THE ACTIVITIES OF THE RECONNAISSANCE SERVICE OF THE HUNGARIAN BORDER GUARD IN 1951 AND 1952

The publication discusses the activities of the reconnaissance service of the Border Guard in 1951 and 1952 on the basis of archival documents. The events that took place at the Yugoslavian and Austrian state borders that were important from the aspect of reconnaissance work are presented, as well as the measures taken, the significant documents published and the particular security situation that developed in that year. The paper describes a few individual events through which we can gain insight into the extraordinary circumstances of border guard reconnaissance work.

Keywords: deployment behind the border, reconnaissance service, Border Guard, networking, agent.

DR. GERENCSÉR ÁRPÁD –
SIPOSNÉ DR. KECSKEMÉTHY KLÁRA

AZ AMUR TÉRSÉG VÁLTOZÓ GEOSTRATÉGIAI JELENTŐSÉGE

A stratégiai fontosságú Amur térség az Oroszországi Föderáció Távol-keleti Szövetségi Körzetében helyezkedik el. Zord éghajlat, gyér lakosság és a perspektíva hiánya miatti elvándorlás következtében növekvő problémák jellemzik. Két geopolitikai szereplő (Oroszországi Föderáció, Kína), regionális hatalom ütközőzónájában, illetve határzónájában helyezkedik el, ez a terület fontos mind az orosz, mind a kínai geopolitikai gondolkodásban. A térség stratégiai jelentősége folyamatosan változott a történelem során. Kína és a Szovjetunió között még fegyveres incidens (határvita) is kirobbant a térségért. Napjainkban egyre fontosabbá válik az Amur térség, mivel Szibéria déli területei folyamatosan felértékelődnek Kína számára az ásvány- és nyersanyagkészletek, az energetikai szektor, a térségen áthaladó kőolaj- és földgázvezetékek, az energetikai infrastrukturális fejlesztések, valamint az Új Selyemút Stratégia (Egy övezet, egy út kezdeményezés) miatt. Az Amur térség a kínai legális és illegális bevándorlás célterülete.

Kulcsszavak: Kína, Oroszország, geostratégiai jelentőség, energetikai szektor, kőolaj- és földgázvezetékek.

ÁRPÁD GERENCSÉR, PhD –
KLÁRA SIPOSNÉ KECSKEMÉTHY, CSc

THE CHANGING GEOSTRATEGIC IMPORTANCE OF THE AMUR REGION

The strategically important Amur region is located in the Far East of the Russian Federation, characterized by a harsh climate, sparse population and emigration due to lack of perspective. The territory is located in the collision zone of two geopolitical players (Russian Federation, China), in the border zone of regional powers, so this area is important in both Russian and Chinese geopolitical thinking. The strategic importance of the region has been constantly changing throughout history. Even an armed incident (border dispute) erupted between China and the Soviet Union over the region. Nowadays, the Amur region is becoming increasingly important as the southern areas of Siberia are becoming more and more valuable to China, due to its mineral and raw material reserves, the energy sector, oil and gas pipelines passing through the region, energy infrastructure developments, and the New Silk Road Strategy (One Belt One Road Initiative, OBOR). The Amur region is a destination for legal and illegal immigration in China.

Keywords: China, Russian Federation, geostrategic significance, energy sector, oil and gas pipelines.

CONTENTS

R & D

HISTORY OF INTELLIGENCE

FORUM

FOR READERS

A KÖTET SZERZŐI

Albert Ágota	LL. M., adatvédelmi tisztviselő
Csutak Zsolt	a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola doktorandusza
Erdész Viktor	főhadnagy, a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola doktorandusza
Felegyi Júlia	a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola doktorandusza
Fórizs Sándor	ny. r. dandártábornok, CSc, habil.,, a Nemzeti Közszolgálati Egyetem ny. egyetemi tanára
Gerencsér Árpád	PhD, a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola végzett doktora
Károly László	alezredes
Kisvári Tamás	ezredes, a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola doktorandusza
Lévai Zsolt	Közlekedéstudományi Intézet, senior kutató
Négyesi Imre	ezredes, PhD, habil., a Nemzeti Közszolgálati Egyetem tanszékvezető egyetemi docense
Pomogács Péter	a Nemzeti Közszolgálati Egyetem Hadtudományi Doktori Iskola doktorandusza
Siposné Kecskeméthy Klára	ezredes, CSc, a Nemzeti Közszolgálati Egyetem egyetemi tanára
Tóth Sándor	alezredes, PhD
Üveges András József	százados, a Nemzeti Közszolgálati Egyetem Katonai Műszaki Doktori Iskola doktorandusza

A FELDERÍTŐ SZEMLÉBEN TÖRTÉNŐ PUBLIKÁLÁS FELTÉTELEI

AZ ÍRÁSMŰVEKKEL SZEMBEN TÁMASZTOTT KÖVETELMÉNYEK

Etikai követelmények:

- az írásmű máshol, ebben a formájában még nem jelent meg;
- a szerző(k) kizárólagos szellemi tulajdona, amelyet a szerzői nyilatkozat aláírásával igazol(nak);
- korrekt, visszakereshető hivatkozásokkal ellátott;
- bibliográfiával ellátott (amely tartalmazza a hivatkozott irodalom jegyzékét, az internetes anyagok jegyzékét a letöltés idejével együtt);
- a szerző(k) saját véleményét is tükrözheti, amely értelemszerűen nem mindig egyezik meg a Szolgálat álláspontjával.

Tartalmi követelmények:

- a folyóiratokban – jellegével összhangban – a honvédelemmel, azon belül elsősorban a nemzetbiztonsággal, hírszerzéssel, felderítéssel, katonai biztonsággal és a biztonságpolitikával kapcsolatos tudományos igényű kérdéseket feldolgozó és elemző írásokat – tanulmányokat, cikkeket és más témákat, anyagokat – jelentetünk meg;
- az írásmű legyen logikus, áttekinthető, tartalmilag összefüggő és jól tagolt;
- a témával kapcsolatos saját koncepció megfogalmazása legyen érthető, a következtetések pedig megalapozottak, érvekkel, adatokkal alátámasztottak legyenek.

Formai követelmények (és a kapcsolódó információk)**:**

- a szerzői kéziratok terjedelme lehetőleg ne haladja meg az egy szerzői ívet (40 ezer karakter, illetve 20–21 gépelt oldal);
- a kéziratot elektronikus formában, Times New Roman 12 pontos betűkkel, másfeles sortávolsággal írva, a képeket és ábrákat feldolgozható (.jpg vagy .tif) formátumban kérjük megküldeni a deak.anita@knbsz.gov.hu e-mail címre. A kézirathoz kérjük mellékelni a szerző vagy szerzők nevét, rendfokozatát, beosztását vagy munkakörét, állandó lakcímét, telefonon és interneten történő elérhetőségét;

- a közlésre elfogadott írásokért – a szerzői nyilatkozattal létrejött megállapodás figyelembevételével – szerzői honorárium fizethető;
- a kéziratokat a Szerkesztőbizottság minden esetben lektoráltatja. A kiadványban megjelentetni kívánt írásokat a Szolgálat kompetens, tudományos fokozattal rendelkező munkatársai vagy más szakértők lektorálják;
- a Szerkesztőbizottság – a lektori vélemények figyelembevételével – fenntartja a jogot, hogy a megjelenésre alkalmatlannak ítélt kéziratokat – indoklás nélkül – nem közli. Az ilyen írásokat nem küldi vissza és nem őrzi meg;
- a kiadványban bárki publikálhat, akinek az írását a Szerkesztőbizottság az etikai, tartalmi és formai követelmények alapján, kiadványban történő megjelentetésre, valamint az interneten történő közzétételre alkalmasnak tartja. A közlésre nem került kéziratot csak az adott naptári év végéig őrizzük meg, de a szerző kérésére azt visszaadjuk;
- a közleményhez rövid tartalmi összefoglalót (Absztrakt/Rezümé) kell mellékelni, maximum 10–12 sorban, magyar és angol nyelven;
- a közleményhez három–öt kulcsszó megadása szükséges, magyar és angol nyelven.
- az írás angol nyelvű címét is kérjük megküldeni.

A KÖZLEMÉNYEKKEL SZEMBEN TÁMASZTOTT FORMAI KÖVETELMÉNYEK

A folyóirat kizárólag az MSZ ISO 960 szabvány alapján készített hivatkozásokkal ellátott tanulmányt, cikket jelentet meg.

A közleményhez szükséges megadni:

A SZERZŐ, SZERZŐK NEVE (rendfokozata);

AZ ÍRÁS CÍME (magyarul, angolul);

REZÜMÉ (magyarul, angolul);

KULCSSZAVAK (magyarul, angolul);

SZERZŐI NYILATKOZAT.

BIBLIOGRÁFIAI HIVATKOZÁS

A társadalomtudományokban a megszokott számozott hivatkozást az idézések jegyzetben[1] módszerrel kérjük alkalmazni.

Abban az esetben, ha a szerző nem ezt a módszert alkalmazza, a kéziratot lektorálás nélkül visszaküldjük átdolgozásra!

Idézések jegyzetben:

A szövegen belüli idézést követően felső indexként megadott sorszámok jegyzetekre utalnak, amelyeket a szövegbeli megjelenésük sorrendjében kell közölni. Ezek a jegyzetek tartalmazhatják az idézéseket.

Első idézés:

Ha az idézések jegyzetben vannak megadva, egy dokumentumra vonatkozó első idézésnek tartalmaznia kell az idézés és a bibliográfiai hivatkozások külön jegyzékében lévő kapcsolódó tétel pontos megfeleltetéséhez szükséges adatokat. Az első idézésnek tartalmazni kell: legalább a szerző(k) nevét és a teljes címet úgy, ahogy azok a bibliográfiai hivatkozásokban meg vannak adva, továbbá az idézett rész oldalszámát, ha az szükséges.

Példák:

(1) ÁCS Tibor: A reformkor hadikultúrájáról. p. 34.

(2) BEREK Lajos: A hadtudományi kutatómunka alapjai. p. 33.

(3) KOVÁCS Jenő: Az új magyar hadtudomány gyökerei, fejlődésének szemléleti problémái. p. 6.

(4) www.globalsecutity.org/army/iraq; letöltés: 2012.04.19.

Bibliográfiai hivatkozások jegyzéke:

A bibliográfiai hivatkozások jegyzékében a hivatkozásokat az első adatelem betűrendjében kérjük megadni.[2]

Példák:

(1) ÁCS Tibor: A reformkor hadikultúrájáról. Zrínyi Kiadó, Budapest, 2005. ISBN 963 9276 45 6

(2) BEREK Lajos: A hadtudományi kutatómunka alapjai. In: SZILÁGYI Tivadar (szerk.): Szemelvények. Zrínyi Miklós Katonai Akadémia, Budapest, 1994. pp. 31–50.

---

[1] Bibliográfiai hivatkozások. Magyar Szabvány, MSZ ISO 690. pp. 19–20.
[2] Bibliográfiai hivatkozások. Magyar Szabvány, MSZ ISO 690. p. 18.

(3) KOVÁCS Jenő: Az új magyar hadtudomány gyökerei, fejlődésének szemléleti problémái. In: Új Honvédségi Szemle, 1993. 47. évf. 6. sz. pp. 1–7. ISSN 1216-7436

(4) www.globalsecutity.org/army/iraq; letöltés: 2012.04.19.

Ábra, vázlat, térkép, diagram, egyéb melléklettel szembeni követelmények:

- az ábra, vázlat sorszáma (például 1. ábra.);
- az ábra, vázlat címe;
- az ábra, vázlat forrása (vagy: Szerkesztette: …);
- idegen nyelvű ábra, vázlat esetén lehetőség szerint magyar nyelvű jelmagyarázat.

Rövidítések, idegen kifejezésekkel kapcsolatos követelmények:

- az idegen kifejezéseket, rövidítéseket magyarul és eredeti idegen nyelven kell az írásműben az első alkalommal feloldani lábjegyzetben;

Példa:

- WFP – World Food Program – ENSZ Világélelmezési Programja.

SZERKESZTŐBIZOTTSÁG

ELÉRHETŐSÉGEINK

Postacím: Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa
1021 Budapest, Budakeszi út 99–101.

Katonai Nemzetbiztonsági Szolgálat Tudományos Tanácsa
1525 Budapest, Pf. 74.

E-mail: Dr. Deák Anita alezredes
06(1) 386-9344/5210, HM 65-210
e-mail: deak.anita@knbsz.gov.hu