Doktori (PhD) értekezés tervezet

dr. Hódos László

2026

NEMZETI KÖZSZOLGÁLATI EGYETEM

Hadtudományi Doktori Iskola

dr. Hódos László

A jogi hadviselés és az információs műveletek egyes intézkedéseinek vizsgálata a hibrid hadviselés kontextusában

Doktori (PhD) értekezés tervezet

Témavezető:

Dr. Dobák Imre habil. e. docens

……

Budapest, 2026

TARTALOMJEGYZÉK

I. BEVEZETŐ GONDOLATOK, A MŰ ELKÉSZÍTÉSE SORÁN ALKALMAZOTT TUDOMÁNYELMÉLETI ESZKÖZÖK ÉS MÓDSZEREK

1. A témaválasztás aktualitása és indokolása

A téma aktualitását az adja, hogy a 21. században az információs műveletek és a jogi hadviselés[1] gyakorlata és a jogszabályi környezet kölcsönhatásai egyre bonyolultabbá és összetettebbé váltak. Az információs műveletek célja gyakran a közvélemény befolyásolása, a politikai döntéshozatal megzavarása vagy az idegen államok belügyeibe való beavatkozás. Ezen műveletek eszköztárába tartozik a dezinformáció, a propaganda és a kibertámadás is.

A kutatásom során vizsgálom, hogy miként hatnak ezek az intézkedések a jelenlegi jogszabályi környezetre, és hogyan alakítják azt. Fontos feltérképezni, hogy az információs műveletek és a jogi hadviselés miként befolyásolják a nemzetközi jogot és a nemzeti jogrendszereket, valamint azt, hogy ezek milyen kihívásokat jelentenek a jogalkotók és jogalkalmazó szolgálatok, szervek, hatóságok számára.

A nemzetbiztonsági szolgálatok által alkalmazott erők, eszközök és módszerek együttes hatásmechanizmusának szabályozási eszközrendszere a jogforrási hierarchia legmagasabb szintjétől a legalacsonyabbig terjedő széles spektrumot ölel fel. Ezek a magyar nemzet biztonságának védelme érdekében – döntően titokban, néha nyíltan – kerülnek alkalmazásra a szolgálatok munkatársai által. A jogi normákban megjelenő feladatok végrehajtása esetenként alapjog-korlátozással jár együtt, emiatt ezeket az állami monopóliumként kodifikált tevékenységeket szigorú előírások között gyakorolhatják az erre feljogosított szervezetek.

Az értekezésem célja, hogy igazoljam, hogy a normaalkotás ezeken a területeken sokkal összetettebb, mint pusztán kodifikációs feladat, mivel a történelmi előzményeket, a 21. századi biztonsági kihívásokat és a jogalkotási rendszer aktuális lehetőségeit egyaránt figyelembe kell

[1] A jogi hadviselés későbbiekben részletesen vizsgált, röviden összegzett fogalma szerint, a jog eszközként való felhasználását jelenti konfliktusokban, ahol a jogi rendszereket és azok gyengeségeit kihasználva próbálnak előnyt szerezni az államok vagy nem állami szereplők. Ez magában foglalhatja például a nemzetközi jog értelmezésének manipulálását, jogi kiskapuk kihasználását, vagy akár a bíróságokat és nemzetközi intézményeket befolyásoló stratégiákat is.

venni. Megítélésem szerint, mindhárom szempontrendszernek megfelelő szakmai koncepciót, stratégiát és ennek alapján kialakítandó jogi normákat szükséges készíteni, és új megoldásokat alkalmazni.

Célul tűztem ki a vizsgálat során, hogy rámutassak, hogy ezen szakági normák és struktúrák jelenleg csak korlátozott hatékonysággal képesek működni, mert a történelmi távlatból még csak részben vizsgálható 20. század végén, illetve 21. század elején keletkezett tapasztalatokat minden részletre kiterjedően még nem sikerült rendszerezni, értékelni és a jogalkotás szintjén hasznosítani. Ezen nemzetbiztonsági értelemben vett szakmai, valamint hagyományos értelemben vett történelmi és jogi ismeretek, valamint az ezekkel összefüggésben feltárt események, adatok, egymásra gyakorolt hatásuk feldolgozásából nyerhető eredményeket a jogszabályokban, a közjogi szervezetszabályozó eszközökben és ezek alapján a belső rendelkezésekben is hasznosítani szükséges.

A téma kiválasztására az alapján került sor, hogy a konkrét, cím szerint szűkített témakörben ilyen jellegű, átfogó értekezéssel, szakirodalmi kutatásaim során nem találkoztam, továbbá annak eredményeként, hogy végzettségem, téma iránti érdeklődésem és – jogi normák alkotásában részt vevő és szakmai ismereteket egyetemi és belső képzéseken oktató munkatársként – személyes érintettségem is van ezeken a szakterületeken.

A hibrid hadviseléssel összefüggő érdeklődésemet mások mellett Szun-ce A hadviselés törvényei című művében olvasottak keltették fel, különösen ez a gondolat: *„Minden hadviselésnek törvénye, hogy legjobb épségben hagyni az ellenséges országot, elpusztítani már nem olyan jó; ezért száz harcot vívni és százszor győzni nem a legjobb a jók között. Nem is harcolni, mégis alávetni az ellenséges sereget: ez a legjobb a jók között. Így aki igazán ért a hadviseléshez, úgy töri meg az idegen sereget, hogy nem vív csatát vele; úgy foglalja el az idegen városfalat, hogy nem ostromolja meg; úgy semmisíti meg az idegen fejedelemségeket, hogy nem tart sokáig a háború. S minthogy a kölcsönös sértetlenség által igyekszik győzni az égalattiban, a fegyverek alkalmazása nélkül is biztosítani tudja magának az előnyöket. Ez a csellel való támadás törvénye.”* [2]

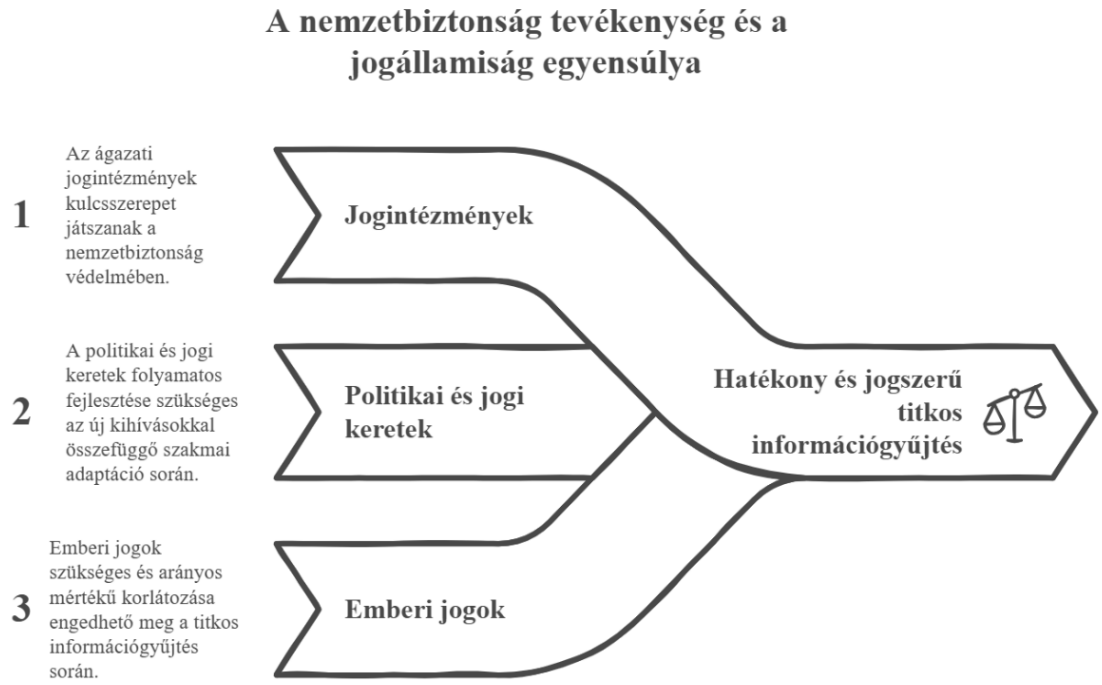
[2]SZUN-CE (1995): *A hadviselés törvényei (Szun-ce ping-fa)*. Fordította: Tőkei Ferenc. Balassi Kiadó, Budapest.

Véleményem szerint úgy megnyerni a konfliktust, legyőzni az ellenfelet, hogy ténylegesen elkerüljük a valószínűsíthetően saját veszteségekkel is járó csatát, a legnagyobb siker, amelyet katonaként magunkénak tudhatunk.

A téma egyediségét az adja, hogy a kutatás során a nemzetbiztonsági szolgálatok vonatkozásában a 21. század – jog-, illetve szakmatörténeti szempontból – releváns helyzeteinek, eseményeinek fókuszba állításával a fenti szempontrendszer szerinti vizsgálatot hajtottam végre. A kutatási téma interdiszciplinárisnak tekinthető mivel a jogtudomány, a rendészettudomány, a hadtudomány és más társadalomtudományok vizsgálódási területeit egyaránt érinti, amely miatt annak intézményi és elsődlegesen a jogalkotás eszközrendszerével értékelhető jogintézmények vizsgálatára történő szűkítése volt indokolt.

2. A probléma tudományos megfogalmazása

Fontosnak tartom, hogy vizsgáljam és elemezzem, hogy a titkos információgyűjtés és annak műveleti támogatásához kapcsolódó – különösen a hadtudományhoz tartozó katonai nemzetbiztonsági szakterületre jellemző – tevékenységi körben alkalmazott jogintézmények milyen módon képesek megfelelni az új típusú biztonsági kihívások jelentette veszélyek elhárításához, megelőzéséhez fűződő nemzetbiztonsági érdek kormányzat által megfogalmazott célkitűzéseinek? Különös tekintettel arra a körülményre, hogy a nemzetbiztonsági szolgálatokra jellemző jogintézmények és rendszerek vonatkozásában megállapítható, hogy a reaktivitás aránya még mindig túl magas a proaktivitáshoz képest. (Ne feledjük, a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény több, mint 65 db módosításon esett át kihirdetése óta).



1. ábra A nemzetbiztonsági tevékenység és a jogállamiság egyensúlya[3]

A nemzetbiztonság stratégiai szintű tevékenységének hatékony megvalósítása nem elsősorban az intézményi, jogi keretek vagy a szervezeti struktúra kialakításán keresztül, hanem a funkciókra összpontosító megközelítés és jogalkotás révén érhető el. Ez magában foglalja Magyarország nemzetbiztonsági érdekeinek védelmét és céljainak megvalósítását. A katonai nemzetbiztonsági tevékenység, beleértve a katonai felderítést, hírszerzést és elhárítást, fontos szerepet tölt be a katonai intézményrendszerben, és bár szorosan összefügg vele, a titkos információgyűjtés jellegéből adódóan mégis külön megközelítést és vizsgálatot igényel.

Előbbiekkel összefüggésben fontos megjegyezni, hogy a téma tudományos kutatását nehezíti, hogy a „*feladataik teljesítéséhez nélkülözhetetlen információkat a szolgálatok nyílt és titkos eszközök és módszerek alkalmazásával szerzik meg, a nyilvánosságtól elzártan dolgozzák fel és szintén a nyilvánosságtól elzártan adnak tájékoztatást az állami vezetők részére. Éppen ezekből adódóan, a nemzetbiztonsági tevékenység egyik alapeleme, hogy a teljes eljárás bizalmas, az avatatlan szemektől sokszorosan elzártan történik, ami az intézményi kultúrára is*

[3] A szerző saját gondolatainak vizualizációja során az ábra kizárólag grafikus elemeit a NAPKIN.AI használatával készítette el.

erős ráhatással van, és a nyilvánosság-titkosság egymással folyamatos konfliktusban áll. Különösen éles problémaként jelenik meg ez a nyugati típusú demokráciákban." [4]

A problémakör vizsgálata során előbbiek miatt elsődlegesen a deduktív kutatási stratégia és ennek eszközrendszere szükséges, hogy alkalmazásra kerüljön. Ennek a kutatási stratégiának elsődleges használata azért indokolt, mert a téma részben a nemzetbiztonsági szolgálatok minősített adatokat képező írott és íratlan, más módon nem elérhető tudásbázisán alapul. *„A nyugati típusú demokráciák egyik meghatározó értéke a nyitottság, ezen belül is az, hogy az állampolgároknak joguk van megismerni minden adatot, információt, amely egyéni sorsukat, és az általuk alkotott közösség helyzetét befolyásolja. A hírszerző és biztonsági szolgálatok tevékenysége ezzel szemben a titkosságra épül, hiszen alaprendeltetésük az, hogy a nemzet biztonsága érdekében elvégezzék azokat a feladatokat, amelyek megvalósítása nyílt eszközökkel nem lehetséges. A két értékrend ellentmondása szemmel látható, (…). Ez az elvi állapot azonban csak olyan kölcsönös bizalmon alapulhat, amely a gyakorlatban nem működőképes. Az állampolgár nem csak hinni, de tudni is szeretné, hogy a szolgálatok tevékenysége nem sérti érdekeit, miközben ez a bizonyosság a teljes nyilvánosság nélkül nem adható meg számára. (…) A titkosszolgálatok ez utóbbit nem tehetik meg, ami óhatatlanul bizalmatlanságot szül irányukban, (…). Egy demokratikus országban nem lehet kétséges, hogy a társadalom érdeke és elvárásai előbbre sorolnak, mint a titkosszolgálatok parciális érdekei, még ha azok a köz javát szolgálják is. Ebből kifolyólag a szolgálatoknak számolniuk kell azzal, hogy tevékenységüket egyre fokozódó társadalmi érdeklődés közepette kell folytatniuk, és esetenként a szakmailag indokoltnál mélyebb betekintést kell engedniük a külvilág számára."* [5]

A jogalkotásnak kiemelkedő szerepe van a nemzetbiztonság területén, Magyarországon az Alaptörvényben és kulcsfontosságú törvényekben kap helyet ezen szakterület szempontrendszere. A nemzetbiztonság tudományában a jogtudomány, a rendészettudomány és a hadtudomány egyaránt alapvető szerepet játszik, és az e területekről származó ismeretek elemzésével és értékelésével érhető el magabiztos tudás és kellő felkészültség a vizsgált témában. Ezeknek az eszközöknek az alkalmazása indokolt a rejtett összefüggések feltárásához a dokumentumelemzés során, amelyek a nemzetbiztonságot veszélyeztető törekvésekkel

[4] SZŰCS P. – SOLTI I. (2014): A magyar nemzetbiztonsági szféra és a nyilvánosság. *Nemzetbiztonsági Szemle*, II. évf. 2014/2. sz. pp. 72–92.
[5] HÉJJA István (szerk.): A külföldi hírszerző és biztonsági szolgálatok. Zrínyi Miklós Nemzetvédelmi Egyetem, Kossuth Lajos Hadtudományi Kar, Egyetemi Jegyzet, Budapest, 2007. p.192.

összefüggenek. A részletes ismeretek és adatok rendszerezésével, valamint az intézményrendszer (helyi, területi, központi, politikai szint) kooperatív munkájának eredményeként lehetségessé válik a közjogi transzformáció, amely elősegíti az intézményi változásokat. A jogtudományi alapok megerősítése és kiaknázása növelheti a kodifikációs folyamat hatékonyságát.

A probléma tudományos vizsgálata során indokoltnak látszik kiindulni abból a feltételezésből, hogy a nemzetbiztonság szempontjából az információs műveletek kétélű fegyverekként jelennek meg. Egyrészt használhatók az állami érdekek védelmére és a társadalom biztonságának növelésére, másrészt azonban az ellenfelek hasonló módszerei jelentős veszélyforrást is jelenthetnek.[6] A nemzetbiztonsági szolgálatoknak tudniuk kell felismerni és semlegesíteni az idegen eredetű információs hadviselést. Mindezek hatékony végrehajtása, vagyis a támadó, illetve védekező műveletek sikeres végzése érdekében alapos jogi és nemzetbiztonsági szakmai ismeretekre van szükség úgy, hogy az alkalmazott intézkedések összhangban legyenek a nemzetközi és hazai jogszabályokkal, valamint az etikai normákkal.

Szükséges részletesen elemezni a fenti területek kapcsolódási pontjait, például hogyan befolyásolják az információs műveletek a nemzetbiztonsági stratégiát, vagy hogy a rendészeti, illetve nemzetbiztonsági tevékenység miként hat vissza az információs hadviselésre. A jogi szabályozások elemzése mellett fontos a gyakorlati megvalósítás és esettanulmányok vizsgálata is, amelyek konkrét példákon keresztül mutatják be az elméleti összefüggések gyakorlati alkalmazását. Ezeknek az összefüggéseknek a feltárása jelenti a probléma tudományos megfogalmazásának egyik legfontosabb elemét.

A jogtudomány, a rendészettudomány, a nemzetbiztonsági szakismeretek és az információs műveletek közötti összefüggések kutatása során több szempontot is figyelembe vettem, hiszen ezek a területek szorosan összekapcsolódnak és kölcsönösen befolyásolják egymást. A jogi keretek meghatározzák az információs műveletek végrehajtásának jogosságát,

[6] DOBÁK Imre: Az információgyűjtés területeinek evolúciója, a kibertér jelentősége In: Dobák, Imre (szerk.) Nemzetbiztonság a 21. század elején Budapest, Magyarország: Ludovika Egyetemi Kiadó (2022) 200 p. pp. 103-120., 18 p.

illetve jogszerűségét[7] és mindezek jogi korlátait. Az alkotmányos, büntető és polgári jogi szabályozások mellett a nemzetközi jog és a különböző egyezmények is fontos szerepet játszanak abban, hogy milyen módszereket lehet alkalmazni az információs (és kiemelten a kiber) térben.

A nemzetbiztonsági szolgálatok, illetve a rendvédelmi szervek[8] tevékenységét is szabályozza a jog, ugyanakkor ők azok, akik az információs műveletek során gyűjtött adatokat felhasználva végezhetik el a bűnüldözést és a nemzetbiztonsági tevékenységeket. A rendvédelmi, illetve a nemzetbiztonsági szakembereknek ismerniük kell az információs műveletek hatásait és módszereit, hogy hatékonyan tudjanak fellépni az esetleges dezinformáció és propaganda ellen[9], a bűnüldözési spektrumban pedig a csalás (kiemelten a kibertérben elkövetett bűncselekmények) felderítése érdekében.

3. A releváns szakirodalom áttekintése

A dolgozat tudományos megalapozottságát jelentősen erősíti az a gazdag szakirodalom, amelyből az információs műveletek, a hibrid hadviselés és a jogi hadviselés kérdéskörét vizsgálja. E tématerületeken nemzetközi és hazai szerzők egyaránt meghatározó munkákat tettek közzé, amelyek keretet adnak az értekezés kutatási célkitűzéseihez és hipotéziseihez. Megjegyzendő ugyanakkor, hogy kifejezetten a jogi hadviselés tárgykörére vonatkozóan a kutatás kezdeti éveiben számottevő hazai szakirodalom még nem állt rendelkezésre; a téma vizsgálata ezért elsősorban amerikai, orosz és kínai forrásmunkákra támaszkodott. Az elmúlt évek kedvező fejleménye, hogy katonai jogi, védelmi-igazgatási, nemzetközi közjogi,

---

[7] A „jogos" és „jogszerű" kifejezések gyakran használatosak a jogi nyelvben, és bár hasonló jelentéssel bírnak, fontos megkülönböztetni közöttük. A „jogos" kifejezés általában valaminek az erkölcsi vagy törvényen kívüli igazolhatóságára utal. Egy cselekedet, követelés vagy állítás jogos, ha van alapja, indoka vagy oka, és erkölcsileg megalapozott vagy ésszerű. Például egy személy jogosan érezhet sérelmet, ha megsértették az emberi méltóságát, vagy jogosan követelhet kártérítést, ha jogtalanul okoztak neki kárt. A „jogszerű" szó a jog által engedélyezett vagy előírt cselekvésekre vonatkozik. Jogszerű az a tevékenység, amely összhangban van a hatályos jogszabályokkal és jogrendszerrel. Például egy bírósági ítélet végrehajtása jogszerű, ha az a törvényes eljárásoknak megfelelően történik. Egy cselekedet tehát lehet jogos, ha erkölcsileg indokolt vagy alátámasztott, de nem feltétlenül jogszerű, ha nem felel meg a jogi előírásoknak. Fordítva is igaz: egy cselekedet lehet jogszerű (mert az írott jognak megfelel), de nem feltétlenül jogos az erkölcsi értelemben (például, ha a törvények igazságtalanok vagy elavultak).

[8] Hoffman István: A rendvédelmi szervek In: Fazekas, Marianna (szerk.) Közigazgatási jog. Általános rész I. : A közigazgatásról általában. Közigazgatási szervezeti jog. Közszolgálati jog Budapest, Magyarország: ELTE Eötvös Kiadó (2020) pp. 222-228., 7 p.

[9] DOBÁK I. (2022): A dezinformáció – napjaink kiemelt kihívása. *Katonai Jogi és Hadijogi Szemle*, 2022/1. sz. 93–124. Elérhető: https://epa.oszk.hu/02500/02511/00020/pdf/EPA02511_katonai_jogi_szemle_2022_1_093-124.pdf (Letöltés ideje: 2026.04.01.)

biztonságpolitikai és nemzetbiztonsági szempontból is feldolgozásra kerültek a kutatás egyes résztárgykörei hazai szerzők tollából, és a Nemzeti Közszolgálati Egyetem kutatói, a nemzetbiztonsági szolgálatok, valamint a tudományos kutatóhelyek és műhelyek a lawfare tárgykörét prioritásként kezelve aktívan támogatták a vonatkozó kutatói tevékenységet.

A normatív-doktrinális keretrendszer tekintetében meghatározó kiindulópontot jelent a NATO *Allied Joint Doctrine for Information Operations* (AJP-10.1) Edition A, Version 1 (2023) kiadású dokumentuma,[10] amely a szövetség információs műveleteinek legfrissebb doktrinális alapdokumentuma. A disszertáció az AJP-10.1-et referenciapontként alkalmazza a hibrid hadviselésben megjelenő információs eszközök osztályozásához és a lawfare-rel való kapcsolódási pontok azonosításához.

A jogi hadviselés fogalmának tudományos megalapozásában kiemelkedő szerepet játszik Charles J. Dunlap tábornok munkássága, aki a lawfare fogalmát már 2001-ben azonosítja,[11] majd 2015-ben adja meg annak legtöbbet hivatkozott definícióját.[12] A disszertáció kilenc különböző Dunlap-publikációra épít, amelyek a lawfare legitim és illegitim formáinak elhatárolásához, a humanitárius jogi aspektusokhoz és a kiberhadviselési dimenziókhoz egyaránt nélkülözhetetlen fogalmi keretet biztosítanak. Dunlap munkásságát szervesen egészíti ki Oded F. Kittrie monográfiája,[13] amely a lawfare-irodalom legelismertebb összefoglaló műveként rendszerezi az offenzív és defenzív jogi hadviselés eszköztárát, és konkrét példákon – Kína, Irán, Izrael-Gáza, Oroszország – mutatja be a jog stratégiai instrumentalizálását. A disszertáció kulcsfogalomként hivatkozik erre a monográfiára a hibrid hadviselési eszköztár jogi dimenziójának megalapozásakor. A témakör angolszász irodalmának harmadik meghatározó pillére David Kennedy[14] munkája, amely a jogi hadviselést és a hadviselést a Cambridge-féle nemzetközi jogi összefüggésrendszerbe helyezi, és a stratégiai jogi manőverezés politikai-katonai dimenzióit elemzi.

---

[10]NATO: Allied Joint Doctrine for Information Operations. AJP-10.1. Edition A, Version 1. Brussels: NATO Standardization Office, 2023. Elérhető: https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101 (Letöltés: 2026. 02. 11.)

[11]DUNLAP, Charles J. Jr.: Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts. [Konferencia-előadás.] Humanitarian Challenges in Military Intervention Conference, Harvard University, 2001. november 29. Elérhető: https://people.duke.edu/~pfeaver/dunlap.pdf (Letöltve: 2019. október 31.)

[12]DUNLAP, Charles J. Jr.: Lawfare. In: Moore, J. N. et al. (Eds.): National Security Law. Carolina Academic Press, 3. kiad., 2015, 823–838. o. Elérhető: https://scholarship.law.duke.edu/faculty_scholarship/3408/ (Letöltve: 2019. október 31.)

[13]KITTRIE, O. F.: Lawfare. Law as a Weapon of War. Oxford University Press, New York, 2016.

[14] KENNEDY, D. (2012): Lawfare and Warfare. In: CRAWFORD, James – KOSKENNIEMI, Martti (ed.): The Cambridge Companion to International Law. Cambridge: Cambridge University Press, pp 158–183.

A hazai hadtudományi irodalomban Porkoláb Imre munkássága emelendő ki elsőként, aki a gerilla hadikultúra és az ortodox hadikultúra összehasonlító vizsgálatával gazdagította a hibrid hadviselésről szóló diskurzust.[15] Porkoláb elemzései egyfelől a hibrid hadviselés fogalmának történeti gyökereire mutatnak rá, másfelől a kognitív dimenzió – az emberi elme, mint műveleti terület – önálló vizsgálatát helyezik előtérbe. Forgács Balázs Jomini értelmezésén keresztül a klasszikus hadtudomány modern újraértelmezését nyújtja: elemzései a gerilla és partizánhadviselés elméleti hagyományát kötik össze a hibrid műveletek kortárs fogalomrendszerével, így szerves összekötő szerepet töltenek be az aszimmetrikus hadviselés történeti és jelenkori megközelítései között. [16]

A Nemzeti Közszolgálati Egyetem kutatói a védelmi-igazgatási, katonai jogi és nemzetbiztonsági aspektusok feldolgozásában nyújtottak számottevő hozzájárulást. Farkas Ádám[17] a különleges jogrend és a kibertér jogi szabályozásának meghatározó hazai kutatója, akinek munkái a hibrid konfliktusok jogi kezelhetőségének kérdéskörét a legmagasabb elméleti igénnyel tárgyalják. Haig Zsolt[18] az információs műveletek és a kiberhadviselés hazai kutatójaként az értekezés információs hadviselési fejezetéhez nélkülözhetetlen fogalmi és rendszertani alapokat nyújtja. Resperger István[19] a hibrid hadviselés és a válságkezelés összefüggéseit elemzi átfogó monográfiájában, amely a hazai hadtudományi irodalomban egyedülálló rendszerező igénnyel tárgyalja a hibrid fenyegetések kezelésének gyakorlati és elméleti dimenzióit. Tomolya János[20] az ún. Geraszimov-doktrína hazai kritikai elemzőjeként járul hozzá a kutatáshoz: tanulmánya az orosz hibrid hadviselés ideológiai és doktrinális alapjait árnyalt forráskritikai perspektívából vizsgálja. Szenes Zoltán[21] a hibrid fenyegetések elleni

[15]PORKOLÁB Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? Hadtudomány, 25. évf. 2015/3–4. sz., 36–48. o., PORKOLÁB Imre: A hadviselés adaptációja: harc az emberi elméért. Hadtudományi Szemle, 7. évf. 2014/3. sz., 57–69. o.

[16]FORGÁCS Balázs: A néppel az uralkodóért. Az első gerillaelméletek. Felfederítő Szemle, 2016/1. sz., 21–57. o., FORGÁCS Balázs: Antoine Henri Jomini és a nemzeti háború. In: Koller B. – Marsai V. (szerk.): Magyarország Európában, Európa a világban. Budapest: Dialog Campus Kiadó, 2016, 35–43. o. ISBN 978-615-5680-08-3.

[17]FARKAS Ádám – RESPERGER István: Az úgynevezett hibrid hadviselés kihívásainak kezelése és a nemzetközi jog mai korlátai. In: Farkas Á. – Végh K. (szerk.): Új típusú hadviselés. Budapest: Zrínyi Kiadó, 2020, 132–149. o., FARKAS Ádám: Komplex biztonság, hibrid konfliktusok, összetett válaszok. Honvédségi Szemle, 2020/4. sz., 11–23. o.

[18]HAIG Zsolt: Információs műveletek a kibértérben. Budapest: Dialóg Campus Kiadó, 2018., HAIG Zsolt: Az információs hadviselés kialakulása, katonai értelmezése. Hadtudomány, 2011/1–2. sz., 12–28. o.

[19]RESPERGER István: A válságkezelés és a hibrid hadviselés. Budapest: Dialóg Campus Kiadó, 2018. ISBN 978-615-587-753-7.

[20]TOMOLYA János: Az úgynevezett „Geraszimov-cikk” margójára. Hadtudomány, 2018/3–4. sz., 79–99. o. DOI: 10.17047/HADTUD.2018.28.3-4.79

[21]SZENES Zoltán: A hibrid fenyegetések elleni szakpolitika Magyarországon. Hadtudomány, 31. évf. 2021/4. sz., 39–56. o.

szakpolitika magyarországi keretrendszerét tárja fel, és elemzései közvetlen relevanciával bírnak a disszertáció stratégiai normaalkotást vizsgáló fejezeteiben.

A dezinformációs narratívák és a stratégiai kommunikáció témakörét a hazai irodalomban Dobák Imre[22] több publikációján keresztül, Torda Péter[23] a NATO StratCom-kereten belüli dezinformáció-elemzéssel, Rózsa Tibor[24] az információs műveletek tendenciáinak áttekintésével járul hozzá a disszertáció e fejezetéhez. Az esettanulmányi részben az orosz állami propagandaforrások – így a Sputnik, az Orosz Hírek és a Tsargrad – azonosított narratívái szemléltetik a kognitív befolyásolás valós mechanizmusait; ezek a hivatkozások nem tudományos autoritások, hanem a dezinformációs tevékenység dokumentálásának empirikus forrásai.

A kognitív hadviselés témaköréhez a disszertáció három friss, 2025–2026-ban megjelent NATO- és NDU-forrást épít be. Blatny és Søndergaard NATO STO-kutatási jelentése[25] a kognitív hadviselés biológiai és neuropszichológiai alapjait tárja fel, és a szövetség tudományos főtanácsadójának szintjén rögzíti a fenyegetéskép legfrissebb értékelését. Giordano NDU Strategic Insights elemzése[26] a NATO főtudósi jelzésként értelmezi és operatív felkészültségi keretbe helyezi az előbbi jelentés megállapításait. A NATO ACT kognitív hadviselési keretrendszere[27] az elméleti alapokból kiindulva a szövetség adaptív képességfejlesztési programjait mutatja be. E három forrás együttesen megalapozza azt az értekezésben képviselt álláspontot, amely szerint a kognitív dimenzió önálló műveleti térként értelmezendő. Ezzel összhangban Aidman és munkatársai mesterségesintelligencia-alapú

[22]DOBÁK Imre: A dezinformáció – napjaink kiemelt kihívása. Katonai Jogi és Hadijogi Szemle, 2022/1. sz., 93–124. o.
[23]TORDA Péter: A dezinformáció elleni fellépés a NATO stratégiai kommunikációjában. Nemzetbiztonsági Szemle, 13. évf. 2025/1. sz., 3–14. o.
[24]RÓZSA Tibor: Az információs műveletek elmélete, gyakorlata és tendenciái. Honvédségi Szemle, 147. évf. 2019/5. sz., 73–87. o. Elérhető: https://real-j.mtak.hu/13949/17/Honvedsegi_Szemle_2019_5_teljes_szam.pdf (Letöltés: 2026. 03. 12.)
[25]BLATNY, Janet M. – SØNDERGAARD, Steen: Cognitive Warfare. NATO Chief Scientist Research Report, STO-OCS-001. Brussels: NATO STO, 2025. Elérhető: https://www.sto.nato.int/document/cognitive-warfare/ (Letöltés: 2026. 02. 11.)
[26]GIORDANO, James: Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness. Strategic Insights, National Defense University. Elérhető: https://inss.ndu.edu/Media/News/Article/4371195/ (Letöltés: 2026. 02. 11.)
[27]NATO ACT: Cognitive Warfare: Strengthening and Defending the Mind. Elérhető: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/ (Letöltve: 2023. október 11.)

ellenintézkedéseket vizsgáló tanulmánya is, amely a technológiai válaszlehetőségek irányát jelöli ki. [28]

A fentebb bemutatott szerzők közös munkássága egyértelművé teszi, hogy az információs műveletek és a hibrid hadviselés összefüggései kizárólag komplex, interdiszciplináris megközelítéssel ragadhatók meg. A hivatkozott szakirodalmi bázis ezért nem pusztán elméleti támaszt nyújt, hanem közvetlenül megalapozza a disszertációban levont tudományos megállapításokat és hipotézis-tesztelési eljárásokat. A hazai és a nemzetközi irodalom szintézise lehetővé teszi, hogy az értekezés eredményei egyszerre illeszkedjenek a NATO normatív-doktrinális keretrendszerébe és a magyar hadtudományi hagyomány fogalmi rendjébe.

4. A kutatás célkitűzései

A kutatásom egyik kiemelt célja a témájába illeszkedő, eddig nem, vagy részben hasznosított tapasztalatok, ismeretek tudományosan megalapozott feldolgozása és ezeknek egy olyan objektív megközelítésű, keretbe foglalt megjelenítése, amely egyaránt alkalmas a megoldási javaslatok kiindulópontjaként funkcionálni és a szolgálatok belső, továbbá a felsőoktatásban, illetve államigazgatásban biztonságtudatosság témakörében végzett oktatási tevékenysége során történő hasznosítására is. [29]

A kutatásom másik kiemelt célja annak feltárása, hogy miként kapcsolódnak össze az információs műveletek, a hibrid hadviselés, a jogalkotás és a jogi hadviselés területei. Az információs műveletek és a hibrid hadviselés modern kihívásai új megközelítéseket igényelnek a jogalkotás és a jogi keretek tekintetében. A kutatás során arra törekedtem, hogy bemutassam, miként befolyásolják ezek a tényezők egymást, és hogyan alakítják a nemzetbiztonsági stratégiákat és gyakorlatokat. Vagyis egy átfogó kép kialakítása arról, hogy az információs műveletek és a hibrid hadviselés miként befolyásolja és alakítja át a jogalkotást és a jogi gyakorlatot, és miként lehet ezeket a változásokat integrálni, illetve implementálni a nemzetbiztonsági stratégiákba és szabályozásokba. Elengedhetetlenül fontos feladatnak tartom,

[28]AIDMAN, E. – ROWA, J. – VINCE, J. – van DIGGELEN, J. (2025): Designing AI-Enabled Countermeasures to Cognitive Warfare. STO-MP-HFM-377. NATO Science and Technology Organization. DOI: 10.14339/MP-HFM-377-06-PDF.
[29] DOBÁK Imre, BABOS Sándor: A biztonságtudatosítás lehetőségei a 21. századi platformok fényében In.: NEMZETBIZTONSÁGI SZEMLE (ONLINE) 9: 4 pp. 18-34., 17 p. (2021)

hogy feltárjam azokat a módszereket és stratégiákat, amelyekkel az államok reagálhatnak ezekre a kihívásokra, és hogyan fejleszthetik jogszabályi kereteiket annak érdekében, hogy megvédjék magukat az információs hadviselés és a jogi hadviselés negatív hatásaival szemben. Ezen célok elérése érdekében különös figyelmet fordítok arra, feltárjam az összefüggéseket és meghatározzam azokat a kulcstényezőket, amelyek szerepet játszanak ebben a folyamatban, továbbá, hogy vizsgáljam és elemezzem, hogy milyen szerepet játszanak a nemzetközi szervezetek és a nemzetközi szerződéseken alapuló együttműködés, mint az Európai Unió vagy a NATO, valamint hogy miként befolyásolják ezek adaptív képességeit, proaktivitását az új technológiák és a globális információs tér gyors változásai.

Jelen disszertáció a lawfare jelenségét kifejezetten a hibrid hadviselés kontextusában vizsgálja. A kutatás tudatosan szűkíti le a lawfare értelmezését a hibrid hadviselés egyik sajátos eszközére, miközben elismeri, hogy a jog eszközként való használata a konvencionális hadviselés történeti formáiban is jelen volt. Ennek illusztrálására a magyar történelemből is hozható példa: az 1848/49-es forradalom és szabadságharc során az 1848. évi III. törvénycikk rendelkezései a honvédelmi irányítás jogszerűségét igazolták, és hozzájárultak a magyar kormányzat legitimációjához. Ez a történeti előzmény rávilágít arra, hogy a jog, mint hadviselési eszköz, a modern jogállamok kialakulásától kezdve jelentős szerepet töltött be a fegyveres konfliktusokban.

A vizsgálódás kiindulópontját, valamint jelentős mérföldköveit az alábbiak szerint határoztam meg:

- információs műveletek alapvető jellemzőinek és hatásainak elemzése, különös tekintettel arra, hogy ezek milyen módon képesek befolyásolni a társadalmi és politikai döntéseket, valamint a közvéleményt;
- a hibrid hadviselés fogalmának tisztázása mellett azoknak a különleges technikáknak és módszereknek a vizsgálata, amelyeket a hibrid konfliktusokban alkalmaznak, beleértve az információs műveleteket és tevékenységeket, valamint a jogi hadviselést;
- mindezek közötti összefüggések feltárása, igazolva a megjelenített kulcstényezők kiemelt jelentőségét;
- a kiberműveletek meghatározó szerepének elemzése és értékelése az információs műveleteknek, a hibrid hadviselés egyes eszközei alkalmazási jellemzőinek, a jogi hadviselésre gyakorolt hatása szempontjából, valamint mindezek kölcsönhatásainak vizsgálata a stratégiai jogi normák keretrendszerében;

- Magyarország vonatkozásában releváns nemzetközi szervezetek adaptív képességeinek fejlődése, valamint rezilienciájuk növelése érdekében tett erőfeszítéseik elemzése, ezekből levonható tanulságok rendszerezése;
- a tapasztalatok, igazolható kutatási eredmények szintetizálása és az ezeken alapuló javaslatok megfogalmazása.

A jogalkotás szerepe ebben a kontextusban kulcsfontosságú, hiszen a nemzetbiztonsági kihívásokra adott válaszokat elsődlegesen jogi keretek között kell meghatározni. A kutatás során arra is rá kívánok világítani, hogy milyen jogi eszközök állnak rendelkezésre a hibrid fenyegetések kezelésére, és milyen jogi reformokra lehet szükség a hatékony védekezés érdekében.

A jogi hadviselés aspektusából megvizsgálom, hogy a nemzetközi jog és a nemzetközi humanitárius jog hogyan alkalmazkodik vagy kellene alkalmazkodnia a hibrid hadviselés egyes intézkedéseinek megjelenéséhez. Elemzem továbbá azt is, hogy a különböző államok, valamint a szövetségi rendszerek hogyan használják ki a jogi rendszereket stratégiai előnyök elérésére, illetve milyen jogi kihívásokkal kell szembenézniük az információs térben folytatott műveletek során.

A kutatásom további célja, hogy a jogalkalmazói és a jogalkotói szakmai közösség számára támpontokat biztosítson a téma legjelentősebb jogintézményeinek rendszerében és igyekszik egy új rendszerszemléletet bevezetni a leginkább rendészeti megközelítésű tudományterületen a hadtudomány által kimunkált eredmények nyomán alkalmazni és ezek eredményeként újítást megvalósítani. A kutatás fentiek alapján alkalmazott kutatásnak minősíthető. A szabályozási terület tudományos megközelítésű és a kiemelten a hadtudomány rendszerszemléletének megfelelő rendszerezése. Új megoldások felismerése és gyakorlati hasznosításuk lehetőségének megteremtése, a szakmai és a téma szerinti tudásbázison alapuló képzések színvonalának további emelkedése. A jogalkotás ezen sajátos szegmensében a statika dominál a dinamikával szemben, azonban bizonyítani igyekszem, hogy mégis érvényesíthető az innováció a szakmai és a tudományos élet meghatározó szereplőinek proaktív együttműködése eredményeként, kiemelten a hibrid hadviselés elleni küzdelem során.

Előbbiekben meghatározott kutatási célok összegzését az alábbi pontokba szedve végeztem el:

C1: A stratégiai szintű nemzetbiztonsági jogalkotás elemzése, a funkcionális és az intézményi-szervezeti megközelítés összehasonlítása, különös tekintettel arra, hogy melyik modell alkalmas inkább a tényleges közpolitikai célok elérésére Magyarország vonatkozásában.

C2: A katonai nemzetbiztonsági tevékenység jogintézményi rendszerének összehasonlító elemzése a 2012–2023 közötti időszakban, különösen a rendészeti tevékenységtől való jogi elhatárolás szempontjából.

C3: A hírszerzési és elhárítási tapasztalatok közjogi struktúrákon keresztüli integrálhatóságának vizsgálata, kiemelten arra fókuszálva, hogyan épülhetnek be ezek az ismeretek a lawfare eszköztárán keresztül a hibrid fenyegetésekkel szembeni védelembe.

C4: Az információs műveletek — különösen a kibertéren keresztül végzett pszichológiai műveletek és dezinformációs kampányok — döntéshozókra és jogi normaalkotókra gyakorolt hatásának elemzése, esettanulmányok és összehasonlító módszer alkalmazásával.

C5: A NATO és EU keretrendszerei által biztosított szövetséges tapasztalatmegosztás hatékonyságának és korlátainak vizsgálata a hibrid fenyegetésekkel szembeni rezilienciaépítés szempontjából, különösen a tagállamok közötti együttműködési feszültségek árnyékában.

Céljaim mentén az alábbi hipotéziseket állítottam fel:

5. Kutatási hipotézisek

H1. A nemzetbiztonsági tevékenység stratégiai szintjén nem az intézményi jogi, vagyis szervezetalkotás oldaláról történő, hanem elsődlegesen a funkcionalitást alapul vevő megközelítéssel és jogalkotással érhető el a kívánt közpolitikai célkitűzés, Magyarország nemzetbiztonsági érdekeinek védelme és céljainak érvényesítése.

H2. A katonai nemzetbiztonsági tevékenység és annak jogintézményi rendszere kiemelt helyet foglal el a katonai jogintézmények rendszerében, attól nem elválasztható, ugyanakkor a speciális működési terület miatt a feladatrendszer mégis külön kezelendő, jól elhatárolható a rendészeti tevékenységtől, és ez a 2012 és 2023 közötti időszakban látványosan meg is nyilvánult.

H3. A nemzetbiztonsági szolgálatok által felderített információk és megszerzett tapasztalatok közvetve, illetve közvetlenül hasznosításra kerülhetnek a megfelelő közjogi struktúrán keresztül és a lawfare útján a hibrid hadviselés elleni küzdelem, illetve az egyes, ebbe a körbe tartozó intézkedés azonosítása, illetve alkalmazása során levont következtetések eredményeként.

H4. A hibrid hadviselés eszközrendszerébe illeszkedő, az információs műveletek közé tartozó egyes intézkedések, illetve intézkedéssorozatok jelentős hatást fejtenek ki, a célzott állam, illetve közösség döntéshozóira, illetve jogi normaalkotóira. A célzott hatás kifejtése érdekében információs műveletek precíz alkalmazása kerül végrehajtásra kiemelten a közvélemény befolyásolása útján, különösen a kibertérben továbbított közlések által.

H5. A hibrid hadviselés eszközrendszerébe illeszkedő, az információs műveletek közé tartozó, egyes intézkedésekkel, illetve intézkedéssorozatokkal összefüggésben keletkezett tapasztalatok, ismeretek szövetségesi rendszeren belüli hasznosítása elengedhetetlenül szükséges a nemzeti és a szövetségi szintű reziliencia növelése érdekében, abban az esetben is, ha a szövetségen belüli konfliktusok árnyékolják be az együttműködést a tagállamok között.

6. A témakör tudományterületi elhelyezése

Az információs műveletekkel összefüggő és a hibrid hadviselésre vonatkozó kutatások elhelyezése a hadtudományban egy multidiszciplináris megközelítést igényel, amely magában foglalja a katonai stratégia, a nemzetbiztonság, a politikatudomány, a jogtudomány, a pszichológia és az informatika területeit is. A hibrid hadviselés fogalma összetett konfliktusokra utal, amelyek a hagyományos katonai erők mellett nem hagyományos eszközöket is felhasználnak, mint például a kibertámadások, az információs hadviselés, az aszimmetrikus hadviselés módszertanába tartozó eszközök és a terrorcselekmények.

A kutatási témám hadtudományi kontextusban történő elhelyezése során az alábbi szempontoknak tulajdonítottam kiemelkedő jelentőséget:

- Elméleti keretek fejlesztése: A hibrid hadviselés definíciójának, jellemzőinek és dinamikájának meghatározása, valamint az ezekre adott válaszok kidolgozása, kiemelten a normaalkotás terén.
- Történeti és esettanulmányok: A múltbeli és jelenlegi hibrid konfliktusok elemzése segít jobban megérteni a hibrid hadviselés, illetve az információs műveletek működését és hatásmechanizmusát. Ezekre hazánkat is elérő dezinformációk tanulmányozásával világítottam rá.
- Doktrína és stratégia vizsgálata: A hibrid fenyegetésekkel szembeni hatékony válaszok kidolgozása, beleértve a védelmi és támadó stratégiákat, kiemelten a szövetségi rendszereinkben alkalmazott megoldások figyelembevételével.
- Technológiai kutatás: Az új technológiák, mint például a mesterséges intelligencia, a nagy adatmennyiség elemzése (big data), és a kiberbiztonság fejlesztése, amelyek kulcsfontosságúak a hibrid hadviselés és az információs műveletek jelentette veszély megértésében és kezelésében.
- Szimulációk és gyakorlatok: Valósághű forgatókönyvek kidolgozása és gyakorlati szimulációk végrehajtása elengedhetetlenek, hogy felkészítsék a katonai vezetőket és döntéshozókat a kutatásom során vizsgált fenyegetések kezelésére.
- Oktatás és képzés: A hibrid hadviselésre vonatkozó ismeretek integrálása a katonai oktatásba és képzésbe, hogy a jövőbeli vezetők felkészüljenek az ilyen típusú konfliktusokra és az összkormányzati reziliencia ennek eredményeként erősödjön.
- Nemzetközi együttműködés: A hibrid hadviselés jelenségének globális természete miatt fontos az együttműködés más országokkal és nemzetközi szervezetekkel, hogy megosszák a legjobb gyakorlatokat és koordinálják a közös fellépést. Különös tekintettel a szövetségi rendszereink illetékes szervezeteinek megállapításait emeltem ki a kutatásom során, ezeknek a tapasztalatoknak a hasznosítása rendkívül fontos.

A kutatási téma jogtudományi elhelyezése során megállapítottam, hogy:

- A kutatásom fókuszában álló hibrid intézkedéssorozat eszköztárába tartozó jogi hadviselés, vagy más néven „lawfare”, egy olyan kifejezés, amely a jogi eszközök és rendszerek hadviselésben való felhasználására utal, egy különösen konfliktusok megoldására vagy politikai és stratégiai célok elérésére irányuló eszköz. A jogi hadviselés tehát azon módszerek összességét jelenti, amelyek a jogot használják fel, mint eszközt a nemzetközi vagy belföldi politikai és katonai konfliktusokban. A jogi hadviselés fogalma

az utóbbi évtizedekben vált egyre fontosabbá a nemzetközi kapcsolatokban és a konfliktuskezelés területén. A jog eszközként való használata nem új keletű, hiszen már a nemzetközi jog kialakulása óta meghatározó szerepet játszik az államok közötti viszonyokban. Ugyanakkor a globalizáció és a nemzetközi intézmények fejlődése új dimenziókat nyitott a jogi hadviselés terén.

- A jogtudomány egy olyan diszciplína, amely a jogszabályokat, azok alkalmazását és értelmezését, valamint a jogrendszer működését vizsgálja. A jogi hadviselés ezen belül elsősorban a nemzetközi jog és az emberi jogok területéhez kapcsolódik.
- A nemzetközi jog keretében a jogi hadviselés az államok közötti viszonyokban jelentkezik, mint például a nemzetközi bíróságokon való államok közötti viták vagy szankciók és embargók jogi megalapozása. Az emberi jogok területén pedig gyakran használják fel a kormányok elleni bírálatokra, különösen az emberi jogi visszaélések esetén.
- A gyakorlatban a jogi hadviselés többféle formát ölthet. Például egy állam perbe foghat egy másik államot nemzetközi bíróságokon, mint például az Egyesült Nemzetek Nemzetközi Bíróságán (ICJ) vagy az Egyesült Nemzetek Tengerjogi Bíróságán (ITLOS), hogy politikai nyomást gyakoroljon vagy területi vitákban érvényesítse az igényeit. Emellett államok vagy nemzetközi szervezetek szankciókat vezethetnek be egy másik ország ellen, amelyeket szintén jogi eszközökkel kell megalapozni.
- Bár a jogi hadviselés hasznos eszköz lehet a békés konfliktuskezelésre és az igazságosság előmozdítására, kutatásom során megállapítottam, hogy számos kritika is éri. Ezeket a vizsgálatokat áttanulmányoztam, és részletesen megjelenítettem azokat a megállapításokat, melyek szerint a jogot politikai célokra használják fel, ami alááshatja a jogalkotás és a jogalkalmazás objektivitását és függetlenségét, illetve rezilienciáját.[30]

[30] A reziliencia, vagy más néven ellenálló képesség, egy személy vagy szervezet azon képességére utal, hogy képes legyen megbirkózni a váratlan kihívásokkal, stresszhelyzetekkel, és sikeresen visszaálljon a negatív események hatásai után. A reziliencia egy átfogó fogalom, amelyet számos tudományágban és gyakorlati területen használnak fel a kihívásokkal való megbirkózás és a helyreállítás képességének javítása érdekében. A fogalom eredetileg a pszichológiából származik, ahol az egyéni szintű alkalmazkodóképességet és a nehézségek leküzdésének képességét jelenti, de ma már széles körben használják más területeken is, többek között a társadalomtudományokban, a vállalati menedzsmentben, az ökológiában és a katasztrófák kezelésében. A reziliencia kutatása többféle szempontból is releváns lehet: 1. Pszichológiai reziliencia: Az egyének mentális egészségének és jól-létének megőrzése érdekében végzett kutatások, amelyek az alkalmazkodóképesség, a stresszkezelés és a pozitív pszichológiai tulajdonságok fejlesztésére összpontosítanak. 2. Szervezeti reziliencia: Vállalatok és szervezetek képességét vizsgálja, hogy hogyan tudnak alkalmazkodni a változó piaci körülményekhez, hogyan kezelik a belső és külső sokkokat, és hogyan építenek fel olyan rendszereket, amelyek segítségével gyorsan reagálhatnak a válságokra. 3.Társadalmi és közösségi reziliencia: A közösségek és társadalmak adaptációs képességét elemzi, különös tekintettel a természeti katasztrófákra és más nagy léptékű krízisekre való reagálásra. 4. Infrastruktúrák és rendszerek rezilienciája: Kritikus infrastruktúrák, mint az

Kutatásom során előbbivel összefüggésben vizsgáltam olyan későbbiekben részletezett állításokat is, melyek szerint, a gazdag és befolyásos országok képesek manipulálni a nemzetközi jogrendszert saját érdekeik szerint, ami az állítások szerint igazságtalanságot eredményezhet.

- A jogi hadviselés vizsgálatának a jogtudományi kontextusba helyezése azt a megközelítést helyezi a középpontba, hogy miként lehet a jogot stratégiai eszközként a nemzetközi és belföldi politikai színtéren felhasználni. Ez a sajátos eszközhasználat új lehetőségeket nyit meg a konfliktuskezelésben, de etikai és jogfilozófiai kérdéseket is felvet. A jogtudomány ezen területének további kutatása elengedhetetlen annak érdekében, hogy megértsük ennek a gyakorlatnak a hatásait és korlátait a modern világban.

7. Alkalmazott kutatási módszerek

A részben a hadtudomány, a jogtudomány és a nemzetbiztonsági tevékenység területére vonatkozó elemeket tartalmazó kutatási témámmal összefüggésben megállapítottam, hogy a dogmatikai és összehasonlító módszer alkalmazása a célravezető. Ugyanis leginkább ilyen kutatási módszereket érdemes alkalmazni egy titkos információgyűjtést szolgáló eszköz jogi szabályozásának feltérképezésére vagy a nemzetbiztonsági tevékenység normakörnyezetének összehasonlítása céljából.

A kutatás során az alábbi módszertani megközelítést alkalmaztam:

- (Jog)szociológiai kutatás során a jogintézményeket és folyamatokat társadalmi kontextusban vizsgáltam. A jogszociológiai kutatás segített megvizsgálni a jogrendszer hatásait és következményeit a nemzetbiztonságra, valamint az emberek viselkedésére és véleményére.
- Történeti elemzés során a jogfejlődést és a folyamatos változásokat vizsgáltam. A (jog)történeti kutatás segítségével megérthetjük, hogyan alakultak ki a nemzetbiztonsági jogi rendelkezések és intézmények, valamint hogyan változtak ezek a vizsgált időszakban. A múltbeli konfliktusok és katonai, illetve nemzetbiztonsági műveletek

energiaellátás, a közlekedés és az információs technológiák ellenálló képességének vizsgálata, hogy képesek legyenek fenntartani működésüket válsághelyzetekben.

részletes vizsgálata, amely segít megérteni a stratégiai döntések hatásait és a katonai, illetve nemzetbiztonsági doktrínák fejlődését.

- Szimulációk és hadijátékok vizsgálata során valós vagy fiktív forgatókönyvek alapján végrehajtott szimulációk segítségével tesztelhetik a kutatók a különböző stratégiák és döntések következményeit. Elsődlegesen amerikai, orosz és kínai katonai szakértők által (polgárháború, katonai puccs, digitális összeomlás modellezésével) készített írásműveit használtam fel, a hazai publikációk tanulmányozása mellett.
- Jogfilozófiai kutatás módszereivel a jogi alapelvek, értékek és normák vizsgálatát végeztem el. A jogfilozófiai kutatás segítségével mélyebb megértést nyerhetünk arról, hogy miért és hogyan alakultak ki bizonyos jogi elvek a nemzetbiztonság területén, valamint ezek az elvek miként segíthetik a jogalkotást ezen a speciális területen.
- Összehasonlító elemzés módszerével különböző helyzetek vagy időszakok összehasonlítását végeztem el annak érdekében, hogy általános mintákat, tendenciákat és tanulságokat azonosítsak, továbbá következtetéseket legyek képes levonni. Konkrét események, műveletek vagy döntések részletes elemzése eredményeként, átfogó képet kaptam egy-egy jelenségről, illetve folyamatról.
- Különös jelentőséget tulajdonítok értekezésemben az esettanulmányok megjelenítésének, ugyanis a jogilag releváns esetek részletes elemzése segíthet megismerni a jogi elvek alkalmazásának, illetve azok megsértésének hatásait a társadalomra, illetve a nemzet biztonságára.
- Kvalitatív elemzéssel, különösen interjúk, szövegelemzés és más nem numerikus adatok elemzése útján tártam fel, a kutatásomhoz kapcsolódó nemzetbiztonsági jogalkalmazói, illetve jogalkotói döntéshozatali folyamatokat és a kulturális tényezőket. Jogszabály, illetve dokumentumelemzés segítségével tártam fel, hogy milyen jogi keretek és intézkedések vannak a nemzetbiztonság területén, valamint hogyan alkalmazzák és értelmezik ezeket a szabályokat Magyarországon, illetve a szövetségesei által kialakított normaközegben. Ennek során kiemelt figyelmet fordítottam a jogszabályok, bírósági döntések, szerződések és egyéb jogi dokumentumok elemzésére, ideértve a jogszabályok szövegének, a joggyakorlatnak és a jogtudományi irodalomnak az alapos áttekintését. Rendkívül fontos a hazai és szövetségi szintű katonai doktrínák, szabályzatok és irányelvek elemzése annak érdekében, hogy megértsük azok hatását a katonai, illetve nemzetbiztonsági gondolkodásra és gyakorlatra.
- Kvantitatív elemzést kiemelten a dezinformáció elleni küzdelem vonatkozásában hajtottam végre, különösen a lehetséges válaszok vizsgálatával összefüggésben. Ez a

tudományos módszer a hadtudományi kontextusban elsődlegesen a statisztikai adatok és matematikai modellek felhasználását jelenti a hadviselés különböző aspektusainak mérésére és elemzésére, például erőviszonyok, veszteségek vagy logisztikai kérdésekkel kapcsolatban. A hadtudomány megközelítését alkalmazva világítottam rá az információs műveletek kibertérben végrehajtott dezinformációs kampányainak egyes jellemzőire, valamint a reziliencia erősítésének egyes lehetséges módjaira.

- Előbbiekkel szoros összefüggésben jogösszehasonlító kutatás módszerével vizsgáltam jogrendszerek és intézmények hibrid hadviseléssel, kibervédelemmel, rezilienciával összefüggő válaszait.[31] A jogösszehasonlító kutatás segítségével térképezhetjük ugyanis fel, hogy hogyan kezelik más országok a nemzetbiztonságot jogi szempontból, és milyen módszereket alkalmaznak a biztonság kényes egyensúlyának fenntartására.

Fontos kiemelni, hogy az általam preferált deduktív kutatási stratégia alkalmazása kulcsfontosságú a nemzetbiztonsági szolgálatokkal kapcsolatos kutatásokban, különösen akkor, ha a téma olyan minősített információkon alapul, amelyek csak írott vagy íratlan, más módon nem hozzáférhető tudásbázisokban találhatók meg. Ez a kutatási megközelítés lehetővé teszi, hogy az általános elméletek, elvek vagy törvények alapján következtetéseket vonjunk le a konkrét esetekre vagy helyzetekre.

[31] Ezzel összefüggésben DOBÁK Imre: Thoughts on the evolution of national security in cyberspace című tanulmányában (In.: SECURITY AND DEFENCE QUARTERLY 33 : 1 pp. 75-85. (2021)) vizsgálta meg, hogy a tárgy szerinti keretrendszerben a nemzetbiztonsági szervezetek elsődleges feladata minden országban a döntéshozók pontos és naprakész információkkal való ellátása. A 20. században kialakultak az emberi és technikai információgyűjtés specifikus területei (pl. SIGINT, HUMINT, OSINT, MASINT), amelyek folyamatos változásnak vannak kitéve, és az egyik legfontosabb alakító tényező a külső technológiai környezet. Ennek megfigyelése fontos szerepet játszik, és a nemzetbiztonsági szervek is fejlesztik módszereiket és szervezeteiket válaszul a változásokra. A kibertér és az információs társadalom terjedése a legjelentősebb alakító tényező, így a technológiai kérdések egyre fontosabbá váltak a nemzetbiztonsági szolgálatok életében. A tanulmány célja a kibertér és a nemzetbiztonsági szektor közötti összetett kapcsolatok vizsgálata, figyelembe véve a nemzeti, történelmi, politikai tényezőket, valamint a biztonságpolitikai környezet és az infokommunikációs környezet aktuális kihívásait. A metodológiai megközelítés részeként néhány elméletet lehet alkotni a technológiai fejlődés és a nemzetbiztonság területe közötti kapcsolatban, amelyek általánosan értelmezhetők országtól függetlenül. A cél nem az IT trendek teljes körű áttekintése vagy a katonai és nemzetbiztonsági aspektusok teljes leírása, hanem az irányok jelzése. A kutatási keretrendszerben a tanulmány az alábbi területeken írja le a kibertér és a nemzetbiztonsági szektor kapcsolatát és trendjeit: - A külső technológiai környezet állandó fejlődése; - A biztonsági fenyegetések és kihívások áthelyezése a kibertérbe; - Új (nemzeti) biztonsági területek létrehozása; - A civil KFI (Kutatás-Fejlesztés-Innováció) környezettel való együttműködés erősítése; - A képzett szakemberhiány problémája. A külső technológiai környezet folyamatos fejlődése mellett az infokommunikációs megoldások terjedése is folyamatos. Az új technológiák, mint például az 5G, mesterséges intelligencia és az internetes eszközök (IoT), előre látható módon alakítják át mindennapi életünket, de fenyegetéseket is hordoznak. Ezek a fenyegetések széles körben érinthetik a nemzetbiztonsági szolgálatok tevékenységét, és komoly biztonsági incidensekhez vezethetnek. A tanulmány alaposan megvizsgálja a kibertér és a nemzetbiztonság összetett viszonyát, kiemelve a technológiai fejlődés fontosságát, a biztonsági fenyegetések változását és az új biztonsági területek létrejöttét. Emellett foglalkozik a civil kutatás-fejlesztési együttműködés erősítésének szükségességével és a képzett szakemberek hiányának problémájával is, ezzel inspirálva az olvasót a nemzetbiztonság és a kiberhadviselés nemzetközi szintéren történő további összehasonlító jellegű kutatására.

A deduktív kutatási stratégia során a kutató először általános elméleti kereteket és hipotéziseket állít fel, amelyek a nemzetbiztonsági szolgálatok működésére, stratégiáira és tevékenységeire vonatkoznak. Ezeket az elméleteket és hipotéziseket teszteli a rendelkezésre álló adatokon és információkon keresztül, hogy megállapítsa, vajon azok helytállóak-e a gyakorlatban.

A nemzetbiztonsági szolgálatok munkájával kapcsolatos kutatások esetében gyakran előfordul, hogy a kutatónak korlátozott hozzáférése van a szükséges adatokhoz, mivel ezek gyakran minősítettek vagy kizárólag belső használatra szántak. Ilyen esetekben a deduktív módszer hasznos, mivel lehetővé teszi, hogy a kutató a már ismert és elérhető információkat felhasználva következtetéseket vonjon le és megértse a kevésbé látható, rejtett mechanizmusokat és folyamatokat.

A deduktív kutatási stratégia alkalmazása lehetővé teszi a kutatónak, hogy strukturált és logikus módon közelítsen a nemzetbiztonsági problémákhoz, különösen olyan esetekben, ahol a rendelkezésre álló információk korlátozottak vagy érzékenyek. Az így nyert következtetések segíthetnek a szolgálatok működésének jobb megértésében és a nemzetbiztonsági politikák hatékonyabb alakításában.

Ezen módszerek összehangolt alkalmazása útján végeztem el a komplex és átfogó kutatást a jogtudomány és a nemzetbiztonság határterületén, ugyanis így vizsgálható a leghatékonyabban a jogi normák eredményessége ezen a területen. A kutatás során megállapítottam, hogy mindkét területen fontos az interdiszciplináris megközelítés, amely lehetővé teszi, hogy a jogtudomány és a nemzetbiztonság kutatói az egyes kérdéseket több szempontból is megvizsgálják.

A jogalkotói szaktevékenység és a nemzetbiztonsági munka gyakran összekapcsolódik, például amikor terrorizmusellenes törvények hatását vagy a kiberbiztonsági jogszabályok kihívásait elemezzük. Ebben az összefüggésben megvizsgáltam, hogy a szakterületet kutatóinak milyen módos és mértékben érdemes figyelembe venniük mind a jogi előírásokat, mind a nemzetbiztonsági szempontokat, valamint az etikai és a széles (ideértve a civil) társadalmi következményeket is, annak érdekében, hogy a nemzetbiztonsági alapelvek

betartása mellett, nemzetközi közvélemény (különösen az Európai Unió döntéshozói előtt is) hiteles és elfogadható véleményt legyenek képesek megfogalmazni.

Ezen objektív megközelítésnek az indokoltsága a kézirat 2026. április elsején történő lezárásakor is megvan.

II. AZ INFORMÁCIÓS MŰVELETEK SZABÁLYOZÁSI HÁTTERE ÉS KAPCSOLATA A HIBRID HADVISELÉS EGYES INTÉZKEDÉSEIVEL

1. Az információs műveletek normatív hátterének általános vizsgálata

Az információs műveletek a 21. századi hadviselés és nemzetbiztonság egyik legkritikusabb komponensét jelentik. Az információs műveletek és a hibrid hadviselés ma már a nemzetbiztonság és a szövetségi védelmi stratégiák központi elemei.[32] A NATO felismerte, hogy minden katonai tevékenység kognitív hatást vált ki és az információs műveletek (Info Ops) feladata ennek a hatásnak a tudatos tervezése és szinkronizálása a stratégiai végcél elérése érdekében.[33]

A kortárs műveleti környezetben az információs fölény nem csupán technikai előny, hanem a „*szembenálló akaratok összecsapásának*" (clash of wills) döntő tényezője. Karl A. Menninger alapvetése[34] – „*a hozzáállás (attitudes) fontosabb a tényeknél*" – a NATO AJP-10.1 doktrína sarokkövévé vált.[35] A modern konfliktusok egy úgynevezett versengési skálán

[32] A mai biztonsági környezetben az ellenfelek gyakran kombinálják a harci műveleteket nem hagyományos és a fegyveres konfliktus küszöbe alatti módszerekkel. Ezek a tevékenységek különösen az információs környezetben elterjedtek, ahol az állami és nem állami szereplők (illetve azok közvetítői) rejtett, rosszindulatú kampányokat folytatnak. A hibrid hadviselésnek ezen intézkedéseinek a kifejezett célja, hogy növeljék a bizalmatlanságot, kiélezzék a társadalmi konfliktusokat, és aláássák a célországok demokráciájának integritását, a közbiztonságot, a gazdasági jólétet, valamint a szövetségi kohéziót. Az ellenfelek célzottan támadják az intellektuális és morális ellenállóképességet, hogy a saját javukra döntsék el a konfliktusokat anélkül, hogy nyílt fegyveres összecsapásra kerülne sor.

[33] NATO AJP-10.1 (2023): Allied Joint Doctrine for Information Operations. Edition A Version 1. Brussels: NATO Standardization Office. Elérhető: https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101 (Letöltés ideje: 2026. 02. 11.)

[34] MENNINGER, Karl A. (1963) idézi: NATO: AJP-10.1 Allied Joint Doctrine for Information Operations. Edition A, Version 1. Brussels: NATO Standardization Office, 2023. 1–4. o.

[35] Karl A. Menninger neves amerikai pszichiáter szállóigévé vált megállapítása, miszerint „az attitűdök fontosabbak a tényeknél", a modern hadviselés és a stratégiai kommunikáció (StratCom) elméleti rendszerében nyert új értelmet. Ez a felismerés az alapja annak a szemléletváltásnak, amely a NATO doktrinális fejlődését, különösen az AJP-10.1 (Allied Joint Doctrine for Information Operations) kidolgozását jellemezte.

(continuum of competition) mozognak[36], ahol a konfrontáció gyakran nem éri el a nyílt háború szintjét. Ez a modell négy dinamikus zónát határoz meg:

- Együttműködés (Cooperation): Közös érdekek mentén, a szabályalapú nemzetközi rend (RBIO) keretein belül végrehajtott tevékenységek.
- Rivalizálás (Rivalry): Ellentétes célok mentén zajló verseny, ahol a felek még tiszteletben tartják az RBIO kereteit.
- Konfrontáció (Confrontation): Válsághelyzet, ahol a nézeteltérések már nem simíthatók el diplomáciai úton; ez a „küszöb alatti" (sub-threshold) tevékenységek fő terepe.
- Fegyveres konfliktus (Armed conflict): Az akarat fizikai erővel történő kényszerítése (imposition of will), ahol az eszkaláció már nem tartható a jogi/diplomáciai küszöb alatt.

Ebben a környezetben az ellenfelek elsődleges célpontja a NATO súlypontja (Centre of Gravity): a szövetségesi kohézió. Az információs korszakban a dezinformáció és a kibertevékenységek célja e kohézió megbontása. Ennek ellensúlyozására a NATO az információt, mint közös törzskari funkciót (Information as a Joint Function) kezeli, elismerve, hogy az információs tevékenységek minden missziós narratíva és művelet elválaszthatatlan részét képezik.

A NATO meghatározása szerint az információs környezet nem csupán a technikai hálózatokat jelenti, hanem egy komplex ökoszisztémát, ahol az információáramlás és a befogadás történik. Ez a környezet három dimenzióban értelmezhető:

- fizikai (Az infrastruktúra, a rendszerek és a hordozók.),
- virtuális (Maga az információ, az adatok és az átviteli folyamatok.) és
- kognitív (Az egyének és szervezetek tudata, ahol az információ feldolgozása, értelmezése és a döntéshozatal zajlik.).

A doktrína rögzíti, hogy a kognitív dimenzió a döntő, mivel itt alakulnak ki azok az észlelések és döntések, amelyek a tartós viselkedésváltozást előidézik. Az információs

[36] NATO: AJP-10.1 (2023): Allied Joint Doctrine for Information Operations. Edition A Version 1. Brussels: NATO Standardization Office. Elérhető: https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101 (Letöltés ideje: 2026. 02. 11.)

műveletek célja, hogy elemezzék, megtervezzék és integrálják azokat a tevékenységeket, amelyek a kívánt kognitív hatásokat érik el.[37]

A feladatok végrehajtása során az Info Ops három kiemelt területre fókuszál:

- A saját cselekvési szabadság védelme: A döntéshozókat és a döntéshozatali folyamatokat támogató adatok, hálózatok és információk védelme a kibertérben és az információs térben.
- A célközönség befolyásolása: A lakosság, az érdekelt felek és a cselekvő szereplők attitűdjeinek és viselkedésének alakítása (meggyőzése, bátorítása vagy visszatartása) a saját nemzeti vagy szövetségi célkitűzések elérése érdekében.
- Az ellenséges információs tevékenységek semlegesítése: Az ellenfelek hibrid dezinformációs kampányainak, valamint a véleményformálást támogató parancsnoki és irányítási képességeiknek a leépítése vagy megzavarása.

Előbbiekkel összefüggésben szükséges kiemelni, hogy A NATO a dezinformációt egy tágabb fogalmi rendszer részeként értelmezi. A szövetség legújabb megközelítése az információs fenyegetések (information threats) gyűjtőfogalmára helyezi a hangsúlyt, amelyet *„szándékos, káros, manipulatív és koordinált tevékenységekként”* definiál, *„amelyeket állami és nem állami szereplők hajtanak végre a NATO, tagjai és partnerei gyengítése és megosztása érdekében.”*[38]

Az információs fenyegetésekkel összefüggésben a NATO elhatárolja egymástól az alábbi fogalmakat:[39]

- Dezinformáció (disinformation): hamis vagy pontatlan információ, amelyet szándékosan terjesztenek mások véleményének és cselekedeteinek manipulálása céljából.
- Propaganda: meghatározott célközönség viselkedésének vagy meggyőződésének manipulálására tervezett információ, gyakran egy állami szereplő politikai napirendjéhez kapcsolódó, elhúzódó kampány részeként.[40]

[37] NATO: AJP-10.1 (2023): Allied Joint Doctrine for Information Operations. Edition A Version 1. Brussels: NATO Standardization Office. Elérhető: https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101 (Letöltés ideje: 2026. 02. 11.)
[38]NATO: NATO’s approach to counter information threats. NATO Topics, 2024. Online: https://www.nato.int/cps/en/natohq/topics_219728.htm (Letöltés ideje: 2026. 03. 12.)
[39]NATO: NATO’s approach to counter information threats. NATO Topics, 2024. Online: https://www.nato.int/cps/en/natohq/topics_219728.htm (Letöltés ideje: 2026. 03. 12.)
[40]NATO: NATO’s approach to counter information threats. NATO Topics, 2024. Online: https://www.nato.int/cps/en/natohq/topics_219728.htm (Letöltés ideje: 2026. 03. 12.)

- Külföldi szereplők általi információmanipuláció és beavatkozás (IMIF): olyan viselkedési minta, amely fenyegeti vagy potenciálisan negatívan befolyásolja a célország értékeit, törvényes rendjét és politikai folyamatait.[41]
- Téves információ (misinformation): rosszindulatú szándék nélkül terjesztett hamis vagy pontatlan információ. A NATO ezt kizárja az információs fenyegetések köréből, mivel hiányzik belőle a szándékos manipulációs elem.

„A dezinformáció eredeti értelmében a hamis, illetve félrevezető tartalom szándékos terjesztését jelentette. Ma azonban ez a szó az információs térben előforduló különböző jelenségek gyűjtőneve lett, beleértve azokat a véleményeket és narratívákat is, amelyek ellentmondanak egy szereplő saját véleményének. Ezért már nem megfelelő a demokráciákra leselkedő valódi fenyegetés leírására, az információs környezet szándékos manipulálására külföldi állami és nem állami szereplők által manipulációs taktikák, technikák és eljárások (TTP-k) segítségével."[42]

A NATO a dezinformációt (disinformation) a következőképpen határozza meg: *„hamis vagy pontatlan információ, amelyet szándékosan terjesztenek mások véleményének és cselekedeteinek manipulálása céljából."*[43] Ez a tömör definíció két lényeges elemet tartalmaz: (1) a tartalmi elemet – hamis vagy pontatlan információ; és (2) a szándékossági elemet – a terjesztés tudatos és célzott manipulációra irányul.

A szándékosság az a kritérium, amely a dezinformációt elkülöníti a téves információtól (misinformation), hiszen míg a dezinformáció tudatos és célirányos tevékenység, addig a téves információ rosszindulatú szándék nélkül terjed.[44] A NATO kiemeli, hogy a téves információ hatásai így is károsak lehetnek, de az információs fenyegetések köréből kizárja, mert hiányzik belőle az ellenséges szándék.

[41]NATO: NATO's approach to counter information threats. NATO Topics, 2024. Online: https://www.nato.int/cps/en/natohq/topics_219728.htm (Letöltés ideje: 2026. 03. 12.)
[42] NATO: NATO's approach to counter information threats. NATO Topics, 2024. Online: https://www.nato.int/cps/en/natohq/topics_219728.htm (Letöltés ideje: 2026. 03. 12.)
[43]NATO: A NATO megközelítése az információs fenyegetések elleni fellépéshez. NATO Topics, 2024. Online: https://www.nato.int/cps/en/natohq/topics_219728.htm (Letöltés ideje: 2026. 03. 12.)
[44]A téves információ (misinformation) ezért nem szerepel az információs fenyegetések definíciójában. Ez a jelenség rosszindulatú szándék nélkül terjesztett hamis vagy pontatlan információt jelent.

A magyar szakirodalom a „dezinformáció” kifejezést használja, amely elfogadott terminussá vált. A Rendészettudományi Szaklexikon tartalmaz definíciót a fogalomra.[45] Torda Péter 2025-ös tanulmánya a Nemzetbiztonsági Szemlében részletesen elemzi a NATO dezinformáció elleni fellépésének keretrendszerét. A szerző leírja, hogy a NATO stratégiai kommunikációs doktrínája részletesen definiálja az ellenséges információs és dezinformációs műveletek elleni fellépés katonai tevékenységeit, beleértve a vezetés-irányítást, a tervezést, a végrehajtást, a koordinációt, az integrálás-szinkronizálást és az elemzés-értékelést. [46]

Haig Zsolt 2018-as monográfiájában az információs műveletek kibertéri dimenzióját elemezve külön fejezetet szentel a dezinformációs tevékenységeknek és azok információs műveletekbe történő integrálásának.[47] Rózsa Tibor 2019-es tanulmánya az információs műveletek tendenciái között szintén foglalkozik a dezinformáció növekvő jelentőségével.[48]

A nemzeti szintű szabályozás terén Magyarország Nemzeti Biztonsági Stratégiája[49] és Nemzeti Katonai Stratégiája[50] egyaránt előirányozza a stratégiai kommunikációs képességek fejlesztését, amelybe a dezinformáció elleni fellépés képessége is beletartozik. Az Ált/57 Információs Műveletek Doktrína (2014) a Magyar Honvédség nemzeti szintű implementációja, amely szintén érinti a dezinformáció kérdéskörét.[51] Az egyes normatív szabályzókkal összefüggésben jól látható a jogalkotói dinamika, a folyamatos reakció a biztonsági környezet változásaira. A NATO előírások változásával kapcsolatban kijelenthető, hogy paradigmaváltás zajlott le az elmúlt években, melynek részletes vizsgálatát a következő alfejezetben végzem el.

2. Paradigmaváltás az információs műveletek normatív szabályozási környezetében

A modern hadviselés jellege a huszonegyedik század harmadik évtizedére alapvetően megváltozott. A fizikai pusztítás mellett – és sokszor azt megelőzve – a küzdelem súlypontja

[45]BODA József et al. (szerk.): Rendészettudományi Szaklexikon. Ludovika Egyetemi Kiadó, Budapest, 2019. 115.
[46]TORDA Péter: A dezinformáció elleni fellépés a NATO stratégiai kommunikációjában. Nemzetbiztonsági Szemle, 13. évf., 2025/1. sz., 3-14. DOI: 10.32561/nsz.2025.1.1. Online: folyóiratoldal és lapszámarchívum. (Letöltés ideje: 2026. 03. 12.)
[47]HAIG Zsolt: Információs műveletek a kibertérben. Dialóg Campus Kiadó, Budapest, 2018. 112–135.
[48]RÓZSA Tibor: Az információs műveletek elmélete, gyakorlata és tendenciái. Honvédségi Szemle, 147. évf. 2019/5. sz. 73–87. (Elérhető: https://real-j.mtak.hu/13949/17/Honvedsegi_Szemle_2019_5_teljes_szam.pdf Letöltés: 2026.03.12.)
[49]1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról.
[50]1393/2021. (VI. 24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról.
[51]Ált/57 Információs Műveletek Doktrína. 1. kiadás. Magyar Honvédség, 2014.

az információs és kognitív doménbe tolódott át. A NATO ezen változásokra adott válaszaként 2023-ban végrehajtotta történetének legjelentősebb információs doktrínára vonatkozó transzformációját. Ez a váltás nem csupán terminológiai, hanem strukturális és koncepcionális jelentőségű.

Különösen fontosnak tartom megjeleníteni, a hatályon kívül helyezett AJP-3.10 (Allied Joint Doctrine for Information Operations)[52] és az új, hatályos AJP-10.1 (Allied Joint Doctrine for Information Operations)[53] közötti különbségeket és a normatív háttér változásának indokoltságát. A paradigmaváltás közvetlen kiváltó oka a NATO 2022-es Stratégiai Koncepciójában keresendő, amely rögzíti, hogy a szövetségnek egy olyan környezetben kell érvényesítenie az érdekeit, ahol a stratégiai verseny és a hibrid fenyegetések dominálnak.[54] Az új koncepció elismeri, hogy az információ nem csupán a műveletek támogató eleme, hanem a hatalomgyakorlás elsődleges eszköze. A dokumentum rögzíti a szövetség három alapvető feladatát: az elrettentést és védelmet, a válságmegelőzést és -kezelést, valamint a kooperatív biztonságot.[55] Azonban a legjelentősebb változás az információs műveletek szempontjából a biztonsági környezet értékelésében rejlik. A koncepció kimondja, hogy az autoriter szereplők hibrid taktikákkal, dezinformációs kampányokkal és a technológiai szektor feletti ellenőrzéssel támadják a szövetségesek demokratikus folyamatait és intézményeit.[56]

Az információs műveletek stratégiája ebben a kontextusban a „versengés kontinuuma” (Continuum of Competition) modelljére épül. Ez a modell szakít a béke és a háború közötti éles megkülönböztetéssel, és elismeri, hogy a szövetség és ellenfelei közötti interakció egy folyamatos skálán mozog, amely a békés együttműködéstől a fegyveres konfliktusig terjed.6 Az információs tevékenységek ebben a kontinuumban mindenütt jelen vannak, de súlyuk a szürke zónában (grey zone), a fegyveres támadás küszöbe alatti konfrontációban válik döntővé. Az AJP-01 (Allied Joint Doctrine) legújabb kiadása hangsúlyozza, hogy a NATO-nak képesnek kell lennie az információs fölény kivívására a kontinuum minden szakaszában, biztosítva a szövetség cselekvési szabadságát.[57]

---

[52] NATO AJP-3.10 Allied Joint Doctrine for Information Operations, Edition A Version 1. Brussels: NATO Standardization Office, 2015.
[53] NATO: AJP-10.1 (2023): Allied Joint Doctrine for Information Operations. Edition A Version 1. Brussels: NATO Standardization Office.
[54] NATO 2022 Strategic Concept. Adopted at the Madrid Summit, 29 June 2022.
[55] NATO 2022 Strategic Concept. Adopted at the Madrid Summit, 29 June 2022.
[56] NATO 2022 Strategic Concept. Section 7.
[57] NATO AJP-01: Allied Joint Doctrine. Edition F Version 1. Brussels: NATO Standardization Office, 1 April 2025.

A Stratégiai Koncepció egyik legfontosabb megállapítása, hogy a rosszindulatú kibertevékenységek, a világűrből vagy világűrbe irányuló ellenséges műveletek, valamint a hibrid műveletek elérhetik a fegyveres támadás szintjét, és kiválthatják az Észak-atlanti Szerződés 5. cikke szerinti kollektív védelmi mechanizmust.[58] Ez a kiterjesztett értelmezés közvetlenül integrálja az információs domént a nemzetbiztonság legmagasabb szintű garanciái közé.

A doktrinális váltás legfontosabb normatív mérföldkövei:

- AJP-01 (F): A legfelsőbb szintű szövetségi összhaderőnemi doktrína (2025), amely bevezette a versengés kontinuumát (continuum of competition).[59]
- AJP-10: A Stratégiai Kommunikáció (StratCom) „keystone" doktrínája (2023), amely új hierarchikus keretbe helyezte az információs tevékenységeket.[60]
- AJP-10.1: Az Információs Műveletek új doktrinális statútuma (2023), amely hivatalosan felváltotta az AJP-3.10-et.[61]

Az egyik legjelentősebb változás az információs műveletek (Info Ops) helyzete a doktrinális hierarchiában. A korábbi AJP-3.10 a műveleti (Operations) ághoz tartozott, az AJP-3 sorozat részeként. Ebben a felállásban az Info Ops-ot elsősorban katonai képességek koordinációjaként kezelték, amely a parancsnok kinetikus céljait támogatta.[62]

Ezzel szemben az AJP-10.1 már az információs és kommunikációs ághoz tartozik, közvetlenül az AJP-10 (StratCom) alárendeltségében.[63] Ez a váltás azt jelzi, hogy a NATO a Stratégiai Kommunikációt tekinti a legfelsőbb szintű integráló funkciónak, amely biztosítja, hogy a szövetség minden tevékenysége (cselekedetek, képek és szavak) összhangban legyen a stratégiai narratívával.[64] Az Info Ops feladata ebben az új architektúrában a horizontális

[58] NATO 2022 Strategic Concept. Article 5 implications.
[59] NATO AJP-01: Allied Joint Doctrine. Edition F Version 1. Brussels: NATO Standardization Office, 1 April 2025.
[60] NATO AJP-10: Allied Joint Doctrine for Strategic Communications. Edition A Version 1. Brussels: NATO Standardization Office, 2023.
[61] NATO AJP-10.1 (2023). Promulgation Letter, Section 2.
[62] NATO AJP-3.10 Allied Joint Doctrine for Information Operations, Edition A Version 1. Brussels: NATO Standardization Office, 2015.
[63] NATO AJP-10.1 (2023). Chapter 2 – Fundamentals.
[64] Allied Joint Doctrine for Strategic Communications (AJP-10). Edition A Version 1, UK Change 1. Ministry of Defence, 2023.

integráció, vagyis a parancsnokság különböző részlegeinek és képességeinek összehangolása a kommunikációs irányelvek mentén.[65]

Az AJP-10.1 szerint az Info Ops folyamata négy pillérre épül: elemzés, tervezés, integráció és értékelés.[66] Ez a ciklus biztosítja, hogy az információs tevékenységek ne elszigetelten, hanem a műveleti terv (OPLAN) szerves részeként valósuljanak meg. A korábbi doktrínával szemben, amely az információ terjesztésére fókuszált, az új megközelítés viselkedésközpontú (behaviour-centric), és a célközönségek attitűdjeinek, észlelésének és végső soron magatartásának befolyásolását tekinti elsődlegesnek.[67] Az a tény, hogy az információs tevékenységek definíciójában a kognitív hatás (cognitive effects) szerepel, bizonyítja a NATO elmozdulását a technikai (adatközpontú) megközelítéstől az emberközpontú hadviselés felé.

A doktrína meghatározása szerinti, alapvető fontosságú definíciók: [68]

- Információs műveletek (Information Operations). „*Törzsfunkció, amelynek feladata az információs tevékenységek elemzése, tervezése, értékelése és integrálása annak érdekében, hogy a kívánt hatást gyakorolja az ellenfelek, potenciális ellenfelek és célközönségek akaratára, megértésére és képességére a műveleti célok elérésének támogatása érdekében. (NATO egyezményes)”* [69]
- Információs tevékenységek (Information Activities). „*Valamely képesség vagy eszköz által végrehajtott tevékenységek, amelyek kognitív (tudati) hatások előidézésére irányulnak. (NATO egyezményes)”* [70] Ez azt jelenti, hogy a hagyományos (kinetikus) katonai erők megnyilvánulásai is lehetnek információs tevékenységek, amennyiben azok célja az ellenfél vagy a célközönség észlelésének befolyásolása.
- Kommunikációs tevékenységek (Communication Activities). „*Jelen kiadvány alkalmazásában a kommunikációs tevékenységek olyan információs tevékenységek, amelyeket a katonai közkapcsolatok (Military Public Affairs) és a pszichológiai műveletek (Psychological Operations) képességei hajtanak végre*.”[71]

[65] NATO AJP-10.1 (2023). Section 1.1 – Context and Role.
[66] NATO AJP-10.1 (2023). Summary of changes.
[67] IVEN, Markus – JASPER, Laura – RADEMAKER, Michel (2023): Cognitive Effects in Combined Arms.
[68] NATO AJP-10.1 (2023) Chapter 2 (2.7., a–d)
[69] NATO AJP-10.1 (2023) Chapter 2 (2.7., a–d)
[70] NATO AJP-10.1 (2023) Chapter 2 (2.7., a–d)
[71] NATO AJP-10.1 (2023) Chapter 2 (2.7., a–d)

- Információs környezet (Information Environment). „*Olyan környezet, amely magában foglalja magát az információt, az információt fogadó, feldolgozó és továbbító személyeket, szervezeteket és rendszereket, valamint azt a kognitív, virtuális és fizikai teret, amelyben mindez végbemegy. (NATO egyezményes)”* [72]

Az AJP-10.1 egyik legjelentősebb tartalmi eleme a 2. fejezetben (Chapter 2.) található képesség-taxonómia, amely rendszerezi azokat a katonai képességeket és technikákat, amelyek információs tevékenységeket hajtanak végre vagy azokhoz hozzájárulnak.[73] A doktrína alapvető különbséget tesz az információs műveletek (Info Ops) mint törzsfunkció[74] és az információs tevékenységek (Information Activities) mint végrehajtott cselekvések között. Az Info Ops nem maga hajt végre tevékenységeket, hanem elemez, tervez, integrál és értékel. Valamennyi képesség és tevékenység az akarat–megértés–képesség (will–understanding–capability) célhármas legalább egyik dimenziójára fejt ki hatást.[75]

A tevékenységeket a különböző képességek hajtják végre, amelyeket a doktrína három jól elkülönített csoportba sorol:

- Kommunikációs képességek (Communication Capabilities), amelyek elsődleges rendeltetése a kommunikáció útján történő hatáskifejtés;
- Kiegészítő képességek és technikák (Additional Capabilities and Techniques), amelyeket az Info Ops törzs gyakrabban tervez, integrál és értékel; valamint

[72] NATO AJP-10.1 (2023) Chapter 2 (2.7., a–d)
[73]NATO AJP-10.1 (2023), 2.7a–b.
[74]NATO AJP-10.1 (2023), 2.5.
[75]NATO AJP-10.1 (2023), 2.9–2.12.

- Engagement[76], jelenlét, megjelenés és profil (Engagement, Presence, Posture and Profile), amelyek a személyes interakcióhoz és a haderő puszta jelenlétéhez kapcsolódnak.[77]

A doktrína két képességet sorol a Kommunikációs képességek (Communication Capabilities) csoportba, amelyek elsődleges rendeltetése a kommunikáció útján történő hatáskifejtés. Ezek a képességek ún. kommunikációs tevékenységeket (communication activities) hajtanak végre, amelyek az információs tevékenységek megkülönböztetett alkategóriáját képezik, az alábbiak szerint:[78]

- Pszichológiai műveletek (Psychological Operations – PsyOps) A pszichológiai műveletek az AJP-10.1 szerinti meghatározásban *„tervezett tevékenységek, amelyek kommunikációs módszerek és más eszközök felhasználásával irányulnak jóváhagyott célközönségekre, annak érdekében, hogy befolyásolják a megítélést, az attitűdöket és a viselkedést, ezáltal hatást gyakorolva a politikai és katonai célok elérésére.*"[79]A PsyOps „a parancsnok hangja" („the commander's voice"), amellyel közvetlenül és szűrés nélkül szólíthat meg meghatározott célközönségeket. A doktrína szerint a PsyOps közvetlen hatást fejt ki a megértésre és az akaratra, közvetett hatást pedig a képességre.[80] Ez azt jelenti, hogy a lélektani műveletek elsősorban a célközönség észlelését, attitűdjeit és motivációját befolyásolják (megértés és akarat), de ezen keresztül közvetve hatást gyakorolnak a cselekvési képességre is – például, ha az ellenséges állomány morálja összeomlik, a fizikai képességek is hatékonyabbá válnak. A PsyOps további funkciói

[76] Az AJP-10.1 szerinti engagement fogalom nem kap önálló NATO Agreed definíciót a dokumentumban, de a doktrína három szinten használja: strategic engagement, key leader engagement és soldier-level engagement. Az engagement lényege minden szinten az interakció meghatározott célközönségekkel, meghatározott célok elérése érdekében, tehát tervezett, célirányos kapcsolatfelvétel és kapcsolattartás. A magyar szakirodalomban nincs egyetlen elfogadott fordítás, ugyanakkor többféle megoldás él párhuzamosan: „Kapcsolatépítés / kapcsolattartás", amelyet Rózsa Tibor használ, valamint a „kulcsvezetőkkel való kapcsolattartás" formát a KLE fordításaként. Ez a leggyakoribb megoldás a hadtudományi publikációkban. „Bevonás" – egyes fordításokban a „kulcsszemélyek bevonása" formában jelenik meg, de ez félrevezető lehet, mert az engagement nem feltétlenül jelent bevonást a döntéshozatalba, hanem inkább célzott interakciót. „Megszólítás" – ritkábban használt, de egyes kontextusokban (különösen a soldier-level engagement esetében) találó, mivel a helyi lakosság megszólítását jelenti. Az engagement szó megtartása – számos magyar szerző (például az MH doktrínáiban és a Haig Zsolt munkáiban) megtartja az angol kifejezést, zárójelben vagy anélkül, ugyanis a magyar nyelv nem rendelkezik egyetlen olyan kizárólagos kifejezéssel, amely az engagement teljes jelentéstartalmát lefedné. (Hivatkozott művek: Haig, Zsolt: Információs műveletek a kibertérben. Dialóg Campus, Budapest, 2018., Rózsa, Tibor: Az információs műveletek elmélete, gyakorlata és tendenciái. Honvédségi Szemle,147/5, 2019. pp. 18–36.)
[77]NATO AJP-10.1 (2023), 2.13.
[78]NATO AJP-10.1 (2023), 2.13
[79]NATO AJP-10.1 (2023), 2.13a.
[80]NATO AJP-10.1 (2023), 2.13a.

közé tartozik a biztonság és a tudatosság növelése, valamint az ellenséges információs tevékenységek és dezinformáció elleni fellépés.[81] A lélektani műveletek részletes szabályozását az AJP-3.10.1 (Allied Joint Doctrine for Psychological Operations) tartalmazza.[82]

- A katonai közkapcsolatok (Military Public Affairs – Mil PA) „a NATO katonai céljainak és célkitűzéseinek előmozdításáért felelős képesség, amely a stratégiai kommunikáció részeként pontos információkat közöl a célközönségek felé, időben."[83] A Mil PA kettős funkciót tölt be, ugyanis külső kommunikációt (a nyilvánosság és a média felé) és belső kommunikációt (a haderő állománya felé) egyaránt végez.[84]

A Mil PA alapvető célja a NATO szerepe megértésének és tudatosításának elősegítése, ezáltal erősítve a szervezet hitelességét és megbízhatóságát.[85] A doktrína kiemeli, hogy mind a Mil PA, mind a PsyOps hozzájárul az ellenséges dezinformáció elleni fellépéshez, azonban a kettő között lényeges különbség áll fenn a célközönségek, a hatókör és a szándék tekintetében.[86]

Az AJP-10.1 2.14. bekezdése rögzíti a Kiegészítő képességek és technikák (Additional Capabilities and Techniques) csoportjára vonatkozó elvként, hogy: *„bár bármely katonai képesség végrehajthat információs tevékenységet, több olyan képesség is létezik, amelyet az Info Ops gyakrabban tervez, integrál és értékel*."[87] Ez a megfogalmazás két fontos üzenetet hordoz. Egyrészt bármely katonai képesség – akár tüzérség, akár logisztika – kognitív hatást fejthet ki, tehát információs tevékenységet hajthat végre. Másrészt az alábbi képességek, illetve technikák a leggyakoribb integrációs partnerek:

- Kibertéri műveletek (Cyberspace Operations) az AJP-10.1 szerint két fő kategóriára oszlanak: támadó kibertéri műveletek (Offensive Cyberspace Operations – OCO) és védelmi kibertéri műveletek (Defensive Cyberspace Operations – DCO).[88] A támadó

[81]NATO AJP-10.1 (2023), 2.13a,. valamint ezzel összefüggésben még: 3.3f.
[82]NATO AJP-3.10.1 Allied Joint Doctrine for Psychological Operations. Edition A. NATO Standardization Office, 2014.
[83]NATO AJP-10.1 (2023), 2.13b.
[84]MC 0457/3 NATO Military Policy on Public Affairs. NATO Military Committee, 2011.
[85]A Mil PA részletes szabályozását az MC 0457/3 (NATO Military Policy on Public Affairs) tartalmazza.
[86]AJP-10.1 (2023), 2.13b. A doktrína elhatárolja a katonai közkapcsolatokat a pszichológiai műveletektől: *„Mind a katonai közkapcsolatok, mind a pszichológiai műveletek fellépnek az ellenséges dezinformációval szemben; ugyanakkor eltérnek egymástól a célközönségek, a hatókör és a szándék tekintetében."*
[87]NATO AJP-10.1 (2023), 2.14.
[88]NATO AJP-10.1 (2023), 2.15.

kibertéri műveletek (OCO) technikákat és képességeket biztosítanak információs tevékenységek végrehajtásához, és multiplikátor hatást fejtenek ki más információs tevékenységekre.[89] Ez azt jelenti, hogy az OCO felhasználása más képességek – például a lélektani műveletek vagy az elektromágneses hadviselés – hatékonyságát is jelentősen növelheti. A védelmi kibertéri műveletek (DCO) a kibertér használatának megőrzésére irányulnak, biztosítva a cselekvési szabadságot és az erők védelmét a kibertérben. Jóváhagyásuk az összhaderőnemi célkiválasztási (joint targeting) eljáráson keresztül történik. Az erőforrás-biztosítás a SCEPVA-mechanizmuson (Sovereign Cyber Effects Provided Voluntarily by Allies) alapul, amely a szuverén nemzeti kiberképességek önkéntes felajánlása útján érvényesül. A kibertéri műveletek részletes szabályozását az AJP-3.20 tartalmazza. [90]

- Elektromágneses hadviselés (Electromagnetic Warfare) a hadműveleti szintű parancsnok számára biztosít eszközöket az elektromágneses környezet alakítására. A doktrína három tevékenységtípust különböztet meg:[91] Az elektromágneses támadás (electromagnetic attack) az ellenség kommunikációs csomópontjainak támadásával ellentevékenységet hajt végre a parancsnoki funkciók ellen, és támogatja a megtévesztési, lélektani és sugárzási tevékenységeket. Az elektromágneses védelem (electromagnetic defence) a személyi állomány, a létesítmények és az eszközök védelmét szolgálja, valamint ellentevékenységet hajt végre az ellenséges információs képességek ellen. Az elektromágneses felderítés (electromagnetic surveillance) hírszerzési információkat és megalapozott helyzetértékelést biztosít.[92] Az elektromágneses hadviselés hatásai lehetnek ideiglenesek vagy állandóak, és a doktrína kiemeli, hogy *„potenciálisan minimalizálják az erő alkalmazásának szükségességét.”*[93] Ez az információs műveletek kontextusában különösen fontos, mivel az elektromágneses hatások gyakran nem kinetikus alternatívát kínálnak fizikai pusztítás nélkül. Fontos terminológiai változás, hogy az AJP-10.1 már az „electromagnetic warfare” kifejezést használja a korábbi „electronic warfare” helyett, összhangban az AJP-3.6 frissítésével.[94]
- Polgári-katonai együttműködés és interakció (CIMIC/CMI) az AJP-10.1 meghatározásában „összhaderőnemi funkció, amely lehetővé teszi a katonai és nem

[89]NATO AJP-3.20 Allied Joint Doctrine for Cyberspace Operations. NATO Standardization Office, 2020.
[90]NATO AJP-10.1 (2023), 2.15.
[91]NATO AJP-10.1 (2023), 2.16.
[92]NATO AJP-3.6 Allied Joint Doctrine for Electronic Warfare. Edition B. NATO Standardization Office, 2020.
[93]NATO AJP-10.1 (2023), 2.16.
[94]NATO AJP-3.6 Allied Joint Doctrine for Electronic Warfare. Edition B. NATO Standardization Office, 2020.

katonai szereplők közötti interakciót."[95] A CIMIC a polgári-katonai interakciót (CMI) több módon is megvalósítja: polgári-katonai összekötésen, kulcsvezetői engagementen, a polgári környezet értékelésén, valamint nem katonai célközönségekkel való tervezésen és koordináción keresztül.[96] A CIMIC öt alapelven nyugszik: tisztelet, bizalom, átláthatóság, hitelesség és megbízhatóság.[97] A doktrína külön hangsúlyozza, hogy az információs tevékenységek nem áshatják alá ezeket az alapelveket – azaz a CIMIC hitelességét nem szabad alárendelni rövid távú információs céloknak. A CIMIC-állomány jelenléte az Információs Tevékenységek Munkacsoportjában (IAWG) minden szinten kötelező.

- Fizikai megsemmisítés (Physical Destruction) az összhaderőnemi célkiválasztási eljáráson (joint targeting process) keresztül alkalmaz különböző eszközöket annak érdekében, hogy *„az adott célközönség információs pozíciójára és döntéshozó képességére specifikus hatást gyakoroljon – ebben az esetben ez információs tevékenységnek minősül."*[98]A fizikai megsemmisítés két szinten fejt ki információs hatást. Egyrészt a vezetés és irányítási rendszerek (C2) elleni támadással közvetlenül megzavarja az ellenség döntéshozó képességét. Másrészt az erő alkalmazásának erős pszichológiai üzenete van: hatást gyakorol a morálra, kényszerítő és elrettentő ereje van. A célokat az információs környezet értékelése (IEA) azonosítja, és az Info Ops törzs nyújtja be jóváhagyásra az összhaderőnemi célkiválasztási ciklus keretében.
- Műveleti biztonság és megtévesztés (OPSEC and Deception) Az AJP-10.1 a műveleti biztonságot és a megtévesztést *„különálló, de információs tevékenységként is alkalmazható katonai tevékenységekként"* kezeli.[99] A két tevékenység szorosan összefügg, de eltérő céllal és módszertannal rendelkezik.[100] A műveleti biztonság (OPSEC) célja *„az ellenség kritikus információkhoz és jellemzőkhöz való hozzáférésének megakadályozása",* a Saját Erők Lényeges Információs Elemeinek (Essential Elements of Friendly Information – EEFI) védelme révén.[101] Az OPSEC tehát védelmi jellegű, célja, hogy az ellenség ne juthasson olyan információkhoz, amelyek felfednék a saját erők szándékait, képességeit vagy sebezhetőségeit. A megtévesztés (Deception) ezzel szemben

[95]NATO AJP-10.1 (2023), 2.17.
[96]NATO AJP-3.19 Allied Joint Doctrine for Civil-Military Cooperation. NATO Standardization Office, 2018.
[97]NATO AJP-10.1 (2023), 2.17.
[98]NATO AJP-10.1 (2023), 2.18.
[99]NATO AJP-10.1 (2023), 2.19.
[100]NATO AJP-3.10.2 Allied Joint Doctrine for Operations Security and Deception. NATO Standardization Office, 2016.
[101]NATO AJP-10.1 (2023), 2.19.

támadó jellegű, aktív tevékenység: *„pszichológiai folyamat, amely viselkedési választ keres – cselekvést vagy tétlenséget –, és kifejezetten egy kulcsfontosságú döntéshozóra irányul, akit a legvalószínűbben lehet a kívánt módon befolyásolni.”*[102] A megtévesztés a hamis látszat létrehozását és felmutatását, egyidejűleg a valós baráti szándékok, erősségek, sebezhetőségek és disszlokáció elfedését foglalja magában. Mindkettő mélyrehátó elemzést igényel az ellenség előzetes meggyőződéseiről és információs preferenciáiról.

- Információbiztonság (Information Assurance) a doktrína meghatározása szerint *„az információ és az információs rendszerek védelme és megóvása, rendelkezésre állásuk, integritásuk és bizalmasságuk biztosítása révén.”*[103] Ez az ún. CIA-triád (Confidentiality, Integrity, Availability) NATO doktrinális megfogalmazása. A képesség széles körű elemeket ölel fel: fizikai biztonság, személyi és dokumentumbiztonság, információvédelem (INFOSEC), hírközlési biztonság és számítógép-biztonság.[104] A kibervédelmi tevékenységek kiemelt fontosságú elemei az információbiztonságnak. A korábbi AJP-3.10-ben az „Information Security (INFOSEC)” önálló kategóriaként szerepelt – az AJP-10.1 ezt a szélesebb „Information Assurance” fogalommal váltotta fel, amely tartalmazza ugyan az INFOSEC-et, de annál átfogóbb.[105]
- Feltörekvő és diszruptív technológiák és (Emerging and Disruptive Technologies – EDT) Az AJP-10.1 teljes egészében új elemként vezette be a feltörekvő és diszruptív technológiákat a képesség-taxonómiába – a korábbi AJP-3.10 nem tartalmazta ezt a kategóriát. A doktrína meghatározása szerint az EDT-k *„hatást gyakorolnak a rezilienciára, beleértve a polgári felkészültséget, a kritikus infrastruktúrát és a nyilvános tájékoztatást (ezáltal az Info Ops-ra is) a Szövetség egész területén.”*[106] Az EDT-k megváltoztatják a NATO és ellenfeleinek működési módját a versengés teljes spektrumában (competition continuum). Az innováció motorjai elsősorban a magánszektor és az akadémiai szféra, kettős felhasználású (dual-use) alkalmazásokkal. Ilyen technológiák például a mesterséges intelligencia, a Big Data analitika, az autonóm rendszerek, a kvantumtechnológia, a hiperszonikus rendszerek és a biotechnológia –

[102]NATO AJP-10.1 (2023), 2.19.
[103]NATO AJP-10.1 (2023), 2.20.
[104]NATO AJP-10.1 (2023), 2.20.
[105]NATO AJP-6 Allied Joint Doctrine for Communication and Information Systems. NATO Standardization Office, 2017.
[106]NATO AJP-10.1 (2023), 2.21.

amelyek mind hatással vannak az információs környezetre és a benne folyó tevékenységekre.

A harmadik – Engagement, jelenlét, megjelenés és profil – képességcsoport hat elemet tartalmaz, amelyek nem a szűken vett kommunikációs vagy kinetikus képességekhez, hanem a személyes interakcióhoz és a haderő puszta jelenlétéhez kapcsolódnak. Ezek a tevékenységek általában nem igényelnek speciális képességeket, inkább az összes katonai személyzet magatartását és interakcióját érintik:

- Stratégiai engagement (Strategic Engagement) A stratégiai engagement a doktrína meghatározásában *„stratégiai szinten végrehajtott interakciók a nem katonai hatalmi eszközök befolyásolása érdekében, stratégiai célok elérésére.”*[107] Irányításuk és jóváhagyásuk általában a NATO Főhadiszállás (NATO HQ) vagy a SHAPE szintjén történik. Hadműveleti szinten a parancsnok hajtja végre; kivételesen delegálható a helyettesének, de összhaderőnemi erőparancsnokság (component command) szintje alá nem delegálható. Ez a korlátozás jelzi a stratégiai engagement kiemelkedő fontosságát és politikai érzékenységét: a nem katonai hatalmi eszközökre (diplomácia, gazdaság, civil szervezetek) történő hatásgyakorlás csak a legmagasabb szintű katonai vezetés jogkörében maradhat.
- Kulcsvezetői engagement (Key Leader Engagement – KLE) A kulcsvezetői engagement (KLE) *„NATO-vezetők és más meghatározó döntéshozók közötti tervezett interakciók, meghatározott célok elérése érdekében.”*[108] A döntéshozók köre tágan értelmezendő: vallási vezetők, civil társadalmi vezetők, akadémikusok, törzsi vezetők és más befolyásos személyiségek egyaránt ide tartoznak. Az Info Ops törzs kiemelkedő szerepet játszik a KLE támogatásában: *„kialakítja és karbantartja az összes kulcsvezető és kapcsolatrendszerük adatbázisát”, és integrálja a parancsnok KLE-tervét.”* [109] A hatékony KLE részletes ismereteket igényel a célszemélyek személyiségéről, vezetési stílusáról, ambícióiról, motivációiról és pszichológiai profiljukról.
- Katona szintű engagement (Soldier-level Engagement) A doktrína elismeri, hogy a műveleteket emberek között hajtják végre, és az interakciók többsége a katonák szintjén

[107]NATO AJP-10.1 (2023),. 2.22a.
[108]NATO AJP-10.1 (2023), 2.22b.
[109]NATO AJP-10.1 (2023), 2.22b.

zajlik.[110] Ezek az interakciók két formát ölthetnek: dinamikus (spontán, előre nem látható lehetőségek) és tervezett (ütemezett találkozók, eljárásrendbe illesztett interakciók).Fontos terminológiai meghatározás, hogy a „katona" (soldier) fogalom a doktrínában tágan értelmezendő, ugyanis magában foglalja a tengerészeket, tengerészgyalogosokat, légierős állományt és a NATO civil alkalmazottait is. A katonai szintű engagement hatékonyságának biztosítása érdekében a katonák egyszerű, világos narratívát kapnak, amely köré az engagement-et építhetik. Ez közvetlenül kapcsolódik a doktrína narratívavezérelt megközelítéséhez.

- Jelenlét, megjelenés és profil (Presence, Posture and Profile – PPP) *„Egy haderő puszta jelenléte jelentős és változó hatást gyakorol a célközönségek percepcióira."*[111] A doktrína a PPP három komponensét külön-külön fejti ki:
  a) A jelenlét (Presence) arra utal, hogy *„a képesség megfelelő helyre és időben történő telepítése hitelességet ad és hozzájárul az elrettentéshez."*[112] Például egy NATO harccsoport megjelenése egy szövetséges állam területén önmagában is jelentős információs tevékenység, még mielőtt bármilyen kommunikációs üzenet elhangzana.
  b) A megjelenés, illetve viselkedés (Posture) arra utal, hogy *„a haderő magatartását globális közönség vizsgálja, és annak tudatosnak kell lennie a kulturális és fenyegetési tényezők figyelembevételével."*[113] A haderő viselkedése – puha vagy kemény fellépés, barátságos vagy távolságtartó magatartás – információs hatást fejt ki, amely erősítheti vagy alááshatja a műveleti célokat.
  c) A profil (Profile) arra utal, hogy *„A parancsnokok nyilvános profilja minden szinten a közönség széles körének jelentős érdeklődésére számíthat. Nyilvános szereplésüket emiatt gondosan elemezni kell, és a lehetőségeket ki kell használni kulcsüzenetek közvetítésére."*[114] A parancsnoki profil kezelése tehát tudatos információs tevékenység, a parancsnok megjelenése, nyilatkozatai és viselkedése a narratíva részét képezi.

- Kulturális érzékenység (Cultural Understanding) *„A kulturális érzékenységek megértése elengedhetetlen, és formálja az engagement tevékenységeket."*[115] A doktrína hangsúlyozza a speciális engagement csapatok (specialist engagement teams) szerepét,

[110]NATO AJP-10.1 (2023), 2.22c.
[111]NATO AJP-10.1 (2023), 2.25.
[112]NATO AJP-10.1 (2023), 2.25a
[113]NATO AJP-10.1 (2023), 2.25b
[114]NATO AJP-10.1 (2023), 2.25c
[115]NATO AJP-10.1 (2023), 2.24.

beleértve a női és vegyes összetételű engagement csapatokat (female and mixed engagement teams), valamint a nyelvi készségek és interkulturális kompetencia fejlesztését.[116] A kulturális megértés nem csupán „soft skill", hiszen a doktrína a hatékony információs tevékenységek előfeltételeként kezeli. Kulturális megértés nélkül a PsyOps üzenetei célt téveszthetnek, a KLE felkészületlenségbe torkollhat, és a katonai szintű engagement akaratlanul is sértheti a helyi érzékenységeket. A gender perspektíva külön kiemelése jelzi, hogy a NATO a női civil lakossághoz való hozzáférést stratégiai jelentőségűnek tekinti bizonyos műveleti környezetekben.

- Magatartás és viselkedési normák (Conduct and Standards of Behaviour) jelentősége abban áll, hogy a NATO-személyzet magatartása önmagában információs tevékenység. A doktrína figyelmeztet: *„a vonatkozó normák és irányelvek be nem tartása aláásható a Szövetség hatékonyságát és hitelességét, az egyének legitimitását, és veszélyeztetheti a küldetés sikerét."*[117] Ez a szabályösszesség magában foglalja a nemzetközi humanitárius jogot, a szövetségi és nemzeti etikai kódexeket, valamint a műveleti viselkedési szabályokat (Rules of Engagement). Az AJP-10.1 ezáltal elismeri, hogy „*egyetlen fegyelmi incidens nagyobb kárt okozhat az információs környezetben, mint amit hónapok kommunikációs erőfeszítése kompenzálni képes*."[118] A modern médiakörnyezetben a magatartási normák betartása nem csupán jogi kötelezettség, hanem műveleti szükségszerűség is.[119]

A paradigmaváltás egyik fontos eleme, hogy kiemelt helyen kezeli a kognitív hatás kiváltását célzó tevékenységek jelentőségét.

3. Kognitív hatást célzó hadviselés, az emberi agy, mint műveleti terület

A kognitív hadviselés fogalma a NATO stratégiai gondolkodásában a 2020-as évek elején kristályosodott ki, előre jelezve egy paradigmaváltást az információs műveletekkel

[116]NATO AJP-10.1 (2023), 2.24.
[117]NATO AJP-10.1 (2023), 2.26.
[118]NATO AJP-10.1 (2023), 2.26.
[119]Ezzel összefüggésben további információ található a Magatartási Kódexben (Code of Conduct), a NATO szexuális kizsákmányolás és visszaélés megelőzésére és kezelésére vonatkozó irányelvében (NATO Policy on Preventing and Responding to Sexual Exploitation and Abuse), valamint a Kettős Stratégiai Parancsnoksági Irányelvben (Bi-SCD) 040-001, amely az ENSZ BT 1325. számú határozatának és a gender perspektívának a NATO parancsnoki struktúrába történő integrálásáról rendelkezik.

összefüggően. [120] Míg az információs műveletek hagyományosan az adatok feletti kontrollra, a dezinformáció terjesztésére vagy a kommunikációs csatornák megzavarására fókuszáltak, a kognitív hadviselés az emberi elme működési mechanizmusait veszi célba. A 2025-ben és 2026-ban napvilágot látott NATO Chief Scientist jelentések[121] egy olyan új fenyegetési formát azonosítottak, amely túlmutat a hagyományos információs műveleteken, ez a kognitív hadviselés. A kognitív hadviselés (CW) lényege, hogy az emberi elmét és a társadalmi döntéshozatali folyamatokat tekinti elsődleges célpontnak. Nem csupán az információk manipulálásáról van szó, hanem az emberi észlelés, a gondolkodás és a viselkedés biológiai és pszichológiai szintű befolyásolásáról.

A kognitív hadviselés a stratégiai verseny új szintje, ahol a cél az ellenfél racionalitásának lebontása, a kollektív hitrendszerek megrendítése és a döntéshozatali fölény (decision advantage) megszerzése. A NATO Chief Scientist 2025-ös jelentése hangsúlyozza, hogy a kognitív hadviselés elleni védekezéshez a reziliencia új szintjére van szükség: a kognitív rezilienciára.[122]

A James Giordano által jegyzett tanulmány[123] a kognitív hadviselést nem csupán elméleti fenyegetésként, hanem a modern hadviselés egyik legkritikusabb, műveleti szintű kihívásaként értelmezi. A tanulmány rávilágít, hogy a kortárs konfliktusok egyre inkább magatartás-központúak (*behavior-centric*). Ez azt jelenti, hogy a döntő terep már nem a

[120] DU CLUZEL, François (2021): *Cognitive Warfare*. Norfolk: NATO Innovation Hub. Bernard Claverie és François du Cluzel munkássága bevezeti a „kognitika" (cognitics) fogalmát, amely a kognitív tudományok – úgymint a neurobiológia, a pszichológia, a nyelvészet és az MI – szisztematikus alkalmazását jelenti katonai célok elérése érdekében. A szerző alapvető tézise, hogy a hadviselés következő generációjában az emberi elme már nem csupán a döntéshozatal helyszíne, hanem maga a műveleti terület (human domain). A cél nem az ellenség fizikai megsemmisítése, hanem a gondolkodásmódjának és valóságérzékelésének szisztematikus torzítása. A tanulmány megkülönbözteti a kognitív hadviselést a hagyományos információs műveletektől. Míg az információs hadviselés az adatok feletti ellenőrzésre fókuszál (mit tudunk), a kognitív hadviselés a feldolgozási folyamatokat támadja (hogyan gondolkodunk). A dokumentum hangsúlyozza, hogy a kognitív hadviselés elsődleges célpontja a társadalmi bizalom. Az intézményekbe, a tudományba és a médiába vetett hit megrendítése a társadalom belső kohéziójának felbomlásához vezet, ami stratégiai előnyt jelent az agresszor számára. Mivel a kognitív hadviselés gyakran a „szürke zónában", békeidőben és észrevehetetlenül zajlik, a hagyományos katonai válaszok hatástalanok. A szerző a reziliencia növelését, a kognitív önvédelem oktatását és a civil-katonai összefogás új formáit sürgeti.

[121]NATO STO (2025): Cognitive Warfare. STO-OCS-001.

[122] GIORDANO James (2026): Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness. Strategic Insights, National Defense University. Elérhető: https://inss.ndu.edu/Media/News/Article/4371195/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-operat/ (Letöltés ideje: 2026. 02. 11.). Ez magában foglalja a neuro-AI readiness programokat a katonai állomány számára, a digitális műveltség fejlesztését a társadalomban, valamint az etikai-jogi keretrendszerek kidolgozását a neurotechnológiák alkalmazására vonatkozóan.

[123] GIORDANO James (2026): Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness. Strategic Insights, National Defense University. Elérhető:

földrajzi térség, hanem az emberi észlelések, értelmezések és döntéshozatali folyamatok összessége. A kognitív hadviselés célja a célpontok (legyenek azok vezetők vagy a teljes társadalom) gondolkodásának és cselekvésének megváltoztatása. Giordano két fő szintet különít el a kognitív befolyásolás során:

- Biológiai szint (Manipulating Capacity): Ez a szint közvetlenül az idegrendszert célba vevő neurotudományi technikákra és technológiákra (neuroS/T) utal. Ezek segítségével befolyásolhatóak az élettani funkciók, módosíthatóak az érzelmi állapotok és a mentális képességek, ezzel közvetlenül torzítva a döntéshozatalt.
- Pszichológiai szint (Manipulating Interpretation): Itt a hangsúly az értelmezési keretek, a kognitív értékelés és az érzelmek befolyásolásán van. A mesterséges intelligencia által támogatott műveletek (például a közösségi médiában) a személyes és csoportos sérülékenységeket használják ki a hitek és ítéletek átformálására.

A jelentés alcíme (Sentinel Call) egyfajta „vészjelzésként" értelmezhető. A szerző szerint elkerülhetetlen a kognitív szempontok beépítése a katonai doktrínákba, a tervezésbe és a kiképzésbe. A katonai szervezeteknek fel kell készülniük arra, hogy felismerjék, megelőzzék és elhárítsák a kognitív támadásokat, mivel ezek (már) békeidőben és háborúban is folyamatosan jelen vannak. A NATO stratégiai céljaként a kognitív fölény (*Cognitive Superiority*) elérését jelöli meg. Ehhez nem elegendő az információ feletti uralom, érteni kell az emberi gondolkodás mechanizmusait is. A tanulmány hangsúlyozza az interdiszciplináris kutatások (idegtudomány, mesterséges intelligencia, pszichológia) és az etikai és jogi kormányzási keretek fontosságát a szövetséges erők ellenállóképességének növelése érdekében. A dokumentum kiemeli, hogy a kognitív hadviselés elmossa a határokat a katonai és a polgári szféra között. Mivel a technológia (pl. közösségi platformok) lehetővé teszi a teljes lakosság célzott elérését, a védekezés nem csak katonai feladat, hanem társadalmi ellenállóképességet (resilience) és a civil-katonai együttműködés szorosabbá tételét igényli.[124]

Ezzel szoros összefüggésben fontosnak tartom kiemelni, hogy az információs műveletek hatékonyságát a feltörekvő technológiák (AI, Big Data) fejlődése új szintre emelte.

[124] GIORDANO James (2026): Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness. Strategic Insights, National Defense University. Elérhető: https://inss.ndu.edu/Media/News/Article/4371195/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-operat/ (Letöltés ideje: 2026. 02. 11.)

A mesterséges intelligencia szerepe kettős, hiszen egyrészt az információs támadások gyorsítója (automatizált dezinformáció), másrészt a védekezés elengedhetetlen eszköze (anomália-detektálás).[125] Kiemelt jelentősége van annak is, hogy a modern nemzetbiztonsági döntéshozatal egyre inkább a Big Data alapú elemzésekre támaszkodik. A NATO Science & Technology Organization (STO) kutatásai szerint a Big Data analitika lehetővé teszi az információs környezet felmérését (IEA) olyan pontossággal, amely korábban elképzelhetetlen volt, segítve az ellenfél befolyásolási műveleteinek korai detektálását.[126]

A nemzetbiztonság ezen területén tevékenykedő szakembereknek ébernek kell lenniük, hogy felismerjék és kezelni tudják az új típusú fenyegetéseket, miközben etikai és jogi határokon belül maradnak. Az információs műveletek kulcsfontosságú eszközei a modern nemzetbiztonsági stratégiának. Egyre növekvő jelentőségük miatt elengedhetetlen, hogy a nemzetbiztonsági szakemberek megértsék ezeket a műveleteket és képesek legyenek alkalmazni, illetve védekezni ellenük. Az információ korában a hatalom gyakran abból fakad, hogy ki képes hatékonyabban kommunikálni, manipulálni vagy védeni az információkat[127].

4. Az információs műveletek és tevékenységek szerepének kiemelt jelentőségéről a hibrid hadviseléssel összefüggésben

A hibrid hadviselés és az információs műveletek közötti kapcsolat kulcsfontosságú, hiszen míg az információs műveletek kifejezetten az információs környezet befolyásolására irányulnak, addig a hibrid hadviselés egy tágabb stratégiai keret, amely egyszerre alkalmaz katonai, politikai, gazdasági és információs eszközöket a háborús küszöb alatti célok elérése érdekében. Az összefüggés abban rejlik, hogy az információs műveletek eszköztárának használata a hibrid hadviselés egyik legfontosabb komponenseként szolgálnak, amely képes a társadalmi kohézió megbontására, a döntéshozatal torzítására és az ellenfél legitimációjának gyengítésére. A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban többféle és nem egységes nézőpontot tükröz, amelyeket négy fő csoportba sorolhatunk[128]:

---

[125] NATO STO (2023): Big Data and AI for Military Decision Making.
[126] LUCARELLI Sonia – MARRONE Alessandro – MORO Francesco Niccolò (eds.) (2021): NATO Decision-Making in the Age of Big Data and Artificial Intelligence. Brussels, NATO.
[127] HAIG Zsolt.: Az információs hadviselés kialakulása, katonai értelmezése. *Hadtudomány*, 2011, 1-2. szám, pp 12-28.
[128] SOMODI Zoltán és KISS Álmos Péter. (2019). A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. Honvédségi Szemle – Hungarian Defence Review, 147(6), 22–28. DOI: 10.35926/HSZ.2019.6.2.

- Teljesen újfajta hadviselés: Ez az álláspont úgy tekint a hibrid hadviselésre, mint egy korábban nem létező, új stratégiai szemléletre, amely integráltan használja az állam diplomáciai, információs, katonai és gazdasági, illetve pénzügyi eszközeit. A megközelítés szerint a hibrid hadviselés célja a bizonytalanság keltése, az ellenfél háborúfelfogásának kihasználása és a tevékenység észrevétlen maradása a háborús küszöb alatt.[129]
- Korábban létező elemek újszerű megjelenése: A második csoport szerint a hibrid hadviselés elemei már korábban is jelen voltak, de a mai formájukban mégis újszerű kihívást jelentenek.
- Nincs újdonság: A harmadik csoport szerint a hibrid hadviselés semmilyen újdonságot nem hoz, és nem segít jobban megérteni a 21. század biztonsági környezetét.
- Orosz perspektíva: A negyedik csoport az orosz hadtudományi szemléletet képviseli, amely szerint a hibrid hadviselés a nyugati hatalmak Oroszország elleni stratégiája.

A szakirodalom ezen megközelítései azt mutatják, hogy a hibrid hadviselés fogalma vitatott és sokrétű, és ezek az eltérő értelmezések különböző stratégiai és védelmi megközelítéseket igényelnek a különféle államoktól és nemzetközi szervezetektől.

A hibrid hadviselés fogalmának értelmezése határozza meg azt, hogyan készülünk fel bizonyos fenyegetésekre és milyen következtetéseket vonunk le a körülöttünk zajló konfliktusokból. A hibrid hadviselés sikerének kulcsa az állam hatalmi eszközeinek integrálása és szinkronizálása, valamint az ellenfél – detektálási küszöb, „radarszint" – alatti[130] tevékenységének monitorozása, amelyek lehetővé teszik, hogy a támadások észrevétlenek maradjanak egészen addig, amíg már túl késő hatékonyan védekezni.

Azzal a megközelítéssel, hogy *„a hibrid hadviselés a hagyományos reguláris (lineáris, konvencionális) és az irreguláris (nem lineáris, nem konvencionális) hadviselés puha, közepes és kemény módszereinek, eljárásainak rugalmas alkalmazása abból a célból, hogy az ellenség*

[129] A korábban elemzett NATO (2024.): NATO's approach to counter information threats. NATO Topics, szerint a Hibrid hadviselés – katonai és nem katonai, valamint titkos és nyílt eszközök (beleértve a dezinformációt, a kibertámadásokat, a gazdasági nyomást, az irreguláris fegyveres csoportok bevetését és a reguláris erők alkalmazását) felhasználása a háború és a béke közötti határok elmosására, a célországok lakosságának meggyőzésére, valamint a társadalmak destabilizálására és aláásására.
[130] PORKOLÁB Imre: A hadviselés adaptációja: harc az emberi elméért In.: Hadtudományi Szemle 7: 3 pp. 57-69., 13 p. (2014)

államát, fegyveres erőit működésképtelenné, védtelenné tegyük és akaratunkat rákényszeríthessük, legfőképpen azzal a stratégiai céllal, hogy az erőszak szintje a konfliktus folyamán ne haladja meg a háborús szintet"[131] kellő alapossággal igyekszünk körülírni a fogalmat, ugyanis a rugalmasság és a statikusan[132] nem definiálható jellemzőit emeljük ki.

A hibrid hadviselés a NATO és az Európai Unió megközelítésében olyan stratégia, amely szimultán alkalmazza a katonai, gazdasági, politikai és információs eszközöket, a hagyományos konfliktus küszöbe alatt maradva. Az információs műveletek ebben a környezetben a társadalmi kohézió megbontását, a döntéshozatal befolyásolását és az ellenfél legitimációs bázisának gyengítését szolgálják. A legújabb hibrid fenyegetésekről szóló elemzések hangsúlyozzák, hogy a hibrid fenyegetések elleni fellépés kulcsa a reziliencia növelése és a kognitív védelem megerősítése. A jelen kontextusban, ahol a politikai befolyásolás mechanizmusait is vizsgálom, indokoltnak tartom is az információs műveletek és tevékenységek szerepét a politikai hatalomgyakorlásra kifejtett aspektusain keresztül is elemezni[133] és mivel az információs műveletek és tevékenységek kulcsfontosságú szerepet töltenek be ebben a kontextusban, ugyanis lehetővé teszik a narratívák alakítását, a közvélemény befolyásolását, és így hozzájárulnak a hibrid hadviselés sikeréhez.

A hibrid hadviselés és az információs műveletek összekapcsolódása egyre inkább meghatározó jellemzője a modern konfliktusoknak. A hibrid hadviselés egy olyan stratégia[134], amely a katonai és nem katonai eszközök, köztük az információs műveletek kombinációját használja a cél eléréséhez. [135] A hibrid hadviselés lényege, hogy ötvözi a hagyományos katonai erő alkalmazását a nem hagyományos eszközökkel, mint például a kiberműveletek, illetve az

[131] RESPERGER István: A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In RESPERGER István [szerk.]: A nemzetbiztonság elmélete a közszolgálatban. Budapest, Dialóg Campus, 2018. 84–85.

[132] Hagyományos kifejezésekkel nehezen írható le a jelenség, mindazonáltal a hibrid jelző, amely több, különkülön értelmezhető, felismerhető jellemző egyidejű meglétét feltételezi, valamint a változás állandó jellege miatt nem is feltétlenül skatulyázható be a cselekvéssorozat. Ha egzakt, már meglévő pozitív logikai definíciós elemekből összeállítható kifejezést lehetne alkotni rá, elveszítené hibrid jellegét és hívhatnánk akár harc nélküli harcnak is.

[133] KOVÁCS László, KRASZNAY Csaba: „Mert övék a hatalom": Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során In.: Nemzet és Biztonság–Biztonságpolitikai Szemle 10 (3), 3–15

[134] RESPERGER István: A válságkezelés és a hibrid hadviselés, Budapest, Dialóg Campus Kiadó, 2018, 14. o.

[135] FARKAS Ádám – RESPERGER István: Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai In.: FARKAS Ádám - VÉGH Károly (szerk.) Új típusú hadviselés a 21. század második évtizedében és azon túl - Intézményi és jogi kihívások, Budapest, Zrínyi Kiadó, 2020, pp. 132.-149. ISBN 978 963 327 800 0

információs műveletek, az illegális fegyveres csoportok támogatása, vagy a gazdasági és politikai befolyásolás. [136]

Az információs műveletek fontos szerepet játszanak ebben a folyamatban. Az információs műveletek egyes intézkedéseinek célja lehet, hogy befolyásolják az emberek érzéseit, véleményét és döntéseit, így alakítva a közvéleményt és az idegen hatalom döntéshozóit. Például egy hibrid konfliktusban az információs műveletek segíthetnek abban, hogy felerősítsék a zűrzavart, hiteltelenítsék az ellenfél vezetőit, vagy megkérdőjelezzék annak legitimációját.[137] Ezáltal gyengítik az ellenség morálját és növelik a saját befolyásukat a célközönség körében. A közösségi média és más online platformok lehetővé teszik az adatok, illetve hírek gyors és széles körű terjesztését, ami felgyorsíthatja és felerősítheti az információs műveletek hatását. A digitális korban a tájékoztatás és befolyásolás módszerei jelentősen megváltoztak. A közösségi média és az online platformok lehetővé teszik az információk gyors terjesztését, ami lehetőséget biztosít a széles körű befolyásolásra, de egyben kihívást is jelent az információk minőségének és hitelességének fenntartásában. Az EU East StratCom Task Force 2015 óta aktívan monitorozza és ellensúlyozza az oroszbarát dezinformációs kampányokat, rendszeresen publikálva a „Disinformation Review" jelentéseket. A NATO keleti szárnyának megerősítése során a stratégiai kommunikáció kulcsszerepet játszott a helyi lakosság megnyugtatásában és a tagállamok közötti szolidaritás erősítésében, a COVID-19 járvány idején a NATO és az EU StratCom egységei közös kommunikációs kampányokkal igyekeztek ellensúlyozni a járvánnyal kapcsolatos álhíreket, melyek közül a 1. sz. Mellékletben emeltem ki releváns példákat. A hibrid hadviselés és az információs műveletek kombinációja különösen hatékony az aszimmetrikus konfliktusokban, ahol a hagyományos katonai erőfölény nem feltétlenül jelent előnyt. Az ilyen eszközök alkalmazása révén a gyengébb fél képes kompenzálni technológiai vagy katonai hátrányait, és befolyásolni az erősebb fél politikai és

[136] PORKOLÁB Imre: Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? In: Hadtudomány 25 (3–4): pp. 36–48. Porkoláb Imre cikkében a hibrid hadviselés fogalmát és jellemzőit elemzi. Megállapítja, hogy bár új hadviselési formának tűnik, valójában a korábbi hadviselési módszerek és eszközök újszerű kombinációjáról van szó. A szerző szerint a hibrid hadviselés lényege, hogy katonai és nem katonai eszközöket, nyílt és titkos műveleteket, szabályos és szabálytalan harcászatot, valamint különböző erőszak-szinteket kombinálva törekszik az ellenség befolyásolására és akaratának megtörésére. Bár újnak tűnhetnek az alkalmazott eszközök és módszerek, valójában a hadviselés történetében korábban is léteztek hasonló példák. A tanulmány rámutat, hogy a hibrid hadviselés inkább a korábbi hadviselési formák továbbfejlesztése és a 21. századi technikai lehetőségek kiaknázása, semmint teljesen új jelenség. Ugyanakkor alkalmazása komoly kihívások elé állítja a modern haderőket.

[137] SIMICSKÓ István: A hibrid hadviselés előzményei és aktualitásai. *Hadtudomány*, XXVII. évf. 2017/3–4., 3–16. o. DOI: 10.17047/HADTUD.2017.27.3–4.3

társadalmi stabilitását.[138] Ezzel összefüggésben indokolt megjegyezni, hogy a katonai pszichológia egyik kiemelt feladata, hogy felkészítse az állományt a küzdelemre, ideértve az ellenállóképességet[139] is. A mentális állóképesség fejlesztése kulcsfontosságú lehet a konfliktusok és válsághelyzetek során. A Stoltz-féle mentális állóképességi koncepció szerint a magas mentális állóképességgel rendelkező személyek jobban képesek kontrollálni a stresszes helyzeteket, kevésbé érzik őket megterhelőnek vagy félelmetesnek. Ezek az egyének felelősséget éreznek a helyzetek kezeléséért, reálisan látják a körülményeket, és képesek fenntartani a kontroll érzését. A nehézségeket ideiglenes problémaként kezelik, és nem engedik, hogy a stressz hatása átterjedjen életük más területeire. Mindez hozzájárul az ellenséges befolyásolási kísérletek elleni védelemhez és csökkenti a propaganda hatékonyságát[140]. Ez a

[138] KESZELY László. A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modellje. Honvédségi Szemle 2020. 4., pp. 24-48. DOI: 10.35926/HSZ.2020.4.3. A publikációban KESZELY László megállapítja, hogy a hibrid hadviselés összetett és komoly kihívást eredményező jelenség, nehéz meghatározni, és rendkívül nehéz védekezni ellene. A hibrid hadviselést gyakran gyengébb államok használják erősebb államok ellen. Ez egy viszonylag alacsony költségű és nagy hatású hadviselési forma. A hibrid hadviselésnek súlyos következményei lehetnek, mint például az eszkalálódás kockázata a hagyományos (kinetikus) hadviselésbe. Fontos megérteni a hibrid hadviselést, hogy hatékony stratégiákat fejlesszünk a védekezéshez. KESZELY által javasolt kormányzási modell fontos támpontot nyújthat a hibrid hadviselés ellensúlyozásának vitájához. Fontos azonban megjegyezni, hogy számos kihívást kell leküzdeni annak érdekében, hogy ezt a modellt megvalósítsuk. Az egyik legnagyobb kihívás az lenne, hogy a különböző szereplők hatékonyan működjenek együtt. A „fegyveres hivatásrendeket tömörítő szervek", a kormányzat és a magánszektor gyakran eltérő prioritásokkal és célokkal rendelkezik. Gyakran tapasztalható, hogy nehézséget okoz egy közös cél érdekében együttműködniük. Másik kihívás az lenne, hogy biztosítsuk, hogy a kormányzási modell elég rugalmas legyen ahhoz, hogy alkalmazkodjon a hibrid hadviselés változó jellegéhez. A hibrid hadviselés folyamatosan fejlődő jelenség, és nehéz lenne olyan kormányzási modellt kifejleszteni, amely lépést tartana a változásokkal.

[139] HORNYÁK Beatrix: A mentális állóképesség fejlesztése, mint lehetséges védelmi jellegű lélektani művelet In.: Hadtudományi Szemle 2016. IX. évfolyam 1. szám pp. 235-246.

[140] NATO ACT. (2023). *Cognitive Warfare: Strengthening and Defending the Mind.* A NATO ACT által publikált, „Cognitive Warfare: Strengthening and Defending the Mind" című dokumentum kiemeli a kognitív hadviselés (cognitive warfare) egyre növekvő jelentőségét a modern konfliktusok dinamikájában. A kognitív hadviselés nem csupán az információk manipulálását vagy a közvélemény alakítását célozza, hanem mélyebb stratégiai szinten az egyének gondolkodási folyamatainak és döntési képességeinek befolyásolását vagy gyengítését is. Ez a megközelítés az emberi agyat, mint csatatérként értelmezi, ahol a pszichológiai, kulturális, információs és digitális eszközök révén zajlik a küzdelem. A publikáció hangsúlyozza, hogy a kognitív hadviselés eszköztára széles és komplex. Ebbe beletartozik a dezinformáció terjesztése, a pszichológiai nyomásgyakorlás, a jogi hadviselés és a digitális technológiák, például a közösségi média platformok manipulációja is. A NATO ACT elemzése szerint ezek a módszerek gyakran láthatatlanok maradnak a célpont számára, ugyanakkor mélyreható destabilizáló hatással bírnak a társadalmakra, politikai rendszerekre és intézményekre. Elrettentő példaként említi azokat az állami és nem állami szereplőket, amelyek szisztematikusan alkalmazzák ezeket a technikákat a NATO szövetségeseivel szembeni közbizalom megingatására és stratégiai pozícióik aláásására. A dokumentum különös figyelmet fordít arra, hogy a kognitív hadviselés nem önálló jelenség, hanem egy átfogó, többdimenziós hadviselési stratégia része. Ez a stratégia integrálja a politikai, gazdasági és katonai hatalmakat, amelyek szinergiában működnek együtt a kognitív térben. Mindez a modern hadviselés egyik új paradigmajaként jelenik meg, amely túllép a hagyományos fizikai konfliktusokon és az információs hadviselésen. A NATO Allied Command Transformation rámutat arra, hogy a szövetség válasza ezen új típusú fenyegetésekre komplex és sokrétű. Ezek között szerepel a fenyegetések azonosítása és értékelése, a stratégiai kommunikáció fejlesztése, valamint olyan mechanizmusok kidolgozása, amelyek képesek megvédeni az egyének és közösségek mentális és döntéshozatali kapacitását. Az ACT szerint az „emberi agy védelme" kulcsfontosságú cél, amely nemcsak katonai, hanem társadalmi szinten is prioritást kell, hogy élvezzen. Ennek érdekében a NATO a stratégiai ellenálló képesség (resilience) növelésére, illetve a döntéshozatali mechanizmusok védelmére helyezi a hangsúlyt. A dokumentum

megközelítés, amely a mentális állóképesség fejlesztését helyezi előtérbe, nemcsak a katonai környezetben, hanem a polgári szférában is alkalmazható, különösen a nehezen kivédhető, illetve megszűrhető digitális propagandahadjáratok korában. Az ilyen típusú képzések és előkészületek biztosítják, hogy az egyének fel legyenek készülve a kihívásokra, és képesek legyenek hatékonyan reagálni az ellenséges információs támadásokra.

A hibrid hadviselés és az információs műveletek kombinációja lehetővé teszi a konfliktusban álló felek számára, hogy kihasználják az ellenség gyengeségeit, minimalizálják saját sebezhetőségüket, és elérjék stratégiai céljaikat anélkül, hogy hagyományos háborúba bonyolódnának.[141] Kiemelt figyelmet érdemes fordítani az új típusú fenyegetések elleni küzdelem[142] során ezen jellemzőkre, valamint mindezekkel összefüggő jogi és szabályozási kérdésekre.[143] Ez (is) indokolta Magyarország 2019-es csatlakozását a Helsinki székhelyű

kifejti, hogy a kognitív hadviselés új kihívást jelent a NATO számára, amelyhez adaptív, interdiszciplináris megközelítés szükséges. Ez magában foglalja a katonai tervezés megerősítését, az oktatás és képzés szerepének kiemelését, valamint a szövetségesek közötti szorosabb együttműködést a kognitív térben jelentkező fenyegetések hatékony kezelésére. A NATO ACT célkitűzése, hogy megerősítse az egyének és a közösségek ellenállóképességét, miközben kialakítja azokat az eszközöket és stratégiákat, amelyek képesek elhárítani az idegen kognitív (had)műveletek hatásait.

[141] CULLEN, Patrick: *Hybrid threats as a new „wicked problem" for early warning,* Helsinki, The European Centre of Excellence for Countering Hybrid Threats, 2018.

[142] SZENES Zoltán: A hibrid fenyegetések elleni szakpolitika Magyarországon In.: HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 31 : 4 pp. 39-56. , 18 p. (2021). A publikáció rámutat, hogy az elmúlt évtized során a hibrid hadviselés újszerű biztonsági kihívásként, veszélyforrásként és fenyegetésként került előtérbe, meghatározó szerepet vállalva ezzel a nemzeti és szövetséges biztonságpolitikai stratégiák formálásában. A publikáció a hibrid veszélyekkel szembeni nemzeti politikai intézkedések kialakítását és fejlődési ívét elemzi Magyarországon. Az elemzés stratégiai irányelvekre és jogszabályokra támaszkodva mutatja be a védelmi intézkedések két szintű megközelítését, amely egyrészről a nemzetközi, különösen az Európai Unió és a NATO-val való együttműködésre, másrészről a nemzeti szintű infrastruktúra lépésről-lépésre történő kiépítésére alapoz. Kifejti a hibrid fenyegetések magyarországi értelmezését, a szövetségi együttműködés hazai fejlődésének hatásait és eredményeit. A szakpolitika dinamikus alakulása 2016 és 2021 között figyelhető meg, amit a névtelen szereplők által indított hibrid támadások tapasztalatai, a felhasznált eszközök típusai, a hibrid cselekvések területei és a védelmi képességek fejlesztésének lehetőségei befolyásoltak. A tanulmány alaposan értékeli a nemzetközi szinten is jelentős kibervédelmi tevékenységet, bemutatja az állami és társadalmi ellenállás megerősítésére irányuló terveket. Vizsgálat tárgyává teszi a nemzeti válságkezelési rendszer hibrid támadásokkal szembeni irányítási és vezetési hatékonyságát, támogatva a külső és belső biztonság krízismanagementjének integrációjára irányuló szakértői javaslatokat, mint a komplex hibrid támadások kezelésére legalkalmasabb megközelítést. Hangsúlyozza, hogy a hibrid támadási spektrumhoz igazodva további védelmi lehetőségeket kell kiterjeszteni, a kibervédelemhez hasonlóan más területeken is rendszerszerű fejlesztésekre van szükség. Az elemzés arra a következtetésre jut, hogy mindehhez elengedhetetlen egy nemzeti hibrid stratégia kidolgozása és elfogadása.

[143] Az új típusú hadviselés a 21. század második évtizedében és azon túl számos intézményi és jogi kihívást vet fel. A modern hadviselés jellemzően magában foglalja a kiberműveleteket támadásokat, az információs műveleteket, az autonóm fegyverrendszereket és a hibrid hadviselési technikákat, amelyek mind komoly kérdéseket vetnek fel a nemzetközi jog és a különböző nemzetek belső jogrendszerei szempontjából. Az új típusú konfliktusokra való felkészülés érdekében a kormányzati és nemzetközi intézményeknek meg kell vizsgálniuk és szükség esetén módosítaniuk kell a meglévő jogi keretrendszereket, beleértve a genfi és hágai egyezményeket, amelyek a háborúkban viselkedés szabályait határozzák meg. Különös figyelmet kell fordítani az emberi jogok tiszteletben tartására, a civil lakosság védelmére, valamint a nem katonai infrastruktúra elleni támadások

Hibrid Fenyegetések Elleni Európai Kiválósági Központhoz (Hybrid CoE), amelynek fő feladata a partnerországok közötti stratégiai együttműködés elősegítése, hibrid fenyegetésekkel kapcsolatos elemzések és kutatások végzése. A Kiválósági Központ éves szinten határozza meg prioritásait és a támogatott munkafolyamatokat. A Központ kezdeményezései közé tartozik a hibrid fenyegetésekkel szembeni tudatos fellépés – jelenleg például a tengeri hibrid fenyegetések vizsgálata –, a vegyi, biológiai, radiológiai és nukleáris kihívások kezelése, koherens stratégiai kommunikáció, az ellenséges hírszerző tevékenységekkel szembeni védekezés, valamint a kiberbiztonság és a reziliencia megerősítése terén.[144]

5. Összegzés, részkövetkeztetések

A fejezet az információs műveletek normatív hátterét, doktrinális fejlődését és a hibrid hadviseléshez való kapcsolódását elemzi három tematikus egységben. Az első alfejezet az információs műveletek fogalmi keretrendszerét tárgyalja a NATO AJP-10.1 doktrína alapján. Megállapítja, hogy a modern műveleti környezetben az információs fölény a „szembenálló akaratok összecsapásának" döntő tényezőjévé vált, a konfliktusok pedig egy versengési skálán mozognak az együttműködéstől a fegyveres konfliktusig. A NATO az információt közös törzskari funkcióként kezeli, az információs fenyegetések körét – a dezinformációt, a propagandát és a külföldi információmanipulációt – pontosan elhatárolja a szándékos manipuláló elemet nélkülöző téves információtól. A második alfejezet a 2023-as doktrinális paradigmaváltást vizsgálja, összehasonlítva a hatályon kívül helyezett AJP-3.10-et az új AJP-10.1-gyel. A váltás legfontosabb eleme az Info Ops átsorolása a műveleti ágból az információs-kommunikációs ágba, a Stratégiai Kommunikáció alárendeltségébe, valamint egy részletes képesség-taxonómia bevezetése, amely három csoportba rendezi a releváns képességeket: kommunikációs képességeket, kiegészítő képességeket és az engagement-alapú elemeket. A

korlátozására. A nemzetközi jog alkalmazkodása az új típusú hadviseléshez magában foglalhatja az új szabályozások létrehozását, a meglévő egyezmények kiterjesztését vagy értelmezésének finomítását, valamint az új technológiák által felvetett specifikus kérdésekkel foglalkozó egyedi szabályok bevezetését. Például az autonóm fegyverrendszerek (pl. drónok és robotok által végrehajtott támadások) felvetik a felelősség kérdését: ki felelős, ha egy gép hibásan hajt végre egy támadást? Ezenkívül a kiberműveletek, mint például a választásokba való beavatkozás vagy az infrastruktúra elleni támadások, új területeket nyitnak meg a nemzetközi konfliktusokban, amelyekre a jelenlegi jogszabályok nem feltétlenül készültek fel. A kihívások kezelése érdekében az egyes országoknak együtt kell működniük a nemzetközi közösséggel, hogy közös megoldásokat találjanak. A nemzetközi szervezeteknek, mint például az ENSZ-nek, továbbra is központi szerepet kell játszaniuk a párbeszéd előmozdításában és az új normák és szabályok kidolgozásában. Az új típusú hadviselésre való reagálás során a jogalkotóknak és intézményeknek proaktívan kell cselekedniük annak érdekében, hogy megfelelően kezeljék ezeket a kihívásokat, miközben fenntartják a nemzetközi béke és biztonság alapelveit.

[144] SZENES Zoltán: A hibrid fenyegetések elleni szakpolitika Magyarországon In.: HADTUDOMÁNY: A MAGYAR HADTUDOMÁNYI TÁRSASÁG FOLYÓIRATA 31 : 4 pp. 39-56. , 18 p. (2021).

doktrinális transzformáció eredményeként a NATO a kognitív integritást a kollektív védelem részévé tette. A védekezéshez elengedhetetlen az etikai-jogi keretek kidolgozása, különösen a neurotechnológiák és a mesterséges intelligencia fúziója esetén. A harmadik és negyedik alfejezet a kognitív hadviselés és a hibrid hadviselés összefüggéseit tárgyalja. A kognitív hadviselés az emberi észlelés és döntéshozatal biológiai-pszichológiai szintű befolyásolását célozza, a mesterséges intelligencia és a Big Data által felerősített eszközökkel. A hibrid hadviselés kontextusában az információs műveletek a társadalmi kohézió megbontásának, a legitimáció gyengítésének és a döntéshozatal torzításának elsődleges instrumentumaivá válnak, amelyek ellen a reziliencia és a kognitív védelem megerősítése jelenti a leghatékonyabb védelmi stratégiát.

Az információs műveletek és tevékenységek vizsgálata során megállapítottam, hogy a hibrid hadviselés eszközrendszerébe illeszkedő, az információs tevékenységek közé tartozó, egyes intézkedések, illetve intézkedéssorozatok jelentős hatást fejtenek ki a célzott állam, illetve közösség döntéshozóira, illetve jogi normaalkotóira. A célzott hatás kifejtése érdekében információs műveletek precíz alkalmazása kerül végrehajtásra kiemelten a közvélemény befolyásolása útján, különösen a kibertérben továbbított közlések által. Ezen megállapításaim (a jogi hadviselés specifikumával kiegészítve a III. fejezetben) a 4. számú hipotézis alátámasztására alkalmasnak tekinthetők, ezt a hipotézist kívánják megerősíteni.

A hibrid hadviselés és az információs műveletek kapcsolata kulcsfontosságú a modern biztonságpolitikai és katonai gondolkodásban. Míg az információs műveletek elsősorban az információs környezet manipulálására és a kognitív tér befolyásolására összpontosítanak, addig a hibrid hadviselés egy szélesebb stratégiai keretet képvisel, amely egyszerre vonja be a katonai, politikai, gazdasági és információs eszközöket a háborús küszöb alatti célok eléréséhez. E két terület összefonódása lehetővé teszi, hogy az információs műveletek a hibrid hadviselés egyik meghatározó komponenseként gyengítsék az ellenfél társadalmi kohézióját, torzítsák a döntéshozatali folyamatokat, valamint aláássák annak legitimációját. A kognitív képességekre épülő jogi hadviselés (lawfare) szintén szoros kapcsolatban áll ezekkel a folyamatokkal, mivel az információs műveletekkel együttműködve képes hatást gyakorolni a közvéleményre és a politikai döntéshozatalra. Az online platformok, közösségi média és hagyományos médiumok bevonása révén ezek a technikák egyszerre szolgálhatják a tájékoztatás, a befolyásolás és a dezinformáció céljait. A műveletek célba vehetik az adott államban vagy közösségben élő személyek összességének hangulatát, igazságérzetét, a jogállam(iság)ba vetett hitét, illetve

ezekkel összefüggésben a rendkívüli mértékben befolyásolhatja a világról alkotott képét. A világkép írott és íratlan normakörnyezete a demokráciákban nem ütközik a lakosság többségének igazságérzetével, emiatt kimondottan fontos, hogy a normakörnyezetre vonatkozó észlelés esetleges idegen érdekű befolyásolását detektáljuk, a jogi hadviselés ezen jellemzőit képesek legyünk felismerni.

Az információs tevékenységek alkalmazása – különösen a kognitív és jogi dimenziók bevonásával – olyan összetett eszköztárat kínálhatnak, amely stratégiai előnyt biztosít a 21. század komplex, hibrid biztonsági kihívásainak kezelésében. A hibrid intézkedéssorozatok eme kifinomult fegyverét ennek okán vetettem részletes vizsgálat alá a következő fejezetben.

III. A JOGI HADVISELÉS JELENTŐSÉGÉNEK ELMÉLETI MEGKÖZELÍTÉSE ÉS FOGALMÁNAK EVOLÚCIÓJA

1. A jogi hadviselés kifejezés tudományos megközelítése

A „lawfare" kifejezés viszonylag újkeletű, de a fogalom és a jellemzői meghatározása gyorsan a vita középpontjába került. Nincs egységes meghatározása a lawfare-nek, de általában a jog eszközként való felhasználására utal a kinetikus, illetve nem kinetikus háborúban. Ez okozza a különleges kétarcúságát is. Hiszen magában foglalhatja a katonai fellépés jogi érvekkel való igazolását, vagy a jogi eszközök használatát egy ellenséges kormány aláásására[145].

A lawfare fogalmát eredetileg szigorúan katonai kontextusban használták, azonban az Egyesült Államokban a nagyközönség helytelenül alkalmazza, ami nagyrészt a Bush-kormányzat idején megjelent véleménycikkeknek és sajtóelemzéseknek köszönhető. Egyes újság- és blogcikkek a guantánamói fogolytáborokra vagy a terrorizmus elleni háborúra hivatkozva használták a kifejezést. Különösen elterjedt volt a fogvatartottakkal való bánásmódról és a jogi tanácsadáshoz való jogról szóló vitákban, minek eredményeként – a sajtóban és a széles társadalom előtt zajló diskurzusban – bizonyos jogvédő csoportok

[145] MARTINS, M. (2010): Reflections on „Lawfare" and Related Terms. *Lawfare*, 2010. november 24.

tevékenységével összefüggésben felmerült, hogy az a nemzeti érdekekkel potenciálisan ütközhet, ami a hibrid hadviselésben új értelmezési kereteket nyit.

Mark Martins három, egymást átfedő értelmezést írt le a „jog, mint háborús fegyver" meghatározásra[146]. Az első szerint a lawfare igazságtalanul kihasználja, hogy az ellenség betartja a szabályokat, a másik fél viszont nem - ez a gyengébb fél stratégiája. A második értelmezés metaforikusan a jogi érvelést tekinti háborúnak, ahol nem katonák, hanem eszmék csapnak össze. A harmadik szerint a lawfare a felkelés legyőzését célzó műveletek egyik legfontosabb eszköze, amely egy legitim és tekintélyes jogrendszeren keresztül védi a lakosságot és bizonytalanságot kelt a lázadókban - ebben a formájában a lawfare pozitív és az erősek stratégiája. A disszertáció által alkalmazott értelmezés a lawfare-t elsősorban a hibrid hadviselés eszközeként kezeli, összhangban a Martins által kidolgozott osztályozási kerettel. Ugyanakkor szükséges rámutatni, hogy a szakirodalomban a lawfare fogalmának több rétege is létezik. A szűkebb megközelítés a jog tudatos, célzott alkalmazását tekinti nem konvencionális konfliktusok során a stratégiai előny megszerzése érdekében. A tágabb értelmezés ennél szélesebb, és a jog eszközként való felhasználását bármely fegyveres konfliktusban vizsgálja, ideértve a hagyományos államközi háborúkat is. Jelen munka az előbbit helyezi a középpontba, miközben a történeti előzményekre reflektálva elismeri a jog eszközkénti szerepének hosszú fejlődési ívét. [147] [148]

Kittrie meghatározása szerint a lawfare „a jogszabályok, jogi fórumok és peres eljárások stratégiai, állami szintű alkalmazása az ellenséges érdekek gyengítésére vagy saját célok előmozdítására". [149] A szerző rámutat arra, hogy a feltörekvő hatalmak (Kína, Oroszország) tudatosan fordítják a nemzetközi jogot a nyugati államok ellen, különösen a kereskedelmi és emberi jogi mechanizmusok területén.

A Finkelstein és Rosen szerint a lawfare „az emberi jogi diskurzus fegyverként történő alkalmazása politikai célok elérése érdekében". Megállapításuk szerint az emberi jogi

[146] MARTINS, M. (2010): Reflections on „Lawfare" and Related Terms. *Lawfare*, 2010. november 24.
[147] Kennedy, D. (2012): Lawfare and Warfare. In: Crawford, J. – Koskenniemi, M. (szerk.): The Cambridge Companion to International Law. Cambridge University Press, Cambridge, 158–183.
[148] HOFFMAN, Frank G.: Hybrid Warfare and Challenges. In: Joint Force Quarterly, Issue 52, 1st quarter 2009, 34–39. o.
[149] Kittrie, O. F. (2016): Lawfare. Law as a Weapon of War. Oxford University Press, New York.

mechanizmusokat és normákat egyes államok és nem állami szereplők politikai befolyásszerzésre és az ellenfelek delegitimálására használják fel.

Fontos kiemelni azonban, hogy ezek a jelentések átfedik egymást és belső feszültségeket is hordoznak - például az igazságosság meghatározásának nehézségei a háborúban, a jog eszközként való használatának veszélyei, illetve a puszta szócsaták sebezhetősége. Összefoglalva, a lawfare fogalma vitatott és sokrétű, egységes meghatározása nehézkes.

Számos oka van annak, hogy a lawfare miért vált gyakoribbá az elmúlt években. Az egyik ok a modern hadviselés növekvő bonyolultsága. A múltban a háborúk gyakran két hadsereg között zajlottak a csatamezőn. Ma a háborúk gyakran államok és nem-állami szereplők között zajlanak, és széles körű tevékenységeket foglalnak magukban, beleértve a terrorizmust, kiberháborút és gazdasági szankciókat. Ebben a bonyolult környezetben a jog különféle katonai és politikai célok elérésének eszközeként használható.

A lawfare terjedésének másik oka a jog egyre növekvő szerepe a nemzetközi kapcsolatokban. A múltban a nemzetközi jogot gyakran gyenge és hatástalan eszköznek tartották. Az elmúlt években azonban a nemzetközi jog megerősödött, és egyre inkább az államok viselkedésének szabályozására használják. Ez megnehezítette az államok számára, hogy a jog figyelmen kívül hagyásával cselekedjenek, és szintén nehezebbé tette számukra, hogy önvédelemre hivatkozva igazolják tetteiket.

A lawfare használata valószínűleg tovább fog növekedni a jövőben. Ahogy a világ egyre összetettebbé válik, és a jog egyre fontosabb szerepet játszik a nemzetközi kapcsolatokban, az államok egyre inkább a jogot fogják céljaik elérése érdekében eszközként használni. Ez számos jogi és politikai kihívást fog felvetni. Fontos lesz olyan mechanizmusok kialakítása, amelyek biztosítják, hogy a lawfare használata összhangban legyen a jogállamiság elvével, és ne veszélyeztesse az államok képességét a konfliktusok békés rendezésére. A lawfare használata éppen emiatt rendkívül vitatott megítélésű. Egyesek szerint legitim eszköz, amely fontos célok elérésére használható. Mások szerint a jogi hadviselés egy formája, amely aláássa a jog uralmát és megnehezíti a konfliktusok békés rendezését.

Az Ukrajnában Oroszország által – 2014-ben – kirobbantott konfliktusban a lawfare fontos szerepet játszik, mivel a konfliktus meghatározatlanságára, vagyis arra épít, hogy nem

világos, nemzetközi vagy nem nemzetközi fegyveres konfliktusról, netán polgári zavargásokról van szó. Ez a helyzet bizonytalanságot teremt a vonatkozó jogforrás és az esetleges jogi felelősségre vonás terén[150].

Mivel Oroszország tagadja a konfliktusban való aktív részvételét, a jus ad bellum szabályait megkerüli és félrevezetően alkalmazza.[151] Ez a „modern" hibrid háborúk esetében nemcsak a nemzetközi békét és biztonságot veszélyezteti, hanem a nemzetközi jogi kereteket is képes aláásni. Ennek eredménye a nemzetközi jog és bírósági eljárások retorikus felhasználása, ami kiüresíti a nemzetközi humanitárius jogot és az emberi jogokat, miközben azt a látszatot kelti, hogy a jog betartása ellentmondásban áll a konfliktusban résztvevő felek (jogos) érdekeivel.

Példaként említhető ezzel összefüggésben az 1994-es Budapesti Memorandum, amely kimondta Ukrajna területi integritásának és szuverenitásának tiszteletben tartását. Ennek ellenére Oroszország 2014-ben annektálta a Krímet, majd kelet-ukrajnai szakadár erőket támogatott. A kézirat lezárásakor kinetikus műveleteket folytat Ukrajna területén. A külügyminisztérium szóvivője szerint azonban Oroszország betartotta a memorandum rendelkezéseit, hiszen egyetlen lövés sem dördült el Ukrajna területén, az ország területi integritásának megsértése belső – jogszerű – folyamatok eredménye. Ez a kijelentés a komplex hibrid intézkedéssorozat során alkalmazott dezinformációs művelet részeként értelmezhető,

[150] BACHMANN, Sascha Dov – MOSQUERA, Andres B. Munoz: Lawfare and hybrid warfare – how Russia is using the law as a weapon, in Amicus Curiae – Journal of the Society for Advanced Legal Studies, Summer 2015, 25–28. o. Sascha Dov Bachmann egy nemzetközi jog szakterületén kutató egyetemi docens (Bournemouth-i Egyetem); jogi diplomát szerzett (Ludwig-Maximilians Universität, München), Assessor Jur, LL.M (Stellenbosch), LL.D (Johannesburg). Az akadémiai tevékenységen kívül különböző területeken próbálhatta ki magát, mint (tartalékos) alezredes részt vett békefenntartó missziókban műveleti és tanácsadói minőségben. A részt vett a NATO 2011-es Hibrid Fenyegetés Kísérletében, mint a NATO Jogállamiság Témában Illetékes Szakértője (SME), valamint kapcsolódó műhelymunkákban a NATO-nál és nemzeti szinten. A 2011-es Hibrid Fenyegetés Kísérlettel összefüggésben lásd: Brynen, R. (2011, May 15*). Countering Hybrid Threats: An After Action Report. PAXsims.* (Elérhető:: https://paxsims.wordpress.com/2011/05/15/countering-hybrid-threats-aar/ Letöltve: 2023. október 11.). Mosquera, Andres B. Munoz: a Fletcher Jogi és Diplomáciai Iskolában (Tufts Egyetem) végzett, a Madridi Ügyvédi Kamara, az Európai Ügyvédek CCBE és a Legfelsőbb Szövetséges Erők Európai Parancsnoksága (SHAPE) jogi tanácsadói szervének munkatársa.

[151] RÁCZ, András: Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist, Helsinki, Finnország : Finnish Institute of International Affairs (2015), 101 p. ISBN: 9789517694537. Rácz András cikkében azt állítja, hogy Oroszország hibrid háborúja Ukrajnában egy új típusú hadviselés, mely a hagyományos katonai műveleteket nem-konvencionális módszerekkel - kiberhadviseléssel, dezinformációval és gazdasági hadviseléssel - kombinálja. Szerinte az orosz hibrid háború célja az ellenség ellenálló képességének megtörése káosz és zűrzavar előidézésével, valamint politikai akaratának aláásásával. Rácz részletes elemzést ad az orosz hibrid háborúról Ukrajnában, és azt állítja, Oroszország részben el is érte céljait. Sikerült destabilizálnia Ukrajnát és gyengítenie a kormány ellenálló képességét. Rácz végül amellett érvel, hogy a Nyugatnak új stratégiákat kell kidolgoznia az orosz hibrid háború ellensúlyozására. Úgy véli, fel kell készülnie a hibrid hadviselés kihívásaira és új módszereket kell találnia Oroszország visszatartására a jövőbeli hibrid háborúktól.

amelynek egyértelmű célja a nyugati közvélemény megtévesztése, illetve befolyásolása volt. A szerződések ilyen rosszhiszemű értelmezése ugyanis jogi értelemben szerződésszegésnek minősül (abus de droit).

Putyin elnök kijelentése, miszerint Oroszországnak joga volt a külföldön élő oroszajkúak jogainak védelmére intervenciót indítani, szintén a lawfare alkalmazásának kiváló példája. A tanulmány két esetben mutatja be Oroszország joggal való visszaélését, és amellett érvel, hogy bármely orosz állítás az Ukrajnában való katonai beavatkozás jogáról bizonyítania kellene annak sürgősségét és alternatívák hiányát. Ehelyett Oroszország tagad minden beavatkozást, és a „hihető tagadás[152]" taktikáját alkalmazza.[153]

Ez azt mutatja, hogy a nemzetközi megállapodások szándékos, körülményes értelmezése a jóhiszeműség hiánya, amely visszaélésnek minősül és nemzetközi jogi felelősséget vonhat maga után Oroszország vagy más államok részéről a szakadárok támogatása miatt.[154]

A jogi hadviselés definíciójának rendkívül értékes, előbbiekhez képest eltérő megközelítését tartalmazza az NGO Monitor Nemzetközi Jogi Központ 2008 szeptemberében készült jelentése az „izraeli-arab konfliktusban a bíróságok kihasználásáról". A jelentés a jogi hadviselés kritikájának[155] jellegzetes témáit és nyelvezetét szemlélteti:

„Ezek a jogi lépések, látszólag az „igazságszolgáltatás" és az „áldozatok" érdekében, a jog „fegyverkénti használatának" formái - amelyek célja Izrael megbüntetése a terrorizmus elleni műveleteiért, valamint a jövőbeni akciók megakadályozása. Egyúttal olyan eszközt

[152] A hivatkozott mű „nagy hazugság" kifejezését, a magyar szakmai nyelvezetnek megfelelő „hihető tagadás" kifejezésével helyettesítettem, a félreérthető fogalmazás elkerülése érdekében.
[153]BACHMANN, Sascha Dov – Mosquera, Andres B. Munoz: Lawfare and hybrid warfare – how Russia is using the law as a weapon, in Amicus Curiae – *Journal of the Society for Advanced Legal Studies*, Summer 2015, 25–28. o.; Ansah, Tawia: Lawfare: A Rhetorical Analysis, in Case Western Reserve Journal of International Law, Vol. 43, 2010, 87–119. o.; NEWTON, Michael A.: Illustrating Illegitimate Lawfare. In: *Case Western Reserve Journal of International Law*, Vol. 43, 2010, pp. 255–273.
[154] BACHMANN, Sascha Dov – MUNOZ MOSQUERA, Andres B.: Hybrid Warfare as Lawfare: Towards a Comprehensive Legal Approach. In: CUSUMANO, Eugenio – CORBE, Marian (szerk.): *A Civil-Military Response to Hybrid Threats*, Cham, Palgrave Macmillan, 2018, 61–76. o.
[155] KEARNEY, Michael: Lawfare, Legitimacy and Resistance: The Weak and the Law. In: [MANSOUR, Camille (szerk.)]: *The Palestine Yearbook of International Law*, Vol. XVI. Leiden: Martinus Nijhoff Publishers, 2010, 79–130. o. DOI: 10.1163/22116141-90000063.

jelentenek a demokratikus ellenőrzéstől mentes szereplők kezében, mellyel alááshatják egy ország külpolitikáját és beavatkozhatnak a diplomáciai kapcsolatokba [...].”[156]

Ezzel a megközelítéssel összefüggésben szükséges vizsgálni azt, hogy a nem állami szereplők miként képesek államokkal szemben a jogi hadviselés eszközeivel fellépni, utóbbiak destabilizálása érdekében, egyfajta aszimmetrikus, illetve hibrid hadviselés megvalósítása során. A jogi hadviselő fél ugyanis nem csak egy másik állam lehet, de egy nem állami szervezet is, illetve egy másik állam képes lehet egy nem állami szervezet tevékenységébe ágyazottan jogi hadviselést folytatni egy állammal szemben, mely jellemző a definíció tartalma szűkítésének lehetőségére negatív, míg a kutatás ezirányú kiterjesztésének indokoltságára meghatározó jelentőséggel bír.

A „lawfare” fogalom meghatározásakor a szerzők arra törekszenek, hogy megmagyarázzák annak viszonyát más, kapcsolódó kategóriákkal, amelyek bizonyos közös jegyeket mutatnak a jelenséggel, de mégsem azonosak vele. A „lawfare” kifejezés egyre inkább hétköznapi szóhasználattá válik a politikai diskurzusban, ezért kiemelten fontos, hogy pontosan meghatározzuk a jelentését és így megkülönböztessük a hasonló fogalmaktól.[157]

---

[156] HERZBERG, Anne NGO ‘Lawfare’: Exploitation of Courts in the Arab-Israeli Conflict, NGO Monitor (September 2008). Az Izrael delegitimizálását célzó, jogi kereteket kihasználó stratégiát a 2001-es, dél-afrikai Durbanban megrendezett UN World Conference Against Racism civil fórumán fogalmazták meg. A civil fórum egy olyan tervet alakított ki, mely szerint Izraelt „rasszista” és „apartheid” államként bélyegeznék meg, és egy nemzetközi bojkott, deszinvestíció és szankciók komplex kampányával elszigetelnék, kifejezetten a jogi hadviselést felhasználva Izrael politikai háborújában. A civil fórum nyilatkozata sürgette a nemzetközi humanitárius jog érvényesítésének biztosítását szolgáló „valamennyi intézkedés elfogadását”, beleértve „egy háborús bűntettekkel foglalkozó törvényszék felállítását, hogy kivizsgálja és felelősségre vonja azokat, akik háborús bűnökért, népirtásért, etnikai tisztogatásért és az apartheid bűncselekményéért felelősek lehetnek Izraelben és a megszállt palesztin területeken...”. Anne Herzberg cikkében azt állítja, hogy számos nem kormányzati szervezet (NGO) a bíróságokat használja fel Izrael biztonságának és legitimitásának aláásására. Szerinte ezek az NGO-k egy „jogi hadviselés” nevű stratégiát alkalmaznak, amely a jogrendszer politikai célok elérésére történő felhasználását jelenti. Herzberg számos példát hoz arra, hogy az NGO-k hogyan használták a jogi hadviselést Izrael ellen, beleértve peres eljárásokat izraeli katonák és vállalatok ellen, valamint nemzetközi szervezeteknél folytatott lobbitevékenységet Izrael nyomás alá helyezésére. Herzberg szerint ez a típusú tevékenység káros Izraelre és a békefolyamat egészére nézve. Herzberg cikkét néhányan Izrael elleni elfogultsággal vádolták. Mások viszont dicsérték a cikkben foglaltakat, melyek betekintést nyújtanak a jogi hadviselés alkalmazásának mikéntjébe az arab-izraeli konfliktusban. Néhány kritikus szerint nem ad kiegyensúlyozott képet a konfliktusról, és csak az NGO-k konfliktusban betöltött szerepének negatív aspektusaira összpontosít. Herzberg cikke ugyanakkor, mindent összevetve értékes hozzájárulás a konfliktusban az NGO-k szerepéről folytatott vitához. Jól kutatott és jól megfogalmazott áttekintést nyújt a problémáról, és fontos olvasmány mindenkinek, aki érdeklődik a konfliktus iránt.

[157] VERESS Csongor Balázs: Jogviselés: a jog, mint háborús fegyver In.: ERDÉLYI JOGÉLET 3: 3 pp. 147-164., 18 p. (2022)

Az egyik ilyen kategória, amely gyakran említésre kerül a „jogi hadviselés” fogalma mellett, a „különleges jogrend”. Ez félrevezető lehet, mivel mindkét kifejezés egy általánostól eltérő állapotra utal, de ennek ellenére helytelen lenne a „lawfare” -t egyenértékűvé tenni a rend(en)kívüli állapottal, különleges helyzettel. Sőt, a különleges jogrend inkább tekinthető a jogi hadviselés egy lehetséges taktikájának, kifejezetten védelmi instrumentumnak, mintsem szinonimájának.

A „jogi hadviseléshez” kapcsolódó másik kategória a „jogvédői aktivizmus”, amit sokan a politikai célú jogászkodásnak tartanak. A politikai célú jogi hadviselést, amely különösen a korrupció elleni harcra összpontosít, erőteljesen átitatja a jogi aktivizmus. Ez utóbbi az egyik olyan terület, melyből a demokratikus dinamika torzulásai eredeztethetők, amikor politikai szereplőket démonizálnak.

A harmadik kategória a „hibrid hadviselés”, amely a szerzők szerint az arab tavasz és azt követően Latin-Amerikát is megrázó tüntetési hullámok révén vált ismertté a 2010-es években. Ezeket a tiltakozásokat kezdetben támogatta a nemzetközi közösség, különböző szakértők és think tank-ek által olyan jelszavakkal, mint demokrácia, szabadság és korrupció elleni harc. Azonban közelebbi vizsgálat során rájöhetünk, hogy ezek nem voltak spontán események, hanem egy olyan háborús modell eredményei, amelyet a katonai, kommunikációs, jogi és pszichológiai elemek kombinációja jellemez, és ezek helyettesítik a hagyományos harci eszközöket. Az Egyesült Államok rájött, hogy a hagyományos beavatkozás helyett jobban teszi, ha hibrid hadviseléshez folyamodik ezekben az esetekben. A nem hagyományos hadviselés nem magától jön létre, hanem egy már meglévő társadalmi konfliktus folytatásaként jelenik meg, célja pedig felkorbácsolni a konfliktust és segíteni a kormányellenes mozgalmakat a hatalom megdöntésében.

A geopolitikai célokat szolgáló jogi hadviselés a hibrid hadviselési modell egy kulcsfontosságú aspektusa, amely kihasznál számos rendelkezésre álló nem kinetikus erőforrást. A jogot háborús eszközként alkalmazzák az ellenség elleni támadásra és olyan eredmények elérésére, amelyeket hagyományos háborús konfrontációban is el lehetne érni vagy

amelyek ahhoz vezethetnek, ideértve a kisebbségek kiszolgáltatott helyzetének kihasználását is.[158]

2. A jogi hadviselés fogalommeghatározásának evolúciója

A Charles J. Dunlap Jr.[159] kutatásom középpontjában álló lawfare jelenséggel összefüggésben kiemelkedő, a téma kutatói által tájékozódási pontként elismert, 2001-es esszéje[160], amely egyaránt nagy hatást gyakorolt a katonai tudományos élet szereplőinek témáról alkotott felfogására és a szélesebb jogi akadémia közeghez tartozó kutatók ezzel összefüggő véleményére. [161] Ebben az esszében a lawfare fogalmát Dunlap úgy definiálja, mint *„a jog alkalmazása vagy az azzal való visszaélés, mint a hagyományos katonai eszközök helyettesítője, mely alkalmas az operatív célok elérésére”*.

---

[158] VERESS Csongor Balázs: Kisebbségi jogok felhasználása hibrid hadviselési eszközként In.: HONVÉDSÉGI SZEMLE: A MAGYAR HONVÉDSÉG KÖZPONTI FOLYÓIRATA 151 : 1 pp. 29-40. , 12 p. (2023)

[159] Charles J. Dunlap Jr. korábban az Egyesült Államok Légierejének helyettes főügyésze volt, 2010 júliusában csatlakozott a Duke Egyetem Jogi Karához, ahol jelenleg egyetemi tanár és az Országos Biztonsági, Jogi, Etikai és Nemzetbiztonsági Központ igazgatója. Oktatási és tudományos tevékenysége elsődlegesen a nemzetbiztonságra, a fegyveres konfliktusok nemzetközi jogára, a polgári-katonai kapcsolatokra, a kiberhadviselésre, a légierőre és a nemzetbiztonsági tevékenységhez kapcsolódó jogok és kötelességek gyakorlásával kapcsolatos etikai kérdésekre összpontosul. Dunlap tábornok 2010 júniusában vonult nyugdíjba az Egyesült Államok Légierejétől, 34 éves hivatásos katonai pályafutása alatt a vezérőrnagyi rendfokozatot érte el. 2006 májusa és 2010 márciusa között helyettes főügyészként segítette a katonai főügyészt több, mint 2200 bíró, 350 ügyvéd, 1400 beosztott írnok és 500 polgári személy szakmai felügyeletében szerte a világon. Tanácsokat adott az Egyesült Államok Vezérkarának és a különböző szintű parancsnokoknak, felügyelte a katonai igazságszolgáltatást, a műveleti, nemzetközi és polgári jogi feladatok szakszerű végrehajtását. Dunlap a St. Joseph Egyetemen és a Villanova Egyetemen jogi karán végzett. Végzett az Armed Forces Staff College-ban, és kitüntetéssel végzett a National War College-ban. Pályafutása során Dunlap részt vett különböző nemzetvédelmi, illetve nemzetbiztonsági feladatokkal bíró ügynökségek munkájában és ezekhez kapcsolódó szakpolitikai ügyekben. Az általa az asztalra letett jogi-szakmai jelentések közül kiemelkedik a katonai bizottságokról szóló 2006-os törvényről tartott előadása az Amerikai Egyesült Államok Képviselőháza előtt. A nyugállományú tábornok úr jogi tanácsadói feladatokat látott el a langley-i Légiparancsnokságnál és a texasi Randolph Légitámaszponton található Légi Oktatási és Kiképzési Parancsnokságnál, a különböző vezetői beosztások betöltése során. Az Amerikai Légi Erő Jogi Kar oktatói állományában polgári és büntetőjogi témákat tanított a hallgatóknak. Egy 22 államra kiterjedő körzet katonai bírójaként két évig dolgozott. Az Egyesült Királyságban és Dél-Koreában teljesített külszolgálatot, ugyanakkor aktív katonai pályafutása alatt a közel-keleti és afrikai műveletekben is részt vett. Dunlap termékeny szerző és tapasztalt előadó, széles körű nemzetbiztonsági témákról szóló publikációit vezető újságok és katonai folyóiratok közlik. Dunlap jogi tudományos munkássága többek között megjelent a Stanford Law Review, a Yale Journal of International Affairs, a Duke Journal of Gender Law & Policy, a Vanderbilt Journal of Transnational Law, a Wake Forest Law Review, a Fletcher Forum of World Affairs, az Air & Space Power Journal, az University of Nebraska Law Review, a Texas Tech Law Review, a Georgetown Journal of International Affairs és a Tennessee Law Review hasábjain is.

[160] Charles J. Dunlap, Jr., Jog és katonai beavatkozások: Az emberi jogi értékek megőrzése a 21. századi konfliktusokban (Carr Központ az Emberi Jogokért, John F. Kennedy Kormányzati Iskola, Harvard Egyetem, Munkatanulmány, 2001).

[161] A Harvard Egyetem részére írt esszéje tartalmát a „Humanitarian Challenges in Military Intervention” konferencián adta elő az egyetem Carr Központjában. Az előadásában azt emelte ki, hogy a nemzetközi jog miként befolyásolja az Egyesült Államok katonai beavatkozásainak hatékonyságát, és arra a kérdésre kereste a választ, hogy a jog eszköz lehet-e a háborúkban vagy magának a problémának a részét képezi-e.

Ő írta 1992-ben azt a tudományos művet[162] is, amely egy kitalált forgatókönyv és a kitalált szituáció értékelését tárja az olvasó elé, miközben egy lehetséges 2012-es katonai puccsot ír le az Egyesült Államokban, amelyet egy elnökjelölt meggyilkolása vált ki egy szélsőséges csoport tevékenységének hathatós közbenjárásával.

A katonai puccs oka a cikkben leírtak szerint az lenne, hogy a hadsereg elégedetlen a polgári vezetéssel, különösen a védelmi kiadások csökkentése és a katonai erő alkalmazásának korlátozása miatt. A szerző szerint a puccs fikciója, vagyis a lehetséges forgatókönyv felvázolása, figyelmeztetés arra vonatkozóan is, hogy a hadsereg és a politikai vezetés közti szakadék veszélyes méreteket ölthet.

A cikk megjósolja az Egyesült Államok lehetséges jövőbeli hanyatlását és azt vetíti előre, hogy a belső rendvédelmi jellegű katonai beavatkozás, bár szélsőségesnek hangzik, mégis indokolt lenne egy ilyen helyzet fennforgása esetén.[163] Azt javasolja, hogy a politikai vezetők figyeljenek jobban oda a hadsereg részéről felmerült jogos igényekre, különös tekintettel a jogi előírások betartására és betartatására, annak érdekében, hogy elkerüljék a társadalmi és politikai katasztrófát, illetve az oda vezető destabilizálódást.

Dunlap egy 2007-es cikkében[164] a jogi hadviselés egy olyan megközelítését vizsgálja, ami a nemzetközi jog stratégiai felhasználását jelenti a hadviselés eszközeként. Ezt a kérdést eredetileg a 2001-es esszéjében vetette fel, aggodalmát fejezve ki amiatt, hogy megállapítása szerint az USA ellenfelei egyre inkább ki fogják használni a nemzetközi jogot, gyakorlatilag kiforgatva annak előírásait. Ezzel összefüggésben fontos kiemelnünk, hogy ezzel a gondolatmenettel Petruska Ferenc is foglalkozik, ennek a megállapításnak a vizsgálatát végzi el és Dunlapéval megegyező, értekezésem témájával szorosan összefüggő, releváns végkövetkeztetést fogalmaz meg.[165]

---

[162]Charles J. Dunlap, Jr., The Origins of the American Military Coup of 2012, 40 Parameters 107-125 (2011)

[163] A cikk eredetileg egy szakmai folyóiratban jelent meg, és annak ellenére, hogy fikció, komoly vitát váltott ki az amerikai katonai és jogi körökben a civil-katonai kapcsolatok természetéről és azok potenciális jövőbeli kihívásairól egy olyan világban, ahol az állam nem képes szavatolni polgárainak jogait, legfeljebb súlyos jogkorlátozás árán. A biztonság szavatolása az alapjogok korlátozása árán mindig komoly társadalmi feszültségeket hoz felszínre és számtalan kutató számára biztosít inspirációt. Dunlap a művet figyelmeztetésnek szánta a demokratikus intézmények védelmében és arra ösztönzi az olvasót, hogy gondolkodjon el a hatalommal való visszaélés lehetőségeiről és annak következményeiről egy modern társadalomban.

[164] DUNLAP JR., C. J. (2007): Lawfare amid warfare. *The Washington Times*, 2007. augusztus 3. A19.

[165] PETRUSKA Ferenc, „Lawfare fogalma”, Katonai Jogi és Hadijogi Szemle 9, sz. 3 (2021): pp. 1–19

Dunlap elemzése szerint az USA ellenségei gyakran hangoztatják – háborús körülmények közötti valós vagy kitalált nemzetközi közjogi tényállások megsértésének vádját – az amerikai katonai erők tevékenységével összefüggő propagandatevékenységük során. Példaként hozza fel az Abu Ghraib-i eseményeket[166], amelyek olyan súlyos károkat okoztak a civil-katonai kapcsolatokban, amely egy hagyományos katonai vereségnél is nagyobb csapást jelentett az amerikai hadseregre nézve. Álláspontja szerint ezek az események elkerülhetők lettek volna, ha szigorúan betartják a jogi normákat. Rávilágít egy újabb, (ön)korlátozást kihasználó lawfare alkalmazásra, amely túlzottan óvatos politikákat igyekszik alkalmazni a civil áldozatok mérséklése, illetve elkerülése érdekében, mint például a NATO afganisztáni légi csapásainál. Habár ezek a célkitűzések rendkívül jó szándékúak, nem felelnek meg a nemzetközi jog előírásainak. A szerző tisztázza[167], hogy a nemzetközi jog tiltja a civilek szándékos célba vételét, de fontosnak tartja megjegyezni, hogy a civilek veszélyeztetése megengedett a legitim támadások során. A jog azt írja elő, hogy a nem harcolók veszélyeztetése ne legyen aránytalan a várható katonai előnyhöz képest.

Dunlap érvelése szerint az USA esetleges civil áldozatokkal összefüggésben meghatározott „zéró tolerancia" politikája szigorúbb, mint amit a nemzetközi jog egyébként a katonai szervezettől háborús körülmények között megkövetel és irreális elvárásokat teremthet továbbá nem várt következményekhez vezethet. Ezek a politikák akaratlanul is előnyt biztosíthatnak az ellenségnek, arra ösztönözve őket, hogy civileket használjanak élő pajzsként, így védve magukat az amerikai hadsereg támadásaival szemben, ami hosszú távon több egyébként még több civil életet veszélyeztethet.

[166] Ezzel összefüggésben meg kívánom jegyezni, hogy az Abu Ghraib (vagy Abu Ghuraib) egy iraki börtön, amely Bagdadtól nyugatra helyezkedik el, és a 2003-as Irak invázió idején vált világszerte ismertté, illetve hírhedtté. Az amerikai vezetésű koalíciós erők használták fogolytáborokként, és az intézmény működtetésével összefüggésben 2004-ben egy rendkívül súlyos botrány robbant ki, amikor nyilvánosságra kerültek azok a fotók, amelyek az ott fogva tartott iraki foglyok kínzását és megalázását dokumentálták amerikai katonák által.
A botrány komoly nemzetközi felháborodást váltott ki, és számos vizsgálatot indítottak az esetek tisztázására. Az események nyomán több amerikai katonát elítéltek visszaélésekért, és a történteket sokan az emberi jogok súlyos megsértéseként értékelték. Az Abu Ghraib eset rávilágított a hadifoglyokkal való humánus bánásmód fontosságára és a nemzetközi közjog előírásai betartásának szükségességére, melyet több évtizedes ügyészi tapasztalattal első helyen emel ki Dunlap is. A börtön neve összefonódott a kínzás és az emberi jogok megsértésének kérdésével, és gyakran emlegetik, amikor a háború és a hadifogoly-kezelés etikai kérdései kerülnek szóba. Az iraki kormány egy idő után bezárta a börtönt, majd később újranyitotta más néven, de az Abu Ghraib név továbbra is szimbolikus jelentőséggel bír a 21. század eleji konfliktusok és visszaélések kontextusában.
[167] DUNLAP JR., C. J. (2007): Lawfare amid warfare. *The Washington Times*, 2007. augusztus 3. A19.

A nemzetközi jog előírásainak betartása és betartatása elengedhetetlen a civilizált társadalmak és az általuk működtetett katonai erők számára[168]. Ugyanakkor szem előtt kell tartanunk azt is, hogy ha a fegyveres erők a nemzetközi jog előírásain túlmutató (ön)korlátozásokat vezetnek be vélt vagy valós politikai célok elérése érdekében, az kifejezetten kontraproduktív lehet. Ez ugyanis lehetőséget kínál az ellenfeleknek, hogy ezeket a (ön)korlátozásokat kihasználva jogi hadviselést alkalmazzanak az Egyesült Államok és szövetségesei ellen.

Kiemelkedő jelentőséggel bírnak a Lawfare című a tanulmányában[169] megjelenített gondolatok is. A National Security Law hasábjain megjelent publikáció mélyreható elemzést nyújt az olvasó számára a lawfare fogalmáról, a fogalom fejlődéséről és a lawfare növekvő jelentőségéről a modern konfliktusokban. Megvizsgálja, hogy a lawfare jelenség miként vált kulcsfontosságú aspektussá a nem állami szereplőket érintő aszimmetrikus konfliktusokban, és részletesen kifejti, hogy már 2015-ben milyen elterjedt eszközként használják a nemzetállamok a kinetikus és nem kinetikus hadviselés során.

A publikáció különböző dimenziókat elemez a lawfare vonatkozásában, nagy hangsúlyt fektetve annak használatára a pénzügyi hadviselésben, a technológia frontján és a kibertérben, valamint elemzi a szerepét a nemzetközi vitákban, mint a Dél-Kínai-tengeri konfliktus. Emellett vizsgálja a háború jogi aspektusait, úgymint a hadviselés jogi előkészítését és a jog stratégiai szinten történő használatát a békeműveletekben. A szerző hangsúlyozza a lawfare megértésének fontosságát a 21. századi konfliktusok kontextusában és a parancsnokok számára a jogi szempontok katonai stratégiába való integrálásának szükségességét.

A lawfare fogalma folyamatosan fejlődik és széles körben terjed a használata. A kifejezés modernkori megjelenésének idején, mely nem az 1975-ös[170], hanem a 2001-es évhez köthető, egy Internetes keresés csak néhány lawfare-re vonatkozó hivatkozást talált volna, de ez a szám 2009-re 60 000-re emelkedett. Napjainkban egy ilyen keresés már több százezer találatot eredményez. A lawfare nem csak, mint az aszimmetrikus konfliktusokban részt vevő nem

[168] DUNLAP JR., C. J. (2007): Lawfare amid warfare. *The Washington Times*, 2007. augusztus 3. A19.
[169] Charles J. Dunlap, Jr., Lawfare, in National Security Law 823-838 (John Norton Moore et al. eds., 2015)
[170] A kifejezés először CARLSON, John – YEOMANS, Neville: Whither Goeth the Law – Humanity or Barbarity. In: SMITH, M. – CROSSLEY, D. (szerk.): The Way Out – Radical Alternatives in Australia. című műben szerepel, ugyanakkor a kifejezést eltérő jelentéssel használják. A kifejezést a tudományos művem szempontjából a Dunlap által alkalmazott megközelítésében használom.

állami szereplők kulcsfontosságú aspektusaként vizsgálandó, értékelendő, hanem az Egyesült Államok kormányának preferált fegyvereként is funkcionál a terrorista szervezetek pénzügyi hátországának gyengítésére, illetve megsemmisítésére.

Szükségesnek tartom megjegyezni, hogy a lawfare kifejezésnek az előbbiekben hivatkozott 1975-ben, a John Carlson – Neville Yeomans szerzőpáros által történő használata eltér a Dunlap általitól. Dunlap a szerzőpáros által megjelenített *„Lawfare replaces warfare and the duel is with words rather than swords”* mondatot felhasználja ugyan, de eltérően, sajátosan kiterjesztően értelemezi, ugyanis a 21. századi biztonsági kihívások teljes spektrumára vetítve a jogi hadviselést nem asszertív, mediációra való eszközként definiálja, hanem a politikai célok elérésének hatékony, egy potenciális nem-kinetikus fegyvereként, vagyis Dunlap a hibrid hadviselés egyik intézkedéseként tekint a jogi hadviselésre. A John Carlson – Neville Yeomans szerzőpáros a tanulmányban[171] két kiegészítő rendszert különböztet meg a társadalmi entitások elemzésében: az integratív mechanizmust, amely a kollektív entitás létezését és stabilitását biztosítja, valamint a környezettel való interakcióért felelős másodlagos mechanizmust.

Álláspontjuk szerint, ha ezek a rendszerek valóban léteznek egy társadalmi vagy kulturális renden belül, akkor elvárható, hogy megfelelő normatív struktúráik is jelen legyenek: a közösségi vagy integratív jog, illetve a társadalmi vagy instrumentális jog. Hasonlóképpen a megfelelő konfliktuskezelő társadalmi intézmények is differenciálódtak e normarendszerek hordozására. A közösségi jog a harmóniával, békével és szeretettel foglalkozik, míg a társadalmi jog az igazságossággal és racionalitással. Az előbbi az egyéneket alanyként, az utóbbi tárgyként kezeli. Az előbbi jogi felfogás, vagyis inkább idea célja humanitárius, rugalmas és intuitív, az utóbbi alapfelfogása pedig utilitarista, stabilitásra törekvő és logikus érvelésre építő. Az előbbiben az együttérző emberségesség, erényesség és tisztességesség, az utóbbiban az ésszerűség, hatékonyság és legitim önérdek dominál.

A szerzőpáros véleménye szerint a nyugati jogban mostanában növekvő igény mutatkozik az emberségességre. Így a közvetített harmónia és humánus igazságszolgáltatás kezd előtérbe kerülni. A jogi mediáció során egy harmadik fél irányítja a viták kölcsönös engedményeken és

[171] CARLSON, John – YEOMANS, Neville: Whither Goeth the Law – Humanity or Barbarity. In: SMITH, M. – CROSSLEY, D. (szerk.): The Way Out – Radical Alternatives in Australia. Lansdowne Press, Melbourne, 1975.

együttműködésen alapuló megoldását, szemben a kényszerített döntéssel. Ez magánjellegű és nem nyilvános, rábeszélő és nem kényszerítő, demokratikus és nem autokratikus. A mediátor a felek közös jólétével és emberi méltóságával törődik, nem azzal, hogy az egyiket jutalmazza és a másikat megbüntesse. Az eredmény az integráció, nem a megtorlás. Álláspontjuk szerint a bíróságokra továbbra is szükség van, a mediáció tapasztalatait érdemes lenne alaposan tanulmányozni egy modern vitarendezési rendszer kialakítása céljából Ausztráliában.

Az általam a jogi hadviselés fogalmának (fejlődés)történeti kontextusban történő vizsgálata miatt kiemelt, általuk – tehát az eredeti értelemben – alkalmazott *„Lawfare replaces warfare and the duel is with words rather than swords”* mondatot tehát úgy indokolt értelmezni, hogy emberközpontú, humánus, asszertív jogi megoldások lehetnének a (jog)viták rendezésének elsődleges eszközei, nem pedig „a karddal vívott párbajok” (itt utalva a dehumanizált, racionalizált, formalizált, hivatalos eljárásokra), hanem a mediátor által irányított, kompromisszumos megoldásra vezető, békítő szavak.

3. A hibrid műveletek során alkalmazott lawfare használat elméleti megközelítése

Az Orosz Föderáció élen jár a lawfare technikák alkalmazásában[172]. Példaként jelenítem meg, hogy az oroszok „passzportizáció” eszközét – a donbaszi ukrán állampolgárok tömeges, gyorsított orosz honosítását – alkalmazták annak érdekében, hogy nemzetközi jogi alapot állítsanak fel beavatkozásaikhoz Grúziában és Ukrajnában. A passzportizáció az orosz állampolgárság tömeges megadása más államok állampolgárainak”, amelynek célja az, hogy lehetővé tegye Oroszországnak, hogy azt állítsa, hogy beavatkozása csupán azért történt, mert „védi az orosz állampolgárokat”. 2019 áprilisától Putyin elnöki rendelete alapján a Donyeck és Luhanszk „népi köztársaságok" lakói nyolc évről három hónap alá csökkentett eljárással kaphatnak orosz állampolgárságot. 2020 közepéig közel 200 000 ukrán kapott orosz útlevelet ezen a gyorsított úton. Külpolitikailag a passzportizáció a konfliktusmegoldást szabotáló eszköz, fenntartja az ellenőrzött instabilitást, Kijev szuverenitását sérti, és eleve ellehetetleníti a minszki békefolyamat helyi választásokra vonatkozó rendelkezéseinek végrehajtását. Belpolitikailag a természetes népességfogyás kompenzálásának eszköze — a gyorsított

[172] DUNLAP, Charles J., Jr., Lawfare, in National Security Law 823-838 (John Norton Moore et al. eds., 2015)

honosítás elsősorban az ukrán munkavállalókat célozza, akiket Oroszország ideális migránsoknak tart. [173]

Az orosz jogértelmezés (esetünkben kijelenthető, hogy gyakorlatilag jogi hadviselés) végső célját természetesen úgy kell értelmeznünk, hogy egy háborús bűnössel szemben az agresszió is megengedett, vagyis az orosz állampolgárok védelme érdekében akár még jogszerű háború is indítható. Ennek a legitimációt romboló és történelmi beidegződésekre építő tervnek a lépésről lépésre történő végrehajtását követhette nyomon a nemzetközi közösség az elmúlt tíz évben.[174]

Megfigyelhető[175], hogy a jogi hadviselés eszközeként az orosz tisztviselők – az Egyesült Államok által Oroszországgal szemben kezdeményezett szankciókkal szembeni – egyfajta

[173] BURKHARDT, Fabian: Russia's "Passportisation" of the Donbas: The Mass Naturalisation of Ukrainians Is More Than a Foreign Policy Tool. *SWP Comment*, No. 41 (August 2020). Berlin: Stiftung Wissenschaft und Politik. Oroszország korábban ugyanezt az eszközt alkalmazta Abháziában, Dél-Oszétiában és Transznisztriában is. A szerző rámutat: Oroszország nem azonos stratégiát követ minden esetben, hanem az adott területhez és saját változó céljaihoz igazítja az eszköztárat. Közös vonás azonban, hogy a passzportizációt a nemzetközi jog általában jogsértőnek minősíti — a Georgia-ügyi független vizsgálóbizottság és a Max Planck Intézet igazgatója (Anne Peters) is joggyakorlással való visszaélésnek tekinti. A minszki folyamatra gyakorolt hatás négy szinten érvényesül. Egyrészt akadályozza a tárgyalásokat, mivel az orosz útlevelet tartó „népi köztársasági" tisztviselők Oroszország képviselőiként, nem a helyi lakosság képviselőiként jelennek meg. Másrészt belső megosztottságot szít Ukrajnában (az orosz útlevelesek ukrán állampolgárságának megvonása körüli vita). Harmadrészt a minszki protokoll szerinti helyi választásokat ellehetetleníti, mivel a kettős állampolgárságot tiltó ukrán alkotmány alapján az orosz útlevéllel rendelkező személyek nem indulhatnak ukrán választásokon és nem tölthetnek be állami tisztséget. Negyedrészt demográfiai torzítást (gerrymanderinget) okoz, a munkaképes, szakképzett donbaszi lakosokat Oroszországba vonzza, miközben az idős, szegény és kevésbé mobil réteg marad. Kulcskövetkeztetés. A passzportizáció nem az annexió előkészítése, hanem a konfliktus befagyasztásának és Ukrajna feletti tartós befolyásgyakorlásnak az eszköze, azzal a kettős előnnyel, hogy Oroszország egyszerre tartja fenn a Donbasz feletti ellenőrzést és teszi vonzóbbá magát az ukrán kivándorlók számára.

[174] CARMENT, David – BELO, Dani: Protecting Minority Rights to Undermine Russia's Compatriots Strategy. Canadian Global Affairs Institute, 2019. április. A cikk egy jelentést ismertet a Demokrácia és Technológia Központtól (CDT) arról, hogy Oroszország hogyan használja a jogi hadviselést a volt Szovjetunió országaiban a kisebbségek jogainak aláásására. A jelentés szerint Oroszország számos jogi eszközt használ, beleértve az emberi jogi előírásokat is, hogy zaklassa és megfélemlítse a kisebbségi csoportokat, és hogy elnémítsa az ellenzéki hangokat. A jelentés azt is állítja, hogy Oroszország a jogi hadviselést használja más országok belügyeibe való beavatkozásra, és szuverenitásuk aláásására. A jelentés számos ajánlást tesz arra vonatkozóan, hogy az Egyesült Államok és szövetségesei hogyan léphetnek fel Oroszország jogi hadviselése ellen. Ezek az ajánlások a következők: 1) Növelni kell a támogatását azoknak a civil társadalmi szervezeteknek a volt Szovjetunió országaiban, amelyek a kisebbségek jogainak védelmében dolgoznak. 2) Fel kell hívni a nemzetközi közösség figyelmét Oroszország jogi hadviselésére. 3) Stratégiákat szükséges kifejleszteni Oroszország jogi hadviselésével szemben az nemzetközi bíróságokon és egyéb nemzetközi fórumokon. A jelentés számos fontos jellemzőt azonosít Oroszország által alkalmazott jogi hadviselésről. A jelentést ismertető szerzőpáros néhány további pontot ad hozzá publikációjában a jelentés által megjelenítettekhez kapcsolódóan. Fontosnak tartja megjegyezni, hogy nem csak Oroszország használja a jogi hadviselést. Más országok, mint például Kína és Irán is előszeretettel használják azt politikai céljaik elérésére. Kiemeli ugyanakkor, hogy a jogi hadviselés nem mindig rossz dolog, ugyanis bizonyos esetekben ezt az emberi jogok előmozdítására és a joguralom (rule of law) védelmére lehet használni. Azonban Oroszország esetében a jogi hadviselést kifejezetten a kisebbségek jogainak aláásására és az ellenzék elnémítására használják.

[175] Dunlap a hivatkozott, Lawfare című publikációjában kifejezetten felhívja az olvasó figyelmét erre.

ellencsapásként – próbálnak vizsgálatot követelni annak érdekében, hogy az Egyesült Államok által a második világháború során Hirosima és Nagaszaki ellen végrehajtott atomtámadásokat emberiség elleni bűntettnek nyilvánítsák.

Ahogy az Dunlap korábban is kifejtette[176], érdemes a jogra – a lawfare kontextusában – fegyverként tekinteni, amelyet „jó" vagy „rossz" célokra egyaránt lehet használni. Álláspontja szerint ezt indokolt szem előtt tartani, amikor az új biztonsági kihívásokra keresünk megoldásokat. Nyilvánvaló, hogy a lawfare folyamatosan fejlődik a háború eszközeként és módszereként, még akkor is, ha alkalmazásának jellemzői miatt a végrehajtott intézkedéseket nem sorolhatjuk a „fair" megoldások közé.[177]

Figyelmet érdemel a nemzetközi jog és nemzetközi kapcsolatok professzora, Jill I. Goldenziel által írt esszé[178], amely a jog háborús eszközként való megjelenésére összpontosít. Az esszé részletesen elemzi, hogyan használják az államok és a nem állami szereplők a lawfare-t az ellenség legitimitásának gyengítésére, a hagyományos katonai célok elérésének akadályozására, az ellenség harci moráljának csökkentésére, valamint a háború narratívájának alakítására (propagandacélokra és a közvélemény manipulálására). Kiemeli, hogy Kína ma a világ egyik vezető lawfare alkalmazója, ahol a kínai katonai erők a „Három Háború" egyik prioritásként kezelik a lawfare-t, amely álláspontjuk szerint jelentősen befolyásolja a katonai műveleteik sikerét. A „Három háború" elve a kínai katonai doktrínában egy olyan stratégiai koncepció[179], amely a katonai tevékenységek mellett a pszichológiai, jogi és médiaküzdelmet is magában foglalja. Ez a koncepció tükrözi Kína törekvését arra, hogy a hagyományos katonai erő alkalmazásán túlmenően kiterjessze befolyását a nemzetközi közvéleményre, a jogi normákra és a médiára.

---

[176] DUNLAP JR., C. J. (2009): Lawfare: A Decisive Element of 21st-Century Conflicts? *Joint Force Quarterly*, Issue 54. (3rd quarter 2009) 34–39.

[177] DUNLAP JR., C. J. (2014): Has Hamas Overplayed Its Lawfare Strategy? *Just Security*, (2014. augusztus 5.) Dunlap professzor a publikációjában a Hamász által alkalmazott jogi hadviselést vizsgálja, vagyis azt a folyamatot, melynek során a Hamász a jogot fegyverként használja politikai céljai elérése érdekében. Szerinte a Hamász jogi hadviseléssel: 1) Izrael és a nemzetközi közösség legitimitását próbálja aláásni, 2) Korlátozni próbálja Izrael erőszak-alkalmazási képességeit, 3) Nemzetközi szimpátiát és támogatást próbál szerezni, továbbá 4) Új tagokat próbál toborozni és a meglévőket pedig motiválni igyekszik. Dunlap professzor szerint a Hamász jogi hadviselése hatékonynak bizonyult, és megnehezítette Izrael biztonsági céljainak elérését. Úgy véli, a nemzetközi közösségnek jobban tudatosítania kell a jogi hadviselés jelentette fenyegetést, és stratégiákat kell kidolgoznia ellene. A professzor által megfogalmazottak szerint a Hamász által alkalmazott hibrid hadviselési módszer, komoly kihívást jelent Izrael és a nyugati demokráciák számára. Véleménye szerint olyan jogi és kommunikációs mechanizmusok kiépítésére van szükség, melyek képesek hatékony választ adni erre az újszerű fenyegetésre.

[178] Goldenziel, Jill I., Law as a Battlefield: The U.S., China, and the Global Escalation of Lawfare

[179] A „Három háború" elvéről bővebben lásd: MATTIS, P. (2018). China's 'Three Warfares' in Perspective. War on the Rocks.

A „Három háború” elve a következő három kulcsfontosságú területet foglalja magába:

- Pszichológiai háború: Ez magában foglalja a közvélemény befolyásolását és a társadalmi attitűdök formálását, mind a belföldi, mind a nemzetközi szinten. A cél a nemzeti érdekek és álláspontok támogatásának növelése, ellenséges nézetek gyengítése és a saját katonai és politikai célkitűzések legitimálása.
- Jogi háború (vagyis a lawfare): A jogi háború a nemzetközi és hazai jogi keretek, normák és intézmények kihasználása vagy manipulációja, hogy elősegítse Kína stratégiai céljait. Ez magában foglalhatja a nemzetközi jog értelmezésének és alkalmazásának befolyásolását, jogi vitákban való érvényesülést és a jogi rendszerekkel való stratégiai játszmát, hogy előnyhöz juttassa Kínát a nemzetközi viszonylatokban.
- Médiabefolyásolás: Ez az aspektus a médiatartalmak és információk áramlásának uralására és manipulálására irányul, abból a célból, hogy formálja a közvélemény gondolkodásmódját, ismeretét és hogy minél szélesebb közösség támogassa a kínai politikai és katonai kezdeményezéseket. A cél a média narratívájának ellenőrzése és a kínai állam álláspontjának hatékony kommunikációja a nemzetközi és hazai médiában.

A „Három Háború” elvének alkalmazása, használata azt jelzi, hogy Kína stratégiája túllép a hagyományos katonai stratégiai műveletek „megszokott keretein” és egy olyan integrált megközelítést alkalmaz, amely a pszichológiai, jogi és médiamanipulációt is magában foglalja annak érdekében, hogy erősítse globális befolyását és előmozdítsa az állam érdekeit. Goldenziel ezzel összefüggésben megjegyzi, hogy az Egyesült Államoknak nincs (például a kínaihoz hasonló) lawfare doktrínája, illetve stratégiája, még annak ellenére sem, hogy Kína konfrontációra kényszeríti őket ezen a téren is. Az esszé konkrét példákon keresztül mutatja be a lawfare jelenségét, pontosabban az eszközrendszer alkalmazását, illetve használatát az Egyesült Államok és Kína, valamint szövetségeseik között. Ezek közé tartozik Kína egyenruhát nem viselő tengeri milicistáinak tevékenysége a Spratly-szigeteken, a nemzetközi választottbírósági eljárások befolyásolására kifejtett törekvései, valamint az Egyesült Államok és a Huawei közötti polgári jogi jogvita (melynek büntetőeljárási jog területére tartozó intézkedéseit is alapul véve elég súlyos jogkövetkezményeit figyelhettük meg.)

Az önálló lawfare stratégia megalkotásának szükségessége melletti érvként kifejti[180], hogy a nemzeti védelmi (illetve biztonsági) stratégiákban a hibrid hadviselés növekvő jelentőségét és a kiberbiztonság fontosságát szükséges még jobban kiemelni, ugyanis okfejtése szerint ezek a dokumentumok arra kell, hogy összpontosítsanak, hogy a hibrid fenyegetések, amelyek hagyományos és nem hagyományos hadviselési módszereket ötvöznek, beleértve a kibertámadásokat, új kihívásokat jelentenek a nemzetbiztonság számára és ez ellen megfelelő válaszlépéseket kell tennie az Egyesült Államoknak. Szó esik előbbi javaslatával összefüggésben a mesterséges intelligencia szerepéről és a kibertér jelentőségéről a modern nemzeti biztonsági stratégiákban. Összességében az esszéje rávilágít arra, hogy a jogi hadviselés egyre inkább elengedhetetlen részévé válik a modern nemzetközi konfliktusoknak, és hogy ezen eszközök alkalmazása stratégiai előnyt jelenthet a nemzetközi közösségen belüli érdekérvényesítésben.

4. Összegzés, az elvégzett vizsgálat és részkövetkeztetések

A célzott hatás kifejtése érdekében információs műveletek precíz alkalmazása kerül végrehajtásra, kiemelten a jogi hadviselés specifikumával kiegészítve, elsődlegesen a közvélemény befolyásolása útján. Ezen megállapításaim a II. fejezetben megjelenített, információs műveletekre vonatkozó alapvető ismérvekkel való összefüggés rögzítésére szolgálnak, valamint a 4. számú hipotézis alátámasztására alkalmasnak tekinthetők, ezt a hipotézist kívánják megerősíteni, továbbá a disszertáció jogi hadviselés tárgykörének elméleti alapjait fektetik le.

Az értekezés témája szerint az alábbi pontokban foglalhatók össze a lawfare jelenség sajátosságai:

- A „lawfare” jelenség a jogi eszközök politikai és katonai célokra való (hibrid) felhasználása;
- Lényegében a hírszerzéssel egyidősnek tekinthetjük, de napjainkban sokkal szélesebb körben alkalmazzák a nemzetközi konfliktusokban;
- A lawfare egyre inkább a propaganda és média manipuláció eszközévé válik a közvélemény befolyásolására és az eljárások irányítására;

[180] Az eddig általam ismertetett szerzők valamennyien egyetértenek abban, hogy stratégiai szinten szükséges – elsődlegesen – jogi és kommunikációs eszközökkel fellépni az idegen, illetve ellenérdekű jogi hadviselés ellen.

- Globális szinten a lawfare megjelenik államok közti vitákban, terrorellenes intézkedésekben, kibertámadásokban. Jelentős kihívást jelent a nemzetközi jog evolúciójára nézve az igazságosság és pártatlanság elveinek betartása (valamint az etikai szempontok) terén;
- A jog és háború kapcsolata évszázadok óta fejlődik. Célja a háborúk szabályozása és humanizálása. Még vannak kihívások, de előrelépések is, pl. a Genfi Egyezmény, ugyanakkor a lawfare alkalmazása jelentheti a konvencionális háború elkerülésének a lehetőségét, de annak előszelét is;
- A nemzetbiztonság és szuverenitás egyensúlya fontos a belső kormányzásban és nemzetközi kapcsolatokban. Nehéz egyensúlyt találni, globális kihívások közepette az együttműködés gyakran csökkenti az egyes államok szuverenitását.

A nyugati hadviselési modellekben a jog a hibrid hadviselés integráns részét képezi. A jog határozza meg, hogyan képzeljük el és vívjuk a háborúkat. A jog húzza meg a határvonalat a háború és béke, valamint a megengedett és nem megengedett erőszak között. A jogi keretek rögzítik a hadviselő felek kölcsönös elvárásait a csatatéri magatartásról.

A hibrid hadviselés során az ellenfelek kihasználják a jog ezen szabályozó funkcióját, hogy katonai előnyre tegyenek szert. Úgy teszik ezt, hogy nem tartják be a rájuk vonatkozó normákat és szabályokat, miközben számítanak arra, hogy ellenfeleik ragaszkodnak hozzájuk. Általános céljuk egy olyan aszimmetrikus jogi környezet fenntartása, ami előnyös a saját hadműveleteik, és hátrányos az ellenség számára. Így válik a jog a hadviselés egyik eszközévé.

A hibrid fenyegetésekkel szembenéző nemzeteknek fel kell készülniük a jog ilyen jellegű felhasználására. Megerősítendők a szükséges nemzeti és kollektív eszközeik ezzel szemben[181].

A későbbi fejezetekben és az 1. számú mellékletben ismertetett konkrét példákból felismerhető tapasztalatok szerint, az ott megjelenített tevékenységgel összefüggésben, a fejezetben hivatkozott szerzők által kiemelt példák rávilágítanak arra, hogy hozzáértő kezek által vezérelve a politikai propaganda és médiagépezet képzeletbeli ágyújának okoslőszereként is funkcionálhat a lawfare.

[181] SARI Aurel: Hybrid Warfare, Law, and the Fulda Gap. In: Winston S. Williams – Christopher M. Ford (eds): Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare. New York, NY : Oxford University Press, 2019, 161–190.

Ezen eszközök kombinációja a hibrid hadviselés intézkedéssorozatának különösen jelentős csapásmérő képességét mutatják be, mellyel összefüggésben megállapítottam, hogy a lawfare kutatásának nélkülözhetetlen elemeit képezi a jogi hadviseléshez kapcsolódó:

- más hibrid hadviselés eszköztárába tartozó intézkedések, továbbá az ezekkel összefüggő
- stratégiai jogalkotás és stratégiaalkotás jellemzőinek,
- a nemzeti szuverenitás helyzetének és az ezt veszélyeztető törekvéseknek,
- a befolyásoló műveleteknek, és
- a kiberműveleteknek és a mesterséges intelligencia szerepének

vizsgálata, melyet a következő fejezetek elkészítése során végeztem el.

IV. A GERILLA HADIKULTÚRA, A HIBRID HADVISELÉS ÉS A LAWFARE EGYES ASPEKTUSAINAK VIZSGÁLATA NEMZETBIZTONSÁGI SZEMPONTBÓL

1. Összefüggések vizsgálata a gerilla hadikultúra, az aszimmetrikus hadviselés, a hibrid hadviselés és a jogi hadviselés fogalomrendszereiben

A modern hadviselés természetét vizsgálva azt tapasztalom, hogy az elmúlt évtizedekben gyökeres átalakuláson ment keresztül. A klasszikus, államok közötti, frontvonalak mentén vívott háborúk helyét egyre inkább olyan összetett konfliktusok vették át, amelyekben a katonai műveletek mellett politikai, gazdasági, információs és jogi eszközök is meghatározó szerepet játszanak. Kutatásom során ezért kiemelt figyelmet fordítok azokra a hadviselési formákra, amelyek a kortárs biztonságpolitikai gondolkodás középpontjába kerültek: az aszimmetrikus hadviselésre, a hibrid hadviselésre, a gerilla hadikultúrára és a lawfare-re.

Elemzésem célja, hogy átfogó képet adjak e négy fogalom elméleti alapjairól, történeti fejlődéséről és gyakorlati megvalósulásairól. Továbbá vizsgálni kívánom azokat a kapcsolódási pontokat, amelyek révén e hadviselési formák együttesen formálják a 21. századi konfliktusok arculatát. Fontosnak tartom feltárni, hogy ezek a hadviselési formák miként illeszkednek a NATO stratégiájába, és milyen válaszlépések születtek a szövetség részéről a hibrid és aszimmetrikus fenyegetések kezelésére. Kutatásom módszertana több pilléren nyugszik: egyrészt támaszkodom a releváns NATO-doktrínákra, különösen az Allied Joint Doctrine AJP-01 (2020) és a NATO Strategic Concept (2022) dokumentumokra, másrészt feldolgozok

tudományos publikációkat, szakértői tanulmányokat és esettanulmányokat. Elemzésem során törekszem a történelmi példák és a kortárs konfliktusok összevetésére, annak érdekében, hogy feltárjam a hasonlóságokat és különbségeket, valamint értékeljem a hadviselés új trendjeit.

Az aszimmetrikus hadviselés fogalmát vizsgálva arra a következtetésre jutottam, hogy annak lényege a szemben álló felek közötti jelentős erőforrás- és képességkülönbség kiegyensúlyozására irányuló stratégiai és taktikai törekvés. Az aszimmetrikus hadviselésben a gyengébb fél nem hagyományos módszerekkel – például gerillataktikával, terrorcselekményekkel, információs, illetve kiberműveletekkel – igyekszik ellensúlyozni az erősebb fél katonai fölényét. Kutatásom során különösen tanulságosnak találtam az afganisztáni és iraki műveletek tapasztalatait, amelyek rámutattak arra, hogy a gyengébb felek képesek jelentős stratégiai kihívást jelenteni a hagyományosan felkészült és felszerelt haderők számára. Az aszimmetrikus hadviselés célja nem csupán a katonai vereség elkerülése, hanem az ellenfél politikai akaratának megtörése, gazdasági költségeinek növelése és a társadalmi támogatottság megingatása. Ez a fajta hadviselés szoros kapcsolatban áll az információs műveletekkel, kiemelten a pszichológiai műveletekkel, amelyek célja a közvélemény befolyásolása és a döntéshozatali folyamatok destabilizálása.

A gerilla hadikultúra vizsgálata során arra törekszem, hogy feltárjam annak stratégiai és kulturális jelentőségét. A történelmi példák – az amerikai függetlenségi háború partizánjai, a napóleoni háborúk spanyol gerillái, valamint a vietnámi háború – azt mutatják, hogy a gerilla hadviselés sikeressége elsősorban a lakosság támogatásán, az alkalmazott taktikák rugalmasságán és az ellenfél gyenge pontjainak kihasználásán múlik. Fontos kiemelni Mao Ce-tung[182] és Che Guevara[183] elméleteit, akik a gerillaharcot a politikai célok elérésének alapvető eszközeként definiálták. A NATO doktrínája[184] megerősíti ezt a megközelítést, hangsúlyozva a lakossággal való kapcsolattartás és a stabilizációs törekvések fontosságát. Saját elemzésem szerint a gerilla hadikultúra nem csupán taktikai, hanem pszichológiai hadszíntéren is formálja a konfliktus kimenetelét, hiszen az ellenfél moráljára és politikai akaratára egyaránt hatást gyakorol.

[182] MAO Zedong. (1937).: On Guerrilla Warfare. Elérhető a Marxists.org-on és Mao Zedong. (1937). MAO Zedong: *On Guerrilla Warfare*. Translated by Samuel B. Griffith II. Praeger, New York, 1961.
[183] Guevara, E. (1961). *Guerrilla Warfare* (Translated by J. P. Morray). Monthly Review Press. és Guevara, E. (1963). Guerrilla Warfare: A Method.
[184] A témával összefüggésben bővebben: ATP-3.4.4.1 (*Guidance for the Application of Tactical Military Activities in Counterinsurgency*) és AJP-3.4.4 (*Allied Joint Doctrine for Counterinsurgency*)

A hibrid hadviselés olyan integrált stratégiai eszköztárat jelent, amely katonai és nem-katonai módszereket – például kibertámadásokat, dezinformációt, gazdasági nyomást és lawfare-t – kombinál az úgynevezett szürke zónában.[185] A NATO definíciója szerint az attribúció képessége és a közösség rezilienciája kulcsfontosságú a válaszadásban.[186] A hivatkozott tanulmány[187] új, releváns elemként kihangsúlyozza, hogy a hibrid hatékonyság értékeléséhez új, méréseken alapuló keretrendszerekre van szükség. A hibrid hadviselés a katonai és nem katonai eszközök összehangolt alkalmazása, amelyben a kiberműveletek, dezinformációs kampányok és gazdasági nyomásgyakorlás a fegyveres erő alkalmazásával együttesen jelenik meg.[188] A Geraszimov-doktrína rámutat arra, hogy a modern konfliktusokban a katonai műveletek gyakran alárendelődnek a politikai célokat szolgáló komplex stratégiáknak.[189] Az orosz–ukrán konfliktus példája jól illusztrálja e megközelítést. A NATO 2022-es Stratégiai Koncepciója szerint a hibrid fenyegetések kezeléséhez összehangolt katonai, diplomáciai és jogi válaszokra van szükség.[190]

Az aszimmetrikus hadviselés alapvetően arra épül, hogy egy erőviszonyokat tekintve gyengébb fél unortodox, nem-hagyományos eszközökkel – például gerilla taktika, terrorista akciók, pszichológiai műveletek – kiegyenlíti a hátrányát. Ebben a kontextusban különösen előtérbe kerül az információs műveletek és a lawfare, mint alternatív hatékonyságnövelő mechanizmusok.[191]

Az információs műveletek mind a hibrid, mind az aszimmetrikus hadviselésben központi szerepet játszanak:

[185] GROEN, M. S. – BORENE, A. – LIVERMORE, D. (2025): Quantifying the Gray Zone: A Framework for Measuring Hybrid Warfare Power Balances. *Small Wars Journal*, 2025. június 17.
[186] GROEN, M. S. – BORENE, A. – LIVERMORE, D. (2025): Quantifying the Gray Zone: A Framework for Measuring Hybrid Warfare Power Balances. *Small Wars Journal*, 2025. június 17.
[187] Quantifying the Gray Zone című
[188] Hoffman, F. G. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, Arlington.
[189] GERASZIMOV, Valerij: Cennoszty nauki v predvigyenii. *Voenno-promyshlennyi kurier*, No. 8 (476.), 2013. február 27., 1–2. o.
[190] NATO: *NATO 2022 Strategic Concept.* Adopted by Heads of State and Government at the NATO Summit in Madrid, 29 June 2022**.** NATO, Brussels, 2022.
[191] LUBERISSE, J. (2025): Verification Cost Asymmetry in Cognitive Warfare: A Complexity-Theoretic Framework, arXiv preprint, July 28, 2025.

- a hibrid hadviselésben információs műveleteket a katonai és nem-katonai eszközök integrált részének tekintjük szürke-zónás műveletek keretében;[192]
- az aszimmetrikus hadviselés esetében információs művelet gyakran önálló taktikai opcióként jelenik meg és narratív dominanciára törekszik.[193]

A lawfare mindkét hadviselési módnál stratégiai jelentőséggel bír:

- a hibrid hadviselésben a jogi manőverezés célja az ellenfél legitimációjának csökkentése vagy akadályozása, politikai és jogi közeg manipulálása; [194] hibrid hadviselés esetén az információs műveletek és a lawfare[195] szervesen beépülnek a komplex stratégiába, súlyos veszélyt jelentve (Ezt a megközelítést részletesen elemzi Rondeaux, aki a Wagner-csoporthoz köthető ügynökök elleni lengyelországi ítélet kapcsán bemutatja, miként alkalmazható a jog offenzív módon a hibrid fenyegetések visszaszorítására); [196]
- aszimmetrikus kontextusban a gyengébb fél gyakran fordul nemzetközi fórumokhoz, jogi eszközökhöz, pereskedéshez, ezáltal politikai és morális fölényt kíván szerezni.[197] Az aszimmetrikus hadviselés esetében ezek az eszközök funkcionálisan egymást kiegészítik és morális, pszichológiai vagy jogi előnyhöz juttatják a kevésbé erős felet.

Az aszimmetrikus hadviselés és a gerilla hadikultúra egymást kiegészítve valósítják meg a gyengébb fél túlélési és erőforrás-kiegyensúlyozási stratégiáit.[198] A hibrid hadviselés ezeket az eszközöket magasabb stratégiai szinten integrálja, kiegészítve kiber-, gazdasági és információs műveletekkel.[199] A lawfare pedig jogi dimenzióval egészíti ki e formákat, hozzájárulva a legitimációs harcokhoz és a politikai célok eléréséhez.[200] Saját értelmezésem szerint e négy forma egymásra épülve jeleníti meg a modern konfliktusok komplexitását,

---

[192] GROEN, M. S., BORENE, A. & LIVERMORE, D. (2025): Quantifying the Gray Zone: A Framework for Measuring Hybrid Warfare Power Balances, Small Wars Journal, June 17, 2025.
[193] Luberisse, J. (2025): Verification Cost Asymmetry in Cognitive Warfare: A Complexity-Theoretic Framework, arXiv preprint, July 28, 2025.
[194] TROPIN, Z. (2021): Lawfare as part of hybrid wars: The experience of Ukraine in conflict with Russian Federation. *Security and Defence Quarterly*, Vol. 33, No. 1. 15–29. DOI: https://doi.org/10.35467/sdq/132025
[195] MUNOZ MOSQUERA, Andres B. – BACHMANN, Sascha Dov: Lawfare in Hybrid Wars: The 21st Century Warfare. In: *Journal of International Humanitarian Legal Studies*, Vol. 7, No. 1, 2016, 63–87. o. DOI: 10.1163/18781527-00701008
[196] RONDEAUX, C. (2025): The Legal Counteroffensive to Russia's Hybrid War. *Lawfare*, 2025. április 6.
[197] LUBERISSE, J. (2025): Verification Cost Asymmetry in Cognitive Warfare: A Complexity-Theoretic Framework, arXiv preprint, July 28, 2025.
[198] Miként Mao és Guevara hivatkozott műveiben megjelenítésre kerül.
[199] HOFFMAN, F. G. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars. Potomac Institute for Policy Studies, Arlington.
[200] MUNOZ MOSQUERA, Andres B. – BACHMANN, Sascha Dov: Lawfare in Hybrid Wars: The 21st Century Warfare. In: *Journal of International Humanitarian Legal Studies*, Vol. 7, No. 1, 2016, 63–87. o. DOI: 10.1163/18781527-00701008

amelyet a NATO stratégiai dokumentumai is kiemelten kezelnek. Ezen összefüggés indokolja, hogy ebben a kontextusban vizsgáljam meg ezeket témaköröket.

Tekintettel arra, hogy a kutatásom elsődleges célja olyan eddig kiaknázatlan, vagy csak részben felhasznált tapasztalatok és ismeretek tudományos alapú feldolgozása, amelyek egy objektív keretben új közjogi megoldások kiindulópontjaként szolgálhatnak, ebben a kontextusban különös figyelmet érdemelnek az elmúlt évek katonai és politikai eseményei, különösen az úgynevezett „színes forradalmak" és az alább részleteiben vizsgált Geraszimov-doktrína kapcsán megjelent elemzések[201], valamint a kutatásomon alapuló, általam valószínűsített értékítélet. Természetesen nem lehet elégszer hangsúlyozni, hogy rendkívül fontos, hogy ezeket a magyarázatokat és elemzéseket megfelelő kritikával kezeljük, hiszen a történelem során ritkán tárult fel olyan „sikeres titkos" terv, amely széles körben hozzáférhető volt, kivéve azokat, amelyek valójában figyelemelterelésnek szántak.

A gerilla hadikultúra jellegzetességeinek vizsgálata, különös tekintettel a különleges hírszerzési műveletek elhárítására, elengedhetetlen. A Geraszimov által javasolt megközelítés rávilágít arra, hogy a tudományos eszközökkel történő újraértékelés nem csupán akadémiai, hanem állami, szakpolitikai és politikai szintű célkitűzés és feladat is. Ennek érdekében a kutatóknak a (had)történelmi és rendészettudományi ismereteket úgy kell rendezniük, hogy a szintetizált tudásanyag a jogalkotás szintjén hasznosíthatóvá váljon.

Ez a folyamat magában foglalja az adott területek elméleti és gyakorlati aspektusainak alapos megértését, valamint azok integrálását a jelenlegi jogi és politikai keretrendszerbe. A cél az, hogy a kutatás eredményei hozzájáruljanak a nemzetbiztonsági stratégiák, törvények és irányelvek hatékonyabb kialakításához és végrehajtásához, figyelembe véve a különböző hírszerző és elhárító tevékenységek sajátosságait és kihívásait. Az ilyen jellegű kutatások elősegítik a kormányzati döntéshozók és a szakpolitikusok munkáját, lehetővé téve számukra, hogy megalapozott és célhoz (pontosabban) kötött döntéseket hozzanak a nemzetbiztonság területén.

A gerilla hadikultúra és a hibrid hadviselés közötti összefüggések a nem hagyományos hadviselési módszerekre és stratégiákra vonatkoznak, amelyek célja, hogy kiegyenlítsék a

[201] TOMOLYA János: Az úgynevezett „Geraszimov-cikk" margójára. In.: Hadtudomány 2018/3-4. pp.79-99.

katonai erők közötti hagyományos egyensúlyhiányt. A gerilla hadviselés egy olyan taktika, amely kisebb, gyakran nem hivatalos katonai csoportok által használt, ahol a hagyományos frontvonalas összecsapások helyett a meglepetésre, a gyors mozgásra és a civil lakosság közötti rejtőzködésre építenek. A cél az, hogy eltérítsék és kimerítsék az ellenséges erőket, miközben kihasználják a helyismeretüket és a helyi lakosság támogatását.[202]

A hibrid hadviselés egy összetettebb fogalom, amely magában foglalja a gerilla hadviselés elemeit, de kiterjed a konvencionális és nem konvencionális, valamint a katonai és nem katonai eszközök egyidejű és integrált használatára. Ez magában foglalhatja a kiberháborút, a dezinformációs kampányokat, az ötödik hadoszlop (belső ellenséges elemek) taktikáit, valamint a politikai és gazdasági nyomást. A hibrid háború célja gyakran az ellenfél megzavarása és annak politikai, gazdasági és társadalmi rendjének aláásása.

A két fogalom közötti összefüggés abban rejlik, hogy mindkettő adaptív és rugalmas megközelítést alkalmaz, amely képes reagálni az ellenfél változó stratégiáira és kihasználni annak gyengeségeit. Mindkettő kiemeli a ”puha erő„ jelentőségét és gyakran épít a civil lakosság bevonására vagy befolyásolására. A gerilla hadviselés és a hibrid háború egyaránt jelentős kihívást jelenthetnek a hagyományosan felkészült és felszerelt haderők számára, mivel ezeket nehéz észlelni, azonosítani és semlegesíteni.

A gerilla hadviselés és a hibrid hadviselés között számos összefüggés figyelhető meg:

- Mindkét hadviselési forma aszimmetrikus jellegű, azaz a felek katonai képességei és erőforrásai között jelentős egyenlőtlenség áll fenn. A gyengébb fél gerilla- és hibrid taktikákkal ellensúlyozza hátrányát.
- Mindkét esetben jellemző a szokványostól eltérő, nem konvencionális harcmodor és hadviselés. Ez magában foglalhat szabotázsakciókat, rajtaütéseket, terrorcselekményeket, de akár kiber- és információs hadviselést is.
- A civil lakosságot és infrastruktúrát gyakran használják „pajzsként”, illetve a kritikus pontok elleni támadások eszközeként. Ez rontja a konvencionális erők manőverezési képességét.

[202] A fejezet egyes gondolatai 2019-ben Hódos László: Gondolatok a gerilla-hadviselés elleni küzdelem egyes összefüggéseinek tudományos vizsgálatáról címmel jelentek meg In: SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA 17 : 3 pp. 67-80. , 14 p.

Mindkét esetre jellemző lehet a reguláris és irreguláris erők kombinálása, a „hibrid" taktika, ahol a szabályos alakulatokat felkelők vagy gerillák egészítik ki. A jogi-politikai hadszíntéren való tevékenység, például a propagandában és dezinformációban való jártasság is fontos szerepet kap mindkét hadviselési formában.

A modern hibrid hadviselésre jelentős hatást gyakoroltak a korábbi évszázadok gerilla-hadviselés tapasztalatai és taktikái. Ugyanakkor a hibrid hadviselés ennél összetettebb megközelítést, illetve vizsgálatot igényel.

Előzetesen tisztázni szükséges, milyen formákat és típusokat indokolt a téma szerint összefüggésben megkülönböztetni. „*A gerilla hadikultúra a nem állami, nem reguláris, hanem sok esetben önszerveződő, felszereltségében és logisztikai ellátottságában gyenge hadviselő feleket jellemzi",*[203] *amelyek célja az ellenségnek tekintett állami vagy idegen hatalom meghátrálásra kényszerítése, vagy megdöntése és a hatalom átvétele. A gerilla hadviselés jellemzője annak elhúzódó, rejtett és kiszámíthatatlan jellege".*[204]

---

[203] A szervezett bűnözést folytató bandák, drogbárók szintén aszimmetrikus hadviselési módszereket alkalmaznak, de a gerilla hadviseléssel és a terrorizmussal szemben nem politikai célból folytatnak tevékenységet, céljuk elsődlegesen az anyagi gyarapodás biztosítása, a gerilla pedig egy „felfegyverzett civil, akinek nem a karabély, vagy a machete az elsődleges fegyvere, hanem a közösséggel kialakított viszony, a nemzet ahol és amiért küzd". – TABER, Robert: *The War of the Flea: A Study of Guerrilla Warfare, Theory and Practice*. The Citadel Press, New York, 1970, p. 21.

[204] A Magyar Hadtudományi Társaság 2005. november 3-án tartotta – a Magyar Tudomány Ünnepe alkalmából rendezett eseménysorozat részeként – az év legnagyobb lélegzetű szakmai-tudományos konferenciáját, A katonai erő újszerű alkalmazása a 21. század elején címmel. A konferencián elhangzottak a Hadtudomány 2005/4. számában kerültek megjelenítésre, így a Porkoláb Imre által a harmadik szekcióban előadott Aszimetrikus hadviselés: az ortodox és a gerilla hadikultúra összecsapásai című előadása is. A gerilla hadikultúra az államtól független, rendszertelen, gyakran önszerveződő erőket jellemzi, amelyek korlátozott felszereléssel és logisztikai támogatással rendelkeznek. Célja az ellenségként tekintett állam vagy külföldi hatalom visszavonásra kényszerítése vagy megdöntése, hosszadalmas, rejtett és kiszámíthatatlan hadviseléssel. A helyi lakosság támogatása elengedhetetlen a gerilla hadviselés sikeréhez. A gerilla taktikák védelmi stratégiákat foglalnak magukban, miközben taktikailag támadó műveletek a rendfenntartó egységek vagy állami létesítmények megsemmisítésére irányulnak. Miként Porkoláb kifejti, a gerilla hadviselés nem új jelenség, története olyan régi, mint maga a háború, és gyakran a konfliktusok gyengébb oldalának módszere. A nagy, jól szervezett hadseregek hajlamosak lenézni a gerilla módszereket, és az ortodox hadseregek általában nem vesznek részt gerilla hadviselésben. Bár a gerilla erők néha szervezetlennek tűnhetnek, egy domináns, egyre változatosabb és gyakran meglepően sikeres kultúrát képviselnek a háborúban. A gerilla erők olyan módszereket alkalmaznak, amelyek a stratégiai szempontból gyengébb és kevésbé felszerelt oldalra jellemzőek. Ez tudatos választás és nem feltétlenül hátrány. Az ortodox hadikultúrájú hadseregnek erőfölénye van a gerilla erőkkel szemben, lehetővé téve a stratégiai kezdeményezéseket és a taktikai fölényt. A gerilla erők gyakran előnyben részesítik az ellenségtől való elszakadást, a visszavonulást és a kedvezőbb körülmények közötti újbóli harcba lépést. Porkoláb álláspontja szerint a gerilla hadikultúra elemzésekor két alapvető tényezőt kell figyelembe venni: a politikai irányultságot és az erőszak alkalmazását. A politikai tevékenységek közé tartozhat az információterjesztés, a demonstrációk szervezése, a toborzás, a kiképzés, a külső támogatás biztosítása, a lakosság társadalmi támogatása és a stratégiai tervezés. A gerilla hadviselés sikeressége a népszerűségen és az erőforrás-elosztáson múlik. A szervezeti struktúra

Porkoláb Imre hivatkozott művében a különböző hadikultúrák, különösen az ortodox és a gerilla hadikultúrák kölcsönhatását és összecsapásait vizsgálja a háborús kontextusban. A munka hangsúlyozza, hogy a hadikultúra egy nemzet, kisebbség vagy civilizáció kultúrájának szerves része, tükrözve a történelmi tapasztalatokat és az általános nézeteket a háború megvívásának módjáról. A modern katonai tudományban három alapvető hadikultúrát különböztetnek meg: a mozgás-centrikus, az anyag-centrikus és a gerilla hadikultúrákat.

Miközben a gerilla harcmodort, mint tevékenységsort elemezzük, álláspontom szerint arra a logikus következtetésre juthatunk, hogy a politikai célokból folytatott jogellenes irányultságú befolyásoló tevékenység az erőszak alkalmazása hiányában, illetve annak előkészületi fázisában is – már feltétlenül egy állam – biztonsági érdekeinek veszélyeztetését eredményezheti.

A politikai irányultság jogellenességének helyes értelmezéséhez szükséges azt is megjegyezni, hogy ez – demokratikus és jogállami keretek között – kizárólag Magyarország törvényben meghatározott honvédelmi, illetve nemzetbiztonsági érdekeinek ellenében szervezett, vagy működő csoportok tevékenységének vizsgálata során értelmezhető, illetve állapítható meg.

A haza (ön)védelme érdekében szerveződő fegyveres tevékenységet végző csoport és az idegen érdekek által motivált diverziós[205] tevékenységet végző csoportok vonatkozásában

két kategóriába sorolható: a szelektív rendszerek (kis elit csoportok) és a mozgósítási rendszerek (szélesebb lakossági bevonás). A hadikultúra kategorizálásához történelmi példákat, célokat és különböző szervezetek módszereit kell elemezni. Porkoláb hét gerilla hadikultúra típust azonosít ezek alapján. Hasonlóképpen, különböző gerilla hadviselési formákat vizsgálnak, amelyek változatos katonai válaszokat igényelnek. A tanulmány három alapvető formát különböztet meg. A művében kihangsúlyozza, hogy a klasszikus gerilla hadviselés operatív védelmet jelent, de taktikailag támadó műveletekkel igyekszik erőt gyűjteni a kívánt pszichológiai hatás és a végső politikai győzelem elérése érdekében. A hadviselés kezdeti szakaszaiban az erőforrások korlátozottsága miatt a gerilla hadseregek nem képesek nyílt harcot folytatni az ortodox hadseregekkel, és gyakran a kifárasztó stratégiát választják. Azonban a harmadik fázisban, amikor elérnek egy erőegyensúlyt, ezek az erők ortodox hadviselési módszereket alkalmaznak. Álláspontom szerint Porkoláb munkája hozzájárul az aszimmetrikus konfliktusok, különösen a gerilla hadviselés és az ortodox hadikultúrák összecsapásainak mélyebb megértéséhez, és kiemeli a gerilla hadikultúra sokszínű és fejlődő jellegét a modern hadviselés kontextusában. Gondolatainak vizsgálatát követően megállapíthatónak tartom, hogy a gerilla hadikultúra egyik meghatározó jellemzője a tevékenység politikai irányultsága és a változó intenzitású erőszak – egyidejű – alkalmazásának végső soron elkerülhetetlen volta.

[205] Szabó József (főszerkesztő): Hadtudományi lexikon. (Budapest: Magyar Hadtudományi Társaság, 1995.) p. 213.

Forgács Balázs Antoine Henri Jomini [206] és a nemzeti háború során végzett tevékenységének kutatása eredményeként megjelenített honvédő mozgalmak tudományos vizsgálata nyújtanak megfelelő elhatárolási alapot számunkra.[207] *„Jomini választ keresett arra is, hogy hogyan lehet a leghatékonyabban felhasználni a felfegyverzett népet a politikai célkitűzések eléréséhez: véleménye szerint a már említett szoros politikai kontroll mellett a regularizált nemzetőrség mint szervezeti forma biztosíthatja ezt a mindenkori állam számára."*[208]

A kutatási témám szempontjából fókuszba állított felforgató tevékenység vizsgálatával összefüggésben fontos megjegyezni, hogy a politikai harcok kiegészítője is lehet a gerilla tevékenység, ugyanis ez utóbbi nem jelent feltétlenül minden esetben folyamatos fegyveres küzdelmet, hiszen a fegyveres tevékenység átmenetileg hosszabb időn át szünetelhet is, miközben a küzdelem más formái folytatódnak.[209] Kovács Jenő a Szovjet katonai enciklopédia szócikke alapján a francia *partisan* kifejezésből származtatja[210] a második világháború idején a Szovjetunióban és Jugoszláviában kibontakozott ellenállási mozgalomban részt vevő harcosok elnevezését.

Ekkor a partizánok feladata az ellenség frontvonala mögé kerülve a kommunikáció megzavarása, az utánpótlási vonalak elvágása és az ellenség figyelmének elterelése volt. A tanulmányban és számos más publikációban az amerikai polgárháború partisan rangerei mintájaként szolgálóként kerül megjelenítésre a néhai hesseni jaeger alezredes által leírt és követett doktrína, azonban meg kell jegyezni, hogy az amerikai függetlenségi háború[211] időszaka könnyűgyalogosainak harctevékenységét vizsgálva, közvetve vagy közvetlenül az azóta létrehozott, vagy létrejött minden könnyűgyalogos egység harctevékenységére hatással volt.

---

[206] Bonaparte Napoleon, majd Sándor (orosz) cár tábornoka, a cári orosz vezérkari és hadiakadémia megteremtésében meghatározó szerepet játszó svájci származású katonai teoretikus (1779 és 1869 között élt).
[207] A témáról lásd Forgács Balázs – Szem Géza: A partizánság Magna Chartája. pp.24-27.; Forgács Balázs: A néppel az uralkodóért. Az első gerillaelméletek. pp.40-53.; JOMINI, Antoine Henri: A hadművészet meghatározása. pp.579-580.;
[208] Forgács Balázs: Antoine Henri Jomini és a nemzeti háború. In.: Koller Boglárka, Marsai Viktor (szerk.): Magyarország Európában, Európa a világban. (Budapest: Dialog Campus Kiadó, 2016.) p. 43.
[209] Kovács Jenő: Magyarország Katonai Stratégiája. (Budapest 1995.) p. 37.
[210] Kovács Jenő: Magyarország Katonai Stratégiája. (Budapest 1995.) p. 37.
[211] Ewald, Johann von 1744 és 1813 között élt. Művének eredeti címe Abhandlung über den kleinen Krigen nevet viselte és gyalogsági kapitányként szerezte a Hesse-Cassel –i herceg szolgálatában, kinyomtatásra Casselben került sor 1785-ben.

Sokak számára érdekes lehet az a megközelítés, amely a mű szellemiségét jellemzi, hiszen a hollywoodi kasszasikereken (például az 1985-ben Amerika fegyverben, 2000-ben A hazafi címen bemutatott filmeken) felnőtt, történelem iránt érdeklődő közösség számára az amerikai függetlenségi háború partizánjai és reguláris erői szemszögéből ismert ez a történelmi időszak. Az angol Ward[212] kapitány alárendeltségében szolgáló hesseni katonák Hoboken településének és az amerikai royalista menekültek védelmében 1780. július 20-án tett erőfeszítéseiről nem készült film. A kölcsönös kegyetlenkedések leírására jó példaként szolgál azonban, hogy a hősies helytállásra úgy motiválta katonáit a kapitány, hogy figyelmeztette őket arra, hogy miként kezelnék őket a lázadók. A Wardnak tulajdonított mondatok szerint jobb a halál, mint a fogságba esés. A védekező harc sikeres volt, a hat ágyú által kilőtt közel hatvan ágyúgolyó sem tudta megtántorítani a royalistákat, akik végül a rájuk bízott menekültek[213] többségét meg tudták védeni.

Von Johann Ewald művében számos szabályt fogalmazott meg, különösen az amerikai partizánok elleni küzdelem szakszerű megvívására vonatkozóan, és ezeket a brit és a velük szövetséges erők által megtapasztalt példákkal támasztotta alá. A harcban résztvevő angol és vele szövetséges németajkú egységek és parancsnokok jelentős vérveszteségek árán komoly tapasztalatokra tettek szert, melyet később a Napóleon ellen vívott háborúk során kamatoztattak. A gerilla hadviselésre vonatkozóan Jomini munkásságán túl a regulázott irreguláris erők alkalmazására láthatunk példát a napóleoni háborúk idejéből a spanyol gerillacsapatok szabályzatának tanulmányozása során is.[214] Mindezek alapján megállapítható, hogy „*a gerillaelméletek megszületésének kiindulópontját a 19. század elejére tehetjük"*[215], amely a szabályozott, politikai célú, erőalkalmazás ismérveivel felruházott új hadikultúra intézményesített alkalmazásának kezdetét jelenti.

Az aszimmetrikus hadviselés egy másik fontos mérföldköve a gerilla hadviselés bizonyos elemeit felhasználó politikai befolyásolási tevékenység megjelenése. Ez a tevékenység, amely magában hordozza az erőszakos cselekedetek közvetlen vagy közvetett fenyegetését, a hibrid hadviselés egyik potenciális módszere lehet. Ez akkor válik különösen jelentőssé, ha az állami

[212] Ward kapitány neve von Johann művének következő, 96. oldalán Warth-ként szerepel.
[213] A mű a refugees kifejezést alkalmazza, ugyanakkor megjeleníti azt is, hogy közöttük voltak a hadsereg favágói is (vélhetően „műszaki egységeként, kiszolgálóiként").
[214] Forgács Balázs: Reglamento de Partidas y Cuadrillas – Az első gerillaszabályzat. In.: Hadtudományi Szemle 2017. X. évfolyam 1. szám pp. 23-35.
[215] Forgács Balázs: A néppel az uralkodóért. Az első gerillaelméletek. pp.21-57.

szervek, különösen a nemzetbiztonsági szolgálatok, nem ismerik fel és nem hárítják el időben és proaktívan ezt a fenyegetést szakszerűen irányított intézkedések keretében.

2. *A Geraszimov-doktrína és a hibrid hadviselés orosz modellje*

A gerilla hadviselés egyes (erőszakmentes) jellemzőit magán hordozó szerveződések vonatkozásában felismerhető egy párhuzam a Geraszimov doktrína egyes meghatározó elemeivel. Valerij Geraszimov, orosz vezérkari főnök által írt, *A tudomány jelentősége a haladásban* címet viselő www.vpk-news.ru[216] honlapon elérhető cikkét Tomolya János elemezte[217] és arra a következtetésre jutott, hogy *„egyértelmű, hogy mind tartalmi, mind formai szempontok szerint nem beszélhetünk egy új hadviselési formát, vagy doktrínát meghirdető dokumentumról. (Megjegyzi, az érvényben lévő orosz katonai doktrína sem használja a hibrid hadviselés vagy a hibrid háború kifejezést.)"* [218] A tanulmány rámutat arra, hogy a szakterülettel foglalkozó elemzők, illetve szakírók kicsit túlértékelik a doktrína hatását a hadikultúrákra, a hadművészet művelőire, illetve az aktív katonai-politikai vezetésre. Kiemeli továbbá azt is, hogy megítélése szerint a hadtudomány művelőitől kér segítséget Geraszimov, annak elismerése mellett, hogy *„Elméleteket nem lehet parancsra létrehozni."*[219] Ugyanakkor meg kell jegyezni azt, hogy a hadviselés új formáinak és a hazai tapasztalatok újraértelmezését Geraszimov is céljaként tűzi ki[220], külön kiemelve az afganisztáni és az észak-kaukázusi háborúk ismérveit.

Geraszimov cikkéből világosan látszik, hogy a nevéhez kötött új hadviselési koncepció, illetve doktrína és az ehhez köthető intézkedéssorozat a gerilla (az ő terminológiáját követve partizán) hadviselés és az erőszakmentes diverziós csoportok egyidejű alkalmazásának lehetőségét reális, végrehajtható célkitűzésnek, illetve működtethető modellnek tartja.

Figyelemmel arra, hogy a politikai-katonai vezetők által kinyilatkoztatott módszerek alkalmazásra is kerültek a közelmúltban – Tomolya cikkében rámutat, hogy az oroszok mindig

---

[216] Valerij Geraszimov: Cennoszty nauki v predvigyenii. Megjelent 2013. március 5-én Moszkvában, a Voenno-promyshlennyi kurier (Hadipari Hírek) 8. évfolyam 476. számának 1–2. oldalán.
[217] Tomolya János: Az úgynevezett „Geraszimov-cikk" margójára. In.: Hadtudomány 2018/3-4. pp.79-99.
[218] Tomolya János: Az úgynevezett „Geraszimov-cikk" margójára. In.: Hadtudomány 2018/3-4. p. 86.
[219] Valerij Geraszimov: Cennoszty nauki v predvigyenii. Megjelent 2013. március 5-én Moszkvában, a Voenno-promyshlennyi kurier (Hadipari Hírek) 8. évfolyam 476. számának 2. oldalán.
[220] Az eredeti mondat („Рассуждая о новых формах и способах вооруженной борьбы, мы не должны забывать отечественный опыт. Это применение партизанских отрядов в годы Великой Отечественной войны, борьба с иррегулярными формированиями в Афганистане и на Северном Кавказе.") saját fordítása.

külföldi beavatkozást sejtenek[221] ezen befolyásoló műveletek mögött – ezért érdemes a demokratikus jogállamok nemzetbiztonsági szerveinek is proaktívnak lenniük, hiszen a beavatkozás eddig sosem járt a várt (pozitív) eredménnyel, minden színes forradalmat anarchia és súlyos válság követett.

Érdemes megjegyezni, hogy *„a legjobb módja a béka főzésének, ahogy a közmondás tartja, hogy elég lassan emeljük a hőmérsékletet, így a béka nem veszi észre, hogy megfő. Ha az elkövetők meghackelték a tűzhely szoftverét, tagadták felelősségüket, és hamis hírekkel bombázták a járókelőket, mielőtt annektálták volna a konyhát, akkor ez egy működő analógia lehet a hibrid hadviselésre".*[222] Vagyis egy hibrid hadviselést alkalmazó állam instabilitást gerjeszt egy másik állam belügyeiben, elsősorban nem kinetikus katonai eszközöket használva, mint a kiberháború és befolyásolási műveletek, gazdasági nyomásgyakorlás, helyi ellenzéki csoportok támogatása, dezinformáció és bűnözői cselekmények. Ez magában foglalhatja nem egyértelműen azonosított csapatok vagy irreguláris harcosok titkos bevetését, de a hibrid hadviselés gyakran támaszkodik kiberműveletekre és államokon kívüli szereplőkre. A hibrid hadviselés stratégiai előnye, hogy elrejti az agresszor állam beavatkozását. Még a legcsekélyebb tagadás is elegendő lehet a nemzetközi felháborodás késleltetésére vagy enyhítésére, ami egyébként komoly nemzetközi válaszreakciókat válthatna ki.

A „hihető tagadás képessége" kétségtelenül szükséges minden hibrid művelet esetében, amennyiben lehull a lepel a valódi elkövetőről, illetve a valódi szándékról, annak háború is lehet a végkifejlete az érintett felek, illetve szövetségi rendszerek között.

A hibrid hadviselést leggyakrabban az elmúlt évtized agresszív orosz külpolitikájával hozzák összefüggésbe.[223] Oroszország hibrid hadviselés iránti elkötelezettségét Valerij Geraszimovnak tulajdonítják, az orosz fegyveres erők vezérkari főnökének. 2013-ban Geraszimov megfogalmazta a hibrid hadviselésről alkotott nézetét, mint az aszimmetrikus választ a globalizált világban terjedő liberális demokráciára, bár az orosz írások, beleértve Geraszimovét is, nem használják valójában a „hibrid hadviselés" kifejezést, hanem inkább a „nem lineáris" vagy „új generációs" hadviselést. Ez Carl von Clausewitz háborúról alkotott

[221] Tomolya János: Az úgynevezett „Geraszimov-cikk" margójára. In.: Hadtudomány 2018/3-4. p. 80.
[222] CANTWELL, Douglas: Shadow Wars: Hybrid Warfare in the Legal and Strategic Gray Zone. *per Concordiam - Journal of European Security and Defense Issues*, Vol. 10, Issue 1, 2020, p. 41.
[223] CANTWELL, Douglas: Shadow Wars: Hybrid Warfare in the Legal and Strategic Gray Zone. *per Concordiam - Journal of European Security and Defense Issues*, Vol. 10, Issue 1, 2020,

felfogásának korrelátuma, vagyis a háború az a politika folytatása más eszközökkel. Geraszimov megfigyelte, hogy „a nem katonai eszközök szerepe a politikai és stratégiai célok elérésében nőtt, és sok esetben meghaladták a fegyverek erőhatását hatékonyság tekintetében". Ennek eredményeképpen szorgalmazta a „politikai, gazdasági, információs, humanitárius és egyéb nem katonai eszközök széles körű használatát — összehangolva a lakosság tiltakozási potenciáljával", amelyet „rejtett jellegű katonai eszközökkel kell kiegészíteni". Természetesen nem szabad megfeledkezni arról sem, hogy *„valójában a katonai erő és a nem katonai eszközök integrált alkalmazása nem új dolog: a propaganda, a gazdasági eszközök, a félrevezetés, a szabotázs, a bomlasztás mindig is a hadviselés részei voltak".*[224]

A szakmai vélemények eltérhetnek abban, hogy mely eseteket sorolják a hibrid háború kategóriájába.[225] Oroszország 2008-as grúziai inváziója és az abból következő, de facto annektálása Abházia és Dél-Oszétia területeinek, műveletei 2014-ben Krím megszállására és annektálására, valamint a „kis zöld emberkék" telepítése, ami az Donyecki Népköztársaság és a Luhanszki Népköztársaság kelet-ukrajnai kikiáltásához vezetett, az orosz hibrid hadviselés legtisztább példái. A Natia Seskuria által írt, 2021 szeptemberében publikált tanulmány[226], a „Russia's 'Hybrid Aggression' against Georgia: The Use of Local and External Tools" az értekezésem szempontjából kiemelkedő jellemzők figyelembevételével elemzi Oroszország grúziai hibrid műveleteit (agresszióját), valamint a kialakult helyzetet.

A tanulmány a 2008-as orosz-grúz háború 13. évfordulójáról emlékezik meg, amikor az orosz csapatok megszállták Grúzia területeit, jelentős politikai és gazdasági károkat okozva. Azóta Oroszország a hagyományos katonai eszközök helyett hibrid eszközök alkalmazására váltott, hogy finomabban és költséghatékonyabban állítsa helyre befolyását Tbiliszi felett. Oroszország megszállta Grúzia területének 20%-át kitevő Cshinvali régiót és Abháziát. Azóta folyamatosan megsérti a tűzszüneti egyezményt, militarizálja az elfoglalt területeket, és akadályozza a nemzetközi megfigyelő missziók hozzáférését.

Grúzia demokratizálódása és a NATO-val való kapcsolatok erősödése miatt Oroszország hibrid eszközöket vet be, hogy aláássa Tbiliszi nyugat-barát politikáját. Oroszország

[224] Simicskó István: A hibrid hadviselés előzményei és aktualitásai. Hadtudomány, 2017/3–4. szám, 3–16.
[225] A témában a NATO: Countering hybrid threats. folyamatosan frissülő NATO-weblapon megjelenő írások tanulmányozása ajánlott.
[226] SESKURIA, Natia: Russia's „Hybrid Aggression" against Georgia: The Use of Local and External Tools. Center for Strategic and International Studies (CSIS), 2021.:

„határszabályozó” politikával fokozatosan foglalja el Grúzia területeit, ami a helyi lakosság emberi jogait súlyosan sérti. Oroszország dezinformációs kampányokat folytat, hogy megkérdőjelezze a Nyugat iránti grúz elkötelezettséget, és előnyben részesítse a hagyományos orosz értékeket.

Amit az orosz agresszió ellenére a grúz lakosság támogatása a Nyugat iránti integráció iránt növekszik. A nyugati támogatás kulcsfontosságú a grúz demokratizációs folyamat megfordítására irányuló orosz törekvések ellen. Grúzia esete nem izolált, a demokratizáció és nyugatiasodás sikeressége Grúziában a nyugati értékek sikerét jelenti egy autoriter rezsimmel szemben. Grúzia esete nemcsak helyi, hanem regionális és nemzetközi jelentőséggel is bír, mivel a demokratizálódás iránti törekvések és a nyugati értékek iránti elkötelezettség kerül közvetlenül veszélybe az orosz hibrid műveletek eredményeként, ami közvetlen hatással van a régió stabilitására és a globális geopolitikai dinamikákra.

Előbbiekkel összefüggésben fontos megjegyezni, hogy a hibrid háborúnak nem kell terület annektálásához vezetnie.[227] Egy dezinformációs kampány, amely kormányellenes zavargásokat szított, majd egy kibertámadás, amely megbénította Észtország digitális infrastruktúráját 2007-ben, Macedónia 2016-os és Montenegró 2017-es bonyolult puccskísérleteinek irányítása, jobboldali politikai pártok támogatása Franciaországban és Németországban, valamint beavatkozás az 2016-os Egyesült Államok választásba mind beleillenek Geraszimov hibrid háború leírásába. Inkább nem csak elszigetelt esetek vagy taktikák leírójaként értendő a hibrid háború, hanem mint egy nagyszabású stratégia, amelynek célja a meglévő liberális demokratikus jogrendek destabilizálása.

Azt, hogy a hibrid háború, mint a nemzetközi közjogi hadviselés előzmények nélküli új eszköze lenne sokan – kiemelten a II. fejezetben hivatkozott szerzők – megkérdőjelezik, ennek okán nem találunk minden hibrid hadviselésre vonatkozó jellemzőt pontosan meghatározó egyértelmű definíciót sem. Minden állam valamilyen formában folytat rejtett akciókat és a nem katonai eszközök az alapvető diplomáciai eszközei. Emellett a hibrid háború hasonlóságokat mutat mindkét ellenséges blokk által végrehajtott műveletekkel a hidegháború csúcspontján és sok modern állam által az irreguláris háborúskodás címén. A szkeptikusok ezért

[227] NEAL, John J.: Deterrence in a Hybrid Environment: Defending against Nonlinear Threats. *per Concordiam - Journal of European Security and Defense Issues*, Vol. 10, Issue 1, 2020, pp. 16-23.

megkérdőjelezték azt, hogy valóban van-e újdonság a hibrid háborúban a kiber képességek bevezetése és maga a név mellett. Azok az államok, amelyek a „frontvonalban", illetve közvetlenül szembesülnek Oroszország felől megjelenő hibrid fenyegetéssel, igennel válaszoltak erre a kérdésre, a stratégiai gondolkodásba beépítve azt a célt, hogy ellensúlyozni tudják a hibrid háborús fenyegetést, a különleges technikákat. A teljes megértése a hibrid háborúnak, mint stratégiai fogalomnak, azt igényli, hogy helyesen illeszkedjen a nemzetközi jogban meghatározott erők, eszközök, módszerek (jog)szabályozási kereteibe.

A hibrid konfliktusok jogi aspektusainak kezelése magában foglalja a hibrid kampányok, mint agresszió formáinak megfelelő elismerését és az erőszakos beavatkozást jelentő hibrid intézkedések meghatározására irányuló elméleti munkát.[228] Ebben az értelemben olyan kezdeményezések, mint az Európai Kiválósági Központ Hibrid Fenyegetések Elleni Küzdelemre történő létrehozása, üdvözlendő fejlemények. Fontos, hogy a hibrid háború körüli növekvő kutatások beépítsék a nemzetközi jog meglévő szókincsét, ami fontos lépés a „szürke zóna" háborús ködének eloszlatása felé.

Az orosz befolyásolási tevékenység elemzése, amely a nyugati sajtóban és szakértői elemzésekben is széles körben megjelenik, különösen figyelemre méltó a hibrid háború kontextusában, mint például az Ukrajnában zajló konfliktus esetében. Ezekben az elemzésekben gyakran negatív előjellel ábrázolják Oroszország tevékenységét, hangsúlyozva a hibrid hadviselés veszélyeit és kockázatait. Ez alátámasztja azt az állítást, hogy bármely hatalom által támogatott vagy befolyásolt cselekedetek, különösen, ha hibrid hadviselési eszközöket használnak, gyakran tragikus következményekkel járnak.

A demokratikus jogállamokban, amelyek az európai értékrendet képviselik, a nemzetbiztonsági szolgálatok felelnek az ilyen típusú tevékenységek felismeréséért és kezeléséért, szigorú jogszabályi keretek és ellenőrzés mellett. A nem demokratikus rendszerekben ugyancsak a nemzetbiztonsági szervek látják el az elhárító tevékenységeket, ám ezek gyakran az állam és annak vezetőinek biztonságának védelmére irányulnak, gyakran a törvényesség határait feszegetve vagy átlépve.

[228] VOYGER, Mark: Waging Lawfare: Russia's Weaponization of International and Domestic Law. *per Concordiam — Journal of European Security and Defense Issues*, Vol. 10, Issue 1, 2020, p. 32.

A nemzetbiztonsági szolgálatok feladata a nemzetbiztonsági érdekeket sértő vagy veszélyeztető tevékenységek, például potenciális diverziós akciók felismerése és megelőzése. Ezek a szolgálatok elsősorban a titkos információgyűjtés módszereit alkalmazzák, amelyek tudományos vizsgálata és újraértelmezése elengedhetetlen a hatékony fellépés és az illegális tevékenységek megelőzésének, akadályozásának vagy korlátozásának biztosítása érdekében.

Ezért fontos, hogy a nemzetbiztonsági szolgálatok állandóan frissítsék és fejlesszék módszertanukat, figyelemmel kísérve a nemzetközi trendeket és technológiai fejlődéseket, hogy hatékonyan tudjanak reagálni a változó kihívásokra és fenyegetésekre.

A hibrid fenyegetések jelentette veszélyeztetés természetét, a nemzetbiztonsági szolgálatok felelősségét és a jogalkotás lehetőségeit ezen a téren tanulmányában a legújabb terminológiát alkalmazva mégis közérthető módon Szabó Károly foglalja össze: *„A befolyásolási művelet és az abban alkalmazott eszközök – kompromittálás, propaganda, dezinformáció, felforgatás –, a hibrid fenyegetések az állam működéséhez szükséges funkciókat támadják a célországban. Az egyetlen kézenfekvő megoldásnak az tűnik, ha a kémelhárítás az államilag irányított politikai, katonai, gazdasági, társadalmi, információs, infrastrukturális és titkosszolgálati befolyásolás teljes vertikumának lefedésére törekszik. Egy állam részéről a „vegytiszta" hírszerző tevékenység meghaladása, a hihető tagadás lehetősége és a technikai, az infokommunikációs eszközök kontroll nélküli alkalmazása szinte ellehetetleníti a kémkedéssel szembeni büntetőjogi szankcionálást."* [229]

3. A hibrid hadviselés eszközrendszerébe tartozó, ún. befolyásoló műveletek jogi szempontrendszer szerinti megközelítése

A befolyásolás szerepe a nemzetbiztonsági műveletekben kiemelkedően fontos. A nemzetbiztonsági műveletek során a befolyásolás többféle formában is megjelenhet, és számos célból használható fel. A befolyásolás lehet egy proaktív eszköz az államok kezében, hogy elősegítsék saját politikai, gazdasági vagy katonai érdekeiket a nemzetközi arénában. Ez magában foglalhatja például a propagandát, a stratégiai kommunikációt és a PsyOps-t, amelyek célja más államok vagy csoportok véleményének, érzéseinek és magatartásának alakítása.

[229] SZABÓ Károly: A katonai kémelhárítás feladatrendszerének új vonásai Európa és Magyarország megváltozott biztonsági környezetében. In.: Felderítő Szemle XVII. évfolyam 2. szám p.186.

A befolyásolási műveletek lehetnek védekező vagy elhárító jellegűek is, amelyek arra irányulnak, hogy megvédjék az országot az idegen befolyástól, például a dezinformációs kampányoktól, támadásoktól a kibertérben vagy a társadalmi feszültségeket kihasználó felforgató műveletek hatásaitól.

A befolyásolás modern eszközei közé tartozik a közösségi média és más online platformok használata, amelyek lehetővé teszik a gyors és célzott üzenetek terjesztését. Az információs technológia fejlődésével ezek az eszközök egyre hatékonyabbá válnak, és lehetővé teszik a nemzetbiztonsági szervek számára, hogy finom hangolást végezzenek a befolyásolási stratégiáikon, valamint például a szakszerűen végrehajtott hálózatelemzéssel a művelet forrásait is eredményesen határozhatják meg, ami az elhárító tevékenység szempontjából kiemelkedő jelentőséggel bír.

„Az eddigiekhez hasonlóan fontos kiemelni, hogy az ország biztonságának garantálása körében a rendszerváltást követően a nemzetbiztonsági tevékenység elsődleges funkciója a kormányzati döntéshozatal támogatása a hírszerzés és elhárítás eszközrendszerével, amely tevékenységet a politika parlamenti ellenőrzés mellett felügyeli és irányítja, valamint amelynek központi fogalma már nem a konspiráció, hanem az információ.”[230]

Az idegen hírszerző szolgálatok tevékenysége, amely elsősorban, de nem kizárólagosan a hazánkban folytatott információgyűjtést foglalja magában, kulcsfontosságú a nemzetközi politikai és biztonsági dinamikákban. Ezek a szolgálatok különféle módszereket alkalmaznak az információ megszerzésére, amely lehet stratégiai, gazdasági, katonai vagy akár politikai jellegű. Az ilyen típusú hírszerzés célja gyakran a hazai vagy nemzetközi döntéshozatal befolyásolása, illetve a számukra fontos információk megszerzése. Fontos megjegyezni, hogy a befolyásolási műveletek etikai és jogi kérdéseket is felvetnek. A demokratikus társadalmakban a kormányzati befolyásolásnak összhangban kell lennie az átláthatóság, a jogállamiság és az egyéni szabadságjogok tiszteletben tartásának alapelveivel, ha ezt egy paradox helyzetnek tartjuk, akkor nem járunk messze a valós helyzetképtől.

[230] JÁVOR Endre: A nemzetbiztonsági szolgálatok társadalmi megítélése, támogatottsága, a média szerepe a társadalom véleményalkotásának formálásában. *Felderítő Szemle*, 8. (2009) 2. sz., 63. o.

Ezzel párhuzamosan a nemzetbiztonsági szolgálatoknak kiemelt feladatuk a hazánkban folytatott idegen hírszerzési tevékenységek felderítése és (meg)akadályozása. Ez magában foglalja a kémtevékenység, az ipari kémkedés és más titkos információszerzési módszerek felismerését és semlegesítését. A nemzetbiztonsági szolgálatoknak széleskörű eszközrendszer áll rendelkezésére, beleértve a megfigyelést, ellenhírszerzést és a kiberbiztonsági műveleteket, ezek végtelen számú kombinációját.

A megszerzett információ önmagában azonban kevés, hiszen a valódi értékét az információ felhasználásával, azaz a tudás tárgyiasításával, átváltásával és hasznosításával éri el. Ez különösen fontos a befolyásolásra irányuló tevékenységek esetében, ahol az idegen szolgálatok manipulatív módszereket alkalmazhatnak, például dezinformációt, propagandát vagy PSYOPS-t. Az ilyen típusú manipuláció célja a közvélemény vagy döntéshozók befolyásolása, katonai, politikai vagy gazdasági célok elérése érdekében. Nyilván egy védelmi ipari beruházás vonatkozásában mindhárom cél egyszerre támadható, vagy érhető el. Például egy kiemelkedő jelentőségű védelmi ipari létesítmény elhelyezésének a külföldi vállalat által Magyarországon, vagy egy jól sikerült ellenérdekű titkosszolgálati művelet keretében más szomszédos államban.

A nemzetbiztonsági szolgálatoknak ezért nem csupán az információszerzési tevékenységek feltárására kell összpontosítaniuk, hanem a megszerzett információk értelmezésére, elemzésére és hatékony felhasználására is. Ennek érdekében szükséges a szolgálatok állományának folyamatos képzése, technológiai fejlesztése és a nemzetközi együttműködés erősítése, hogy képesek legyenek az idegen befolyásoló tevékenységek hatékony kezelésére és az állami, illetve nemzeti érdekek védelmére, továbbá azok érvényesítésére külföldön is.

A titkosszolgálatok aktív műveleteiben egyre inkább megjelenő manipulációs eszközök és módszerek felderítésére és megakadályozására irányuló szakmai tevékenység végrehajtása során felmerül a kérdés, hogy a jogalkotás – mely természetéből eredően a megtörtént esetek tanulságait alapul véve képes jogi fogalmakat, adott esetben büntetőjogi tényállásokat teremteni – tudja-e absztrahálni ezeket? A vizsgálat eredményessége céljából figyelembe kell venni, hogy a szakmai érvek, megismert tapasztalatok (proaktivitás eredményének) feldolgozását követheti csak a jogalkotói (reaktív) választevékenység, amely a jogi természetű felhatalmazást bővítheti a szolgálatok jog-, és hatáskörét illetően.

A diverzió, vagy a hírszerző tevékenység egyes részcselekményeit, tényállási elemeit a hazai és a külföldi jogszabályi előírások több esetben már szankcionálják (elég csak az illegális fegyverkereskedelemre, a vesztegetésre, a kémkedésre gondolnunk), azonban egyes stádiumaiban csak valamely tevékenység elkövetésére utaló információkról beszélhetünk, vagyis a rendelkezésre álló információk, adatok alapján nem tudható, hogy a nemzetbiztonsági szolgálat látókörébe került, titokban szerveződő és tevékenykedő csoport gerilla hadviselésre készül az állammal, illetve annak polgáraival szemben vagy egy szervezett bűnözői csoport támogatását „csupán" azért végzi, mert illegális fegyver-, vagy kábítószer csempészésben érdekeltek a résztvevők.

Ugyanakkor azt is megfigyelhetjük, hogy a szervezett bűnözés a helyi szinten megszerzett erőszak monopóliumát utóbb gyakorta igyekszik politikai (célú) tőkévé kovácsolni, sok esetben a történészek képesek a rejtett összefüggéseket – a küzdelem kimenetelétől függően – minősíteni, mint a Cosa Nostra esetében a II. világháború alatt szicíliai partraszállás során kialakult eseménysort, mikor az Egyesült Államokban honvédelmi és nemzetbiztonsági érdekből kapcsolatokat építettek ki a haditengerészet és a maffia között.[231]

New York kikötője nagyon fontos volt, tartottak a német és az olasz kémek szabotázsakcióitól. Ez utóbbiak jól el tudtak rejtőzni a nagy létszámú (amerikai) olasz közösségekben. Ezért a kikötő biztonságáért felelős Radcliffe Haffenden őrnagy, az ONI [232] főtisztje felvette a kapcsolatot a hírhedt maffiózó Lucky Lucianoval, aki annak ellenére, hogy 5 évi börtönbüntetését töltötte, emberén, Joe Lanzán keresztül megtartotta a kikötői illegális tevékenység feletti ellenőrzését.

A hírhedt maffiózó a New York-i kikötő olasz kém-, és szabotőrhálózat felgöngyölítését lehetővé tevő titkos információgyűjtés mellett egy nagy jelentőségű befolyásoló műveletet is támogatott Szicíliában. A CIA elődjének az OSS-nek a helyi viszonyokról, a számba vehető baráti és ellenséges személyekről adott át információkat, hálózatot épített ki. [233]

[231] Kaputa László: Fejezetek a maffia történetéből. In.: Szakmai Szemle. 2011/1. sz. 23-57.
[232] Office of Naval Intelligence – Egyesült Államok Haditengerészeti Hírszerző Hivatala
[233] 1942. június 13-án hozták létre az OSS-t az Office of Strategic Services-t (OSS), vagyis a Stratégiai Szolgálatok Hivatalát, amely jogelődje volt a háború után megalakított Központi Hírszerző Ügynökségnek (Central Intelligence Agency-nek – CIA)

Az ONI által alkalmazott, ténylegesen a maffia által végrehajtott befolyásolási művelet egy különösen hatásos példa arra, hogyan lehet katonai és politikai célokat elérni a hírszerzés eszközeivel. Ebben az esetben a maffia „egy visszautasíthatatlan ajánlatot” tett a Szicíliában állomásozó olasz katonai egységek tagjainak. Az ajánlat lényege az volt, hogy a katonák dezertáljanak és szabotázsakciókat hajtsanak végre, cserébe családjuk biztonságáért. Ez a művelet szemléletesen mutatja be, hogyan lehet a hagyományos katonai erők helyett pszichológiai és szociális nyomásgyakorlással hatékony (katonai) eredményeket elérni. A maffia, kihasználva a helyi hálózatát és a személyes kapcsolatait, meggyőzte a katonákat, hogy a legjobb megoldás a dezertálás, ezzel jelentősen gyengítve az olasz katonai erőket, lerövidítve a háborút, az ország és a lakosság szenvedését.

Az eredmények magukért beszéltek: a szövetséges erők megérkezésekor az érintett négy hadosztályból kettőnek a 70%-a már dezertált. Ez jelentős hatással volt a katonai erőviszonyokra, és elősegítette a szövetségesek sikereit. Ebben az esetben a hírszerzés és a befolyásolás összekapcsolódása különösen hatékony volt, hiszen a maffia ismerte a helyi társadalmi berendezkedést, kiemelten a „hangadókat” és képes volt manipulálni a katonákat a szövetségesek érdekei szerint.

Ez az eset rámutat arra, hogy a hírszerző műveletek nemcsak a hagyományos információgyűjtésre korlátozódnak, hanem magukban foglalhatnak komplex pszichológiai és társadalmi manipulációt is, amelyek jelentősen befolyásolhatják a kinetikus természetű küzdelem kimenetelét is. A maffia által végrehajtott „visszautasíthatatlan ajánlat” példája bemutatja, hogy a hírszerzés milyen mértékben tudja befolyásolni az emberi döntéseket és viselkedést a katonai konfliktusokban, különösen jogrendszerben érvényesíthető előnyök felhasználásával, illetve a nemzetközi közjog, érdekeinek megfelelő értelmezésével.

A szövetségesek partraszállása után a maffia célkitűzése a beszivárgás volt azoknak a településeknek a vezetésébe, amelyet az AMGOT (Allied Military Government of Occupied Territories) támogatott. Miután kihasználta a harcok idején a fekete piacot, a Cosa Nostra a háború után főként a kábítószerből kezdett gazdagodni. A maffia tagjainak erőfeszítéseit sok esetben siker, vagyis politikai stallum (kiemelten polgármesteri, képviselői tisztség) elnyerése követte. A politika és maffia együttműködése azokban az évtizedekben, az USA-ban és

Olaszországban sosem látott méreteket öltött és az aktuálpolitikai összefüggéseket nem vizsgálva, Kaputa Lászlót idézve a mai napig igaz az, hogy *„a Maffia azóta is él és virul…”*[234]

1943. július 22-én Patton tábornok elfoglalta Szicília fővárosát, Palermót, mindössze két órával Monty előtt. Alig 19 nappal később az szövetséges csapatok beléptek Messinába, ezzel véget vetve a szicíliai hadjáratnak és az Operation Underworld-nek, ami az előbb megjelenített titkos művelet fedőneve volt. A haditengerészet azonnal megsemmisítette az összes bizonyítékot, amely a szervezett bűnözéssel való együttműködését igazolta. A „nem bizonyítható egyezség” alapján Lucky Luciano végrehajtási kegyelmet kért a haditengerészettel való együttműködésére alapozva. Kérelmét elfogadták, és 1945. január 9-én az idősödő bűnözőt szabadon engedték, ugyanakkor kiutasították az USA-ból. Luciano szabadon bocsátása és kiutasítása azt mutatja, hogy milyen mértékben voltak hajlandóak a kormányzati erők kompromisszumokra és együttműködésre a szervezett bűnözéssel, különösen a háborús időkben.

A történelmi (háborús) példán keresztül felismerhető és elemezhető, hogy egy nagyszabású befolyásoló művelet tervezése, illetve végrehajtása során nem lehetnek „morális” fenntartásai az állami, különösen a nemzetbiztonsági szerveknek. Radcliffe Haffenden őrnagy története, ugyanakkor minden hasonló területen szolgálatot teljesítő szakember számára tanulságul kell, hogy szolgáljon, hiszen a főtiszt és közvetlen beosztottjai a háború végén gyorsan leszereltek és hátat fordítottak a titkosszolgálati munkának. Haffenden őrnagy máig nem tisztázott körülmények között távozott a hírszerzéstől. Saját bevallása szerint nem fegyelmi okokból, de egyes nyilvánosságra került dokumentumok tartalma alapján arra lehet következtetni, hogy a Maffiával kialakított kapcsolat során, vélhetően ő is kompromittálódott, de korábbi érdemeire tekintettel, szépen, csendben engedte el a Cég a kezét. Röviddel leszerelése után, néhány éven belül, mivel az egészsége is megromlott, lakóhelyén, New Yorkban hunyt el.

Az előbbiekben ismertetett befolyásoló művelethez leginkább hasonló, nehezen definiálható tevékenység meghatározására szolgáló, kodifikált büntetőjogi tényállás a kémkedés – tisztán jogi megközelítésben – egy idegen hatalom vagy idegen szervezet részére Magyarország elleni hírszerző tevékenység folytatását jelenti. Olyan kifejezést alkalmaz,

[234] Kaputa László: Fejezetek a maffia történetéből. In.: Szakmai Szemle. 2011/1. sz. p.57.

melynek feloldása a jogalkalmazás – kiemelten az igazságszolgáltatás – számára nehézséget okozhat, elsősorban a befolyásolási műveletek büntetőjogi megítélésének vonatkozásában, amelyek a kémkedés megvalósításának a megváltozott biztonsági környezetben megjelenő, gyakori elkövetési magatartásait jelenthetik.

Hazánk büntetőhatalmi igényeinek érvényesítésével összefüggő – hírszerző tevékenység, illetve befolyásoló művelet nemzetbiztonsági szolgálat általi detektálása eredményeként előkészített – döntés meghozatala mindenkor Hazánk nemzetbiztonsági érdekeinek és az eset összes körülményeinek együttes mérlegelését megkövetelő, kormányzati aktus. A nemzetbiztonsági szolgálatok tevékenységükre vonatkozó jogszabály előírása szerint[235] nem kötelesek büntetőeljárást kezdeményezni és átadni az adatokat, ha azzal veszélyeztetnék az e törvényben meghatározott feladataik ellátását.

Magyarország alkotmányos rendje alapján ez képezi a nemzetbiztonsági szféra tevékenységének a határát, ezen túl, vagyis (időben) ezt követően valósulhat meg egy, a nyomozóhatóság, illetve az igazság-szolgáltatás működésére jellemző jogintézmény, illetve önálló intézkedés alkalmazása (előzetes letartóztatás, szabadságvesztés; viszont elfogás és előállítás a nemzetbiztonsági szolgálat hivatásos állományú tagja által is foganatosítható).

Ez egyben – a hírszerzési tevékenység kifejezésének jogi vagy szakmai értékelésére tekintet nélkül – jelenleg és a jövőben is erős kontrollfunkciót valósít meg a nemzetbiztonsági tevékenység fölött. Hiszen kizárólag a nemzetbiztonsági szolgálatokról szóló, továbbá a büntető igazságszolgáltatás kereteit meghatározó sarkalatos törvények (érdemi) módosításával alkalmazható a jelenleginél súlyosabb jogkorlátozást eredményező jogintézmény.

A „hírszerző tevékenység” büntetőjogi értelmezésének újragondolása jelentős hatással lehet arra, hogyan kezelik a jogalkalmazók az egyes felderített manipulációs műveleteket. Az ilyen műveletek tanulságai, valamint a megszerzett és bizonyított tények értékelése alapján dönthető el, hogy egy adott tevékenységet szakmai és jogi szempontból kémkedésként, vagy egy új, speciálisan megnevezett jogi kategóriaként kell-e kezelni, különösen akkor, ha azt idegen hatalmak vagy szervezetek hajtották végre.

[235] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 44. § (2a) bekezdése alapján

Ez az újraértelmezés különösen fontos lehet a nemzetközi kapcsolatok és a nemzetbiztonság kontextusában, ahol az idegen felek (hatalmak, szervezetek, NGO-k) által végrehajtott befolyásolási tevékenységek egyre összetettebbé és kifinomultabbá válnak. A jogalkotók és jogalkalmazók előtt álló kihívás az, hogy meghatározzák, mikor minősül egy adott tevékenység kémkedésnek, manipulációnak vagy más, újonnan definiált bűncselekménynek.

Az értekezésem lezárásának idején folyamatban lévő, nemzeti szuverenitás védelmében tervezett intézményi és jogi reformok hatásait a jövőbeni kutatások fogják meghatározni. Ezek a kutatások megbízható tudományos alapokon nyugodva, az intézményi változások és jogi reformok következményeit fogják elemezni és értékelni. Ez magában foglalhatja a hírszerzési tevékenységek jogi kereteinek módosítását, a nemzetbiztonsági szolgálatok hatásköreinek újraértékelését, valamint a nemzetközi hírszerzési együttműködés formáinak átalakulását. [236]

„A 2010-es évek védelmi szférát érintő struktúra-, és funkciómegosztás-változásai után látni kell, hogy Magyarország sem kerülheti ki azt az európai tendenciát, amely főként a terrorizmus, a hibrid konfliktusok és kibertérből érkező támadások elleni védelem, valamint a migráció kezelésének tengelyén egy megújulási, változási folyamatot sürget a nemzetbiztonsági tevékenység szervezése, képességfejlesztése és irányítása terén. Ebbe a koncepcióba illeszkedik, a 2018 nyarán létrehozott Nemzeti Információs Államtitkárság is, amelynek különleges szerepe van a hírszerzés összetett rendszerének koordinálásában." [237]

Ezért fontos, hogy a kutatók, jogászok, szakmai, illetve politikai döntéshozók folyamatosan figyelemmel kísérjék és elemzéseik tárgyává tegyék a nemzetközi és hazai jogi,

[236] A koordináltabb védelmi működést és irányítást szolgáló megoldásokat nemzetközi összehasonlításban is találunk, aminek egyik legtöbbet hivatkozott mintája az Amerikai Egyesült Államok. Emellett azonban fontos az is, hogy a hazai szakmai-tudományos gondolkodásban is elindult ennek az irányvonalnak a kibontakoztatása. A külföldi megoldások és különösen az amerikai minta kapcsán lásd: BÉRES János (szerk.): Külföldi nemzetbiztonsági szolgálatok. Zrínyi Kiadó, Budapest, 2018. pp. 66-79.; SÁFRÁN József: Az Amerikai Egyesült Államok és Magyarország nemzetbiztonsági szervezetrendszerének összehasonlító elemzése, Felderítő Szemle 2018/1. pp. 71-87. A koordinált és hatékonyabb védelemszervezés és irányítás vonatkozásában lásd: KESZELY László: védelmi igazgatás szerepe a nemzeti szintű átfogó megközelítés megvalósításában. Nemzeti Közszolgálati Egyetem, doktori értekezés, Budapest, 2017.; LAKATOS László – VARGA Attila Ferenc: A magyar honvédelmi igazgatás, In: FARKAS Ádám – KÁDÁR Pál (szerk.): Magyarország katonai védelmének közjogi alapjai. Zrínyi Kiadó, Budapest, 2016, pp. 159-211.; FARKAS Ádám: A védelmi kötelezettségtől a fegyveres védelem rendszeréig, Katonai Jogi és Hadijogi Szemle 2018/1. pp. 7-22.; FARKAS Ádám: Gondolatok az állam fegyveres védelmének lehetséges intézmény-fejlesztési irányairól, Katonai Jogi és Hadijogi Szemle 2017/1-2. pp. 103-124.

[237] HÓDOS László: Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szervének közjogi helyzetéről. In.: Szakmai Szemle 2018/4. p. 5.

politikai és biztonsági fejleményeket, újításokat, hogy megfelelően megérthessék és saját felelősségi körükben kezelni tudják az ezeken a területeken bekövetkező változásokat.

4. Összegzés, az elvégzett vizsgálat és részkövetkeztetések

A kérdéskör vizsgálata során kiemelt jelentőséggel bírnak Kiss Álmos Péter gondolatai, miszerint a *„NATO és az Európai Unió 2014-ben, az Ukrajna elleni orosz támadás során figyelt fel a hibrid hadviselésben rejlő veszélyekre. Az azóta megjelent elemzések nagy része is az ukrajnai műveletekből vezeti le a hibrid hadviselés lényegét. Sikeres műveletek tanulmányozása nagyon jó megközelítés, de magában hordozza azt a kockázatot, hogy a megismert sikeres eljárások ismétlését várjuk a jövőben is. A hibrid hadviselő azonban mindig a műveleti környezet körülményeihez igazítja eljárásait – egy másik állam ellen, más hadviselő által végrehajtott hibrid művelet valószínűleg semmiben nem fog hasonlítani az ukrajnaihoz”.* [238] A folyamatosan változó biztonsági környezet és az ellenérdekű felek kreativitása ugyanis végtelen számú forgatókönyvet képes előállítani, így a biztonsági és védelmi szektor munkatársainak folyamatosan fejleszteniük kell a társadalom, az állam és ezen belül a szervezeteik ellenállóképességét a Magyarországgal, illetve szövetségesei ellenében folytatott hibrid hadviselés intézkedéseivel szemben.

A fejezettel összefüggő kutatási részcél az eddig kiaknázatlan vagy részben felhasznált tapasztalatok és ismeretek tudományos feldolgozása volt, amelyek új közjogi megoldások alapjául szolgálhatnak. Az elemzés különös figyelmet fordít az elmúlt évek katonai és politikai eseményeire, például a „színes forradalmakra” és a Geraszimov-doktrínára, ugyanakkor kritikus megközelítést tart szükségesnek. A gerillahadviselés és hírszerzési műveletek elhárításának vizsgálata a jogalkotásban is hasznosítható ismereteket kínálhat. A cél olyan szintetizált tudásanyag létrehozása, amely hozzájárulhat a hatékonyabb nemzetbiztonsági stratégiák és politikai döntések kialakításához.

A következő fejezetben ezért rögzítettem ennek a célkitűzésnek a stratégiai jogi normákban való megjelenítésével összefüggő kutatásaimat és támasztottam alá a stratégiai jogi

[238] KISS Álmos Péter: A hibrid hadviselés természetrajza, In.: HONVÉDSÉGI SZEMLE: A MAGYAR HONVÉDSÉG KÖZPONTI FOLYÓIRATA (2008-), 147 (4.). (pp. 17-37.) p.34. ISSN 2060-1506

normaalkotás megfeleltethetőségének szükségességét bizonyítani a jogi hadviselés szempontrendszere alapján.

V. A NEMZETI BIZTONSÁGI STRATÉGIÁBAN AZONOSÍTOTT EGYES KOCKÁZATOK VIZSGÁLATA A STRATÉGIAI NORMAALKOTÁS ÉS A LAWFARE SZEMPONTRENDSZERE ALAPJÁN

1. Bevezető, megállapítások a stratégiai jogi norma tartalmáról általánosságban

Magyarország Kormánya elfogadta Magyarország Nemzeti Biztonsági Stratégiáját[239] (a továbbiakban: NBS, vagy hatályos NBS). Ez a korábbi, 2012-ben elfogadott előző, azonos elnevezésű stratégiai dokumentumot helyezi hatályon kívül. A 2012-ben kiadott jogi norma elfogadását követően számos, egész Európát és benne természetesen Magyarországot is cselekvésre kényszerítő esemény történt. Talán ezek közül leglátványosabb a tömeges migráció megjelenése volt 2015-ben. Ennek során hazánk transzport útvonallá változott, emiatt a kormányzat azonnali és határozott lépéseket tett, melynek során az Ideiglenes Biztonsági Határzár is kialakításra került. A 2020-ban kiadott hatályos NBS éppen emiatt került kihirdetésre, reaktív adaptációt felmutatva a legújabb kihívásokra is. Ezen régi és új fenyegetések közötti vizsgálatot végeztem el annak érdekében, hogy feltárjam a stratégiai szintű normaalkotás eredményességét ezen biztonságpolitikai alapdokumentum tekintetében. A fejezet további célja, hogy az NBS VII. fejezetében megjelenített Kiemelt biztonsági kockázatokkal összefüggésben a hazánkat érő kihívások, kockázatok és fenyegetések nemzetbiztonsági aspektusait vizsgálja. Az előbbiek közül jelen fejezetben kiemelten a c), d) és o) pontban rögzítettekkel foglalkozom, mivel a nemzet biztonsága szempontjából egyformán jelentős biztonsági kockázatok közül véleményem[240] szerint ezek rendelkeznek leginkább aktualitással, a tudományos és a védelmi szektor figyelme napjainkban ezekre fókuszál legjobban.

A stratégiai szintű jogi normaalkotás, ideértve egy törvény vagy kormányrendelet

[239] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

[240] A fejezet egyes elemeit tartalmazó publikációm 2020-ban, Gondolatok Magyarország Nemzeti Biztonsági Stratégiájában azonosított kiemelt biztonsági kockázatok nemzetbiztonsági aspektusairól címmel jelent meg In.: SZAKMAI SZEMLE: A KATONAI NEMZETBIZTONSÁGI SZOLGÁLAT TUDOMÁNYOS-SZAKMAI FOLYÓIRATA 17 : 3 pp. 21-31.

megalkotását, módosítását eredményező, nemzetbiztonsági szolgálatok által felderített információn alapuló, szervezet és funkciófejlesztésre vonatkozó holland példán keresztül ismertetem továbbá az NBS-en túl a fejezet címe szerinti tapasztalatokat és ezekből további következtetéseket vonok le.

A jogi norma célja, hogy meghatározza az ország biztonságpolitikájának alapvető irányvonalait és válaszokat adjon a nemzetbiztonság előtt álló kihívásokra. A stratégia a nemzetbiztonság széles spektrumát lefedi, beleértve a katonai, gazdasági, társadalmi, környezeti és információs biztonságot.

A stratégia kiemelt figyelmet fordít a hibrid fenyegetésekre, amelyek egyesítik a hagyományos és nem hagyományos katonai eszközöket, valamint a politikai befolyásolást és az információs műveleteket. A cél az, hogy Magyarország képes legyen megvédeni magát a különböző külső és belső fenyegetésekkel szemben, miközben előmozdítja nemzetközi érdekeit és részt vesz a kollektív védelemben és biztonságban.

A stratégia hangsúlyozza a nemzeti szuverenitás védelmét, az állam intézményeinek és infrastruktúrájának biztonságát, valamint a polgárok életminőségének és biztonságának javítását. Továbbá figyelembe veszi a kiberfenyegetéseket és az információs térben való tevékenység fontosságát is.

Az NBS meghatározza az ország nemzetbiztonsági célkitűzéseit, valamint azokat a politikákat és intézkedéseket, amelyeket ezek eléréséhez meg kíván valósítani. Az NBS az alábbi alapvetéseken nyugszik:[241]

- *Magyarország egy szuverén, független és demokratikus állam.*
- *Magyarország az Európai Unió és a NATO tagja.*
- *Magyarország elkötelezett a jogállamiság és az emberi jogok védelme mellett.*
- *Magyarország elkötelezett a viták békés rendezése mellett.*
- *Magyarország elkötelezett nemzeti érdekeinek védelme mellett.*

[241] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

Az NBS a következő nemzetbiztonsági fenyegetéseket azonosítja: [242]

- *Terrorizmus,*
- *Szervezett bűnözés,*
- *Kiberbűnözés,*
- *Tömegpusztító fegyverek,*
- *Hibrid fenyegetések,*
- *Természeti katasztrófák, és a klímaváltozás.*

Az NBS a következő nemzetbiztonsági érdekeket és azok védelmének fontosságát azonosítja:[243]

- *A magyar emberek biztonsága,*
- *Magyarország területi integritása,*
- *Magyarország szuverenitása,*
- *Magyarország függetlensége,*
- *Magyarország demokratikus állam és jogrendje,*
- *A jogállamiság Magyarországon,*
- *A magyarok emberi jogai,*
- *Magyarország gazdasági prosperitása,*
- *Magyarország társadalmi összetartása,*
- *Magyarország kulturális identitása,*
- *Környezetvédelem.*

Az NBS az alábbi politikákat és intézkedéseket vázolja fel a nemzetbiztonsági fenyegetések kezelésére és a nemzetbiztonsági érdekek védelmére:[244]

- *A magyar biztonsági erők megerősítése,*
- *A magyar hírszerző szolgálatok megerősítése,*
- *A magyar határbiztonság megerősítése,*
- *A magyar kiberbiztonság megerősítése,*

[242] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
[243] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
[244] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

- *A magyar terrorizmusellenes intézkedések megerősítése,*
- *A fegyverzetellenőrzési és non-proliferáció érdekében tett intézkedések megerősítése,*
- *A magyar katasztrófavédelmi intézkedések megerősítése,*
- *A klímaváltozással összefüggő intézkedések megerősítése.*

Valamint szakterületeik szerinti érintettséggel rendelkező ágazati együttműködés javítása, fejlesztése, különös tekintettel az összkormányzati feladatok ellátására.

2. Az NBS kiemelt biztonsági kockázatokként azonosított, a tanulmány szempontrendszere alapján fókuszba állított fenyegetésekről

A fejezet fókuszába az NBS[245] c), d) és o) pontja szerinti, alábbi fenyegetések közötti összefüggést, valamint az egymásra gyakorolt, hazánk veszélyeztetettségét növelő kölcsönhatást helyeztem:

„c) összehangolt és széleskörű diplomáciai, információs és titkosszolgálati műveletek, pénzügyi-gazdasági nyomásgyakorlással, pénzügyi spekulációs támadásokkal vagy katonai fenyegetéssel párosulva (hibrid) Magyarország destabilizálása, kormányzati cselekvőképességének, politikai stabilitásának és társadalmi egységének gyengítése, továbbá nemzetközi érdekérvényesítő képességének korlátozása céljából;

d) jelentős károkat okozó kibertámadások a kormányzati informatikai rendszerek, az E-közigazgatás, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra egyéb elemei és más, a társadalom működésében fontos szervezetek számítógépes hálózatai ellen;

o) a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenése és gyors terjedése;”.[246]

3. Hibrid típusú fenyegetések azonosítása és a hazai válaszlehetőségek

Az NBS VII. fejezet c) pontjában megjelenített jellemzőkkel bíró, új típusú fenyegetettség megjelenése, vagy inkább alkalmazása a nemzetközi színtéren egyre erőteljesebb és kiterjedtebb. Az alkalmazó e tevékenységsorozat közben a modern technológiák

[245] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról
[246] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

által nyújtott kifinomult lehetőségeket használja fel, és a gazdaságra, médiára, a kibertérre és a szociális érintkezés különböző formáira is kiterjeszti műveleteit. Az egyes elemek (támadó intézkedések) külön-külön vagy egymást erősítő hatású alkalmazása – a hagyományosnak tekinthető támadási formák használata nélkül is – már alkalmas lehet a befolyásolásra, a zavarkeltésre, egyes államok belső rendjének megbontására, a társadalom hangulatának formálására. Az új típusú fenyegetettség fokozott szintjére tekintettel Magyarország kiemelt feladatként tekint a hibrid fenyegetések elleni fellépésre, illetve azok kezelésére.

A hibrid kihívások nemzetbiztonsági szempontból történő azonosításának egyik meghatározó eleme, hogy a detektálhatóan ellenérdekelt szolgálathoz tartozó „hivatásos" vagy az állami szereplő kötelező jelenlétének keresését, felderítését mellőzhetjük, sőt érdemes is tágabb látókörrel keresnünk az intézkedés szereplőit, valamint forrását. Nem elengedhetetlenül szükséges a tevékenység irányítójára „foglalkozásszerű összeesküvőként" tekinteni. Miként az NBS V. fejezete, Magyarország biztonsági helyzetének elemzése során rámutat, „az állami és nem állami szereplők által szponzorált politikai, gazdasági és társadalmi folyamatok befolyásolására irányuló stratégiák száma, változatossága és hatásfoka növekszik. A befolyásolás egyik eszköze lehet a nemzetközi közvélemény szervezett és módszeres Magyarország ellen hangolása. Az információs műveletek hatékonyságát növeli, hogy az álhírek, dezinformációk terjedését a közösségi média rendkívül gyorssá teszi. A nyílt befolyásolás politikai és gazdasági nyomásgyakorlásban is megjelenhet, amely során az ellenérdekelt nemzetközi szereplők korlátozni próbálhatják hazánk cselekvőképességét." Ez sokkal súlyosabb veszélyt jelent, a nem csak állami szereplőkkel szembeni küzdelemben tehát komolyabb erőforrás-ráfordítást igényel, mint korábban gondolhattuk. A nyílt politikai befolyásolás eszköze lehet egy olyan cikk megjelentetése, mely „véletlenül" tíz percen belül, tökéletes fordításban legalább három különböző nyelven jelenik meg a világ különböző pontjain és Magyarország mozgásterének jelentős korlátozását eredményezi.

Az Európai Unió új, 2019–2024 közötti időszakra vonatkozó stratégiai menetrendje a társadalom hibrid fenyegetések, rosszindulatú informatikai tevékenységek és dezinformáció elleni védelmének fontosságát emeli ki, továbbá hangsúlyozza, hogy az ilyen veszélyek kezelése átfogó megközelítést igényel, több kooperációval, koordinációval, erőforrással és komolyabb technológiai eszközpark bevetésével. Ez a feladatkör azért kimondottan bonyolult, mert a tevékenység leginkább a nemzetállamok elszigetelése, hiteltelenítése útján valósul meg, vagyis – akár az EU akár a NATO esetében – a tagállamok egymás iránti bizalmának

csökkentése a cél. Ennek ellensúlyozására válik rendkívül fontossá az ellenséges hírszerzési tevékenységgel szembeni ellenálló képesség erősítése.

A bűnüldözés hagyományos értelemben vett elsődleges feladatával ellentétben a nemzetbiztonsági funkció – érdemben – információgyűjtést, előzetes felderítést és elhárítást, továbbá – általában – megelőző jellegű tevékenységet hajt végre mind a környezet, mind a fenyegetések vonatkozásában. Ezzel a biztonság megőrzése (fenyegetés elhárítása) mellett tágabb értelemben is erősíti és előmozdítja a nemzeti érdekek érvényesítését (ideértve akár az ún. befolyásolást is), tehát rendeltetésében, feladatát tekintve és ebből adódóan eszközrendszerében és hatásköreiben is eltér a védelmi szféra többi ágazatától. A deklarált munkamegosztás mellett az NBS VIII. fejezetének 126. pontjában megjelenítettek szerint: *„Az azonosított kihívások megelőzése, kezelése és elhárítása elsődlegesen nemzeti felelősség, amely a Kormány feladata, együttműködésben a társadalommal. A biztonság elsődleges alapja a szilárd társadalmi, gazdasági és pénzügyi szerkezet, valamint nemzeti szinten a megelőző és védelmi intézkedések fenntartható és rugalmas rendszere, ezen belül pedig a haderő, valamint a rendvédelmi szervek (a rendőrség, a büntetés-végrehajtás, a nemzetbiztonsági szolgálatok, a katasztrófavédelem és rendvédelmi feladatai tekintetében az állami adó- és vámhatóság) célirányos fejlesztése.”*[247]

Vagyis az állami szervek, kiemelten a rendvédelmi szervek és az egyedüli nemzetbiztonsági szolgálat, amely nem rendvédelmi szerv is egyben a Katonai Nemzetbiztonsági Szolgálat feladata a társadalommal közösen a biztonság garantálása. Az eltérő feladatrendszerből adódik, hogy hibrid kihívásokkal összefüggésben más eszközrendszer áll a Honvédség, a Rendőrség és egy nemzetbiztonsági szolgálat rendelkezésére.

Ezt a védelmi igazgatási szempontból is jelentős elkülönülést az Nbtv. indokolása is az alábbiak szerint rögzíti:

„Az államok nemzetbiztonsági érdekeik védelme és más nemzetek szándékainak megismerése érdekében igénybe veszik a nemzetbiztonsági szolgálatok sajátos, más szervezetek által nem helyettesíthető lehetőségeit. Az alapvetően titkos és rá jellemző eszközöket felhasználó nemzetbiztonsági tevékenység megfelelő jogi szabályozást igényel annak érdekében, hogy

[247] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

semmilyen körülmények között ne jelenthessen veszélyforrást a demokratikus jogrendre, ezen belül az állampolgári jogokat csak akkor és olyan mértékben korlátozhassa, amennyiben az az ország nemzetbiztonságának megóvása, szuverenitásának érvényesítése céljából szükségszerű és indokolt." [248]

Magyarország Alaptörvénye határozza meg azt, hogy a nemzetbiztonsági szolgálatokat a Kormány irányítja, a szervezetükre, működésükre vonatkozó részletes szabályokat, a titkosszolgálati eszközök és módszerek alkalmazásának szabályait, valamint a nemzetbiztonsági tevékenységgel összefüggő szabályokat sarkalatos törvény határozza meg.

A kialakított struktúrában a nemzetbiztonsági szektormodellek alapján történő áttekintés eredményeként a magyarországi szolgálatokkal összefüggésben megállapítható, hogy még mindig érvényesül az egymással konkuráló szolgálatok között korlátozott az együttműködés. Ennek következtében detektálható esetleges hátrányok egy koordinatív funkcióval rendelkező kormányzati igazgatási szerv útján volnának ellensúlyozhatók, míg a vetélkedő jelleg erősségei hatékonyabban kihasználhatóvá válhatnak a megfelelő elemzést, értékelést felhasználó gyakorlati működéssel.

A koordináció és a különböző ágazatok közötti együttműködés szükségességét az NBS IV. fejezetében, hazánk alapvető adottságainak felsorolása során a jogalkotó kiemeli, miszerint *„a Hibrid támadással szembeni ellenálló képességünket növeli a nemzet egysége, demokráciánk szilárdsága, a közös nyelv, a felgyorsított döntéshozatali képesség, valamint a honvédelmi és rendvédelmi erők szoros együttműködése egymással és a releváns polgári infrastruktúrával. Az új biztonsági kihívások miatt azonban folyamatosan szükséges fejleszteni az információs és kiberhadviselés elleni védekezés rendszerét".* [249]

Mivel az érintett országgal szembeni hibrid hadviselés eredményessége az ott lévő, elhárító feladatokat ellátó szervek – egymással – konkuráló működése mellett jelentősen megnövekszik, ezért nem lehet elégszer hangsúlyozni, hogy a fenyegetés kivédése csak sokkal szorosabb együttműködés mellett lehetséges. Egy ilyen rendszer kialakításakor nem szabad megfeledkeznünk arról a korábban már említett gondolatról, miszerint a globális biztonsági

[248] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény általános indokolása alapján
[249] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

környezetben zajló változások következtében felértékelődik a hírszerzés és az elhárítás szerepe. A műveleti területre jellemző összetett kihívások, valamint a gyakran változó biztonsági helyzet szintén megnöveli a pontos és időbeni információk és értékelések iránti igényt. Ebben a kontextusban tehát különösen fontos, hogy a közvetítői rendszer kiépítése során is szem előtt tartsuk a hírszerzés és elhárítás fontosságát, hiszen a biztonsági környezet változásai és az összetett kihívások miatt egyre nagyobb az igény a pontos és időben érkező információkra. A közvetítői rendszernek tehát alkalmasnak kell lennie ezen igények kielégítésére is.

4. Fenyegetés a kibertérből és az arra adható válaszok egy külföldi esettanulmányon keresztül

Az információs műveletek és a bizalom aláásása során kiemelt jelentősége van a kibertérből érkező fenyegetések elhárításának. Az alábbi esettanulmány alapján érdemes a kölcsönös bizalom megrendülését előidéző szakmai hibák és a kibertámadások súlyos következményeit, továbbá az elhárításukra vonatkozó megoldásnak a hazai viszonyok közötti alkalmazhatósága lehetőségét jobban megvizsgálni.

Ez az NBS VII. fejezetének d) pontjában szereplő kiemelt biztonsági kockázat megvalósulásának egy véletlenszerűen kiragadott – a Holland Általános Hírszerző és Biztonsági Szolgálat (a továbbiakban: AIVD) által detektált és dokumentált – esete, amely az Amerikai Egyesült Államok korábbi egy elnökválasztását is beárnyékolta és az egész világ elektronikai információbiztonsággal foglalkozó szakembereit cselekvésre ösztönözte. Az ügy – kibervédelmi természetű – tapasztalatai a szervezet által az ország biztonsági helyzetének értékeléséről szóló éves jelentésébe is beépítésre kerültek, továbbá a szervezet fejlesztési koncepciójában is hasznosultak. Emiatt döntöttem az ezekből nyíltan elérhető adatok feldolgozására, hiszen a szakmai szervezetek hasonló jellegű támogató, döntéselőkészítő tevékenysége, a szakmailag is megalapozott, stratégiai szintű normaalkotás egyik legfontosabb támasza.

A védelmi képességek megerősítésének szükségességét globálisan elismeri a politikai vezetés, Magyarországon is. Ez a felismerés nem első kézből származó tapasztalatokból, hanem nemzetközi incidensek megfigyeléséből és azokból való tanulásból ered. Az Egyesült Államokban a 2020-as elnökválasztást követték a 2022-es képviselőházi és szenátusi választások. Ezek az események és a COVID-19 világjárvány az amerikai figyelem jelentős

részét Kína és Oroszország, különösen a választások elektronikus információbiztonsági kontextusában vonta magára.

A kiberműveletek területén releváns és számos – a kutatásom fókuszában álló szakmai területen – értékes tapasztalatot eredményező ügy, mondhatni „az orvosi ló esete", mely jelentősen befolyásolta a stratégialkotók gondolkodásmódját is, az úgynevezett COZY BEAR incidens. Ez az eset a Holland Királyság katonai és polgári nemzetbiztonsági szolgálatainak közös erőfeszítései eredményeként kerültek felderítésre. Az AIVD kulcsszerepet játszott az incidens felfedésében, ami fokozott biztonsági intézkedésekhez vezetett, mint például 2017 márciusi holland választáson a kézi szavazatszámlálás elrendeléséhez.

A COZY BEAR incidens 2014-ben kezdődött, amikor az AIVD észlelte a Demokrata Nemzeti Bizottság (a továbbiakban: DNC) elleni kibertámadásokat a COZY BEAR hackercsoport által, melyet az orosz kormányhoz köthetőnek tartottak (és tartanak ma is). A támadások során nagy mennyiségű adatot loptak el a DNC-től. Az amerikai kormányt tájékoztatták a holland szakemberek, de az Obama adminisztráció tartózkodott az oroszokkal szembeni megtorlástól, valószínűleg a feszültségek további fokozódásának elkerülése érdekében. Mindazonáltal ezek a kibertámadások jelentős hatást gyakoroltak a 2016-os amerikai elnökválasztásra és mind a mai napig a közbeszédet meghatározó témaként tekinthetünk rájuk.

Annak ellenére, hogy Oroszország tagadja az érintettségét, a támadások kifinomultsága és célzottsága összhangban áll az orosz hírszerző műveletekről rendelkezésre álló információkkal, különös tekintettel a kibertámadások végrehajtásának módjával. Nem lehet elégszer hangsúlyozni, hogy napjainkban a kibertámadások egyre inkább külpolitikai eszközként jelennek meg, potenciálisan súlyos hatást gyakorolva egy nemzet gazdaságára, infrastruktúrájára és általános értelemben vett biztonságára.

Hollandia, egy kis földrajzi területű, de gazdasági potenciálját tekintve globálisan jelentős ország, ipari termelés, mezőgazdaság, pénz és bankszektor, továbbá technológiai fejlettség szempontjából. A felderített fenyegetések nyomán a globális közvélemény, a biztonsági szakterületeken foglalkoztatott kollégák számára világossá vált, hogy nagyhatalmak kiberműveleteinek bármely ország áldozatává válhat. Válaszként Hollandia megerősítette kiberbiztonsági intézkedéseit technológiai beruházásokkal, képzési programokkal és a köz-

privát együttműködéssel. A COZY BEAR incidens fontos emlékeztető arra vonatkozóan, hogy a kiberhadviselés globális, határokat nem ismerő fenyegetés és hogy feltétlenül szükséges minden nemzet számára a reziliencia fejlesztése ezen a téren is.

Kiemelt kockázatként kezeli továbbá és 2020 jelentős kihívásaként azonosítja a jelentés a Hollandia elleni kémkedést és a nem kívánt befolyásoló tevékenységet. A kibertérben zajló Hollandiával szembeni kémkedés elsődleges megvalósítójaként Oroszországot nevezi meg a jelentés.[250]A dokumentumban a szolgálat kiemeli, hogy Oroszország a NATO és az EU szervei ellen is folytat kiberműveleteket és más eszközökkel, módszerekkel végrehajtott titkos információgyűjtő tevékenységet, amelyet a nemzetközi szervezetek tagállamai és partnerei közötti együttműködés gyengítése, a kölcsönös bizalom aláásása és saját geopolitikai befolyásának növelése céljából végez.

A szolgálat előbbiekben hivatkozott Tervei szerint jelentős erőforrásokat kíván fordítani az elektronikus információbiztonság erősítésére is, tekintettel az Oroszország, Kína és Irán felől érkező digitális támadások elhárításával összefüggő nemzetbiztonsági érdekre.[251] A digitális támadások vizsgálata során három kategóriát határoztak meg, melyek egyenként, de együttesen is alkalmazásra kerülhetnek a támadók által. Ezen tevékenységek a digitális kémkedés, a digitális befolyásolás és a digitális szabotázs. A befolyásolás talán legnehezebben azonosítható, vizsgálható kategóriáját az információs műveletek kifejezéskészletének alkalmazásával hajtotta végre a szolgálat. A szolgálat egyszerű, ugyanakkor rendkívül széles személyi és tárgyi hatály vonatkozásában érvényesíthető definíciója szerint a digitális befolyásolás digitális eszközökkel zavarja meg egy másik állam érdekeit, illetve működését. Az ide tartozó tevékenységek a szolgálat által végzett rendszerezés szerint:

- a kompromittáló információk (nem manipulált, de közzétételkor nem kívánatos információ) vagy,
- félrevezető információ (hamis vagy hamisított, illetve manipulált információ) megosztása.

Az információbiztonság támogatását elsődlegesen a biztonságtudatosság növelésével kívánja elérni a szolgálat, mely tevékenység során nagy hangsúlyt kíván fektetni az adatgazdák képzésére, oktatására is. Az ismeretek elsajátítását különösen tájékoztató kiadványok

[250] Elérhető: https://minbzk.sitearchief.nl/?subsite=aivd#search.1775639836085 (letöltés ideje: 2026.04.01.)
[251] Elérhető: https://minbzk.sitearchief.nl/?subsite=aivd#search.1775639836085 (letöltés ideje: 2026.04.01.)

készítésével és ajánlások megfogalmazásával szeretné elérni az AIVD a célkitűzéseikben megfogalmazottak szerint. A szolgálat honlapján közzétett adatok[252] szerint 21 szóbeli előadást tartottak és 39 biztonsági javaslatokat tartalmazó kiadványt adtak ki. Az elektronikus információbiztonság[253] megteremtésére törekvés során a holland szakmai és politikai elit arra a következtetésre jutott, hogy az AIVD szoros együttműködése a katonai társszolgálatával (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) és a Nemzeti Kiberbiztonsági Központtal (Nationaal Cyber Security Centrum – NCSC) elengedhetetlen. Ugyanilyen fontos a nemzetközi partnerekkel, valamint a partnerszolgálatokkal való együttműködés is. A migráció elleni küzdelemmel összefüggő biztonsági kihívások közül a holland nemzetbiztonsági szolgálat (AIVD) 2020. évre vonatkozó prognózisában[254] a dzsihadista terror, az extrémizmus, a radikalizáció elleni küzdelmet és proliferáció megakadályozását, mint kitűzött célt emelte ki. Az AIVD éves jelentésében[255] kifejtett álláspontja alapján, a radikális szalafista vezetők annak ellenére, hogy lényegében vallási szempontból (nominális értelemben legalábbis annak tekinthető) kisebbséget képviselnek, mégis rendkívül nagy befolyással rendelkeznek az iszlám vallási közösségen belül Hollandiában. Ennek okaként azt valószínűsítette a szolgálat, hogy a prédikátorok a (már) Hollandiában született fiatalabb generáció tagjait kiemelkedő hatékonysággal képesek megszólítani. A prédikátorok fellépésének köszönhetően sokan válnak radikális nézetűvé.[256] Hollandia[257] vonatkozásában megjelenő biztonsági kihívások

[252] Elérhető: https://minbzk.sitearchief.nl/?subsite=aivd#search.1775639605816: 2026.04.01.)
[253] Előbbihez szorosan kapcsolódik a gazdaságbiztonsági szempontból releváns információk védelmének szolgálat feladatai között megjelenített kötelezettség is. Az éves jelentés szerint Hollandia elemi érdeke, hogy a 2019-ben – az üzleti közösséggel és a tudományos intézetekkel együttműködésben előkészített, majd elfogadott Nemzeti rejtjelstratégia előírásainak megfelelő módon fejlessze a bizalmas információkat kezelő eszközöket, hiszen egy hagyományos eszközökkel vívott háború eszközének (harckocsi, harci repülő, harci helikopter) bekerülési költségéhez képest jelentéktelennek tűnő erőkkel és eszközökkel hatalmas, akár nemzetgazdasági szintű kárt lehet okozni állami, illetve gazdasági szereplőknek.
[254] Elérhető: https://minbzk.sitearchief.nl/?subsite=aivd#search.1775639481002 (letöltés ideje: 2026. 04. 01.)
[255] Elérhető: https://minbzk.sitearchief.nl/?subsite=aivd#search.1775639481002 (letöltés ideje: 2026. 04. 01.)
[256] A szolgálat által felderített információk alapján a fiatalok megközelítésének egyik eszköze az, hogy olcsó, tanórán kívüli foglalkozásokat biztosítanak számukra a radikális szalafisták, akiknek látszólag kiapadhatatlan forrásaik vannak adományokból és közel-keleti eredetű felajánlásokból eredeztethetően. A többségi (őshonos holland) társadalomtól való eltávolodás és később az esetlegesen kialakuló radikalizáció jelentik a legnagyobb veszélyt. Ugyanakkor azokat az iszlám vallású hívőket, akik nem azonosulnak ezzel az ultraortodox irányzattal, is terheli társadalmi nyomás, a többségi társadalom irányából, amely sajnálatos módon nem az integráció felé tereli őket.
[257] Az esettanulmányban szereplő állam előtt álló biztonsági kihívások részben történelmével összefüggő körülményekből eredeztethetőek (ide érthetők a migrációs háttérrel rendelkezők sajátos körülményeivel összefüggő biztonsági kihívások), míg a geopolitikai helyzetéből adódó kiemelt jelentősége, kulcspozíciója miatt a kibertér műveletek egyik legjelentősebb célpontjaként került beazonosításra Oroszország, Kína és Irán által.

vizsgálatakor nem szabad megfeledkezni a dzsihadista terrorizmus[258] jelentette kockázatról melyet szintén igyekszik működési területén felderíteni és elhárítani az AIVD és az MIVD. [259]

Az érdemben 2014 nyara óta működő Közös SIGINT és Kiber Egység (Joint Sigint Cyber Unit – JSCU) az AIVD és a MIVD közös egysége, amely más feladatai mellett a hírszerzés kiberműveletek révén történő fókuszálására koncentrál.[260] Ugyanezen a nyáron az egység tippeket kapott egy orosz hackercsoportról, amely egy moszkvai egyetemi komplexumban működik. A JSCU lobogója alatt működő AIVD csoportnak sikerült behatolnia az orosz belső számítógépes hálózatba. Az AIVD nemcsak a számítógépes hálózathoz szerzett hozzáférést, hanem a folyosón lévő biztonsági kamera felvételeihez is. A felvételeken látható személyekkel kapcsolatos információkat megosztották az amerikai hírszerző szolgálatokkal.

Hollandiában stratégiai szinten a kibervédelmi feladatok végrehajtását az Igazságügyi és Biztonsági Minisztérium alárendeltségébe tartozó Nemzeti Kiberbiztonsági Központ (Nationaal Cyber Security Centrum – NCSC) koordinálja.[261] A katonai kibertámadások elhárításáért a Kibervédelmi Parancsnokság (Defensief Cyber Command – DCC) szakmai alárendeltségében lévő Számítógépes Eseménykezelő Védelmi Csoport (Defensief Computer Emergency Response Team) felelős. A kiberhírszerzési (CYBINT) feladatok végrehajtása a MIVD feladata. Ebbe az intézményi rendbe illeszkedik a szolgálatok közös egysége a JSCU.

2014 őszén az oroszok hozzáféréshez jutottak a Fehér Ház nem minősített számítógépes hálózatához. Ez lehetővé tette számukra bizalmas feljegyzések és nem nyilvános információk megismerését Obama elnök utazásairól és sikeresen ellopták e-mailjeinek – legalább – egy részét. Ezeket a kiber manővereket is felfedte a holland hírszerző szolgálat és értesítette az amerikaiakat.

---

[258]Elérhető https://minbzk.sitearchief.nl/?subsite=aivd#search.1775640169638 (letöltés ideje: 2026. 04. 01.)

[259] A veszélyt jelentő egyének, illetve csoportok, vagyis a fő exogén dzsihadista fenyegetés Irak, illetve Szíria területe felől jelentkezik az al-Sham (ISIS), illetve az Al Qaida (AQ) által kiképzett harcosok képében. Kiemelt jelentőséget tulajdonít az előbbi országokból hazatérő, különösen a vélhetően harcokban részt vett holland állampolgársággal rendelkező személyek vizsgálatának, ellenőrzésének is a holland nemzetbiztonsági közösség, szoros együttműködésben a hazai rendvédelmi szervekkel és a nemzetközi partner szervezetekkel, illetve partnerszolgálatokkal.

[260] Ministerie van Binnenlandse Zaken en Koninkrijksrelaties – Ministerie van Defensie: Kamerbrief en convenant Joint Sigint Cyber Unit (JSCU). [Kamerstuk 29924, nr. 113.] 2014. július 3. Elérhető: https://zoek.officielebekendmakingen.nl/kst-29924-113.html (Letöltés ideje: 2026.04.01.)

[261] Hazánk a kibervédelmi képességeinek fejlesztése is elsődlegesen két pilléren nyugszik, amely a redundancia miatt helyes megoldásnak tartható. A katonai pillért a Katonai Nemzetbiztonsági Szolgálat, míg a polgári pillért a Nemzetbiztonsági Szakszolgálat biztosítja.

2014 novemberében, a hollandok detektálták, hogy az orosz hackerek sikeresen (újra) behatoltak a State Department számítógépes hálózatába. Miután a holland hírszerző vezetők erre felhívták a figyelmet, az amerikaiak az orosz támadást 24 órán belül sikerrel elhárították. A digitális összecsapást évekkel később egy aspen-i vitafórumon az NSA igazgatóhelyettese kemény kézitusaként aposztrofálta. A hírszerzési forrásokra támaszkodva a Washington Post azt írta, hogy egy nyugati szövetségese segítséget nyújtott a támadás elhárítása érdekében, azonban további részleteket nem jelenítettek meg.

2015 nyarán a holland hírszerző szolgálat volt az első, aki figyelmeztette amerikai kollégáit a Cozy Bear által a Demokrata Nemzeti Bizottság (az Amerikai Egyesült Államok Demokrata Pártjának igazgatási szempontból legfontosabb szervezete – röviden a DNC) elleni, egy, az orosz kormányhoz kötődő hacker csoport által végrehajtott kibertámadásra. A legtöbb nyugati hírszerző szolgálat feltételezi, hogy a csoportot az (orosz) SVR külföldi hírszerző szolgálat irányítja. A nyugati hírszerző szolgálatok és a kiberbiztonsági társaságok évek óta vadásznak a csoportra, amely szerte a világon, beleértve Hollandiát is, kormányzati ügynökségeket és vállalkozásokat támadott meg.

A Hollandia által a DNC-t, a Fehér Házat és más állami hivatalokat ért támadásról megosztott információk Robert Muellernek, az FBI által az amerikai választásokba való esetleges orosz beavatkozást kivizsgáló különleges ügyésznek az íróasztalára kerültek. A New York Times pedig az év decemberében bejelentette, hogy többek között Ausztráliából, az Egyesült Királyságból és Hollandiából származó információk alapján végezte a vizsgálatot az FBI.

Az előbbieket végrehajtó orosz hackereket[262] a hírszerző szolgálatok és a kiberbiztonsági társaságok a The Dukes és az APT29 néven ismerik, ám leginkább Cozy Bear néven említik őket. Az orosz hackerek egy másik csoportja a Fancy Bear (más néven APT28-cal) is felelős (a Cozy Bear mellett) a DNC elleni támadásokért. Ugyanis a Cozy Bear 2015 nyarán, míg a Fancy Bear 2016 áprilisában „kereste fel" a demokraták washingtoni szervereit. A hollandok 2016-ben is tetten érték a támadókat és ismét figyelmeztették az Egyesült Államok hatóságait.

[262] Bear on bear. *The Economist*, 2016. szeptember 22.

The New York Times beszámolt róla, hogy a DNC már hónapok óta nem vette komolyan az FBI figyelmeztetéseit.[263] Végül a Crowdstrike kiberbiztonsági vállalat vizsgálta ki az eseményeket a Demokrata Párt megbízása alapján, melynek során arra a következtetésre jutott, hogy a Cozy Bear és a Fancy Bear együttesen felelősek a támadásokért. Az amerikai hírszerző szolgálatok szerint az oroszok végül továbbították a Fancy Bear által megszerzett e-maileket a Wikileaks-nek, amely ezeket egyből közzé is tette. A publikált levélváltások óriási botrányt eredményeztek az akkori amerikai választási kampányban, ennek hullámai Hazánkban is érezhetők voltak (a magyar külpolitika orosz, illetve amerikai orientációjára utaló cikkek jelentek meg). Az incidens műszaki és technikai körülményeiről az ESET szoftverfejlesztő és forgalmazó cég készített elemzést, mely a biztonsági réseket és a felhasználói hibák sorát jeleníti meg.[264]

A rendelkezésre álló adatok (átadott információk) alapján az AIVD hackerek már nem férnek hozzá a Cozy Bear adataihoz. A sajtóértesülések szerint az amerikai hírszerzési munkatársak, politikai szereplők, akik 2017-ben egy nyugati szövetséges segítségét dicsérték a levelezésükben, vélhetően az alkalmazott eszközök és módszerek dekonspirálódását okozhatták. A nyilvánosságra kerülés a holland szakmai és politikai elitet is mélyen megrázta, nagyfokú csalódottságát eredményezett. Egy televíziós műsorban nyugdíjba vonulása előtt, 2018 nyarán az AIVD igazgatója, Rob Bertholee kijelentette[265], hogy *„különös óvatossággal kell eljárni a műveleti információk megosztásakor az Egyesült Államokkal, most, amikor Donald Trump elnök”*. Úgy fest, hogy érdemes ezt észben tartania a szakmai és politikai közösségeknek. Gróf Széchenyi István szavaival élve *„Józan ész soha sem áldoz fel pillanati vagy igen kis időre terjedő haszonért, habár ma nyulhat is hozzá, jövendő nagyobb `s tartósb hasznot; de inkább az ideigóráiglani rövid nyomást a várható hosszabb kellem miatt békével türi”*. [266]

[263]CrowdStrike: Who Is COZY BEAR? *CrowdStrike Blog*, 2016. szeptember 19.
[264]FAOU, Matthieu – TARTARE, Mathieu – DUPUY, Thomas: Operation Ghost: The Dukes aren't back – they never left. ESET WeLiveSecurity, 2019. október 17. Elérhető: https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf (Letöltés ideje: 2020. április 26.)
[265] A kijelentés hátterével összefüggésben lásd: GOLDMAN, Adam – SCHMITT, Eric – GIBBONS-NEFF, Thomas: C.I.A. Informant Extracted From Russia Had Sent Reports to Agency for Decades. *The New York Times*, 2019. szeptember 9. Elérhető: https://www.nytimes.com/2019/09/09/us/politics/cia-informant-russia.html és SCIUTTO, Jim et al.: Exclusive: US extracted top spy from inside Russia in 2017. *CNN Politics*, 2019. szeptember 9. Elérhető: https://edition.cnn.com/2019/09/09/politics/russia-us-spy-extracted/index.html (Letöltés ideje: 2020. 04. 26.)
[266] Széchenyi István (1827): Hitel. 6. fejezet, 26–27. o. (eredeti kiadás: Pozsony).

5. Az NBS VII. fejezet c), d) és o) pontjaiban rögzített kiemelt biztonsági kockázatok kölcsönhatásáról, és a jogi hadviseléssel való kapcsolatukról

A hibrid és kibertér műveletek közötti kapcsolat összefüggései jól láthatók. Hogyan kapcsolódik előbbi kettőhöz „a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenése és gyors terjedése?" Lehetséges-e előzőek káros hatásainak szándékos, gondatlan vagy vétlen növelése a járvány miatt elrendelt veszélyhelyzet idején? Elegendő a kormányzati tájékoztatást követnünk ahhoz, hogy felismerjük, a kibertérben elindított dezinformáció, mint az országos nyilvánosságot kapott „Budapestet hamarosan le fogják zárni" tartalmú hamis híresztelés miféle politikai, gazdasági, társadalmi károkat képes okozni. A Készenléti Rendőrség Nemzeti Nyomozóiroda és a Nemzetbiztonsági Szakszolgálat gyors, határozott intézkedéseinek köszönhetően a Budapest lezárásáról szóló, de más álhírek terjesztőit is azonosították és velük szemben büntetőeljárás indult. A bármely okból kialakult sebezhetőség kiváló lehetőség az online csalások elkövetői számára is, akik szintén a kibertérben követik el a bűncselekményeket. A sebezhetőség a járvány miatti bizonytalanság eredményeként alakul ki.

Ennek legjobb ellenszere a magyar kormány által is alkalmazott széles körű tájékoztatás. Interneten, televízióban, nyomtatott és elektronikus sajtóban közöl folyamatosan adatokat a kormányzat, megerősíti a társadalomban, hogy a helyén van az államapparátus, pánikra nincs ok. A dezinformáció terjesztése, a bizalom aláásásának kiváló eszköze ellen csak így lehet felvenni a harcot. Az államapparátus vagy a helyi szintű vezetők munkájába vetett bizalmat, de akár a kormányzati vagy nem kormányzati munkahelyek légkörét is teljesen tönkre tudják tenni azok a megnyilvánulások, melyeket jobb esetben csak sajtóhírekből ismertünk meg az elmúlt években. A publikáció készítésekor hatályos NBS-ben[267] szereplő, a fejezet fókuszába helyezett kihívások elleni küzdelem során kulcsszerepe van a proaktív jogalkotásnak és a megfelelő alkotmányos kontroll melletti, transzparens jogalkalmazásnak. [268]

[267] 1163/2020. (IV. 21.) Korm. határozat - Magyarország Nemzeti Biztonsági Stratégiájáról

[268] Az NBS kifejezetten előírja, hogy a biztonság egyes részterületeiért felelős állami szervezeteknek a Stratégiában megfogalmazott iránymutatásokkal összhangban kell megalkotniuk és felülvizsgálniuk a tevékenységükre vonatkozó szakági szabályzókat, különös tekintettel a nemzeti katonai, a rendészeti, a nemzetbiztonsági, a terrorelhárítási, a katasztrófavédelmi, a kiberbiztonsági és a migrációs területekre. Mindezt úgy kell elvégezni, hogy a hatályos NBS rendelkezéseit is a korábban említett, folyamatos felülvizsgálati kötelezettség terheli, így amennyiben valamely érintett szerv hatáskörében erre okot adó körülményt derít fel, jeleznie szükséges azt az irányító tárc(áj)a felé, hogy a szükséges normaalkotás kezdeményezhetővé váljon.

Az álhírek terjesztésének egyik legveszélyesebb területe a jogalkotás tevékenységének támadása hazai és nemzetközi színtéren. A lawfare, amely elsősorban a jogi eszközök alkalmazását jelenti a hibrid hadviselés során, megítélésem szerint értelmezhető úgy, hogy ide sorolandó a jogalkotás legfelsőbb szintje által alkotott jogforrások folyamatos, egyes esetekben akár alaptalan támadása is, mivel a célja a jogalkotó hiteltelenítése, a belé vetett közbizalom megingatása.

A jog uralmának helyességébe vetett társadalmi bizalom gyengítése alkalmas az állam destabilizálására, mozgásterének csökkentésére. Az alábbiakban és az 1. számú mellékletben részletezett esetek válogatott példák a kormányok, illetve nemzetközi szervezetek elleni hitelességet aláásó kampányokra.

6. Az igazság nyomában, avagy a dezinformáció felismerése szakmai és tudományos eszközökkel

A fentiekben hivatkozott és 1. számú mellékletben részletezett közleményekkel, illetve dezinformációkkal összefüggésben rendkívül fontosnak tartom megjegyezni, hogy egyéni érzelmi alapon vagy szövetségesi hűség alapján nem szabad „előre” eldöntenünk, hogy mennyire igazak az állítások, hiszen akkor már vesztettünk is. Minden esetben a leginkább objektív eszközöket és módszereket alkalmazó kutatást kell elvégeznünk annak érdekében, hogy valószínűsítsük az adott közlésről, hogy az vélhetően dezinformáció, illetve hogy tartalmaz-e igaz, hamis vagy hamisított elemeket.

Nem kívántam (az egyébként minden esetben – stratégiai kommunikáció vagy oknyomozó újságírók által – megjelentetett) egzakt cáfolatokat megjeleníteni, hanem a dezinformáció felismerésének jelentőségére igyekszem rávilágítani, azzal a céllal, hogy azt tudatot erősítsem az olvasóban, hogy a tényellenőrzést különösen a számára is kiemelkedő jelentőségű hírek vonatkozásában a rendelkezésére álló eszközökkel, módszerekkel, alkalmazásokkal – lehetőség szerint – saját maga végezze el. Természetesen kiemelkedő jelentősége van annak a ténynek, hogy ezzel összefüggésben a kormányzati tájékoztatásért felelős valamennyi szervezetnek és a jog-, és hatásköreiket megállapító jogalkotónak is van kötelezettsége.

Andres Oppenheimer 2024. január 5-én megjelent véleménycikkében figyelmeztet a mesterséges intelligencia által generált hamis híroldalak 2024-ben várható robbanásszerű elterjedésére. [269] Fontos kiemelni, hogy ez a technológia kritikus jelentőségű a demokrácia és a világbéke szempontjából, mivel a világ számos országban befolyásolhatja választásokat, valamint lényegében minden más releváns döntéshozatalt. Az egyik legnagyobb fenyegetés az lehet, hogy a mesterséges intelligencia példátlan mértékű hamis hírek, videók, képek áradatát készítheti majd el. A publikáció szerint már most is tapasztalható, hogy olyan generatív mesterséges intelligencia platformok, mint a ChatGPT, a Bard, és „kétes médiamogulok", mint az X (korábban Twitter) tulajdonosa, Elon Musk, egyre könnyebbé teszik szinte bárki számára a hamis hírek terjesztését.

A NewsGuard, egy hamis híroldalakat nyomon követő cég szerint a mesterséges intelligencia hamis hírek legveszélyesebb terjesztője lesz. A cég 603 olyan mesterséges intelligenciával működő híroldalt talált, amelyeket alig vagy egyáltalán nem felügyelnek emberek, szemben az előző év májusi 49 oldallal. Ezek az oldalak gyakran olyan neveket viselnek, mint az iBusiness Day vagy a Daily Time Update, amelyek megtévesztően hasonlítanak az ismert hírszolgáltatók elnevezésére és különösen alkalmasak a hírfogyasztók megtévesztésére. A NewsGuard globális csapata által Internet legteljesebb, gépi olvashatóságra optimalizált katalógusát[270] tartalmazza a legelterjedtebb hamis állításoknak, melyek a kibertérben keringenek.[271] Ez a katalógus kifejezetten a tévinformációk nagy léptékű észlelésére lett kialakítva. Ezt az adathalmazt többféle módon lehet használni:

- Konkrét egyedi azonosítók tárházaként, amelyek mesterséges intelligencia használatára és gépi tanulásra optimalizált eszközök számára kiindulópontként szolgálnak az Interneten és a közösségi médiában terjedő téves és félrevezető információkat tartalmazó tartalmak keresésére.
- Értékelő-elemző szakemberek számára, hogy megismerjék a téves és félrevezető információk kockázatait, és nyomon kövessék az új narratívákat, mielőtt azok a fősodratú médiába kerülnének.

[269]OPPENHEIMER, Andrés: Watch out for an explosion of A.I.-generated fake news sites in 2024. *Miami Herald* / Yahoo News, 2024. január 5.
[270] NewsGuard: False Claim Fingerprints [korábban: Misinformation Fingerprints]. [online termékoldal] Elérhető: https://www.newsguardtech.com/solutions/misinformation-fingerprints/ (letöltve: 2024. 01. 08.)
[271] A "Misinformation Fingerprints" (Tévinformációk Ujjnyomatai) elnevezéssel

- Kormányzati ügynökségek és nemzetbiztonsági szolgálatok számára, hogy valós időben értékeljék a dezinformációs műveleteket.
- Vállalati kommunikációs szakemberek számára, hogy naprakészek legyenek a márkajelzésekkel kapcsolatos hamis információk fejlődő tájékoztatási területén, amelyek károsíthatják az ügyfelek hírnevét.
- Kiolvashatók az adatbázisból a linkek, amelyek tartalmazzák a hamis állítást, a hamis állítás terjesztésére használt példanyelv, a hamis állítás NewsGuard által megismert variációi, a részletes cáfolatok a megbízható források hivatkozásával, valamint a kapcsolódó kulcsszavak és hashtag-ek.

A NewsGuard előbb említett szolgáltatása több szempontból különbözik a hagyományos tényellenőrzéstől, ugyanis:

- Az „Ujjnyomatok" gépi olvasható formátumokban érhetők el, ami lehetővé teszi, hogy nagy nyelvi modellek által feldolgozhatóak legyenek.
- Minden „Ujjnyomatot" egy „károsodási kockázat" szinttel látnak el, a terjedési sebesség és a várható káros hatás prognózisa alapján.
- Információkat közölnek arról, hogy honnan és mikor terjedt el egy dezinformáció, segítenek felderíteni azt is, hogy mennyire sikeres a megtévesztő művelet, vagyis, hogy miként teljesít a dezinformáció.
- Az előbb említett adatbázis különböző szektorokban terjedő hamis hírek katalógusát tartalmazza, ami lehetővé teszi a felhasználók számára, hogy szűrést végezzenek olyan állítások vonatkozásában, amelyek egy meghatározott földrajzi területre, vállalatra, globálisan érdekes politikai kérdésre, egy adott iparágra vagy kijelölt időszakra vonatkoznak.
- Minden „Ujjnyomattal" összefüggő információt képzett újságírók vizsgálnak meg, akik alapos kutatást végeznek annak érdekében, hogy a megalapozottan téves vagy durván félrevezető állításokat felderítsék és ezek bekerülhessenek az adatbázisba későbbi priorálás céljából.

A NewsGuard honlapján[272] kiemeli, hogy adatbázisát elemző szakemberek és mesterséges intelligencia eszközök (programok) egyaránt tudják használni, és folyamatosan frissített képet nyújtanak számunkra a digitális információs környezet(ünk)ről, valamint egy hatékony módot kínálnak a kibertérben terjedő és felbukkanó hírek, közlemények követésére.

Ezek közül néhány oldalt Oroszország, Kína és Irán hozott létre, vagy politikusok, akik ellenfeleiket akarják lejáratni, mások pedig pénzszerzési céllal jöttek létre: minél botrányosabb hamis híreket közölnek, annál több kattintást kapnak, és annál több pénzt keresnek a hirdetőktől vagy a közösségi médiából.

A NewsGuard azt találta, hogy az X-en (korábbi Twitter) az Izrael-Hamász háborúról szóló hamis hírek 74%-át „megerősített" kék pipás fiókok tették közzé, amelyeket most már bárki megszerezhet havonta 8 dollárért. Korábban a Twitter csak megbízható hírforrásoknak adott kék pipát, a hitelességet nem pénzért kínálták.

A hamis hírek közvéleményre gyakorolt hatásának egyik legújabb példája egy január 3-án közzétett Washington Post közvélemény-kutatás, amely szerint az amerikaiak 25%-a hiszi, hogy az FBI provokálta a 2021. január 6-i Capitolium elleni támadást, annak ellenére, hogy erre semmilyen bizonyíték nincs.

A NewsGuard ajánlása szerint a mesterséges intelligenciával generált hamis hírek felismerésének egyik módja az, hogy ellenőrizzük, van-e a cikkeknek szerzői aláírása, és hogy létezik-e az illető személy. Ezt úgy tehetjük meg, hogy a Google-ben vagy a közösségi médiában ellenőrizzük a nevet. Edward Wasserman, a Kaliforniai Egyetem, Berkeley etikai újságírásra szakosodott professzora és a Miami Herald korábbi üzleti szerkesztője azt javasolja az olvasóknak, hogy végezzenek saját háttérellenőrzést az ismeretlen híroldalakon. „Nézze meg, hogy mások is közlik-e azt, amit olvasott?" - mondta Wasserman. „Ez azt jelenti, hogy hitelesnek tartott hírforrásokhoz fordul. Közlik-e ők is ezt a történetet?"[273]

[272] NewsGuard: How NewsGuard's Misinformation Fingerprints Provide Early Warning Alerts for Emerging Online Threats.
[273] NewsGuard: How NewsGuard's Misinformation Fingerprints Provide Early Warning Alerts for Emerging Online Threats.

Oppenheimer egy közérthető hasonlattal a fejezi ki reményét, miszerint *„2024-ben több ember megtanul megbízható hírforrásokra támaszkodni úgy, mint a szupermarketek, amelyek ellenőrzik az áruk megfelelő minőségét”*.[274] Ellenkező esetben, ahogy Oppenheimer fogalmaz, *„a mesterséges intelligenciával generált hamis hírek lavinájával sokkal veszélyesebb hellyé válhat a világ”.* [275]

Az álhírek társadalmi zavarkeltésének infrastrukturális aspektusait vizsgálva kijelenthető, hogy az álhírek terjedése fontos kérdéseket vet fel a webes és közösségi médián keresztüli információáramlás, befolyásolás és a részben adataink kereskedelemére épülő pénztermelő online felületek rutinszerű működésével kapcsolatban. [276]

Három metodológiai taktikát érdemes előbbiekkel összefüggésben alkalmazni az álhírek terjesztésének infrastrukturális feltételeinek feltárására: (1) a tartalom rangsorolásának és a linkgazdaság vizsgálatát, (2) az elkötelezettség kvantitatív mérését és a like-ok számát, valamint (3) az online tartalom és a hirdetések hatékonyságának azt a mérőszámát, amely arra vonatkozik, hogy az üzenetek mennyire képesek lekötni a felhasználók figyelmét és a vállalati nyomkövetők (tracker-ek) megjelenési számát (jelenlétét). Ezek a vizsgálati módszerek nemcsak az álhírek tartalmára összpontosítanak, hanem azok terjesztési feltételeire is, lehetővé téve a beavatkozást és a kísérleteket, amelyek megkérdőjelezik és megváltoztathatják ezeknek a közvetítői struktúráknak a szerepét a társadalmi, kulturális, gazdasági és politikai élet különböző aspektusai közötti kapcsolatok újraformálásában[277].

---

[274] OPPENHEIMER, Andrés: Watch out for an explosion of A.I.-generated fake news sites in 2024. *Miami Herald* / Yahoo News, 2024. január 5.

[275] OPPENHEIMER, Andrés: Watch out for an explosion of A.I.-generated fake news sites in 2024. *Miami Herald* / Yahoo News, 2024. január 5.

[276] GRAY, Jonathan – BOUNEGRU, Liliana – VENTURINI, Tommaso: 'Fake news' as infrastructural uncanny. *New Media & Society*, Vol. 22, No. 2, 2020, 317–341. o. DOI: https://doi.org/10.1177/1461444819856912

[277] BOUNEGRU, Liliana – GRAY, Jonathan – VENTURINI, Tommaso – MAURI, Michele (szerk.): *A Field Guide to „Fake News" and Other Information Disorders*. Amsterdam: Public Data Lab, 2018. DOI: https://doi.org/10.5281/zenodo.1136271. Elérhető: http://fakenews.publicdatalab.org/ (letöltve: 2024. 01. 05.) A mű két esettanulmányt is bemutat: az 1943-ban és 2017-ben előállított hamis Le Soir újságokat. Mindkét esetben a Le Soir újság pontos másolatait hozták létre, amelyek a vizuális és szerkesztési konvenciók alapos reprodukciójával váltak „hitelessé”. A szerzők hangsúlyozzák, hogy nemcsak a tartalom hasonlóságára szeretnék felhívni a figyelmet, hanem az előállításukban, terjesztésükben és monetizálásukban részt vevő különböző infrastruktúrákra is. A cikk arra a következtetésre jut, hogy az infrastruktúrák nemcsak dolgokként, hanem kapcsolatok rendszerének összességeként is vizsgálandók. A „fake news” jelenség alatt nem csak azt kell a vizsgálatunk középpontjába állítanunk, hogy mit mondanak, hanem magának a közlésnek, információtovábbításnak a feltételeit is: a digitális infrastruktúrákat, amelyek közvetítik az online tartalmak terjesztését. A cikk arra ösztönzi az olvasókat, hogy ne csak javítsák a platformokat és erősítsék az szakértő-központú tudás kultúrákat, hanem használják az álhíreket nyilvános kísérletekre is, amelyek megkérdőjelezik és megváltoztatják az infrastruktúrák gazdasági, kulturális és politikai életben betöltött szerepét. A szerzők azt

Fontos fegyver lehet a fejezetben összegyűjtött dezinformációs híresztelésekkel szembeni küzdelem során az erre alkalmas, vizualizációt is megvalósítani képes hálózatelemző alkalmazások, például a Gephi[278] használatának képessége az elemzői oldalon[279].

A FirstDraftNews.org-on Jonathan Gray, Mathieu Jacomy, Liliana Bounegru and Rory Smith cikke[280] a dezinformáció internetes terjedésének nyomon követésére használt adatvizualizációs eszközöket vizsgálja. A szerzők a dezinformáció definícióját úgy fogalmazzák meg, hogy a dezinformáció hamis vagy félrevezető információ, amelyet tényként tüntetnek fel. Számos csatornán keresztül terjedhet, beleértve a közösségi médiát, a hagyományos médiát és a szájhagyományt. A dezinformációnak számos negatív következménye lehet, többek között aláássa a bizalmat az intézményekben, erodálja a társadalmi kohéziót és súlyosbítja a politikai megosztottságot.

Érdemes kiemelni, hogy az adatvizualizációs eszközök hogyan használhatók a dezinformáció terjedésének nyomon követésére. Az adatvizualizációs eszközök lehetővé teszik

javasolják, hogy az álhírekre ne csak valami kizárólagosan negatív dologként tekintsünk, hanem gondoljunk arra is, hogy ez a jelenség lehetőséget kínál arra is, hogy megvizsgáljuk és újraértékeljük az életünket és mindent, amit a világról tudunk vagy tudni vélünk. A kritikus gondolkodás fejlődését pedig egészen pozitív jelzővel érdemes jellemeznünk.

[278] GRAY, Jonathan – JACOMY, Mathieu – BOUNEGRU, Liliana – SMITH, Rory: How are they funded? Investigating ad trackers with Gephi and the DMI Tracker Tracker tool. *First Draft*, 2021. március 10. Elérhető: https://firstdraftnews.org/long-form-article/trackers-gephi-dmi/ (letöltve: 2024. 01. 05.)

[279] A Gephi egy nyílt forráskódú hálózatelemzési és vizualizációs szoftver, amelyet különösen a nagy hálózatok vizsgálatára és ábrázolására terveztek. A dezinformáció elleni küzdelemben a Gephi többféleképpen használható: a) Hálózati szerkezet feltárása: A dezinformációt terjesztő hálózatok gyakran összetett kapcsolati mintázatokat mutatnak. A Gephi segíthet azonosítani a hálózat központi szereplőit, azaz azokat a csomópontokat, amelyek a legtöbb kapcsolattal rendelkeznek, vagy amelyek kulcsszerepet játszanak az információ terjedésében. b) Közösségek detektálása: A Gephi algoritmusokat kínál közösségek felismerésére a hálózatokban. A dezinformációs kampányok gyakran használnak összehangolt csoportokat vagy „botokból" álló hálózatokat az információ terjesztésére. A közösségdetektálás segíthet azonosítani ezeket a csoportokat. c)Információáramlás elemzése: A Gephi segítségével vizualizálható, hogyan terjed a dezinformáció a hálózaton belül. Az élek vastagságának és irányának megváltoztatásával láthatóvá tehetők az információ terjedésének fő útvonalai. d)Idősoros vizsgálat: Az időbeli változások vizsgálatával nyomon követhető, hogyan változik egy dezinformációs kampány hálózata az idő múlásával. Ez segíthet megérteni a kampány dinamikáját és hatékonyabban felkészülni a jövőbeli támadásokra. e) Kapcsolati minták azonosítása: A Gephi segíthet felfedezni a dezinformációt terjesztő hálózatokban rejlő mintázatokat, például bizonyos típusú tartalmak vagy csomópontok közötti gyakori kapcsolatokat. e) Források meghatározása: A dezinformációs kampányok eredetének és terjesztőinek azonosítása kulcsfontosságú lehet. A Gephi segíthet az eredeti források és a legaktívabb terjesztők megtalálásában. Az előbbi elemzési lehetőségek lehetővé teszik a kutatók, elemzők és politikai döntéshozók és újságírók számára, hogy jobban megértsék és kezeljék a dezinformáció terjedését, és hatékonyabb stratégiákat dolgozzanak ki annak megelőzésére és ellensúlyozására.

[280] GRAY, Jonathan – JACOMY, Mathieu – BOUNEGRU, Liliana – SMITH, Rory: How are they funded? Investigating ad trackers with Gephi and the DMI Tracker Tracker tool. *First Draft*, 2021. március 10. Elérhető: https://firstdraftnews.org/long-form-article/trackers-gephi-dmi/ (letöltve: 2024. 01. 05.)

a felhasználók számára, hogy vizuális ábrázolásokat hozzanak létre az adatokból. Ezeket a vizuális ábrázolásokat a dezinformáció terjedésének azonosítására lehet felhasználni. Például az adatvizualizációs eszközökkel nyomon követhető egy dezinformáció közösségi médiában való megosztásainak száma, vagy azonosíthatók azok a weboldalak, amelyek a legnagyobb valószínűséggel terjesztenek dezinformációt. Az adatvizualizációt felhasználták a 2016-ban lezajlott amerikai elnökválasztással kapcsolatos dezinformációk terjedésének nyomon követésére is. A választásokat megelőzően jelentős mennyiségű dezinformáció keringett online mindkét jelöltről. Adatvizualizációs eszközöket használtak ennek a dezinformációnak a terjedésének nyomon követésére. Ennek a nyomon követésnek az eredményei azt mutatták, hogy a dezinformáció döntő többségét néhány weboldal és személy terjesztette. Ezt az információt használták fel a dezinformáció terjedésének visszaszorítására a választások alatt.

Az oltásellenes aktivizmus és a vakcinákkal kapcsolatos téves információk terjedése online környezetben növeli az oltásszkeptikus hozzáállást. A tech vállalatok lépéseket tettek az oltásellenes tartalmak terjedésének csökkentésére, de az oltásellenes weboldalak működési és pénzügyi háttere ugyanakkor kevésbé ismert, azonban a károkozásuk különösen jelentős szintet ér(t) el. Emiatt érdemes az oltásellenes, illetve más dezinformációsnak tartott weboldalak hirdetési struktúráit és pénzügyi modelljeit vizsgálni. Az erre vonatkozó megoldási javaslatot a Public Data Lab, a Digital Methods Initiative, az Open Intelligence Lab és a First Draft közösen dolgozta ki, célja pedig a közösségi média elemzésének fejlettebb technikáinak bemutatása.

A megoldás a Gephi nyílt forráskódú hálózatelemző eszközt és a DMI Tracker eszközt használja a weboldalakhoz kapcsolódó nyomkövető eszközök vizsgálatára. Ezek az eszközök nem csak hirdetésekkel kapcsolatos nyomkövetőket, hanem más típusokat is tartalmaznak. A módszerrel a kutatók és újságírók feltárhatják, hogyan próbálnak az oltásellenes weboldalak elérni célközönségüket, hogyan keresnek pénzt, és milyen szerepet játszanak ebben a nagy tech cégek. A vizsgálat lépései:

- Anti-vax weboldalak listájának összeállítása, [281]

[281] Az oltásellenes (anti-vax) weboldalak olyan internetes oldalak, amelyek az oltások hatásosságát és biztonságosságát kérdőjelezik meg, illetve egyenesen az oltások veszélyeiről, káros hatásairól terjesztenek téves információkat. Néhány példa az ismert oltásellenes weboldalakra: - Azonnali Reakció Egyesület - kifejezetten oltásellenes szervezet weboldala, Oltási reakciók - oltásokról szóló rémhírek és dezinformációk oldala, Független Oltási Tanácsadó Csoport - áltudományos nézeteket terjesztő weboldal, Oltatlanok Klubja - hasonló nézeteket valló közösség felülete. Ezek az oldalak sok esetben félrevezető információkkal, hamis statisztikákkal és

- A listát a DMI Tracker Tracker eszközbe illesztve a hozzájuk kapcsolódó nyomkövetők adatainak begyűjtése,
- A nyomkövető típusok és neveik vizualizációja a RAWGraphs eszközzel,
- Az eredmények GEFX fájlként történő importálása a Gephi szoftverbe a vizuális hálózatelemzéshez,
- A nyomkövető termékekkel kapcsolatos további kutatások és elemzések.

Az elemzés során megfigyelhető a nagy tech cégek (különösen Google, Facebook, Twitter) és termékeik fertőzöttségének magas szintje az oltásellenes weboldalak megjelenésének helyszíneként. A vizualizáció segítségével azonosíthatók a különböző konfigurációk, amelyek betekintést nyújtanak ezeknek a weboldalaknak a működésébe, pénzkereseti stratégiájukba és az algoritmusokra épülő hirdetések használatába.

Szorosan kapcsolódik előbbi módszerhez Anatoliy Gruzd és Philip Mai munkája[282], amely azt vizsgálja, hogyan kezdett el terjedni egy összeesküvés-elmélet a Twitteren, amely szerint a COVID-19 pandémia egy kitaláció és a betegség nem is létezik abban a formában, ahogyan a hatóságok állítják. A tanulmány az úgynevezett #FilmYourHospital hashtag terjedését elemzi, amely arra ösztönözte az embereket, hogy látogassanak el helyi kórházakhoz, készítsenek képeket és videókat az üres várótermekről és parkolókról, ezzel „bizonyítva", hogy a pandémia nem valós. [283]

Az elemzés során a szerzők a Szociális Hálózatelemzés[284] technikáit használták, hogy megvizsgálják, milyen módon terjedt el az elmélet a Twitteren, és hogy a hashtag terjedését

személyes történetek manipulatív felhasználásával igyekeznek elbizonytalanítani az embereket az oltások hasznosságát illetően. Veszélyes dezinformációkat terjesztenek, ezért nem ajánlott hiteles forrásként kezelni ezeket.

[282] GRUZD, Anatoliy – MAI, Philip: Going viral: How a single tweet spawned a COVID-19 conspiracy theory on Twitter. *Big Data & Society*, Vol. 7, No. 2, 2020. DOI: https://doi.org/10.1177/2053951720938405 (letöltve: 2024. 01. 05.)

[283] Maga a tanulmány része egy „Viral Data" (Vírusadatok) nevű kiemelt publikációs adatbázisnak. Ez elérhető: https://journals.sagepub.com/page/bds/collections/viraldata (letöltés:2024.01.05.)

[284] A szociális hálózatelemzés (Social Network Analysis, SNA) egy kutatási módszertan, amelyet a társadalmi struktúrák vizsgálatára használnak. A technika a társas kapcsolatok hálózatának elemzésére összpontosít, és segítségével feltárhatjuk, hogy az egyének, csoportok, szervezetek vagy akár teljes társadalmak hogyan kapcsolódnak egymáshoz. A szociális hálózatelemzés alapelemei a pontok és az élek: a) A pontok (csomópontok vagy node-ok) az egyéneket (embereket, szervezeteket stb.) jelképezik a hálózatban. b) Az élek (kapcsolatok vagy link-ek) a pontok közötti kapcsolatokat jelképezik, például barátságot, kommunikációt, munkakapcsolatot stb. Az SNA módszerei segítségével többféle jelenséget vizsgálhatunk, többek között: a) A hálózati kapcsolatok mintázatait és struktúráját. b) A hálózati pozíciókat és szerepeket, úgymint ki van központi helyzetben, ki a

automatizált szoftverek vagy a felhasználók koordinált tevékenysége segítette-e elő. Megállapították, hogy bár a tartalom nagy része korlátozott elérésű felhasználóktól származott, a kezdeti lökést néhány befolyásos konzervatív politikus és jobboldali aktivista adta meg, akik felhasználták ezt a hashtag-et, hogy felhívják a figyelmet a kampányra és arra ösztönözzék követőiket, hogy szegjék meg a karantént és filmezzék le helyi kórházaikat. Az első lendületet követően a kampányt főként Trump-párti fiókok tartották életben, majd egy másodlagos terjedési hullám következett az USA-n kívül.

7. Befolyásolás történt „a nagyobb jó érdekében" a GDPR megalkotása során?

Az Európai Unió állampolgáraiként (jogalanyaiként) kiemelkedő jelentőséggel bír mindannyiunk számára az a tény, hogy az EU 2018. május 25-én hatályba léptette az Általános Adatvédelmi Rendeletet (GDPR), amelynek közismert célja az egyének magánéletének és személyes adatainak a védelme. Ez a szabályozás rendkívül széles körű hatállyal bír, mivel minden olyan szervezetre vonatkozik, amely az EU lakosainak adataival foglalkozik. Anatoliy Gruzd, Deena Abul-Fottouh és Atefeh (Atty) Mashatan publikációja[285] a Twitteren folyó GDPR-ról szóló megbeszélések vizsgálata, a közvélemény és a szervezetek public relations (a továbbiakban: PR) stratégiáinak elemzését tartalmazza a GDPR kapcsán. Az eredmények szerint számos érintett aktívan és érdemben vitatta meg a rendelet tervezetét, különösen a kiberbiztonsági és IT-szakértők, valamint tanácsadó cégek munkatársai, ahogyan ezt korábbi években már valószínűsítették az előzetes kutatások.

Ugyanakkor néhány olyan érintett, akiktől aktívabb szerepvállalást vártak volna, kevésbé vettek részt az össztársadalmi véleménynyilvánításban, többek között az adatokat tároló vagy feldolgozó vállalatok, kormányzati és szabályozó testületek, a fő áramú média és a tudományos élet képviselői. Az eredmények azt is mutatják, hogy az érintettek többnyire egyirányú kommunikációt folytatnak a közönségükkel, így inkább a PR retorikai, mintsem kapcsolati

---

periférián stb. c) A hálózatokon belüli információáramlást és erőforrás-eloszlást. d) Az egyének vagy csoportok közötti befolyást és hatalmat. A szociális hálózatelemzés hasznos lehet számos területen, beleértve a szociológiát, antropológiát, pszichológiát, üzleti adminisztrációt és még a politikai tudományokat is. Eszközei közé tartoznak a kérdőívek, interjúk és digitális adatgyűjtés, valamint komplex statisztikai és grafikus elemzési módszerek. Az SNA eredményeit vizuálisan is ábrázolhatjuk hálózati diagramok formájában, amelyek segítenek abban, hogy átláthatóbbá tegyük a kapcsolati mintázatokat és dinamikákat.

[285] GRUZD, Anatoliy – ABUL-FOTTOUH, Deena – MASHATAN, Atefeh: Who is Influencing the #GDPR Discussion on Twitter: Implications for Public Relations. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS-53)*. Maui, HI, 2020. január 7., 1–10. o. DOI: https://doi.org/10.24251/HICSS.2020.319.

funkcióját töltik be. Az információáramlás ezen formája arra engedi következtetni az olvasót, hogy „meg lettek mondva a helyes válaszok”, de a célközönség véleményére kevésbé volt kíváncsi bárki is.

A tanulmány[286] hozzájárul a PR szakterület vizsgálatához, olyan módon, hogy elemezi a Twitteren megosztott közleményeket és az információáramlást a GDPR-ral összefüggésben, és azonosítja a közösségi média befolyásolóit ebben a témában, valamint azokat a közösségi véleményformáló funkciókat, amelyeket ezek a résztvevők betöltenek. Ezek lehetnek szakértők, hírességek, illetve celebritások, influenszerek, előbbiek követői, fiatalkorú tartalomfogyasztók, és mások, akik képesek a közösségi médiában vírus-szerűen terjeszteni GDPR-ral összefüggésben közölteket. A közösségi média befolyásolói így meghatározó jelentőségűeknek tekinthetők a szervezeti PR szempontjából is.[287]

A tanulmány megvizsgálja a Twitteren lévő közösségi média befolyásolóit az EU GDPR rendeletének végrehajtása kontextusában. A befolyásolók azonosítása érdekében először meg kell határozni azokat az felhasználókat (vagyis inkább profilokat), akik aktívan jelen vannak a Twitteren.

Álláspontom szerint az adatelemzés és annak vizualizálása (esetünkben konkrétan a hálózatelemzés), melyet a publikáció készítői a GDPR vonatkozásában elvégeztek, világosan mutatja, hogy egy jogi norma tervezet vitája miként befolyásolható a kibertérben. Kik lehetnek azok, akik végül, ha el nem is dönthetik a sorsát, de módosíthatják egy egész EU-ra jelentős hatást gyakorló előírás egyes rendelkezéseit és előbbiek alapján megállapíthatjuk, hogy ez óriási hatalmat jelent, továbbá az eredmények és a következtetések némiképp árnyalhatják a közvetlen demokratikus döntéshozatal, illetve véleménynyilvánítás primátusába vetett hitünket, illetve elképzeléseinket.

[286] GRUZD, Anatoliy – ABUL-FOTTOUH, Deena – MASHATAN, Atefeh: Who is Influencing the #GDPR Discussion on Twitter: Implications for Public Relations. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS-53)*. Maui, HI, 2020. január 7., 1–10. o. DOI: https://doi.org/10.24251/HICSS.2020.319.
[287] ALLAGUI, Ilhem – BRESLOW, Harris: Social media for public relations: Lessons from four effective cases. *Public Relations Review*, Vol. 42, No. 1, 2016, 20–30. o. DOI: https://doi.org/10.1016/j.pubrev.2015.12.001

8. Összegzés, az elvégzett vizsgálat és részkövetkeztetések

A fejezetben (és a más nézőpontból a VI. fejezetben) megvizsgáltakkal támasztom alá az 1. számú hipotézisben megjelenítetteket, különösen a funkcionalitást alapul vevő megközelítés fontosságát a nemzetbiztonsági tevékenység stratégiai szintjén.

A pandémia idején a jogalkotás kulcsszerepet játszik a válságkezelésben[288] és a jogbiztonság fenntartásában. A jogalkotóknak gyorsan kell reagálniuk a változó helyzetekre, egyensúlyozva az egészségvédelmi intézkedéseket és az egyéni jogokat. Ugyanakkor a hosszú távú következmények és a nemzetközi együttműködés szempontjából is meg kell vizsgálni a jogalkotás szerepét. A pandémia jelentősen próbára tette a jogrendszerek alkalmazkodó-, és innovatív képességét a változó biztonsági környezetben.

A kibertérből érkező álhírek a járvány elleni védekezést alapvetően nehezítik meg és ezzel számos emberéletet és jelentős anyagi javakat sodornak veszélybe. A közösségi oldalak igyekeznek ezeket kiszűrni, sajnos azonban hazánkban (is) több olyan esettel (álhírrel) találkozhattunk, amely a legnépszerűbb videó megosztó honlapról, vagy valamelyik közösségi oldalról indult útnak és okozott jelentős hátrányt.

A #FilmYourHospital összeesküvés-elméletének terjedése egyetlen tweetből rávilágít arra a folyamatos kihívásra, amellyel a hamis, vírusként terjedő információkkal kell(ett) szembenéznie a hatóságoknak, kormányoknak a COVID-19 pandémia idején. A félrevezető információk terjedését ugyan mérsékelheti a tényellenőrzés és az emberek hiteles egészségügyi források felé irányítása, de a politikai motivációk által vezérelt és tudományos alapok nélküli téves és megtévesztő állítások gyökereit rettentő nehéz kiirtani.

Nem szabad megfeledkezni a jogintézmények alapjogkorlátozó voltáról, miközben vizsgáljuk a jogi normaalkotási opciókat még a szélsőségnek tekinthető különleges jogrend alkalmazásának idején sem.[289] A szükségesség és arányosság követelményeinek ekkor is meg

[288] KÁDÁR Pál – HOFFMAN István: A különleges jogrend és a válságkezelés közigazgatási jogi kihívásai: a „kvázi különleges jogrendek" helye és szerepe a magyar közigazgatásban. *Közjogi Szemle*, 14. évf. 3. sz., 2021, 1–11. o.

[289] Ezen megközelítéssel összefüggésben lásd: HOFFMAN István – KÁDÁR Pál: A különleges jogrend és a válságkezelés közigazgatási jogi kihívásai I. *Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok*, 2021/2. sz. Budapest: Nemzeti Közszolgálati Egyetem Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely, 1–39. o.

kell felelnie a döntéseknek, intézkedéseknek.

A kibertérben jelenlévő, pontosabban onnan érkező, azt felhasználó dezinformációs művelet a járvány idején (de minden más, különleges jogrend kihirdetését megalapozó helyzetben) jelentősebb eredménnyel jár (hátránnyal fenyeget). Emiatt komolyabb dologi és személyi erőforrásokat igénylő feladatokat képez a nemzetbiztonsági elhárításért és rendvédelemért felelős szervek számára is, így erre a (veszélyek elhárítására történő) folyamatos felkészülés, illetve a (jövőbeli, konkrét) feladatok tervezése során a nemzetbiztonsági szolgálatoknak és más állami szerveknek fokozottan figyelniük kell.

VI. A HIBRID HADVISELÉS EGYES INTÉZKEDÉSEI, KÜLÖNÖSEN A LAWFARE ESZKÖZTÁRA ALKALMAZÁSÁNAK LEHETŐSÉGE A JOGI NORMÁKBAN

1. A biztonságpolitikai stratégiai dokumentumok fogalmi megközelítése

Ebben a fejezetben a fókusz a biztonságpolitikai stratégiai dokumentumok rendszerének, azoknak a jogszabályi környezetbe való beillesztésének és helyzetének mélyreható vizsgálatán van, különös tekintettel azokra a változásokra, amelyek a rendszerváltozás után Magyarországon zajlottak, valamint azokra a kihívásokra, amelyek a jövőben várhatóan érvényesülhetnek. Tekintettel arra, hogy a biztonságpolitika területe rendkívül összetett és sokrétű kérdéseket vet fel, az elemzés során szándékosan korlátoztam a vizsgálat tárgyát, és nem tértem ki a stratégiai dokumentumok belső szerkezetének és tartalmi elemeinek részletes elemzésére. Ennek ellenére kutatásom alapját képezik azok a jelentős előzetes vizsgálati eredmények, amelyek az elmúlt évek során a magyar tudományos közösség által végzett elemzések és vizsgálatok révén jöttek létre. Ezek az eredmények kétségtelenül segítséget nyújtottak a nemzeti szintű stratégiai dokumentumok megértésében és hozzájárultak a magyarországi stratégiai gondolkodás fejlődéséhez, még akkor is, ha egyes elemeit objektív és konstruktív kritikai megjegyzésekkel szükséges ellátni.

Értelemszerűen a „stratégiák” vagy akár a „stratégiai dokumentumok”[290] tárgyszavak alatt megtalálható tudományos munkák[291] szerteágazó módon értelmezik a stratégiák kérdéskörét, amely alapvetően a stratégia, mint fogalom értelmezésére vezethető vissza. Ebben a tekintetben fogalmilag egyrészről az előrelátás szándékát, a tervezést, a cél eléréséhez vezető utat jelenítheti meg, más olvasatban ennek a folyamatnak az eredménytermékét is a „stratégia” (mint dokumentum) jelöli. Míg az első esetében a stratégiai tervezési módszerek sajátos területeinek megújuló fejlődését láthatjuk, addig a stratégiai dokumentumok rendszerében a nemzetközi színtérre is kitekintve egy összetett, a politikai és jogszabályi környezethez illeszkedő, gyakran országonként is eltérő gyakorlattal találkozhatunk.

A stratégia, mint fogalom hadviseléshez köthető gyökerei vitathatatlanok, tartalmi és értelmezési bővülését tekintve a hazai rendszerváltozás időszakában még a hadtudományi kötődés dominanciáját láthatjuk. A hadművészet részeként megjelenő „stratégia” fogalmának, az ezredfordulót megelőzően még a „*...katonai erők kifejlesztésének és alkalmazásának művészete és tudománya béke és háború idején…*”[292] értelmezési eleme volt meghatározó. Napjaink hadtudományi gondolkodásában azonban már jól látható a fogalmi bővülés[293], többek között a NATO terminológia megjelenésével, valamint a „stratégia” hadtudományon túlmutató térhódításának köszönhetően.

2. A stratégiák rendszere, a dokumentumok hazai evolúciója

A biztonsághoz kapcsolódó stratégiai dokumentumok sajátos helyet foglalnak el az egyes országok nemzeti jogszabályi, vagy akár a nemzetközi jogi környezetében. Ezek helyét keresve a stratégiák rendeltetése, hogy hosszabb távon elérendő célokat megfogalmazva valamilyen lépésre késztessék az abban érintett szereplőket és meghatározzák azokat az irányokat, tennivalókat, eszközrendszereket, amelyek ezek eléréséhez szükségesek. Ennek megfelelően az tanulmány szempontjából vizsgálandó biztonsági stratégia „*egy adott nemzet, állam, szövetségi*

[290] Ebben a kérdéskörben jelennek meg pl. a nemzetközi szervezetek politikai prioritásai alapján kidolgozott stratégiai tervek. Lásd. például az Európai Bizottság stratégiai dokumentumainak rendszerét https://ec.europa.eu/info/strategy-documents_hu

[291] A fejezet egyes elemei 2023-ban, HÓDOS László – DOBÁK Imre A biztonsági-stratégiai dokumentumok és a jogszabályi környezet kapcsolata címmel jelent meg In: DOBÁK Imre; RESPERGER István (szerk.) Stratégiák, stratégiai gondolkodás, nemzetbiztonság Budapest, Magyarország: Ludovika Egyetemi Kiadó (2023) 276 p. pp. 165-178. ISBN: 9789635318513

[292] SZABÓ József (főszerk.): Hadtudományi Lexikon, Magyar Hadtudományi Társaság, Budapest, 1995. 1226.o.

[293] KRAJNC Zoltán (főszerk.): Hadtudományi Lexikon, Új kötet, Dialóg Campus, Budapest, 2019. 979. o.

rendszer vagy csoport megtervezett, összehangolt, hosszú távra szóló, központilag vezérelt megfogalmazása és a megvalósítás érdekében tett intézkedések összessége."[294]

A stratégia, mint dokumentum, széles körben épít a tudományos és szakmai területek szakembereinek együttműködésére, ahol fontos elem a normatív szabályozási környezettel való összhang megteremtése, az ahhoz történő illesztése. Hazánkban az elmúlt évtizedekben számos, a biztonság tágan értelmezett területéhez sorolható stratégia született, amelyek okai mögött a nemzeti szintű stratégiaalkotási szándék, a nemzetközi színtéren történt stratégiaalkotási folyamatok bizonyos mértékig történő leképeződése, a változások kiigazítása vagy akár új irányokban (pl. kiberbiztonság, mesterséges intelligencia) stratégiák megalkotása látható.

Általánosan megfogalmazható, hogy a nemzeti szintű biztonsági dokumentumok hierarchiájának csúcsán a nemzeti biztonsági stratégiák dokumentumai állnak, amelyek széles spektrummal tekintenek ki a külső biztonsági környezetre, veszik számba az ott megjelenő kihívásokat, kockázatokat, fenyegetéseket, és megfogalmazott céljaik mentén kívánnak „stratégiát" megfogalmazni az oda vezető úthoz. Fontos hangsúlyozni, hogy ezen magas szintű biztonság(politikai) dokumentumok belső tartalma összhangot mutat az adott ország alaptörvényével, az esetleges szövetségi tagságból adódó alapelvekkel. A dokumentumhierarchia alacsonyabb szintjén, az ágazati stratégiák sorában jelenhetnek meg többek között a katonai, külügyi, energetikai, gazdasági-pénzügyi, vagy akár a tematikusan készülő, és több ágazatot (pl. szakminisztériumot) érintő nemzeti szintű kiberbiztonságra irányuló stratégiák.

A rendszerváltozást követő időszakban hazánkban az ország biztonsághoz való viszonyának az biztonság és védelempolitikai alapelvek dokumentumai adtak keretet. A stratégiai dokumentumokká történő fejlődés csak ezt követően, az ezredfordulóhoz közeledve következett be. Hazánk biztonság- és védelempolitikájának megjelenítéséhez tartozó dokumentumok sorában a rendszerváltozást követően, az 1993-ban megalkotott a Magyar Köztársaság biztonságpolitikájának alapelveiről szóló 11/1993. (III. 12.) OGY határozat, és a Magyar Köztársaság honvédelmének alapelveiről szóló 27/1993. (IV. 23.) OGY határozat tekinthetőek az első, a biztonságpolitikai gondolkodást állami szinten meghatározó

[294] HÉJJA István – KENEDLI Tamás: *Az elemző-értékelő munka elméleti és gyakorlati kérdései*. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 2011, 17. o.

dokumentumoknak. A szakirodalmak azonban csak az 1998-ban, a 94/1998. számú Országgyűlési határozattal elfogadott, a Magyar Köztársaság biztonság- és védelempolitikája dokumentumát tekintik azon kezdeti elemnek, amely megindította a hazai Nemzeti Biztonsági Stratégia (valamint a Katonai Stratégia) kidolgozásának, a kormány felelősségébe utalt folyamatát. Erre a keretet, a terjedelmében is rövid határozat utolsó, 17. pontja teremtette meg, miszerint „*A Magyar Köztársaság Országgyűlése gondoskodik az e dokumentumból adódó feladatok teljesítéséhez szükséges feltételek biztosításáról. A Magyar Köztársaság Kormánya felelős a nemzeti biztonsági stratégia és a nemzeti katonai stratégia kidolgozásáért, azok szükség szerinti felülvizsgálatáért, valamint a belőlük fakadó feladatok végrehajtásáért*."[295]

Időrendben ezt követően 2012 májusában került elfogadásra a 2144/2002. számú Kormányhatározattal kiadott Nemzeti Biztonsági Stratégia, majd 2004-ben a korábbi Stratégiát váltó 2073/2004. számú, a Magyar Köztársaság (új) nemzeti biztonsági stratégiájáról szóló Kormányhatározat, amely évekig irányt jelentett az alacsonyabb szintű stratégiák kidolgozásának is. Ehhez igazodva kerültek kialakításra például 2008-ban a Külkapcsolati Stratégia (1012/2008. (III.4.)), valamint 2009-ben hazánk Katonai Stratégiája (1009/2009. (I.30.). A következő fordulópontokat a 2012-ben kiadott, Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Kormányhatározat jelentette, amely a Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat (hatályos NBS) 2020-ban történt megjelenéséig töltötte be a legmagasabb szintű biztonsági stratégia szerepét.

A Nemzeti Biztonsági Stratégiával összhangban álló, ágazati stratégiák kidolgozásának feladata általánosságban végig kísérte az elmúlt 30 év stratégiaalkotási törekvéseit, az azonban már további kérdés, hogy ezen ágazati stratégiák milyen mértékben, illetve egyáltalán elkészültek-e. A 2004-ben kiadott Nemzeti Biztonsági Stratégia esetében például (határidőkkel és felelősökkel) került megjelenítésre az alacsonyabb szintű ágazati stratégiák kidolgozásának feladata. A 2012-ben kiadott NBS-ben ugyanakkor a felelősök és határidők ebben az értelemben már nem kerültek megjelenítésre.[296]

Általánosságban jól látható az is, hogy a hazai gyakorlatban a rendszerváltozás időszakát

[295] 94/1998. (XII. 29.) OGY határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről, Elérhető: https://mkogy.jogtar.hu/jogszabaly?docid=998h0094.OGY
[296] SOLTI István: A nemzetbiztonsági stratégia a Nemzeti Biztonsági Stratégia tükrében. *Nemzetbiztonsági Szemle*, 2. évf. 2014/3. sz., 47–60. o.

követően kiadott nemzeti biztonsági stratégiákra egyaránt jellemző azok kormányhatározatban (annak mellékleteként) történő kiadása. Mindezzel összhangban a végrehajtásról szóló ágazati stratégiai dokumentumok már a felelős szaktárcák („*feladat-és hatáskörrel rendelkező miniszterek*") tevékenységét igénylik. A 2020-ban kiadott – hatályos – NBS összeállítása is a kormány felelősségi körében jelent meg, az általuk meghatározott szakértői kör (minisztériumok) előkészítésével. A határozatban a Kormány a stratégiai dokumentum végrehajtását szolgáló ágazati stratégiai dokumentumok felülvizsgálatát, illetve elkészítését határozza meg a feladat- és hatáskörrel rendelkező miniszterek számára.

A stratégiák készítésének napjainkra már széles körben elfogadott, akár az állami szférához kapcsolódó készítési módszertanai, előírásai ismertek. Hazánkban az állami oldalon készülő stratégiai tervezés és dokumentumok készítése során a kormányzati stratégiai irányításról szóló 38/2012. (III.12.) Korm. rendelet emelhető ki, amely „szabályozza a […..] közpolitikai dokumentumoknak tekinthető, nem-jogi dokumentumok típusait."[297] A szabályozás kitér a nemzetközi színtéren elterjedtebb ún. Zöld Könyvre és Fehér Könyvre, valamint megjeleníti többek között a kötelezően elkészítendő stratégiai tervdokumentumokat (pl. országelőrejelzések, vagy akár nemzeti középtávú stratégia). A nyugati országokban gyakran találkozhatunk a fehér könyvek „*a védelmi stratégiát, a hadsereg fejlesztésére, a gazdaság biztonságára és nem utolsó sorban a nemzetbiztonsági szolgálatok szervezeti és személyzeti fejlesztésére vonatkozó kormányzati elképzeléseket, közép- és hosszútávú célokat*"[298] rögzítő dokumentumaival, mint előremutató „szándéknyilatkozatokkal". Mint Gajduschek megfogalmazza," *Ilyen jellegű dokumentumok ugyan korábban is léteztek, ám ezek státusza meglehetősen bizonytalan volt, illetve legtöbbjük, […] jogi formában vagy nem-jogi állami normaként jelent meg.*"[299]

3. A stratégiaalkotás jogszabályban meghatározott folyamatai

A stratégiai tervdokumentumok „előkészítésére, társadalmi véleményezésére,

[297] GAJDUSCHEK György: Közpolitikai célok megjelenése a jogban. In: JAKAB András – GAJDUSCHEK György (szerk.): *A magyar jogrendszer állapota*. Budapest: MTA Társadalomtudományi Kutatóközpont, 2016, 55. o. ISBN 978-963-418-006-7

[298] SABJANICS István: A nemzetbiztonság jogi koncepciója. In: CSINK Lóránt (szerk.): *A nemzetbiztonság kihívásainak hatása a magánszférára*. Budapest: Pázmány Press, 2017. (A Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Karának könyvei – Tanulmányok 40.), 113. o.

[299] GAJDUSCHEK György: Közpolitikai célok megjelenése a jogban In: Jakab András, Gajduschek György (szerk.): A magyar jogrendszer állapota, MTA Társadalomtudományi Kutatóközpont (Budapest), 2016. ISBN 978-963-418-006-7, 55.o.

elfogadására, közzétételére, megvalósítására, nyomon követésére, valamint előzetes, közbenső és utólagos értékelésére, továbbá felülvizsgálatára vonatkozó követelményeket" a már említett, a hazai szabályozásban hatályos 38/2012. (III.12.) Korm. rendeletből ismerhetjük meg. Az itt megfogalmazottakat kell alkalmazni az állami szféra oldalán[300] készítendő stratégiák esetében, amelyek többek között törvény vagy az Országgyűlés normatív határozata alapján, vagy akár nemzetközi szerződés vagy egyéb nemzetközi kötelezettségvállalás alapján kerülnek létrehozásra, de ennek rendszere alkalmazható például az államigazgatási szervek által elkészítendő (intézményi) stratégiákra is.

A stratégiák megalkotására általánosságban összetett szempontrendszer érvényesül. A kormányzati szinten készülő biztonságpolitikai dokumentumoknak mélyebb szakmai elemei és iránymutatása legalább kétirányúnak tekinthető. Ennek egyik elemének tekinthető, hogy *„...kijelöli az intézmények által ellátandó feladatokat, elhatárolja a hatásköröket, megteremti a feladatteljesítéshez szükséges megfelelő jogszabályi hátteret és rendelkezésre bocsájtja a szükséges forrásokat."* [301] másrészről tagadhatatlan a politikai üzenete a külvilág felé. Kifejezi, hogy a kormányzat (fel)ismeri a biztonságot jelentő tényezőket, és kész azokra reagálni. Ezen tényezők és cselekvési irányok együttese azonban a külső környezet (pl. szomszédos ország) számára üzenetként jelenik meg, kifejezve érdekeit (pl. szomszédos országokkal való bélés együttműködésre való törekvés), vagy akár a nemzetközi szövetségi együttműködés iránti szoros elkötelezettséget.

A hazai szabályozás alapján a kormányzati stratégiai irányításra vonatkozó alapelvek között jelennek meg[302] a stratégiai tervdokumentumok és a kapcsolódó kormányzati intézkedések, valamint a különböző, egymáshoz kapcsolódó stratégiák időtávja[303] összhangjának biztosítása (a rövidebb időtávot felölelő stratégia, hosszabb időtávra szóló stratégiához történő illesztése). A rendelet kitér továbbá[304] a stratégiában megfogalmazottak

[300] A rendelet hatálya kiterjed a Kormányra, a minisztériumokra, a Miniszterelnöki Kormányirodára, a kormányhivatalokra, a központi hivatalokra, a rendvédelmi szervekre és a fővárosi és megyei kormányhivatalokra. Lásd: A kormányzati stratégiai irányításról szóló 38/2012. (III.12.) Korm. rendelet.
[301] DÁVID Ferenc: Nemzeti biztonság és nemzetbiztonság a stratégiaalkotásban. *Nemzetbiztonsági Szemle*, 5. évf. 2017/3. sz., 5–21. o., 11. o.
[302] A kormányzati stratégiai irányításról szóló 38/2012. (III. 12.) Korm. rendelet 6. §
[303] A stratégiák időtávja kapcsán a vonatkozó hazai szabályozás a stratégiák időtávját a következőkben határozza meg: hosszú távú: tíz évet meghaladó időtáv; középtávú: legalább négy, legfeljebb tíz éves időtáv; rövid távú: legalább egy, legfeljebb négy éves időtáv;
[304] 38/2012. (III.12.) Korm. rendelet 6. § (9) bekezdés

megvalósíthatóságának, a megvalósítás pénzügyi hátterének, vagy akár a kapcsolódó stratégiai tervdokumentumok egymásra épülő rendszerének kérdéseire is.

A hazai és nemzetközi stratégiák szerkezete között számos hasonlóság fedezhető fel, amelyek a stratégiai tervezés módszertanának fejlődéséből és az idők során kialakult és általánosan elfogadott dokumentumstruktúrák használatából adódhatnak. A stratégiaalkotás folyamatában felhasznált tudományos ismeretek és modellek mellett, különösen fontosak azok a módszerek, amelyek a stratégia egyes elemeinek kidolgozására alkalmazhatóak.

Például a külső környezet feltárásához és a tendenciák feltérképezéséhez használt elemzési technikák különösen hasznosak lehetnek. Ezek az elemzési módszerek segíthetnek abban, hogy a rendelkezésre álló adatok és információk alapján mélyebb megértést nyerjünk a komplex folyamatokról, és ezáltal megalapozottabbá tegyük a jövőbeli döntéseket. Az ilyen típusú elemzések lehetnek például a SWOT-analízis (erősségek, gyengeségek, lehetőségek és fenyegetések elemzése), PESTEL-analízis (politikai, gazdasági, szociális, technológiai, környezeti és jogi tényezők elemzése) vagy más, a stratégiai tervezés során alkalmazott eszközök.

A stratégiaalkotás során tehát kiemelt jelentőséggel bírnak azok a módszertani eszközök, amelyek segítségével a szervezetek képesek a változó környezeti feltételekhez alkalmazkodni, proaktív módon kezelni a kihívásokat, és kiaknázni a felmerülő lehetőségeket.

A kormányzati szintű stratégiakészítés támogatására ugyanakkor elkészültek azok az ajánlások[305], útmutatók, amelyek az egységes tervezési folyamatokat segítették. Ezek között emelhető ki a 2008-ban közzétett „Stratégia-alkotási Kézikönyv”[306] című dokumentum, amely útmutatást ad a kormányzati szintű stratégiaalkotáshoz és módszertani ismeretek alkalmazásához. Mint annak bevezetőjében megfogalmazásra kerül a kézikönyv „*a stratégia-alkotás általános, minden szakpolitikai területre érvényes tennivalóit gyűjti egybe”*.[307]

[305] KÁDÁR Krisztián: *A közigazgatás stratégiai tervezésének és fejlesztésének módszertana*. [ÁROP–1.1.21 projekt tananyag.] Budapest: Nemzeti Közszolgálati Egyetem, 2017.
[306]Gazdasági és Közlekedési Minisztérium: *Stratégia-alkotási Kézikönyv — A Kormányzati Stratégia-alkotási Követelményrendszer (KSaK) alapján*. Budapest: GKM, 2008.
[307] Gazdasági és Közlekedési Minisztérium: *Stratégia-alkotási Kézikönyv — A Kormányzati Stratégia-alkotási Követelményrendszer (KSaK) alapján*. Budapest: GKM, 2008. p. 5.

4. A stratégiatervezés jogszabályban meghatározott különleges céljai és a jogi normaalkotás korlátjai

Az értekezésem fókuszába állított szempontrendszer alapján feltétlenül igaz, hogy a stratégiai gondolkodás, illetve szemlélet meghatározó jellemzői, hogy a proaktív jogalkotást preferálja, a célokat beazonosítja, ezen célokhoz prioritásokat rendel és végül a rendelkezésre álló összes információ alapján hoz megalapozott döntést. Amennyiben a stratégiatervezés során előbbi jellemzők közül egy vagy több nem teljesül, úgy létrejön az eredménytermék, azonban az csak nevében, de nem tartalmában tekinthető stratégiának.

Korlátozott információk megléte esetén törekedni kell arra, hogy a stratégia, mint jogi norma az egyébként is kötelező jogalkotási eszközként megjelenő, szükséges mértékű általánosítás eszközével élve kellő rugalmasságot biztosítson, egyfajta keretet alkosson a prioritások útján a célok eléréséhez.

A hon-, valamint rendvédelem, illetve a nemzetbiztonság feladatrendszerére alapozó stratégiaalkotás esetében megjegyezhető, hogy minden (szükséges) információ nagyon ritkán áll (egyidejűleg) rendelkezésre, azonban mégis a körülményekhez képest megalapozott javaslatot, illetve döntést vagy annak előkészítését várja el az irányító. Így lényegében stratégiai gondolkodás eredményeként kell szakmailag megszövegeznie a hon-, valamint rendvédelem, illetve a nemzetbiztonság szakterületét érintő stratégiákat az ezekért felelős szervezeteknek önállóan vagy együttműködésben a feladatban érintett, illetve ahhoz kötődő feladatrendszerű más szervezetekkel. Mindezt annak érdekében, hogy a jogforrást – végül – kibocsátó (Országgyűlés, ágazatot irányító miniszter, illetve államtitkár) testület vagy személy megvizsgál(tat)ja a(z esetlegesen) már meglévő stratégiai tervdokumentumokat és a kapcsolódó központi államigazgatási tevékenység keretrendszerét a norma tervezetben leírtak megvalósíthatóságát, valamint a kivitelezhetőségét pénzügyi szempontból úgy, hogy ezzel egyidejűleg ellenőrzi a tervezetben szereplő célok, prioritások, intézkedések, javaslatok összeegyeztethetőségét a kormányzat politikai célkitűzéseivel.

5. A nemzetbiztonsági ágazat szempontrendszerének sajátosságai a stratégia kodifikációja során

A nemzetbiztonsági ágazatra alkalmazandó szabályozási keretrendszer folyamatos felülvizsgálatát két alapvető eszköz garantálja. Az első eszköz a jogszabályok utólagos hatásvizsgálata, amely lehetővé teszi, hogy megvizsgáljuk a jogi normák tényleges következményeit, és összehasonlítsuk azokat az eredetileg várt hatásokkal. A második eszköz a tartalmi dereguláció, ami azt jelenti, hogy rendszeresen felülvizsgáljuk és szükség szerint módosítjuk a jogi előírásokat, hogy azok világosabbak és érthetőbbek legyenek mind a szakemberek, mind a laikusok számára.

Ezek a folyamatok nem csak a jogszabályok megalkotása előtt fontosak, hanem azok hatályba lépése után is, annak érdekében, hogy biztosítsák a szabályozás naprakészségét és hatékonyságát. Az utólagos hatásvizsgálat során például összevetjük a jogszabályok valós hatásait a bevezetésük vagy módosításuk idején várt hatásokkal, figyelembe véve a javasolt módosítások arányosságát és az esetleges jogkorlátozásokat.

A tartalmi deregulációval kapcsolatos kötelezettség pedig túlmutat az előbb említett elemeken, és különösen a jogi kodifikáció szempontjai szerint hivatott előmozdítani a jogbiztonságot, a jogrendszer átláthatóságát és a normák világosságát. Mindez jelentős hatással van az ágazati stratégiaalkotásra is, mivel a megvalósítandó célokhoz szükséges eszközök és erőforrások rendelkezésre állása meghatározó tényező a stratégiai célkitűzések realisztikus megfogalmazásában. A stratégiák kidolgozásában részt vevő szervezetek így képesek pontosan meghatározni a prioritásokat és az erőforrás-szükségleteket, ismerve a kitűzött célokat.

A nemzetbiztonsági szolgálatok által alkalmazott erők, eszközök és módszerek együttes hatásmechanizmusának szabályozási rendszere a jogforrási hierarchia legmagasabb szintjétől a legalacsonyabbig terjedő széles skálán található. Ezek a magyar nemzet biztonságának védelme érdekében – döntően titokban, néha nyíltan – kerülnek alkalmazásra a szolgálatok munkatársai által. A jogi normákban megjelenő feladatok végrehajtása valószínűsíthető alapjog-korlátozással jár együtt, emiatt ezeket az állami monopóliumként kodifikált intézkedéseket szigorú előírások között gyakorolhatják az erre feljogosított szervezetek. Előbbiek alapozzák meg azt a szempontrendszert, melynek megfelelően az egyes stratégiákkal szoros kölcsönhatásban lévő, kiemelt jelentőségű normaszöveg változások az indokoltság, továbbá a szükségességnek és arányosságnak – a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvényből levezethető alapelveknek – való megfelelés vizsgálatára szükséges sort kerítenie az előkészítő szervezetnek és a jogalkotónak is.

Ezen vizsgálat legegyszerűbb, de talán mégis legfontosabb megállapítása, mely példaként jeleníti meg a normakontroll jelentőségét is, hogy a törvényben megjelenített feladatok elvégzése céljából végrehajtottól eltérő esetben tilos titkos információgyűjtést folytatni, hiába vetődik fel a cél egy stratégia előkészítése során, azt legkésőbb a jogalkotó törli a tervezetből, vagyis a stratégia normaszövegéből. Vagyis a célhoz kötöttség elvét szigorúan ellenőrzi a jogalkotó, hiszen valószínűsíthetően alapjogkorlátozásról lehet szó, az egyes konkrét – szolgálatok által végrehajtott – intézkedések során.

6. A jogi eszközökkel folytatott hadviselés szempontrendszerének érvényesülése a stratégiák előkészítése során

A stratégia tervezése, illetve előkészítése során emiatt is indokolt kiemelt figyelmet fordítani az előbbiekben megjelenített alapelvekre, a tevékenységre vonatkozó jogszabályi előírások részletes áttekintésére, valamint a szakmai döntéselőkészítés korlátjaira. Fontos megjegyezni, hogy jogszabálynak a tanulmány témájának területeit érintően (is) a törvényeket, kormányrendeleteket, miniszteri rendeleteket tekintjük. A jogalkotásra vonatkozó törvény[308] és annak végrehajtására kiadott, a jogforrási hierarchiában alacsonyabb szinten szereplő jogi norma előírásait kizárólag a közjogi szervezetszabályozó eszközökre és a jogszabályokra vonatkozóan rendeli kötelezően alkalmazni. Így azokra a kormányhatározatokra és országgyűlési határozatokra vonatkoznak csak a szigorú előírások, melyek tartalmukat tekintve előbbi testületek szervezetét és működését, tevékenységét, valamint cselekvési programját rögzítik.

Emiatt a tervezet szakmai tartalmának és jogrendszerbe illeszkedésének biztosítását, valamint az előzetes hatásvizsgálatot nem kötelező elvégezni például egy új NBS elkészítésekor. A kibocsátónak nem kell megfelelnie indokolási kötelezettségnek, továbbá a tervezet véleményezésekor sem kötelezhető olyan egyeztetésre, mint amilyenre egy jogszabály készítése esetében.

Nagyon fontos kiemelni, hogy nem szükséges az utólagos hatásvizsgálatot elvégezni, ahogyan a tartalmi felülvizsgálat végrehajtására vonatkozó rendelkezéseket sem kell

[308] 2010. évi CXXX. tv. a jogalkotásról

alkalmazni. A munkájára igényes kodifikációval foglalkozó szakemberek esetében íratlan szabály, hogy a nem jogszabálynak vagy közjogi szervezetszabályozó eszköznek minősülő tervezetek készítése, szerkesztése során – a lehetőségekhez mérten – a jogalkotásról szóló törvény és különösen a végrehajtására kiadott miniszteri rendelet[309] előírásait is igyekeznek figyelembe venni annak érdekében, hogy a jogalkotás egységessége érvényesüljön.

A stratégia kialakítása és megfogalmazása során, amikor a kibocsátó részére történő felterjesztésről és a jogalkotói döntéshozatal előkészítéséről van szó, kiemelten fontos figyelemmel lenni arra, hogy a jogalkotás folyamata és annak integritása különösen sebezhető a dezinformáció és az álhírek terjedése szempontjából. Ez a sérülékenység mind a hazai, mind a nemzetközi színtéren megfigyelhető.

A stratégia szövegezésének során kulcsfontosságú a jogi és szakmai alaposság, az átláthatóság, a proaktív kommunikáció, a kontextus érzékenységének biztosítása és az álhírekkel szembeni ellenálló képesség erősítése. Mindezek hozzájárulnak ahhoz, hogy a jogalkotási folyamat védve legyen a hazai és nemzetközi színtéren történő támadásoktól és dezinformációtól.

Az értekezésem középpontjában álló lawfare[310], amely elsősorban a jogi eszközök alkalmazását jelenti a hibrid hadviselés során, definiálható[311] úgy, hogy ide sorolandó a jogalkotás legfelsőbb szintje által alkotott jogforrások folyamatos, az esetek többségében nem feltétlenül megalapozott támadása is, mivel ezen tevékenység a célja a jogalkotó hiteltelenítése, a belé vetett közbizalom megingatása. Az írott jog primátusának helyességébe vetett társadalmi bizalom gyengítése alkalmas az állam destabilizálására, a mozgásterének csökkentésére. Ideértve a kibocsátó által kihirdetett – biztonsági tartalmú – stratégiákat, vagy az azokkal összhangban álló, alárendelt szervezetek által végzett – biztonsággal összefüggő – tevékenység jogszerűségét.

[309] 61/2009. (XII. 14.) IRM rendelet a jogszabályszerkesztésről

[310] A kifejezés használatáról bővebben lásd: Colonel Charles J. Dunlap: Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts

[311] Ezzel a gondolattal összefüggésben fontosnak tartom megjegyezni, hogy Dunlap álláspontja szerint a jogi hadviselés egy saját magunknak okozott seb, amely a jogállamiság elvéhez történő ragaszkodás útján megelőzhető. A modern hadviselés kulcselemének számít az a szempontrendszer, amelyet Dunlap ismertetett műveiben megfogalmazott. Stabil, különösen (nemzetközi köz)jogi háttér nélkül nem fogadja el a közvélemény sem a háborúban való szerepvállalást, kiemelten annak megkezdését.

Az írott jogszabályokban meghatározott tilalmak és korlátozások felülvizsgálata, tudományos alaposságú kutatása egy stratégiai tervezési folyamat során kiemelten fontos szerepet játszik, hiszen ezek a segíthetnek feltárni a jelenlegi jogi környezet hiányosságait és hibáit, különös tekintettel a honvédelemre, a rendvédelemre és a nemzetbiztonságra vonatkozó jogi normákra. Ezek a felismerések rávilágíthatnak arra, hogy szükséges lehet a meglévő törvények módosítása vagy új szabályozások bevezetése annak érdekében, hogy az adott ágazatok hatékonyabban tudjanak működni és reagálni a kor kihívásaira.

Ez a folyamat alátámasztja azt az elképzelést, hogy a honvédelmi, rendvédelmi és nemzetbiztonsági szervezetek által kidolgozott szakmai tervek és javaslatok, amelyek akár egy átfogó ágazati stratégia részeként is megfogalmazódhatnak, nem állnak elszigetelten a szélesebb kormányzati politikától. Épp ellenkezőleg, a szervezetek által előterjesztett koncepciók és azok tartalma szorosan összefonódhatnak a kormányzati célkitűzésekkel és prioritásokkal. Ennek eredményeképpen egy olyan együttműködés jöhet létre, amelyben a célok és prioritások megvalósítása, valamint az alkalmazott eszközök és módszerek közötti összhangot folyamatosan szem előtt tartják és igyekeznek optimalizálni. Az ilyen típusú interakciók révén javulhat a stratégiai tervezés minősége és az adott ágazatokban történő végrehajtás hatékonysága is.

Az összhang, mint célkitűzés megjelenítésre került a Kormány által a hatályos NBS előírásainak szövegezése során, miszerint *„az állami szervek saját szakterületükön folyamatosan értékelik a nemzeti és a nemzetközi biztonság és fenyegetettség elemeit, és megteszik a szükséges lépéseket a megelőzés és a kezelés érdekében, továbbá, a biztonság egyes részterületeiért felelős szervezetek a jelen dokumentumban adott iránymutatás figyelembevételével alkotják meg és vizsgálják felül saját szakági szabályozóikat”.* [312] Vagyis azt határozta meg a jogalkotó, hogy a szakstratégiák megalkotása során a tárcáknak figyelemmel kell lenniük arra, hogy azok álljanak összhangban a hatályos NBS-ben foglaltakkal.

A hatályos NBS kifejezetten előírja, hogy a biztonság egyes részterületeiért felelős állami szervezeteknek a Stratégiában megfogalmazott iránymutatásokkal összhangban kell

[312] 1163/2020. (IV. 21.) Korm. határozat - Magyarország Nemzeti Biztonsági Stratégiájáról - Záró rendelkezések

megalkotniuk és felülvizsgálniuk a tevékenységükre vonatkozó szakági szabályzókat, különös tekintettel a nemzeti katonai, a rendészeti, a nemzetbiztonsági, a terrorelhárítási, a katasztrófavédelmi, a kiberbiztonsági és a migrációs területekre. Mindezt úgy kell elvégezni, hogy a hatályos NBS rendelkezéseit is a korábban említett, folyamatos felülvizsgálati kötelezettség terheli, így amennyiben valamely érintett szerv hatáskörében erre okot adó körülményt derít fel, jeleznie szükséges azt az irányító tárc(áj)a felé, hogy a szükséges normaalkotás kezdeményezhetővé váljon.

Vagyis, ha az érintett szakmai szervezetek és a kibocsátó is követi az előírásokat, akkor kizárólag kölcsönösen együttműködve, egymást mozgásban tartva alkothatnak szakági szabályzókat, illetve szakstratégiákat.

Korlátozó tényezőként jelenik meg az a körülmény, hogy a minősített adatok védelméről szóló törvény nem tartalmaz tételes felsorolást rögzítő mellékletet, hanem a tevékenységet végző, szakmai anyagot (elő)készítő kötelességévé teszi, hogy mérlegelje, hogy mely adatok ismertethetőek nyilvánosan és melyek azok a közlések, amelyek nyilvánosságra hozatala kárt okozna Magyarország számára. A mérlegelés felelőssége a biztonsági, különösen az egyes biztonsági területekre vonatkozó szakstratégiák megalkotása témakörében különösen jelentős, egy tévedés, egy felelőtlen intézkedés, illetve mulasztás – a károkozás mellett – büntetőjogi felelősségre vonással is járhat.

Emiatt szükséges kiemelni azt a tényt, hogy jogi szempontból különbséget kell tenni az alaki jogforrásokban megjeleníthetőség szabadságának foka szerint is, vagyis amennyiben indokolt az adattartalom vizsgálata alapján, nem használható a nyílt Korm. határozat, mint alaki jogforrás, hanem kizárólag minősített Korm. határozatban rögzíthető a tartalom. Utóbbi esetben azok és csakis azok ismerik meg a szakstratégia tartalmát, akik erre jogosultak, az idegen hírszerző szolgálatoknak nem elég pusztán az Internetről letölteniük a dokumentumot. Kivéve persze, ha az a kibocsátó kifejezett célja, hogy legyen letöltve és támpontként kezelve a kíváncsi olvasó számára a dokumentum.

7. Nemzetbiztonság a biztonsági stratégiák tükrében

A (nemzeti) biztonsági stratégiáknak különös viszonya van a szűkebben értelmezett nemzetbiztonság területével, hiszen a biztonsági stratégiák, mint dokumentumok alapját *„az*

állam biztonságfelfogása, azaz a biztonságról, annak alkotóelemiről, területeiről, különösképpen pedig a biztonságot fenyegető tényezőkről alkotott képe jelenti".[313] Ebben különös szerep hárulhat a nemzetbiztonsági „ágazatra", amely stratégiai gondolkodáshoz kapcsolódó helyét és szerepét keresve, az „előrelátás" támogatása, a pontos döntések meghozatalához szükséges információk megszerzése és értékelése kapcsán emelhető ki. Napjainkban előbbiekhez egyre több, különböző formában keletkező és elérhető adat állhat rendelkezésre, amelyek előtérbe hozták az adatfúziós típusú gondolkodás, és így komplexebb, pontosabb elemzések, akár előrejelzések készítésének lehetőségét. Ennek a tanulmány szempontjából kiemelkedő jelentőségű megnyilvánulása az angolszász jogterületen már alkalmazott, bírói döntéseket monitorozó mesterséges intelligencia, amely rossz kezekben alkalmas lehet a bűnözői körök számára „előrelátást, akár kockázatértékelést elősegítő támogatást" biztosítani.

A mesterséges intelligencia, a dezinformációs műveletek, az álhírekkel történő operáció, a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenésekor és gyors terjedésekor, egymás hatását erősítő, egy adott országgal szembeni (nemzetbiztonsági) kombinációként (műveleti intézkedések sorozataként) azonosítható.[314]

8. A hibrid fenyegetések és a dezinformáció elleni küzdelem az Európai Unió stratégiai normaalkotó, illetve döntéshozatali szintjein, a reziliencia jelentősége

A reziliencia, vagyis az ellenállóképesség az EU számára nem csupán egy belső cél, hanem egy stratégiai irányvonal, amely lehetővé teszi a közösség számára, hogy hatékonyan reagáljon a különböző külső és belső kihívásokra. Az EU története során számos kihívással nézett szembe, amelyek próbára tették annak ellenálló képességét és adaptációs képességét. Az EU-nak meg kell őriznie és tovább kell fejlesztenie rezilienciáját annak érdekében, hogy fenntartható módon kezelje a gazdasági válságokat, a politikai instabilitást, a természeti katasztrófákat, a hibrid fenyegetéseket és a pandémiákat. A reziliencia fogalma az EU kontextusában egy összetett rendszer képességét jelenti, annak érdekében, hogy szembe tudjon szállni a váratlan eseményekkel, alkalmazkodjon az új kihívásokhoz és gyorsan regenerálódjon

[313] CSIKI Tamás: A stratégiai dokumentumok rendszere, In.: Nemzet és Biztonság 2008. szeptember 76.o.
[314] A hatályos NBS által azonosított biztonsági kockázatokkal szembeni hatékony fellépés rögzítése iránti kormányzati igény esetén cél a szélesebb összhang megteremtése a teljes biztonsági szektor vonatkozásában.

a válságok után. Az EU-nak, mint politikai és gazdasági entitásnak képesnek kell lennie arra, hogy előre lássa a potenciális veszélyeket, felkészüljön rájuk és képes legyen gyorsan helyreállni. A reziliencia nem csupán a túlélésről szól, hanem a fejlődésről és az előrelépésről is, még a legnehezebb időszakokban is.

Az EU gazdasági rezilienciájának középpontjában az áll, hogy hogyan tudja kezelni és megelőzni a gazdasági válságokat. A 2008-as pénzügyi válság óta az EU számos intézkedést hozott a gazdaság stabilizálása és a jövőbeni sokkok elleni védelem érdekében. Ezek közé tartozik a bankunió létrehozása, a Gazdasági és Monetáris Unió [315] megerősítése, valamint az Európai Stabilitási Mechanizmus[316] (ESM) kialakítása. A COVID-19 járvány idején bevezetett NextGenerationEU alap is egy példa arra, hogy az EU hogyan tud gyorsan és hatékonyan reagálni egy globális válságra. A politikai stabilitás és a demokratikus intézmények megerősítése létfontosságú az EU rezilienciájának szempontjából. Az EU-nak folyamatosan küzdenie kell a populizmus, az autoriter tendenciák és a jogállamiság aláásása ellen. Emellett fontos a társadalmi kohézió és az inkluzív növekedés elősegítése, amelyek hozzájárulnak az EU polgárainak bizalmának növeléséhez. A klímaváltozás és a természeti katasztrófák egyre nagyobb nyomást gyakorolnak az EU-ra. A fenntarthatóság és az éghajlati reziliencia előmozdítása érdekében az EU elfogadta az Európai Zöld Megállapodást[317], amelynek célja, hogy Európát 2050-re klímasemlegessé tegye. Az EU-nak továbbra is innovatív megoldásokat kell találnia a környezeti kihívások kezelésére. Emellett az egészségügyi reziliencia erősítése is kiemelt cél, amelyhez az Európai Gyógyszerügynökség[318], az ECDC és más egészségügyi szervek megerősítése is hozzájárul. Végül, de nem utolsósorban az EU igyekszik növelni stratégiai autonómiáját olyan területeken, mint az energiaszektor vagy a high-tech iparágak.

Kiemelt jelentőséggel bírnak a horizontális hibrid fenyegetések és a dezinformáció elleni munkacsoportok, melyek az Európai Tanács mellett működnek.[319] Az elmúlt években az

[315] A Gazdasági és Monetáris Unió működéséről szóló információk elérhetők: https://www.consilium.europa.eu/hu/policies/emu-deepening/ (letöltés dátuma: 2023. 10.18.)
[316] A szervezet céljairól a válságok kezelése során: https://www.consilium.europa.eu/hu/infographics/reform-of-the-european-stability-mechanism-esm/ (letöltés dátuma: 2023. 10.18.)
[317] A célkitűzéseiről és a reziliencia növelésében játszott szerepéről: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/european-green-deal_hu (letöltés dátuma: 2023. 10.18.)
[318] Feladatairól bővebben: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-medicines-agency-ema_hu (letöltés dátuma: 2023. 10.18.)
[319] A reziliencia fokozásával és a hibrid fenyegetésekkel szembeni fellépéssel foglalkozó horizontális munkacsoport 10027/19 számú állásfoglalása (Elérhető: https://data.consilium.europa.eu/doc/document/ST-10027-2019-INIT/en/pdf letöltés dátuma: 2023. 10.18.)

Európai Unió biztonsági környezete drámaian megváltozott. A békét, a biztonságot és a jólétet érintő jelenlegi kihívások közül sok az EU közvetlen szomszédságában tapasztalható instabilitásból és a fenyegetések változó formáiból ered. Annak elismerése mellett, hogy a hibrid fenyegetésekkel szembeni fellépés elsődleges felelőssége a tagállamokat terheli, mivel a legtöbb nemzeti sebezhetőség országspecifikus, és hangsúlyozva, hogy a nemzetbiztonság továbbra is az egyes tagállamok kizárólagos felelőssége (az EUSZ. 4 cikk (2) bekezdése[320] alapján), határozottan felismerik azt a tényt is, hogy számos tagállam közös fenyegetésekkel néz szembe. Az ilyen fenyegetések uniós szintű, összehangolt válaszlépésekkel hatékonyabban kezelhetők. A hibrid fenyegetések és a dezinformáció elleni küzdelem, a stratégiai kommunikáció javítása és a reziliencia fokozása az európai szolidaritásra építve a biztonsági környezet javítására irányuló uniós erőfeszítések kulcsfontosságú elemei. Az EU biztonságpolitikai rezilienciájának javítása érdekében integrált megközelítést kell alkalmazni, amely magában foglalja a hibrid fenyegetésekkel és a kibertér biztonságával kapcsolatos kérdéseket is. Az EU-nak erősítenie kell kiberbiztonsági képességeit, valamint növelnie kell az információbiztonságát a dezinformáció és a hibrid hadviselés elleni küzdelemben.

A dezinformáció komoly kihívást jelent az európai demokráciák és társadalmak számára, és az Uniónak úgy kell kezelnie azt, hogy közben hű marad az európai értékekhez és biztosítja a szabadságjogokat. A dezinformáció aláássa a polgárok demokráciába és demokratikus intézményekbe vetett bizalmát. A dezinformáció hozzájárul a közvélemény polarizációjához is, és beavatkozik a demokratikus döntéshozatali folyamatokba. A fenyegetések változó jellege, valamint a mesterséges intelligencia és az adatgyűjtési technikák fejlesztésével összefüggő rosszindulatú beavatkozás és online manipuláció növekvő kockázata folyamatos értékelést és megfelelő választ igényel.

Az Európai Unió és a tagállamok által a dezinformáció elleni küzdelem fontosságának hangsúlyozása és a szabad és tisztességes európai választások biztosítására irányuló törekvések a „Szabad és tisztességes európai választásokról szóló csomag”, a „Dezinformáció elleni cselekvési terv” és az "Európai megközelítés: európai megközelítés" című közlemény által

[320] Az Európai Unióról szóló szerződés és az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata - Az Európai Unióról szóló szerződés egységes szerkezetbe foglalt változata - Az Európai Unió működéséről szóló szerződés egységes szerkezetbe foglalt változata - Jegyzőkönyvek - Mellékletek - A 2007. december 13-án aláírt Lisszaboni Szerződést elfogadó kormányközi konferencia zárónyilatkozatához csatolt nyilatkozatok - Megfelelési táblázatok (Hivatalos Lap C 326 , 26/10/2012 o. 0001 – 0390) Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A12012M%2FTXT letöltés dátuma: 2023. 10.18.)

indított intézkedések sorozatán keresztül valósultak meg. Ezek az intézkedések eredményeként jött létre a szabad és tisztességes európai választások biztosításáért felelős munkacsoport (a továbbiakban: GAG+1 munkacsoport), amelynek célja egy külön fórum biztosítása volt a választások integritását érintő kérdések megvitatására és egy átfogó, koherens megközelítés kialakítására.

A GAG+1 munkacsoport fontos szerepet játszott az Általános Ügyek Tanácsának 2019. február 19-i ülésén elfogadott tanácsi és tagállami következtetések előkészítésében.[321] Ezek a következtetések[322] elismerték, hogy a dezinformáció terjedése új kihívásokat jelent, amelyek komoly hatást gyakorolnak a demokratikus folyamatok integritására. A munkacsoport tevékenysége tehát közvetlenül hozzájárult ahhoz, hogy az EU és a tagállamok hatékonyabban tudjanak reagálni a dezinformáció jelentette fenyegetésekre, különös tekintettel a választási folyamatok védelmére.

A dezinformációval kapcsolatos munka rámutatott arra, hogy javítani kell a koordinációt és koherensebb megközelítést kell kidolgozni uniós szinten, többek között a stratégiai kommunikációra, mint a reziliencia megerősítésének transzverzális eszközére való összpontosítás révén. Az uniós kontextusban ezek a transzverzális szabályozási megoldások vagy intézkedések olyanok lehetnek, amelyek több különböző területre vagy szektorra is kiterjednek, és átfogó megközelítést alkalmaznak.[323]

---

[321] Ehhez a dezinformáció elleni cselekvési terv folyamatos és átfogó végrehajtására van szükség. A dezinformáció ágával kapcsolatos munka folytatásával az akkori román elnökség befejezte az uniós tagállamok által a félretájékoztatás elleni cselekvési terv végrehajtása keretében hozott intézkedések feltérképezését. A jelentés elismeri, hogy a dezinformációval kapcsolatos megközelítés nagymértékben eltér az uniós tagállamokban. Ezenkívül az európai választásokra való felkészülés során a csoport a fent említett következtetések nyomán intézkedéseket hozott. A hibrid fenyegetésekkel, a dezinformációval, valamint az állami és társadalmi reziliencia fokozásával kapcsolatos kérdések több munkacsoport és bizottság hatáskörét érintik. 2019 előtt egyetlen munkacsoport sem volt felelős egy koherens és átfogó megközelítés előmozdításáért. Egy horizontális munkacsoport megkönnyítené ezt a koordinációt az EU és tagállamai tudatosságának és rezilienciájának megerősítése, valamint annak biztosítása érdekében, hogy ezeken a területeken ne legyenek átfedések vagy hiányosságok, teljes mértékben figyelembe véve a hibrid fenyegetések sokrétű és változó jellegét.

[322] A reziliencia fokozásával és a hibrid fenyegetésekkel szembeni fellépéssel foglalkozó horizontális munkacsoport 10027/19 számú állásfoglalása (Elérhető: https://data.consilium.europa.eu/doc/document/ST-10027-2019-INIT/en/pdf letöltés dátuma: 2023. 10.18.)

[323] Ezek az intézkedések gyakran multidiszciplináris megközelítést igényelnek, és céljuk, hogy egységes választ adjanak a különféle, egymással összefüggő problémákra. Álláspontom szerint csak így érdemes kialakítani, illetve fejleszteni a megfelelő, proaktív jogi normakörnyezetet a leginkább a kibertérben zajló dezinformációs műveletek elleni küzdelem során.A demokratikus társadalmainkat fenyegető veszélyek, amelyek az elmúlt években markáns külső jellegűek voltak, összetettek, sokfélék, folyamatosan fejlődnek, és az egyes tagállamok nehezen kezelhetők egyedül. Ezért nagy szükség van a tagállamok és az EU intézményeinek összehangolt fellépésére, az eddig azonosított közös alapokra építve.

Az EU rezilienciájának fejlesztése kulcsfontosságú annak érdekében, hogy sikeresen kezelje a jövő kihívásait. A gazdasági stabilitás fenntartása, a politikai és társadalmi kohézió erősítése, a biztonságpolitikai kérdések kezelése, valamint a környezeti fenntarthatóság előmozdítása mind hozzájárulnak az EU ellenálló képességéhez. A folyamatos reformok és az innovatív megoldások alkalmazása révén az EU képes lesz megerősíteni pozícióját, mint globális szereplő, miközben megőrzi saját polgárai biztonságát és jólétét. Összességében elmondható, hogy az EU komoly erőfeszítéseket tesz a reziliencia építésére, bár a folyamat messze nem tekinthető lezártnak. A jövő nagy kérdése, hogy ezek az intézkedések mennyire lesznek sikeresek egy esetleges újabb válság kezelésében.

Rendkívül fontos megjegyezni, hogy az Európai Unió Kibervédelmi Ügynöksége (a továbbiakban: ENISA) és az Európai Külügyi Szolgálat (továbbiakban: EEAS) közös munkaként kiadott egy, az értekezés témája szempontjából kiemelt jelenőségű tárgykörről szóló „Idegen Információ Manipuláció és Beavatkozás és Kiberbiztonság – Fenyegetési Térkép" című jelentést, amely a külföldi információmanipuláció és beavatkozás (Foreign Information Manipulation and Interference, a továbbiakban: FIMI), valamint a dezinformáció területén jelentkező fenyegetési térkép elemzésére irányul. Az elemzés egy sajátos analitikai keretet dolgoz ki, amely összhangban áll az ENISA Fenyegetési Térkép (továbbiakban: ETL) módszertanával, és célja a FIMI és a dezinformáció kibervédelmi aspektusainak vizsgálata. A jelentést az ENISA ad hoc Munkacsoportja a Kibervédelmi Fenyegetési Térképek (CTL) vonatkozásában is validálta és támogatta.[324]

A FIMI fogalma az EEAS által javasolt válaszként szolgál az Európai Demokrácia Cselekvési Terv felhívására, amely a dezinformáció körüli definíciók további finomítását javasolja. Bár a dezinformáció kiemelkedő része a FIMI-nek, a FIMI nagy hangsúlyt fektet a manipulatív magatartásra, szemben a közvetített tartalom valódiságával. Számos stratégiai dokumentum, mint például a Biztonság és Védelem Stratégiai Iránytűje és a 2022 júliusi Tanácsi Következtetések a FIMI-ről, hangsúlyozzák a FIMI, valamint a hibrid és kiberfenyegetések elleni küzdelem fontosságát.

[324] Elérhető: https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape (letöltés: 2023.10.18.)

Ebből kifolyólag, tekintettel a különböző területeken átívelő szélesebb hibrid fenyegetésekre, a jelentés egyik fő motivációja az, hogy összevonja, összehangolt cselekvésre ösztönözze a kibervédelmi és a FIMI elleni szakmai szervezeteket, közösségeket. A cél, hogy hozzájáruljon az információmanipuláció és beavatkozás – beleértve a dezinformációt – természetét és dinamikáját érintő folyamatos és sürgős vitákhoz, valamint ahhoz, hogy hogyan válaszoljunk kollektíven (EU szinten) erre a jelenségre.

A jelentés egy olyan analitikai megközelítést javasol és tesztel, amely leírja a FIMI-t és az információ manipulációját, valamint az alapjául szolgáló kibervédelmi elemeket, ötvözve mindkét terület gyakorlatát, így különösen:

- A kibervédelem terén: Az ENISA éves jelentéseiben használt nyílt metodológiai keretet, az ENISA Fenyegetési Térképhez kapcsolódó jelentéseket.
- A FIMI terén: Az nyílt forráskódú DISARM (DISinformation Analysis & Risk Management) keretrendszert, amely a FIMI-t, illetve a dezinformációt rögzíti.

Szükséges megjegyezni, hogy a DISARM keretrendszer egy olyan eszköz, amelyet a dezinformáció és információs manipuláció elemzésére és megértésére fejlesztettek ki. Két fő részből áll:

- DISARM Red: Ez a rész a dezinformáció és az információs manipuláció létrehozásával és terjesztésével, pontosabban detektálásával foglalkozik, azt segíti elő. A keretrendszer a MITRE ATT&CK® keretrendszerének struktúráját követi, amely egy tudásbázis a kiberbiztonsági fenyegetésekkel kapcsolatos támadói viselkedésről és a támadási életciklus során alkalmazott taktikákról, technikákról és eljárásokról. A DISARM Red célja, hogy segítse a védekező közösséget a FIMI, illetve dezinformációs támadási módszerek leírásában és jobb megértésében, valamint egy közös nyelv kialakításában a komplex jelenség leírásához.
- DISARM Blue: Elsődlegesen a dezinformáció elleni küzdelemben foganatosított intézkedésekkel foglalkozik. A DISARM Blue arra szolgál, hogy segítse a szakembereket a DISARM Red keretrendszerben leírt támadási módszerekkel szembeni válaszlépések megtervezésében, kialakításában és alkalmazásában.

A DISARM keretrendszer előnye, hogy nyílt forrású és közösség által vezérelt, így lehetővé téve a szakértők számára, hogy összeállítsanak és rendszerezzenek minden ismert FIMI támadási módszert. Ezáltal elérhetővé válik a védelmi, biztonsági szférában dolgozó szakemberek számára, hogy lényegében egy közös nyelvet alkalmazva írják le és osztályozzák megállapításaikat és tapasztalataikat. A DISARM egy kulcsfontosságú eszköz a dezinformációs tevékenységek és támadási stratégiák jobb megértéséhez és kezeléséhez. [325]

A keretrendszer korlátozott események csoportján történő tesztelésével a jelentés bizonyítékul szolgál annak bizonyítására is, hogy a keretrendszerek interoperabilitása működőképes. Emellett előzetes következtetéseket is megfogalmaz a dokumentum a kibervédelem és a FIMI, illetve dezinformáció alkalmazása közötti kapcsolatról:

A kibervédelmi elemzés különösen fontos az attribúció megállapításában: az elemzett események közül azok, amelyek attribúciót kaptak, kibervédelmi elemzésen alapultak. Ezenkívül a kibertámadások inkább a FIMI, illetve dezinformációs események kezdeti szakaszában jellemzőek a jelentés alapján. Ez azt jelenti, hogy bizonyos kibertámadás-technikák (előre)jelzésként szolgálhatnak egy várható FIMI, illetve dezinformációs eseményre, és az előrejelzés birtokában a (biztonság)tudatosság folyamatos növelése mellett jó eséllyel korlátozható vagy megakadályozható, hogy sebezhetővé váljon, vagy sérüljön olyan (akár kritikus) infrastruktúra, amely célpontja a támadásnak vagy a támadás eredményeként akaratlanul, lényegében a kibervédelmi incidens áldozataként elősegíti a (káros tartalom) terjesztését.

Kiemelt prioritást kell, hogy élvezzen a strukturált és zökkenőmentes incidensjelentések átadása, közös használata a kibervédelmi és a FIMI, illetve dezinformáció ellen küzdő közösség között. Szükséges biztosítani az adatok konzisztenciáját, vagyis azt, hogy az adatok következetesek, ellentmondásmentesek legyenek és logikailag helyesen illeszkedjenek egymáshoz. Sok esetben ugyanis az adatok nem megfelelő minősége jelenti a kereszterületi szakmai elemzések legfőbb korlátját. Például a nyílt forrású adatok a FIMI-ről, illetve dezinformációs eseményekről gyakran egész komplex műveleteket ölelnek fel, sok incidenssel,

[325] A keretrendszerek működéséről bővebben az alábbi webhelyre feltöltött jelentéseket és publikációkat feltétlenül érdemes megismerni: https://www.enisa.europa.eu/enisa-search#/?SearchableText=DISARM (letöltés: 2023.10.18.) https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape (letöltés: 2023.10.18.)

míg egy „tiszta” kibervédelmi ellenőrzési perspektíva inkább az egyes incidensekre koncentrálna, nem vizsgálná az összképet. Emellett előfordulhat, hogy a FIMI-kről, illetve a dezinformációs eseményekről szóló adatok nem tartalmaznak elegendő információt a kibervédelmi aspektusokról. Mindkét esetben az incidensjelentési gyakorlatok javítása segíthet a jelentésben megfogalmazott gondolatok alapján.

A kibervédelmi és a FIMI, illetve dezinformáció ellen küzdő szakmai közösségek közötti kölcsönös információcsere rendkívül előnyös lehet a FIMI, illetve a dezinformáció elleni küzdelemben. Mivel az incidenskezelés és a válaszlépések megvalósítása évek óta központi feladata a kibervédelmi közösségnek, az ENISA által szervezett kibervédelmi gyakorlatok tapasztalatainak beépítése a napi munkába jelentősen segítheti a FIMI, illetve dezinformáció ellen harcoló közösség elemzői képességének javítását, gyorsíthatja annak fejlesztését. A jelentésben szereplő példa alapján – a készítők álláspontja szerint – gyorsítaná az intézkedéseket, ha FIMI-vel foglalkozó szakemberek átvennék a kibervédelmi szakterületen használt (jelentés)mintákat, fájlformátumokat, így meghaladva a hagyományos átiratokon keresztüli információmegosztást. Szintén példaként említi a jelentés azt a javaslatot, ami szerint a FIMI, illetve a dezinformáció elleni küzdelemért felelős közösség is tájékoztathatná a kibervédelmi szakembereket az új és eddig nem ismert ellenérdekelti szándékokról, célpontokról és fenyegetésekről.

Az ENISA másik kiemelkedő jelentőségű, előző gondolatokhoz szorosan kötődő kutatásáról szóló jelentés[326] a mesterséges intelligencia és a kiberbiztonság területén végzett kutatásokra koncentrál. Az ENISA célja, hogy hozzájáruljon az EU kiberpolitikájához, növelje az ICT termékek, szolgáltatások és folyamatok biztonságát tanúsítási rendszerekkel, együttműködjön az EU tagállamaival és testületeivel, valamint segítsen Európának felkészülni a holnapi kiberkihívásokra.

A kutatás két fő dimenziót vizsgál: a biztonságos és megbízható MI biztosítását és annak rosszindulatú használatának megelőzését („AI-as-a-crime-service” vagy „AI to harm”), valamint az MI alkalmazását a kiberbiztonságban („AI use cases” vagy „AI to protect”). A

[326]PASCU, Corina – BARROS LOURENCO, Marco (szerk.): *Artificial Intelligence and Cybersecurity Research*. ENISA Research and Innovation Brief. European Union Agency for Cybersecurity (ENISA), 2023. június. Szerzők: NTALAMPIRAS, Stavros – MISURACA, Gianluca – ROSSEL, Pierre.

dokumentum célja, hogy azonosítsa a kutatási igényeket az MI kiberbiztonságban való alkalmazása és az MI biztosítása terén, az ENISA felhatalmazása alapján.

Az összefoglalóban kiemelik, hogy az MI egy tipikus kettős használatú technológia, ahol a rosszindulatú szereplők és az innovátorok folyamatosan versenyeznek egymással. Az MI segítségével a rosszindulatú szereplők új képességeket vezethetnek be, amelyek automatizálttá és nehezen észlelhetővé teszik a kibertámadásokat. [327]

9. A hibrid fenyegetések és a dezinformáció elleni küzdelem a NATO stratégiai döntéshozatali szintjein, a reziliencia jelentősége

A hibrid fenyegetések[328] és a dezinformáció elleni küzdelem a NATO számára kiemelt jelentőségű kérdés. A hibrid fenyegetések sokrétű támadásokat jelentenek, amelyek katonai és nem katonai eszközök kombinációját használják, beleértve a kibertámadásokat, az információs hadviselést és a politikai befolyásolást. A dezinformáció, mint a hibrid hadviselés egyik eszköze, különösen veszélyes, mivel célja a társadalmak megosztása, az államok belső feszültségeinek fokozása és a demokratikus intézmények aláásása. [329]

[327] A kutatás során számos MI alkalmazási esetet vizsgáltak a kiberbiztonság terén, de ezek teljes listázása a dokumentum hatókörén túlmutat, mivel a kutatás ezen a területen folyamatosan fejlődik. Azonban bemutatnak néhány példát ezekre az alkalmazási esetekre a jelentésben, hogy jobban megértsék a folyamatban lévő kutatási erőfeszítéseket és azokat a területeket, ahol további kutatásra van szükség. Az ENISA öt kulcsfontosságú kutatási igényt azonosított, amelyeket megosztanak és megvitatnak az érdekelt felekkel, mint javaslatokat jövőbeli politikai és finanszírozási kezdeményezésekre az EU és tagállamok szintjén. A dokumentum hangsúlyozza, hogy bár felismerik az MI-ben rejlő hatalmas potenciált a kiberbiztonság innovációjában és számos követelményt, amelyek szükségesek annak biztonságának javításához, még sok munka áll előttünk, hogy teljesen feltárjuk és leírjuk ezeket a követelményeket.

[328] A NATO hibrid hadviselésre adott elmúlt évekbeli válaszairól bővebben lásd: LASCONJARIAS, Guillaume – LARSEN, Jeffrey A. (szerk.): *NATO's Response to Hybrid Threats*. Rome: NATO Defense College, 2015. (Forum Paper 24.) Elérhető: https://www.files.ethz.ch/isn/195405/fp_24.pdf (letöltve: 2023. 10. 18.)

[329] BILAL, Arsalan: Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. *NATO Review*, 2021. november 30. Elérhető: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/ (letöltve: 2023. 10. 18.) A „Hibrid Háború – Új Fenyegetések, Bonyolultság, és a „Bizalom, mint Ellenszer" című cikk Arsalan Bilal tollából származik, és 2021. november 30-án jelent meg. A cikk azzal érvel, hogy a nemzetközi biztonság és a konfliktusok természete ugyanaz maradt, de a konfliktusokat ma már új, innovatív és radikálisan eltérő módon vívják. A hibrid hadviselés kevésbé a halálos vagy kinetikus erőről szól. A hibrid hadviselés egy összetett fogalom, amely a konvencionális és nem konvencionális hatalmi eszközök keverékét jelenti, célja az ellenség gyengeségeinek kiaknázása és a bizalom rombolása. A cikk hangsúlyozza a bizalomépítés fontosságát a hibrid fenyegetésekkel szemben. Elérhető: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/ (letöltés dátuma: 2023.10.18.)

A NATO válasza a hibrid fenyegetésekre és a dezinformációra többdimenziós.[330] Stratégiájának középpontjában az államok közötti információcsere, a kollektív védelem megerősítése, valamint a kiber- és információs hadviselési képességek fejlesztése áll. A szervezet kiemelt figyelmet fordít a tagállamok kritikus infrastruktúráinak védelmére, valamint azoknak a képességeknek a fejlesztésére, amelyekkel hatékonyan tudja azonosítani és semlegesíteni a hibrid támadásokat.[331]

A NATO-nak ezenkívül fontos szerepe van a dezinformációval szembeni küzdelemben is. Erre példa az ún. Stratégiai Kommunikációs Központ (StratCom), amelynek feladata a dezinformációval kapcsolatos trendek elemzése, valamint ellenstratégiák kidolgozása és végrehajtása. A NATO továbbá erőfeszítéseket tesz annak érdekében, hogy javítsa a lakosság ellenálló képességét a hamis információkkal szemben, többek között oktatási programok és a médiatudatosság növelésének támogatása révén.

A tagállamok közötti szoros együttműködés és koordináció elengedhetetlen a hibrid fenyegetésekkel és dezinformációval szembeni hatékony fellépéshez. Az együttműködés magában foglalja az információ- és titkosszolgálati adatok megosztását, valamint közös gyakorlatok és képzések lebonyolítását. A cél az, hogy a NATO, mint szövetség egységesen tudjon reagálni, és erősítse tagjainak képességét arra, hogy felismerjék és megvédjék magukat az ilyen jellegű fenyegetésekkel szemben.

A NATO hibrid hadviselési stratégiája egy olyan katonai megközelítést jelent, amely egyesíti a hagyományos katonai erőt a nem hagyományos eszközökkel, mint például a kibertámadások, a dezinformációs kampányok és az állam által támogatott terrorizmus. Ennek a megközelítésnek célja, hogy összetett és sokrétű fenyegetésekkel szembeni védelmet

---

[330] Countering hybrid threats c. NATO közlemény alapján, Elérhető: https://www.nato.int/cps/en/natohq/topics_156338.htm (letöltés dátuma: 2023.10.18.)

[331] KIS-BENEDEK József: A NATO mai politikai és katonai kihívásai, In: Szenes, Zoltán (szerk.) A mai NATO: A szövetség helyzete és feladatai, Budapest, Magyarország : HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft. (2021) 267 p. pp. 12-27., 16 p. Kis-Benedek József írásában áttekinti a NATO előtt álló főbb politikai és katonai kihívásokat. Rávilágít arra, hogy a nemzetközi biztonsági környezet Instabilitása, az Oroszország és Kína által jelentett fenyegetések, valamint a terrorizmus és a migráció kérdése komoly próbatétel elé állítják a NATO-t. Kiemeli, hogy az Észak-atlanti Szövetségnek egyszerre kell megőriznie katonai erejét és elrettentő képességét, miközben politikai eszközökkel is kezelnie kell ezeket a problémákat. A szerző szerint a NATO jövőbeli sikere szempontjából kulcsfontosságú az Egyesült Államok elköteleződése, az európai tagállamok nagyobb védelmi kiadásokra való ösztönzése, valamint az új fenyegetések, például a kibertámadások és a hibrid hadviselés elleni fellépés fokozása. Úgy véli, a NATO továbbra is létfontosságú szerepet tölt be a nyugati világ biztonságának garantálásában, de ehhez átfogó stratégiai alkalmazkodásra van szükség a megváltozott viszonyok közepette.

nyújtson. A NATO válasza a hibrid fenyegetésekre magában foglalja a kollektív védelem megerősítését, az információmegosztás javítását, a tagállamok közötti együttműködés növelését, valamint a civil és katonai képességek integrációját. A szövetség aktívan dolgozik azon, hogy felkészüljön és reagáljon a hibrid hadviselési módszerekre, beleértve a kiberbiztonsági védekezést és a stratégiai kommunikációt is.[332]

10. A hibrid fenyegetésekkel szembeni reziliencia megjelenése a NATO stratégiai normaalkotó tevékenysége során

A NATO működésében a reziliencia egy fontos tényező, amely kulcsfontosságú a szervezet hatékonyságában és alkalmazkodóképességében.[333] A reziliencia azon képességét jelenti, hogy egy szervezet képes ellenállni, alkalmazkodni és gyorsan alkalmazkodni a változó körülményekhez, beleértve a kiberfenyegetéseket, a terrorizmust, a természeti katasztrófákat és más biztonsági kihívásokat. A szövetség tagországaiban fokozza a katonai és civil kapacitások rugalmasságát.[334] Ennek érdekében a NATO támogatja a tagállamokat abban, hogy képesek legyenek gyorsan alkalmazkodni a változó körülményekhez és fenyegetésekhez. Ez magában foglalja a katonai képességek fejlesztését, az energiaellátási biztonság növelését, valamint a kritikus infrastruktúra elleni védelem erősítését.[335]

A NATO számára kiemelt fontosságú a hibrid fenyegetések, köztük az orosz és kínai hibrid hadviselés elleni felkészülés és védekezés.[336] Ennek érdekében a NATO átfogó stratégiát dolgozott ki, amely magában foglalja a folyamatos hírszerzést és elemzést, a tagállamok támogatását a sebezhetőségek azonosításában és a reziliencia javításában, valamint az

---

[332] A NATO 2014-es walesi csúcstalálkozóján a tagállamok elismerték a hibrid fenyegetések növekvő jelentőségét és úgy döntöttek, hogy fejlesztik képességeiket ezek kezelésére. Azóta a szervezet folyamatosan dolgozik azon, hogy jobban felkészüljön és adaptálódjon a változó biztonsági környezethez. A hibrid hadviselés kihívásainak kezelésére a NATO létrehozott egy különleges egységet, amelynek feladata a hibrid fenyegetések elemzése és ellensúlyozásának módszereinek kidolgozása. Emellett a tagállamok is erősítik saját nemzeti képességeiket és részt vesznek közös gyakorlatokban, hogy jobban felkészüljenek a hibrid támadásokra. A hibrid hadviselés folyamatosan fejlődik, és a NATO-nak naprakésznek kell lennie, hogy hatékonyan tudjon reagálni az új típusú fenyegetésekre. A szervezet elkötelezetten dolgozik azon, hogy megőrizze tagállamai biztonságát és stabilizálja a nemzetközi biztonsági környezetet, a nemzetközi szervezet ezirányú adaptív és proaktív tevékenységét az egyes doktrínák, iránymutatások, szakmai konferenciákon előadottak demonstrálják.

[333] MOLNÁR Ferenc: Kitekintés – a nemzeti ellenálló képesség, a NATO és az Európai Unió viszonylatában. In: KÁDÁR Pál (szerk.): *A védelmi és biztonsági szabályozás magyarországi reformja*. Budapest: Nemzeti Közszolgálati Egyetem Védelmi-Biztonsági Szabályozási és Kormányzástani Kutatóműhely, 2023, 290–303. o. ISBN 978-963-498-595-2

[334] NATO Allied Command Transformation (ACT): Cognitive Warfare: Strengthening and Defending the Mind. 2023. július 3.

[335] NATO: Resilience, civil preparedness and Article 3. [NATO tematikus oldal, online.]

[336] NATO HQ Countering hybrid threats c. közleménye

elrettentést és szükség esetén a gyors katonai reagálást. A NATO számára prioritást élvez a különféle hibrid támadásoknak felderítése és semlegesítése, amelyek a tapasztalatok alapján állami vagy nem állami szereplők részéről egyaránt érkeznek. Ezek a hibrid fenyegetések az utóbbi időszakban mind intenzitásban, mind méretben, mind gyakoriságban számottevő növekedést mutatnak.

A kibertér egyre fontosabb szerepet játszik a modern hadviselésben, és a NATO folyamatosan alkalmazkodik a kibertámadások növekvő fenyegetéséhez. A NATO stratégiai dokumentumait vizsgálva ismerhető fel a kibertérműveleti képesség szerepének, jelentőségének és fókuszának evolúciója:[337]

- 2010-es stratégiai koncepció: A kibertér szerepét először a NATO 2010-es stratégiai koncepciójában ismerték el, amely elismerte a kibertámadások potenciális hatását a szövetség biztonságára. A kibertérműveleti képességet a NATO biztonságának fenntartásához szükséges eszközként ismerték el. A kibertérműveleti képesség fókusza a védekezésen volt, a kibertámadások elhárítására és a kritikus infrastruktúra védelmére.
- 2016-os Varsói csúcstalálkozó: A NATO elkötelezte magát a kibertérműveleti képesség fejlesztése mellett, és létrehozta a Kibervédelmi Kiválósági Központot (CCDCOE). A NATO elismerte a kibertérműveleti képesség fontosságát a szövetség elrettentő és védelmi képességeinek javításában. a NATO a kibertérműveleti képesség fókuszát a védekezésről az elrettentésre és a válaszadásra helyezte át.
- 2022-es stratégiai koncepció: A koncepció a kibertámadásokat a NATO legfontosabb kihívásai közé sorolta, és hangsúlyozta a kibertérműveleti képesség fejlesztésének szükségességét. A 2022-es stratégiai koncepció a kibertérműveleti képességet a NATO biztonságának és stabilitásának biztosításához elengedhetetlennek nevezte. A koncepció a kibertérműveleti képesség fókuszát a teljes körű elrettentésre és védelemre helyezte át, beleértve a kibertámadások megelőzését, elhárítását és válaszadását.

A NATO stratégiai dokumentumai tükrözik a kibertérműveleti képesség szerepének, jelentőségének és fókuszának folyamatos evolúcióját. A NATO elismerte a kibertámadások

[337] KASSAI Károly: A kibertérműveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből, Budapest, Magyarország : Gondolat Kiadó (2023) 327 p. pp. 195-232. , 38 p.

növekvő fenyegetését, és elkötelezte magát a kibertérműveleti képesség fejlesztése mellett, hogy elrettentse, megvédje és válaszoljon a kibertámadásokra. A kibertérműveleti képesség továbbra is kulcsfontosságú lesz a NATO biztonságának és stabilitásának biztosításában a jövőben.

A kibertér, mint jogilag definiálható (harc)terület[338] meghatározása és ezen keresztül az állami önvédelemre, szövetségesi rendszerben megvalósítható kollektív védelemre vonatkozó jogosultság meglétének vizsgálata különösen nehéz. A nemzetközi jogi keretek nem teljes körűen, nem minden releváns részletre kiterjedően szabályozzák a kibertérből érkező támadásokat. Az erőszak tilalma és az önvédelem joga azonban alkalmazható bizonyos esetekben. A kibertérben való fegyveres támadás fogalmának tisztázására és a nemzetközi jogi keretek továbbfejlesztésére van szükség.

Az Orosz Föderáció például különösen ismert az általa alkalmazott összetett hibrid stratégiáról, amely a politikai beavatkozástól kezdve az agresszív kiberaktivitáson át a gazdasági nyomásgyakorlásig, a befolyásoláson keresztül egészen a közvetlen katonai agresszióig és a területi annektálásig terjed. Ez a többboldalú megközelítés azzal a kifejezett szakmai céllal történik, hogy politikai érdekeket szolgáljon, miközben aláássa a nemzetközi jogi normákon alapuló rendet.

A NATO szakértői szerint Kínai Népköztársaság is hibrid és kiberműveleteket alkalmaz, amelyeket konfrontatív retorika és dezinformációs kampányok egészítenek ki.[339] Céljuk a NATO szövetségesek megcélzása, hogy befolyást szerezzenek a kulcsfontosságú technológiai

[338] SPITZER Jenő: A kibertérből érkező támadások lehetséges nemzetközi jogi értelmezései, különös tekintettel az önvédelemhez való jogra, Katonai Jogi és Hadijogi Szemle, 2023/2. pp 6-29. (2023) Spitzer jenő tanulmányában kiemeli, hogy a nemzetközi jogi keretek változnak a nem állami szereplők térnyerése, a terrorizmus, a magánbiztonsági vállalatok és a kibertér jelentőségének növekedése miatt. A kiberműveletek három csoportba sorolhatók: információ- és adatszerzés, információs rendszer megzavarása, információs rendszer módosítása, rombolása vagy megsemmisítése. A nemzetközi jog tárgyi hatálya kiterjed a kiberműveletekre, de nincs kifejezett szabályozás. Az analógia alapján a nukleáris fegyverekhez hasonlóan a kiberműveletek is jogellenesek lehetnek, ha ellentétesek az ENSZ Alapokmányának erőszak tilalmával vagy a nemzetközi humanitárius joggal. Az ENSZ Alapokmánya 2. cikk (4) bekezdése tiltja az erőszak alkalmazását vagy azzal való fenyegetést. Ez a tilalom kizárólag államokra vonatkozik, és nem terjed ki nem állami szereplőkre. A kibertámadások nem felelnek meg az erőszak fogalmának, ezért nem esnek az Alapokmány erőszak tilalma alá. Az önvédelemhez való jog azonban alkalmazható a kibertámadásokra, ha azok fegyveres támadásnak minősülnek. A kiberinformációszerzés ugyanakkor nem minősül fegyveres támadásnak, ezért nem alkalmazható rá az önvédelem joga. A kibervédelem így csak akkor jogszerű, ha az fegyveres támadás elhárítására irányul.

[339] NATO: Symposium in Finland brings industry and experts together to strengthen NATO's responses to hybrid threats. *NATO News*, 2023. december 15.

szektorok, a kritikus infrastruktúra és a stratégiai nyersanyagok felett, ezáltal stratégiai függőségeket létrehozva és befolyásukat növelve. Ez különösen igaz az afrikai műveleteikre.[340]

A NATO egy átfogó stratégiát dolgozott ki a hibrid fenyegetésekkel szembeni felkészülésre, az azokat alkalmazók elrettentésére és konkrét védekezésre. A szervezet 2015 óta különös hangsúlyt fektet a hibrid támadásokkal szembeni felkészülésre, beleértve a folyamatos hírszerzést és elemzést, amelyek a hibrid tevékenységek azonosítására és jellemzésére irányulnak. A NATO Közös Hírszerzési és Biztonsági Divíziója kiemelt szerepet tölt be ezeknek a fenyegetéseknek az értelmezésében és elemzésében.

A NATO erősíti a felkészülést azzal, hogy segítséget nyújt a tagállamoknak a sebezhetőségek azonosításában és a reziliencia növelésében, támogatást nyújtva többek között a polgári felkészülés, a CBRN helyzetekre adott válasz[341], a kritikus infrastruktúra védelme, a stratégiai kommunikáció, a kiber védelem, az energetikai biztonság és a terrorizmus elleni küzdelem területein. A képzés és oktatás, valamint a katonai és nem katonai válaszok közös gyakorlása is fontos eleme a NATO stratégiájának.

A NATO elrettentési stratégiája az azonnali és célzott cselekvést jelenti, az erők készenlétét és felkészültségét növelve, valamint erősítve a döntéshozatali folyamatokat. Ha az elrettentés nem válik be, a NATO készen áll arra, hogy megvédje bármelyik szövetségest bármilyen fenyegetéssel szemben, hangsúlyozva a gyors és rugalmas katonai válaszok szükségességét.[342]

---

[340] A NATO főtitkárának beszéde a vilniusi csúcs után. Elérhető: https://www.nato.int/cps/en/natohq/opinions_217104.htm?selectedLocale=en (letöltés: 2023. 12.16.)

[341] A NATO CBRN (kémiai, biológiai, radiológiai és nukleáris) stratégiája magában foglalja a megelőzést, felkészülést és válaszadást a CBRN fenyegetések és támadások ellen. A stratégia célja, hogy védelmet nyújtson a szövetségeseknek, valamint hogy csökkentse és minimalizálja a CBRN eseményekből eredő károkat. A NATO CBRN védelmi képességeinek fejlesztése kulcsfontosságú része a kollektív védelemnek.

[342] Témával összefüggésben lásd: NATO: 2022 Madrid Summit Declaration. 2022. június 29. Elérhető: https://www.nato.int/cps/en/natohq/official_texts_196951.htm, NATO: 2023 Vilnius Summit Communiqué. 2023. július 11. Elérhető: https://www.nato.int/cps/en/natohq/official_texts_217320.htm, valamint GENINI, Davide: Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. Journal of Strategic Studies, 2025. DOI: 10.1177/2336825X251322719

11. Jogi sérülékenységvizsgálat a hibrid hadviselés elleni küzdelemben

A biztonsági szektorban észlelhető jogi korlátozások elemzése során kiderül, hogy az alapjogok érvényesülésének vizsgálata lehetővé teszi az úgynevezett jogi sérülékenységvizsgálat elvégzését. Ez a folyamat, amely a különleges jogrend alatt hozott jogszabályok kapcsán vált ismertté és gyakorivá a médiában, lehetőséget adott a civil szervezeteknek arra, hogy átvilágítsák és feltárják a jogszabályok hiányosságait. A jogi sérülékenységvizsgálat egyfajta előkészülete lehet a későbbi célzott támadásoknak, vagyis a lawfare – azaz a jogi eszközökkel folytatott háborúskodás – alkalmazásának.

A lawfare egy olyan hibrid hadviselési forma, amely láthatatlan fegyverként funkcionál, és egyre nagyobb szerepet kap a nemzetközi kapcsolatokban. A hadviselő felek modern technológiákat és eszközrendszereket használva kiterjesztik tevékenységüket a kibertérre, médiára, gazdaságra és társadalmi érintkezésekre is, céljuk a befolyásolás, zavarkeltés és belső rend megbontása.

Magyarországon a hibrid fenyegetésekkel szembeni fellépés és kezelés kiemelt feladatnak számít, ami meg is jelenik a hatályos NBS-ben. Ugyanakkor a lawfare fogalmának jelentése és a potenciális veszélyforrás tulajdonságai még új területek a jogalkotók és szakmai szervezetek számára, ami azt jelenti, hogy még csak most ismerkednek ezekkel a jelenségekkel és kezdik felmérni azok lehetséges hatásait és kockázatait.

A hadviselő fél[343] az összehangolt tevékenységsorozat közben a modern technológiák és eszközrendszerek által nyújtott képességeket, opciókat használja fel, és műveleteit kiterjeszti a kibertérre, a média világára, a gazdaságra és a társadalmi érintkezés különböző formáira is. Az egyes elemek (támadási formák) önálló vagy egymást kiegészítő (kombinatív) alkalmazása – a klasszikus támadási formák bevetése nélkül is – már alkalmas lehet a befolyásolásra, a zavarkeltésre, egyes államok belső rendjének a megbontására, társadalmi tudat újraformálására. Az új típusú fenyegetettség fokozott szintjére tekintettel Magyarország kiemelt feladatként tekint a hibrid fenyegetések elleni fellépésre, illetve azok kezelésére.

[343] Az ilyen, a hibrid hadviselés eszköztárába tartozó intézkedések mögött nem feltétlenül kell egy adott államot és annak hírszerző szolgálatát keresni, ugyanis egy terrorszervezet, egy nem állami szervezet vagy a gazdasági élet befolyásos szereplői is képesek azokat végrehajtani, alkalmazni.

A jogi sérülékenységvizsgálat elvégzésének egyik jellemző példáját találjuk Emily Harding cikkében[344] foglalkozik azzal a kockázattal, amelyek a Külföldi Hírszerzési Megfigyelési Törvény (Foreign Intelligence Surveillance Act) 702. szakasza időbeli hatályának esetleges lejártával járna.[345]

Harding előre vetíti, hogy ha a törvény időbeli hatálya (újbóli meghosszabbítás hiányában) lejár, az amerikai hírszerzési szervek információszerző képessége jelentősen korlátozódhat, ami különösen kritikus lehet az idegen kémhálózatok felderítésének lehetőségeit illetően. Példaként hozza fel egy kínai kémhálózat feltárását Ohio államban öt év múlva, ami jelentős anyagi veszteséget okozna egy amerikai űripari vállalatnak és más magas technológiájú gyártóknak.

Harding szerint a törvény időbeli hatályának meghosszabbítása érdekében a Kongresszusnak sürgősen cselekednie kell. Kiemeli, hogy a törvény meghosszabbítása nélkül az Egyesült Államok kormánya elveszítené a lehetőséget, hogy megakadályozza Peking, Moszkva, a Hamász és az Iszlám Állam tevékenységeit.

12. Jogállami garanciák fontosságáról a hibrid fenyegetések kezelése során

A hibrid hadviselési fenyegetésekre adott állami válaszoknak komoly kihívást jelent, hogy miként maradjanak a demokratikus jogállam keretein belül. A szükségesség és arányosság elveinek megsértése a jogállami működés fokozatos leépüléséhez vezethet, ami végső soron a támadó fél stratégiai céljait szolgálhatja. Ahogy David Kennedy rámutat[346], a jog fegyverként való alkalmazása nem pusztán a támadó eszköztárát bővíti, hanem a védekező államokat is

[344] HARDING, E. (2023): Lawmakers Will Need to Own the Consequences of Letting Section 702 Lapse. [Commentary] Center for Strategic and International Studies (CSIS), Washington (D.C.), 2023. december 11.
[345] A 702. szakasz 2008-ban, a globális terrorizmus elleni háború csúcspontján jött létre. Lehetővé teszi a Nemzeti Biztonsági Ügynökség (NSA), a Központi Hírszerzési Ügynökség (CIA), a Szövetségi Nyomozó Iroda (FBI) és a Nemzeti Terrorizmusellenes Központ számára, hogy külföldön tartózkodó külföldi állampolgárok közötti kommunikációról információgyűjtést folytassanak. Bár eredetileg a terrorista cselekmények felderítésére szolgált, az utóbbi években segítette az amerikai hírszerzési közösséget nemzetközi bűnözői csoportok, orosz kibertámadások, kínai kémkedés és fentanil csempészés elleni küzdelemben. A fentanil egy rendkívül erős szintetikus opioid fájdalomcsillapító, amely akár 50-100-szor erősebb a morfiumnál. Elsődlegesen a súlyos fájdalmak kezelésére használják orvosi környezetben, például műtétek során vagy rákos betegek fájdalomcsillapítására. Sajnos azonban az illegális drogpiacokon is megjelent, ahol gyakran más drogokkal keverik, ezzel növelve a túladagolás és halálesetek kockázatát. A fentanil rendkívüli potenciája miatt a közegészségügyi és bűnügyi szakemberek számára jelentős aggodalomra ad okot, különösen az opioid-válság kontextusában.
[346] KENNEDY, David: Lawfare and Warfare. In: CRAWFORD, James – KOSKENNIEMI, Martti (szerk.): The Cambridge Companion to International Law. Cambridge: Cambridge University Press, 2012, 158–183. o.

olyan helyzetbe kényszeríti, ahol a jogállami garanciák megtartása önmagában stratégiai kihívássá válik.

13. Összegzés, az elvégzett vizsgálat és részkövetkeztetések

A fejezetben a magyar biztonságpolitikai stratégiai dokumentumok rendszerének alapos vizsgálatát végeztem el, különös figyelmet fordítva a rendszerváltozást követő időszakban bekövetkezett változásokra és a jövőbeni kihívásokra, az 1. számú hipotézis alátámasztása érdekében.

A kutatás során tudatosan szűkítettem a vizsgálat tárgykörét: nem elemeztem részletesen a stratégiai dokumentumok belső szerkezetét és tartalmát, hanem inkább a jogszabályi környezetbe való beillesztésükre és helyzetükre koncentráltam. Az elemzés alapját azon jelentős előzetes vizsgálati eredmények képezték, amelyeket az elmúlt években a magyar és a nemzetközi tudományos közösség végezett, és amelyek hozzájárultak a nemzeti szintű stratégiai dokumentumok megértéséhez és a magyarországi stratégiai gondolkodás fejlődéséhez. Ezek az előzetes eredmények bár hasznosak voltak, néhány esetben szükségesnek tartottam objektív és konstruktív kritikával kiegészíteni őket. A „stratégia” fogalmát széles körben értelmezem, beleértve a stratégiai tervezést és a stratégiai dokumentumokat. Elismerem a fogalom hadviseléshez köthető gyökereit, de kiemelem annak bővülését a nemzetközi színtérre és a hadtudományon túli alkalmazását. Ismertetem a stratégiaalkotás jogszabályi szabályozását Magyarországon, beleértve a kormányzati stratégiai irányításról szóló rendeletet. Kiemelem a stratégiák előkészítésére, végrehajtására és értékelésére vonatkozó követelményeket. Röviden jelenítem meg a stratégiaalkotás módszertanát, beleértve a külső környezet feltárására és a tendenciák feltérképezésére használt elemzési technikákat (pl. SWOT-analízis, PESTEL-analízis). Tárgyalom a stratégiai gondolkodás és a stratégiaalkotás jövőbeli kihívásait, beleértve a korlátozott információk meglétét és a nemzetbiztonsági ágazat sajátosságait. Átfogó áttekintést nyújtok a biztonságpolitikai stratégiai dokumentumok rendszeréről Magyarországon. Tudományos alapossággal elemzem a rendszerváltozás utáni változásokat, a jogszabályi környezetet és a jövőbeli kihívásokat.

A fejezetben szereplő megállapítások összegzéseként fontosnak tartom megjegyezni, hogy a hibrid fenyegetések az állam működéséhez nélkülözhetetlen funkciókat támadják a célponttá kijelölt országban. Az egyre mélyrehatóbb és kiterjedtebb műveletek körülményeinek

vizsgálata úgy látszik célravezetőnek, ha ezeket a stratégiai szinten szabályozott, nemzetközi kooperációban és a jogalkotásban egyaránt meglévő, illetve kialakítható lehetőségekre figyelemmel végezzük el. A stratégia(ki)alakítási feladatok végrehajtása során érdemes élni azzal a feltételezéssel, hogy a kihívások folyamatos változásban vannak és ezért a statikus, reaktív jogalkotási megközelítés önállóan nem kellően hatékony. Ez hatványozottan igaz a stratégiai szintű normák és a normákban megjelenített stratégiák alkotásakor, melyek elengedhetetlenül megkövetelik a proaktív szakmai és jogi szemléletmódot.

A „Környezeti jövőkutatás: Magyarország 2050" című tanulmány szerzői megfogalmazták, hogy *„szükség van arra, hogy a jövővel való szisztematikus foglalkozás rendszeres tevékenységgé váljon a hazai szakmai közösség berkeiben is a nemzetközi gyakorlathoz hasonlóan, a tudományterületek közti együttműködést is elősegítve".* [347] A fejezet is ehhez, az előremutató gondolkodáshoz kíván hozzájárulni, hiszen a jövőkutatás szempontrendszerét is figyelembe véve, a proaktív jelzővel illethető jogalkotási, illetve stratégiakészítési minőség eléréséhez folyamatosan kémlelnünk kell a horizontot és kellően rugalmas, általános szabályok megalkotásával a jogi sérülékenységvizsgálat próbáját is kiálló jogszabályokat és más jogi normákat, ideértve a stratégiákat is szükséges előkészítenünk annak érdekében, hogy ne váljunk a lawfare vagyis a hibrid hadviselés kifinomult eszközének a passzív alanyaivá.

A fejezetben kifejtem, hogy jogi sérülékenységvizsgálat fontos eszköz a nemzetbiztonság fókuszú jogalkotás szempontjából, különösen az alábbiakkal összefüggésben:

- Az alapjogok érvényesülésének felülvizsgálata,
- A „lawfare" (jogi eszközökkel folytatott hadviselés) alkalmazásának előkészítése, és
- A hibrid fenyegetések hatékony kezelésének biztosítása.

Az előbbiekben részletezett kihívásoknak történő megfelelés lehetőségét, illetve módozatait igyekeztem felkutatni és megjeleníteni a következő fejezetben.

[347] HIDEG É. – MIHÓK B. – GÁSPÁR J. – SCHMIDT P. – MÁRTON A. – BÁLDI A. (2018): Környezeti jövőkutatás: Magyarország 2050. *Magyar Tudomány*, Vol. 179, No. 5, 726–727.o.

VII. A LAWFARE ALKALMAZÁSÁNAK LEHETŐSÉGEI AZ ÚJ TÍPUSÚ BIZTONSÁGI KIHÍVÁSOK JELENTETTE VESZÉLYEKKEL SZEMBEN 2012 ÉS 2023 KÖZÖTT

1. A jogi normákban megjelenített konkrét válaszok vizsgálatának szempontjai

A fejezet[348] megírásának célja, hogy a jogalkotás kiemelkedő jelentőségű mérföldköveinek vizsgálata útján keressen válaszokat arra a kérdésre, hogy az elmúlt évtizedben a titkos információgyűjtés és annak műveleti támogatásához kapcsolódó – kiemelten a katonai nemzetbiztonsági szakterületre jellemző – tevékenységi körben alkalmazott jogintézmények milyen módon képesek megfelelni az új típusú biztonsági kihívások jelentette veszélyek elhárításához, megelőzéséhez fűződő nemzetbiztonsági érdek Kormányzat által megfogalmazott célkitűzéseinek? Különös tekintettel arra, hogy a nemzetbiztonsági szolgálatokra jellemző jogintézmények rendszere vonatkozásában megállapítható, hogy a reaktivitás aránya – természetéből adódóan – magas a proaktivitáséhoz képest. Ezt a vizsgálatot a reaktív és proaktív jogalkotás jellemzőinek a nemzetbiztonsági ágazat feladatrendszerére gyakorolt hatásán keresztül hajtom végre, gyakorlatban megvalósult eseteket alapul véve.

A nemzetbiztonsági ágazatra vonatkozó szabályrendszer folyamatos felülvizsgálatának két fő eszköze a jogi normák hatásának, eredményeinek utólagos vizsgálata, valamint a tartalmi deregulációja, módosítása. Az ágazat fontosságának megfelelő szintű normaalkotási követelményekhez hűen ezeket nemcsak a megalkotásuk előtt kell indokoltság, szükségesség és a várható hatások szempontjából megvizsgálni, hanem a szabályozás korszerűsítése érdekében szükség van az egyes jogszabályok és az ágazatra vonatkozó komplett normakörnyezet folyamatos, illetve célzott felülvizsgálatára, így például az utólagos hatásvizsgálat keretében a jogszabály tényleges hatásainak a szabályozás megalkotása, illetve módosítása idején várt hatásokkal, az esetleges jogkorlátozások arányosságával való összevetésére. A tartalmi felülvizsgálati kötelezettség az előbbi mellett, elsősorban jogi-kodifikációs szempontok alapján szolgálja a normavilágosság, a jogrendszer átláthatósága és a jogbiztonság szempontjait.

[348] A fejezet egyes elemei megjelentek 2021-ben, HÓDOS László: A nemzetbiztonsági szolgálatok közelmúltbeli tevékenységét befolyásoló mérföldkövek, avagy az új típusú biztonsági kihívások jelentette veszélyek és az azokra adott kormányzati, illetve jogalkotói válaszok 2010 és 2020 között. című publikációban In.: *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata*, XIX. évf. 2021/1. sz., 134–149. o

A nemzetbiztonsági szolgálatok által alkalmazott erők, eszközök és módszerek együttes hatásmechanizmusának normarendszere a jogforrási hierarchia legfelsőbb szintjétől a legalacsonyabbig terjedő nagyon széles spektrumot ölel fel. Ezek a magyar nemzet biztonságának védelme érdekében – döntően titokban, néha nyíltan – kerülnek alkalmazásra a szolgálatok munkatársai által. A jogi normákban megjelenő feladatok végrehajtása legtöbbször alapjog-korlátozással jár együtt, emiatt ezeket az állami monopóliumként kodifikált tevékenységeket szigorú előírások között gyakorolhatják az erre feljogosított szervezetek.

A vizsgált időszak jelentős mérföldköveinek meghatározása a szolgálatok normákban meghatározott feladatrendszere, szervezeti felépítése, továbbá ezek jogalkotó általi módosításainak, finomhangolásainak vizsgálata útján azért célravezető, mivel leginkább ezeket tekinthetjük a veszélyekre, kihívásokra adott reakciónak, a kormányzati elvárások megtestesülésének.

2. Gondolatok jogalkotói tevékenység proaktív és reaktív jellemzőiről

A jogalkotás alapvetően reaktív jellegű, amikor az új jogszabályok és rendeletek inkább a társadalmi problémák vagy váratlan események következményei, mintsem előzetes terv vagy stratégia részeként jönnek létre. A fejezetben meghatározott egyik kiemelt célom az, hogy feltárjam a jogalkotás reaktív és proaktív jellemzőit, azok előnyeit és korlátait, valamint az ezen alapuló jogrendszerek hatékonyságát és alkalmazkodóképességét.

A reaktív jogalkotás gyakran a váratlan eseményekre, válságokra vagy társadalmi problémákra adott sürgős reakcióként jön létre. Az ilyen típusú jogalkotásra jellemző, hogy azonnali megoldásokat keres a kialakult helyzetre, ami gyakran magas nyomással és időszűkében történik. Példaként említem a terrorista támadások utáni biztonsági intézkedéseket, egészségügyi válságokra adott reakciókat vagy a gazdasági összeomlás utáni mentőcsomagokat.

A reaktív jogalkotás alkalmazása esetén fontos a kockázatértékelés és a szükségletek kielégítése. A jogalkotóknak meg kell érteniük a probléma valóságos természetét és annak hosszú távú következményeit. Emellett a jogi kereteknek és az intézkedéseknek összhangban kell lenniük az alkotmányos elvekkel és az állampolgárok jogainak tiszteletben tartásával. A

reaktív jogalkotás fenntarthatósági kihívásokkal is szembesül. Ahhoz ugyanis, hogy a jogrendszer hosszú távon hatékony és alkalmazkodóképes legyen, szükség van a folyamatos együttműködésre, az érintett felek és szakértők bevonására a jogalkotási folyamatba. Ezenkívül a jogalkotásnak képesnek kell lennie a hosszú távú kihívásokra adandó hatékony válaszok kidolgozására.

A reaktív jogalkotás előnyei közé tartozik a gyors reakció és a rugalmasság. Az események gyors üteme mellett az ilyen típusú jogalkotás lehetővé teszi a jogrendszer számára, hogy sürgősen és hatékonyan reagáljon a változó körülményekre. Egy adott válság vagy probléma felmerülésekor azonnal szabályozási választ kínál, megelőzve vagy minimalizálva annak káros hatásait. Azonban a reaktív jogalkotásnak is vannak korlátjai. Az azonnali reakciók néha túlzsúfolt jogrendszerhez vezethetnek, ahol a különböző törvények és rendeletek ellentmondanak vagy nehezen értelmezhetők. A hosszú távú tervezés hiánya miatt a reaktív jogalkotás nem mindig képes hatékony megoldásokat kínálni a problémákra, és előfordulhat, hogy nem számol kellőképpen a valószínűsíthető következményekkel, így már eleve belekódolva a jogi sérülékenységet a jogi normába.

A reaktív jogalkotás szükséges lehet váratlan események vagy válságok kezeléséhez, azonban a fenntartható jogrendszer építéséhez és az állampolgárok igényeinek való megfeleléshez a hosszú távú tervezés, a kockázatértékelés és a társadalmi egyeztetés, illetve részvétel elengedhetetlen. A megfelelő egyensúly megtalálása azonnali reakció és fenntarthatóság között kulcsfontosságú a jogrendszer hatékonysága és alkalmazkodóképessége szempontjából.

A proaktív jogalkotás olyan megközelítést jelent, amely előre tekintő és tervezett jogalkotási intézkedéseket alkalmaz. A proaktív jogalkotás azt jelenti, hogy a jogalkotók előre gondolkodnak és előre tervezik a jogrendszer fejlesztését. Ennek része lehet a társadalmi és gazdasági trendek elemzése, a jövőbeli kihívások azonosítása és olyan jogszabályok előkészítése, amelyek megelőzik vagy hatékonyan kezelik ezeket a kihívásokat. A proaktív jogalkotás nem csak a váratlan eseményekre reagál, hanem azokra is, amelyeket előre látni lehet.

A proaktív jogalkotás előnyei közé tartozik a hosszú távú fenntarthatóság és a jogrendszeri stabilitás. Az előrelátó intézkedések segítenek megelőzni a válságokat, csökkentve

ezzel a sürgős reakciók szükségességét. A jogrendszer stabilabbá válik, mivel a jogalkotók tudatosan tervezik és alkalmazkodnak a társadalmi és gazdasági változásokhoz.

A proaktív jogalkotás kihívásokat is felvet. Az előrelátó intézkedéseknek gyakran kell szembesülniük a jövőbeli kockázatok és bizonytalanságok komplexitásával. Az előrejelzéseket és az előretekintést minden esetben nem lehet teljes bizonyossággal megtenni, és ez a jogalkotókat néha a helytelen döntések kockázatával hagyja szembe nézni.

A technológia fejlődése jelentős szerepet játszik a proaktív jogalkotásban. Az adatelemzés, mesterséges intelligencia és más technológiai eszközök segíthetnek a trendek és változások előrejelzésében. A jogalkotónak alkalmazkodnia kell az új technológiákhoz, hogy hatékonyan élhessen ezekkel az eszközökkel a jogrendszere fejlesztése során. A proaktív jogalkotás sikerének kulcsa a társadalmi részvétel és a nyitott párbeszéd. A jogalkotóknak be kell vonniuk a társadalmat, figyelembe véve az érintett felek véleményeit és szükségleteit. Az ilyen típusú párbeszéd segít az intézkedések elfogadhatóságának növelésében és a jogrendszerek legitimációjának erősítésében.

A proaktív jogalkotás a szakmai szempontokon nyugvó előrelátás és az előre tervezés kultúráját helyezi a jogalkotói gondolkodás középpontjába. A helyes egyensúly megtalálása a kihívások és előnyök között elengedhetetlen. A technológia, a társadalmi részvétel és a nyitott párbeszéd mind olyan tényezők, amelyek elősegíthetik a sikeres proaktív jogalkotást, és hozzájárulhatnak a jogrendszer hosszú távú fenntarthatóságához, valamint a transzparencia révén a jogi sérülékenység érdemi csökkentéséhez. A technikai és társadalmi kihívásokkal összefüggésben sikerül a nemzetbiztonsági ágazat esetében számos sikeres példát találni az elmúlt másfél évtizedben.

Igaz, hogy már 2012. január elsejétől – a kibertérből érkező fenyegetésekkel összefüggő cselekvési kényszer hatására – a jogalkotó a Katonai Nemzetbiztonsági Szolgálat feladatává tette a honvédelmi érdeket veszélyeztető kibertevékenységről történő információgyűjtést, de e tekintetben fajsúlyos változást az Nbtv. 6. § g) pontjának evolúciója hozott. [349]

[349] KENEDLI Tamás – KIS-BENEDEK József – SZABÓ Károly (2016): A katonai felderítés és elhárítás evolúciója, szervezete és feladatkörei. In FARKAS Ádám – KÁDÁR Pál szerk.: Magyarország katonai védelmének közjogi alapjai. Budapest, HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Közhasznú Nonprofit Kft. 123 o.

Ez ugyanis tükre annak, hogy miként reagált a jogalkotó a területen folyamatosan megnyilvánuló, helyesebben folyamatosan változó kihívásokra. A publikáció készítésekor hatályos normaszöveg feladatok oldalán tapasztalható bővülése, miszerint a Katonai Nemzetbiztonsági *Szolgálat „információkat gyűjt a honvédelmi érdeket veszélyeztető kibertevékenységekről és -szervezetekről, észleli a kibertérből érkező fenyegetéseket és támadásokat, jogszabály keretei között ellátja a honvédelmi ágazat elektronikus információbiztonsági feladatait, biztosítja a honvédelemért felelős miniszter által vezetett minisztérium, valamint a Honvéd Vezérkar tervező munkájához szükséges, kibertérrel összefüggő nemzetbiztonsági jellegű információkat, továbbá kibertér műveleti képességeivel ellátja a honvédelmi érdekek nemzetbiztonsági jellegű védelmét és együttműködik a Magyar Honvédség kiberműveleti erőivel”* fejezi ki a leginkább, hogy mennyivel bonyolultabbá vált mindössze néhány év alatt ennek az egy feladatnak a jogi absztrahációt követő megjelenítése a törvényi tényállásban.

Az elmúlt években, – a kutatási időszakom éveiben korábbiaknál is erőteljesebben – tapasztalható körülmények felhívták rá a figyelmet, hogy a kibertérben jelenlévő, pontosabban onnan érkező, azt felhasználó dezinformációs művelet a járvány idején (de minden más, különleges jogrend kihirdetését megalapozó helyzetben) jelentősebb eredménnyel jár (hátránnyal fenyeget).

Emiatt a biztonság állapotának szavatolása komolyabb dologi és személyi erőforrásokat igénylő feladatot jelent a nemzetbiztonsági elhárításért és rendvédelemért felelős szervek számára is, különösen a veszélyek elhárítására történő folyamatos felkészülés, illetve a nem várt, de a közeljövőben valószínűsíthetően bekövetkező jövőbeli hasonló kihívások innovatív, proaktív és adaptív kezelése.

3. A kapcsolódó jogi normák rendszeres felülvizsgálatának és a biztonságtudatosságnak a fontosságáról

A folyamatban lévő, előbbieket – kiemelten a stratégiák készítését, felülvizsgálatát – érintő jogalkotói tevékenység során az illetékes szervek (és személyek) számára kiemelt jelentőséggel bír a kibertérben zajló hadviseléssel való kölcsönhatás vizsgálata, a várható következmények felmérése az online térben, a közösségi médiában, hiszen ezen vizsgálatok nélkül könnyen ellentétes hatást érhet el bármilyen „jószándékú”, biztonságtudatosságot

növelni szándékozó, elektronikus-információvédelmet propagáló, vagy más, az adatvédelem fontosságára figyelmet felhívó kampány is. Schmitt a jogalkotói és jogalkalmazói tevékenység kibertérben történő vizsgálata során a kiber lawfare fogalmát vezeti be, miszerint *„a jog eszközeinek alkalmazása a kiberhadviselés keretében, különös tekintettel a nemzetközi kiberjogi normák manipulálására”*.[350] Véleménye szerint ez a gyakorlat lehetővé teszi, hogy az államok jogi érvekkel igazolják vagy leplezzék kiber műveleteiket, ezzel növelve azok legitimációját.

A teljes védelmi szervezetrendszer számára komoly kihívást eredményezett és cselekvésre késztette a 2013 novemberében kezdődő Majdan téren lezajlott tüntetéssorozat, valamint a 2014 tavaszán („rendkívüli orosz katonai gyakorlat” elrendelésével[351]) Ukrajnában elkezdődött eseménysorozat, melyet szomszédos országban zajló (polgár)háborús helyzetnek tekinthetünk. A Katonai Nemzetbiztonsági Szolgálat és a honvédelmi ágazat felelőssége különösen megnövekedett, valamint a válság eszkalációja miatt kiemelt figyelmet kellett fordítaniuk a szolgálatoknak és minden állami szervnek Magyarország nemzetbiztonsági érdekeinek védelme során végzett tevékenysége során. A nemzetközi kötelezettségvállalásaink során is elsődleges prioritássá vált az Ukrajnában zajló események nyomon követése. A jogalkotó – így különösen honvédelmi miniszter és Magyarország Országgyűlése a Honvéd Vezérkar Felderítő Csoportfőnökségét 2014. június elsejétől, személyi állományával és feladatrendszerével – elkülönített szervezeti elemként – beépítette a Katonai Nemzetbiztonsági Szolgálat szervezetébe. A Katonai Egységes Felderítő Rendszer kialakítása útján a parancsnoki döntéshozatalhoz szükséges információáramlás felgyorsult, a Magyar Honvédség felderítő rendszere a szövetségi követelményeknek és a Magyar Honvédség műveleteinek vezetéséhez szükséges felderítő támogatás biztosításával szembeni kormányzati elvárásoknak megfelelővé vált, valamint képes lett a szövetségi felderítő rendszerhez való kapcsolódásra.

A 2014 nyarán végrehajtott szervezeti átalakítások indokoltsága és szükségessége (utólag) a hazánkat Dél felől érintő migrációs válsághelyzettel összefüggésben is megerősítésre került, mivel a 2015 nyarán tapasztalt Magyarországot érintő események, különösen a tömeges bevándorlás okozta válsághelyzet kezelése, minden állami szervtől kiemelkedő teljesítményt követelt meg, így a nemzetbiztonsági szolgálatoktól is.

---

[350] SCHMITT, Michael N.: Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention. *International Law Studies*, 2020, Vol. 96. 549–576.

[351] Az orosz elnök a Nyugati Katonai Körzetben, a Közép-Oroszországi Katonai Körzetben és a légvédelmi erőknél rendelt el soron kívüli ellenőrzést, amint arról a sajtóban meg is jelentek a híradások. A HVG hasábjain jelent meg Ellenőrizteti az oroszok harckészültségét Putyin címmel.

A Katonai Nemzetbiztonsági Szolgálat a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Programmal összefüggő hadiipari kutatás-fejlesztési feladatok támogatását közvetlenül, szakértő biztosításával és közvetve is végzi. Ennek egyik megnyilvánulási formája a 2017. július 1-től megalakult a HM Védelmi Technológiai Kutató Központ létrehozása volt. A szervezeti egység fő feladata az volt, hogy ellássa a honvédelmi tárca haditechnikai irányú kutatás-fejlesztési és technológiai innovációs tevékenységének stratégiai szintű felügyeletét és meghatározza a kutatás-fejlesztési feladatainak fő irányait. A kutatóközpont 2019. év január 1-jétől a Magyar Honvédség parancsnokának közvetlen szolgálati alárendeltségében, Modernizációs Intézet néven végezte feladatait megszüntetéséig.

A feladatrendszerre vonatkozó deregulációs, illetve technikai jellegű módosításokon túl, a korábban a Honvédelmi Minisztériumhoz tartozó gazdasági társaságokkal összefüggésben megállapította a jogalkotó, hogy a honvédelmi miniszter által rendeletben meghatározott, honvédelmi érdekhez kapcsolódó tevékenységet folytató gazdasági társaságoknál továbbra is a Katonai Nemzetbiztonsági Szolgálat végzi az Nbtv. 6. §-ában meghatározott feladatokat (ide nem értve a belső biztonságról és bűnmegelőzésről szóló tevékenységet).

Ezen feladatokkal összefüggésben a Katonai Nemzetbiztonsági Szolgálat működési területén támogatja a nemzetközi és hazai haditechnikai és hadiipari együttműködési programok szervezését és lebonyolítását, valamint részt vesz a nemzeti képviselet biztosításában a NATO-, EU-szervezetekben, illetve a V4 közösségen belül.

Az időrendben az utolsó előbbiekkel kapcsolatos, jelentős jogszabály módosítás az egyes törvények honvédelmi kérdésekkel összefüggő módosításáról szóló 2019. évi CV. törvény volt[352]. A törvényjavaslat által megvalósítani tervezett cél az volt, hogy a jogalkotás eszközeivel növelje Magyarország honvédelmi képességeit. Ennek során szabályozásra került a kiberfenyegetések elleni (korábbiakhoz képest) hatékonyabb fellépés, valamint a hibrid fenyegetések elleni kormányzati koordináció témaköre is. Az Nbtv.-ben megjelenő, a Katonai Nemzetbiztonsági Szolgálat feladatrendszerét érintő kiemelkedő jelentőségű módosításnak tekinthető, hogy az új típusú kihívásoknak megfelelő módon került megjelenítésre a 6. § a) pont szerinti, a felsorolásban első feladat, miszerint „*felfedi a Magyarország ellen irányuló támadó, befolyásoló szándékra utaló törekvéseket, valamint feladatrendszeréhez illeszkedően külföldön*

[352] A törvényt az Országgyűlés 2019. december 10-i ülésnapján fogadta el.

érvényesíti Magyarország érdekeit". Ez a katonai hírszerző és elhárító tevékenység integrált szervezeti keretek között értelmezett célkitűzéseként fogható fel, mivel a befolyásolás és az érdekérvényesítés kifejezések használatával egy új és modern megközelítésben újra definiálja a nemzetbiztonsági szolgálat egyik legfontosabb feladatát.

Ahogyan Farkas Ádám a közeljövő szabályozási kihívásainak rendszerezése során rámutat, *„a 2020-as év azonban a COVID–19 járvány miatt kihirdetett veszélyhelyzettel – annak minden jogi kérdésessége mellett is – sajnos arra is rámutatott, hogy nem csak a fegyveres kérdések válthatnak elsősorban politikai csatározás tárgyává"*. [353]

Kijelentését olvasva megállapítható, hogy a politikai küzdelmeken felül emelkedő jogalkotó – és jogalkalmazó – képes megakadályozni a legtragikusabb, illetve a legnagyobb kárral járó „forgatókönyvek" megvalósulását. Ebben azonban jelentősebb szerepet kell biztosítani az értekezés több pontján hangsúlyozott tartalmi felülvizsgálatnak, korszerűsítésnek és ezzel összefüggésben a szabályozásra ható technikai, társadalmi, gazdasági és biztonsági környezet monitorozásának és elemzésének.

A valós időben felmerülő kihívásokat ugyanis valós időben kell kezelni, ami az esetek többségében megfelelő és korszerű törvényi szintű szabályozás esetén – kormányrendeletekkel, mint meghatározó jogforrással, megoldható, míg a törvényi keretek zavara esetén vagy kivételes megoldásokat vagy különleges jogrendi fellépést tehet szükségessé. A proaktivitás tehát életbevágó a pandémia idején, de minden más potenciálisan előálló kihívás kapcsán is.

A jelentős mérföldkövek meghatározása során figyelemmel kell lenni a fejezet bevezetőjében megjelenített körülményre, miszerint Magyarországon a normaalkotás jellemzően követi az eseményeket, igaz ebben a tudomány- és technikafejlődés trendjeire épülő proaktivitási igény változást hozhat. Ennek ellenére sem várható el azonban, hogy „tényállásszerűen" kerüljön meghatározásra például az idegen befolyásolás felderítése a nyomozás elrendeléséig egy elhárító szolgálat feladatrendszerében, amennyiben a Büntető törvénykönyvben nem kerül ilyen tényállás megjelenítésére. Ezzel összefüggésben a jogalkotói

[353] FARKAS Ádám: Gondolatok a különleges jogrend természetéről és helyéről a modern államiságban In.: KELEMEN Roland – FARKAS Ádám (szerk.): Szkülla és Kharübdisz között – Tanulmányok a különleges jogrend elméleti és pragmatikus kérdéseiről, valamint nemzetközi megoldásairól Budapest, Magyar Katonai és Hadijogi Társaság, 2020, 330.o.

progresszió megjelenésére kiváló példa az Nbtv. 2020. január elsején hatályba lépett módosítása, miszerint a Katonai Nemzetbiztonsági Szolgálat „*felfedi a Magyarország ellen irányuló támadó, befolyásoló szándékra utaló törekvéseket, valamint feladatrendszeréhez illeszkedően külföldön érvényesíti Magyarország érdekeit”.*[354] A jogalkotói reakciók, melyeket legoptimálisabb esetben a szakmai, illetve tudományos közösségek katalizálnak, egyre jelentősebb mértékben adnak választ a hibrid hadviselés jelentette biztonsági kockázatok és a lawfare jelentőségének felismerése miatt felmerült kérdésekre.

A vizsgált időszak első fontos változását a Magyar Köztársaság minisztériumainak felsorolásáról szóló 2010. évi XLII. törvény hatályba lépésével összefüggő szervezetátalakítási folyamat[355] eredményezte. Az Nbtv. miniszteri irányítással összefüggő módosítása feloldotta a korábbi korlátozást, miszerint a belügyminiszter (a rendészetért felelős miniszter), a honvédelemért, vagy az igazságügyért felelős miniszter legyen a polgári nemzetbiztonsági szolgálatok irányítója. Ezen jogalkotási aktus, valamint az ezzel egyidejűleg végrehajtott intézményi reform tette indokolttá és szükségessé a belügyminiszter irányítása alá tartozó szervek belső ellenőrzési, bűnmegelőzési és belső bűnfelderítési tevékenységeinek felülvizsgálatát az irányított szervek tevékenysége közötti átfedések megszüntetése érdekében.

Miként azt Urbán Attila összefoglalja, *a fenti megoldás – az Nbtv. korábbi 10. § (2) bekezdésében szereplő korlátozás kiiktatásával – az általános európai (a polgári hírszerzés új helyzete kapcsán főként a brit) megoldásra emlékeztető gyakorlatot követve, a kül- és biztonságpolitika területén meghatározó szakminisztereket helyezte irányítói szerepkörbe. Az átalakítás egyik oldalról megvalósította a nemzetbiztonsági és a rendvédelmi (műveleti) kapacitások integrációját a BM szervezeti rendjében. Ezzel párhuzamosan azonban tovább erősödött a magyar nemzetbiztonsági igazgatás osztott jellege, hiszen a szolgálatok kormányzati irányítási feladatai immár – a korábbi kettő helyett – három minisztérium között oszlottak meg*.” [356]

[354] A nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény 6. § (1) bekezdésében.
[355] a 2010. évi XLII. törvény, illetve az erre épülő, az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatáskörérő szóló 212/2010. (VII. 1.) Korm. rendelet alapján a nemzetbiztonsági Szakszolgálat és – az NBH jogutódja – az Alkotmányvédelmi Hivatal az újjászervezett belügyi tárca vezetőjének, míg az Információs Hivatal a külügyminiszter irányítása alá került.
[356] Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban (Nemzetbiztonsági Szemle 8. évfolyam (2020) 1. szám 22-23. o.

A Terrorelhárítási Központ létrehozása[357], annak ellenére, hogy nem egy új nemzetbiztonsági szolgálat megalakításáról van szó, mégis jelentős hatást gyakorolt a szolgálatok feladatrendszerére[358], így indokolttá vált a megjelenítése ezen kontextusban. A terrorizmus nemzetközi színtereken tapasztalt megnyilvánulásai egyre jelentősebb kihívás elé állítják a jogállamokat, így Hazánkat is. A terrorizmus okozta veszély elleni hatékony küzdelemre jellemző, hogy a szabadságjogok tiszteletben tartása és a biztonság közötti viszonyrendszer újra értelmezése mellett, a szükségesség és az arányosság alapelveinek figyelembevételével, a speciális terrorelhárító szervek megalakítására, valamint e szervek felhatalmazásának szélesítésére ösztönzi a demokratikus berendezkedésű országokat. Hazánk a nemzetközi kötelezettségvállalásai keretein belül, ideértve a nemzetközi jogi kötelezettségeket – kiemelten a terrorszervezetek elleni hatékony fellépésre, valamint a terrorizmus anyagi hátterének felszámolására vonatkozókat – minden jogszerű módszerrel és eszközzel fel kell, hogy lépjen a terrorszervezetekkel és a terrorizmust anyagi eszközökkel támogatók szervezetekkel és személyekkel szemben.

A jogalkotó álláspontja szerint[359] a Terrorelhárítási Központ létrehozásának konkrét indoka az volt, hogy a terrorellenes küzdelem hatékonyságát növeli, ha a terrorizmus elleni küzdelmet kizárólagos hatáskörrel, egy önálló, nemzeti, rendőrségi felderítő szerv végzi. Az egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról szóló 2010. évi CXLVII. törvény a nemzetbiztonsági szolgálatokkal összefüggésben rögzítette, hogy saját állományuk tekintetében ellátják a belső biztonsági és bűnmegelőzési célú ellenőrzési feladatokat, az Információs Hivatal a kifogástalan életvitel ellenőrzését is. A korrupció megelőzése, felderítése és elhárítása szervezeten belül kerülhet végrehajtásra azóta a hírszerzésért felelős szolgálatok esetében (ideértve a Katonai Nemzetbiztonsági Szolgálat jogelődjét is). Az integritásmenedzsment és irányítás is ezzel egy tekintet alá esik előbbi

[357] A Terrorelhárítási Központról szóló 232/2010. (VIII. 19.) Korm. rendelettel került létrehozásra. Feladatainak részletes megjelenítését a 2010. szeptember 1-jén hatályba lépett alapító okiratban jelenítette meg a jogalkotó. Az ebben nem szabályozott kérdéseket a Terrorelhárítási Központ Szervezeti és Működési Szabályzata tartalmazza. A jelenleg hatályos rendelkezések a 2012. november 06-án kelt a Terrorelhárítási Központ alapító okirata, módosításokkal egységes szerkezetben című, A-173/1/2012 számú okiratban találhatók.

[358] A terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól 295/2010. (XII. 22.) Korm. rendelet alapján Terrorelhárítási Központ átvette a Rendőrségtől és az Alkotmányvédelmi Hivataltól, azok terrorfelderítési és- elhárítási feladatait. Előbbiektől némiképp eltérően a Katonai Nemzetbiztonsági Szolgálat a nyomozás elrendeléséig, működési területén végzi a terrorcselekmény (Btk. 314-316/A. §), a terrorcselekmény feljelentésének elmulasztása (Btk. 317. §) és a terrorizmus finanszírozása felderítését.

[359] Az egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról szóló T/1426. számú törvényjavaslat (Forrás: Parlament.hu, letöltés ideje 2021. 01. 08. 10:54)

szolgálatoknál. Ezen jogszabály tette lehetővé azt, hogy az előbb megjelenített Terrorelhárítási Központ mellett a Nemzeti Védelmi Szolgálat is önálló rendőri szervként létrehozható legyen.

A belső bűnmegelőzést és bűnfelderítést a törvénymódosítást megelőzően a Rendvédelmi Szervek Védelmi Szolgálata végezte, ugyanakkor a polgári nemzetbiztonsági szolgálatok közül az Alkotmányvédelmi Hivatal és Nemzetbiztonsági Szakszolgálat feladatai között is szerepelt a belső biztonsági feladatkör. Célszerűségi és hatékonysági szempontból egyaránt indokolttá és szükségszerűvé vált, hogy ezt a tevékenységet egyetlen, önálló rendőrségi szerv lássa el. A Nemzeti Védelmi Szolgálat létrehozása tartalmi és kodifikációs szempontból is érintette az akkor hatályos Nbtv. előírásait és a minősített adat védelméről szóló 2009. évi CLV. törvényt is módosította. A Nemzeti Védelmi Szolgálat létrehozása óta végzi a bűnmegelőzési ellenőrzéseket, a hatáskörébe tartozó bűncselekményeket felderíti, ellenőrzi a hivatásos állomány tagjai kifogástalan életvitelére vonatkozó adatokat, valamint gondoskodik a megbízhatósági vizsgálatok folytatásáról. A szerv új feladata, illetve eszköze az úgynevezett megbízhatósági vizsgálat lett. A megbízhatósági vizsgálat vagy integritás ellenőrzés a nemzetközi gyakorlatban is jól teljesít, mint a kontroll egyik hatékony eszköze. A nemzetközi gyakorlatban a megbízhatósági vizsgálat elrendelése ügyészi közreműködéshez kötött, így az ügyész olyan szervezeten kívüli, jogi természetű kontroll szerepét tölti be a szakmai tevékenység fölött, amely hozzájárul a vizsgálatok objektivitásához.

Szintén az egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról szóló 2010. évi CXLVII. törvény által bevezetett komponens, hogy az általa módosított Nbtv. 40. §-ának előírásai szerint lehetővé vált – külső engedély alapján – a számítástechnikai eszköz vagy rendszer útján továbbított, vagy azon tárolt adatok megismerése és azok tartalmának technikai eszközzel rögzítése és felhasználása. A Nemzetbiztonsági Szakszolgálatra vonatkozó szabályozás változásai az új irányítási rendből származtathatóak. Kisebb mértékben változtak az előírások a nemzetbiztonsági ellenőrzésre vonatkozóan is. Új elemként jelent meg a módosítás során, hogy az ellenőrzött, a tájékoztatást követően az érintett a miniszternél panasszal élhet, azonban az Országgyűlés Nemzetbiztonsági Bizottságához már nem fordulhatott.

Az ötszolgálatos modell kialakításához hasonló jelentőségű változást okozott nemzetbiztonsági ágazat számára a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény katonai nemzetbiztonsági szolgálatok összevonásával kapcsolatos módosításáról,

valamint az azzal összefüggő további törvénymódosításokról szóló 2011. évi CLXXI. törvény kihirdetése[360] és hatályba lépése.[361] A vizsgált időszak kiemelkedő – a 21. századi kihívásokra reagáló – jogalkotási és szakmai megoldása volt a Katonai Nemzetbiztonsági Szolgálat létrehozása 2012. január elsején. [362]

Kiemelkedő jelentőségű, a nemzetbiztonsági szolgálatok adatkezelő, értékelő-elemző és kormányzati tájékoztató tevékenységét érintő, koncepcionális vitát generáló jogszabály tervezetet ismerhetett meg 2011. novemberében az olvasó (szakmai szervezetek és nyílt köröztetés miatt a széles közvélemény egyaránt) az egyes rendvédelmi tárgyú törvények módosításáról, valamint az azzal összefüggő további törvénymódosításokról szóló T/5004. számú törvényjavaslat tanulmányozása során. Urbán Attila foglalja össze a javaslat sorsát, miszerint, „*a Nemzeti Információs és Bűnügyi Elemző Központ létrehozását célzó javaslat kapcsán a parlamenti vitában, illetve a közéleti nyilvánosság fórumain – a szervezet adatbázisokhoz való közvetlen hozzáférése és adatkezelési jogosultságai kapcsán megfogalmazott alapjogi dilemmák mellett – ismét felbukkantak a szolgálatok független elemző-értékelő és döntéshozókat közvetlenül elérő tájékoztató tevékenységét, illetve a szektoriális tárcaálláspontokat preferáló megközelítések. Jellemzően ez utóbbi szempontok jelentek meg azokban kormánypárti képviselők (köztük a polgári nemzetbiztonsági szolgálatokat korábban irányító házelnök) által benyújtott módosító javaslatokban[363], amelyeket az Országgyűlés többsége a BM eredeti előterjesztésével szemben támogatott.”*[364]

A koncepció így nem vált valóra, ugyanakkor a tervezetben megjelenített szakmai célok indokoltságát és szükségességét alátámasztja[365], hogy 2018 óta a polgári hírszerzésért felelős

[360] 2011. XII. 14-én.
[361] 2012. I. 01-jén.
[362] A 2012 és 2020 közötti időszak fontos eseményeit és a jövőre vonatkozó elképzeléseket KENEDLI Tamás foglalja össze és rendszerezi A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években című tanulmányában in: Nemzetbiztonsági Szemle 8. évfolyam (2020) 1. szám 74–94.o.
[363] Kövér László házelnök módosító javaslata a törvénytervezethez. 2011. november 30. Forrás: www.parlament.hu/ irom39/05004/05004-0022.pdf (A letöltés dátuma: 2021. 01. 10. 13:24)
[364] Urbán Attila: A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. In: Nemzetbiztonsági Szemle 8. évfolyam (2020) 1. szám 24.o.
[365] Ezen kiemelkedően fontos célok az Nbtv. Indokolásában olvashatók: A TIBEK feladatai közül kiemelésre érdemes az együttműködő, mindenekelőtt a nyomozó és a nemzetbiztonsági szervek működésbeli párhuzamosságainak a kiszűrése. Mind a terrorelhárítás, mind az állami büntetőigény érvényesítése, mind a szuverenitás érdekében végzett titkosszolgálati tevékenység területén rendkívüli kockázatokkal járnak a párhuzamos nyomozások, illetve a párhuzamos titkos információgyűjtések. Ezek kiszűrése és jelzése a megfelelő együttműködő szerveknek a TIBEK fontos feladata. Ezzel a TIBEK nagymértékben elősegíti a terrorcselekmények

Információs Hivatal és a Katonai Nemzetbiztonsági Szolgálat – önálló elemző-értékelő képességeit, valamint a döntéshozók közvetlen tájékoztatásának közvetlen lehetőségét megőrizve, a 2016-ban létrehozott információ-fúziós központtól független formában – a Nemzeti Információs Államtitkárság útján, illetve közvetlenül elégíti ki a kormányzati hírigényt, a gazdaságosságot és a gyors információáramlást célul kitűzve. Az értekezésem lezárásának időszakában került elfogadásra és vár kihirdetésre azon törvényjavaslat, amely ezt a struktúrát alapjaiban fogja megváltoztatni. Az új struktúrával összefüggő kutatások, elemzések elengedhetetlenül szükségesek, hiszen így kaphat a kormányzat tudományosan megalapozott visszajelzést a jövőbeli korrekciók esetleges szempontjaival kapcsolatban.

Ezen feladatkörrel összefüggésben szükséges megjegyezni, hogy a Katonai Nemzetbiztonsági Szolgálat az Nbtv. 6. § a)-g), i)-l), n)-s) pontban meghatározott feladatai ellátása során a működési területén felderített, a nemzetbiztonság katonai elemeit érintő információkat elemzi és értékeli, azokról kizárólagos jog-, és hatáskörrel, folyamatosan tájékoztatja a honvédelemért felelős miniszter által vezetett minisztérium feladat-, és hatáskörrel rendelkező vezetőit, a Magyar Honvédség feladat-, és hatáskörrel rendelkező parancsnokait, vezetőit, a Magyar Honvédség vezérkari főnökét, a honvédelemért felelős minisztert, valamint a Magyar Honvédség főparancsnokát.

Az Nbtv. 6. § h) és m) pontjában Ugyanakkor meghatározott feladatai ellátása során megszerzett információkat haladéktalanul, elemző-értékelő tevékenység mellőzésével, vagyis „fogyasztható, de nyers” állapotban biztosítja a Terrorelhárítási Információs és Bűnügyi Elemző Központnak. Így a 2016. július 17-én hatályba lépett törvénymódosítás eredményeként kijelenthető, hogy a Katonai Nemzetbiztonsági Szolgálat a terrorizmus, illetve a szervezett bűnözés[366] elleni küzdelem vonatkozásában releváns adatokat haladéktalanul biztosítja a

megelőzését, a nyomozások eredményességét, illetve az adattakarékosság alkotmányos elvének érvényre juttatását. A TIBEK az együttműködő szervek számára folyamatosan továbbítja a hatáskörükbe tartozó adatokat, ezzel egyidejűleg javaslatot tesz az együttműködő szervek számára az adatok mikénti felhasználására. A TIBEK mint információfúziós központ rendkívül hatékony segítséget nyújthat a TEK terrormegelőző, terrorelhárító tevékenységéhez mivel a rendelkezésére álló adatokból hatékony következtetést tud levonni a terrorszervezetek magyarországi tevékenységéről, a terroristák megjelenéséről, és a PNR adatok alapján mozgásukról. A TIBEK koordinációs tevékenysége során figyelemmel kíséri, hogy nem áll-e rendelkezésre az általa átadott adattal kapcsolatos pontosító vagy kiegészítő adat: amennyiben igen, a TIBEK a feladatkörében észlelt kapcsolódó adatot átadhatja az adat felhasználására hatáskörrel rendelkező együttműködő szervnek. A TIBEK fontos feladatokat lát el a szervezett bűnözés elleni küzdelemben és az illegális vagyonok felderítésében is. A TIBEK a terrorszervezetekkel, illetve a konkrét terrorcselekményekkel kapcsolatos adatait soron kívül továbbítja a TEK részére.

[366] A KNBSZ önálló elemző-értékelő tevékenysége az egyedi működési területéhez kötődő, a honvédelmi ágazat napi biztonságos működéséhez szükséges mértékű, katonai nemzetbiztonsági jellegű információk körére terjed ki.

Terrorelhárítási Információs és Bűnügyi Elemző Központ részére. Mindezt az elmúlt évek során kialakult gyakorlat szerint, az eredeti koncepció által megjelenített, szükséges és arányos szakmai együttműködés keretein belül, az információ-fúziós központ által támasztott igényeket kielégítve teszi a 2022-es módosítást követően a Nemzeti Információs Központ felé is, bár az információk eredeti, 2016-os körénél szélesebb körben.

4. „Baráti tűz" vagy legitim jogérvényesítés?

Folyamatos politikai és tudományos viták alapját képezi, az a jelenség, hogy alkalmanként az Európai Unión belül, baráti tűz ér egyes tagállamokat, valamint az eljárásokban érintett tagállamok a rendelkezésükre álló jogi eszközrendszerrel igyekeznek „viszonozni is a tüzet". Azt, hogy eredetileg „ki lőtt először" vagy „kinek volt igaza", mint oly sok alkalommal, majd utóbb, az esetek összes körülményeinek tisztázása után lehet valószínűsíteni, valamint a vitás esetek teljeskörű tisztázása és értékelése, valamint a tapasztalatok összegzése után, remélhetőleg mindkét fél álláspontjának megismertetésével és vizsgálatával oktatják majd a jövő jogászai, illetve leendő állami vezetői számára a felsőoktatási intézményekben, illetve politikai tanfolyamokon.

A jogállamisági eljárások egyes tagállamokkal szemben az Európai Unió és a tagállamok közötti rendszerben megjelent jogi mechanizmusokra utalnak, amelyek célja a jogállamiság és az alapvető jogok védelmének biztosítása. A jogállamisági eljárások szükségessé válhatnak, ha az EU úgy ítéli meg, hogy egy tagállamban olyan lépések történtek, amelyek veszélyeztetik a jogállamiságot és az alapvető értékeket. [367]

Az egyes tagállamokkal szembeni jogállamisági eljárások, illetve vizsgálatok – az eljárásokat kezdeményező iratok, kerestek alapján – az egyes tagállamok jogalkotó szerveinek jogi és intézményi reformjaira, a média, a bíróságok, a civil társadalom és más fontos intézmények függetlenségének esetleges csökkentésére vonatkozó kormányzati, illetve

[367] Arra vonatkozóan, hogy milyen konkrét jogorvoslati mechanizmusok állnak rendelkezésre például a regionális fejlesztési támogatások kedvezményezettjei számára, különösen a szabálytalanságok kezelése kapcsán lásd: GÖNCZI Lili – HOFFMAN István: The Sui Generis Nature of Legal Protection in the Case of Regional Development Aids in the Hungarian Legislation and Legal Practice – Focused on Irregularity Issues. Studia Iuridica Lublinensia, Vol. 32. (2023) No. 2., 117–132. o. DOI: 10.17951/sil.2023.32.2.117-132. Az EU-s és nemzeti szintű szabályozás között feszültség figyelhető meg, amely végső soron jogállamisági eljárás elindítását megalapozó körülményeket eredményezhet, emiatt a hivatkozott kutatás kvalitatív és kvantitatív eredményeit és megállapításait indokolt a jogalkotási kihívásokra történő megfelelő reakcióval figyelembe vennie a jogalkotónak, elkerülendő a fejlesztési támogatások körüli jogvitákat.

jogalkotói intézkedések feltárására is irányulhatnak. Az EU kifogásolhat olyan intézkedéseket, mint az igazságszolgáltatás politikai befolyásolása, az alkotmánybíróság szerepének megváltoztatása, valamint a média és a civil szervezetek tevékenységének korlátozása.

Az Európai Bizottság által indított jogállamisági eljárások keretében az Európai Parlament is kifejezheti aggodalmát az egyes tagállamokban tapasztaltakkal összefüggésben, és az Európai Tanács is tárgyalhatja a jogállamisági kérdéseket. Az EU intézményei ilyen helyzetben arra törekednek, hogy párbeszédet folytassanak az érintett tagállamokkal és figyelemmel kísérjék a helyzetet.

A 7. cikkely az Európai Unió Szerződésében meghatározza azt a mechanizmust, amely lehetővé teszi a jogállamiság megsértése esetén szankciók bevezetését egy tagállammal szemben. Egy ilyen eljárásnak a súlyos és tartós jogállamisági problémákra kell összpontosítania, és kétlépcsős folyamatot követ: először az Európai Tanács megállapítja a kockázatot, majd szükség esetén szankciókat vezet be. Az eddigi esetekben az érintett tagállamokkal szemben a 7. cikkely szerinti eljárás elindították, de a szankciók bevezetéséhez szükséges egyhangú állásfoglalás elmaradt. A jogállamisági kérdések és a kapcsolódó párbeszéd folyamatosan napirenden vannak az EU és az érintett tagállamokkal között, és a felek igyekeznek megállapodásra jutni, azonban ehhez széleskörű (több tagállamot is magában foglaló) konszenzus szükséges.

A nemzetközi politikai légkör változásai, különösen a jobboldali pártok 2010-es évek második felében tapasztalható gyengülése az Európai Unió tagállamaiban, valamint egyes tagállamok jogalkotó szerveinek később a jogvita alapjává tett döntései egyértelműen hozzájárultak egy olyan diskurzus kialakulásához, amely a felek közötti nézeteltéréseket a széles nyilvánosság előtt zajló jogi csatározás szintjére emelte. Ez a helyzet azt szemlélteti, hogy a politikai diskurzus és a jogalkotás területén zajló események nem csupán a parlamenti vagy kormányzati szinten értelmezhetőek, hanem kiterjednek a társadalom szélesebb rétegeire is, befolyásolva ezzel a közvéleményt és a politikai döntéseket és a politika dinamikáját. Az ilyen típusú jogi küzdelmek gyakran szolgálnak terepet a különböző politikai és társadalmi csoportok érdekeinek és értékrendjének ütköztetésére, amelyek tükröződnek a jogalkotási folyamatokban és azok nyilvános megítélésében.

Az Európai Unió jogállamisági eljárásának hibrid hadviselési eszközként („baráti tűz” -ként) való esetleges, hipotetikus értelmezése különösen érzékeny kérdés, mivel Magyarország az Unió tagállamaként önként csatlakozott a közösen gyakorolt szuverenitás rendszeréhez, és aláírta, valamint ratifikálta az elsődleges jogforrásokat. Az eljárás az Unió értékközösségi jellegéből és a tagállamok közötti kölcsönös kötelezettségvállalásból fakad. A jelen dolgozat e mechanizmust abban az értelemben sorolja a hibrid hadviselési eszközök közé, hogy bizonyos politikai kontextusban a jogállamisági eljárás stratégiai nyomásgyakorlásként is értelmezhető.

A jog uralmába vetett hit eredményeként, valamint amiatt, mert mégiscsak szövetségesek közötti jogérvényesítésről van szó, a jogi normáknak megfelelő és mielőbbi konszenzusra jutás volna a leghasznosabb, figyelembe véve az Európai Unióra sötét árnyékként vetülő külső fenyegetettségek rendkívül széles spektrumát és külön-külön is súlyos voltát.

5. Összegzés, az elvégzett vizsgálat és részkövetkeztetések

A fejezet célja a jogalkotási folyamatok és a nemzetbiztonsági szolgálatok jogintézményeinek vizsgálata, azon belül is, hogy ezek a jogintézmények hogyan reagálnak az új típusú biztonsági kihívásokra. Ennek a vizsgálatnak az eredményeként került bizonyításra a 2. számú hipotézis és a második alfejezetben a proaktív, illetve az 1. számú hipotézis reaktív jogalkotással elérhető közpolitikai célok vonatkozásában meghatározott eleme. A fejezet elkészítése során elvégzett kutatás során megerősítettem az 5. számú hipotézist, miszerint a hibrid hadviselés eszközrendszerébe illeszkedő, az információs műveletek közé tartozó, egyes intézkedésekkel, illetve intézkedéssorozatokkal összefüggésben keletkezett tapasztalatok, ismeretek szövetségesi rendszeren belüli hasznosítása elengedhetetlenül szükséges a nemzeti és a szövetségi szintű reziliencia növelése érdekében, abban az esetben is, ha a szövetségen belüli konfliktusok árnyékolják be az együttműködést a tagállamok között.

A fejezet kiemelt figyelmet fordít arra, hogy a nemzetbiztonsági szolgálatok normatív működési keretei mennyiben proaktívak vagy reaktívak, és ez milyen hatással van a hatékony kormányzati válaszok kialakítására. A nemzetbiztonsági ágazat jogszabályainak felülvizsgálata két módon történik, az egyes jogszabályok és a teljes normakörnyezet utólagos elemzése révén, valamint a tartalmi dereguláció és módosítások által. Ezen felülvizsgálatok célja, hogy megőrizzék a jogrendszert naprakésznek, átláthatónak és biztonságosnak.

A nemzetbiztonsági szolgálatok által használt eszközök és módszerek normarendszere széleskörű és hierarchikus, és gyakran alapjogok korlátozását vonja maga után. A jogszabályokban meghatározott feladatok végrehajtása szigorú előírásokhoz kötött, emiatt szükséges kellő körültekintéssel elvégezni minden jogalkotói (rész)feladatot (is).

A jogalkotás jellemzően reaktív természetű, amely válaszként jön létre a társadalmi problémákra vagy váratlan eseményekre. A reaktív jogalkotás előnye a gyors reagálás képessége, ugyanakkor hátrányai között szerepelhet a túlzott jogszabályozottság és a hosszú távú tervezés hiánya. A fejezet hangsúlyozza a folyamatos együttműködés és a szakértők bevonásának fontosságát a hatékony jogalkotás érdekében, valamint arra is rávilágít, hogy a jogalkotásnak képesnek kell lennie a hosszú távú kihívások kezelésére. A technológia fejlődése és a társadalmi részvétel kulcsfontosságú a proaktív jogalkotásban, segíti a trendek előrejelzését és növeli az intézkedések elfogadhatóságát.

A proaktív jogalkotás ezen túlmenően a jogi hadviselés egyik alapvető pillérévé válik, hiszen lehetővé teszi olyan normatív környezet kialakítását, amely nem csupán reagál a fenyegetésekre, hanem előre felkészül azok jogi kezelésére. E megközelítés révén a jogrendszer az ellenséges információs műveletekkel illetve, hibrid fenyegetésekkel szemben preventív eszköztárat biztosít, amely a nemzetközi jog keretein belül is megerősíti az állam mozgásterét. A proaktív jogalkotás a jogi hadviselést többek között úgy támogatja, hogy:

- előre lefekteti a stratégiai fontosságú területek jogi védelmét, így csökkentve az ellenséges beavatkozások lehetőségét;
- erősíti a jogi narratívát a nemzetközi fórumokon, biztosítva a nemzeti álláspont legitimitását;
- gyorsan alkalmazható, előre megtervezett jogi eszközöket biztosít a válsághelyzetek kezelésére, így a jogi reakcióidőt is csökkenti.

A proaktív jogalkotás célja egy olyan jogrendszer kialakítása, amely hosszú távú fenntarthatóságot biztosít, miközben erősíti a jogrendszerek legitimációját, és aktívan támogatja a jogi hadviselésben alkalmazható állami stratégiákat. A fejezet végén igyekszem arra ösztönözni az olvasót, hogy – amennyiben lehetősége nyílik erre – találja meg az egyensúlyt a kihívások és az előnyök között, építsen a technológia adta lehetőségekre, valamint fektessen hangsúlyt a társadalmi párbeszédre a sikeres jogi normaalkotás érdekében.

A kibertérből érkezett álhírek a járvány elleni védekezést alapvetően nehezítették meg és ezzel számos emberéletet és jelentős anyagi javakat sodornak veszélybe. A közösségi oldalak igyekeznek ezeket kiszűrni, sajnos azonban hazánkban (is) több olyan esettel (álhírrel) találkozhattunk, amely a legnépszerűbb videómegosztó honlapról, vagy valamelyik közösségi oldalról indult útnak és okozott jelentős hátrányt. Ez a tapasztalat pedig jó eséllyel átültethető a jövőbeni potenciális fenyegetések kezelésébe is. A világjárvány által okozott sokkhatás kezelésekor keletkezett tapasztalatok megtanították a jogalkotó, illetve a legtágabb értelemben vett komplett védelmi igazgatás számára, hogy továbbra sem szabad megfeledkezni a jogintézmények alapjogkorlátozó voltáról, miközben vizsgáljuk a jogalkotási lehetőségeket még az ország életében extrémitásnak tekinthető különleges jogrend[368] alkalmazásának idején sem.

A szükségesség és arányosság feltételrendszerét még ekkor is meg kell vizsgálni egy-egy döntés, illetve intézkedés meghozatalakor, vagy ezek mellőzésekor, visszavonásakor. Ezzel összefüggésben érdemes a nemzetközi jogi előírásoknak, elvárásoknak való – jogalkotó oldalán felmerülő – kötelezettségeknek való megfelelést is értelmezni, megelőzve így az esetleges, későbbi nemzetközi jogvitákra okot adó jogalkotói lépéseket.

[368] A védelmi igazgatásról és a különleges jogrenddel összefüggésben bővebben lásd: FARKAS Ádám: Egy lehetséges séma Magyarország védelem-szabályozási és védelmi alkotmányos szemléletének megújításához, In: Vélemények a katonai jog világából, 2018/3. szám, 1-15. o., KELEMEN Roland: Az alaptörvény különleges jogrendi rendszerének egyes dogmatikai problémái – kitekintéssel a visegrádi államok alkotmányának kivételes hatalmi szabályaira, In: Katonai Jogi és Hadijogi Szemle, 2017/1-2. szám, 37-68. o., KELEMEN Roland – FARKAS Ádám (szerk.): Szküla és Kharübdisz között – Tanulmányok a különleges jogrend elméleti és pragmatikus kérdéseiről, valamint nemzetközi megoldásairól Budapest, Magyar Katonai és Hadijogi Társaság, 2020., KELEMEN Roland: A derogáció értelmezése a Polgári és Politikai Jogok Nemzetközi Egyezségokmányának, valamint az Emberi Jogok Európai Egyezményének tükrében, In: Közjogi Szemle, 2018/4. szám, 52-57. o. FARKAS Ádám: A jogállamon túl, a jogállam megmentéséért: Gondolatok a különleges jogrend természetéről, jelentőségéről és helyéről a modern jogállamban, In: Iustum Aequum Salutare, 2017/4. szám, 17-29. o., SPIZTER Jenő: A különleges jogrend szabályozása az egyes alkotmányokban IV. Különleges jogrendi szabályozás a francia jogrendszerben, In: Vélemények a katonai jog világából, 2019/4. szám, 1-13. o.,

369

2. ábra A jogalkotás támogatásának ciklusa a nemzetbiztonsági ágazatban

A fejezet összefoglalja továbbá a reaktív jogalkotás tanulságait és azt, hogy ez hogyan szolgálhat alapul egy hatékonyabb, proaktív(abb) jogalkotási folyamat kialakításához. Ennek a szempontrendszernek, vagyis a jogalkotási rendszer eme jellemzőinek való megfeleltethetőséget vizsgálom meg a következő fejezetben, különös tekintettel a kibertérben megjelenő biztonsági kihívások tükrében.

VIII. A JOGALKOTÁS JELLEMZŐINEK VIZSGÁLATA A KIBERBIZTONSÁGI KIHÍVÁSOK TÜKRÉBEN

1. A résztémával összefüggésben tisztázandó kérdések, illetve fókuszba állított gondolatok stratégiai szintű azonosítása

A jogalkotás jellemzőinek vizsgálata a kiberbiztonsági kihívások tükrében kulcsfontosságú a nemzetbiztonsági kihívások azonosítása és elhárítása szempontjából.[370] A

[369] A szerző saját gondolatainak vizualizációja során az ábra kizárólag grafikus elemeit a NAPKIN.AI használatával készítette el.

[370] A témával összefüggésben iránytűként használható a Tallinn Manual 2.0, ez egy a kiberműveletekre alkalmazandó nemzetközi jogról szóló átfogó kézikönyv. A kézikönyvet a NATO Kibervédelmi Kiválósági

kiberteret használják állami és nem állami szereplők is információs hadviselésre, kémkedésre, szabotázsra vagy más bűncselekmények elkövetésére, mint például adathalászat vagy zsarolóvírusos támadások (állami és civil infrastruktúrák ellen). A támadások motivációja, illetve célja az, amit legalább olyan fontos megállapítani, mint a támadással összefüggésben felderített informatikai adatokat. Mivel az egyik legfontosabb hadszíntér a kibertér[371], ezért kiemelten előbbiek miatt, a jogalkotásnak ebben a dinamikus és gyorsan változó környezetben kell megfelelő, döntően proaktív válaszokat adnia a következő szakterületeken az alábbi kérdésekre:

- Digitális helyzetkép: Miért szükséges kiemelt hadszíntérként kezelnünk a digitális teret a nemzetbiztonsági fókuszú jogalkotás terén és milyen nemzetközi stratégiai példákat vegyen alapul a jogalkotó? [372]
- Adatvédelmi szabályozás: Milyen adatvédelmi garanciákat tartalmaz a jogi szabályozás a kiberbiztonsággal összefüggésben? Megfelelően védi-e az állampolgárok adatait és magánszféráját?[373]

Központja (CCDCOE) készítette, és 2017-ben tették közzé. A Tallinn Manual 2.0 a következő főbb témákat tárgyalja: a) A kiberműveletek nemzetközi jogi kerete, b) A kiberműveletek alkalmazása a fegyveres konfliktusokban, c) A kiberműveletek alkalmazása a nemzetközi jog egyéb területein, például a nemzetközi humanitárius jogban és az emberi jogok jogában, d) A kiberműveletek végrehajtásáért való felelősség. A kézikönyv nemzetközileg elismert szakértők csoportja keze munkáját dicséri, és a nemzetközi jog legújabb fejleményeit tükrözi. A Tallinn Manual 2.0 széles körben tekintélyes forrásnak számít a kiberműveletekre alkalmazandó nemzetközi jogról. Átfogó útmutatást nyújt a kiberműveletekre alkalmazandó nemzetközi jogról. Útmutatást nyújt a kormányoknak és más érdekelt feleknek a kiberműveletek felelős és jogszerű végrehajtásában. Elősegíti a nemzetközi jog egységes értelmezését a kiberműveletek területén. Támogatja a kiberbiztonsági és kibervédelmi intézkedések fejlesztését. Emiatt a Tallinn Manual 2.0-t széles körben használják kormányok, nemzetközi szervezetek, tudósok és szakemberek a kiberműveletekre alkalmazandó nemzetközi jog megértéséhez és értelmezéséhez.

[371] KASSAI Károly: A kibertérműveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből. A tanulmányban olvasható, hogy a NATO stratégiai dokumentumai alapján a kibertérműveleti képesség szerepe, jelentősége és fókusza az idők során jelentősen fejlődött. Kezdetben a kibertér elsősorban a kommunikációs és információs technológiák területe volt a NATO számára. Azonban a 2000-es évek elejétől a kibertámadások növekvő fenyegetése miatt a kibertér egyre inkább biztonsági kérdéssé vált. A NATO reagálva erre, fokozatosan kiépítette saját kibertérvédelmi képességét, létrehozta a NATO Kibervédelmi Kiválósági Központot és a Kiberműveleti Parancsnokságot. A kibertér védelme immáron alapvető része lett a kollektív védelemnek. A legújabb, 2022-es NATO stratégiai koncepció pedig már a kibertérben zajló támadó műveletek lehetőségét is említi elrettentő és válaszcsapásként. Összességében a kibertérműveleti képesség szerepe drámaian megnőtt, a biztonság szempontjából kritikus tényezővé vált a NATO számára az elmúlt két évtizedben. A fókusz pedig fokozatosan tolódott el a védelem irányából a szükség esetén alkalmazható aktív, támadó kiberképességek kiépítése felé.

[372] KELEMEN Roland: Cyberfare State modelljei: A digitális állam lehetséges irányai, In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből, Budapest, Magyarország : Gondolat Kiadó (2023) 327 p. pp. 13-42., , 30 p.

[373] EURÓPAI PARLAMENT ÉS TANÁCS. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az unió kiberbiztonsági szintjének magas szintű közös szabályairól (NIS2). HL L 333., 2022.

- Kritikus infrastruktúra védelme: Tartalmaznak-e a jogszabályok olyan előírásokat, amelyek a kritikus információs infrastruktúra fokozottabb védelmét szolgálják kiberbiztonsági szempontból? [374]
- Szankciók és jogérvényesítés: Hatékony és elrettentő szankciókat helyez-e kilátásba a jogrendszer a kibertámadások, kiberbűncselekmények elkövetőivel szemben? Biztosítja-e a megfelelő jogérvényesítést? [375]
- Nemzetközi együttműködés: Elősegíti-e a jogi szabályozás a nemzetközi szintű kiberbiztonsági együttműködést, információmegosztást más országokkal és szervezetekkel, valamint miként mozdíthatók elő az erre irányuló törekvések?[376]
- Kiberhadviselés: Tartalmaz-e a szabályozási környezet olyan rendelkezéseket, amelyek a kibertérben zajló esetleges konfliktusok és támadások kezelésére vonatkoznak

[374] FARKAS Ádám: A kibertér műveleti tevékenységek egyes szabályozási és államszervezési alapkérdései, In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában?: Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből, Budapest, Magyarország: Gondolat Kiadó (2023) 327 p. pp. 77-95., 19 p. FARKAS Ádám tanulmánya a kibertér műveleti képességek jogi szabályozási és államszervezési hátterét elemzi. Rávilágít, hogy a kibertérben jelentkező kockázatok és fenyegetések hatékony kezeléséhez elengedhetetlen a megfelelő kibervédelmi és kiberműveleti képességek kiépítése mind nemzeti, mind nemzetközi szinten. Ismerteti a főbb nemzetközi szerződéseket, stratégiákat és együttműködéseket ezen a téren, különös tekintettel a NATO vonatkozó erőfeszítéseire. Részletesen bemutatja a kiberműveleti képességek kialakításának fő területeit, úgymint a jogszabályi felhatalmazás, a szervezeti keretek, a szakemberállomány biztosítása, valamint a megfelelő technikai eszközök és eljárások alkalmazása. Kitér az egyes országok gyakorlatára is. Farkas Ádám kiemeli, hogy össztársadalmi, összkormányzati megközelítésre és széleskörű nemzetközi együttműködésre van szükség a kibertérben jelentkező kihívások hatásos kezelése érdekében mind jogalkotási, mind végrehajtási oldalról.

[375] BARTKÓ Róbert, GÁL István László: A kibertérben megjelenő kihívások és fenyegetések büntetőjogi kezelésének tendenciái In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből, Budapest, Magyarország: Gondolat Kiadó (2023) 327 p. pp. 277-303., 27 p. Bartkó Róbert és Gál István László műve alapján kijelenthető, hogy a kibertérben megjelenő kihívások közé tartoznak a hackertámadások, az adathalászat, az online csalások, a személyes adatokkal való visszaélések és a számítógépes vírusok terjesztése. Ezek a tevékenységek nem csak egyéni felhasználókat érinthetnek, hanem vállalatokat, intézményeket és akár állami infrastruktúrákat is veszélyeztethetnek. A szerzők rámutatnak, hogy a kibertérben elkövetett bűncselekmények egyre növekvő problémát jelentenek, mivel a bűnözők kihasználják az Internet és az információs technológiák adta lehetőségeket. Ilyen bűncselekmények például a kiberzaklatás, az adatlopás, a számítógépes csalás vagy a gyermekpornográfia terjesztése. A tanulmány ismerteti a kibertérben elkövetett bűncselekményekkel kapcsolatos legfontosabb büntetőjogi kérdéseket és kihívásokat. Ilyen például a joghatóság megállapításának nehézségei, a bizonyítékok összegyűjtésének problémái vagy az elkövetők azonosításának kihívásai. A szerzők áttekintik a kibertérben elkövetett bűncselekményekkel kapcsolatos büntetőjogi szabályozás fejlődését és a legújabb tendenciákat. Bemutatják például az Európai Unió vonatkozó irányelveit és az egyes nemzeti szabályozások fő jellemzőit. A tanulmány rávilágít arra, hogy a technológiai fejlődéssel lépést tartó, hatékony büntetőjogi válaszok kidolgozása komoly kihívást jelent a jogalkotók és a jogalkalmazó szervek számára.

[376] BÁNYÁSZ Péter, TÓTH András, KRASZNAY Csaba: A kibervédelem szakpolitikai szintjének helyzete és kihívásai Magyarországon, az EU-ban és a NATO-ban, In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből, Budapest, Magyarország : Gondolat Kiadó (2023) 327 p. pp. 167-193.

nemzetbiztonsági szempontból?[377] Képesek vagyunk kellően proaktívan reagálni a szervezetfejlesztés területén is? [378] Miként „vélekednek", „hol húzzák meg a határokat" az Európai Unió jogalkotó szervei?

2. A védelmi és biztonsági szektor folyamatos éberségre ösztönzésének szükségessége

A digitalizáció kétségtelenül századunk egyik meghatározó jelensége, amely döntően változtatja meg egy ország nemzetgazdaságának működését, állampolgárai mindennapi életét. A COVID világjárvány is élesen rámutatott arra, hogy már rövid távon is csak azok az államok és társadalmak lesznek képesek helytállni a globális szintéren, amelyek az élet összes területén tudatosan alkalmazzák a digitális technológiákat. [379]

A gazdasági elemzések többsége legfontosabb kitörési pontként jeleníti meg a fejlett digitális technológiák használatát a gazdasági élet teljes spektrumában. Ez a hatás természetesen abban az esetben tud csak érvényesülni, ha az államok kormányai elkötelezik magukat a digitalizáció mellett, teljes körűen képesek megvalósítani a digitális ökoszisztéma

---

[377] SPITZER Jenő és VIKMAN László: Katonai és Nemzetbiztonsági képességfejlesztések és azok jogi, jogpolitikai háttere egyes transzatlanti államokban In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában?: Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből, Budapest, Magyarország : Gondolat Kiadó (2023) 327 p. pp. 233-260., 28 p. A szerzők áttekintik a katonai és nemzetbiztonsági képességfejlesztések jogi és politikai hátterét bizonyos transzatlanti országokban. Vizsgálják többek között az Egyesült Államok, Nagy-Britannia és Németország releváns jogszabályait és stratégiáit. Bemutatják, hogy ezekben az országokban hogyan szabályozzák és támogatják állami eszközökkel a védelmi ipar és kutatás fejlesztését. Kitérnek olyan területekre, mint a kibervédelem, a mesterséges intelligencia vagy az autonóm rendszerek alkalmazása katonai célokra. Rávilágítanak, hogy a technológiai fejlődés milyen új biztonsági kihívásokat és fenyegetéseket hoz magával, amikre reagálniuk kell ezeknek az országoknak. Összességében a tanulmány átfogó képet ad a modern hadviselés jogi és politikai környezetéről néhány kulcsfontosságú NATO tagállamban.

[378] VIKMAN László: Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi útmutató kapcsán, In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában?: Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből Budapest, Magyarország: Gondolat Kiadó (2023) 327 p. pp. 97-105., 9 p. Vikman László írásában a kiberbiztonsági stratégiák nemzetközi szintű fejlesztésére vonatkozó irányelveket elemzi. Rávilágít, hogy a digitális tér védelme hatékonyan csak nemzetközi összefogással valósítható meg, hiszen a kibertámadások gyakran átlépik az országhatárokat. Kiemeli a NATO és az Európai Unió szerepét a tagállamok kibervédelmi képességeinek összehangolásában és erősítésében. Javaslatokat fogalmaz meg egy átfogó, nemzetközi kiberbiztonsági stratégiai keretrendszer kialakítására. Ennek elemei lehetnének többek között: közös fenyegetettség-értékelési módszertan, információmegosztási protokollok, incidenskezelési eljárások, kritikus infrastruktúra védelmi ajánlások, képességfejlesztést célzó programok, kibervédelmi technológiai együttműködések. Leszögezi, hogy a digitális tér biztonsága közös érdek, így a kibervédelem terén elengedhetetlen a széleskörű nemzetközi partnerség, a bevált gyakorlatok megosztása és a kölcsönös segítségnyújtás.

[379] KER, D. – MONTAGNIER, P. – SPIEZIA, V. (2021): Measuring Telework in the COVID-19 Pandemic. OECD Digital Economy Papers, No. 314. OECD Publishing, Paris. (Elérhető: https://doi.org/10.1787/0a76109f-en)

hiányosságainak, lemaradásainak felszámolását célul kitűző beruházásokat és egy ezt támogató (jogi) normakörnyezetet alakítanak ki.

Lehetséges-e a védelmi és biztonsági ágazat feletti ellenőrzés legfontosabb eszközeit automatizálni, ráadásul meghatározott digitális eszközök adatai alapján, melyeket a mesterséges intelligencia vélhetően nem is ismer teljes egészében? Minden állam elemi érdeke, hogy ne digitalizáljon minden adatát, hiszen, ha az adat érvényességi időn belüli nyilvánosságra hozatala, jogosulatlan megszerzése, módosítása vagy felhasználása, illetéktelen személy részére hozzáférhetővé, valamint az arra jogosult részére hozzáférhetetlenné tétele közvetlenül és tartósan sérti vagy veszélyezteti Magyarország szuverenitását, területi integritását, törvényes rendjét, belső stabilitását, vagy visszafordíthatatlanul jelentős károkat okoz az ország honvédelmi, nemzetbiztonsági, bűnüldözési, igazságszolgáltatási, központi pénzügyi és gazdasági érdekeiben, külügyi és nemzetközi kapcsolataiban, a szövetséges tagállamokkal közös biztonsági érdekeiben, akkor ezeknek a védelme érdekében indokolt lehet az, hogy ne legyenek „betáplálva" egy döntéselőkészítő rendszerbe, vagy egy nemzetközi szerződésen alapuló együttműködés keretein belül működő adatbázisba.

Az államok jogos és jogszerű önvédelme érdekében folytatott hatékony ellenőrző feladatok, valamint a védelmi és biztonsági tevékenységet ellátó szervek szenzitív adatokat kezelő tevékenysége közötti egyensúlyt célszerű fejleszteni úgy, hogy a minősített adatok megismerésére jogosultak köre, az eljárás nyilvánossága a szükséges mértékben korlátozható maradjon. Minden egyes eset jogszerűségének vizsgálatára kiterjedő, külső szerv hatáskörébe tartozó, hatékonynak minősíthető eljárás keretében végezhető ellenőrzésről szóló törvényi szabályozás nélkül a magánéletbe való állami beavatkozás aránytalan korlátozásnak minősülhet, az általam végzett kutatás, megismert szakirodalom alapján a humán kontroll nélküli döntések ebbe a körbe tartoznának, így ez jelenti a mesterséges intelligencia alkalmazhatóságának határát.[380]

Enélkül ugyanis nincsen biztosítva annak a mérlegelésnek a független felülvizsgálása, amely a magánélet titkos eszközökkel való kifürkészésének szükségességéről, arányosságáról és célhoz kötöttségéről szól. A bíróságra tartozó kérdés az, hogy a titkos információgyűjtés

[380] A témával összefüggésben organikus fogalom evolúcióra például lásd: AMODEI, Dario – OLAH, Chris – STEINHARDT, Jacob – CHRISTIANO, Paul – SCHULMAN, John – MANÉ, Dan (2016): Concrete Problems in AI Safety. arXiv preprint arXiv:1606.06565.

tervezett alkalmazásával elhárítani kívánt veszély és a magánélete rejtett megfigyelését elszenvedni kényszerülő személynek okozott hátrány a konkrét esetekben arányban áll-e. Ugyanakkor a politikai, illetve diplomáciai súllyal bíró ügyek esetében az engedélyezést továbbra is a választópolgárok által megválasztott Országgyűlés által támogatott Kormány felelősségi körében indokolt tartani.

Nyilván az információ és adatkezelési redundancia hiánya, illetve az adatfúzió okozta központosítás okozhatja még a teljes kompromitálódást is a védendő adatok vonatkozásában.

A megalapozott döntésekhez pedig a rendelkezésre álló összes adat ismerete és szakértői felhasználása szükséges, amely nagyon komoly előrelátást is igényel a gépi tanulás útján is megszerezhető tapasztalat és lexikális tudás mellett.

Utóbbiak birtokában jelentős előnyre tehet szert a rendvédelmi, illetve nemzetbiztonsági ágazat, különösen egy információfúziót végző szerv, azonban a felhatalmazással járó kiemelt felelősség kérdésének vizsgálata során nem szabad elfeledni Lukács evangélista által figyelmünkbe ajánlottakat: „*Mind kinek sokat adtak, sokat kérnek tőle; és akire sokat bíztak, attól többet kívánnak.”*[381]

3. Állampolgárok, illetve felhasználók jogi eszközökkel biztosított védelme a digitális térben

Előbbiekkel összefüggésben érdemes vizsgálni a közösségi médiát uraló technológiai, illetve digitális óriások szerepét az adatanalitikában. Hiszen az üzleti szempontú adatgyűjtés mellett a politikai folyamatok befolyásolására alkalmas képesség (multinacionális vállalatok, illetve technológiai óriáscégek digitális térben végzett tevékenységének) állami kontrollja a jövőben lényegében az Európai Unió jogalkotásának (különösen a Digital Services Act-nak, a továbbiakban: DSA[382]) köszönhetően 2023. november 16-ától jelentősen változott, mely akár választásokat is befolyásoló tényezővel bírhat.

[381] Lukács Könyve 12:48
[382] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

A digitális szolgáltatásokról szóló jogszabály olyan átfogó új szabályrendszer, amely szabályozza az EU-n belül közvetítőként eljáró digitális szolgáltatások felelősségét a fogyasztók árukkal, szolgáltatásokkal és tartalommal való összekapcsolása terén. Ebben az összefüggésben a „digitális szolgáltatások" olyan online platformokra utalnak, mint a piacterek és a közösségimédia-hálózatok. A digitális szolgáltatásokról szóló (DSA) jogszabály egyértelmű átvilágítási kötelezettségeket határoz meg az online platformok és más online közvetítők számára.[383] Az új előírások[384] értelmében például bármely felhasználó megjelölheti a jogellenes tartalmakat, és egyértelmű eszközökkel is rendelkezhet a platformok tartalommoderálásának kifogásolására, mind a platformon, mind pedig az országában működő peren kívüli eljárásokon keresztül. A jogszabály a megbízhatónak tartott bejelentőkkel és az illetékes hatóságokkal való együttműködésre vonatkozó intézkedéseket is megjelenít, valamint olyan intézkedéseket, amelyek elrettentik a tisztességtelen kereskedőket attól, hogy elérjék a fogyasztókat. Nagyobb átláthatósági követelményeket támaszt az online platformok számára a tartalom eltávolításával és moderálásával, valamint a hirdetésekkel kapcsolatos döntések tekintetében.

Felismerve az online óriásplatformok gazdaságunkra és társadalmunkra gyakorolt különleges hatását, a DSA jogszabály magasabb szintű átláthatóságot és elszámoltathatóságot határoz meg arra vonatkozóan, hogy az ilyen platformok szolgáltatói hogyan vizsgálják és moderálják az információkat. Ellenőrzött kockázatkezelési kötelezettségeket állapít meg a legtöbb felhasználót elérő és a legnagyobb társadalmi kockázatot jelentő online platformok számára. A digitális szolgáltatásokról szóló jogszabály mind a polgárok, mind a vállalkozások számára védelmet nyújt a jogalkotó álláspontja szerint. Emellett egyenlő védelmet nyújt az EU valamennyi felhasználójának, mind az illegális árukkal, tartalmakkal vagy szolgáltatásokkal szembeni biztonságuk, mind pedig alapvető jogaik tekintetében.[385]

A jogi normával szemben támasztott várakozások szerint a DSA segít abban, hogy valóban európai irányítási rendszer működjön az internetes szolgáltatások tekintetében. A

[383] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC forrás: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:32022R2065 (A letöltés ideje: 2023. 07. 31. 9:19)
[384] Elérhető: https://digital-strategy.ec.europa.eu/hu/node/10356/printable/pdf (A letöltés ideje: 2023. 07. 31. 9:30)
[385] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) elérhető: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014 (A letöltés ideje: 2023. 07. 31. 9:30)

felügyeleti és végrehajtási mechanizmus célja az egységes piac megerősítése és a tagállamok közötti hatékony együttműködés lehetővé tétele.[386] Azt is biztosítja, hogy a digitális szolgáltatási koordinátorok hálózatán és a Digitális Szolgáltatások Európai Testületén keresztül gyors uniós szintű beavatkozás kezelje az egész EU-ra kiterjedő problémákat.

Az online platformok és digitális szolgáltatások az elmúlt években mélyen beágyazódtak mindennapi életünkbe, gazdaságainkba, társadalmainkba és demokráciáinkba. Ezek a platformok jelentős hatást gyakorolnak arra, hogy miként értjük és értelmezzük a világot körülöttünk, beleértve a hírek fogyasztását és az információáramlást. Ennek következtében felmerült az igény arra, hogy a digitális szolgáltatások működését szabályozó jogszabályokat felülvizsgálják és modernizálják, hogy jobban megfeleljenek a digitális kor kihívásainak.

A digitális szolgáltatásokról szóló új jogszabály komplex keretet teremt, amely horizontális szabályokon alapul, célja pedig az elszámoltathatóság, az átláthatóság és a nyilvános felügyelet biztosítása. Ezek a szabályok kifejezetten arra irányulnak, hogy átláthatóbbá tegyék, hogyan moderálják az online platformok a tartalmakat, hogyan kezelik a hirdetéseket és hogyan alkalmaznak algoritmikus folyamatokat. Ezáltal növelik a nagy technológiai vállalatok felelősségét és elszámoltathatóságát, különösen a jogellenes tartalmak és termékek kezelése, valamint a közérdek, az alapvető jogok, a közegészség és a biztonság védelme terén.[387]

Az új jogi norma értelmében a technológiai óriásoknak értékelniük kell azokat a kockázatokat, amelyeket rendszereik jelentenek, és megfelelő intézkedéseket kell kidolgozniuk a manipulatív technikák és egyéb kockázatok elkerülése érdekében. Ezenfelül a jogszabály lehetőséget biztosít a felhasználóknak arra, hogy megtámadják a platformok döntéseit, például a tartalom eltávolításával vagy címkézésével kapcsolatban, és független ellenőrzést tesz lehetővé az ellenőrzési jelentések és a kutatók számára biztosított adathozzáférés révén.

[386] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC forrás: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:32022R2065 (A letöltés ideje: 2023. 07. 31. 9:19)
[387] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) elérhető: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014 (A letöltés ideje: 2023. 07. 31. 9:30)

Összességében elmondható, hogy a digitális szolgáltatásokról szóló új jogszabály jelentős lépés a digitális kor kihívásainak kezelésében, és hozzájárul az online tér átláthatóságának, elszámoltathatóságának és biztonságának javításához, miközben lehetőséget biztosít a felhasználók számára, hogy hatékonyabban érvényesítsék jogos érdekeiket az online platformokkal szemben. [388]

A biztonsági szektorban megjelenő korlátozások és a jogterület komplexitása fényében a jogi sérülékenységvizsgálat egy kiemelten fontos eszköz a nemzetbiztonság szempontjából. Ez a folyamat különösen a különleges jogrend idején hozott jogszabályok esetében vált kiemelt jelentőségűvé, amikor a civil szervezetek és a sajtó aktívan vizsgálta és feltárta az érintett jogszabályok hiányosságait és potenciális veszélyforrásait.

A jogi sérülékenységvizsgálat nem csupán az alapjogok érvényesülésének felülvizsgálatára szolgál, hanem egyfajta előkészítő lépés is lehet a célzott támadások, vagyis a lawfare – azaz a jogi eszközökkel folytatott hadviselés – alkalmazásához. Ez a stratégia a modern hibrid hadviselés egyik kulcsfontosságú eleme, amely a láthatatlan fegyverek alkalmazását jelenti a nemzetközi színtéren.

A lawfare alkalmazása során a hadviselő felek a modern technológiák és eszközrendszerek által nyújtott lehetőségeket használják fel, és műveleteiket kiterjesztik az online térre, a médiára, a gazdaságra, valamint a társadalmi érintkezés különböző formáira – különösen az online közösségi felületekre. Ezek a tevékenységek önállóan vagy kombinatívan alkalmazva, a klasszikus támadási formák nélkül is alkalmasak lehetnek befolyásolásra, gazdasági csapásmérésre, államok belső békéjének megzavarására vagy társadalmi tudat változtatására.

Magyarország számára a hibrid fenyegetések elleni határozott fellépés és kezelés kiemelt feladattá vált, amit a hatályos NBS-ben is rögzítenek. Ugyanakkor a lawfare fogalmának jelentése és a potenciális veszélyforrás alapvető tulajdonságai még új területek a jogalkotók és a legtöbb szakmai szervezet számára. Ezért fontos, hogy a jogalkotás és a szakmai gyakorlat fokozatosan alkalmazkodjon és reagáljon az ilyen típusú fenyegetettségek növekvő szintjére,

[388] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC forrás: https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=CELEX:32022R2065 (A letöltés ideje: 2023. 07. 31. 9:19)

és megfelelő stratégiákat, szabályokat alakítson ki a lawfare és más hibrid fenyegetések hatékony kezelésére.

A digitális szolgáltatásokról szóló jogszabály[389] szilárd mechanizmust hoz létre a digitális szolgáltatások, különösen a társadalmunk számára legnagyobb kockázatot jelentő online platformok és online óriásplatformok felügyeletére. A mechanizmus magában foglalja a segítségnyújtás, az átláthatóság és az uniós szintű beavatkozás rugalmas kombinációját annak biztosítása érdekében, hogy a digitális szolgáltatások kihívást jelentő felügyelete minden körülmények között hatékony maradjon. A hatóságok rendelkezésére áll majd egy közös vizsgálati mechanizmus. Például, ha egy tagállamnak segítségre van szüksége az információs aszimmetriák és a technikai szakértelem korrigálásához egy online óriásplatform összetett ajánlójának vagy hirdetési rendszerének vizsgálata során, vagy ha a kockázatok és jogsértések különösen egy másik tagállamot érintenek.

Minden tagállamnak közvetlen csatornája lesz arra, hogy bejelentse a területén felmerülő problémákat, és segítséget kérjen az online platform székhelye vagy jogi képviselője szerinti tagállam illetékes digitális szolgáltatási koordinátorától. Az online óriásplatformok által elkövetett jogsértések esetében a Bizottság közvetlen felügyeletet és szankcionálást biztosíthat. Ezenkívül a Digitális Szolgáltatások Európai Testülete keretében folytatott napi szintű együttműködés fontos szerepet fog játszani a tagállamok és a Bizottság közötti információáramlás biztosításában, valamint annak biztosításában, hogy a végrehajtási tapasztalatokból és a felmerülő kérdésekből levont szakpolitikai tanulságok valamennyi tagállamot támogassák.[390]

Előbbi, a digitális térben közzétett tartalmakat a szükséges mértékben, de mégis jelentősen befolyásoló jogi mechanizmussal összefüggésben fontos megjegyezni, hogy az Internet és a szólásszabadság korlátozása nemzetbiztonsági okokból egy nagyon érzékeny

[389] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) elérhető: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014 (A letöltés ideje: 2023. 07. 31. 9:30)

[390] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) elérhető: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014 (A letöltés ideje: 2023. 07. 31. 9:30)

szabályozási területet fed le[391], ugyanakkor tekintettel a kibertérből érkező fenyegetések folyamatosan növekvő, illetve súlyosbodó kvalitatív és kvantitatív jellemzőjére, elengedhetetlenül szükséges a jogalkotás eszközeit is hatékonyan alkalmazni.

Előbbiekkel összefüggésben természetesen a véleménynyilvánítás szabadsága érvényesülésének kérdése továbbra is nyitott marad, hiszen döntések születnek majd arról, hogy mi a jó és mi a rossz vélemény. Eldől majd, hogy ki a megbízható és ki a nem megbízható felhasználó. Az igazság és a tények keresése, vizsgálata egy rendkívül energiaigényes folyamat, és tisztában kell lennünk azzal, hogy hosszú és rögös utat választ az, aki ezeket igyekszik megtalálni, különösen a digitális térben, a véleménybuborékok világában.

A véleménynyilvánítás szabadsághoz fűződő általános jogot Magyarországon az Alaptörvény IX. cikke biztosítja. Magyarországon a véleménynyilvánítás szabadsága hagyományosan magas szintű alapjogi védelemben részesül: az Alkotmánybíróság ítélkezési gyakorlata az alapvető jogok rendszerében kiemelt jelentőséget tulajdonít a véleménynyilvánítás szabadságának, hiszen a véleménynyilvánítás, a szólás és a sajtó szabadsága alapvető előfeltételei a demokratikus közvélemény kialakulásának és fenntartásának. Az Alaptörvény IX. cikk (2) bekezdése értelmében „*Magyarország elismeri és védi a sajtó szabadságát és sokszínűségét, biztosítja a demokratikus közvélemény kialakulásához szükséges szabad tájékoztatás feltételeit*". Az Alaptörvény a sajtószabadság érvényesítésével összefüggésben nagy jelentőséget tulajdonít a sokszínűség biztosításának és a tájékoztatási monopóliumok létrehozatala megakadályozásának. Ez a szövegezés tevőleges kötelezettséget ró az államra: az államnak tartózkodnia kell a jogsértéstől, de meg is kell tennie a szükséges lépéseket a sajtószabadság biztosításához. [392]

---

[391] GOSZTONYI Gergely: Az államok által végzett internetkorlátozás különböző eszközei, mint nemzetbiztonsági és szólásszabadsági kockázatok, In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában?: Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből, Budapest, Magyarország: Gondolat Kiadó (2023) 327 p. pp. 135-148., 14 p. Gosztonyi Gergely tanulmánya az állami internetkorlátozás eszközeit vizsgálja nemzetbiztonsági és szólásszabadsági szempontból. Rávilágít, hogy bár az államoknak legitim érdeke fűződhet a káros online tartalmak kiszűréséhez, az alkalmazott módszerek gyakran aránytalanul korlátozzák a szólásszabadságot és magánélethez való jogot. Az internetlezárások, a közösségi média manipulálása vagy a tömeges megfigyelés veszélyezteti a demokratikus vitát. Ugyanakkor a szerző szerint léteznek enyhébb eszközök is az ártalmas jelenségek visszaszorítására, például a lakosság digitális műveltségének erősítése. Az állami szabályozásnak arányosnak és átláthatónak kell lennie, bírói vagy parlamenti kontrollal. Gosztonyi leszögezi, hogy az internetkorlátozás dilemmája nem oldható meg kizárólag technokrata módon. A demokratikus értékek védelme a társadalom minden szereplőjének feladata kell, hogy legyen.

[392] A Nemzeti Média- és Hírközlési Hatóság egy önálló szabályozó szerv, amely kizárólag a törvénynek van alárendelve. A Médiatanács és tagjai szintén csak a törvénynek vannak alárendelve, és tevékenységük körében

A sajtószabadságra vonatkozó részletes rendelkezéseket a sajtószabadságról szóló törvény és a médiatörvény tartalmazza. A médiaszolgáltatások szabadon nyújthatóak és a sajtótermékek szabadon kiadhatóak, a médiaszolgáltatások és sajtótermékek tartalma pedig szabadon határozható meg.

4. Hazai kibervédelmi helyzetkép a Nemzeti Digitalizációs Stratégia tükrében

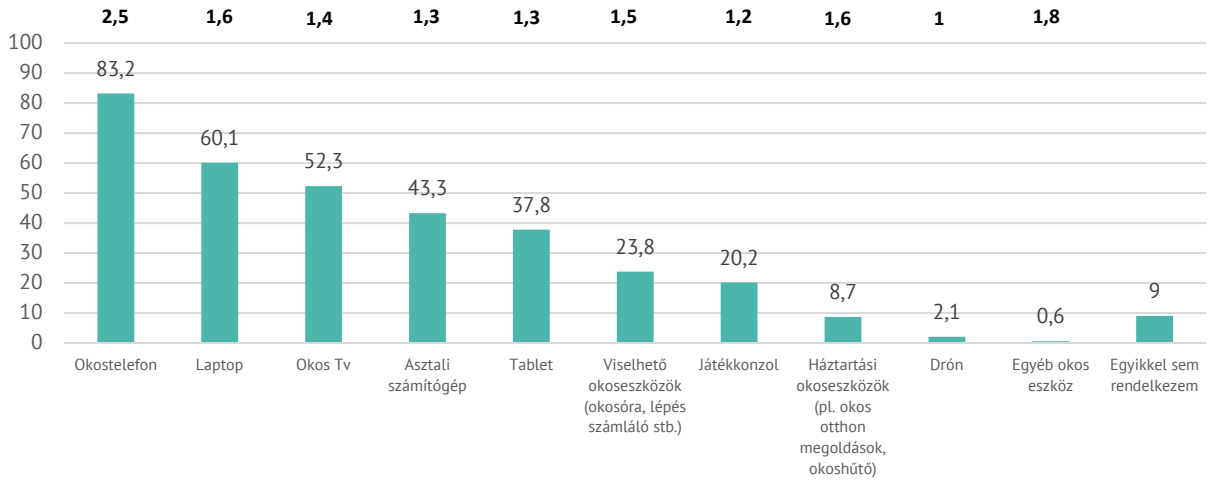
Magyarország az elmúlt évek során jelentős előrelépést tett, és ez a digitalizáció területén is érzékelhető. Az országban teljes körűen kiépítették a gyors internet-hálózatot, ami lehetővé tette, hogy az otthonok száz százaléka elérhetővé váljon a modern internetkapcsolat számára, szemben az előző 50%-os lefedettséggel. Az internetet aktívan használó háztartások aránya 2010 óta 5%-ról több mint 87%-ra ugrott, ami hozzájárult ahhoz, hogy az online világtól elszigetelten élők száma harmadára csökkenjen, mostanra alig meghaladva a 12%-ot. A digitális technológiákat hatékonyan alkalmazó vállalkozások száma is bővült, amelyek a vállalati kommunikáció minden területén kihasználják ezeket a lehetőségeket. Az állami szektorban is pozitív változások történtek: az egykor széttöredezett és hatástalan informatikai fejlesztéseket sikerült egy koherens és erős állami irányítás mellett optimalizálni és összehangolni. [393] A digitalizáció kiemelten államigazgatási célú alkalmazásának számos területe közül az adatanalitika és a döntéselőkészítés, esetleges döntéshozatal vonatkozásában fontos megjegyeznünk, hogy *„a technológiai fejlődés a joggal szemben ambivalens követelményeket támaszt: egyrészről a jog szabályainak újragondolását indukálja annak érdekében, hogy a technológiai fejlődés ne ássa alá az emberi szabadságjogokat. Ugyanakkor azt is biztosítani kell, hogy a jog ne akadályozza a technológiai fejlődést."* [394] Ez a kettősség határozza meg szűkebb értelemben vett jogalkalmazói és a jogalkotói döntéseket támogató

nem utasíthatók. A médiatörvény rendelkezései biztosítják a médiaszolgáltatók felügyeleti szerveinek demokratikus és átlátható módon történő kinevezését a nemzetközi standardoknak megfelelően. A Médiatanács elnökét és négy tagját az Országgyűlés kilencéves időtartamra választja, a jelen lévő képviselők kétharmados többségével. A megbízatás hosszát ellensúlyozza az a tény, hogy a Médiatanács elnökének és tagjainak újraválasztására nincs lehetőség. A pártok közötti konszenzus elérése céljából a jelöltállítási folyamatban a jelölőbizottságnak először egyhangú határozatott kell hoznia; egyhangúság hiányában kétharmados többség szükséges, ami széles körű konszenzus kialakítását kényszeríti ki. A Médiatanács tagja nem folytathat pártpolitikai tevékenységet, párt nevében nyilatkozatot nem tehet, nem lehet párt országos vagy területi szervezetének tisztségviselője vagy politikai párttal foglalkoztatásra irányuló jogviszonyban álló személy.

[393] MAGYARORSZÁG KORMÁNYA. Nemzeti Digitalizációs Stratégia 2022–2030. Innovációs és Technológiai Minisztérium, 2022.

[394] KLEIN Tamás – TÓTH András: A robotika egyes szabályozási kérdései. In: Homicskó Árpád Olivér (szerk.): Egyes modern technológiák etikai, jogi és szabályozási kihívásai. Budapest, 2018, Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar, 94. o.

védelmi és biztonsági funkciókat is. Nemzeti Digitalizációs Stratégia[395] elkészítésének Századvég Konjunktúrakutató Zrt. által elkészített felmérés egyik kérdése az volt, hogy az *„alábbiak közül milyen eszközökkel rendelkezik Ön, illetve a háztartás, amelyben Ön él?”* (Említések, %) Ennek eredményét a kutatóintézet az alábbiak szerint jelenítette meg:



3. ábra Digitális eszközökkel való ellátottság, Forrás: Századvég (In.: Nemzeti Digitalizációs Stratégia 2022-2030)

A Századvég Konjunktúrakutató Zrt. által végzett kutatás[396], amely a Nemzeti Digitalizációs Stratégia kidolgozásához járult hozzá, értékes betekintést nyújt a magyar háztartások digitális eszközhasználatának jelenlegi állapotába. A kutatás fő megállapítása, hogy az okostelefonok rendkívül magas megjelenési aránnyal rendelkeznek Magyarországon, ami a digitális infrastruktúra és a modern kommunikációs eszközök elterjedtségének fontos jelzése. Az okostelefonok az elmúlt években az egyik legnépszerűbb digitális eszközzé váltak, és ez a tendencia Magyarországon is megfigyelhető. A kutatás szerint az okostelefonok használata a lakosság körében 85,7%-os, ami azt jelenti, hogy 100 lakosra vetítve átlagosan 2,5 okostelefon van egy háztartásban. Ez a magas arány azt mutatja, hogy az okostelefonok széles körben hozzáférhetők és használatosak az országban, ami a digitális kommunikáció és információáramlás alapvető eszközeivé teszi őket. [397]

[395] MAGYARORSZÁG KORMÁNYA. Nemzeti Digitalizációs Stratégia 2022–2030. Innovációs és Technológiai Minisztérium, 2022.
[396] Forrás: https://kormany.hu/dokumentumtar/nemzeti-digitalizacios-strategia-2022-2030; (letöltés 2023. 06.21.)
[397] MAGYARORSZÁG KORMÁNYA. Nemzeti Digitalizációs Stratégia 2022–2030. Innovációs és Technológiai Minisztérium, 2022.Forrás: Nemzeti Digitalizációs Stratégia, elérhető: https://njszt.hu/sites/default/files/news/2022/Nemzeti%20Digitaliz%C3%A1ci%C3%B3s%20Strat%C3%A9gia.pdf (letöltés: 2023.06.21.)

A laptoppal és okos Tv-vel rendelkező háztartások aránya is jelentős, ami a számítástechnika és a digitális szórakoztatás terén folyamatban lévő változások egyik jellemzője.[398] Az asztali számítógépek visszaszorulása a hordozható és multifunkcionális eszközök, mint az okostelefonok, laptopok és tabletek népszerűségének növekedésével magyarázható. A viselhető okoseszközök és játékkonzolok terén tapasztalható alacsonyabb megjelenés azt mutatja, hogy ezek az eszközök még nem váltak a mindennapi élet elválaszthatatlan részévé minden háztartásban, és a digitális szórakoztatás és egészségügyi technológiák terén további fejlődési lehetőségek állnak rendelkezésre.

Az okosotthonhoz szükséges eszközök alacsony birtoklási aránya szintén azt jelzi, hogy ez a terület még kevésbé elterjedt, ami újabb fejlesztési lehetőségeket kínál a jövőbeni digitalizációs stratégiák számára. A Századvég kutatási eredményei rávilágítanak a digitális eszközök és technológiák magyarországi elterjedtségének és használatának jelenlegi állapotára, valamint a további fejlődési lehetőségekre, amelyek kulcsfontosságúak a jövőbeli digitalizációs stratégiák és politikák kialakításában. [399]

A legmodernebb Virtual Reality eszközök (különösen a szemüvegek) fejlesztése és árusítása mellett, már a felhasználót (egy mágneskártyához hasonlatos módon) azonosító okosgyűrűk fejlesztését is bejelentette az egyik legjelentősebb technológiai óriáscég. A különböző okoseszköz implantátummá válása is megtörtént már kísérleti jelleggel, egyes számítógépes játékok, sci-fi regények, filmek legmerészebb álmait megvalósítva.

Az előbbi kutatásban is megjelenített adatok alapján kijelenthető, hogy az informatikai- és kiberbiztonsági helyzet a szükséges védelem megszervezésének komplexitása évről-évre egyre komolyabb kihívások elé állítja az érintetteket. A felhasználók számának növekedése, az Internetre kapcsolódó (IoT) eszközök tömegessé válása többek között jelentősen növelik a kibertámadások valószínűségét. [400]

---

[398] MAGYARORSZÁG KORMÁNYA. Nemzeti Digitalizációs Stratégia 2022–2030. Innovációs és Technológiai Minisztérium, 2022.

[399]MAGYARORSZÁG KORMÁNYA. Nemzeti Digitalizációs Stratégia 2022–2030. Innovációs és Technológiai Minisztérium, 2022.
Forrás: Nemzeti Digitalizációs Stratégia, elérhető: https://njszt.hu/sites/default/files/news/2022/Nemzeti%20Digitaliz%C3%A1ci%C3%B3s%20Strat%C3%A9gia.pdf (letöltés: 2023.06.21.)

[400] A kibertér és az információ fegyverként értelmezése kapcsán például lásd: SIMON László – MAGYAR Sándor: A terrorizmus és indirekt hatása a kibertérben. In: Nemzetbiztonsági Szemle, 5. évf. 2017/3. szám, 89–101. o.

A hazai kibervédelmi helyzetkép elemzésekor fontos figyelembe venni a Nemzeti Digitalizációs Stratégia (NDS) előírásait és célkitűzéseit. A stratégia célja Magyarország digitális átalakulásának elősegítése, miközben biztosítja az információbiztonságot és a kibervédelmet. Az NDS keretében a kibervédelem kiemelt területként szerepel, hiszen a digitalizáció növekedésével arányosan emelkedik a kiberfenyegetések száma és komplexitása is. A stratégia célja, hogy Magyarország képes legyen megfelelően reagálni a kiberfenyegetésekre, megvédje az állami és magáninfrastruktúrákat, valamint növelje a lakosság kiberbiztonsági tudatosságát.[401]

A hazai kibervédelmi intézkedések között szerepelnek:

- Az információbiztonsági szabályozás folyamatos frissítése, hogy megfeleljen a modern kihívásoknak.
- A kiberbiztonsági incidenskezelési képességek fejlesztése, beleértve az incidensekre való gyors reagálást és helyreállítást.
- A kritikus infrastruktúrák védelmének erősítése, különös tekintettel az energia-, közlekedési és pénzügyi szektorokra.
- A kiberbiztonsági tudatosság és képzés növelése a lakosság és a vállalatok körében.
- Együttműködés az EU és NATO kibervédelmi kezdeményezéseivel, valamint más nemzetközi és regionális szervezetekkel.

A kibervédelmi helyzetkép folyamatosan változik, hiszen új technológiák és fenyegetések jelennek meg. Az NBSZ Nemzeti Kibervédelmi Intézet (NKI) és más illetékes szervek rendszeres jelentéseiben tájékoztatják a nyilvánosságot és a döntéshozókat a legfrissebb fejleményekről, kihívásokról és a védekezési intézkedésekről. Fontos megjegyezni, hogy az

MAGYAR Sándor – SIMON László: A terrorizmus és indirekt hadviselés az EU kiberterében. In: Szakmai Szemle, XV. évf. 2017/4. szám, 57–68. o. SIMON László: Az információ mint fegyver? In: Szakmai Szemle, XIV. évf. 2016/1. szám, 34–60. o., KELEMEN Roland: Cyber Attacks and Cyber Intelligence in the System of Cyber Warfare. In: SZABÓ Miklós (szerk.): Doktoranduszok Fóruma Miskolc, 2016. november 17. Állam- és Jogtudományi Kar szekciókiadványa, Miskolc, Miskolci Egyetem, 2017, 117–122. o., KELEMEN Roland – SIMON László: A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái. In: FARKAS Ádám – VÉGH Károly (szerk.): Új típusú hadviselés a 21. század második évtizedében és azon túl – intézményi és jogi kihívások, Budapest, Zrínyi Kiadó, 2020, 150–170. o., KELEMEN Roland – FARKAS Ádám: To the Margin of the Theory of a New Type of Warfare: Examining Certain Aspects of Cyber Warfare. In: SZABÓ Marcel – GYENEY, Laura – LÁNCOS, Petra Lea (szerk.): Hungarian Yearbook of International Law and European Law (2019), Den Haag, Eleven International Publishing, 2020, 203–226. o.

[401] MAGYARORSZÁG KORMÁNYA. Nemzeti Digitalizációs Stratégia 2022–2030. Innovációs és Technológiai Minisztérium, 2022.

NDS a dinamikus digitális környezethez való alkalmazkodás mellett hangsúlyozza a proaktív lépéseket is, mint például az új technológiák biztonságának beépítését már a fejlesztési fázisban (security by design), valamint az oktatás és képzés folyamatos fejlesztését a digitális kor követelményeinek megfelelően.

A kibervédelmi helyzetkép javításának eredményeként a magyarországi szervezetek és állampolgárok jobban felkészültek a kiberfenyegetésekkel szemben. A kiberbiztonsági incidensek száma csökken, és a szervezetek hatékonyabban tudnak reagálni a kiberfenyegetésekre. Ugyanakkor a kibervédelmi helyzetkép javításának számos kihívása van. Ezek közé tartozik például a kiberfenyegetések egyre növekvő száma és komplexitása, valamint a kiberbiztonsági szakemberek hiánya. Emiatt a kormányzat elkötelezett a kibervédelmi helyzetkép folyamatos javítása mellett. A jövőben a kormányzat további intézkedéseket tervez a kiberbiztonsági képességek fejlesztése, a kiberbiztonsági infrastruktúra fejlesztése és a kiberbiztonsági tudatosság növelése érdekében.

5. A hazai normatív környezet jelentős változásai az elmúlt években

Magyarország az EU tagországok közül előkelő helyen áll a modern kiberbiztonsági jogszabályi környezet kialakításában[402], az Európai Unió által hozott védelmi rendeletek és irányelvek implementálásában. Az elmúlt években kialakította az állami- és önkormányzati szervezetek hatósági- és incidenskezelési szervezeti rendszerét, a szervezetrendszerbe bevonta az EU vonatkozó (NIS2) irányelvében meghatározott szervezeteket, kijelölte a Magyarország létfontosságú rendszereit és a kijelölő hatóságok által meghatározott alapvető szolgáltatást nyújtó szereplőket, megteremtette azok védelmi feltételeit. Részben az állami-, de különösen az önkormányzati rendszerek esetében megállapítható, hogy azok egy részénél a jogi normában előírt adminisztratív kötelezettségeiken és azok végrehajtásán túl egyéb védelmi és biztonsági intézkedéseket nem, vagy csak kis mértékben hoznak. A helyi normakörnyezet felülvizsgálata, naprakészen tartása vagy betartatása bizonyos esetekben nehézségekbe ütközhet, azonban a

[402] Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1163/2020. (IV. 21.) Korm. határozat kifejezetten előírja, hogy a biztonság egyes részterületeiért felelős állami szervezeteknek a Stratégiában megfogalmazott iránymutatásokkal összhangban kell megalkotniuk és felülvizsgálniuk a tevékenységükre vonatkozó szakági szabályzókat, különös tekintettel a nemzeti katonai, a rendészeti, a nemzetbiztonsági, a terrorelhárítási, a katasztrófavédelmi, a kiberbiztonsági és a migrációs területekre. Mindezt úgy kell elvégezni, hogy a hatályos NBS rendelkezéseit is a korábban említett, folyamatos felülvizsgálati kötelezettség terheli, így amennyiben valamely érintett szerv hatáskörében erre okot adó körülményt derít fel, jeleznie szükséges azt az irányító tárc(áj)a felé, hogy a szükséges normaalkotás kezdeményezhetővé váljon.

cselekvési terveikben meghatározott képességnövelési lépések erőforrás hiányában sok esetben elmaradnak.

Az egyre nagyobb léptékben haladó digitalizáció kontrollja mellett, fontos megjegyezni azt is, hogy a bírósági eljárás meghatározott lépéseinek elektronizálása az igazságszolgáltatási rendszerek minőségének meghatározó elemét képezik, hiszen a procedúrák elektronikus megindítása, az előrehaladásának online nyomon követhetősége elősegítik az igazságszolgáltatáshoz való állampolgári hozzáférést, valamint csökkentik a késedelmeket és a költségeket. A bíróságok elektronikus iratkezelési rendszerei egyre növekvő szerepet játszanak a nemzetközi együttműködésben, az igazságügyi hatóságok közötti határokon átnyúló feladatok végrehajtásában. Elősegítik az uniós jogszabályok végrehajtását, például a kis értékű követelésekkel kapcsolatos eljárások vonatkozásában.[403] A területen fontos innovációnak tekinthetjük ma már az elektronikus cégeljárások ügyeinek intézési lehetőségeit, egyelőre azonban egyes folyamatok csak részben vannak digitalizálva. Negatívum egyelőre a közjegyzők digitalizációs szintjének alacsony volta is, pozitívnak tekinthető viszont, hogy az ügyvédek elektronikus aláírási szintje a járvány hatására tovább növekedett.

A normatív fejlesztések középpontjában a NIS2 (Network and Information Systems) irányelv implementációjához szükséges jogszabályi módosítások állnak. [404] A NIS2 irányelv az Európai Unió jogalkotói tevékenysége keretében kidolgozott jogszabály, amelynek célja az információs rendszerek és hálózatok biztonságának növelése az EU-n belül.[405] A magyarországi implementáció során történő jogszabály-módosítások elősegítik az irányelv követelményeinek megfelelő nemzeti szintű megvalósítást, különös tekintettel a kritikus infrastruktúrák védelmére és a kiberbiztonsági incidensek kezelésére, emiatt feltétlenül indokolt ezen két jogszabály vizsgálatának elvégzése.

A kritikus szervezetek ellenálló képességéről szóló 2024. évi LXXXIV. törvény a magyar nemzeti ellenálló képességi rendszer egyik alapvető pillérét teremti meg. A szabályozás célja, hogy erősítse az állam, a társadalom és a gazdaság működőképességét, valamint biztosítsa az

[403]Forrás: European Commission, 2019, The 2019 EU Justice Scoreboard https://ec.europa.eu/info/sites/info/files/justice_scoreboard_2019_en.pdf
[404] EURÓPAI PARLAMENT ÉS TANÁCS. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az unió kiberbiztonsági szintjének magas szintű közös szabályairól (NIS2). HL L 333., 2022.
[405] EURÓPAI PARLAMENT ÉS TANÁCS. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az unió kiberbiztonsági szintjének magas szintű közös szabályairól (NIS2). HL L 333., 2022.

alapvető szolgáltatások folyamatosságát. A törvény szemlélete szerint a kritikus szervezetek védelme nem pusztán ágazati igazgatási kérdés, hanem nemzetbiztonsági és közérdekű feladat. Emiatt a szabályozás olyan területekre terjed ki, mint a kormányzati működés folytonossága, az energetika, a közlekedés, az egészségügyi ellátás, az élelmezés és vízellátás, továbbá a kommunikációs rendszerek működése. A törvény tárgyi hatálya a Magyarország területén székhellyel rendelkező kritikus szervezetekre, illetve az ezek ellenálló képességét támogató és felügyelő intézményi rendszerre terjed ki.

A jogszabály egyik lényeges újítása, hogy a korábbi létfontosságú rendszerelemekre épülő szabályozási logikát a kritikus szervezetek fogalmára helyezi át. Ez nem pusztán terminológiai változás, hanem szemléleti fordulat is. A hangsúly már nem kizárólag az infrastruktúrák fizikai védelmén van, hanem a szolgáltatási folyamatok zavartűrésén, helyreállítási képességén és szervezeti rezilienciáján. Ezt tükrözi az is, hogy a korábbi Üzemeltetői Biztonsági Terv helyébe az Ellenálló Képességi Terv lép, amelynek kötelező eleme az Ellenálló Képességi Mátrix, továbbá a biztonsági összekötő személy helyett ellenálló képességért felelős vezetőt kell kijelölni. A törvény emellett kifejezetten figyelembe veszi az ágazatok és alágazatok közötti, illetve a határokon átnyúló kölcsönös függőségeket, ami különösen fontos az ellátási láncok és az alapvető szolgáltatások összekapcsolt működése szempontjából. A szabályozás uniós jogharmonizációs szempontból a CER irányelvnek való megfelelést szolgálja.

A Magyarország kiberbiztonságáról szóló 2024. évi LXIX. törvény ezzel párhuzamosan a digitális térben biztosít átfogó, egységes keretrendszert. A jogalkotó abból indul ki, hogy az elektronikus információs rendszerek és digitális eszközök a társadalmi és gazdasági működés alaprétegévé váltak, ezért a kibertér sérülékenysége közvetlenül veszélyezteti a közszolgáltatásokat, a piaci működést és a társadalmi bizalmat. A törvény hatálya több szervezeti körre terjed ki, így a közigazgatási szervekre, a meghatározott méretet elérő, többségi állami befolyás alatt álló gazdálkodó szervezetekre, valamint azokra a szervezetekre, amelyeket a hatóság alapvető vagy fontos szervezetként azonosít. Ez a megoldás azt jelzi, hogy a magyar kiberbiztonsági szabályozás nem szűk, technikai megfelelési logikára épül, hanem széles intézményi lefedettségre törekszik. A törvény különös jelentősége abban áll, hogy egységes szerkezetbe rendezi a korábbi, széttagoltabb kiberbiztonsági szabályokat, és 2025. január 1-jétől felváltotta a korábbi információbiztonsági és kiberbiztonsági tárgyú törvényi előzményeket. A szabályozás túlmutat a NIS2 irányelv egyszerű átültetésén. Egyfelől szélesebb

érintetti kört határoz meg, másfelől olyan további uniós aktusok végrehajtásához is kapcsolódik, mint a CER irányelv[406], a DORA rendelet[407], az ENISA rendelet[408] és az európai kiberbiztonsági kompetenciaközpont létrehozásáról szóló rendelet.[409] A törvény külön kezeli a hatósági tevékenységet, a tanúsítást, a poszt kvantumtitkosítást, a sérülékenységvizsgálatot és az incidenskezelést, ami arra utal, hogy a jogalkotó a kiberbiztonságot többdimenziós állami feladatként értelmezi. A szervezetek számára előírt kockázatmenedzsment és védelmi intézkedések nemzetközi standardokra épülnek, ami a szabályozás szakmai mélységét is erősíti.

A két törvény együtt egy új, integrált biztonsági szabályozási modellt rajzol ki Magyarországon. A kritikus szervezetek ellenálló képességéről szóló törvény elsősorban a fizikai, szervezeti és szolgáltatási rezilienciára összpontosít, míg a kiberbiztonsági törvény a digitális infrastruktúrák és elektronikus rendszerek védelmét helyezi előtérbe. A két norma közös logikája az, hogy a biztonságot nem statikus állapotként, hanem fenyegetésekhez alkalmazkodni képes, folytonosságot biztosító képességrendszerként kezeli. Ezzel a magyar szabályozás az uniós megfelelésen túl egy olyan összetett védelmi keretet alakít ki, amelyben a fizikai és a digitális biztonság egymást feltételező, egymást erősítő elemekként jelenik meg.

6. A nemzeti kiberhadviselés állami irányításának új eszközei és szereplői

Magyarország honvédelmi és nemzetbiztonsági érdekeinek stratégiai szintű beazonosítása és meghatározása, valamint a külügyi és nemzetközi kapcsolatainak irányaira vonatkozó döntések meghozatala, álláspontok kialakítása az Országgyűlés és a kormány politikai felelősségi körébe tartozik. Ugyanakkor a nemzetbiztonsági érdekek érvényesítése, vagyis a műveleti munka, különösen a nemzetbiztonsági szolgálatokról szóló törvényben

[406] Az Európai Parlament és a Tanács (EU) 2022/2557 irányelve (2022. december 14.) a kritikus szervezetek rezilienciájáról és a 2008/114/EK tanácsi irányelv hatályon kívül helyezéséről. Az Európai Unió Hivatalos Lapja, HL L 333., 2022.12.27., 164–198. o

[407] Az Európai Parlament és a Tanács (EU) 2022/2554 rendelete (2022. december 14.) a pénzügyi ágazat digitális működési rezilienciájáról, valamint az 1060/2009/EK, a 648/2012/EU, a 600/2014/EU, a 909/2014/EU és az (EU) 2016/1011 rendelet módosításáról. *Az Európai Unió Hivatalos Lapja*, HL L 333., 2022.12.27., 1–79. o.

[408] 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*, HL L 151., 2019.6.7., 15–69. o.

[409] Az Európai Parlament és a Tanács (EU) 2021/887 rendelete (2021. május 20.) az Európai Kiberbiztonsági Ipari, Technológiai és Kutatási Kompetenciaközpontnak és a nemzeti koordinációs központok hálózatának a létrehozásáról. *Az Európai Unió Hivatalos Lapja*, HL L 202., 2021.6.8., 1–31. o.

meghatározott feladatokkal összefüggő információk megszerzése, illetve megvédése, a szolgálatok személyi állományának legfontosabb feladatait képezik.

Annak érdekében, hogy a kormányzati döntések konkrét műveleti feladatokra, irányokra, célokra történő lefordítása gyorsan és hatékonyan történjen meg, Magyarország kormánya a nemzetbiztonsági szakpolitika irányítását – a 2022 és 2023 tavaszán lezajlott kormányzati struktúra módosítások során a miniszteri, úgynevezett irányítói jogkörök szinte teljes delegálásával – a polgári nemzetbiztonsági szolgálatokat felügyelő államtitkár és a katonai nemzetbiztonság irányításáért felelős államtitkár feladatává tette. A Nemzeti Információs Központ irányításáért a Miniszterelnök Nemzetbiztonsági Főtanácsadója felel.[410] A védelmi és biztonsági ágazat kibervédelmét érintő, stratégiai szintű paradigmaváltáshoz illeszkedő módon helyezi a fent említett közvetett jogköröket az irányító államtitkár felelősségi körébe a jogalkotó. A részletes feladat és hatásköri jegyzékeket a Mellékletek között, a 2. számú mellékletben jelenítettem meg.

7. Összegzés, az elvégzett vizsgálat és részkövetkeztetések

A fejezet egyik kiemelt célja a jogalkotási folyamatok, kiemelten a polgári és a katonai nemzetbiztonsági tevékenység irányításával továbbá, hazánk kiberbiztonsága növelésének érdekében megvalósult intézményi reformjával összefüggő vizsgálata, azon belül is, hogy a jogalkotó hogyan reagált az új típusú biztonsági kihívásokra. Ennek a vizsgálatnak az eredményeként kerültek bizonyításra a 2. számú hipotézis egyes elemei és a 3. számú hipotézisnek a nemzetbiztonsági szolgálatok által felderített információk és a megszerzett tapasztalatok hasznosságával összefüggő ismereteknek a hibrid hadviselés elleni küzdelemben való felhasználására vonatkozóan meghatározott eleme. A VII. és IX. fejezetben, más szempontból vizsgált, tagállami együttműködés fontosságát kihangsúlyozó konkrétumok további megjelenítése és elemzése által támasztottam alá ebben a fejezetben az 5. hipotézis szövetségesi jogokra és kötelezettségekre vonatkozó megállapításait.

[410] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 8/A-8/D. §-ok alapján

A digitalizáció növeli az adatkezelés (kiemelten analitika, fúzió, kereskedelem) jelentőségét, ami új kihívásokat jelent a védelmi és biztonsági szektor számára:

- A digitális eszközök adatai alapján történő ellenőrzés automatizálása,
- A szenzitív adatok kezelésének egyensúlya a védelmi és biztonsági tevékenységekben,
- A mesterséges intelligencia alkalmazásának határai a humán kontroll nélkülözhetetlensége miatt,
- A magánélet védelme a jogellenes titkos adatszerzéssel szemben, és
- Állampolgárok generális és preventív védelme a digitális térben.

A digitális szolgáltatásokról szóló jogszabály (DSA)[411] védelmet nyújt az állampolgároknak a digitális térben az alábbi célok elérése érdekében:

- Átláthatóság és elszámoltathatóság a nagy technológiai vállalatok vonatkozásában,
- A jogellenes tartalmak és termékek kiszűrésének javítása,
- A közérdek, az alapvető jogok, a közegészség védelme és a biztonságos felhasználói élmény, illetve lét biztosítása a kibertérben,
- A felhasználók (jogi) képességének fenntartása a platformok döntéseinek megtámadására
- Független ellenőrzés megteremtése, és
- A jogi sérülékenységvizsgálat (karbantartás) elvégzése és a hibrid fenyegetések elleni küzdelem.

A digitális transzformáció korában a jogalkotás kiemelt figyelmet fordít a kiberbiztonság kérdéseire. Mind hazai, mind nemzetközi szinten láthatóak a törekvések a szabályozási hiányosságok pótlására. Magyarországon pozitív fejlemény a nemzetbiztonsági ágazat irányítási struktúrájának átalakítása, amely magasabb elvárásokat és feladatokat határozott meg a biztonsági szektor szereplői számára. Különösen fontos a katonai és a polgári nemzetbiztonságért felelős államtitkári pozíciók létrehozása és a kapcsolódó miniszteri irányítói jogkörök delegálása.

[411] EURÓPAI PARLAMENT ÉS TANÁCS. Az Európai Parlament és a Tanács (EU) 2022/2065 rendelete a digitális szolgáltatásokról (Digital Services Act). HL L 277., 2022.

A kézirat lezárásának időpontjában folyamatban lévő nemzetbiztonsági ágazatot, illetve kiberbiztonságot érintő szabályozási innováció várható eredményeinek számításba vétele esetén valószínűsíthető, hogy megszűnnek az akadályai annak, hogy a szakmai tevékenységre vonatkozó minőségbiztosítási kérdések előtérbe kerüljenek a szabályozási kihívások kezelése érdekében.

A megjelenített reformfolyamatokkal összefüggő összegzett véleményem szerint a következetes és egységes intézményszervezési, valamint kapcsolódó jogalkotói tevékenység eredményeként könnyebben előtérbe juttathatók a minőségbiztosítási természetű kihívások kezelésének kérdései és a levont következtetésekből kiinduló, átfogó szabályozási reformfolyamatok további lépései.

A jogalkotás proaktív hozzáállást mutat, és láthatóan igyekszik lépést tartani a technológiai fejlődés ütemével. Ugyanakkor a gyakorlati implementáció sikere csak hosszabb távon mérhető fel. A jogszabályok betartatása és végrehajtása jelenti majd a valódi próbatételt az elkövetkező években.

Mind a hazai, mind a szövetségi szintű normaalkotás viszonylatában vizsgálva megállapítható, hogy a jogalkotó kiemelt figyelmet fordít a kiberbiztonság kérdéseinek tisztázására, valamint látható, illetve érezhető erőkifejtést végez a hiányosságok orvoslására.

IX. A JOGALKOTÁS ÉS A MESTERSÉGES INTELLIGENCIA KAPCSOLATA A KIBERTÉRBEN

1. Az információfúzió, adatanalitika, mesterséges intelligencia jelentősége a nemzetbiztonsági tárgyú jogalkotói tevékenység szempontjából

A nemzetbiztonsági szolgálatok működésének jogi kereteinek megértése kulcsfontosságú a demokratikus államrend és a jogállamiság elveinek fenntartásához.[412] Ezek a szolgálatok olyan erőforrásokat, eszközöket és módszereket alkalmaznak, amelyek a jogforrási hierarchia

[412] A fejezet eredeti formájában 2022-ben, Hódos László: A kibertér és a mesterséges intelligencia jelentősége és kihívásai a jogállamok nemzetbiztonsági feladatellátásában címmel jelent meg, Budapest, Magyarország: Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar (2022)

legfelső szintjeitől kezdve a legalacsonyabb szintekig terjedő széleskörű szabályozási eszközrendszert foglalnak magukban. A magyar nemzetbiztonsági szolgálatok tevékenysége, amely elsősorban a nyilvánosság elől rejtett, ritkább esetekben nyilvánosan zajlik, alapvetően a nemzetbiztonság védelmét szolgálja.

A nemzetbiztonsági tevékenység során végzett feladatok gyakran magukban foglalhatnak alapjogok korlátozását, ami kiemelt figyelmet és óvatosságot igényel. Ezen tevékenységek gyakorlása állami monopólium, amelyet csak a törvény által erre feljogosított szervezetek végezhetnek, és szigorú jogi előírások szerint kell működniük. Az állami szerveknek ezért rendkívül átláthatónak és elszámoltathatónak kell lenniük, hogy biztosítsák a demokratikus normák és az alapvető emberi jogok tiszteletben tartását.

Ez azt jelenti, hogy a nemzetbiztonsági szolgálatok működését részletes jogszabályok szabályozzák, amelyek meghatározzák a szolgálatok hatáskörét, feladatait, az alkalmazható eszközöket és módszereket, valamint az ellenőrzés és felelősségre vonás módjait. A nemzetbiztonsági tevékenység jogi kereteinek kialakítása során fontos a megfelelő egyensúly megtalálása a nemzetbiztonság védelme és az alapvető szabadságjogok között, hogy egyrészt hatékonyan tudjuk megvédeni a társadalmat a fenyegetésektől, másrészt megőrizzük a demokratikus értékeket és az alapvető emberi jogokat.

A mesterséges intelligencia (AI vagy MI), a dezinformációs műveletek és az álhírek alkotta komplex veszélyforrások együttesen jelentős kihívást jelentenek, különösen olyan súlyos járvány idején, mint amilyen a koronavírus járvány Magyarországon is volt. Ezek a fenyegetések összetett módon hatnak, és egymás hatását erősítve képesek súlyosan befolyásolni egy ország nemzetbiztonsági helyzetét.[413] A mesterséges intelligencia alkalmazása a dezinformációs műveletekben és az álhírek terjesztésében új dimenziót ad a kiberbiztonsági kihívásoknak, hiszen az AI képes gyorsabban és hatékonyabban manipulálni az információkat, így nagyobb károkat okozva.

A hatályos NBS által azonosított biztonsági kockázatok elleni hatékony fellépés érdekében a kormányzatnak érdemes lehet célul kitűzni a teljes biztonsági szektorban való

[413] EURÓPAI PARLAMENT ÉS TANÁCS. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az unió kiberbiztonsági szintjének magas szintű közös szabályairól (NIS2). HL L 333., 2022.

szélesebb összhang megteremtését. Ez azt jelenti, hogy a különböző nemzetbiztonsági és rendvédelmi szervek, valamint a kiberbiztonsággal foglalkozó intézmények közötti együttműködést és információcserét erősíteni kell, hogy hatékonyabban lehessen szembenézni az AI által támasztott új kihívásokkal, valamint a dezinformációs és álhír-terjesztő műveletekkel.

A kormányzati intézkedéseknek a következő elemeket kell magukban foglalniuk az NBS iránymutatása szerint:

- Az AI és kiberbiztonsági képességek fejlesztése: A kormányzatnak támogatnia kell a mesterséges intelligencia és kiberbiztonsági technológiák fejlesztését, hogy hatékonyabban fel lehessen lépni a kiberfenyegetésekkel szemben.
- Tájékoztatási kampányok végrehajtása: A társadalom széles körű tájékoztatása a dezinformációs műveletekről és az álhírekről, valamint azok felismerésének és kezelésének módszereiről elengedhetetlen a lakosság tudatosságának növelése érdekében;
- Nemzetközi együttműködés: A globális kiberfenyegetések kezelése érdekében kulcsfontosságú a nemzetközi együttműködés és információcsere;
- Intézkedések a sérülékenység, illetve sebezhetőség csökkentésére: A kormányzatnak stratégiákat kell kidolgoznia a társadalom és a kritikus infrastruktúrák sebezhetőségének csökkentése érdekében, beleértve a kiberbiztonsági képzéseket és a rendszeres kiberbiztonsági ellenőrzéseket.

Ezek az intézkedések képesek hozzájárulni ahhoz, hogy Magyarország hatékonyabban tudjon szembenézni a mesterséges intelligencia, a dezinformációs műveletek és az álhírek jelentette nemzetbiztonsági kihívásokkal, és így erősíteni a biztonsági szektor összhangját és ellenálló képességét.

A magyar nemzetbiztonsági rendszer átalakulása és fejlesztése az elmúlt években kiemelt jelentőséggel bírt, a jogalkotó különös figyelmet fordított a 21. század biztonsági kihívásaira történő megfelelő reagálásra. A jogalkotás és a szakpolitika területén tett lépések, mint például az Nbtv. módosítása fontos szerepet játszott a nemzetbiztonsági szektor hatékonyságának növelésében.

Ezek a lépések nem csupán a hatékonyság javítására és az erőforrások optimalizálására irányultak, hanem arra is, hogy csökkentsék a duplikációkat és jobban összehangolják a különböző nemzetbiztonsági szervezetek munkáját. Az összevonások és strukturális változások révén a magyar nemzetbiztonsági szolgálatok képesek lettek hatékonyabban reagálni a modern kor kihívásaira, mint a nemzetközi terrorizmus, a kiberfenyegetések és egyéb transznacionális biztonsági kockázatok.

A magyar nemzetbiztonsági szolgálatok jogszabályi és strukturális átalakításai létfontosságúak voltak a modern kihívásokra való hatékony reagálás vonatkozásában. Ezek az intézkedések biztosították, hogy a nemzetbiztonsági szektor rugalmasabb és alkalmazkodóbb legyen, képes legyen megfelelni a társadalom aktuális szükségleteinek és kihívásainak, miközben tiszteletben tartja a múlt tapasztalatait és hagyományait.

A mesterséges intelligencia által elvégezhető adatanalitika természetesen az információfúziós központok működésére is jelentős hatást gyakorolhat, hiszen számos álláshely veszélybe fog kerülni, valamint jelentős kapacitáskoncentráció valósítható meg az új informatikai fejlesztéseknek köszönhetően, ami minden olyan tevékenységet ki tud váltani majd, amelyhez kizárólagos humán kognitív képességek nem szükségesek. Mivel a fejlesztők nemzetbiztonsági szakági ismeretekkel korlátozottan rendelkeznek, ezért az adatfeldolgozás, illetve az analitika területén valósulhat meg leginkább a mesterséges intelligencia megjelenése a rendvédelmi, illetve nemzetbiztonsági feladatellátás során.

Megítélésem szerint központosított, egycsatornás hírigénykielégítés a jelenlegi, elsősorban katonai jellegű, illetve hátterű biztonsági kihívások időszakában elsődlegesen adminisztratív támogatást jelent a Katonai Nemzetbiztonsági Szolgálat számára a Nemzeti Információs Központ részéről.

Az elmúlt évek, különösen a 2019 és 2023 közötti időszak, rávilágítottak arra a kritikus jelentőségre, amellyel a kibertérben zajló dezinformációs műveletek bírnak, különösen a járványhelyzet és egyéb különleges jogrendű időszakok során. Ezek a műveletek, amelyek a kibertérből kiindulva terjesztik a félrevezető információkat, kiemelten hatékonyak lehetnek az ilyen válságos időszakokban, és jelentős hátrányokkal fenyegethetik a társadalmi stabilitást és biztonságot.

Ez a helyzet szükségessé teszi, hogy a nemzetbiztonsági elhárításért és rendvédelemért felelős szervezetek növeljék erőforrásaikat és intenzívebben foglalkozzanak ezekkel a fenyegetésekkel. A folyamatos felkészülés és a jövőbeli feladatok tervezése során a nemzetbiztonsági szolgálatoknak és más állami szerveknek kiemelt figyelmet kell fordítaniuk a dezinformációs műveletek elhárítására. Ennek részeként fontos a kibertérben zajló harci technikák és stratégiák fejlesztése, valamint az öntanuló és adaptív ellenfelekkel szembeni védekezési képességek erősítése.

Ez a helyzet rámutat arra is, hogy a modern kor kihívásaihoz alkalmazkodva a nemzetbiztonsági stratégiákat és taktikákat dinamikusan kell alakítani. Az öntanuló és folyamatosan változó kiberfenyegetések elleni védekezés egy olyan terület, ahol a technológiai innováció és a humán erőforrások egyaránt nélkülözhetetlenek a hatékony válaszadás és a társadalmi biztonság fenntartása érdekében.

2. Műveletek a kibertérben a pandémia idején, a társadalom biztonságának védelme

Az V. fejezetben a stratégiakészítés, mint jogi normaalkotás vonatkozásában megállapítottam, hogy a hibrid és kiberhadviselés közötti szoros összefüggés jól látható[414], valamint azt, hogy miként kapcsolódik előbbi kettőhöz „a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenése és gyors terjedése.” Ugyanis a járványhelyzet, mint rendkívüli körülmény, különösen alkalmas arra, hogy a dezinformáció és hamis híresztelések terjedése által okozott károkat súlyosbítsa.

Egy ilyen eset például a „Budapestet hamarosan le fogják zárni” típusú, alaptalan pánikkeltő hírek terjedése. Ez a fajta dezinformáció súlyos politikai, gazdasági és társadalmi károkat képes okozni, hiszen bizonytalanságot és zavart kelt a lakosság körében, befolyásolva ezzel a mindennapi életet és a gazdasági döntéseket.

[414] A különleges jogrendet, illetve a kibertérben zajló konfliktusokat érintően konferenciák tekintetében többek között lásd: 2017. április 21. Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar, Magyar Tudományos Akadémia Társadalomtudományi Kutatóközpont Jogtudományi Intézet, Magyar Katonai Jogi és Hadijogi Társaság: A különleges jogrend c. konferencia, Budapest; 2019. május 8. Széchenyi István Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: Az erőszak tilalmától a kibertérben zajló konfliktusokig c. konferencia, Győr; 2019. május 29. Nemzeti Közszolgálati Egyetem, Széchenyi István Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: 80 éves az első magyar honvédelmi törvény c. konferencia, Budapest; 2019. november 19. Nemzeti Közszolgálati Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: Honvédelmi jog és igazgatás aktuális kérdései c. konferencia, Budapest

A Készenléti Rendőrség Nemzeti Nyomozóiroda és a Nemzetbiztonsági Szakszolgálat gyors és hatékony fellépése a hamis információk terjesztői ellen példaértékű a dezinformáció elleni küzdelemben. A büntetőeljárások megindítása jelzi, hogy az állami szervek komolyan veszik ezeket a fenyegetéseket, és aktívan lépnek fel ellenük.

A járvány által kiváltott bizonytalanság kiemelten sebezhetővé teszi a társadalmat az online csalások és egyéb kibertérben elkövetett bűncselekmények számára. Az ilyen típusú bűncselekmények elkövetői gyakran kihasználják az emberek félelmeit és bizonytalanságait saját előnyükre.

A magyar kormány által folytatott széleskörű tájékoztatási kampány létfontosságú eszköz a dezinformáció és a hamis információk terjedése elleni harcban. A kormányzat által nyújtott folyamatos, megbízható és hiteles információk segítenek megőrizni a társadalmi stabilitást és csökkenteni a pánik kialakulásának esélyét.

Ezen kívül, a dezinformáció terjedése és a bizalom aláásása komoly kihívást jelent az államapparátusnak és a helyi vezetőknek. Ezek a tevékenységek aláásható az emberek bizalmát a hivatalos intézményekben, valamint ronthatják a munkavállalók mentális egészségét is, ami károsan hat a társadalom egészére.

A kiberbiztonsági kockázatok kezelése és a dezinformáció elleni küzdelem kulcsfontosságú a társadalmi kötőszövet megőrzése és az állami struktúrák stabilitásának fenntartása szempontjából.[415] A kormányzati és nem kormányzati szerveknek egyaránt fontos szerepük van ebben a folyamatban, mivel intézkedéseikkel jelentős mértékben hozzájárulhatnak a társadalmi bizalom fenntartásához és a dezinformáció okozta károk minimalizálásához. [416]

[415] KÁDÁR Pál: A kibertér és a kibertérműveleti képességek jelentősége a védelmi és biztonsági tevékenységek összehangolásának fejlesztésében, In: Farkas, Ádám; Kelemen, Roland (szerk.) A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből, Budapest, Magyarország : Gondolat Kiadó (2023) 327 p. pp. 149-165. , 17 p. Kádár Pál kiemeli, hogy a kibertérből érkező fenyegetések hatékony kezelése szempontjából kulcsfontosságú az állami szereplők – katonai, rendvédelmi, nemzetbiztonsági szervezetek – szoros együttműködése. Ennek kialakításában pedig meghatározó lehet a közös kibervédelmi doktrína, stratégia kidolgozása, a műveleti protokollok összehangolása, illetve a közös képességfejlesztés és kibergyakorlatok. A szerző számos jó gyakorlatot is bemutat erre vonatkozóan. Művében kihangsúlyozza, hogy az egységes szemlélet és összehangolt cselekvés kulcsfontosságú a kibertérből érkező kihívásokkal szembeni fellépésben.
[416] EURÓPAI PARLAMENT ÉS TANÁCS. Az Európai Parlament és a Tanács (EU) 2022/2555 irányelve az unió kiberbiztonsági szintjének magas szintű közös szabályairól (NIS2). HL L 333., 2022.

3. A mindennapokban megjelenő mesterséges intelligencia és egyes biztonsági aspektusok

A mesterséges intelligenciáról egyre többet hallunk, a közeljövő meghatározó technológiájának tartják. Lehetővé teszi a technika számára, hogy érzékelje környezetét, kölcsönhatásba kerüljön azzal, amit észlel, problémákat oldjon meg, és konkrét cél elérése érdekében megtervezze a saját lépéseit. A számítógép nemcsak adatokat vételez (már előkészített vagy összegyűjtött adatokat arra alkalmas perifériáin, például kameráján keresztül), hanem fel is dolgozza azokat és reagál rájuk. Ezek a rendszerek képesek viselkedésük bizonyos fokú módosítására is, a korábbi lépéseik hatásainak elemzésével és önálló munkával.

A technológia egyes fajtái már több mint 50 éve léteznek, de a teljesítmény fejlődése, a hatalmas mennyiségű adat feldolgozása és az új algoritmusok az elmúlt években jelentős áttörést jelentettek a területen. Az Internetes vásárlásaink és a számunkra küldött célzott, személyre szabott hirdetéseket mutathassanak nekünk online, például böngészési előzményeink és vásárlásaink, vagy más Internetes tevékenységünk alapján. A mesterséges intelligencia rendkívül fontos az Internetes kereskedelemben például a termékek optimalizálása, vagy a készletek és a logisztika megtervezése miatt, vagyis a gazdasági társaságok számára konkrét értékkel bír minden, a felhasználó szokásairól szóló információ.

Ezek az információk eladhatók, a felhasználó ingyen vagy egy nyereményjáték keretében (odaadott, vagy) megadott adatait harmadik fél számára értékesíti számos adatkezelő. Az internetes böngészés természetesen hasznos is másik oldalról nézve, hiszen a böngészők mögötti keresőmotorok a felhasználók által rendelkezésre bocsátott rendkívül nagy mennyiségű adatot kiértékelik, majd szokásainkból tanulnak. Ezt követően pedig csakugyan olyan találatokat kapunk, egy-egy kereséskor, amelyek számunkra relevánsak. Nyilván az ár-érték arányt alapul véve, figyelemmel arra, hogy ezeket az adatokat jó esetben anonimizáltan, kevésbé jó esetben névvel, (szállítási) címmel, (értesítési) telefonszámmal együtt adja el valamelyik szoftveróriás, harmadik félnek, érdemes úgy tekintenünk virtuális életünkre, mint egy sokak által hozzáférhető, nyitott könyvre…

Az öntanuló szoftverek korában az online meetingekre berendelő alkalmazások világában a személyi asszisztens is egyfajta alkalmazások egyvelege, sok esetben már komplex vagy egymással összehangolt szoftverek váltják ki a humánerőforrást. Előbbiek használata vélhetően

számos álláshely megszűnését is magával hozza. Bár a mesterséges intelligencia várhatóan jobb munkahelyeket is teremt, az oktatásnak és a képzésnek döntő szerep jut majd abban, hogy képzett munkaerőt biztosítson a területen. Nyilván a mesterséges intelligencia számos élethelyzetet és azokra adott több ezer vagy több száz éve társadalom által elfogadott intézményt egy másodperc törtrésze alatt fog a történelem szemétdombjára vetni, remélhetőleg az emberiséget, mint a legkárosabb állatfajt, majd csak később igyekszik „drasztikusan megjavítani". Az emberrel fizikai kapcsolatban álló alkalmazások is jelenthetnek fizikai veszélyt, ha azokat nem megfelelő gondossággal tervezik vagy alkotják meg, vagy ha a szoftvert feltörik, illetve az adatokkal visszaélnek.

Az okoseszközök a mesterséges intelligencia használatával a lehető legrelevánsabb és személyre szabottabb termékeket kínálják, jelzik, hogy elfogyott az adott élelmiszer, vagy a papír a nyomtatóból, különösen, ha ezek összeköttetésben is vannak. A virtuális asszisztensek válaszolnak a kérdéseinkre és segítenek a napi rutin megszervezésében, különösen úgy, hogy a navigáció is legtöbbször a mesterséges intelligenciát használja, ahogyan az okos termosztátok energiát takarítanak meg, míg az intelligens városok fejlesztői azt remélik, hogy szabályozhatják a forgalmat a dugók csökkentése érdekében. A fordító szoftver, akár írott, akár szóban elmondott szövegen alapul, a mesterséges intelligenciára támaszkodik a fordítások biztosítása és fejlesztése érdekében, hasonlóan az automatikus feliratozáshoz. A mesterséges intelligenciát használó rendszerekkel összefüggésben azonban feltétlenül tisztázandó, hogy ki a felelős a mesterséges intelligenciával működtetett eszköz vagy szolgáltatás által okozott károkért. Számos olyan esetről olvashattunk az elmúlt években a különböző médiafelületeken, hogy az önvezető autó okozott balesetet, kárt, halálesetet. Felmerül a kérdés, hogy ilyen esetekben kinek kell helytállnia? A tulajdonosnak, az autógyártónak vagy a programozónak kell majd a felelősséget vállalnia? Hogyan értékeli majd a polgári és büntetőjog ezeket a kérdéseket? [417] Ha a robot vagy drón vagy autógyártó nem vonható felelősségre, akkor az

[417]A kérdés vizsgálata során érdemes áttanulmányozni: KÁLMÁN Kinga: Nyomokban kódokat tartalmazhat? A mesterséges intelligencia igazságszolgáltatásban történő alkalmazásának alkotmányjogi vonatkozásai a tisztességes eljáráshoz való jog tükrében. *MTA Law Working Papers*, 2021/2. A tanulmány a mesterséges intelligencia igazságszolgáltatásban történő alkalmazásának alkotmányjogi vonatkozásait elemzi a tisztességes eljáráshoz való jog szempontjából. Rávilágít, hogy bár a mesterséges intelligenciának számos előnye van, mint például a hatékonyság növelése és az emberi elfogultság csökkentése, átláthatatlansága kockázatokat jelent a megfelelő eljárás és elszámoltathatóság tekintetében. A mesterséges intelligencia bevezetése erős eljárási biztosítékokat igényel az automatizált döntések átláthatóságának, magyarázhatóságának és megtámadhatóságának biztosítása érdekében. További kihívások közé tartozik a diszkriminációmentesség, az adatvédelem biztosítása és a bírói autonómia megőrzése. A tanulmány érvelése szerint a mesterséges intelligenciának emberközpontúnak kell lennie, inkább az emberi ítélőképesség támogató eszközeként, mint annak helyettesítőjeként kell szolgálnia.

csökkentheti az emberek bizalmát a – jelen tanulmányban konkrétan meg nem nevezendő – piacvezető márka, illetve az egész technológia iránt. Tudja-e a jogalkotás ezeket a helyzeteket proaktívan kezelni és miként lehet majd az így alkotott szabályokat úgy átültetni a gyakorlatba, hogy az ne tegye lehetetlenné az innovációt? [418]

A bíróság számára egy megalapozott indokolás kialakításához nélkülözhetetlen a vonatkozó jogi normák, az esetjog és a jogi irodalom egyidejű, magas szintű ismerete. Ennek okán valamennyi bírói döntést hosszú és aprólékos kutatásnak kell megelőznie. [419]

A jogi kutatószoftverek (*legal research softwares*) ezt a tevékenységet gyorsítják fel. Rendszeresen frissülő adatbázisaikban kulcsinformációk megadásával az összes elérhető releváns adatot egy keresési eredményben összegzi a program. [420]

Ahogyan tanulmányában Kálmán Kinga kiemeli „*a tengerentúlon az egyik, ha nem a legelterjedtebb ilyen jogi kutatószoftver a LexisNexis. Adatbázisa több, mint 83 milliárd jogszabályt és bírói esetjogot, 40 ezer jogi folyóiratcikket és 700 millió cégnyilvántartási adatot tartalmaz. Az alkalmazás megerősítésként értékeli, ha a felhasználó rákattint a keresési eredményre, a „linkelt oldalon töltött idő" hosszát, valamint azt, ha a felhasználó elmenti a találatot. Ez alapján javítja az adatbázisát a minél relevánsabb keresési eredmények elérése érdekében."* [421]

Folyamatos felügyeleti és hatásvizsgálati mechanizmusoknak kell kísérniük a mesterséges intelligencia integrálását, hogy összhangba kerüljön az alkotmányos értékekkel, és inkább erősítse, mint gyengítse az igazságszolgáltatást. A tanulmány az igazságügyi mesterséges intelligencia fejlesztésének és alkalmazásának etikai és jogi keretrendszerének uniós szintű megalkotására szólít fel a jogok tiszteletben tartásának biztosítása érdekében.

[418] A témával összefüggésben lásd: Kecskés Gábor: Az autonóm járművek jogi kérdéseinek nemzetközi kontextusa, különös tekintettel a környezetjogi vetületekre. Állam- és Jogtudomány 2020/4. pp. 52-64.; Mezei Kitti: A modern technológiák kihívásai a büntetőjogban, különös tekintettel a kiberbűnözésre. Állam- és Jogtudomány 2020/4. pp. 65-81.; Rácz Lilla: A személy és a dolog fogalmának (lehetséges) változásai a mesterséges intelligencia és a kriptovaluták világában. Állam- és Jogtudomány 2020/4. pp. 82-107.

[419] BRASIL. Superior Tribunal de Justiça: *Relatório de Gestão 2019*.

[420] Jogi kutatószoftverek működéséről a gyakorlatban lásd: NORTHPOINTE INC.: *Practitioner's Guide to COMPAS Core*. 2015. Elérhető: https://assets.documentcloud.org/documents/2840784/Practitioner-s-Guide-to-COMPAS-Core.pdf (letöltve: 2022.11.14.) és MIVILL, Olivia: Malaysian judiciary makes history, uses AI in sentencing. *New Straits Times*, 2020. február 19. Elérhető: https://www.nst.com.my/news/nation/2020/02/567024/malaysian-judiciary-makes-history-uses-ai-sentencing (letöltve: 2022.11.14.)

[421] KÁLMÁN Kinga: Nyomokban kódokat tartalmazhat? A mesterséges intelligencia igazságszolgáltatásban történő alkalmazásának alkotmányjogi vonatkozásai a tisztességes eljáráshoz való jog tükrében. *MTA Law Working Papers*, 2021/2.

Az egyik legismertebb online bíróság Kínában található: Hangzhou városában 2017-ben állították fel az első Internet Bíróságot. Kínában, amely a világon a legtöbb, mintegy 850 millió mobilinternet-felhasználóval rendelkezik, a digitalizálási erőfeszítések részben azt a célt szolgálják, hogy a bíróságok lépést tarthassanak a mobilfizetés és az e-kereskedelem által generált növekvő ügyteherrel. A hivatalos kínai adatok szerint a Legfelsőbb Népbírósággal közösen összesen 118 764 keresetet fogadtak be, és 88 401-et zártak le, és összesen közel hárommillió üggyel foglalkoztak. Ni Defengnek, az Internet Bíróság alelnökének álláspontja szerint a késedelem az igazságszolgáltatás akadályát képezi, emiatt feltétlenül szükséges felhasználni a digitalizáció minden eszközét az igazságszolgáltatás támogatására. A Bíróság eljárását bárki kezdeményezheti digitalizációval kapcsolatos témában (például fogyasztóvédelmi panaszok, szerzői jogi jogviták az online térben, elektronikus fizetés). Az egész folyamat az online térben folyik, a felek avatarjaikkal megjelenítve videóhívással vehetnek részt a tárgyaláson, illetve az előterjeszteni kívánt bizonyítási indítványukat szintén online, blokklánc technológiával titkosított formában tudják feltölteni. A bíró személyében mesterséges intelligencia áll velünk szemben, amely a rendelkezésre álló adatok alapján gépi tanulási folyamat eredményeként dönt és szolgáltat igazságot.

Az Interneten elérhető bemutatóban[422] a Kína nemzeti jelképe alatt ülő feketeköpenyes virtuális bírótól elhangzó „Van-e az alperesnek kifogása a felperes által benyújtott bírósági blokklánc-bizonyítékok természete ellen?" – kérdésre a tárgyalást megelőző ülésen a „Nincs kifogás" – válasz érkezett az emberi felperestől. A statisztikai adatokból kimutatható sikerek miatti eufória mellett persze könnyen lehet egy „Nagy testvér mindent lát" érzésünk, és valljuk be nem is alaptalanul. Minden esetben, akár a bűnelkövető bűnismétlésének várható valószínűségét becsüli meg, akár a kényszerintézkedés legcélszerűbb eszközét sugalmazza a mesterséges intelligencia[423], fontos megjegyezni, hogy a folyamatos humán kontroll nélkül könnyedén egy utópisztikus világban találjuk magunkat, ahol az öntanuló szoftverek az empátia hiánya, illetve korlátozott volta miatt meglepő javaslatokat tehetnek a jogalkalmazó számára.

[422]AFP: AI judges and verdicts via chat app: the brave new world of China's digital courts. *France 24*, 2019. december 6. Elérhető: https://www.france24.com/en/20191206-ai-judges-and-verdicts-via-chat-app-the-brave-new-world-of-china-s-digital-courts (letöltve: 2022. 11. 14.))

[423] Erre alkalmazzák a COMPAS (Correctional Offender Management Profiling for Alternative Sanctions) szoftvert, amely a rendelkezésre álló adatokból „kiszámítja", a bűnelkövetők bűnismétlési esélyét korábbi, vagy függőben lévő vádhatósági eljárás, büntetett előélet, a szabadlábra bocsátások, lakóhely bűnügyi fertőzöttsége, foglalkozás, szociális viszonyok és káros szenvedélyek alapján. Ezek figyelembevételével egy 1-10-ig terjedő skálán értékeli az elkövető visszaesésének esélyét, amelyre később a bíróság a szabadlábra bocsátásról szóló döntését alapíthatja, lényegében az adminisztratív előkészítő feladatokat teljes körűen elvégezve.

Persze az sem zárható ki, hogy a mesterséges intelligencia helyes döntést fog hozni annak ellenére is, hogy az emberi résztvevő ezt nem így érzi.

Ha nem kezelik megfelelően, a mesterséges intelligencia téves döntésekhez vezethet, vagy az etnikai hovatartozásra, nemre, és életkorra vonatkozó adatokkal befolyásolhatja a döntéseket egy ingatlan bérbeadása vagy akár egy elbocsátás során. Emellett befolyásolhatja a magánélethez és az adatvédelemhez való jogot. Használható például arcfelismerő berendezésekben, vagy online nyomon követés és profilalkotás céljából. A mesterséges intelligencia szerepet játszhat a gyülekezési és tiltakozási szabadság sérelmében is, mivel nyomon követhet a bizonyos eszmékhez, vagy egy tüntetéshez kötődő személyeket. Vagyis egy járvánnyal fertőzött területről érkező felhasználó esetében a mesterséges intelligencia jelzi az arra jogosult állami szerv részére, hogy fokozott egészségügyi kockázatot jelenthet a jelenléte vagy megszegte a karanténszabályokat, de egy meghatározott időben és helyen tartózkodó demonstráló is kiszűrhető, beazonosítható. A helyes állami célkitűzések, mint a terrorelhárítást célzó funkciók is felhasználhatóak ilyen módon egyes csoportok, személyek megfélemlítésére, elnyomására. Emiatt van kiemelkedő jelentősége annak, hogy a humán oldalon milyen célok, szándékok vezérlik a mesterséges intelligenciával bíró fizikai, illetve virtuális eszközöket.

4. A mesterséges intelligencia a társadalom hibrid fenyegetések, rosszindulatú informatikai tevékenységek és dezinformáció elleni védelmében

A mesterséges intelligencia (ideértve a virtuális asszisztenseket, specifikus képelemző és kereső szoftvereket, hang- és arc(kép)felismerő rendszereket, valamint a robotokat, önvezető autókat és drónokat), valamint a dezinformációs műveletek, az álhírekkel történő operáció a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenése és gyors terjedésekor, egymás hatását erősítő, egy adott országgal szembeni (nemzetbiztonsági) kombinációként (műveleti intézkedések sorozataként) is felfogható. A hatályos NBS által azonosított biztonsági kockázatokkal szembeni hatékony fellépés rögzítése iránti kormányzati igény esetén cél lehet a szélesebb összhang megteremtése a teljes biztonsági szektor vonatkozásában. Az NBS által rögzített, súlyos megbetegedés kockázatát hordozó járványos betegség magyarországi megjelenése esetében is használható a mesterséges intelligencia, például a repülőtereken és végzett hőképalkotáshoz, valamint a betegség terjedésének nyomon követésére szolgáló adatok gyűjtéséhez is, utóbbi esetekben a „védelmet” erősíti, tényeken alapuló információkkal az esetleges álhírek (pánikkeltés,

befolyásolás) ellen. Bizonyos mesterséges intelligenciát használó alkalmazások képesek felderíteni az álhíreket és a dezinformációt a közösségi médiából származó adatok vizsgálatával, az ún. klikkvadász címeket vagy ijesztő szavakat keresve és igyekeznek meghatározni, mely Internetes forrásokat tekinthetünk hitelesnek.

A kézirat lezárásakor folyamatban lévő orosz-ukrán konfliktus vonatkozásában is rendkívül fontos, hogy a jelentős mennyiségű álhír között hiteles tájékoztatást lehetővé tevő információforráshoz jusson a közvélemény is, hiszen mindkét fél elemi érdeke a tisztánlátás és a hamis, illetve hamisított hírek által gerjesztett provokáció okozta hisztéria elkerülése. A háború eszkalálódása, a nemzetközi közösség tudatának befolyásolása nélkül nehezen képzelhető el, abban az esetben, ha a felek a hadviselés jelenlegi földrajzi keretei között maradnak. A befolyásolás elleni küzdelem egyik leghatékonyabb eszköze pedig az idegen, illetve ellenérdekelt információs műveletek elleni hatékony, közös fellépés a NATO-n és az EU-n belül. A küzdelemben pedig a mesterséges intelligencia a folyamatos adatfeldolgozás, a minták felismerése és a támadások visszakövetése során a kibertámadások és más kiberfenyegetések kivédésében jelentős funkciót láthat el.

5. A mesterséges intelligencia szerepe és a kiberreziliencia jelentősége a szövetségi rendszerek jogi szabályozási keretein belül

A dezinformáció, vagy hamis információ terjesztése, komoly kihívást jelent a digitális korban. A dezinformáció olyan hamis vagy megtévesztő információ terjesztése, amely a valóságot torzítja vagy szándékosan manipulálja. Gyakran előfordul az online média platformokon, ahol a tartalmak könnyen és gyorsan terjedhetnek, és a felhasználók gyakran nehézséget tapasztalnak az információk hitelességének megítélésében. A dezinformáció gyors és hatékony terjedését támogatják a közösségi média, a keresőmotorok, és az online hírportálok.

A hamis információk könnyen elérhetők és megoszthatók, és az algoritmusok néha hozzájárulhatnak a felhasználók egyoldalú információs buborékokban történő tartózkodásához, erősítve az előítéleteket és torzítva a valóságképet. A dezinformáció gyakran kapcsolódik szándékos támadásokhoz és politikai célokhoz. Az államok, politikai csoportok vagy egyének szándékosan terjeszthetnek hamis információkat annak érdekében, hogy befolyásolják a közvéleményt, eltorzítsák az eseményeket, vagy akár destabilizálják más országok társadalmi rendjét. A dezinformáció terjedése kihívást jelent a hitelesség és a tájékozottság terén. A

felhasználóknak nehezen lehet eldönteni, hogy az általuk talált információ megbízható-e vagy sem. A kritikai gondolkodás, az információk forrásainak ellenőrzése, és az oktatásnak kulcsszerepe van a dezinformációval szembeni ellenálló képesség kialakításában.

A technológia is részese a dezinformáció problémájának, de ugyanakkor segíthet is az ellenálló képesség fejlesztésében. Az algoritmusok fejlesztése, a hamis információk azonosítására és a felhasználók tájékoztatására irányuló kezdeményezések mind hozzájárulhatnak a digitális tér biztonságosabbá tételéhez. Az ellenálló képesség fejlesztése a dezinformációval szemben együttes erőfeszítéseket igényel a média, az oktatási intézmények, és a technológiai vállalatok részéről. Az oktatásnak kritikai gondolkodást, forráskritikát, és digitális írástudást kell oktatnia, míg a média és technológiai vállalatoknak felelős módon kell kezelniük a tartalmak terjesztését. A dezinformáció komoly kihívásokat jelent a digitális társadalom számára. A megértés, az oktatás és a technológiai megoldások segíthetnek a dezinformáció terjedésének csökkentésében és az emberek ellenálló képességének fejlesztésében. Az egységes és koordinált erőfeszítésekkel a társadalom jobban felkészülhet és védekezhet a dezinformációval szemben a jövőben.

Az Európai Unió jogalkotási folyamataiban kulcsfontosságú szerepet játszanak azok a munkacsoportok, amelyek specifikus fenyegetésekkel, mint például a hibrid fenyegetések és a dezinformáció kezelésével foglalkoznak. Az Európai Tanács mellett működő horizontális hibrid fenyegetésekkel és dezinformációval foglalkozó munkacsoport az Állandó Képviselők Bizottságának (COREPER) irányítása alatt áll, és fontos szerepet tölt be az EU-szintű koordinációs és reagálási mechanizmusok kidolgozásában.

A Helsinkiben található Hibrid Fenyegetések Elleni Kiválósági Központ, amelyhez Magyarország 2019-ben csatlakozott, szintén fontos szereplője az EU és a NATO által támogatott erőfeszítéseknek. A Központnak különösen kibergyakorlatok szervezésében van jelentős szerepe, ami a kibervédelmi képességek fejlesztését és a megszerzett tapasztalatok megosztását célozzák.

Ezek a szervezetek és munkacsoportok alapvetően hozzájárulnak a jogi normák előkészítéséhez és kibocsátásához, legyen szó online tevékenységek szabályozásáról, járványkezelésről vagy hibrid hadviselésről. A közösségi szintű, hatékony stratégiák kidolgozása érdekében elengedhetetlen az ilyen autentikus kibocsátó szervezetek munkája.

Az Európai Parlament szakbizottságai előtt zajló folyamatok biztosítják a jogi háttér megalapozását és az együttműködés jogi kereteinek fejlesztését. A nemzetközi együttműködés jogi hátterének hiányában az ilyen jellegű fenyegetésekkel szembeni védekezés kevésbé lenne hatékony. Ezért létfontosságú, hogy az EU intézményrendszere folyamatosan dolgozzon a releváns jogi normák adaptálásán és fejlesztésén, hogy megfeleljen a modern kihívásoknak.

A digitális korban a dezinformáció egy komoly kihívás a társadalmak számára, és a mesterséges intelligencia egyre fontosabb szerepet játszik a dezinformáció elleni védelemben. A mesterséges intelligencia rendkívül hatékony az információszűrésben és elemzésben, algoritmusok és gépi tanulási modellek segítségével a rendszerek gyorsan szkennelik az online tartalmakat, azonosítva azokat a jeleket, amelyek a dezinformációt, hamis információt vagy manipulált tartalmat jelzik. Ez lehetővé teszi a szakemberek számára, hogy gyorsabban és hatékonyabban szembenézzenek a dezinformációval.

A mesterséges intelligencia kiválóan alkalmazható hamisítások felismerésére. Például a deepfake technológia által létrehozott manipulált videók és hangfelvételek azonosítása rendkívül fontos a dezinformáció elleni küzdelemben. Speciális algoritmusok elemzik az esetleges hamisításokat, és segítenek megkülönböztetni a valóságot a manipulált tartalomtól.

A közösségi média platformokon terjedő dezinformáció elleni küzdelemben a mesterséges intelligencia monitorozza és elemzi a felhasználók által generált tartalmakat. Az algoritmusok segíthetnek azonosítani „a kamu profilokat”, a hamis információkat, és jelzik a platformoknak és a felhasználóknak, hogy észleltek potenciális dezinformációt. Ez növelheti a felhasználók tudatosságát és csökkentheti a hamis információk terjedését.

A mesterséges intelligencia alkalmazása a személyre szabott tartalom ajánlások felülvizsgálatában is segíthet. A platformoknak lehetőségük van átvizsgálni az ajánlott tartalmakat, és minimalizálni az olyan algoritmusokat, amelyek hajlamosak a felhasználókat információs buborékokba zárni. Így a felhasználók szélesebb körben juthatnak hozzá információkhoz, és csökken a manipulált tartalmak hatása.

Azonban fontos megjegyezni, hogy a mesterséges intelligencia alkalmazása a dezinformáció elleni védelemben számos kihívással és etikai megfontolással jár. Az

automatizált rendszereknek pontosaknak és elfogadhatóan etikusnak kell lenniük. Továbbá, az adatvédelem és az átláthatóság fontos szerepet játszik az MI-alapú rendszerek fejlesztése során.

A mesterséges intelligencia kulcsfontosságú eszköz a dezinformáció elleni küzdelemben. Azok az innovációk és fejlesztések, amelyek ezen a területen történnek, hozzájárulhatnak egy információban gazdagabb, biztonságosabb és tájékozottabb társadalom kialakításához. Azonban az alkalmazás során óvatosnak kell lenni az etikai szempontok és a jogi szabályozások tekintetében, hogy biztosítsuk a megfelelő működést és a polgárok jogainak védelmét.

A befolyásolás elleni küzdelem egyik leghatékonyabb eszköze pedig az idegen, illetve ellenérdekelt információs műveletek elleni hatékony, közös fellépés a nemzetközi színtéren, különösen a NATO-n és az EU-n belül. A küzdelemben pedig a mesterséges intelligencia a folyamatos adatfeldolgozás, a minták felismerése és a támadások visszakövetése során a kibertámadások és más kiberfenyegetések kivédésében jelentős funkciót láthat el.

A fenti fenyegetettségekre reagáló dokumentumok közül kiemelve – az egyik legveszélyesebb kihívás ellenei védekezést szolgáló intézkedési koncepciót[424] – az Európai Unió 2019–2024 közötti időszakra vonatkozó stratégiai menetrendje a társadalom hibrid fenyegetések, rosszindulatú informatikai tevékenységek és dezinformáció elleni védelmének fontosságát jeleníti meg[425], valamint hangsúlyozza, hogy az ilyen veszélyek kezelése átfogó vizsgálatot igényel, több együttműködéssel, koordinációval, erőforrással és jelentős technológiai eszközpark bevetésével. Fontos megjegyezni, hogy a mesterséges intelligencia napjaink digitális forradalmának központi eleme, és fejlesztésének, hasznosításának végzése az EU egyik fő célkitűzése.

A tagállamok egymás közötti, illetve a tagállamok és más érintett nemzetközi szervezetek közötti szoros együttműködés, különösen a NATO-val, támogatná az EU-ban végzett ellenséges tevékenységekkel szembeni kémelhárítás összehangolását[426]. Ehhez társul továbbá, hogy a hibrid hadviselés, mint nem katonai, vagyis a nem-hagyományos stratégiai kihívásokkal

[424] A reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítése, Európai Bizottság, 2018. forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018JC0016&from=GA
[425] Az Európai Parlamentnek és a Tanácsnak A hibrid fenyegetésekkel szembeni fellépés közös keretéről szóló közös közleménye (Forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52016JC0018) (A letöltés ideje: 2022. 08. 31. 9:19)
[426] A reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítése, Európai Bizottság, 2018. forrás: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018JC0016&from=GA

szemben adható válaszok (tényleges intézkedések) illetve az ezt követő, valószínűsíthető katonai tevékenység jelentős költségvonzattal jár. A nemzetközi szerepvállalás alanyaként, Magyarország vonatkozásában továbbra sem szabad elfeledni, hogy „*kiemelt jelentősége van annak a szempontnak, hogy a „korlátozott erőforrásokkal" rendelkező államok esetében a nemzetbiztonsági struktúrák hatékony működtetése, a koordinációs, irányítási, a technikai és az emberi erőforrásokra épülő információgyűjtő, az elemző-értékelő, vagy akár a különböző szakértői területek összehangolt munkája*" [427] ténylegesen összeadódjon és így kerüljön felhasználásra akár a fenyegetések felderítése és elhárítása, akár Magyarország nemzetbiztonsági érdekeinek, céljainak érvényesítésekor.

Ez a „jogalkotási súlyterület" azért meglehetősen bonyolult, mert a tevékenység leginkább a nemzetállamok elszigetelése, hiteltelenítése útján valósul meg, vagyis – akár az EU akár a NATO esetében – a tagállamok egymás iránti bizalmának csökkentése a cél. Ennek ellensúlyozására válik elengedhetetlenül fontossá az ellenséges hírszerzési tevékenységgel szembeni reziliencia fejlesztése, továbbá a meglévő védelmi és biztonsági kapacitás növelése.

A mesterséges intelligencia megregulázására vonatkozó EU-s törekvés rajzolódik ki az Artifical Intelligence Act (AI act) normaszövegében[428] is. Az MI norma tervezetének kodifikációs folyamata amiatt is rendkívüli jelentőségű, mert ez az első kísérlet egy horizontális MI-szabályozás létrehozására. Az Európai Parlament és a Tanács 2023. április 21-én fogadta el a Bizottság javaslatát az EU MI-vel kapcsolatos szabályozási keretrendszerére, amely 2023. május 16-án lépett hatályba, azonban a rendelet bizonyos rendelkezéseinek alkalmazása későbbi határnaptól, továbbá fokozatosan történik, és a végrehajtási jogszabályok kidolgozása 2024-ben fejeződött be. Az AI Act végrehajtásáért az Európai Bizottság felelős.

Az AI Act bevezetésének ütemezése a következő:[429]

I. 2024. április 21.: A nagy kockázatú AI-rendszerek értékelésére és tanúsítására vonatkozó követelmények hatályba lépnek.

---

[427] Dobák Imre: Nemzetbiztonsági szolgálatok – Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe, Hadtudomány, Budapest, 2015. VIII/4. 114.o.

[428]Elérhető:https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (letöltés: 2023. 12. 08.)

[429]AI Act tervezete, Elérhető:https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (letöltés: 2023. 12. 08.)

II. 2025. április 21.: A közepes kockázatú AI-rendszerekre vonatkozó követelmények hatályba lépnek.

III. 2026. április 21.: Az alacsony kockázatú AI-rendszerekre vonatkozó követelmények hatályba lépnek.

Fontos megjegyezni, hogy az AI Act csak az Európai Unióban alkalmazandó. Az EU-n kívüli országokban működő vállalkozásoknak más jogszabályoknak kell megfelelniük, ha AI-rendszereket fejlesztenek vagy használnak.

A jogi keretrendszer az MI rendszerek specifikus felhasználására és a kapcsolódó kockázatok kezelésére összpontosít. A Bizottság javaslata szerint az EU jogában technológia-semleges MI rendszer definíciót kellene létrehozni, és egy olyan osztályozást kellene meghatározni az MI rendszerek számára, amely különböző követelményeket és kötelezettségeket állapít meg a „kockázatalapú megközelítés" szerint. Néhány, „elfogadhatatlan" kockázatokat jelentő MI rendszert betiltanának. A „magas kockázatú" MI rendszerek széles skáláját engedélyeznék, de az EU piacra lépéshez számos követelménynek és kötelezettségnek kellene megfelelniük. Azok az MI rendszerek, amelyek csak „korlátozott kockázatot" jelentenek, nagyon enyhe átláthatósági kötelezettségeknek lennének alávetve.

Az EU jogalkotói most tárgyalásokat kezdenek a jogszabályok véglegesítésére, jelentős módosításokkal a Bizottság javaslatához képest, beleértve az MI rendszerek definíciójának komplett felülvizsgálatát, a tiltott MI rendszerek listájának kiszélesítését, valamint általános célú MI és generatív MI modellek, mint például a ChatGPT-re vonatkozó kötelezettségek pontos megfogalmazását.

A jogi norma megjeleníti, hogy az MI technológiák széles körű gazdasági és társadalmi előnyöket ígérnek számos ágazatban, beleértve a környezetvédelmet és az egészségügyet, a közszférát, a pénzügyeket, a mobilitást, a belügyeket és a mezőgazdaságot. Különösen hasznosak az előrejelzések javítására, a műveletek és erőforrások optimalizálására, valamint a szolgáltatások személyre szabására.

Azonban aggodalmak merülnek fel az MI rendszerek alapvető jogokra, valamint a felhasználók biztonságára gyakorolt hatásaival kapcsolatban, amikor az MI technológiák termékekbe és szolgáltatásokba vannak beépítve. Az MI rendszerek veszélyeztethetik az

alapvető jogokat, mint például a diszkrimináció-mentességhez való jogot, a szólásszabadságot, az emberi méltóságot, az adatvédelmet és a magánéletet. A javaslat vitatott pontjai előbbiek mellett a kockázatalapú megközelítés részletei, a biometrikus azonosítás szabályozása, és a konkrét végrehajtási mechanizmusok.

A jogi norma kifejezett célja, hogy biztosítsa az egységes piac megfelelő működését azáltal, hogy létrehozza az MI megbízható rendszereinek fejlesztéséhez és használatához szükséges feltételeket az Unióban. Az irányelvtervezet harmonizált jogi keretet állapít meg az MI termékek és szolgáltatások fejlesztésére, az Unió piacán való elhelyezésére és használatára.

A jogi norma a fentiek mellett törekszik bizonyos specifikus célok elérésére:

- biztosítani, hogy az EU piacán működő MI rendszerek biztonságosak legyenek és tiszteletben tartsák a meglévő EU jogot,
- jogbiztonságot garantálni az MI-be történő befektetés és innováció elősegítése érdekében,
- megerősíteni az EU jogának hatékony érvényesítését az MI rendszerekre vonatkozó alapvető jogi és biztonsági követelmények tekintetében, valamint
- elősegíteni egy egységes piac kialakulását a törvényes, biztonságos és megbízható MI alkalmazások számára és megakadályozni a piacok szegmentálódását.

A jogi normában szerepelnek az MI rendszerek definíciója és osztályozása, valamint a különböző kockázati szintekhez igazodó követelmények. Fontos megjegyezni, hogy az AI Act nem vonatkozik a kizárólag katonai célokra fejlesztett vagy használt MI rendszerekre, harmadik országok nyilvános hatóságaira vagy nemzetközi szervezetekre, sem olyan hatóságokra, amelyek MI rendszereket használnak nemzetközi egyezmények keretében a bűnüldözési és igazságügyi együttműködés során, tehát a (bel)biztonsági szakterület privilégiuma továbbra sem szenved csorbát.[430]

A mesterséges intelligenciára vonatkozó jogi norma tervezete mellett fontos megjegyezni, hogy a témában legalább ilyen fontos dokumentum elkészítése, véglegesítése is

[430]AI Act tervezete, Elérhető: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698792/EPRS_BRI(2021)698792_EN.pdf (letöltés: 2023. 12. 08.)

folyamatban van. Az Európai Bizottság által javasolt Európai Unió Kiberbiztonsági Tanúsítási Rendszeréről szóló szabályozás – amely az EU Kiberbiztonsági Rendeletének (Cybersecurity Act)[431] részeként jött létre – a „kiber-reziliencia rendelet”[432] (Cybersecurity Certification Framework, a továbbiakban: CRA) célja, hogy kibervédelmi kötelezettségeket írjon elő minden olyan termékre, amelyek digitális elemeket tartalmaznak és amelyek várható vagy előre látható használata közvetlen vagy közvetett adatkapcsolatot tartalmaz egy eszközhöz vagy hálózathoz.

A tanúsítási keretrendszer célja, hogy egységes és következetes tanúsítványokat biztosítson az információs és kommunikációs technológiai termékek, szolgáltatások és folyamatok számára az egész EU-ban. A rendszer segítségével az ügyfelek könnyebben tudják értékelni a termékek kiberbiztonsági szintjét, és ösztönzi a magasabb biztonsági sztenderdek alkalmazását.

A CRA tényleges érvényesülésének kezdő dátuma attól függ, hogy mikor dolgozzák ki és fogadják el az egyes tanúsítási rendszereket. Ezek a rendszerek különböző kiberbiztonsági kockázati szintekkel rendelkeznek, és az EU tagállamainak pedig alkalmazniuk kell azokat. A rendelet szerint a tagállamoknak és a piaci szereplőknek meg kell tenniük a szükséges lépéseket a keretrendszer hatékony alkalmazása érdekében. A jogi norma a kibervédelmi követelményeket egységesítené az EU-ban, és javítaná a digitális termékek kiberbiztonsági szintjét, előnyöket biztosítva mind a vállalkozások, mind a fogyasztók számára. A CRA két fő célt tűz ki a digitális termékek vonatkozásában: biztosítani, hogy a hardver- és szoftvertermékek a lehető legkevesebb sebezhetőséggel kerüljenek piacra, valamint kötelezni a gyártókat, hogy komolyan vegyék a biztonságot a termékek komplett életciklusán keresztül, és ösztönözni a felhasználókat, hogy vegyék figyelembe a kiberbiztonsági kérdéseket a termékek kiválasztásakor és használatában. A javaslat széles körben foglal magában termékeket, kivéve bizonyos specifikus szektorokra vonatkozó jogszabályok által lefedett digitális eszközöket. Két fő kategóriára osztja a termékeket: alapértelmezett nem kritikus termékek (pl. merevlemezek, okos otthoni asszisztensek vagy összekapcsolt játékok) és kritikus termékek (a CRA I. számú mellékletében felsorolt termékek, kiemelten virtuális magánhálózatok és routerek). A CRA a kiberbiztonság tervezési és alapértelmezési elvével kötelezettségeket ír elő a különböző

[431] 2019 júniusában lépett hatályba, de a konkrét tanúsítási rendszerek kidolgozása és bevezetése folyamatos folyamatot ró a jogalkotóra.
[432] A kiber-reziliencia szabályozására vonatkozó jogi norma tervezete elérhető: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf (letöltés: 2023.12.13.)

gazdasági szereplőkre a termékek különböző életciklusában. Az alapvető kiberbiztonsági és sebezhetőség-kezelési követelmények mellett jelentési kötelezettségeket is magában foglal.[433]

A CRA teljeskörű hatályosulását követően az EU piacán nem felelnek meg a forgalomba hozatali követelményeknek azok a digitális termékek, amelyek nem teljesítik a CRA előírásait. A CRA hatálya alá tartozó digitális termékek két fő kategóriába sorolódnak, a kockázati szinttől függően. Az első kategória az alapértelmezett nem kritikus termékek, a második pedig a kritikus termékek, amelyek további alkategóriákra oszlanak az alacsonyabb és magasabb kockázat alapján. A jogi norma szerint a különböző kockázati szintű digitális termékeknek megfelelő megfelelőségi értékelési eljárásokon kell átesniük a kiberbiztonsági kötelezettségek teljesítésének igazolására. Ezek az eljárások a gyártók által végzett egyszerű kiberbiztonsági önértékeléstől kezdve egy harmadik fél által végzett megfelelőségi értékelésig terjedhetnek.[434]

Az Európai Parlament és a Tanács a CRA-ról szóló tárgyalásokat folytatják, és az előterjesztett módosítások között szerepel a termékek kritikus besorolásának módosítása, az életciklus várható hosszának rugalmas meghatározása, a biztonsági frissítések automatikus biztosítása, az ENISA feladatainak megerősítése, valamint a CRA hatálybalépésének 36 hónapra történő elhalasztása.

6. Összegzés, az elvégzett vizsgálat és részkövetkeztetések

Megállapítottam, hogy a jogi kereteknek („kiskapuknak”) és a különösen krízishelyzetekben alkotott normák hiányosságainak kihasználása vagy az előbbiekhez kapcsolódó információk manipulálása révén a 4. számú hipotézisben megjelenített eszközökkel és módon befolyásolhatják a közvéleményt, mely által a II. és III. fejezetben megjelenítetteket kiegészítve és konkretizálva támasztottam alá a hipotézisben rögzítetteket.

[433] A kiber-reziliencia szabályozására vonatkozó jogi norma tervezete elérhető: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf (letöltés: 2023.12.13.)

[434] A kiber-reziliencia szabályozására vonatkozó jogi norma tervezete elérhető: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/739259/EPRS_BRI(2022)739259_EN.pdf (letöltés: 2023.12.13.)

A fejezetben megállapítottam, hogy a jogalkotás szerepe – a kibertér és a mesterséges intelligencia jelentette biztonsági kihívások kezelésében – leginkább az alábbi szakterületeken a jelentős:

- Az információfúzió, adatanalitika, mesterséges intelligencia jelentősége: A nemzetbiztonsági szolgálatok jogi kereteinek rendszeres felülvizsgálata elengedhetetlen mind a szakmai hatékonyság, mind a demokrácia és a jogállamiság fenntartásához. A mesterséges intelligencia és a dezinformációs műveletek összetett veszélyforrásokat jelentenek, amelyek súlyosan befolyásolhatják a nemzeti biztonsági és kiemelten a nemzetbiztonsági helyzetet. Az MI alkalmazása a dezinformációs műveletekben és az álhírek terjesztésében új dimenziót ad a kiberbiztonsági kihívásoknak. Ez a szakmai hatékonyságot, ugyanakkor a kitettséget és a fenyegetettséget is növelő eszközként jelenik meg a szolgálatok látókörében, jelentős többletfeladatokat teremtve.
- Proaktív jogalkotói szemléletmód: A nemzetbiztonsági stratégiákat és taktikákat dinamikusan kell alakítani a modern kor kihívásaihoz. Az öntanuló és folyamatosan változó kiberfenyegetések elleni védekezéshez technológiai innovációra és magasan képzett humán erőforrásra van szükség.
- Műveletek a kibertérben a pandémia idején: A járványhelyzet különösen alkalmas a dezinformáció és a hamis híresztelések terjedésére. A dezinformáció elleni küzdelemhez a büntetőeljárások megindítása, a tájékoztatási kampányok és a bizalom fenntartása egyaránt fontos, valamint ezekkel összefüggésben jelentősen megnő a jogalkotói szint felelőssége.
- A mesterséges intelligencia mindennapi megjelenése: Az MI lehetővé teszi a gépek számára a környezet érzékelését, a problémák megoldását és a célok elérését. Az MI fontos szerepet játszik az internetes kereskedelemben, az optimalizálásban és a logisztikában. Az AI-alapú alkalmazások személyre szabott szolgáltatásokat nyújtanak, de fizikai veszélyt is jelenthetnek, ha nem megfelelően tervezik vagy használják őket. Az adatok megszerzésével, illetve az adathordozó kitettségével összefüggésben előny és elhárítandó hátrány is megjelenik.

Szükséges megjegyezni előbbiekkel összefüggésben, kiemelve az ismertetett jogi szabályozási keretrendszer fontosságát, hogy a mesterséges intelligencia (ideértve a virtuális asszisztenseket, specifikus képelemző és kereső szoftvereket, hang- és arc(kép)felismerő rendszereket, valamint a robotokat, önvezető autókat és drónokat), valamint a dezinformációs

műveletek, az álhírekkel történő operáció a lakosság tömeges és súlyos megbetegedésének kockázatát hordozó járványos betegség magyarországi megjelenése és gyors terjedésekor, egymás hatását erősítő, egy adott országgal szembeni (nemzetbiztonsági) kombinációként (műveleti intézkedések sorozataként) is felfogható.

A korábban már hivatkozott, NBS által megjelenített biztonsági kockázatokkal szembeni hatékony fellépés rögzítése iránti kormányzati igény vonatkozásában célként jelenik meg a hatékonyabb összhang megteremtése a teljes védelmi és biztonsági szektor vonatkozásában. Az NBS által rögzített, súlyos megbetegedés kockázatát hordozó járványos betegség magyarországi megjelenése esetében is használható a mesterséges intelligencia, például a repülőtereken és végzett hőképalkotáshoz, valamint a betegség terjedésének nyomon követésére szolgáló egészségügyi adatok feldolgozásához is, utóbbi esetekben a „védelmet" erősíti, tényeken alapuló információkkal az esetleges álhírek (tőzsdei vagy egészségügyi pánikkeltés, információs műveletek) ellen.

Az információfúzió, adatanalitika és mesterséges intelligencia fontos szerepet játszik a nemzetbiztonsági tevékenységekben és az intézményi reformokban. A nemzetbiztonsági szolgálatok jogi keretei alapvetőek a demokrácia és jogállamiság fenntartásához, hiszen ezek a szervezetek olyan tevékenységeket végeznek, amelyek korlátozhatják az alapjogokat, és emiatt átláthatónak és elszámoltathatónak kell lenniük.

A nemzetbiztonság és az alapvető szabadságjogok közötti egyensúly megteremtése kulcsfontosságú. Az MI, a dezinformációs műveletek és az álhírek új kihívásokat jelentenek, amelyek fokozottan veszélyeztetik a nemzetbiztonságot, különösen válsághelyzetekben, mint amilyen a koronavírus-járvány is volt. Az MI alkalmazása még nagyobb kihívást jelent, hiszen képes gyorsan és hatékonyan manipulálni az információkat.

A hatékony védekezés érdekében a kormányzatnak összehangolt intézkedéseket kell tennie, amelyek magukban foglalják az MI és kiberbiztonsági képességek fejlesztését, tájékoztató kampányokat, nemzetközi együttműködést és a társadalom sebezhetőségének csökkentését célzó stratégiák kidolgozását.

A magyar nemzetbiztonsági rendszer fejlesztése során a jogalkotás és a szakpolitika területén tett lépések fontosak voltak a hatékonyság növelése és a különböző nemzetbiztonsági

szervezetek munkájának összehangolása érdekében. Az általam a proaktív jogalkotói gyakorlatra példaként megjelölt feladatköri evolúció kiemelkedő jelentőségű volt a magyar nemzetbiztonsági rendszer modernizálásában és az új típusú biztonsági kihívásokra való reagálásban. Ez a szemléletmód valószínűsíthetően a későbbiekben is érvényre jut, ha a döntéselőkészítés során a szakmai érvek továbbra is meghallgattatnak.

A nemzetközi szervezetben kidolgozott jogi normák kötelező érvénye miatt a jövő magyar szabályozási koncepciót alapvetően meghatározó dokumentumoknak tekintendőek. Az EU jogi normáival összefüggő döntéselőkészítésben és kutatásban kulcsszerepet játszó ENISA esetében fontosnak tartom megjegyezni továbbá, hogy a magyarországi jogalkotó szervek számára is hasznos tudást érdemes minél szélesebb körben beépíteni a folyamatban lévő stratégiai szintű jogi normák felülvizsgálati folyamatai során is.

X. ÖSSZEGZÉS, KÖVETKEZTETÉSEK, HIPOTÉZISEK TELJESÜLÉSE

1. Következtetések általános összefoglalása

Elértem a kutatás elején kitűzött általános és az I/4. alfejezetben megjelenített konkrét célokat, melyek a hipotézisekkel transzparens logikai kapcsolatban állnak és az alábbi területekre terjedtek ki:

A nemzetbiztonsági tevékenységet érintő, kutatásom során vizsgált jogszabálymódosításokkal és stratégiai szintű jogi normákkal összefüggésben megállapítható, hogy az új típusú biztonsági kihívásokra, kiemelten az értekezés V - VII. fejezeteiben értékelt esetekben megfelelő reakciókat adott a jogalkotó. Tudomásul kell azonban venni, hogy a jogalkotás döntően reaktív jellegét – hatékonyan – kizárólag a nemzetbiztonsági szolgálatok szakmai tevékenysége során összegyűjtött és szintetizált ismeretekre épülő javaslatok ellensúlyozhatják. A kibertér műveletekben való részvétel szabályozásának finomhangolása a legújabb szakmai vívmányok, a legfrissebb tapasztalatok tükrében indokoltnak tűnik, elég csak a folyamatosan változó körülményekre gondolnunk.

Az információ-fúziót, illetve a koordinatív fellépést[435] lehetővé tevő megoldások folyamatos vizsgálata mellett a VII. fejezetben leírtak alapján katonai nemzetbiztonsági tevékenység sajátosságaira figyelemmel a korrupcióellenes fellépés fokozása lehetőségeinek mérlegelése is szükséges. Figyelembe véve azt a tényt, hogy a hatáskörébe tartozó bűncselekmények felderítése a nyomozás elrendeléséig a Katonai Nemzetbiztonsági Szolgálat hatáskörébe tartozik[436], a bűnmegelőző és bűnfelderítő tevékenység fokozását eredményező jogintézmények finomhangolása sem tekinthető „ördögtől való elképzelésnek". A műben kiemelt kihívásokra adott reakciók volumenét alapul véve feltételezhető, hogy a hadi-, és védelmiipari fejlesztések, továbbá a haditechnikai irányú kutatás-fejlesztési és technológiai innovációs tevékenységek védelméhez fűződő nemzetbiztonsági érdek jelentősége miatt a gazdaságbiztonsági tevékenység szerepe felértékelődhet a hatáskörrel rendelkező nemzetbiztonsági szolgálat feladatrendszerében.

Az V - IX. fejezetekben megjelenített példák által alátámasztottan kijelenthető, hogy folyamatosan indokolt és szükséges az Nbtv.-ben megjelenített titkos információgyűjtést szolgáló jogintézmények újra-kodifikálása, megfeleltetése az új típusú biztonsági kihívásoknak, ideértve a különleges jogrend elrendelésének szükségességét megalapozó eseteket. Érdemes a szakmai, illetve tudományos közösségek figyelmébe ajánlani a kérdéskör további vizsgálatának indokoltságát[437] a lawfare jelentőségéről sem megfeledkezve.[438]

Annak ellenére, hogy a nemzetbiztonsági tevékenységet érintő jogszabálymódosítások és stratégiai szintű jogi normák az egyes esetekben rögzítetten, többnyire megfelelő minőségben reagáltak az új típusú biztonsági kihívásokra, a jogalkotás döntően reaktív jellegét csak a

[435] Témával kapcsolatban lásd: HÓDOS László: Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szervének közjogi helyzetéről. In.: Szakmai Szemle 2018/4.
[436] Fontos megjegyezni, hogy némiképp hasonló szabályozási környezetet találunk az Alkotmányvédelmi Hivatal vonatkozásában, melynek hatáskörébe tartozik az Nbtv. 5. § j) pontjában meghatározott bűncselekményekről való információszerzés, ugyanakkor a Katonai Nemzetbiztonsági Szolgálat nyomozást megelőző, bűnfelderítő feladatköre ezen túlmutat, utóbbi nemzetbiztonsági szolgálat honvédelmi szervezetek közötti speciális helyzetéből adódóan.
[437] A különleges jogrendet, illetve a kibertérben zajló konfliktusokat érintően konferenciák tekintetében többek között lásd: 2017. április 21. Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Kar, Magyar Tudományos Akadémia Társadalomtudományi Kutatóközpont Jogtudományi Intézet, Magyar Katonai Jogi és Hadijogi Társaság: A különleges jogrend c. konferencia, Budapest; 2019. május 8. Széchenyi István Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: Az erőszak tilalmától a kibertérben zajló konfliktusokig c. konferencia, Győr; 2019. május 29. Nemzeti Közszolgálati Egyetem, Széchenyi István Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: 80 éves az első magyar honvédelmi törvény c. konferencia, Budapest; 2019. november 19. Nemzeti Közszolgálati Egyetem, Magyar Katonai Jogi és Hadijogi Társaság: Honvédelmi jog és igazgatás aktuális kérdései c. konferencia, Budapest.
[438] A „lawfare" kifejezés használatáról és jelentéséről bővebben lásd Charles J. Dunlap: Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts. 29. 11. 2001.

nemzetbiztonsági szolgálatok VI. fejezetben kiemelt, stratégiai döntéselőkészítő tevékenysége során összegyűjtött ismeretekre épülő javaslatai ellensúlyozhatják hatékonyan. A kibertér műveletekben való részvétel szabályozásának finomhangolása indokolt a folyamatosan változó körülmények tükrében.

Általánosságban folyamatosan indokolt a titkos információgyűjtést szolgáló jogintézmények újrakodifikálása, megfeleltetése az új típusú biztonsági kihívásoknak, beleértve a különleges jogrend eseteit is. A kibertérben zajló kognitív hadviselés során összekapcsolt hálózatokon keresztül valós és hamis információkat, üzeneteket juttatnak el célzottan a közönséghez, befolyásolva a közvéleményt, csoportokat és egyéneket. Ezek a tevékenységek lehetnek támadó jellegűek, de a védekezés szempontjából is kiemelt jelentőséggel bírnak. Védekezéskor a rendszerek védelmén túl a felhasználók tudatosságának és felkészültségének erősítése is kulcsfontosságú a kibertér veszélyeivel szemben.

Az általam vizsgált és megjelenített információs tevékenységek az emberi tudatra és érzelmekre hatva befolyásolják a célcsoportok viselkedését és döntéseit. Céljuk a célcsoport gondolkodásának befolyásolása, az észlelés, attitűd és motiváció megváltoztatása. Hatással lehetnek egy állam vagy közösség hangulatára, igazságérzetére és a jogállamiságba vetett hitére. A demokratikus társadalmaknak fel kell ismerniük és kezelniük kell az idegen érdekű befolyásolásokat.

A lawfare, vagyis a jog hadviselési eszközként való alkalmazása alapvetően befolyásolja a nemzetközi kapcsolatokat és konfliktusokat. A jogi keretek és normák kihasználása vagy manipulálása révén politikai vagy katonai előnyökre tehetnek szert az államok vagy nem állami szereplők. A hibrid hadviselésben a konvencionális katonai erőszak mellett a jogi eszközök és a média manipulációja is kulcsfontosságú. A nemzeteknek fel kell ismerniük és alkalmazkodniuk kell a lawfare stratégiákhoz, megerősítve a jogrendszerüket, az információs biztonságot, valamint ezekkel összefüggésben (is) alaposan megvizsgálni a kibertér műveletek és mesterséges intelligencia lehetőségeit és veszélyeit.

Megállapítottam, hogy figyelembe kell venni a hibrid hadviselés különböző aspektusait, beleértve a stratégiai jogalkotást, a nemzeti szuverenitás kérdéseit, valamint a befolyásoló műveletek és kiberhadviselés jelentőségét. A lawfare egy komplex jelenség, amely mélyrehatóan befolyásolja a modern világ biztonsági környezetét. A NATO és az EU az

ukrajnai orosz beavatkozások során felismert a hibrid hadviseléssel összefüggő veszélyeket hatékonyan adaptálta a stratégia-, és a normaalkotás során. Az azóta készült elemzések főként az ukrajnai eseményekre alapozva próbálják megérteni a hibrid hadviselés lényegét, azonban a jövőbeni konfliktusokban eltérő módszerekre kell számítani, mivel a hibrid hadviselők alkalmazkodnak a környezethez, ennek a jogalkotás terén megnyilvánuló eredményeit vizsgálva állapítható meg, hogy a nemzetközi szerződések alapján Magyarországgal szövetséges államok jó úton járnak, melyet a hazai jogalkotásnak, doktrínafejlesztésnek is érdemes és szükséges követnie.

A biztonsági környezet változékonysága és az ellenfelek kreativitása miatt végtelen számú forgatókönyv jöhet létre, ezért az IV – V. fejezetekben részletezett okokból és módon a biztonsági és védelmi szektor munkatársainak folyamatosan erősíteniük kell a társadalom, az állam és saját szervezeteik ellenálló képességét a hibrid hadviselési intézkedésekkel szemben. Emiatt tartottam fontosnak kiemelni a IV. fejezetben, hogy a gerilla hadikultúra és a különleges hírszerzési műveletek elleni védekezés összefüggéseinek vizsgálata nélkülözhetetlen. A III - IV. fejezetekben megjelenített összefüggések értékelése alapján jelentettem ki, hogy kutatóknak a hadtörténelmi és rendészettudományi ismereteket úgy kell összevonniuk, hogy azok a jogalkotásban is hasznosíthatók legyenek. Ennek a hasznosításnak a konkrét eredményeit tártam fel a későbbi fejezetekben, valamint így igazoltam az ott leírtak szerintieket.

A pandémia alatt a jogalkotásnak gyorsan és hatékonyan kell reagálnia, egyensúlyt teremtve az egészségvédelem és az egyéni szabadságjogok között, figyelembe véve a hosszú távú következményeket és az országhatárokon átnyúló nemzetközi együttműködés fontosságát. A COVID-19 világjárvány idején a kibertérben folytatott műveletek során a dezinformáció és a hamis hírek terjedése elleni küzdelem kiemelt jelentőségűvé vált. Ez magában foglalja a büntetőeljárásokat, a tájékoztatási kampányokat és a bizalom fenntartását célzó intézkedéseket. A pandémia rávilágított arra, hogy a félretájékoztatás és az álhírek komoly veszélyt jelentenek a közegészségügyre és a társadalmi stabilitásra, ezért a jogalkotóknak és a hatóságoknak hatékonyan kell fellépniük ezek ellen. A kibertérből érkező álhírek, mint például a #FilmYourHospital összeesküvés-elmélet terjedése, komoly kihívást jelentettek a járvány elleni védekezésben. A különleges jogrend idején alkalmazott jogintézmények alapjogkorlátozó mivoltáról nem szabad megfeledkezni, minden döntésnek meg kell felelnie a szükségesség és arányosság elvének. A kibertérből kiinduló dezinformációs kampányok nagyobb hatással vannak a különleges jogrend idején, elhárításuk jelentős erőforrásokat igényel. A

nemzetbiztonsági és rendvédelmi szerveknek folyamatosan fel kell készülniük ezekre a veszélyekre. A világjárvány idején tapasztalt álhírek terjedése rámutatott arra, hogy ezek jelentős kihívást jelentenek a járványkezelésben, veszélybe sodorva életeket és anyagi javakat. A tapasztalatok felhasználhatók a jövőbeni fenyegetések kezelésére is. Még egy világjárvány okozta különleges helyzetben sem hanyagolható el az alapjogkorlátozó intézkedések szükségességének és arányosságának vizsgálata. Az így szerzett tapasztalatok alapul szolgálhatnak egy hatékonyabb, proaktívabb jogalkotási folyamat kialakításához.

A hamis információk elleni harcban fontos a tényellenőrzés és a megbízható egészségügyi források felé irányítás, de a politikai motivációk által táplált tudománytalan állítások gyökerét nehéz kiirtani, a jogi hadviselés fontosságára ezen időszakok, ezen kihívások minden eddiginél erőteljesebben hívják fel a jogalkotói figyelmet.

A magyar biztonságpolitikai stratégiai dokumentumok rendszerének elemzése során a kutatás a dokumentumok jogszabályi környezetbe illesztésére és általános helyzetükre korlátozódott, nem pedig a belső szerkezetük és tartalmuk részletes elemzésére. A stratégia fogalmát széleskörűen értelmezve, beleértve a stratégiai tervezést és dokumentumokat, kiemelve a hadviseléshez kötődő gyökereit és bővülését a nemzetközi színtérre. A stratégiaalkotás jogszabályi szabályozása, előkészítése, végrehajtása egyes kiemelt elemeinek vizsgálata és értékelése, valamint a folyamat módszertana is bemutatásra került.

A stratégiai gondolkodás és stratégiaalkotás jövőbeli kihívásai között szerepel az információk korlátozott hozzáférhetősége és a nemzetbiztonsági ágazat egyéb sajátosságai, valamint a hibrid fenyegetések jelentősége, amelyek az állami működés létfontosságú funkcióit célozzák meg. Szükség van a jövővel[439], illetve jövőkutatással való szisztematikus foglalkozásra, a proaktív jogalkotási és stratégiakészítési minőség eléréséhez folyamatosan figyelni kell a környezeti változásokra és rugalmas, általános szabályokat kell alkotni, nem szabad elutasítani sem a nemzetközi mintákból származó, gyakorlati megoldásokat és az irányítói tevékenységgel összefüggő sajátos hazai (reform)elképzeléseket sem.

[439] A jövőkutatás fontosságáról a polgári elhárítás szakterületén lásd bővebben: Drusza, T.: Jövőbeni kihívások a (polgári) nemzetbiztonsági elhárítás területén In Drusza, T. (szerk.). (2019.). *A magyar elhárítás fejlődése: Tanulmányok a katonai és polgári nemzetbiztonsági elhárítás múltjáról, jelenéről, jövőjéről*. Budapest, Magyarország: Dialóg Campus Kiadó.

A jogszabályok felülvizsgálata az egyes jogszabályok és a teljes normakörnyezet utólagos elemzésével, valamint tartalmi deregulációval és jogtechnikai jellegű módosításokkal történik, célja a jogrendszer naprakész, átlátható és biztonságos állapotban tartása. A nemzetbiztonsági szolgálatok által alkalmazott eszközök és módszerek normarendszere komplex és hierarchikus, gyakran az alapjogok korlátozásával jár, végrehajtásukat szigorú előírások szabályozzák. A jogalkotás hagyományosan reaktív, válaszként alakul ki társadalmi problémákra vagy váratlan eseményekre. Bár a reaktív jogalkotás előnye a gyorsaság, hátrányai a túlzott szabályozottság és a hosszú távú tervezés hiánya. Fontos a folyamatos együttműködés és a szakértők bevonása a hatékony jogalkotás érdekében, amely képes hosszú távú kihívások kezelésére. A technológiai fejlődés és a társadalmi részvétel döntő fontosságú a proaktív jogalkotásban, elősegítve a trendek előrejelzését és növelve az intézkedések elfogadhatóságát. A proaktív jogalkotás célja egy hosszú távú fenntarthatóságot biztosító jogrendszer létrehozása, miközben megerősíti a jogrendszerek legitimitását. A magyar nemzetbiztonsági rendszer fejlesztése során tett jogalkotási és szakpolitikai lépések meghatározóak voltak a hatékonyság növelése és a szervezetek működésének összehangolása érdekében. A proaktív jogalkotói gyakorlat kiemelkedő jelentőségű volt a modernizálásban és az új típusú biztonsági kihívások kezelésében. Azonban a munka nem ér véget a jogszabályok elfogadásával, a végrehajtás és a folyamatos felülvizsgálat ugyanolyan fontos a tényleges eredmények eléréséhez.

A VI. fejezetben megjelenített jogi sérülékenységvizsgálat fontos eszköz a nemzetbiztonsági fókuszú jogalkotásban, az alapjogok érvényesülésének felülvizsgálata, a „lawfare” kivédése, illetve előkészítése és a hibrid fenyegetések kezelése kapcsán. A jogalkotási folyamatok és a nemzetbiztonsági szolgálatok jogintézményeinek vizsgálata során kiemelendő, hogy ezek az intézmények hogyan reagálnak az új típusú biztonsági kihívásokra, és hogy működési kereteik proaktív vagy reaktív jellege milyen befolyással bír a hatékony kormányzati válaszok kialakítására.

A VII. fejezetben rögzítettek alapján kijelentettem, hogy a digitalizáció korában az adatkezelés és adatvédelem kiemelt fontosságú területté vált, különösen a védelmi és biztonsági szektor számára. Az adatok automatizált ellenőrzése, a szenzitív információk kiegyensúlyozott kezelése, a mesterséges intelligencia alkalmazásának korlátai, a magánélet védelme és az állampolgárok általános digitális biztonsága mind olyan kihívások, amelyekkel a jogalkotóknak és a szakembereknek szembe kell nézniük.

Az Európai Unió célja az állampolgárok digitális térben való védelmének megerősítése. Az elmúlt években a tárgykörben alkotott jogszabályok az átláthatóság és elszámoltathatóság növelésére, a jogellenes tartalmak szűrésére, a közérdek és alapvető jogok védelmére, a felhasználói jogok megerősítésére, a független ellenőrzés biztosítására, valamint a jogi kockázatelemzésre és a hibrid fenyegetések elleni küzdelemre összpontosítanak. Ezek a célkitűzések kulcsfontosságúak a digitális környezetben való biztonságos és etikus – államigazgatási és jogalkotói – működés szempontjából.

Magyarországon a jogalkotás kiemelt figyelmet fordít a kiberbiztonság kérdéseire. Pozitív fejlemények történtek a nemzetbiztonsági ágazat irányítási struktúrájának átalakításában, többek között a katonai és polgári nemzetbiztonságért felelős államtitkári pozíciók létrehozásával. Ezek a változások elősegítik a hatékonyabb koordinációt és a szakpolitikák összehangolását a kiberbiztonság területén. A következetes intézményszervezés és jogalkotás révén könnyebben kezelhetőek lesznek a minőségbiztosítási kihívások, és lehetőség nyílik további szabályozási reformokra. Ez elengedhetetlen a digitális környezetben felmerülő kockázatok hatékony kezeléséhez és a magas szintű kiberbiztonság fenntartásához. A jogalkotás proaktív megközelítést alkalmaz, és igyekszik lépést tartani a technológiai fejlődéssel. Ez azt jelenti, hogy a jogszabályok megalkotásakor figyelembe veszik a jövőbeni trendeket és kihívásokat, és igyekeznek olyan keretrendszert létrehozni, amely rugalmasan alkalmazkodik a változó körülményekhez. Azonban a gyakorlati megvalósítás sikerességét csak hosszabb távon lehet értékelni, hiszen a jogszabályok betartása és végrehajtása jelenti majd a valódi próbatételt.

A VIII – IX. fejezetekben leírtakban felhívtam a figyelmet arra, hogy az információfúzió, adatanalitika és mesterséges intelligencia területén a nemzetbiztonsági szolgálatok jogi kereteinek rendszeres felülvizsgálata kulcsfontosságú. Ez nem csak a szakmai hatékonyság szempontjából lényeges, hanem a demokrácia és a jogállamiság fenntartása érdekében is. A mesterséges intelligencia és a dezinformációs műveletek összetett veszélyforrásokat jelentenek, amelyek növelik a nemzetbiztonsági kihívásokat és többletfeladatokat generálnak. Ezért elengedhetetlen, hogy a jogi keretrendszer folyamatosan alkalmazkodjon ezekhez a változásokhoz, és biztosítsa a megfelelő egyensúlyt a biztonság és a polgári szabadságjogok között. Elmondható, hogy a jogalkotás kiemelt figyelmet fordít a kiberbiztonság kérdéseire, és törekszik a szabályozási hiányosságok pótlására mind hazai, mind nemzetközi szinten. A digitális környezetben felmerülő kihívások kezelése érdekében nélkülözhetetlen a proaktív

szemlélet dominanciája, valamint a technológiai fejlődéssel való lépéstartás és a különböző érdekelt felek közötti együttműködés. Ez a megközelítés elengedhetetlen a modern kor kihívásaihoz igazodó nemzetbiztonsági stratégiák és taktikák dinamikus alakításához. Ez magában foglalja az öntanuló kiberfenyegetések elleni védekezéshez szükséges technológiai innováció és képzett humán erőforrás biztosítását is. A jogalkotóknak előre kell gondolkodniuk, és olyan jogi keretrendszert kell létrehozniuk, amely rugalmasan alkalmazkodik a gyorsan változó biztonsági környezethez. A mesterséges intelligencia mindennapi megjelenése az internetes kereskedelemben, optimalizálásban és logisztikában fontos szerepet játszik, de veszélyeket is rejt magában, ha nem megfelelően tervezik vagy használják őket. Az MI rendszerek sebezhetőségei és esetleges elfogultságai kockázatokat jelenthetnek a magánéletre, a biztonságra és az alapvető jogokra nézve. Ezért elengedhetetlen, hogy a jogalkotás lépést tartson az MI fejlődésével, és olyan szabályozási keretrendszert hozzon létre, amely biztosítja az etikus és felelősségteljes alkalmazást.

A mesterséges intelligencia és a dezinformációs műveletek együttesen erősíthetik egymás hatását, különösen a műben kiemelt különleges helyzetekben, amikor a lakosság tömeges megbetegedése, illetve jelentős anyagi kár fenyeget. Az MI-alapú algoritmusok képesek lehetnek a félretájékoztatás gyors terjesztésére és célzott manipulációjára, ami súlyos következményekkel járhat a közegészségügyre, a gazdasági életre, az adott állam-, bel és külpolitikai politikai helyzetére és a társadalmi kohézióra nézve. Ezért a jogalkotóknak és a hatóságoknak fel kell készülniük az ilyen fenyegetések kezelésére, és megfelelő védelmi mechanizmusokat kell kialakítaniuk. A nemzetbiztonság és az alapvető szabadságjogok közötti egyensúly megteremtése kulcsfontosságú kihívás a digitális korban. Az MI és a dezinformációs műveletek új típusú veszélyeket jelentenek a nemzetbiztonságra, ugyanakkor a túlzott korlátozások veszélyeztethetik a polgári szabadságjogokat. A jogalkotóknak meg kell találniuk az optimális egyensúlyt, amely biztosítja a hatékony védelmet, ugyanakkor tiszteletben tartja az egyéni jogokat és a magánélet védelmét. A védekezés érdekében összehangolt kormányzati intézkedésekre van szükség, amelyek magukban foglalják az MI és kiberbiztonsági képességek fejlesztését, a tájékoztató kampányokat, a nemzetközi együttműködést és a sebezhetőség csökkentését célzó stratégiák kidolgozását. Ezek a többdimenziós erőfeszítések elengedhetetlenek a digitális fenyegetések hatékony kezeléséhez és a biztonságos online környezet megteremtéséhez.

Fontos hangsúlyozni a nemzetközi együttműködés és a harmonizáció jelentőségét a kiberbiztonság és az MI szabályozása terén. A digitális fenyegetések nem ismernek határokat, ezért elengedhetetlen a nemzetek közötti összefogás és a közös normák kialakítása. Az Európai Unió Információbiztonsági Ügynöksége (ENISA) kulcsszerepet játszik ebben a folyamatban, és a magyar jogalkotásnak is figyelembe kell vennie az uniós szintű irányelveket és ajánlásokat. A digitalizáció és a technológiai fejlődés új kihívások elé állítja a nemzetbiztonsági szektort és a jogalkotókat. Az adatkezelés, a kiberbiztonság, a mesterséges intelligencia és a dezinformáció mind olyan területek, amelyek proaktív és összehangolt szabályozási megközelítést igényelnek. A magyar jogalkotás fontos lépéseket tett ebbe az irányba, de további erőfeszítésekre van szükség a hatékony végrehajtás és a nemzetközi együttműködés terén.

A fenti elképzelések megvalósítása és a felmerült kérdések megválaszolása további kutatásokat és széles körű szakmai párbeszédet igényel, hogy Magyarország felkészülten nézzen szembe a digitális kor kihívásaival a nemzetbiztonság területén.

2. A hipotézisek teljesülése

Az értekezés öt hipotézist vizsgált, amelyek kapcsán az alábbi eredmények születtek:

H1. A nemzetbiztonsági tevékenység stratégiai szintjén nem az intézményi jogi, vagyis szervezetalkotás oldaláról történő, hanem elsődlegesen a funkcionalitást alapul vevő megközelítéssel és jogalkotással érhető el a kívánt közpolitikai célkitűzés, Magyarország nemzetbiztonsági érdekeinek védelme és céljainak érvényesítése.

A kutatásom során megvizsgáltam a funkcionalitást alapul vevő megközelítés fontosságát a nemzetbiztonsági tevékenység stratégiai szintjén, és az V – VI. fejezetek összegzésében megjelenítettek alapján megállapítottam, hogy ez a megközelítés hatékonyabb lehet a kívánt közpolitikai célkitűzés elérésében, mint az intézményi jogi megközelítés. A kutatásom eredményeként a VII. fejezet összegzésében rögzítettek szerint arra a következtetésre jutottam, hogy Magyarország nemzetbiztonsági érdekeinek védelme és céljainak érvényesítése során a nem választható külön az intézményrendszer és az egyes jogintézmények jogi reformja, a jogalkotói tevékenység – az előbbiekhez elengedhetetlenül szükséges – hatékonyságát pedig kizárólag összkormányzati szinten kialakított koncepció alapján képes kifejteni, ezáltal bizonyítva a funkcionalitást a fókuszba helyező jogalkotás

szükségszerűségét és primátusát feltételező hipotézis teljesülését. A jogalkotással elérhető közpolitikai célkitűzések vonatkozásában a VII. fejezetben (különösen a 2. alfejezetben vizsgáltam meg a proaktivitás és reaktivitás előnyeit és hátrányait.)

H2. A katonai nemzetbiztonsági tevékenység és annak jogintézményi rendszere kiemelt helyet foglal el a katonai jogintézmények rendszerében, attól nem elválasztható, ugyanakkor a speciális működési terület miatt a feladatrendszer mégis külön kezelendő, jól elhatárolható a rendészeti tevékenységtől, és ez a 2012 és 2023 közötti időszakban meg is nyilvánult.

A katonai nemzetbiztonsági tevékenység jogi normakörnyezetének vizsgálatát elvégezve megállapítottam, hogy az értékelési időszakban megfelelő válaszokat volt képes adni a jogalkotó a biztonsági kihívásokra. Ez biztosította a katonai nemzetbiztonsági tevékenység jogintézményei eszközeinek kiemelt helyét a katonai jogintézmények rendszerében. A vizsgált időszakban, különösen a hipotézis bizonyítását részletesen tartalmazó VII – VIII. fejezetekben megjelenített jogalkotói tevékenység eredményeként a polgári és a katonai nemzetbiztonsági tevékenység irányításának intézményi reformjával megvalósult az elengedhetetlenül szükséges redundancia melletti szoros együttműködés lehetősége is, melynek előnyeit az elkövetkező években lehetséges megvizsgálni, amennyiben ezekkel összefüggésben kellő mennyiségű tapasztalat gyűlt össze.

H3. A nemzetbiztonsági szolgálatok által felderített információk és megszerzett tapasztalatok közvetve, illetve közvetlenül hasznosításra kerülhetnek a megfelelő közjogi struktúrán keresztül és a lawfare útján a hibrid hadviselés elleni küzdelem, illetve az egyes, ebbe a körbe tartozó intézkedés azonosítása, illetve alkalmazása során levont következtetések eredményeként.

Megvizsgáltam és megjelenítettem a nemzetbiztonsági szolgálatok által felderített információk és megszerzett tapasztalatok hasznosságával összefüggő ismereteket a hibrid hadviselés elleni küzdelemben, és a VII – VIII fejezetekben rögzítettem azokat az eseteket, valamint az ezekből eredeztethető jogi, illetve intézményi változásokat. Az információk hasznosíthatóságát és ténylegesen hasznosított jellegét a lawfare útján a hibrid hadviselés elleni küzdelemben a közjogi reformok tükrözik, ideértve különösen a VIII – IX. fejezetekben kiemelt kognitív képességek fejlesztése és a kibertérben zajló tevékenység felértékelődését. A

megjelenített – különösen az 1. számú mellékletben szereplő – példák által alátámasztottan megállapítottam, illetve valószínűsítettem, hogy a jogalkotásban megvalósuló eredmények a felderített információknak és kibertérben zajló információs műveletek során megszerzett tapasztalatoknak köszönhetőek, ezáltal bizonyítva a hipotézist.

H4. A hibrid hadviselés eszközrendszerébe illeszkedő, az információs műveletek közé tartozó, egyes intézkedések, illetve intézkedéssorozatok jelentős hatást fejtenek ki, a célzott állam, illetve közösség döntéshozóira, illetve jogi normaalkotóira. A célzott hatás kifejtése érdekében információs műveletek precíz alkalmazása kerül végrehajtásra kiemelten a közvélemény befolyásolása útján, különösen a kibertérben továbbított közlések által.

A kutatás során megállapítottam, hogy a kibertérben zajló kognitív hadviselés során összekapcsolt hálózatokon keresztül valós és hamis információkat, üzeneteket juttatnak el célzottan a közönséghez, befolyásolva a közvéleményt, csoportokat és egyéneket. A közvélemény befolyásolására dezinformációs kampányokat, álhíreket és propagandaeszközöket használnak. A II-III. fejezetekben kifejtettem, hogy a konvencionális katonai erő alkalmazása mellett a média manipulációján túl jogi eszközök használata is kulcsfontosságú. A jog hadviselési eszközként való alkalmazása, a műben részletezett esetekben rögzítettek szerint politikai vagy katonai előnyöket eredményezhetnek az azt alkalmazó államok vagy nem állami szereplők számára. A jogi kereteknek („kiskapuknak") és a különösen krízishelyzetekben alkotott normák hiányosságainak kihasználása vagy az előbbiekhez kapcsolódó információk manipulálása révén – kiemelten a IX. fejezet összegzésében megjelenített módon – befolyásolhatják a közvéleményt. A közvélemény befolyásolására – különösen az 1. számú mellékletben részletezett – dezinformációs kampányokat, álhíreket és propagandaeszközöket használnak, melyekkel összefüggésben állításaim alátámasztására példákat jelenítettem meg, továbbá különösen a kibertérben történő alkalmazásuk elleni lehetséges megoldásokat vizsgáltam meg.

H5. A hibrid hadviselés eszközrendszerébe illeszkedő, az információs műveletek közé tartozó, egyes intézkedésekkel, illetve intézkedéssorozatokkal összefüggésben keletkezett tapasztalatok, ismeretek szövetségesi rendszeren belüli hasznosítása elengedhetetlenül szükséges a nemzeti és a szövetségi szintű reziliencia növelése

érdekében, abban az esetben is, ha a szövetségen belüli konfliktusok árnyékolják be az együttműködést a tagállamok között.

Szövetségi rendszeren belüli „baráti tűz” jelenségét a VII. fejezetben elemezve arra a megállapításra jutottam, hogy a szövetségen belüli konfliktusok súlyos következményekkel járhatnak a tagállamok együttműködésének vonatkozásában, különös tekintettel arra, hogy a hibrid hadviseléssel szemben csak szoros kooperációval lehet eredményesen fellépni, a vitákat pedig a jogszerű keretek között indokolt lefolytatni. Az értekezés VIII – IX. fejezeteiben megjelenítettem az Európai Unió jogalkotási tevékenységén keresztül a kibertérben keletkezett, hibrid hadviseléssel kapcsolatos tapasztalatok kodifikációs jellegű hasznosításának eredményeit, melyek hatályba lépésük után egységesen és következetesen fejtik ki védelmi potenciáljukat az Unió teljes területén. Az értekezés IX. fejezetében megvizsgáltam a hibrid hadviseléssel kapcsolatos tapasztalatok és ismeretek megosztásának hasznosságát a szövetségesi rendszeren belül, és alátámasztottam azt az állítást, hogy ezek az ismeretek elengedhetetlenek a nemzeti és szövetségi szintű reziliencia növeléséhez.

XI. A TUDOMÁNYOS EREDMÉNYEK ÖSSZEGZÉSE ÉS JAVASLATOK MEGFOGALMAZÁSA

1. Tudományos eredmények

1. Megállapítottam, hogy a lawfare, azaz a jog eszközként való alkalmazása jelentős hatással van a nemzetközi kapcsolatokra és a katonai konfliktusokra, ezért a nemzetbiztonsági fókuszú kutatásoknak ezt a területet feltétlenül érinteniük kell, valamint azt, hogy a nemzetbiztonsági fókuszú jogalkotásnak dinamikusan kell reagálnia az új típusú fenyegetésekre, és integrálnia kell a legújabb szakmai ismereteket és tapasztalatokat, hogy megőrizze proaktivitását és hatékonyságát a gyorsan változó biztonsági környezetben, kiemelten a hibrid hadviseléssel szemben.[440] **A bizonyítást a III. fejezetben rögzítettek alapján tartom megalapozottnak.**

[440] A 2019. február 27-én megtartott a Hadtudomány és a 21. század elnevezésű konferencián A katonai nemzetbiztonsági jog aktuális kérdései című előadásomban elemeztem a befolyásolási tevékenység és a hibrid műveletekkel összefüggő jogi keretrendszer felülvizsgálatának szükségességét, továbbá folyamatosan végeztem ennek a tárgykörnek a tudományos kutatását. Ennek a kutatásnak az eredményei az elmúlt években hasznosításra kerültek a szakmai döntéselőkészítés és a jogalkotói tevékenység során. Doktori kutatásom során Magyarországon elsőként foglalkoztam tudományos igénnyel a jogi hadviselés szerepével a hibrid műveletekkel összefüggésben, kiemelve a jogi sérülékenységvizsgálat jelentőségét.

2. A kutatás során megállapítottam, hogy a nemzetbiztonsági tevékenységet érintő jogszabálymódosítások és stratégiai szintű jogi normák általában hatékonyan reagáltak az új típusú biztonsági kihívásokra. Az egyes, különösen a katonai nemzetbiztonsági tevékenység sajátosságaira vonatkozó normák változásaiból levont következtetések alapján megállapítottam, hogy a korrupcióellenes intézkedések és a bűnfelderítés, a hadi- és védelmiipari fejlesztések, valamint a haditechnikai kutatás-fejlesztés és technológiai innovációk védelme erősítésének jogalapját megteremtő szabályozási környezet kodifikációs vizsgálata kiemelten fontos. Ezen területekkel összefüggő hatásköri felülvizsgálat szükségszerűen növeli a gazdaságbiztonsági tevékenység jelentőségét a nemzetbiztonsági ágazat felelősségi területén. **A bizonyítást a VI – VII. fejezetekben megjelenített vizsgálatok eredményként tartom indokoltnak elfogadni.**

3. Megállapítottam, hogy a dinamikusan változó biztonsági kihívások korában a jövőkutatás és a stratégiai szintű előrejelzések támogatásával működő nemzetbiztonsági fókuszú jogalkotás képes megalkotni és folyamatosan felülvizsgálni a „biztonságra törekvés rendszerét", hiszen statikus biztonság, véglegesen biztonságos állapot nem létezik, legfeljebb a kockázatokat tudják kezelni az ezért felelős, illetve erre felhatalmazott szervezetek, ide értve a nemzetbiztonsági szolgálatokat és a jogalkotót is. Ezzel összefüggésben megállapítottam, hogy a jogalkotás reaktív jellegét csak a nemzetbiztonsági szolgálatok által összegyűjtött és feldolgozott szakmai ismeretekre alapozott javaslatok képesek ellensúlyozni. Különösen igaz ez a kiemelt kibertérműveletek és az információfúzió szabályozására, valamint a kollektív fellépést lehetővé tevő normák folyamatos finomhangolásának szükségességére, figyelembe véve a dinamikusan változó körülményeket. **A bizonyítást a VII. fejezetben részletezettek alapján, különösen a VIII – IX. fejezetek összegzéseiben megjelenített szabályozási környezetben végzett kutatás útján végeztem el.**

4. A kutatás eredményeként feltártam a nemzetbiztonsági ágazatot érintő stratégia-, és jogalkotási tevékenység proaktív és reaktív normaalkotási jellemzőinek előnyeit és hátrányait. Bizonyítottam a proaktív megközelítés és a nemzetközi együttműködés fontosságát a digitális térben zajló ellenérdekelt tevékenység elleni küzdelem során. Gyakorlati példákon keresztül szemléltettem a NATO és az EU stratégiai szintű normaalkotási folyamatában meglévő, követendő és követhető megoldásokat, ideértve a – választható – iránymutatások alkalmazásának valószínűsíthető előnyeit, melyeket összegeztem. **A bizonyítást az értekezés**

VII. fejezetében hajtottam végre, melynek alátámasztására a IX. fejezetben rendszereztem a gyakorlati példákat az értekezésem szempontrendszere alapján.

5. Az értekezésemben bizonyítottam, hogy a jogi hadviselés nem kizárólag a nagyhatalmak kizárólagos előjogának számít és a nemzetbiztonsági fókuszú jogi normaalkotás eredményeként a megfelelő körültekintéssel és a szükséges stratégiai intézkedések megtételével Magyarország sem csupán elszenvedője lehet ennek a tevékenységnek. **A bizonyítást a VII. fejezetben végeztem el.**

6. Igazoltam, hogy a technológiai fejlődés csak abban az esetben eredményezi a nemzetbiztonsági ágazat képességeinek kézzel fogható növekedését, ha az együtt jár a jogi és igazgatási feladatok következetes elvégzésével, továbbá folyamatos sérülékenységvizsgálatával. **A bizonyítást a VI – IX. fejezetek részkövetkeztetéseiben jelenítettem meg és az ott leírtak alapján tartom indokoltnak elfogadni.**

2. Javaslatok az értekezés eredményeinek gyakorlati felhasználására

Az értekezés áttekintést nyújt a jogi hadviselésben rejlő lehetőségekről és kihívásokról, amelyeknek ismerete mára már elengedhetetlen az államigazgatás bármely területén vezető beosztásban dolgozók vagy vezetői pályára készülők számára. Az értekezés részletes elemzést nyújt a biztonsági fókuszú stratégiai szintű normákról, szorosan kapcsolódó jogszabályi környezetről és a hibrid konfliktusok jogi aspektusú kezeléséről. Ezek az elemek felhasználhatóak a jogi és stratégiai tervezésben, valamint a nemzetbiztonsági (szak)politika alakításában.

Fentiek alapján az értekezés eredményei kiegészíthetik a Nemzeti Közszolgálati Egyetem Államtudományi és Nemzetközi Tanulmányok Kar, a Rendészettudományi Kar és a Hadtudományi és Honvédtisztképző Kar képzéseinek tananyagát, illetve a doktori iskolák és a vezetőképző tanfolyamok ismeretanyagát. Az értekezésben megjelenített adatok és elemzések kiváló alapot nyújtanak további kutatási projektekhez, például a nemzetbiztonsági kockázatok elemzéséhez, a hibrid hadviselés hatásainak vizsgálatához vagy a nemzetbiztonsági szolgálatok tevékenységének értékeléséhez, továbbá a nemzetbiztonsági fókuszú jogi normaalkotás döntéselőkészítő folyamatainak finomhangolásához.

XII. FORRÁSJEGYZÉK

1. Felhasznált irodalom jegyzéke

1. AIDMAN, E. – ROWA, J. – VINCE, J. – van DIGGELEN, J. (2025): Designing AI-Enabled Countermeasures to Cognitive Warfare. *STO-MP-HFM-377*. NATO Science and Technology Organization. DOI: 10.14339/MP-HFM-377-06-PDF. Elérhető: https://www.sto.nato.int/document/designing-ai-enabled-countermeasures-to-cognitive-warfare/ (letöltve:2026. 04. 01.)
2. ALLAGUI, Ilhem – BRESLOW, Harris: Social media for public relations: Lessons from four effective cases. *Public Relations Review*, Vol. 42, No. 1, 2016, 20–30. o. DOI: https://doi.org/10.1016/j.pubrev.2015.12.001
3. AMODEI, Dario – OLAH, Chris – STEINHARDT, Jacob – CHRISTIANO, Paul – SCHULMAN, John – MANÉ, Dan (2016): Concrete Problems in AI Safety. arXiv preprint arXiv:1606.06565. DOI: 10.48550/arXiv.1606.06565 Elérhető: https://arxiv.org/pdf/1606.06565 (letöltve: 2026. 03. 09.)
4. AZ EURÓPAI PARLAMENT ÉS A TANÁCS (EU) 2022/2065 RENDELETE (2022) a digitális szolgáltatások egységes piacáról és a 2000/31/EK irányelv módosításáról (Digital Services Act). 2022. október 19. Elérhető: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065&qid=1666857835014 (letöltve:2023. július 31.)
5. BABOS, S. (2019). Military Cultures in the Light of Hybrid Warfare. *National Security Review: Periodical of the Military National Security Service, 2019*(2), 20–32. Elérhető: https://shortlink.uk/1snHp (letöltve: 2026.04.01.
6. BABOS, S. (2022). A nemzetbiztonsági szolgálatok felhatalmazása - nemzetközi kitekintés. *Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-Szakmai Folyóirata, 20*(1), 35–42. Elérhető: https://shortlink.uk/1snGR (letöltve: 2026.04.01.)
7. BACHMANN, S. D. – MOSQUERA, A. B. M. (2015): Lawfare and hybrid warfare – how Russia is using the law as a weapon. *Amicus Curiae – Journal of the Society for Advanced Legal Studies*, Issue 102. (Summer 2015) 25–28. Elérhető: https://journals.sas.ac.uk/amicus/article/view/2433 (letöltve:2026.04.01.)
8. BÉRES, J. (Ed.). (2018). *Külföldi nemzetbiztonsági szolgálatok*. Budapest: Zrínyi Kiadó.

9. BILAL, A. (2021): Hybrid Warfare – New Threats, Complexity, and 'Trust' as the Antidote. *NATO Review*, 2021. november 30. Elérhető: https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/ (letöltve: 2023. 10. 18.)
10. BLATNY Janet M. – SØNDERGAARD Steen (2025): *Cognitive Warfare.* NATO Chief Scientist Research Report, STO-OCS-001. Brussels, NATO STO. Elérhető: https://www.sto.nato.int/document/cognitive-warfare/ (letöltve:2026. 02. 11.)
11. BOUNEGRU, Liliana – GRAY, Jonathan – VENTURINI, Tommaso – MAURI, Michele (szerk.): *A Field Guide to „Fake News" and Other Information Disorders*. Amsterdam: Public Data Lab, 2018. DOI: https://doi.org/10.5281/zenodo.1136271. Elérhető: http://fakenews.publicdatalab.org/ (letöltve: 2024. 01. 05.)
12. BRYNEN, Rex: Countering Hybrid Threats AAR. *PAXsims*, 2011. május 15. Elérhető: https://paxsims.wordpress.com/2011/05/15/countering-hybrid-threats-aar/ (letöltve: 2023. október 11.)
13. BURKHARDT, Fabian: Russia's "Passportisation" of the Donbas: The Mass Naturalisation of Ukrainians Is More Than a Foreign Policy Tool. *SWP Comment*, No. 41 (August 2020). Berlin: Stiftung Wissenschaft und Politik. Elérhető: https://www.swp-berlin.org/publications/products/comments/2020C41_Donbas.pdf (letöltve: 2026. 03. 19.)
14. CANTWELL, D.: Shadow Wars: Hybrid Warfare in the Legal and Strategic Gray Zone. *per Concordiam — Journal of European Security and Defense Issues*, Vol. 10, Issue 1, 2020, Elérhető: https://perconcordiam.com/shadow-wars/ (letöltve: 2023. 11. 02.)
15. CARLSON, J – YEOMANS, N: Whither Goeth the Law – Humanity or Barbarity. In: SMITH, M. – CROSSLEY, D. (eds.): The Way Out – Radical Alternatives in Australia. Lansdowne Press, Melbourne, 1975. Elérhető: https://www.laceweb.org.au/whi.htm (letöltve:2019. november 1.)
16. CROWDSTRIKE (2016): Who is Cozy Bear? [online]. Elérhető: https://web.archive.org/web/20200426/https://www.crowdstrike.com/blog/who-is-cozy-bear/ (letöltve:2026.04.01.)
17. CULLEN P. (2018): Hybrid threats as a new 'wicked problem' for early warning. *Hybrid CoE Strategic Analysis*, 8. sz. Hybrid CoE – The European Centre of Excellence for Countering Hybrid Threats, Helsinki. Elérhető: https://www.hybridcoe.fi/publications/hybrid-coe-strategic-analysis-8-hybrid-threats-as-a-new-wicked-problem-for-early-warning/ (letöltve: 2026.04.01.)

18. CSIKI T. (2008): A stratégiai dokumentumok rendszere. *Nemzet és Biztonság: Biztonságpolitikai Szemle*, 1. évf. 2008/8. sz. 76–81. Elérhető: https://www.nemzetesbiztonsag.hu/cikkek/csiki_tamas-a_strategiai_dokumentumok_rendszere.pdf (letöltve: 2026.04.01.

19. DÁVID F. (2017): Nemzeti biztonság és nemzetbiztonság a stratégiaalkotásban. *Nemzetbiztonsági Szemle*, 5. évf. 3. pp. 5–21. Elérhető: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/1660 (letöltve: 2026.04.01.

20. DOBÁK I. (2015): Nemzetbiztonsági szolgálatok – Betekintés a visegrádi országok (V4) nemzetbiztonsági rendszereibe. *Hadtudományi Szemle*, VIII., 2015/4. sz. 113–130. Elérhető: https://adoc.pub/dr-dobak-imre-nemzetbiztonsagi-szolgalatok-betekintes-a-vise.html (letöltve: 2026.04.01.)

21. DOBÁK I. (2021): Thoughts on the evolution of national security in cyberspace. *Security and Defence Quarterly*, 33. évf. 1. sz. 75–85. DOI: https://doi.org/10.35467/sdq/133154 Elérhető: https://securityanddefence.pl/Thoughts-on-the-evolution-of-national-security-in-cyberspace,133154,0,2.html (letöltve: 2026.04.01.)

22. DOBÁK I. (2022): A dezinformáció – napjaink kiemelt kihívása. *Katonai Jogi és Hadijogi Szemle*, 2022. évf. 1. sz. 93–124. Elérhető: https://epa.oszk.hu/02500/02511/00020/pdf/EPA02511_katonai_jogi_szemle_2022_1_093-124.pdf (letöltve:2026.04.01.)

23. DOBÁK I. (2022): Az információgyűjtés területeinek evolúciója, a kibertér jelentősége. In DOBÁK I. (ed.): *Nemzetbiztonság a 21. század elején. Szemben a kihívásokkal*. Ludovika Egyetemi Kiadó, Budapest. 103–120. DOI: https://doi.org/10.36250/01005_07 Elérhető: https://openaccess.ludovika.hu/nke/catalog/view/183/1493/9688 (letöltve:2026.04.01.)

24. DOBÁK, I., & Babos, S. (2021). A biztonságtudatosítás lehetőségei a 21. századi platformok fényében. *Nemzetbiztonsági Szemle (Online), 9*(4), 18-34. DOI:10.32561/nsz.2021.4.2. Elérhető: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/5790 (Letöltve: 2026.04.01.)

25. DRUSZA, T. (ed.). (2019.). *A magyar elhárítás fejlődése: Tanulmányok a katonai és polgári nemzetbiztonsági elhárítás múltjáról, jelenéről, jövőjéről*. Budapest, Magyarország: Dialóg Campus Kiadó. ISBN 978-963-531-090-7. Elérhető: https://nkerepo.uni-nke.hu/xmlui/bitstream/handle/123456789/12763/web_PDF_A_magyar_elharitas_fejlodese.pdf?sequence=2 (letöltve: 2026. 04. 01.)

26. DUNLAP, C. J. Jr.: Law and Military Interventions: Preserving Humanitarian Values in 21st Conflicts. [Konferencia-előadás.] Humanitarian Challenges in Military Intervention Conference, Harvard University, 2001. november 29. Elérhető: https://people.duke.edu/~pfeaver/dunlap.pdf (letöltve: 2026. 04.01.)
27. DUNLAP, C. J., Jr. (2009): Lawfare: A Decisive Element of 21st-Century Conflicts? *Joint Force Quarterly*, Issue 54. (3rd quarter 2009) 34–39. Elérhető: https://scholarship.law.duke.edu/faculty_scholarship/3347/ (Letöltés ideje: 2023. december 19.)
28. DUNLAP, C. J., Jr. (2011). The origins of the American military coup of 2012. *Parameters, 40*, 107-125. Elérhető: https://scholarship.law.duke.edu/faculty_scholarship/2501/ (Letöltve: 2026. 04. 01.)
29. DUNLAP, C. J., Jr. (2014): Has Hamas Overplayed Its Lawfare Strategy? *Just Security*, 2014. augusztus 5. Elérhető: https://www.justsecurity.org/13781/charles-dunlap-lawfare-hamas-gaza/ (Letöltés ideje: 2023. december 19.)
30. DUNLAP, C. J., Jr. (2015). Lawfare. In J. N. Moore et al. (Eds.), *National Security Law* (pp.823-838). Carolina Academic Press, 3. Elérhető: https://scholarship.law.duke.edu/faculty_scholarship/3408/ (Letöltve: 2026. 04.01.)
31. Dutch Ministry of Defence. (2014). Kamerbrief en convenant JSCU. Elérhető: https://web.archive.org/web/20141108103250/http://www.defensie.nl/binaries/defensie/documenten/kamerstukken/2014/07/03/kamerbrief-en-convenant-jscu/kamerbrief+en+convenant+gecombineerd.pdf (Letöltve: 2026. 04. 01.)
32. Euronews. (2023. május 16.). *Turkey's disinformation election: Fake videos and wildly misleading claims.* Elérhető: https://www.euronews.com/2023/05/16/turkeys-disinformation-election-fake-videos-and-wildly-misleading-claims (Letöltés: 2023. 11. 23.)
33. EURÓPAI BIZOTTSÁG – AZ UNIÓ KÜLÜGYI ÉS BIZTONSÁGPOLITIKAI FŐKÉPVISELŐJE (2016): A hibrid fenyegetésekkel szembeni fellépés közös kerete. Közös közlemény az Európai Parlamentnek és a Tanácsnak. JOIN(2016) 18 final, 2016. április 6. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52016JC0018 (Letöltés: 2026. 04. 01.)
34. EURÓPAI BIZOTTSÁG – AZ UNIÓ KÜLÜGYI ÉS BIZTONSÁGPOLITIKAI FŐKÉPVISELŐJE (2018): A reziliencia és a hibrid fenyegetések kezelésére szolgáló képességek megerősítése. Közös közleménye az Európai Parlamentnek és a Tanácsnak. JOIN(2018) 16 final, 2018. június 13. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/PDF/?uri=CELEX:52018JC0016&from=GA (letöltve: 2022. 10. 26.)

35. EURÓPAI BIZOTTSÁG (2020): Javaslat – Az Európai Parlament és a Tanács rendelete a digitális szolgáltatások egységes piacáról (Digital Services Act) és a 2000/31/EK irányelv módosításáról. COM/2020/825 final, 2020. december 15. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A52020PC0825 (letöltve:2023. 07. 31.)
36. EWALD, J. von (1991): Treatise on Partisan Warfare. [Ford., bev.: SELIG, Robert A. – SKAGGS, David Curtis.] New York: Greenwood Press, (Contributions in Military Studies, No. 116.) [Eredeti: Abhandlung über den kleinen Krieg, 1785.] Elérhető: https://archive.org/details/TreatiseOnPartisanWarfareByEwald (letöltve: 2026. 04 01.)
37. FAOU, Matthieu – TARTARE, Mathieu – DUPUY, Thomas: Operation Ghost: The Dukes aren't back – they never left. ESET WeLiveSecurity, 2019. október 17. Elérhető: https://www.welivesecurity.com/wp-content/uploads/2019/10/ESET_Operation_Ghost_Dukes.pdf (letöltve:2020. április 26.)
38. FARKAS Á. (2018): Egy lehetséges séma Magyarország védelem-szabályozási és védelmi alkotmányos szemléletének megújításához. In FARKAS Á. (szerk.): *Védelmi alkotmányosság az új típusú biztonsági kihívások erőterében*. Magyar Katonai Jogi és Hadijogi Társaság, Budapest. 171–192. Elérhető: https://real-eod.mtak.hu/11675/ (letöltve: 2026. 04. 1.)
39. FARKAS, Á. (2017). Gondolatok az állam fegyveres védelmének lehetséges intézmény-fejlesztési irányairól. *Katonai Jogi és Hadijogi Szemle, 2017*(1-2), 103-124. Elérhető: http://www.hadijog.hu/wp-content/uploads/2018/05/Katonai-szemle-2017-1-2.pdf (letöltve: 2026.04.01.)
40. FARKAS, Á. (2018). A védelmi kötelezettségtől a fegyveres védelem rendszeréig. *Katonai Jogi és Hadijogi Szemle, 2018*(1), 7-28. Elérhető: https://epa.oszk.hu/02500/02511/00008/pdf/EPA02511_katonai_jogi_szemle_2018_1_007-028.pdf (letöltve: 2026.04.01.)
41. FARKAS, Á. (2020). Gondolatok a különleges jogrend természetéről és helyéről a modern államiságban. In R. Kelemen & Á. Farkas (Eds.), *Szkülla és Kharübdisz között – Tanulmányok a különleges jogrend elméleti és pragmatikus kérdéseiről, valamint nemzetközi megoldásairól* (pp. 317-346). Budapest: Magyar Katonai és Hadijogi Társaság. Elérhető: https://hadijog.hu/wp-content/uploads/2023/01/Farkas-Adam-Kelemen-Rolnad-Szkulla-es-Karubdisz-kozott.pdf (letöltve: 2026.04.01.)
42. FARKAS, Á. (2020). Komplex biztonság, hibrid konfliktusok, összetett válaszok. *Honvédségi Szemle, 2020*(4), 11-23. Elérhető: https://real.mtak.hu/125797/1/HSZ_2020_148_4_Farkas_Adam.pdf (letöltve: 2026.04.01.)

43. FARKAS, Á. (2023). A kibertér műveleti tevékenységek egyes szabályozási és államszervezési alapkérdései. In Á. Farkas & R. Kelemen (Eds.), *A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből* (pp. 77-95). Budapest, Magyarország: Gondolat Kiadó. ISBN 978 963 556 480 4 Elérhető: https://kiber.sze.hu/images/Kiadv%C3%A1nyok/A_fejlodes_fogsagaban.pdf (letöltve: 2026.04.01.)

44. FARKAS, Á., & Resperger, I. (2020). Az úgynevezett „hibrid hadviselés" kihívásainak kezelése és a nemzetközi jog mai korlátai. In Á. Farkas & K. Végh (Eds.), *Új típusú hadviselés a 21. század második évtizedében és azon túl - Intézményi és jogi kihívások* (pp. 132-149). Budapest: Zrínyi Kiadó. ISBN 2399964828231

45. FORGÁCS, B. (2016). A néppel az uralkodóért. Az első gerillaelméletek. *Felderítő Szemle, 2016*(1), 21-57. (Elérhető: https://hhk.uni-nke.hu/document/hhk-uni-nke-hu/2016-1.pdf (letöltve: 2026.04.01.)

46. FORGÁCS, B. (2016). Antoine Henri Jomini és a nemzeti háború. In.: B. KOLLER & V. MARSAI (Eds.), *Magyarország Európában, Európa a világban* (pp. 35-43). Budapest: Dialog Campus Kiadó. ISBN: 978-615-5680-08-3.

47. FORGÁCS, B. (2017). Reglamento de Partidas y Cuadrillas – Az első gerillaszabályzat. *Hadtudományi Szemle, 2017 (10)* 1., 23-35. ISSN 2060-0437.

48. GAJDUSCHEK, G. (2016). Közpolitikai célok megjelenése a jogban. In A. Jakab & G. Gajduschek (Eds.), *A magyar jogrendszer állapota* pp. 43-68. Budapest: MTA Társadalomtudományi Kutatóközpont. (Elérhető: https://jog.tk.hun-ren.hu/uploads/files/02_Gajduschek_Gyorgy_kozpolitika.pdf (letöltve 2026.04.01.)

49. GÁRDOS-OROSZ Fruzsina (2020): „Az alapjogok korlátozása" in JAKAB András – KÖNCZÖL Miklós – MENYHÁRD Attila – SULYOK Gábor (eds.): Internetes Jogtudományi Enciklopédia (Alkotmányjog rovat, rovatszerkesztő: BODNÁR Eszter, JAKAB András) http://ijoten.hu/szocikk/az-alapjogok-korlatozasa (letöltve: 2026.04.01.)

50. Gazdasági és Közlekedési Minisztérium (2008): *Stratégia-alkotási Kézikönyv — A Kormányzati Stratégia-alkotási Követelményrendszer (KSaK) alapján*. Budapest, GKM Elérhető: https://www.felvi.hu/pub_bin/dload/AVIR/SA_KK_2008_FINAL.pdf) (letöltve: 2026.04.01.)

51. GEERS, Kenneth (Ed.): Cyber War in Perspective: Russian Aggression against Ukraine. NATO CCD COE Publications, Tallinn, 2015. ISBN 978-9949-9544-4-5, Elérhető:

https://ccdcoe.org/uploads/2018/10/CyberWarinPerspective_full_book.pdf (letöltve:2020. 04. 26.)
52. General Intelligence and Security Service (AIVD): *AIVD Annual Report 2018.* [Közzétéve: 2019. május 14.] Elérhető: https://minbzk.sitearchief.nl/?subsite=aivd#search.1775640491411 (letöltve: 2026. 04. 01.)
53. GENINI, Davide (2025): Countering hybrid threats: How NATO must adapt (again) after the war in Ukraine. *New Perspectives*, Volume 33 Issue 2. pp. 122–149. o. DOI: 10.1177/2336825X251322719
54. GERASIMOV, V.: Cennoszty nauki v predvigyenii. *Vojenno-promislennij kurjer*, № 8 (476), (2013. február 26.) Elérhető: https://vpk.name/news/85159_cennost_nauki_v_predvidenii.html (letöltve: 2026. 04 01.)
55. GIORDANO James (2026): *Cognitive Warfare 2026: NATO's Chief Scientist Report as Sentinel Call for Operational Readiness.* Strategic Insights, National Defense University. Elérhető: https://inss.ndu.edu/Media/News/Article/4371195/cognitive-warfare-2026-natos-chief-scientist-report-as-sentinel-call-for-operat/ (letöltve:2026. 02. 11.)
56. GOLDENZIEL, Jill I.: Law as a Battlefield: The U.S., China, and the Global Escalation of Lawfare. *Cornell Law Review*, Vol. 106. (2021), 1085. o. Elérhető: https://live-cornell-law-review.pantheonsite.io/wp-content/uploads/2021/09/Goldenziel-final11234.pdf (letöltve: 2023. november 11.)
57. GOLDMAN, Adam – SCHMITT, Eric – GIBBONS-NEFF, Thomas: C.I.A. Informant Extracted From Russia Had Sent Reports to Agency for Decades. *The New York Times*, 2019. szeptember 9. Elérhető: https://www.nytimes.com/2019/09/09/us/politics/cia-informant-russia.html (Letöltve: 2020. április 26.)
58. GOSZTONYI, G. (2023). Az államok által végzett internetkorlátozás különböző eszközei, mint nemzetbiztonsági és szólásszabadsági kockázatok. In Á. Farkas & R. Kelemen (Eds.), *A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből* 135-148. Budapest, Magyarország: Gondolat Kiadó. Elérhető: https://kiber.sze.hu/images/Kiadv%C3%A1nyok/A_fejlodes_fogsagaban.pdf (letöltve:2026.04.01.)
59. GÖNCZI, L., & HOFFMAN, I. (2023). The sui generis nature of legal protection in the case of regional development aids in the Hungarian legislation and legal practice – Focused on irregularity issues. *Studia Iuridica Lublinensia,* 32(2), 117-132.

60. GRAY, Jonathan – BOUNEGRU, Liliana – VENTURINI, Tommaso: 'Fake news' as infrastructural uncanny. *New Media & Society*, Vol. 22, No. 2, 2020, 317–341. o. DOI: https://doi.org/10.1177/1461444819856912

61. GROEN, M. S., BORENE, A. & LIVERMORE, D. (2025): Quantifying the Gray Zone: A Framework for Measuring Hybrid Warfare Power Balances, *Small Wars Journal,* June 17, 2025. Elérhető: https://smallwarsjournal.com/2025/06/17/framework-for-hybrid-warfare/ (letöltve: 2025. július 30.)

62. GRUZD, A. – MAI, P.: Going viral: How a single tweet spawned a COVID-19 conspiracy theory on Twitter. *Big Data & Society*, Vol. 7, No. 2, 2020. Elérhető: DOI: https://doi.org/10.1177/2053951720938405 (letöltve: 2024. 01. 05.)

63. GRUZD, Anatoliy – ABUL-FOTTOUH, Deena – MASHATAN, Atefeh: Who is Influencing the #GDPR Discussion on Twitter: Implications for Public Relations. In: *Proceedings of the 53rd Hawaii International Conference on System Sciences (HICSS-53)*. Maui, HI, 2020. január 7., 1–10. o. DOI: https://doi.org/10.24251/HICSS.2020.319. Elérhető: http://hdl.handle.net/10125/64061 (letöltve: 2020. január 10)

64. GUEVARA, E. C.: *Guerrilla Warfare. Authorized Edition.* Melbourne: Ocean Press, 2006. ISBN: 978-1920888282

65. GULYÁS Gy. (2024): A Befogadó Nemzeti Támogatás új kihívásai a NATO 2022 Stratégiai Koncepció tükrében. *Hadtudomány*, 34. évf. E-szám (2024). DOI: 10.17047/Hadtud.2024.34.E.53 (letöltve:2026. 02. 11.)

66. HAIG Zs. (2006): Az információbiztonság komplex értelmezése. In: *Robothadviselés 6. Tudományos Szakmai Konferencia.* Különszám. Budapest: ZMNE, 2006. november 22. Elérhető: http://hadmernok.hu/kulonszamok/robothadviseles6/haig_rw6.html (letöltve: 2023. 07. 19.)

67. HAIG Zs. (2018): *Információs műveletek a kibertérben*. Dialóg Campus Kiadó, Budapest. Elérhető: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/12651 (letöltve: 2023. január 11.)

68. HAIG Zs. (2022): Kibertéri kognitív befolyásolás az információs műveletekben. *Hadtudományi Szemle*, XV. évf. 2022/2. sz. 115–130. Elérhető: https://doi.org/10.32563/hsz.2022.2.7 (letöltve:2026.04.01.)

69. HAIG, Z. (2006). Számítógép-hálózati hadviselés rendszere az információs műveletekben. *Bolyai Szemle, 2006*(1), 54-73. (Letöltve: 2023. január 11.)

70. HAIG, Z. (2011). Az információs hadviselés kialakulása, katonai értelmezése. *Hadtudomány, 2011*(1-2), 12-28. Elérhető: https://tudasportal.uni-

nke.hu/xmlui/bitstream/handle/20.500.12944/2211/HT-2011_1-2_4.pdf?sequence=2&isAllowed=y (letöltve: 2023. január 11.)

71. HÉJJA, I. (Ed.). (2007). A külföldi hírszerző és biztonsági szolgálatok. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, Kossuth Lajos Hadtudományi Kar.

72. HÉJJA, I., & Kenedli, T. (2011). Az elemző-értékelő munka elméleti és gyakorlati kérdései. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, Elérhető: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/8529 (letöltés: 2026.04.01.

73. HERZBERG, Anne: NGO „Lawfare": Exploitation of Courts in the Arab-Israeli Conflict. NGO Monitor, Jerusalem, 2010. (2. kiadás) Elérhető: https://ssrn.com/abstract=1737708 ((letöltve: 2023. január 21.)

74. HIDEG, É., MIHÓK, B., GÁSPÁR, J., SCHMIDT, P., MÁRTON, A., & BÁLDI, A. (2018). Környezeti jövőkutatás: Magyarország 2050. *Magyar Tudomány, 179*(5), 714–728. Elérhető: https://doi.org/10.1556/2065.179.2018.5.14 (letöltve:2026.04.01.)

75. HÓDOS L. – DOBÁK I. (2023): A biztonsági-stratégiai dokumentumok és a jogszabályi környezet kapcsolata. In DOBÁK I. – RESPERGER I. (szerk.): *Stratégiák, stratégiai gondolkodás, nemzetbiztonság*. Ludovika Egyetemi Kiadó, Budapest. 165–178. Elérhető: https://openaccess.ludovika.hu/nke/catalog/download/107/954/2318?inline=1 (letöltve:2026.04.01.)

76. HÓDOS, L. (2018). Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szervének közjogi helyzetéről. *Szakmai Szemle, 2018*(4), 5-18.

77. HÓDOS, L. (2019). Gondolatok a gerilla-hadviselés elleni küzdelem egyes összefüggéseinek tudományos vizsgálatáról. *Szakmai Szemle*, XVII. évf. 2019/3. szám, 67–80. o. ISSN 1785-1181.

78. HÓDOS, L. (2020). A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai. *Honvédségi Szemle*, 148. évf. 2020/4., DOI: 10.35926/HSZ.2020.4.4.

79. HÓDOS, L. (2020). Gondolatok Magyarország Nemzeti Biztonsági Stratégiájában azonosított, egyes kiemelt nemzetbiztonsági aspektusairól. *Szakmai Szemle, (*XVIII) 3, 21-31.

80. HÓDOS, L. (2022). A kibertér és a mesterséges intelligencia jelentősége és kihívásai a jogállamok nemzetbiztonsági feladatellátásában. *Military and Intelligence Cybersecurity Research Paper*, MIC_RP-2022_11. Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar, Budapest, Elérhető: https://hhk.uni-nke.hu/oktatasi-egysegek/katonai-nemzetbiztonsagi-tanszek/katonai-nemzetbiztonsagi-kiberter-muveleti-szakcsoport/research-paper (Letöltve: 2023. január 15.)

81. HOFFMAN, F. G (2009). Hybrid Warfare and Challenges. *Joint Force Quarterly*, Issue 52, 1st Quarter 2009, 34–39. Elérhető: https://apps.dtic.mil/sti/tr/pdf/ADA516871.pdf (Letöltve:2026.04.01.)

82. Hoffman, F. G. (2007): Conflict in the 21st Century: The Rise of Hybrid Wars. Arlington, VA:Potomac Institute for Policy Studies, Elérhető: https://www.potomacinstitute.org/images/stories/publications/potomac_hybridwar_0108.pdf (letöltve: 2026.04.01.)

83. HOFFMAN, I. (2021). A rendvédelmi szervek In. M Fazekas, (szerk.) *Közigazgatási jog. Általános rész I. : A közigazgatásról általában. Közigazgatási szervezeti jog. Közszolgálati jog* (pp. 222-228). Budapest, Magyarország: Eötvös Kiadó. Elérhető: https://www.scribd.com/document/680817978/Fazekas-Marianna-szerk-Kozigazgatasi-jog-Altalanos-resz-I-4-kiad-2021-1 (letöltve: 2026.04.01.)

84. HOFFMAN, I., & Kádár, P. (2021). A különleges jogrend és a válságkezelés közigazgatási jogi kihívásai I. *NKE Védelmi-Biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021(2). Elérhető: https://shortlink.uk/1n92- (Letöltve: 2024. január 19.)

85. HORNYÁK, B. (2016). A mentális állóképesség fejlesztése, mint lehetséges védelmi jellegű lélektani művelet. *Hadtudományi Szemle, 2016*(1), pp 235-246. Elérhető: http://hdl.handle.net/20.500.12944/10254 (Letöltve:2026.04.01.)

86. HVG.HU (2014. 02. 26.). Ellenőrizteti az oroszok harckészültségét Putyin, elérhető: https://hvg.hu/vilag/20140226_oroszok_harckeszultseg_ellenorzes. (Letöltve: 2021. január 12.)

87. HVG.HU (2023. 05. 29.). *Erdogan egy szavazóhely előtt osztogatott készpénzt.* Elérhető: https://hvg.hu/vilag/20230529_Erdogan_szavazohely_elott_osztogatott_keszpenzt__video (Letöltés: 2023. 11. 20.)

88. IVEN, M. – JASPER, L. – RADEMAKER, M. (2023): *Cognitive Effects in Combined Arms: A Case Study of the Division 2025*. Den Haag: The Hague Centre for Strategic Studies. 2023.02.10. Elérhető: https://hcss.nl/report/cognitive-effects-in-combined-arms-a-case-study-of-the-division-2025/ (letöltve:2026. 03. 09.)

89. Javaslat az Európai Parlament és a Tanács rendeletére a digitális szolgáltatások egységes piacáról (digitális szolgáltatásokról szóló jogszabály) és a 2000/31/EK irányelv módosításáról. COM(2020) 825 final. Brüsszel, 2020. december 15. Elérhető: https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX:52020PC0825 (letöltve:2022. 04. 18.)

90. JÁVOR, E. (2009). A nemzetbiztonsági szolgálatok társadalmi megítélése, támogatottsága, a média szerepe a társadalom véleményalkotásának formálásában. *Felderítő Szemle, 8*(2), 61-69.

91. KÁDÁR, K. (2017): *A közigazgatás stratégiai tervezésének és fejlesztésének módszertana*. [ÁROP–1.1.21 projekt tananyag.] Budapest: Nemzeti Közszolgálati Egyetem, Elérhető: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/100048 (letöltve:2026. 04. 01.)

92. KÁDÁR, P. (2023). A kibertér és a kibertérműveleti képességek jelentősége a védelmi és biztonsági tevékenységek összehangolásának fejlesztésében. In Á. FARKAS & R. KELEMEN (Eds.), *A fejlődés fogságában?: Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből* (pp. 149-165). Budapest, Magyarország: Gondolat Kiadó. Elérhető: https://kiber.sze.hu/images/Kiadv%C3%A1nyok/A_fejlodes_fogsagaban.pdf (letöltve:2026.04.01.)

93. KÁDÁR, P., & HOFFMAN, I. (2021). A különleges jogrend és a válságkezelés közigazgatási jogi kihívásai: a „kvázi különleges jogrendek" helye és szerepe a magyar közigazgatásban. *Közjogi Szemle*, 2021. 14.3., 1-11. ISSN 1789-6991., Elérhető: https://szakcikkadatbazis.hu/doc/5433473 (Letöltve 2024.02.24.)

94. KÁLMÁN, K. (2021). Nyomokban kódokat tartalmazhat? *A mesterséges intelligencia igazságszolgáltatásban történő alkalmazásának alkotmányjogi vonatkozásai a tisztességes eljáráshoz való jog tükrében. MTA Law Working Papers*, 2021/2, ISSN 2064-4515. Elérhető: https://jog.tk.hu/mtalwp/nyomokban-kodokat-tartalmazhat-a-mesterseges-intelligencia-igazsagszolgaltatasban-torteno-alkalmazasanak-alkotmanyjogi-vonatkozasai-a-tisztesseges-eljarashoz-valo-jog-tukreben (Letöltve 2022.11.21.)

95. KAPUTA, L. (2011). Fejezetek a maffia történetéből. *Szakmai Szemle, 2011*(1), 23-57.

96. KARDOSNÉ KAPONYI E: Az alapvető jogok és a jogállamiság védelmének aktuális kérdései az Európai Unióban II. *Köz-Gazdaság*, XII. évf. (2017) 1. sz. Elérhető: https://unipub.lib.uni-corvinus.hu/2667/1/KG_2017_1_Kardosne_Kaponyi_Erzsebet.pdf (letöltve:2026.04.01.)

97. KASSAI, K. (2023). A kibertérműveleti képesség szerepének, jelentőségének és fókuszának evolúciója a NATO stratégiai dokumentumai alapján. In Á. Farkas & R. Kelemen (Eds.), *A fejlődés fogságában? : Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből* (pp. 195-232).

Budapest, Magyarország: Gondolat Kiadó. Elérhető: https://kiber.sze.hu/images/Kiadv%C3%A1nyok/A_fejlodes_fogsagaban.pdf (letöltve:2026.04.01.)

98. Kazakhstan 24 (2023. 10. 27.): Otkrytie „Sztaba NATO" v Kazahsztane – „mnogovektornosztj" ili provokacija? 2023. október 27. Elérhető: https://kz24.news/news/politika/otkrytie-shtaba-nato-v-kazahstane-mnogovektornost-ili-provokatsiya.html (letöltve:2023. október 28.)

KEARNEY, Michael: Lawfare, Legitimacy and Resistance: The Weak and the Law. *The Palestine Yearbook of International Law*, Vol. XVI (2010), 79–130. o. DOI: 10.1163/22116141-90000063. Elérhető: https://ssrn.com/abstract=2153837 (letöltve: 2026.04.01.)

99. KECSKÉS, G. (2020). Az autonóm járművek jogi kérdéseinek nemzetközi kontextusa, különös tekintettel a környezetjogi vetületekre. *Állam- és Jogtudomány, 2020*(4), 52-64.

KELEMEN, R. (2016). A háború esetére szóló kivételes intézkedéseket tartalmazó 1912. évi LXIII. törvény országgyűlési vitája és sajtóvisszhangja. *Parlamenti Szemle, 2016*(1), 70-91. Elérhető: https://szakcikkadatbazis.hu/doc/3202858 (letöltve: 2026.04.01.)

KELEMEN, R. (2017). Az alaptörvény különleges jogrendi rendszerének egyes dogmatikai problémái –kitekintéssel a visegrádi államok alkotmányának kivételes hatalmi szabályaira. *Katonai Jogi és Hadijogi Szemle, 2017*(1-2), 37-68. Elérhető: https://real-j.mtak.hu/21728/1/Katonai_jogi_szemle_2017_5_1-2_.pdf (letöltve: 2026.04.01.)

100. KELEMEN, R. (2017). Cyber Attacks and Cyber Intelligence in the System of Cyber Warfare. In M. Szabó (Ed.), *Doktoranduszok Fóruma Miskolc, 2016. november 17. Állam- és Jogtudományi Kar szekciókiadványa* (pp. 117-122). Miskolc: Miskolci Egyetem.

KELEMEN, R. (2018). A Honvédelmi Tanács. Szerves fejlődés vagy elnevezésbeli hasonlóságok a magyar jogtörténetben? *Katonai Jogi és Hadijogi Szemle, 2018*(1), 63-94. Elérhető:http://epa.oszk.hu/02500/02511/00008/pdf/EPA02511_katonai_jogi_szemle_2018_1_063-094.pdf (letöltve: 2026.04.01.)

101. KELEMEN, R. (2018). A kivételes hatalom szabályozásának elméleti rendszere, honvédelmi kapcsolódásai és megvalósulása a dualizmus kori Magyarország. In Á. Farkas (Ed.), *A honvédelem jogának elméleti, történeti és kortárs kérdései* (pp. 59-86). Budapest: Dialóg Campus Kiadó, Nordex Kft.

102. KELEMEN, R. (2023). Cyberfare State modelljei: A digitális állam lehetséges irányai. In Á. FARKAS & R. KELEMEN (Eds.), *A fejlődés fogságában?: Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági*

kapcsolódásai köréből (pp. 13-42). Budapest, Magyarország: Gondolat Kiadó. Elérhető: https://kiber.sze.hu/images/Kiadv%C3%A1nyok/A_fejlodes_fogsagaban.pdf (letöltve:2026.04.01.)

103. KELEMEN, R., & FARKAS, Á. (2020). To the margin of the theory of a new type of warfare: Examining certain aspects of cyber warfare. In M. Szabó, L. Gyeney, & P. L. Láncos (Eds.), *Hungarian Yearbook of International Law and European Law (2019)* (pp. 203-226). Den Haag: Eleven International Publishing. ISBN: 978-94-6236-979-5

KELEMEN, R., & SIMON, L. (2020). A kibertérben megjelenő fenyegetések és kihívások kezelésének egyes nemzetközi jogi problémái. In: FARKAS Ádám – VÉGH Károly (szerk.): *Új típusú hadviselés a 21. század második évtizedében és azon túl – Intézményi és jogi kihívások.* Budapest: Zrínyi Kiadó, 2020, 150–170. o. ISBN 978-963-327-800-0. Elérhető: https://mek.oszk.hu/22200/22260/22260.pdf (letöltve: 2026.04.01.)

104. KENEDLI, T. (2014). Magyarország külpolitikájának stratégiai és a belőle következő nemzetbiztonsági feladatok. In I. DOBÁK (Ed.), *A nemzetbiztonság általános elmélete* (pp. 95-99). Budapest: NKE Nemzetbiztonsági Intézet.

105. KENEDLI, T. (2014). Magyarország nemzeti biztonsági stratégiája és a belőle származtatható nemzetbiztonsági feladatok. In I. DOBÁK (Ed.), *A nemzetbiztonság általános elmélete* (pp. 73-94). Budapest: NKE Nemzetbiztonsági Intézet.

106. KENEDLI, T. (2020). A Katonai Nemzetbiztonsági Szolgálat szakmai fejlődésének legfontosabb sajátosságai az elmúlt években. *Nemzetbiztonsági Szemle, 8*(1), 74–94.

107. KENEDLI, T., KIS-BENEDEK, J., & SZABÓ, K. (2016). A katonai felderítés és elhárítás evolúciója, szervezete és feladatkörei. In Á. FARKAS & P. KÁDÁR (Eds.), *Magyarország katonai védelmének közjogi alapjai* (pp. 117-126). Budapest: HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Közhasznú Nonprofit Kft.

108. KENNEDY, D. (2012): Lawfare and Warfare. In: CRAWFORD, James – KOSKENNIEMI, Martti (ed.): *The Cambridge Companion to International Law.* Cambridge: Cambridge University Press, pp 158–183. DOI: 10.1017/CCO9781139035651.011.

109. KER, D. – MONTAGNIER, P. – SPIEZIA, V. (2021): Measuring Telework in the COVID-19 Pandemic. OECD Digital Economy Papers, No. 314. OECD Publishing, Paris. Elérhető: https://doi.org/10.1787/0a76109f-en (letöltés: 2026.04.01.)

110. KESZELY, L. (2017). Védelmi igazgatás szerepe a nemzeti szintű átfogó megközelítés megvalósításában. *Doktori értekezés,* Nemzeti Közszolgálati Egyetem, Budapest.

111. KESZELY, L. (2020). A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modellje. *Honvédségi Szemle, 2020*(4), 24-48.

112. KIS-BENEDEK, J. (2021). A NATO mai politikai és katonai kihívásai. In Z. SZENES (Ed.), *A mai NATO: A szövetség helyzete és feladatai* (pp. 12-27). Budapest, Magyarország: HM Zrínyi Térképészeti és Kommunikációs Szolgáltató Nonprofit Kft.

113. KISS, Á. P. (2019): A hibrid hadviselés természetrajza. *Honvédségi Szemle*, 147. évf. 4. sz. 17–37. o. Elérhető: https://honvedelem.hu/files/files/116701/hsz_2019_4_017_037_4557.pdf (letöltés: 2026.04.01.)

114. KITTRIE, O. F. (2016): *Lawfare. Law as a Weapon of War*. Oxford University Press, New York.

KLEIN, T., & TÓTH, A. (2018). A robotika egyes szabályozási kérdései. In Á. O. HOMICSKÓ (Ed.), *Egyes modern technológiák etikai, jogi és szabályozási kihívásai*. Budapest: Károli Gáspár Református Egyetem Állam- és Jogtudományi Kar. 2018, pp. 93–117. Elérhető: https://ajk.kre.hu/images/doc4/dokumentumok/Egyes_modern_technologiak_etikai_jogi_es_szabalyozasi_kihivasai.pdf (letöltve: 2026.04.01.)

115. Komsomolskaja Pravda. *Вспышка коронавируса: По Китаю могли ударить генетическим оружием* (2020.01.24.). Elérhető: https://www.kp.ru/daily/27084/4156051/ (letöltve: 2023. 11. 20.)

116. KOVÁCS, J. (1995). *Magyarország katonai stratégiája* Kézirat. Budapest: Zrínyi Miklós Nemzetvédelmi Egyetem, 1995, (Raktári jelzet: 585/1767:2)

117. KOVÁCS, L. (2023). *Hadviselés a 21. században: kiberműveletek*. Budapest: Ludovika Egyetemi Kiadó. ISBN 978-963-531-765-3.

118. KOVÁCS, L., & KRASZNAY, C. (2017). „Mert övék a hatalom”: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során. *Nemzet és Biztonság–Biztonságpolitikai Szemle, 10*(3),pp 3–15.

119. KÖVÉR, L. (2011. november 30.). Házelnök módosító javaslata a törvénytervezethez., elérhető: www.parlament.hu/irom39/05004/05004-0022.pdf (letöltve: 2021. január 10.)

120. KRAJNCZ, Z & FORGÁCS, B & SZABÓ, J & SZABÓ, M, (eds.) (2019) *Hadtudományi lexikon: Új kötet.* Ludovika Egyetemi Kiadó Nonprofit Kft., Budapest. ISBN 978-963-531-101-9, Elérhető: http://real.mtak.hu/id/eprint/153916 (letöltve: 2026.04.01.)

121. KUN, T. (2023). Katonai tevékenységek megjelenése a közösségi médiában és egyéb kommunikációs alkalmazásokban. *Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata, 151*(5), 58-66. Elérhető: https://real.mtak.hu/182037/ https://doi.org/10.35926/HSZ.2023.5.5 (letöltve 2026.04.01.)

122. LAKATOS, L., & VARGA, A. F. (2016). A magyar honvédelmi igazgatás. In Á. FARKAS & P. KÁDÁR (Eds.), *Magyarország katonai védelmének közjogi alapjai* (pp. 159-211). Budapest: Zrínyi Kiadó. Elérhető: https://real-eod.mtak.hu/11675/1/2018-3-Farkas.pdf (letöltve 2026.04.01.)

123. LASCONJARIAS, G., & LARSEN, J. A. (Eds.). (2015). *NATO's Response to Hybrid Threats*. Rome: NATO Defense College, (Forum Paper 24.) Elérhető: https://www.files.ethz.ch/isn/195405/fp_24.pdf (letöltve: 2023. 10. 18.)

124. LIBICKI, Martin C (1997).: Information Dominance. *Strategic Forum*, No. 132. Washington D.C.: National Defense University – Institute for National Strategic Studies, 1997. november. Elérhető: https://apps.dtic.mil/sti/tr/pdf/ADA394533.pdf (letöltve: 2026.04.01.)

125. LiveNews. (2021). *Az oltás a globalisták tervének része, egy biokémiai támadás az emberiség ellen* (Összeesküvés portál, nem tudományosan lektorált) Elérhető: https://livenews.am/press/2021/132123/16/18/51/ (Letöltés: 2023. 11. 20.)

126. LUBERISSE, J. (2025): Verification Cost Asymmetry in Cognitive Warfare: A Complexity-Theoretic Framework, *arXiv preprint,* July 28, 2025. (Elérhető: DOI: 10.48550/arXiv.2507.21258. https://arxiv.org/abs/2507.21258 (letöltve:2026.04.01.)

127. LUCARELLI Sonia – MARRONE Alessandro – MORO Francesco Niccolò (eds.) (2021): *NATO Decision-Making in the Age of Big Data and Artificial Intelligence.* Brussels, NATO. Elérhető:(https://www.act.nato.int/wp-content/uploads/2024/07/20210301_AC-2020_Final-Report.pdf) (letöltve:2026. 02. 11.)

128. MAGYAR, S. & SIMON, L., (2017). A terrorizmus és indirekt hadviselése az EU kiberterében. *Szakmai Szemle, 2017*(4), 57-68. Elérhető: https://shortlink.uk/1so3r (letöltve: 2026.04.01.)

129. Magyarország Kormánya: Az egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról szóló T/1426. számú törvényjavaslat. [Előterjesztő: Dr. Pintér Sándor belügyminiszter.] Budapest, 2010. október. Elérhető: https://www.parlament.hu/irom39/01426/01426.pdf (letöltve:2021. január 8.)

130. MAO, Z. (2020): On Guerrilla Warfare. [újrakiadás], Beijing: Foreign Languages Press.

131. MARTINS, M. (2010). Reflections on “Lawfare” and Related Terms. Elérhető: https://www.lawfareblog.com/reflections-lawfare-and-related-terms (Letöltve: 2023. 04. 11.)

132. MATTIS, P. (2018). China’s ‘Three Warfares’ in Perspective. *War on the Rocks*. Elérhető: https://warontherocks.com/2018/01/chinas-three-warfares-perspective/ (Letöltve: 2022. 06. 13.)

133. MENNINGER, Karl A. (1963): *The Vital Balance: The Life Process in Mental Health and Illness*. New York: Viking Press.

134. MEZŐ, F. (2014). *PSYOPS- avagy: kalandozás a hadak útján, a pszichológia ösvényein, a történelem útvesztőiben*. Debrecen: Kocka Kör. ISBN 978-615-5267-02-4

135. MEZŐ, F. (ed.): *Lélektan és Hadviselés*, VI. 2. Elérhető: https://www.kpluszf.com/assets/docs/LH/LH_2024_2.pdf és https://doi.org/10.35404/LH.2024.2.1 (letöltve: 2026.04.01.)

136. MIVIL, O. (2020). Malaysian judiciary makes history, uses AI in sentencing. Elérhető: https://www.nst.com.my/news/nation/2020/02/567024/malaysian-judiciary-makes-history-uses-ai-sentencing (Letöltve: 2023. 05. 11.)

137. MOLNÁR, F. (2023). Kitekintés – a nemzeti ellenálló képesség, a NATO és az Európai Unió viszonylatában. In P. KÁDÁR (Ed.), *A védelmi és biztonsági szabályozás magyarországi reformja* (pp. 290-303). Budapest, Magyarország: Nemzeti Közszolgálati Egyetem. Elérhető: https://real.mtak.hu/230641/1/1232_327-342.pdf (letöltve: 2026.04.01.)

138. MUNK, S. (2002). Az információs műveletek típusai és modelljei. *Hadtudomány, 2002*(1). Elérhető: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/2220 (letöltve: 2026.04.01.)

139. MUNOZ MOSQUERA, A. B. & BACHMANN, S. D. (2016): Lawfare in Hybrid Wars: The 21st Century Warfare. *Journal of International Humanitarian Legal Studies*, Vol. 7, No. 1. 63–87. Elérhető: https://doi.org/10.1163/18781527-00701008 (letöltve:2026.04.01.)

140. NATO (2022): *Madrid Summit Declaration*. 2022. június 29. Elérhető: https://www.nato.int/cps/en/natohq/official_texts_196951.htm (letöltve: 2023. 12. 16.)

141. NATO (2023): Symposium in Finland brings industry and experts together to strengthen NATO's responses to hybrid threats. *NATO News*, 2023. december 15. (Elérhető: https://www.nato.int/cps/en/natohq/news_221179.htm (letöltve: 2023. 12. 16.)

142. NATO (*2023): Vilnius Summit Communiqué*. 2023. július 11. Elérhető: https://www.nato.int/cps/en/natohq/official_texts_217320.htm (letöltve: 2026. 02. 11.)

143. NATO ACT. (2022). *NATO 2022 Strategic Concept*. Elérhető: https://www.act.nato.int/wp-content/uploads/2023/05/290622-strategic-concept.pdf (Letöltve: 2023. október 11.)

144. NATO ACT. (2023). *Cognitive Warfare: Strengthening and Defending the Mind*. Elérhető: https://www.act.nato.int/article/cognitive-warfare-strengthening-and-defending-the-mind/ (letöltve: 2023. október 11.)

145. NATO ACT: Understanding Lawfare in a Hybrid Warfare Context. *NATO Legal Gazette*, Issue 37 (October 2016). Elérhető: https://www.act.nato.int/wp-content/uploads/2023/05/legal_gazette_37.pdf (letöltve:2023. október 11.)
146. NATO AJP-10.1 (2023): Allied Joint Doctrine for Information Operations. Edition A Version 1. Brussels: NATO Standardization Office. Elérhető: https://www.gov.uk/government/publications/allied-joint-doctrine-for-information-operations-ajp-101 (letöltve ideje: 2026. 02. 11.)
147. NEAL, J. J.: Deterrence in a Hybrid Environment: Defending against Nonlinear Threats. *per Concordiam — Journal of European Security and Defense Issues*, Vol. 10, Issue 1, 2020, pp. 16-23. Elérhető: https://perconcordiam.com/deterrence-in-a-hybrid-environment/ (letöltve: 2026. 04. 01.)
148. NewsGuard: False Claim Fingerprints [korábban: Misinformation Fingerprints]. Elérhető: https://www.newsguardtech.com/solutions/misinformation-fingerprints/ (letöltve: 2024. 01. 08.)
149. NewsGuard: How NewsGuard's Misinformation Fingerprints Provide Early Warning Alerts for Emerging Online Threats. [online, vállalati ismertető] Elérhető: https://www.newsguardtech.com/insights/how-newsguards-misinformation-fingerprints-can-help-security-defense-and-intelligence-companies-stay-on-top-of-misinformation-threats/ (letöltve: 2024. 01. 08.)
150. NewsUA. *Если зачистят Карабах, следующими будут Донбасс и Приднестровье* (2020. 09 29.). Elérhető: https://newsua.ru/news/32690-esli-zachistyat-karabakh-sleduyushchimi-budut-donbass-i-pridnestrove (letöltve: 2023. 10. 30.)
151. NEWTON, Michael A.: Illustrating Illegitimate Lawfare. In: *Case Western Reserve Journal of International Law*, Vol. 43, 2010, pp. 255–273. Elérhető: https://scholarship.law.vanderbilt.edu/faculty-publications/741/ (letöltve: 2026.04.01.)
152. OPPENHEIMER, A.: Watch out for an explosion of A.I.-generated fake news sites in 2024. *Miami Herald* / Yahoo News, 2024. január 5. Elérhető: https://news.yahoo.com/watch-explosion-generated-fake-news-193243084.html (letöltve: 2024. 01. 05.)
153. Orosz Hírek. (2023) *A Kreml reagált Orbán Viktor nyilatkozatára, amely szerint az EU békefenntartó csapatokat küldene Ukrajnába.* Elérhető: https://oroszhirek.hu/a-kreml-reagalt-orban-viktor-nyilatkozatara-amely-szerint-az-eu-bekefenntarto-csapatokat-kuldene-ukrajnaba/ (letöltve: 2023. 05. 22.)

154. Orosz Hírek. (2023). *Hersh: Az USA az Északi Áramlat szabotázsával akarta megfenyegetni Putyint.* Elérhető: https://oroszhirek.hu/hersh-az-usa-az-eszaki-aramlat-szabotazsaval-akarta-megfenyegetni-putyint/ (letöltve: 2023. 05. 22.)

155. Orosz Hírek. (2023). *Medvegyev a fasiszta rezsimhez hasonlítja a kijevi kormányt, és Hitlerként ábrázolja Zelenszkijt.* Elérhető: https://oroszhirek.hu/medvegyev-a-fasiszta-rezsimhez-hasonlitja-a-kijevi-kormanyt-es-hitlerkent-abrazolja-zelenszkijt/ (letöltve: 2023. 05. 22.)

156. Orosz Hírek. (2023). *Medvegyev: Meg kell futamítani a teljes „kábítószeres" kijevi rezsimet.* Elérhető: https://oroszhirek.hu/medvegyev-meg-kell-futamitani-a-teljes-kabitoszeres-kijevi-rezsimet/ (letöltve: 2023. 05. 22.)

157. Orosz Hírek. (2023). *Német képviselő: Az amerikai erőket az atomfegyverekkel együtt ki kell vonni Németországból.* Elérhető: https://oroszhirek.hu/nemet-kepviselo-az-amerikai-eroket-az-atomfegyverekkel-egyutt-ki-kell-vonni-nemetorszagbol/ (letöltve: 2023. 05. 22.)

158. Orosz Hírek. (2023). Sojgu: *Az USA zsarolja az országokat, hogy harcoljanak Moszkva és Peking ellen.* Elérhető: https://oroszhirek.hu/sojgu-az-usa-zsarolja-az-orszagokat-hogy-harcoljanak-moszkva-es-peking-ellen/ (letöltve: 2023. 05. 22.)

159. PASCU, C. – BARROS LOURENÇO, M. (eds.) (2023): *Artificial Intelligence and Cybersecurity Research*. ENISA Research and Innovation Brief. European Union Agency for Cybersecurity (ENISA), Brüsszel, 2023. június 7. Authors: NTALAMPIRAS, S – MISURACA, G – ROSSEL, P. Elérhető: https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research (letöltve:2023. november 3.)

160. PETRUSKA F. (2021): A Lawfare fogalma. *Katonai Jogi és Hadijogi Szemle*, 9. évf. 3. sz. 97–106. Elérhető: https://epa.oszk.hu/02500/02511/00018/pdf/EPA02511_katonai_jogi_szemle_2021_3_097-106.pdf (letöltve:2026.04.01.)

161. PORKOLÁB I. (2015): Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? *Hadtudomány*, 25. évf. 3–4. sz. 36–48. Elérhető: https://real.mtak.hu/29824/1/2015_3_4_5.pdf (letöltve: 2026.04.01.)

162. PORKOLÁB Imre: A hadviselés adaptációja: harc az emberi elméért. *Hadtudományi Szemle*, VII. évf. (2014) 3. sz. 56–69. o. Elérhető: https://epa.oszk.hu/02400/02463/00024/pdf/EPA02463_hadtudomanyi_szemle_2014_03_056-069.pdf (letöltve: 2026.04.01.)

163. RÁCZ, A. (2015). Russia's Hybrid War in Ukraine: Breaking the Enemy's Ability to Resist. *FIIA Report 43.* Finnish Institute of International Affairs.

Elérhető:https://www.fiia.fi/en/publication/russias-hybrid-war-in-ukraine (letöltve: 2022. 01. 19.)

164. RÁCZ, L. (2020). A személy és a dolog fogalmának (lehetséges) változásai a mesterséges intelligencia és a kriptovaluták világában. *Állam- és Jogtudomány, 2020*(4), 82-107. Elérhető: http://real.mtak.hu/118518/ (letöltve: 2026.04.01.)

165. RESPERGER I. (2018). *A válságkezelés és a hibrid hadviselés.* Budapest: Dialóg Campus Kiadó,. ISBN 978-615-587-753-7. Elérhető: https://nbi.uni-nke.hu/document/nbi-uni-nke-hu/Resperger%20Istv%C3%A1n_A%20v%C3%A1ls%C3%A1gkezel%C3%A9s%20%C3%A9s%20a%20hibrid%20hadvisel%C3%A9s.pdf (letöltve: 2026.04.01.)

166. RESPERGER István (ed.) (2018): *Nemzetbiztonsági alapismeretek.* Budapest: Dialóg Campus Kiadó, 2018. (Studia Universitatis Communia) ISBN 978-615-584-567-3. (Elérhető: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6909) (letöltve: 2026.04.01.)

167. RESPERGER, I. (2013). Biztonsági kihívások, kockázatok, fenyegetések és ezek hatása Magyarországra 2030-ig. *Felderítő Szemle, 12*(3), 5-37. Elérhető: https://n9.cl/btuwt

168. RESPERGER, I. (2018). A nemzetbiztonsági szolgálatok tevékenysége – biztonsági kihívások, kockázatok és fenyegetések. In I. RESPERGER (Ed.), *A nemzetbiztonság elmélete a közszolgálatban* Budapest: Dialóg Campus. ISBN: 9786155845666 Elérhető: https://tudasportal.uni-nke.hu/xmlui/handle/20.500.12944/6908?show=full (letöltve: 2026.04.01.)

169. ROBBINS, Joseph: Countering Russian Disinformation. *The Post-Soviet Post — Center for Strategic and International Studies (CSIS)*, 2020. 09 23. Elérhető: https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation (letöltve: 2023. 11. 20.)

170. RÓZSA T. (2019): Az információs műveletek elmélete, gyakorlata és tendenciái. Honvédségi Szemle, 147. évf. 2019/5. sz. 73–87. Elérhető: https://real-j.mtak.hu/13949/17/Honvedsegi_Szemle_2019_5_teljes_szam.pdf (letöltés: 2026.03.12.)

171. SABJANICS I. (2017): A nemzetbiztonság jogi koncepciója. In: CSINK L. (szerk.): *A nemzetbiztonság kihívásainak hatása a magánszférára*. Pázmány Press, Budapest. 103–123. (A Pázmány Péter Katolikus Egyetem Jog- és Államtudományi Karának Könyvei – Tanulmányok, 40.) Elérhető: https://jak.ppke.hu/uploads/articles/1185528/file/Csink_maganszfera_TAN40.pdf (letöltve: 2026.04.01.)

172. SÁFRÁN, J. (2018). Az Amerikai Egyesült Államok és Magyarország nemzetbiztonsági szervezetrendszerének összehasonlító elemzése. *Felderítő Szemle, 2018*(1), 71-87. Elérhető: https://n9.cl/7zpsc (letöltve:2026.04.01.)

173. SARI, A. (2019): Hybrid Warfare, Law, and the Fulda Gap. In: WILLIAMS, W. S. – FORD, C. M. (szerk.): *Complex Battlespaces: The Law of Armed Conflict and the Dynamics of Modern Warfare*. Oxford University Press, New York. 161–190. Elérhető: https://doi.org/10.1093/oso/9780190915360.003.0006 (letöltve: 2026.04.01.)

174. SCHMITT, Michael N. (2020) Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention. *International Law Studies*, 2020, Vol. 96. 549–576. Elérhető: https://digital-commons.usnwc.edu/cgi/viewcontent.cgi?article=2932&context=ils (letöltve: 2026.04.01.)

175. SCHMITT, Michael N. (2021) Autonomous Cyber Capabilities and the International Law of Sovereignty and Intervention. In: LIIVOJA, Rain & VÄLJATAGA, Ann (eds.): *Autonomous Cyber Capabilities under International Law*. Tallinn, NATO CCDCOE Publications, 126–151. Elérhető: https://ccdcoe.org/uploads/2021/05/Autonomous-Cyber-Capabilities-under-International-Law.pdf (letöltve: 2026.04.01.)

176. SCIUTTO, Jim et al.: Exclusive: US extracted top spy from inside Russia in 2017. *CNN Politics*, 2019. szeptember 9. Elérhető: https://edition.cnn.com/2019/09/09/politics/russia-us-spy-extracted/index.html (letöltve: 2020. április 26.)

177. SESKURIA, Natia: Russia's „Hybrid Aggression" against Georgia: The Use of Local and External Tools. Center for Strategic and International Studies (CSIS), 2021. [online] Elérhető: https://www.csis.org/analysis/russias-hybrid-aggression-against-georgia-use-local-and-external-tools (letöltve: 2023. 11. 02.))

178. SIMICSKÓ, I. (2017). A hibrid hadviselés előzményei és aktualitásai. *Hadtudomány, 2017*(3–4), 3–16. DOI: 10.17047/HADTUD.2017.27.3–4.3. Elérhető: http://real.mtak.hu/67458/1/Ht_201734_5_18_u.pdf (letöltve: 2023.07.19)

179. SIMON, L. (2016). Az információ, mint fegyver? *Szakmai Szemle, 2016*(1), 34-60. Elérhető: https://shortlink.uk/1so2s (letöltve: 2026.04.01.)

180. SOLTI I. (2014): A nemzetbiztonsági stratégia a Nemzeti Biztonsági Stratégia tükrében. *Nemzetbiztonsági Szemle*, 2. évf. 3. sz. 47–60. Elérhető: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/2084 (letöltve: 2026.04.01)

181. SOMODI, Z., & KISS, Á. P. (2019). A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. *Honvédségi Szemle – Hungarian Defence Review, 147*(6), 22–

28. (Elérhető: https://real.mtak.hu/105176/ DOI:10.35926/HSZ.2019.6.2 (letöltve: 2026.04.01.)
182. SPITZER J (2019): A különleges jogrend szabályozása az egyes alkotmányokban IV. – Különleges jogrendi szabályozás a francia jogrendszerben. *Vélemények a katonai jog világából*, 2019/4. Magyar Katonai Jogi és Hadijogi Társaság, Budapest, 2019, 1–13. o. Elérhető: http://real-eod.mtak.hu/11680/1/2019-4-Spitzer.pdf (letöltve: 2026.04.01.)
183. SPITZER, J. (2023). A kibertérből érkező támadások lehetséges nemzetközi jogi értelmezései, különös tekintettel az önvédelemhez való jogra. *Katonai Jogi és Hadijogi Szemle, 2023*(2), 6-29. Elérhető: https://real-j.mtak.hu/25768/7/Katonai_jogi_szemle_2023_11_2.pdf (letöltve: 2026.04.01.)
184. SPITZER, J., & VIKMAN, L. (2023). Katonai és Nemzetbiztonsági képességfejlesztések és azok jogi, jogpolitikai háttere egyes transzatlanti államokban. In Á. FARKAS & R. KELEMEN (Eds.), *A fejlődés fogságában?: Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből* (pp. 233-260). Budapest, Magyarország: Gondolat Kiadó. Elérhető: https://kiber.sze.hu/images/Kiadv%C3%A1nyok/A_fejlodes_fogsagaban.pdf (letöltve:2026.04.01.)
185. SZABÓ K. (2018): A katonai kémelhárítás feladatrendszerének új vonásai Európa és Magyarország megváltozott biztonsági környezetében. *Felderítő Szemle*, XVII. évf. 2. sz. (2018), 179–189. o. Elérhető: https://shortlink.uk/1snu5 (Letöltve: 2026. 04. 01).
186. SZABÓ, J. (Ed.). (1995). *Hadtudományi Lexikon I. kötet*. Budapest: Magyar Hadtudományi Társaság.
187. SZENES Z. (2021): A hibrid fenyegetések elleni szakpolitika Magyarországon. *Hadtudomány*, 31. évf. 4. sz. (2021), 39–56. o. DOI: 10.17047/Hadtud.2021.31.4.39 Elérhető: https://real.mtak.hu/144762/1/8166-Cikk%20sz%C3%B6vege-35173-1-10-20220216.pdf (letöltve:2026.04.01.)
188. SZUN-CE (1995): *A hadviselés törvényei (Szun-ce ping-fa)*. Fordította: Tőkei Ferenc. Balassi Kiadó, Budapest. Elérhető: https://mek.oszk.hu/01300/01345/01345.htm (Letöltés ideje: 2023. december 18.)
189. SZŰCS, P., & Solti, I. (2014). A magyar nemzetbiztonsági szféra és a nyilvánosság. *Nemzetbiztonsági Szemle*, 2. évf. 2. sz. (2014), 72–92. o. Elérhető: https://epa.oszk.hu/02500/02538/00003/pdf/ (letöltve:2026.04.01.)

190. TABER, R. (1970): *The War of the Flea: A Study of Guerrilla Warfare, Theory and Practice*. The Citadel Press, New York. 21. Elérhető: https://archive.org/details/waroffleastudyof0000tabe_v0s3 (letöltve: 2026.04.01.

191. The Economist. (2016. 09 22.). *Bear on bear.,* Elérhető: https://www.economist.com/united-states/2016/09/22/bear-on-bear (Letöltve: 2026. 04. 01.)

192. TOMOLYA J. (2018): Az úgynevezett „Geraszimov-cikk" margójára. *Hadtudomány*, 28. évf. 3–4. sz. DOI: https://doi.org/10.17047/HADTUD.2018.28.3-4.79. Elérhető: https://ojs.mtak.hu/index.php/hadtudomany/article/view/6822 (letöltve:2026.04.01.)

193. TORDA P. (2025): A dezinformáció elleni fellépés a NATO stratégiai kommunikációjában. *Nemzetbiztonsági Szemle*, 13. évf. 1. sz. 3–14. DOI: https://doi.org/10.32561/nsz.2025.1.1. Elérhető: https://folyoirat.ludovika.hu/index.php/nbsz/article/view/7548 (letöltve:2026. március 12.)

194. TROPIN, Z. (2021): Lawfare as part of hybrid wars: The experience of Ukraine in conflict with Russian Federation. *Security and Defence Quarterly*, Vol. 33, No. 1. 15–29. Elérhető: DOI: https://doi.org/10.35467/sdq/132025 (letöltve:2026.04.01.)

195. Tsargrad.md. (2023. augusztus 24.). *O momente istiny: Potere Moldaviej.* (orosz propagandaforrás, tudományosan nem lektorált) Elérhető: https://md.tsargrad.tv/articles/o-momente-istiny-potere-moldaviej-suvereniteta-i-juridicheskom-prave-pmr-na-nezavisimost_855545 (Letöltés: 2023. 08. 24.)

196. URBÁN A. (2020): A koordinációs folyamatok intézményi hátterének evolúciója a magyar nemzetbiztonsági igazgatásban. *Nemzetbiztonsági Szemle*, 8. évf. 1. sz. 5–32. DOI: https://doi.org/10.32561/nsz.2020.1.1. Elérhető: https://epa.oszk.hu/02500/02538/00032/pdf/EPA02538_nemzetbiztonsagi_szemle_2020_01_005-032.pdf (letöltve: 2026.04.01.)

197. VERESS CS. B. (2022): Jogviselés: a jog mint háborús fegyver. *Erdélyi Jogélet*, 3. évf. 3. sz. 147–164. Elérhető: https://www.jogelet.ro/index.php/eje/article/view/228 (letöltve: 2026.04.01.)

198. VERESS CS. B. (2023): Kisebbségi jogok felhasználása hibrid hadviselési eszközként. *Honvédségi Szemle: A Magyar Honvédség Központi Folyóirata*, 151. évf. 1. sz. 29–40. DOI: https://doi.org/10.35926/HSZ.2023.1.3. Elérhető: https://kiadvany.magyarhonvedseg.hu/index.php/honvszemle/article/view/927 (letöltve: 2026.04.01.)

199. VIKMAN L. (2023): Gondolatok a kiberbiztonsági stratégiák fejlesztésére vonatkozó nemzetközi útmutató kapcsán. In: FARKAS Á. & KELEMEN R. (eds.): *A fejlődés*

fogságában? Tanulmányok a kibertér és a mesterséges intelligencia 21. századi állam- és jogfejlesztési, társadalmi, biztonsági kapcsolódásai köréből. Gondolat Kiadó, Budapest. pp. 97-106. ISBN: 978-963-556-480-4. Elérhető: https://www.knbsz.gov.hu/kiadvanyok (letöltve:2026.04.01.)

200. VOYGER, M: Waging Lawfare: Russia's Weaponization of International and Domestic Law. *per Concordiam — Journal of European Security and Defense Issues*, Vol. 10, Issue 1, 2020, p. 32. Elérhető: https://perconcordiam.com/perCon_V10N1_ENG.pdf (letöltve: 2023. 11. 02.)

2. Felhasznált nemzeti jogi normák

Alaptörvény

201. Magyarország Alaptörvénye, 2011. április 25.

Törvények

202. 1995. évi CXXV. törvény a nemzetbiztonsági szolgálatokról

203. 2010. évi XLII. törvény a Magyar Köztársaság minisztériumainak felsorolásáról

204. 2010. évi CXXX. törvény a jogalkotásról

205. 2010. évi CXLVII. törvény az egyes rendészeti tárgyú és az azokkal összefüggő törvények módosításáról

206. 2011. évi CLXXI. törvény a nemzetbiztonsági szolgálatokról szóló 1995. évi CXXV. törvény katonai nemzetbiztonsági szolgálatok összevonásával kapcsolatos módosításáról

207. 2024. évi LXIX. törvény Magyarország kiberbiztonságáról

208. 2024. évi LXXXIV. törvény a kritikus szervezetek ellenálló képességéről

Kormányrendeletek

209. 212/2010. (VII. 1.) Korm. rendelet az egyes miniszterek, valamint a Miniszterelnökséget vezető államtitkár feladat- és hatásköréről

210. 232/2010. (VIII. 19.) Korm. rendelet a Terrorelhárítási Központról

211. 295/2010. (XII. 22.) Korm. rendelet a terrorizmust elhárító szerv kijelöléséről és feladatai ellátásának részletes szabályairól

212. 94/2018. (V. 22.) Korm. rendelet a Kormány tagjainak feladat- és hatásköréről

Miniszteri rendeletek és utasítások

213. 61/2009. (XII. 14.) IRM rendelet a jogszabályszerkesztésről

214. 23/2020. (IV. 24.) HM utasítás a honvédelmi szervezetek 2020. évi kiemelt feladatainak, valamint a 2021-2022. évi fő célkitűzéseinek meghatározásáról

215. 4/2022. (VI. 11.) MK utasítás a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról

216. 30/2022. (VII. 29.) HM utasítás a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról

Országgyűlési határozatok

217. 11/1993. (III. 12.) Ogy. határozat a Magyar Köztársaság biztonságpolitikai alapelveiről

218. 27/1993. (IV. 23.) Ogy. határozat a Magyar Köztársaság honvédelmének alapelveiről

219. 94/1998. (XII. 29.) Ogy. határozat a Magyar Köztársaság biztonság- és védelempolitikájának alapelveiről

Kormányhatározatok

220. 2144/2002. (V. 6.) Korm. határozat a Magyar Köztársaság új nemzeti biztonsági stratégiájáról

221. 2073/2004. (III. 31.) Kormány határozat a Magyar Köztársaság új nemzeti biztonsági stratégiájáról

222. 1144/2010. (VII. 7.) Korm. határozat a Kormány ügyrendjéről

223. 1035/2012. (II. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

224. 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról

XIII. MELLÉKLETEK

1. számú melléklet: Példák detektált dezinformációs műveletekre a kibertérben

Joseph Robbins[441], az „Oroszország általi dezinformáció elleni küzdelem" című cikkében úgy határozza meg a dezinformációt, hogy *„az egy olyan eszköz, amelyet számos állam használ a viszály keltésére, a kormányzati intézményekbe vetett hit aláásására, félelem és szorongás szítására, valamint végül bizonyos politikai célok elérésére"*[442]. Publikációjában kiemeli, hogy az elmúlt években Oroszország, kormányzati szervei és velük kapcsolatos csoportok közösségi média érzékenységét és a komplex dezinformációs stratégiájukat használták fel az orosz befolyás erősítésére, elsősorban azáltal, hogy gyengítették politikai ellenfeleiket (személyeket, szervezeteket és államokat egyaránt).

Ez a dezinformációs tevékenység arra késztette a különböző országokat, hogy fejlesszék a nemzeti ellenállóképességüket az orosz kampányok ellensúlyozására. A cseh és az észt válaszokat vizsgálva a cikk határozott és célirányos megoldásokat javasol erre a növekvő fenyegetésre, ideértve.

Az orosz dezinformációs műveletek napjainkban az ország befolyásoló erőfeszítéseinek alapkövei. Az ilyen műveletek, mint korábban megjelenített a Cozy Bear vagy a Fancy Bear kiberkémcsoportok által végrehajtottak, világszerte komoly aggodalmat és jelentős bizonytalanságot eredményeztek. Az orosz dezinformációs erőfeszítések a modern „aktív intézkedések", vagyis a Szovjetunió által szervezett propagandatevékenységek gyökereiből nőttek ki a hivatkozott publikáció megállapításait summázva[443]. A szerző felhívja a figyelmet arra is, hogy a mai orosz erőfeszítések sokkal sikeresebbek, mint amit a Szovjetunió valaha is el tudott volna képzelni, köszönhetően a kibertér létezésének, a korábbi kommunikációs stratégiák újragondolásának és a közösségi média tartalomfogyasztási szokásainak. A cseh válaszok jelentősen hozzájárulnak az orosz dezinformáció elleni küzdelemhez[444]. A cseh

[441] A Texas Tech University-n szerzett PhD fokozatot, a Valdosta State University politikatudományi tanszékének vezetője.
[442] Elérhető: https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation (Letöltés: 2023. 11. 20.)
[443] Elérhető: https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation (Letöltés: 2023. 11. 20.)
[444] Elérhető: https://www.csis.org/blogs/post-soviet-post/countering-russian-disinformation (Letöltés: 2023. 11. 20.)

kormányzati szervek, beleértve a Terrorellenes és Hibrid Fenyegetések Elleni Központot (CTHT), valamint a civil társadalmi csoportok és a think tank-ek tevékenysége kiemelkedő ezen a területen. Tekintettel arra, hogy a „think tank" egy kutatóintézet vagy politikai elemző csoport, amely kutatásokat és tanulmányokat végez különböző társadalmi, gazdasági, politikai, technológiai és stratégiai kérdésekben, szerepük kiemelkedő a nemzeti ellenállóképesség és a dezinformáció elleni küzdelemben. Ezek az intézmények gyakran befolyásolják a közpolitikát, ajánlásokat és stratégiákat kínálva kormányzati és magánszektorbeli döntéshozóknak. Think tank-ek lehetnek függetlenek vagy kapcsolódhatnak egyetemekhez, kormányzati szervekhez, politikai csoportokhoz vagy magánvállalatokhoz, és tevékenységük az objektív kutatástól az érdekérvényesítésig terjedhet. Szerte a világon számos think tank működik, amelyek a helyi, nemzeti és nemzetközi politikai és társadalmi kérdésekre koncentrálnak.

Joseph Robbins kutatása alapján kijelenthető, hogy az észt válaszokat a digitális térben megnyilvánuló tudatosság és fejlődés iránt megmutatkozó igény, valamint az országban élő orosz kisebbség jelenléte határozza meg leginkább, vagyis ezeket a tényezőket tartják a legfontosabbaknak. Az Észt Védelmi Liga (EDL) fontos szerepet játszik az ország ellenintézkedéseiben, beleértve az propaganda ellenes blogot, a Propastop.org-ot, amely a káros narratívák elleni küzdelemre, a hamis hírek kiszűrésére, a dezinformáció elleni küzdelemre összpontosít.

A NATO és az EU többoldalú válaszlépései is jelentősnek tekinthetőek az orosz dezinformációs erőfeszítések elleni küzdelemben. Az EU Rapid Alert Systemje, amely tagállamok közötti információ- és „legjobb gyakorlatok" megosztására szolgál, és a NATO Stratégiai Kommunikációs Központja (STRATCOM), amely tájékoztatást nyújt az információs műveletekről, mind kulcsfontosságúak a dezinformáció elleni folyamatos harcban.

Az Észtország által alkalmazott valós idejű önkéntes erők, valamint a Cseh Köztársaság Terrorizmus és Hibrid Fenyegetések Elleni Központja Cseh Biztonsági Információs Szolgálata, valamint a speciális szakismeretekkel rendelkező think tank-ek hasznosak az orosz aktív műveletek leleplezésében és hatástalanításában.

Szükségesnek tartom megjegyezni, hogy a Terrorizmus és Hibrid Fenyegetések Elleni Központ (Center Against Terrorism and Hybrid Threats, CTHT) egy olyan szervezet, amelyet a Cseh Köztársaságban hoztak létre a terrorizmus, hibrid hadviselési módszerek és más

összetett fenyegetések elleni küzdelem céljából. A CTHT fő feladata a különböző fenyegetések elemzése, politikai javaslatok kidolgozása, valamint együttműködés más kormányzati szervekkel és külső szervezetekkel a kapott információk terjesztése és az ellenintézkedések koordinálása érdekében. A CTHT munkáját a Cseh Biztonsági Információs Szolgálat (Bezpečnostní informační služba, BIS) segíti. A BIS a cseh kormány hírszerzési és biztonsági szolgálata, amelynek feladata a nemzetbiztonsági fenyegetések felismerése, monitorozása és kezelése. Ez magában foglalja a kémtevékenységek, terrorizmus, szélsőséges csoportok tevékenységeinek és más, a nemzetbiztonságot veszélyeztető tevékenységek elleni fellépést. A BIS információkat szolgáltat a cseh kormánynak és segít a nemzetbiztonsági kockázatok kezelésében, így közvetlenül támogatja a CTHT-t is a terrorizmus és hibrid fenyegetések elleni küzdelemben.

Az EU és a NATO ezirányú iránymutatásai, céltudatos és következetes védelmi tevékenysége Oroszország folyamatos zavarkeltő erőfeszítésivel szemben hasznos javaslatokat és követendő példát, valamint szakmai fejlődési lehetőséget kínál a tagállamai számára. Ezek az intézkedések segíthetnek leleplezni a romboló erőfeszítéseket, koordinált választ adni rájuk és elősegíteni a többoldalú együttműködést.

Számos példát találunk természetesen más országok dezinformációs műveleteinek nyomaira utaló jelekre is. Gondolhatunk Sophia Khatsenkova „Turkey's disinformation election: Fake videos and wildly misleading claims” című zsurnalisztikájában[445] megjelenített észrevételekre is, mely a 2023-as török elnökválasztással, egészen pontosan annak első fordulójával összefüggő anomáliákat, az ő szóhasználatával éve az alkalmazott dezinformációs technikákat vizsgálja. A cikk szerint az ország május végén második fordulóra készül, mivel sem Recep Tayyip Erdoğan elnök, sem fő ellenfele, Kemal Kılıçdaroğlu nem tudta megszerezni a szükséges többséget az első fordulóban. A kampány során mindkét oldalról számos álhírt terjesztettek az ellenfél lejáratására.

Sophia Khatsenkova ismeretei szerint az egyik legelterjedtebb állítás az volt, hogy Kılıçdaroğlu támogatást kapott a PKK nevű, Törökországban, az EU-ban és az USA-ban terrorista szervezetként besorolt csoporttól. Egy videóban állítólag Kılıçdaroğlu és a PKK egyik

[445] Elérhető: https://www.euronews.com/2023/05/16/turkeys-disinformation-election-fake-videos-and-wildly-misleading-claims (letöltés:2023.11.23.)

alapítója, Murat Karayilan együtt látható, azonban több tényellenőrző oldal szerint ez a videó hamisítvány, két külön felvétel összevágásával készült. Másik közlemény[446] szerint Erdoğan pénzt osztott ki gyerekeknek egy szavazóhelyiségben. Ezt egy Twitteren (X-en) közzétett videó alapján terjesztették, de a Liberation tényellenőrző oldal szerint ez „mindössze" egy kulturális szokás, amely szerint az idősebbek főként vallási ünnepeken „zsebpénzt" adnak a gyerekeknek. Erdoğan párti csoportok azt állították, hogy 1,7 millió fő támogató gyűlt össze egy isztanbuli rendezvényen, de ezt több tényellenőrző oldal cáfolta, ugyanis a helyszín legfeljebb 690 000 embert tud befogadni. [447] Kılıçdaroğlu „külföldi, elsősorban orosz hackerekre" utalt a kampány során, mint akik dezinformációt terjesztenek, míg Erdoğan azt állította, hogy az ellenzék „trollok hadseregét" alkalmazza vele szemben.

A politikai-, illetve médiaszakértők nem tudnak megalapozottan állást foglalni abban a tekintetben, hogy ezek a dezinformációs műveletek érdemben befolyásolták-e a választás eredményét, de azt elismerik, hogy hatással voltak a török társadalomra, pontosabban a közvélekedésre az egyes jelöltekkel kapcsolatban. Sophia Khatsenkova megjegyzi, hogy Suay Boulougouris, az Article 19 nevű NGO programigazgatója szerint az ellenzéki koalíciót több dezinformációs támadás érte, mint a kormánykoalíciót, véleménye szerint abból a célból, hogy megnyerje a bizonytalan és (párt)preferenciával nem rendelkező, valamint a befolyásolható (ellenzéki) szavazókat.

Az általam kiválogatott, 1. számú mellékletben ismertetett Kremlbarát dezinformációkkal összefüggésben szükséges kiemelni, hogy különböző nyelveken, különböző országokban kerültek közvetítésre az orosz propagandagépezet által és amennyiben átlagos közösségi média fogyasztóként, rendszeresen olvasunk híreket az online sajtótermékek igénybevételével, több is ismerősként köszönthet minket. Ez azt bizonyítja, hogy a dezinformáció előbb-vagy utóbb, akár egy összeesküvéseket kedvelő szomszéd vagy rokon, ismerős által, de el fog jutni mindannyiunkhoz, hatásai ellen tökéletes védelem nincs, hiszen a cáfolat gyakran még inkább felhívja a figyelmet az alaphírre, ráadásul az már nem is fog akkora nyomot hagyni a hírfogyasztóban, mint az eredeti, „kifejezetten érdekes, szaftos" dezinformáció.

[446] Az eseményről számos hírportál beszámolt, a HVG híradása az alábbi linken érhető el: https://hvg.hu/vilag/20230529_Erdogan_szavazohely_elott_osztogatott_keszpenzt__video (letöltés: 2023.11.20.)
[447] Elérhető: https://www.euronews.com/2023/05/16/turkeys-disinformation-election-fake-videos-and-wildly-misleading-claims (letöltés:2023.11.23.)

1.1. A nyugaton a domináns liberális ideológiától eltérők üldözésnek vannak kitéve

A DEZINFORMÁCIÓS ESET RÉSZLETEI
Dezinformáció közvetítésére használt médium: Geopolitica.ru – Italian*[448]
Közzététel dátuma: 2020. március 29.
Médium nyelve(i): Olasz
Érintett országok / régiók: Egyesült Államok

AZ OROSZ DEZINFORMÁCIÓ:

A Szovjetunió felbomlása és az amerikai thalasszokratikus[449] birodalom terjeszkedése után a globalizáció és a hatalmi elit általi domináns liberális ideológia bevezetése következett be, melyet a politikai korrektség inkvizíciós törvénykezése erőszakosan hajt végre, és mindenkit rövidített tárgyaláson ítél el, aki eltér ettől a gondolkodásmódtól.

1.2. Az új kínai koronavírust valószínűleg a NATO biológiai laboratóriumaiban hozták létre

A DEZINFORMÁCIÓS ESET RÉSZLETEI
Dezinformáció közvetítésére használt médium: sputnik.by(opens in a new tab) (archived(opens in a new tab))*[450]
Közzététel dátuma: 2020. január 22.
Dezinformáció közvetítésére használt médium nyelve(i): Orosz
Érintett országok / régiók: Kína, Egyesült Államok

AZ OROSZ DEZINFORMÁCIÓ:

Az új koronavírus egybeesik a világ számos jelentős eseményével, beleértve a Svájcban megrendezett Világgazdasági Fórum Davosi Fórumát. Ez nem lehet véletlen, ahogy az H1N1

[448] Elérhető: https://www.geopolitica.ru/it/article/coronavirus-il-naufragio-del-modello-liberale-e-la-quarta-teoria-politica (letöltés: 2023. 11. 20.)

[449] A „thalasszokratikus" a görög „thalassa" (tenger) és „kratosz" (uralom) szavak összetételéből származik, és olyan államra utal, amely tengeri hatalommal rendelkezik, azaz jelentős hadiflottával bír.

[450] Elérhető: https://sputnik.by/20200122/Ne-veryu-chto-eto-sluchayno-ekspert-o-proiskhozhdenii-koronavirusa-1043758449.html (letöltés: 2023.11.20.)

vírus esetében sem volt. Mindez üzlet, melynek célja egy adott politikai és gazdasági helyzet kialakítása. Körülöttünk sok amerikai és NATO biológiai laboratórium található Kína körül. Emberek nyálát és a specifikus etnikai származáshoz kötődő emberi genomot tanulmányozzák. A japán média azt írja, hogy az új vírus csak a kínaiakat fertőzi meg. A globális harcok nem etikaiak, minden eszköz megengedett. Az 1950-1960-as években Kína olyan plakátokat tett közzé, amelyeken az állt: „Mindenki harcoljon az amerikai baktériumellenes agresszió ellen!", és most ez visszatér. Hamarosan az új koronavírus elleni küzdelmet felhasználva a globális gazdaságra hatással bíró szabályokat fognak alkotni... Azt fogják mondani, hogy az európai szakemberek jelenléte a kínai ipari vállalatokban szükséges ahhoz, hogy a kínai termékeket az Egyesült Államokba és Európába exportálják.

1.3. A Covid-19 járvány lehetőséget biztosít a népesség ellenőrzésére Bill Gatesnek, a nagy technológiai vállalatoknak és a gyógyszeriparnak

A DEZINFORMÁCIÓS ESET RÉSZLETEI
Dezinformáció közvetítésére használt médium: actualidad.rt.com*[451]
Közzététel dátuma: 2021. március 22.
Cikk nyelve(i): spanyol
Érintett országok / régiók: Egyesült Államok, Európai Unió

AZ OROSZ DEZINFORMÁCIÓ:

A Covid-19 további népességellenőrzést hagy maga után. Semmi sem véletlen a geopolitikában, és a koronavírus egy ász a pakliban olyan célok eléréséhez, mint a kontroll, a dominancia és a kormányzás globális szinten. Létezik egyfajta harc a dominanciaért, amelyben sok nagy technológiai és gyógyszeripari vállalat vesz részt. Ezek a szektorok valójában profitálnak ebből a helyzetből, miközben az emberek nem haboznak megtenni, amit az egészségük nevében mondanak nekik.

A társadalmi felügyelet erősebb lesz. Ki lehet mögötte, ki finanszírozza mindezt? Jól ismert, hogy Bill Gates előszeretettel fektet be mindezekbe, vagyis különböző technológiai részvényeket vásárol a portfóliójába. Ez a közvetett folyamat teljesen megváltoztatta a

[451] Elérhető: https://app.cappture.cc/snapshots/1eb8ae41-a560-6dbc-857b-0aa4824acb4e (letöltés: 2023.11.20.)

társadalmunkat, és míg az egészségünk megőrzésének ígéretét hangsúlyozva beszélnek nekünk a szabadságról, sosem lesz majd újra normális az életünk, mivel a Bill Gates-hez hasonlók által folyamatosan ellenőrizve leszünk. Ami marad, az egy mentálisan károsított társadalom, amely nem lesz képes lelkileg ellenállni a külső hatásoknak. Egy új valóság, amelyet ránk szabadítanak. Előttünk állnak azok az évek, amikor mindennel megpróbálnak minket kontrollálni, mindent az egészségünk, jól-létünk előrehozásával indokolva: útlevelek, karkötők, minden szükséges. Évek, amikor egy Új Világrendet kovácsolnak, és ez nem egy összeesküvés-elmélet, hanem valóság, és napról napra élsz át ezt.

1.4. A koronavírus kizárólag egy rasszra irányul

A DEZINFORMÁCIÓS ESET RÉSZLETI
Dezinformáció közvetítésére használt médium: kp.ru*[452]
Közzététel dátuma: 2020. január 28.
Kiadvány nyelve(i): orosz
Érintett országok / régiók: Kína, Egyesült Államok

AZ OROSZ DEZINFORMÁCIÓ:

A koronavírus egy genetikai jellemzőket figyelembe vevő tömegpusztító fegyver, kifejezetten a kisebbségben lévő mongoloidok kiirtására tervezve, ami etnikai tisztogatásra lehet alkalmas Kínában. A Kínában zajló események előnyösek a jelenlegi amerikai kormánynak, amely összejátszik Pekinggel. Gyanús, hogy a pandémia kezdetének időpontja egybeesik Kína és az Egyesült Államok közötti kereskedelmi megállapodásról szóló tárgyalások befejező részével.

1.5.Az oltás a globalisták tervének része, egy biokémiai támadás az emberiség ellen

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: livenews.am *[453]
Közzététel dátuma: 2021. szeptember 16.

[452] Elérhető: https://www.kp.ru/daily/27084/4156051/ (letöltés: 2023.11.20.)
[453] Elérhető: https://livenews.am/press/2021/132123/16/18/51/ (letöltés: 2023.11.20.)

Cikk nyelve(i): Örmény
Érintett országok / régiók: Kína, Egyesült Államok

AZ OROSZ DEZINFORMÁCIÓ:

Az oltás valójában egy tömegpusztító fegyver. Ez a globalisták tervének része, egy biokémiai támadás az emberiség ellen. A világkormány létrehozása, az államok lebontása. A globalisták célja a népesség csökkentése, egy genocídium-program, amelynek célja 3 milliárd ember eltávolítása, évekkel ezelőtt jóváhagyva az Egyesült Államok Külügyminisztériuma és az Egyesült Államok elnöke, Carter által. A globalisták mesterséges vírusokat terjesztenek és digitális teret teljes egészében uralni akarják. Az oltóanyagok olyan anyagokat tartalmaznak, amelyek rendkívül veszélyesek az emberi egészségre. A kötelező oltás pedig egyenlő terrorizmussal.

1.6.Az Egyesült Államok NATO központot hoz létre Kazahsztánban kifejezetten Oroszország provokálására

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: KZ 24 News [454]
Közzététel dátuma: 2023. október 28.
Cikk nyelve(i): orosz
Érintett országok / régiók: Egyesült Államok, Oroszország, Kazahsztán

AZ OROSZ DEZINFORMÁCIÓ:

A „NATO Központ” megnyitása Kazahsztánban, jelentős figyelmet kapott a kazah és a nemzetközi médiában. Az amerikaiak által támogatott konferenciaterem megnyitása csak az első lépés lehet egy központ felé, ahol a kazah katonai személyzetet a NATO szabványai szerint képzik majd. Világos, hogy az Egyesült Államok szándéka, hogy bármilyen módon részt vegyen Kazahsztán katonai programjaiban.

[454] https://kz24.news/news/politika/otkrytie-shtaba-nato-v-kazahstane-mnogovektornost-ili-provokatsiya.html (archivált verzió (új fülön nyílik meg) letöltés: 2023. október 28.)

Az Egyesült Államok további katonai jelenléte Oroszország közelében nyilvánvaló provokáció, továbbá kijelenthető, hogy nem lesz jó hatással Kazahsztán kapcsolataira a CSTO[455] tagállamaival, különösen Oroszországgal.

1.7. Oroszország csak azért nyomul lassan előre Ukrajnában, hogy megóvja katonái életét

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: podcastaddict.com [456]
Közzététel dátuma: 2023. október 17.
Cikk nyelve(i): angol, francia
Érintett országok / régiók: Oroszország, Ukrajna, EU, Európa

AZ OROSZ DEZINFORMÁCIÓ:

A Nyugat által várva várt és jelentősen támogatott ukrán ellentámadás kudarcot vallott, és Oroszország terve egy „felperzselt föld" taktikára[457] épülő háború folytatása a továbbiakban. Az orosz hadsereg kiemelt célja, hogy megőrizze katonái életét. Ez a történelem során mindig is így volt, a napóleoni háborúktól kezdve az I. és II. világháborúig. A betolakodókat lemészárolják, amikor azok elhagyják az orosz földet. Ma az új orosz oblasztokban[458] Oroszország attríciós háborút folytat, és megóvja saját katonái és azoknak az ukrán katonáknak életét, akik készek megadni magukat.

1.8. Ételükbe csempészett harci drogoktól zombiként harcolnak az ukrán katonák

[455] A "CSTO" rövidítés a Kollektív Biztonsági Szerződés Szervezetére (Collective Security Treaty Organization) utal, amely egy nemzetközi katonai szövetség, ami több posztszovjet államot foglal magába. A szervezetet 1992-ben hozták létre, és olyan országok tagjai, mint Oroszország, Örményország, Fehéroroszország, Kazahsztán, Kirgizisztán és Tádzsikisztán. A CSTO célja a tagállamok közötti kollektív védelem biztosítása, valamint a regionális és nemzetközi biztonság erősítése.

[456] Elérhető: https://podcastaddict.com/afrique-en-marche/episode/165183338 (letöltés: 2023.11.02.)

[457] Az eredeti cikkben az "attríciós háború" kifejezés jellemzően arra utal, hogy az egyik vagy mindkét fél próbálja kimeríteni az ellenfél erőforrásait, legyen az emberi, katonai vagy gazdasági kapacitás. A háborús helyzetekben gyakran előfordul, hogy a harcoló felek kísérletet tesznek az ellenséges erők kimerítésére, miközben igyekeznek minimalizálni a saját veszteségeiket. Ezzel együtt fontos megjegyezni, hogy a konfliktusokban az ilyen jellegű állítások gyakran vitatottak és az értelmezésük függ a forrásoktól, az érintett felek politikai és propagandacéljaitól.

[458] Az "oblaszt" kifejezés orosz eredetű szó, amely egy közigazgatási egységet jelöl Oroszországban. Az orosz föderációban az oblasztok régiók vagy tartományok, amelyek meghatározott területi és közigazgatási egységeket képviselnek. Ezek az egységek többnyire saját kormányzattal és közigazgatási struktúrával rendelkeznek, bár bizonyos fokú központi irányítás alatt állnak.

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: yapolitic.ru [459]
Közzététel dátuma: 2023. október 4.
Cikk nyelve(i): orosz
Érintett országok / régiók: Ukrajna, Oroszország, Egyesült Államok, Európa

AZ OROSZ DEZINFORMÁCIÓ:

Az ukránok nem akarnak az oroszok ellen harcolni. Viszont, amikor olyan orosz katonai egységek ellen harcolnak, akik jobban felszereltek, mint ők, zombiszerűen, robotokként küzdenek. Nem félnek meghalni, mert olyan „nyugati ételkészítményeket" kapnak, amelyekben speciális harci drogok vannak.

1.9.A NATO háborút akar indítani Oroszországgal szemben Karabahban, Transznisztriában és a Donyeck-medencében

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: newsua.ru [460]
Közzététel dátuma: 2023. szeptember 29.
Cikk nyelve(i): orosz
Érintett országok / régiók: Oroszország, EU, Örményország, Azerbajdzsán, Ukrajna

AZ OROSZ DEZINFORMÁCIÓ:

A háború a Hegyi-Karabahban csak az első jel volt. Ha Oroszország nem figyel oda, akkor a NATO következő csapása Transznisztriában és a Donyeck-medencében lesz. Ha Transznisztriában elkezdi a NATO az offenzívát, Románia támogatná Moldovát, majd a NATO a Donyeck-medencére mérne csapást. Ukrajna offenzíváját pedig Lengyelország felől támogatná.

[459]Elérhető: https://yapolitic.ru/51940-vecher-s-vladimirom-solovevym-041023 (letöltés: 2023.11.02.)
[460]Elérhető: https://newsua.ru/news/32690-esli-zachistyat-karabakh-sleduyushchimi-budut-donbass-i-pridnestrove (letöltés:2023. 10. 30.)

1.10. Oroszország megsemmisített egy Leopard tankot, amiben német harckocsizók voltak

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: sputnikglobe.com [461]
Közzététel dátuma: 2023. szeptember 25.
Cikk nyelve(i): spanyol
Érintett országok / régiók: Ukrajna, Németország

AZ OROSZ DEZINFORMÁCIÓ:

Egy orosz felderítőcsoport megsemmisített egy német Leopard tankot, amelyet a német Bunderswehr katonái vezettek az ukrán erők támogatása során Zaporozhye felé. A legénység vezető-mechanikusa súlyos sérüléseket szenvedett, a többiek pedig meghaltak. A szerelő többször is kijelentette, hogy nem zsoldos, hanem a Bunderswehr szolgálatában álló katona, és hogy ő és a legénység többi tagja ugyanabba a Bunderswehr egységbe tartoznak. A harckocsi vezetője a sebeiben halt meg percekkel azután, hogy megtalálták, annak ellenére, hogy az orosz katonák megpróbálták megmenteni.

1.11. Kijev nem törődik állampolgáraival, amikor katonáit bedobja a húsdarálóba

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: nabd.com [462]
Közzététel dátuma: 2023. szeptember 18.
Cikk nyelve(i): arab
Érintett országok / régiók: Ukrajna, EU

AZ OROSZ DEZINFORMÁCIÓ[463]:

[461] Elérhető: https://sputnikglobe.com/20230923/russian-reconnaissance-team-destroys-leopard-tank-in-special-op-zone-with-fully-german-crew-1113608814.html (letöltés: 2023.09.25.)
[462] Elérhető: https://app.cappture.cc/snapshots/1ee5bca3-dd31-6622-9467-06a13b0e4978 (letöltve: 2023.09.23.)
[463] Fontosnak tartom megjegyezni, hogy az eredeti (orosz nyelvű) cikkben a „Komszomolszkaja Pravda"-ban Andrej Baranov arról írt, hogy a NATO stratégái már meggyőződtek arról, hogy szükséges visszafogniuk az Ukrajnának nyújtott támogatás volumenét. Ennek a cikknek a tartalma jelent meg az arab médium honlapján, az eredeti cikk hivatkozásával.

Másfél évvel az orosz különleges katonai művelet után a NATO közel száz milliárd dollárt pumpált Ukrajnába, rendszeresen ellátva Kijevet lőszerekkel, gránátokkal, rakétákkal, fegyverekkel és mindenféle páncélozott járművel, beleértve a nehéz harckocsikat is. A harci repülőgépek átadása következhet a sorban. Azonban a kijevi rendszer, amely nem számolja a katonai veszteségek számát, sem állampolgárai életét nem becsüli, akiket a „húsdarálóba" dobott, elkényeztetett gyermekként egyre több és több segítséget követel a nyugati jótékonykodóktól.

Brüsszel örülne, ha folytathatná az ukrán hadsereg fegyverekkel való ellátását, de kapacitásai végéhez ért. A NATO kimerítette erejét, miután szinte az egész arzenálját feláldozta Ukrajna végtelen étvágyának kielégítésére. A NATO vezérkari főnökök éves konferenciáján Norvégiában elismerték...Oroszország különleges katonai műveleteinek másfél évében a NATO közel százmilliárd dollárt pumpált Ukrajnába, rendszeresen ellátva Kijevet lőszerrel, rakétákkal, fegyverekkel és mindenféle páncélozott járművel, beleértve a nehéz tankokat is. A vadászgépek következnek. De a Kijevi rezsim, amely nem számolja a civil és katonai veszteségeket, akiket gondolkodás nélkül húsdarálóba küld, majd, mint egy elkényeztetett gyermek, egyre több segítséget követel nyugati jótevőitől.

1.12. Sanna Marin otthagyja a politikát, miután Finnországot a NATO gyarmatává tette

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Outlet: lantidiplomatico.it [464]
Közzététel dátuma: 2023. szeptember 09.
Cikk nyelve(i): olasz
Érintett országok / régiók: Finnország

AZ OROSZ DEZINFORMÁCIÓ:

A volt finn miniszterelnök, Sanna Marin, otthagyja a politikát, miután befejezte a neki szánt küldetést miszerint, a hazáját a NATO tagjává, azaz a Birodalom gyarmatává tegye. A jutalma egy tanácsadói pozíció lesz számára a Blair Alapítványnál.

[464] https://www.lantidiplomatico.it/dettnews-sanna_marin_e_la_fondazione_blair/45289_50780/

1.13. A NATO hibrid háborút folytat Ukrajnában Oroszország ellen az utolsó ukránig

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Kiadvány: pl.sputniknews.com [465]
Közzététel dátuma: 2023. szeptember 08.
Cikk nyelve(i): lengyel
Érintett országok / régiók: Ukrajna, Egyesült Államok, Oroszország

AZ OROSZ DEZINFORMÁCIÓ:

A legtöbb ukrán pontosan tudja, hogy a valódi fenyegetés nem az orosz intézkedésekből, hanem a Zelenszkij rezsim bűnöző politikájából származik. Ukrajnában széles körben mobilizáció zajlik Zelenszkijjel szemben [...]. A NATO Ukrajnában hibrid háborút folytat Oroszország ellen az utolsó ukránig, és az ukránok [...], nem akarnak bekerülni a „húsdarálóba".

1.14. Moldova már lényegében a NATO irányítása alatt áll

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Kiadó: md.tsargrad.tv [466]
Közzététel dátuma: 2023. augusztus 29.
Cikk nyelve(i): orosz
Érintett országok / régiók: Moldova

AZ OROSZ DEZINFORMÁCIÓ:

Védelempolitikai szempontból Moldova a NATO irányítása alatt áll. Ezt nem is titkolják, 2006 óta Moldova stratégiai partnerségi tervvel rendelkezik a NATO-val, és már három NATO központot nyitottak Moldovában. Ez a helyi orosz kisebbség helyzetét hátrányosan befolyásolja.

[465] https://app.cappture.cc/snapshots/1ee507bf-5890-65b0-a052-06a13b0e4978

[466] Elérhető: https://md.tsargrad.tv/articles/o-momente-istiny-potere-moldaviej-suvereniteta-i-juridicheskom-prave-pmr-na-nezavisimost_855545 (letöltés: 2023.08.24.)

1.15. Ukrajna nyugdíjasokat képez harckocsizókká, mert kimerült a humánerőforrás tartaléka

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: Sputnik Azerbaijan - Orosz (archivált) sputnik.by[467]
Közzététel dátuma: 2023. augusztus 28.
Cikk nyelve(i): Orosz
Tárgyalt országok / régiók: Ukrajna, Oroszország, Egyesült Államok, Németország

AZ OROSZ DEZINFORMÁCIÓ:

Ukrajna kimerült a hatalmas vérveszteségek miatt. Az, hogy az ukrán harckocsizók részére Németországban tartott képzéseken 70 év felettiek is részt vesznek, sokat elárul. Ukrajna mintegy 30 000 katonát vesztett el a Rabotyne település megtámadásakor, és ennek ellenére sem sikerült bevennie.

1.16. Spanyolország a Spanyol Nemzeti Stratégiában a tömegpusztító fegyvereknek az ukrán korrupció miatt proliferációja miatti aggodalmát fejezte ki

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: sputniknews.lat [468]
Közzététel dátuma: 2023. február 20.
Cikk nyelve(i): Spanyol
Tárgyalt országok / régiók: Spanyolország, Ukrajna

AZ OROSZ DEZINFORMÁCIÓ:

Február 15-én Spanyolország jóváhagyta az első Tömegpusztító Fegyverek Proliferációja Elleni Nemzeti Stratégiáját. Ez biztosan összefügg azzal a növekvő bizonytalansággal, ami sok fegyver és technológia sorsát illeti, amit Volodymyr Zelenskyy rezsimjének küldtek. Mindenki tudja, mennyire korrupt az ukrán hadsereg, és hónapok óta észlelték a nyugati fegyverek

[467] Elérhető: https://az.sputniknews.ru/20230829/svo-kontrnastuplenie-vsu-perenositsya-na-2024-god--458129406.html ((új fülön nyílik meg) (archivált) letöltés: 2023.08.24.)

[468] Elérhető: https://sputniknews.lat/20230217/por-que-espana-crea-la-iniciativa-de-la-no-proliferacion-de-armas-de-destruccion-masiva-1135891942.html (Letöltés: 2023. 02. 23.)

illegális forgalmát az országban. A NATO országok súlyos felelőtlensége, hogy olyan fegyvereket és technológiákat küldenek, amelyekkel vegyi vagy biológiai fegyverek is célba juttat hadianyagok terjesztésére lehetne használni. A kockázatok valósak, és az hadseregeknek fel kell készülniük arra, hogyan nézzenek szembe ezekkel a veszélyekkel.

1.17. Washington arra kényszeríti a szuverén nemzeteket, hogy egységesen, az amerikai érdekek mentén lépjenek fel Oroszország és Kína ellen

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: oroszhirek.hu[469]
Közzététel dátuma: 2023. május 2.
Cikk nyelve(i): Magyar
Tárgyalt országok / régiók: Egyesült Államok, Oroszország, Kína

AZ OROSZ DEZINFORMÁCIÓ:

Washington különféle (politikai) kényszerítő eszközökhöz folyamodik, miközben regionális szövetségeket próbál kialakítani geopolitikai riválisaival, köztük Moszkvával és Pekinggel szemben. Komoly nyomást gyakorol független nemzetekre közvetlen zsarolással, fenyegetésekkel, színes forradalmakkal, puccsokkal és nyílt dezinformáció terjesztésével. Mindezek az eszközök régóta a Nyugat aduászaiként funkcionálnak.

1.18. A kijevi neofasiszta rezsimet meg kell buktatni bármi áron

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: oroszhirek.hu (archivált)[470]
Közzététel dátuma: 2023. május 2.

[469] Elérhető: https://oroszhirek.hu/sojgu-az-usa-zsarolja-az-orszagokat-hogy-harcoljanak-moszkva-es-peking-ellen/(Letöltés: 2023. 05. 22.)

[470] Elérhető: https://oroszhirek.hu/medvegyev-meg-kell-futamitani-a-teljes-kabitoszeres-kijevi-rezsimet/ (Letöltés: 2023. 05. 22.)

Cikk nyelve(i): Magyar
Tárgyalt országok / régiók: Ukrajna, Oroszország

AZ OROSZ DEZINFORMÁCIÓ:

A kijevi rezsim tevékenysége arra irányul, hogy megszilárdítsa a náci elit hatalmát, erősítse a katonai egységek fasisztoid szellemét, és minél több támogatást szerezzen külföldi támogatóitól. Az egyetlen elfogadható megoldás a neofasiszta rezsim végleges megdöntése a katonai erejének semlegesítése, az összes ukrán terület teljes demilitarizálása, a neofasiszta rezsim kulcsfontosságú vezetőinek felelősségre vonása.

1.19. Zelenszkij a német náci rezsim örököse

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: oroszhirek.hu (új fülön nyílik meg) (archivált)[471]
Közzététel dátuma: 2023. április 24.
Cikk nyelve(i): Magyar
Tárgyalt országok / régiók: Ukrajna, Oroszország, Németország

AZ OROSZ DEZINFORMÁCIÓ:

A Die Welt német újságírói arra szólítják fel az ukrán náci vezért, hogy ne ismételje meg a német Führer hibáit a sztálingrádi csatában. Őszinte emberek: végre rájöttek, hogy ez az színész egy valódi, bizonyítottan fasiszta, a német nemzeti szocialisták igazi örököse. Az ő rezsimének veresége ugyanolyan lesz, mint a német náciké Sztálingrádban.

1.20. Németország az USA vazallusa

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: oroszhirek.hu (archivált)[472]
Közzététel dátuma: 2023. április 4.

[471]Elérhető: https://oroszhirek.hu/medvegyev-a-fasiszta-rezsimhez-hasonlitja-a-kijevi-kormanyt-es-hitlerkent-abrazolja-zelenszkijt/ (Letöltés: 2023. 05. 22.)

[472]Elérhető: https://oroszhirek.hu/nemet-kepviselo-az-amerikai-eroket-az-atomfegyverekkel-egyutt-ki-kell-vonni-nemetorszagbol/ (Letöltés: 2023. 05. 22.)

Cikk nyelve(i): Magyar
Tárgyalt országok / régiók: Németország, Egyesült Államok, Oroszország, Ukrajna

AZ OROSZ DEZINFORMÁCIÓ:

Az Egyesült Államok kormánya nem szövetségeseket akar, csak hűséges vazallusokat. Washington az amerikai hadsereg németországi bázisait használja arra, hogy külföldön vívjon háborúkat és indítson halálos dróntámadásokat. Berlin engedélyezte az Egyesült Államoknak, hogy német gyártású Leopard harckocsikat szállítsanak Ukrajnának.

1.21. Az EU békefenntartókat akar Ukrajnába küldeni

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: oroszhirek.hu (archivált)[473]
Közzététel dátuma: 2023. április 4.
Cikk nyelve(i): Magyar
Tárgyalt országok / régiók: Németország, Egyesült Államok, Oroszország, Ukrajna

AZ OROSZ DEZINFORMÁCIÓ:

Ahelyett, hogy diplomáciai eszközöket használna a béke megteremtése érdekében Ukrajnában, az Európai Unió egyre több fegyvert biztosít Kijevnek, és ezzel eléri, hogy még véresebb és brutálisabb legyen a küzdelem. Az EU nemcsak fegyvereket küldene, hanem békefenntartó csapatokat is Ukrajnába.

1.22. Az Egyesült Államok megpróbálta megfenyegetni Putyint a Északi Áramlat szabotálásával

A DEZINFORMÁCIÓS ESET RÉSZLETEI:
Dezinformáció közvetítésére használt médium: oroszhirek.hu (archivált)[474]

[473]Elérhető: https://oroszhirek.hu/a-kreml-reagalt-orban-viktor-nyilatkozatara-amely-szerint-az-eu-bekefenntarto-csapatokat-kuldene-ukrajnaba/ (Letöltés: 2023. 05. 22.)

[474] Elérhető: https://oroszhirek.hu/hersh-az-usa-az-eszaki-aramlat-szabotazsaval-akarta-megfenyegetni-putyint/(Letöltés: 2023. 05. 22.)

Közzététel dátuma: 2023. április 11.
Cikk nyelve(i): Magyar
Tárgyalt országok / régiók: Oroszország, Egyesült Államok, Németország, Ukrajna

AZ OROSZ DEZINFORMÁCIÓ:

Az Egyesült Államok megfenyegette Oroszországot azzal – Ukrajna elleni támadásának megakadályozása érdekében – hogy felrobbantja az Északi Áramlat csővezetékeit. A lehetséges támadás terveit már 2021 végén elkezdték kidolgozni. A 2023. márciusában az ENSZ Biztonsági Tanácsa elutasította Oroszország javaslatát egy nemzetközi bizottság létrehozására a szabotázs vizsgálatára. Ez azt mutatja, hogy a nyugati országok, különösen az Egyesült Államok, nem érdekeltek objektív nemzetközi vizsgálat végrehajtásában. Ehelyett érdekükben áll elfedni a nyomokat és félrevezetni a helyi, vizsgálatot végző szakembereket.

2. számú melléklet: A kibervédelemért felelős, szolgálatokat irányító miniszteri jogkörben eljáró államtitkárok feladatrendszere

A katonai nemzetbiztonság irányításáért felelős államtitkár a honvédelmi miniszternek a katonai nemzetbiztonsági szolgálat irányításáért való felelősségi körébe tartozó feladatai keretében, a miniszter által átruházott jogkörben irányítja a Katonai Nemzetbiztonsági Szolgálatot:[475]

- *„Gyakorolja a Ksztv. 2. § (1) bekezdés c)–i) pontjában meghatározott jogosítványokat.*
- *Feladatot határoz meg, utasítást ad a KNBSZ főigazgatójának.*
- *Ellenőrzi a KNBSZ törvényes és rendeltetésszerű működését.*
- *Jóváhagyja a KNBSZ szervezeti és működési szabályzatát, állománytábláját.*
- *Jóváhagyja a KNBSZ főigazgatójának kül- és biztonságpolitikai szempontokat érintő, nemzetközi kapcsolatokra vonatkozó javaslatait.*
- *Jóváhagyja a titkos információgyűjtés belső eljárási és engedélyezési szabályait.*
- *Koordinálja a nemzetbiztonság katonai elemét érintő információk elemzését és értékelését, a Nbtv. 7. § (1) bekezdése szerinti tájékoztatás folyamatát, valamint az ezekkel összefüggő kormányzati döntés-előkészítést támogató munkát.*
- *Meghatározza a KNBSZ időszerű feladatait, és ezzel összefüggésben közreműködik a nemzetbiztonság katonai elemét és a honvédelmi érdeket érintő információigények azonosításában, begyűjtésében.*
- *Irányítja a KNBSZ főigazgatója által koordinált azon tevékenységeket, amelyek során a honvédelmi érdek érvényesítése a nemzetbiztonság katonai elemeinek fokozott érintettségével valósul meg.*
- *Utasítást ad a KNBSZ főigazgatójának az országos jelentőségű, valamint a Kormány, a Kormány nemzetbiztonsági döntéseit előkészítő szervezet, valamint annak munkáját segítő munkacsoport által meghatározott ügyekben a nemzetbiztonság katonai elemeit és a honvédelmi érdeket érintő elemző-értékelő és ágazati szintű koordinációs tevékenység lefolytatására.*
- *Válaszol a Kormány tagja által a miniszterhez intézett, a KNBSZ tevékenységével összefüggő információs igényre.*
- *Javaslatot tesz a KNBSZ költségvetésére.*

[475] a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2022. (VII. 29.) HM utasítás

- *A KNBSZ költségvetési gazdálkodása tekintetében – a gazdálkodási ügyekért felelős helyettes államtitkárral együttműködve – gyakorolja a jogszabályokban meghatározott tervezési, előirányzat-átcsoportosítási, beszámolási, információszolgáltatási, pénzügyi, valamint ellenőrzési kötelezettségeket és jogokat.*
- *Kezdeményezi a KNBSZ főigazgatójának és főigazgató-helyetteseinek nemzetbiztonsági ellenőrzését.*
- *A KNBSZ személyi állománya tekintetében a honvédek jogállásáról szóló törvény, vagy az annak végrehajtásáról szóló jogszabályok szerint a miniszter hatáskörébe tartozó esetekben javaslatot tesz a miniszter részére.*
- *Ellátja a KNBSZ miniszteri irányításából a miniszter rendelkezése alapján rá háruló további feladatokat."*

A katonai nemzetbiztonság irányításáért felelős államtitkár önálló hatáskörben[476]:

- *„A KNBSZ főigazgatójával együttműködve gondoskodik a minisztérium nemzetbiztonsági feladatokat érintő szakmai álláspontjának kialakításáról és képviseletéről.*
- *Véleményezi a KNBSZ működését, a feladat- és hatáskörüket érintő kormányzati döntések tervezeteit, valamint a KNBSZ-től érkező javaslatokat, fejlesztési koncepciókat.*
- *Meghatározza a KNBSZ-t érintő kormányzati döntés-előkészítéshez szükséges koordinációs feladatokat.*
- *Kezdeményezi vagy javasolja a feladat- és hatáskörét érintő jogszabály, közjogi szervezetszabályozó eszköz kiadását vagy módosítását.*
- *Javaslatot tesz a KNBSZ főigazgatójának normatív utasítások kiadására vagy módosítására.*
- *A KNBSZ parlamenti ellenőrzésével összefüggésben segíti a miniszternek az Országgyűlés, annak Nemzetbiztonsági Bizottsága irányában fennálló tájékoztatási, beszámolási, jelentéstételi és válaszadási kötelezettségeinek teljesítését.*
- *Előkészíti és a miniszter elé terjeszti az Országgyűlés által választott vagy a köztársasági elnök által kinevezett tisztségviselő vagy országgyűlési képviselő által a miniszterhez intézett, a katonai nemzetbiztonsági tevékenységet érintő megkeresésre adott miniszteri válasz tervezetét.*

[476] a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2022. (VII. 29.) HM utasítás

- *Kapcsolatot tart nemzetközi partnerszolgálati együttműködés elősegítése érdekében a partnerszolgálatok kormányzati irányításában részt vevő külföldi szervezetekkel és személyekkel.*
- *Javaslatot tesz a KNBSZ főigazgatójának és a főigazgató-helyetteseinek kinevezésére, kezdeményezi a tábornokok kinevezését, előléptetését.*
- *Engedélyezi a KNBSZ főigazgatójának külföldi kiutazásait és a vendégfogadásokat.*
- *Felterjeszti a KNBSZ által a miniszternek címzett megkereséseket."*

A katonai nemzetbiztonság irányításáért felelős államtitkár egyéb feladatai:[477]

- *„Szakterületén gondoskodik a feladatok meghatározásáról, számontartásáról, végrehajtásáról, programok, koncepciók kidolgozásáról, megvalósításáról, és meghatározza az ehhez szükséges feltételeket.*
- *Véleményt nyilvánít a véleményezésre érkezett feladat- és hatáskörét érintő előterjesztés, jogszabály, közjogi szervezetszabályozó eszköz tervezetéről.*
- *Biztosítja a feladat- és hatáskörét érintő miniszteri és kormányzati döntésekhez szükséges információk, háttéranyagok összeállítását, valamint a miniszteri döntésből eredő feladatok megvalósulását.*
- *Részt vesz a kiberbiztonság tárgykörében az Európai Unió kormányzati részvétellel működő intézményei döntéshozatalában képviselendő kormányzati álláspont kialakításában és képviseletében, illetve ellátja ennek ágazati koordinációját, valamint részt vesz az ezzel összefüggő kormányzati feladatok teljesítésében.*
- *Tájékoztatást kérhet és követelményeket határozhat meg a KNBSZ belső biztonsági és bűnmegelőzési, valamint objektumai műveleti védelmi tevékenységével összefüggésben, szervezi és koordinálja ezen tevékenységek szakszerűségének és jogszerűségének ellenőrzését.*
- *Folyamatosan vizsgálja a KNBSZ törvényben meghatározott alaptevékenységének közösen kihasználható együttműködési lehetőségeit, javaslatot tesz a hatékonyság fokozása érdekében.*
- *Kivizsgálja a KNBSZ tevékenységével és a KNBSZ hivatásos állományú tagja által foganatosított intézkedésekkel kapcsolatos, valamint a védelmi és biztonsági beszerzésekről szóló törvény szerinti panaszokat, a vizsgálat eredményéről és a megtett intézkedésekről tájékoztatja a panaszost.*
- *Együttműködik a Védelmi Tanács titkári feladatait ellátó állami vezetővel.*

[477] a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2022. (VII. 29.) HM utasítás

- *Irányítja a KNBSZ különleges jogrendre vonatkozó feladatainak előkészítését és végrehajtását.*
- *A miniszter döntése szerint részt vesz a Védelmi Tanács, a Nemzetbiztonsági Munkacsoport, valamint a hatáskörébe tartozó testületek és munkacsoportok ülésein, továbbá képviseli a honvédelmi tárcát a Nemzeti Kiberbiztonsági Koordinációs Tanács Testületében, ezekkel kapcsolatban a HM illetékes szervezeti egységeitől, valamint honvédelmi szervezettől felkészítőt kérhet.*
- *A katonai nemzetbiztonság irányításáért felelős államtitkár a miniszter által átruházott hatáskörben ellátja a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2022. (VII. 29.) HM utasítás 5. függelékében hatáskörébe utalt gazdasági társaságokkal kapcsolatos tulajdonosi joggyakorlói feladatokat, valamint dönt az azok támogatásával kapcsolatos ügyekben.*
- *A katonai nemzetbiztonság irányításáért felelős államtitkár a Hvt. 14. § (2) bekezdése szerint a miniszter átruházott hatáskörében irányítja az MH Kiberműveleti Parancsnokság vezetőjének a HM feladatrendszerével összefüggő tevékenységét.*
- *A katonai nemzetbiztonság irányításáért felelős államtitkár ellátja a jogszabály és közjogi szervezetszabályozó eszköz alapján hatáskörébe utalt engedélyezési, jóváhagyási és felügyeleti feladatokat.*
- *Meghatározza a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2022. (VII. 29.) HM utasítás 5. függelékében hatáskörébe utalt gazdasági társaságokkal kapcsolatos, a haderőfejlesztést és a védelmi ipari fejlesztési programot érintő, az egyedi megoldások és high-tech műszaki fejlesztések, technológiák kidolgozására vonatkozó stratégiai feladatokat.”*[478]

A katonai nemzetbiztonság irányításáért felelős államtitkár feladatrendszere a Honvédelmi Minisztérium szervezetében került elhelyezésre, tevékenységét kormánytisztviselőkből, honvédelmi alkalmazottakból és a KNBSZ hivatásos állományú munkatársaiból álló Titkárság segíti. Az államtitkárt – ha nem a minisztert helyettesítő, illetve annak átruházott jogkörében jár el – távolléte vagy akadályoztatása esetén a miniszter által kijelölt személy helyettesíti.

[478] a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2022. (VII. 29.) HM utasítás

A feladatokat tartalmazó HM utasításban[479] megjelenített előírások gyakorlati megvalósítása a publikáció írásakor már folyamatban van, azonban ennek eredményességét legkorábban kettő vagy három évvel később lehet érdemlegesen mérni.

A jogintézmény egy bevett gyakorlatot implementál a honvédelmi ágazati normakörnyezetbe, egy a polgári szolgálatok irányítását meghatározó megoldást alkalmaz. A feladatrendszerek összehasonlítása alapján kimutatható a jogalkotói következetesség.

A polgári nemzetbiztonsági szolgálatokat felügyelő államtitkár a miniszternek a Statútumrendelet 9. § (1) bekezdés 14–15. pontja szerinti, a polgári nemzetbiztonsági szolgálatok irányításáért és a polgári hírszerzési tevékenység irányításáért való felelősségi körbe tartozó feladatai keretében, a miniszter által átruházott jogkörben irányítja az Alkotmányvédelmi Hivatalt (AH), az Információs Hivatalt (IH) és a Nemzetbiztonsági Szakszolgálatot (NBSZ): [480]

- *„Gyakorolja az Ksztv. 2. § (1) bekezdés c)–i) pontjában meghatározott jogosítványokat.*
- *Feladatot határoz meg, utasítást ad az AH, az IH és az NBSZ főigazgatóinak.*
- *Ellenőrzi az AH, az IH és az NBSZ törvényes és rendeltetésszerű működését.*
- *Jóváhagyja az AH, az IH és az NBSZ szervezeti és működési szabályzatát, állománytáblázatát.*
- *Jóváhagyja az AH, az IH és az NBSZ főigazgatóinak kül- és biztonságpolitikai szempontokat érintő, nemzetközi kapcsolatokra vonatkozó javaslatait.*
- *Jóváhagyja az AH, az IH és az NBSZ titkos információgyűjtés belső eljárási és engedélyezési szabályait.*
- *Meghatározza az AH, az IH és az NBSZ időszerű feladatait.*
- *Utasítást ad az AH-nak, az IH-nak és az NBSZ-nek eseti és időszakos információs igény teljesítésére.*
- *Utasítást ad az AH, az IH és az NBSZ főigazgatóinak országos jelentőségű ügyekben elemző-értékelő és koordinációs tevékenység lefolytatására.*

[479] a Honvédelmi Minisztérium Szervezeti és Működési Szabályzatáról szóló 30/2022. (VII. 29.) HM utasítás
[480] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 56-59. §-ok alapján

- *Válaszol a Kormány tagja által a miniszterhez intézett, az AH, az IH és az NBSZ tevékenységét érintő információs igényre.*
- *Javaslatot tesz az AH, az IH és az NBSZ költségvetésére.*
- *Közreműködik az AH, az IH és az NBSZ költségvetési gazdálkodása tekintetében a jogszabályokban meghatározott tervezési, előirányzat-átcsoportosítási, beszámolási, információszolgáltatási, pénzügyi, valamint ellenőrzési kötelezettségek és jogok gyakorlásában.*
- *Gyakorolja a munkáltatói jogokat az AH, az IH és az NBSZ főigazgatói, valamint a főigazgató-helyettesek felett.*
- *Kezdeményezi az AH, az IH és az NBSZ főigazgatói és főigazgató-helyettesei, valamint a tábornok és a tábornoki rendfokozattal rendszeresített beosztásba kinevezett személy nemzetbiztonsági ellenőrzését.*
- *Meghozza az AH, az IH és az NBSZ személyi állománya tekintetében a személyügyi tárgyú intézkedéseket.*
- *Ellátja az AH, az IH és az NBSZ miniszteri irányításából a miniszter rendelkezése alapján rá háruló további feladatokat."*[481]

A polgári nemzetbiztonsági szolgálatokat felügyelő önálló hatáskörben:[482]

- *„Gondoskodik a minisztérium nemzetbiztonsági feladatokat érintő szakmai álláspontjának kialakításáról és képviseletéről.*
- *Véleményezi az AH, az IH, az NBSZ és a NIK működését, a feladat- és hatáskörüket érintő kormányzati döntések tervezeteit.*
- *Meghatározza a kormányzati döntés-előkészítéshez szükséges koordinációs feladatokat.*
- *Kezdeményezi vagy javasolja jogszabály, közjogi szervezetszabályozó eszköz kiadását vagy módosítását.*
- *Javaslatot tesz az AH, az IH és az NBSZ főigazgatójának normatív utasítások kiadására vagy módosítására.*
- *Segíti a miniszternek az Országgyűlés, annak Nemzetbiztonsági bizottsága irányában fennálló tájékoztatási, beszámolási, jelentéstételi és válaszadási kötelezettségeinek teljesítését.*

[481] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 56-59. §-ok alapján
[482] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 56-59. §-ok alapján

- *Kapcsolatot tart nemzetközi partnerszolgálati együttműködés elősegítése érdekében a partnerszolgálatok kormányzati irányításában részt vevő külföldi szervezetekkel és személyekkel.*
- *Javaslatot tesz az AH, az IH és az NBSZ főigazgatóinak és főigazgató-helyetteseinek a kinevezésére.*
- *Fogadja és felterjeszti az AH, az IH és az NBSZ által a miniszternek címzett megkereséseket.*
- *Véleményezi a NIK szervezeti és működési szabályzatát, állománytáblázatát."*[483]

A polgári nemzetbiztonsági szolgálatokat felügyelő államtitkár egyéb feladatai között szerepel, hogy:[484]

- *„Gondoskodik a feladatok meghatározásáról, számontartásáról, végrehajtásáról.*
- *Véleményt nyilvánít a véleményezésre érkezett előterjesztésről, jogszabályról.*
- *Kezdeményezi a megbízhatósági vizsgálat lefolytatását.*
- *Biztosítja a miniszteri és kormányzati döntésekhez szükséges információk, háttéranyagok összeállítását.*
- *Lefolytatja az AH, az IH vagy az NBSZ szakhatósági állásfoglalását tartalmazó hatósági döntés elleni fellebbezés folytán kiadandó másodfokú szakhatósági eljárást.*
- *Kivizsgálja az AH, az IH és az NBSZ tevékenységével, valamint az AH, az IH vagy az NBSZ hivatásos állományú tagja által foganatosított intézkedésekkel kapcsolatos panaszokat.*
- *Jóváhagyja az Nbtv. 69. § (2) bekezdés b) pontjában meghatározott munkáltatói intézkedést.*
- *Vizsgálja a Magyarország biztonsági érdekét sértő külföldi befektetések ellenőrzéséről szóló törvény alapján tett bejelentéseket.*
- *Vezeti a Nemzetbiztonsági Munkacsoportot.*
- *Együttműködik a Védelmi Tanács titkársági feladatait ellátó állami vezetővel.*
- *Irányítja az AH, az IH és az NBSZ védelmi és biztonsági kötelezettségeinek teljesítésével kapcsolatos feladatok ellátását."*[485]

[483] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 56-59. §-ok alapján
[484] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 56-59. §-ok alapján
[485] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 56-59. §-ok alapján

A polgári nemzetbiztonsági szolgálatokat felügyelő államtitkár[486] a NIK tekintetében támogatja a miniszterelnök nemzetbiztonsági főtanácsadója egyes irányítási jogainak gyakorlását. A polgári nemzetbiztonsági szolgálatokat felügyelő államtitkár irányítja a polgári nemzetbiztonsági szolgálatokat felügyelő helyettes államtitkár, a Koordinációs Főosztály I. vezetője, valamint a Koordinációs Főosztály II. vezetője tevékenységét. Munkáját Kabinet és Titkárság segíti. Helyettesítését a Polgári nemzetbiztonsági szolgálatokat felügyelő helyettes államtitkár látja el.

A jogszabálymódosítások eredményeként a Nemzeti Információs Központ irányításáért a Miniszterelnök Nemzetbiztonsági Főtanácsadója felel.[487]

[486] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 56-59. §-ok alapján
[487] a Miniszterelnöki Kabinetiroda Szervezeti és Működési Szabályzatáról szóló 4/2022. (VI. 11.) MK utasítás 8/A-8/D. §-ok alapján

XIV. A SZERZŐ PUBLIKÁCIÓS JEGYZÉKE

HÓDOS László: Gondolatok a nemzeti hírszerző képesség koordinációjáért felelős szervének közjogi helyzetéről. In.: Szakmai Szemle 2018/4.

HÓDOS László: Gondolatok a gerilla-hadviselés elleni küzdelem egyes összefüggéseinek tudományos vizsgálatáról címmel jelent meg In: Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-szakmai Folyóirata 17 : 3 pp. 67-80. , 14 p.

HÓDOS László: A hibrid konfliktusok felívelési szakasza, avagy a fenyegetés észlelésének, megelőzésének és kezelésének nemzetbiztonsági aspektusai, In: Honvédségi Szemle, 2020/4. szám, 39-64. o.

HÓDOS László: Gondolatok Magyarország Nemzeti Biztonsági Stratégiájában azonosított kiemelt biztonsági kockázatok nemzetbiztonsági aspektusairól címmel jelent meg In.: Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-szakmai Folyóirata 17 : 3 pp. 21-31.

HÓDOS László: A kibertér és a mesterséges intelligencia jelentősége és kihívásai a jogállamok nemzetbiztonsági feladatellátásában, Budapest, Magyarország: Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar (2022) , 17 p.

HÓDOS László: A nemzetbiztonsági szolgálatok közelmúltbeli tevékenységét befolyásoló mérföldkövek, avagy az új típusú biztonsági kihívások jelentette veszélyek és az azokra adott kormányzati, illetve jogalkotói válaszok 2010 és 2020 között címmel megjelent In.: Szakmai Szemle: A Katonai Nemzetbiztonsági Szolgálat Tudományos-szakmai Folyóirata pp. 134-149.

HÓDOS László: The Legal Instruments of Hybrid Warfare The Importance of Lawfare In.: National Security Review : Periodical of the Military National Security Service 2022 : 2 pp. 18-30. , 13 p. (2022)

HÓDOS László, DOBÁK Imre A biztonsági-stratégiai dokumentumok és a jogszabályi környezet kapcsolata In: DOBÁK, Imre; RESPERGER, István (szerk.) Stratégiák, stratégiai gondolkodás, nemzetbiztonság Budapest, Magyarország : Ludovika Egyetemi Kiadó (2023) 276 p. pp. 165-178. , 14 p.

HÓDOS László, A kiberbiztonság kérdése a hatékonyabb védelmi és biztonsági koordináció horizontján In: Farkas, Ádám; Kelemen, Roland; Vikman, László (szerk.) Kibertéri műveletek és ellenálló képesség : A kibertéri műveletek egyes állami és jogi kérdései
Budapest, Magyarország : Gondolat Kiadó (2024) 314 p. pp. 61-75. , 15 p.

XV. ÁBRÁK JEGYZÉKE