DOI: 10.59851/imr.13.1.8 IN MEDIAS RES 2024/1. • 8, 153–165

Gondolatok az információs műveletek és az információs tér szabadsága kapcsán

FARKAS ÁDÁM*

A tanulmány célja rávilágítani arra, hogy az információs technológiák és az információs környezet fejlődése szükségképpen együtt jár az információk befolyásolásra való intenzívebb alkalmazásával. Ez az információs műveletek fogalmával kapcsolható össze, amely a komplex biztonság vonatkozásában a katonai értelmezésnél tágabban határozható meg: szolgálhatnak katonai, hírszerzési, politikai-diplomáciai, gazdasági, de akár különféle illegitim célokat is. Ezekkel szemben hatékony védelemre van szükség, ami egyrészt hiteles és aktív ellentevékenységet feltételez, másrészt korlátozások alkalmazását. Azonban a transzatlanti térség modern jogállamaiban a vélemény szabadsága alapjog, amely korlátozható, de az információs tér szempontjából rendkívüli jelentőségű. A kortárs jogállamok döntő többsége a vélemény szabadságának, az egyéni és a társadalmi kapcsolatok fejlesztésének, valamint a személyiség kibontakoztatásának kulcsfontosságú érvényesülési dimenziójaként tekint az információs térre. Ennek szabadsága tehát alapvető érték, amit első ránézésre az információs műveletek megvalósítása és az azok elleni védekezés is korlátoz. A jelen tanulmány célja rávilágítani arra, hogy az információs műveletek és az információs tér szabadsága közti viszony mégsem írható le nulla összegű játszmaként.

Kulcsszavak: információs tér, információs társadalom, információs műveletek, nemzeti érdek, geopolitika

Thoughts about information operations and freedom of information space

The aim of the study is to highlight that the development of information technologies and the information environment necessarily goes hand in hand with the intensified use of information to influence. The latter can be linked to the concept of information operations, which in the context of complex security can be defined in a broader sense than the military. Information operations in the broad sense may serve military, intelligence, political-diplomatic, economic or even various illegitimate purposes. These require effective protection, which implies both credible and active counteraction and the application of restrictions. However, in the modern constitutional states of the transatlantic area, freedom of expression is a fundamental right which, although it can be restricted, is of the utmost importance in the information space. The vast majority of contemporary states see the information space as a key dimension of freedom of expression, the development of individual and social relations and the development of the personality. Its freedom is therefore a fundamental value, which at first sight is limited by the implementation of information operations and the protection against them. The aim of this

* Tudományos főmunkatárs, Széchenyi István Egyetem Deák Ferenc Állam- és Jogtudományi Kar; Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar.

paper is to point out, in principle, that the relationship between information operations and freedom of information space cannot, however, be described as a zero-sum game.

Keywords: information space, information society, information operations, national interest, geopolitics

1. Bevezetés

Az információs tér és az abban kibontakozó információs társadalom a jellegéből adódóan hálózatos, ami az információs platformokhoz való hozzáférés mind egyszerűbbé válásával egyértelműen a decentralizált működés erősítése irányába hat.[1] Ez a jelleg önmagában véve is kettős: jelenthet ellenerőt és garanciát a pluralizmus ellen ható folyamatokkal és cselekményekkel szemben, de lehetőséget teremthet olyan információk vírusszerű terjedéséhez is, amelyek a normál működés, a stabilitás, a társadalmi bizalom és vele az állam legitimitása ellen hathatnak.[2]

Ez utóbbi lényegében az információs műveletek alapjait teremti meg.[3] Ezen a ponton azonban fontos előre jelezni, hogy az információs műveletek hagyományos, katonai értelmezésétől eltérve a jelen tanulmány célja egy tágabb értelmezés alkalmazása, amely szerint az információk szisztematikus, stratégiai elgondoláshoz illeszkedő alkalmazásával a célközönség tudata befolyásolható, méghozzá a műveletet végrehajtó érdekeinek megfelelően, ami jellemzően nem szolgálja a célközönség valós érdekeit. Az információs műveletek e tágabb értelmezése meglátásunk szerint jobban értelmezhetővé teszi a jelenséget a katonai szembenálláson túl a nem állami szereplők jelentette, valamint a hibrid fenyegetések viszonylatában, amely utóbbiak lényegesen szélesebb körben kapcsolódnak a társadalomhoz és az információs tér sokrétű lehetőségeihez és szabadságához.

Az információs tér szabadságának értékként kezelése egyértelműen felhajtóerőt jelenthet a társadalmi és az állami fejlődésnek a világban, hiszen a vélemények sokszínűsége egyebek mellett élénkítheti a demokratikus kultúra erősödését, a különféle társadalmi jelenségek megvitatását, a tudományos teljesítményeket, valamint a jogállami fékek és ellensúlyok érvényesülését is.[4] Az in-

---

1 A témáról átfogóan lásd például Manuel Castells: *A hálózati társadalom kialakulása* (ford. Rohonyi András). Budapest, Gondolat, 2005; Armand Mattelart: *Az információs társadalom története* (ford. Gelléri Gábor). Budapest, Gondolat, 2004; Nicholas Negroponte: *Digitális létezés* (ford. Csaba Ferenc). Budapest, Typotex, 2002; Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora.* Budapest, Ludovika, 2022; Kelemen Roland – Németh Richárd: Társadalmi hálózatok és reziliencia. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/13., 1–31.

2 A téma kapcsán lásd Krekó Péter: *Tömegparanoia.* Budapest, Athenaeum, 2018; Krekó Péter: *Tömegparanoia 2.0.* Budapest, Athenaeum, 2021; Lee McIntyre: *Post-Truth.* Cambridge, MIT, 2018, https://doi.org/10.7551/mitpress/11483.001.0001; Michael A. Peters et al. (szerk.): *Post-Truth, Fake News.* Singapore, Springer Nature, 2018, https://doi.org/10.1007/978-981-10-8013-5.

3 Átfogóan lásd Christopher White – A. Trevor Thrall – Brian M. Mazanec (szerk.): *Information Warfare in the Age of Cyber Conflict.* New York, Routledge, 2021, https://doi.org/10.4324/9780429470509; Csutak Zsolt: Új idők új hadviselése – kognitív biztonság az információs és a kiberhadviselés korában. *Honvédségi Szemle,* 2018/5., 33–45.; Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/18., 1–27.

4 A téma kapcsán bővebben lásd Koltay András – Török Bernát (szerk.): *Sajtószabadság és médiajog a 21. század*

formációs korszak egyik sajátossága, hogy az információs térben érvényesülő egyéni és társadalmi folyamatok a korábbi társadalmi kapcsolatokhoz sajátos pszichés viszonyulással párosulnak.[5] Ez különösen a korlátozó intézkedések fogadtatásában tapasztalható, ami mind az internetet érintő korlátozások, mind pedig a covid-járvány miatt bevezetett intézkedések kapcsán jól érezhető volt a fiatalabb, az információs technológiák szempontjából „bennszülött" generációknál.

A technikai lehetőségek kérdései mellett az ellenérdekelt információs műveletekkel szembeni korlátozó fellépés társadalmilag és politikailag is problémásabb jelenleg, mint korábban. Ezt a cenzúra kérdését vizsgáló újabb kutatások, valamint az internetszabályozás demokratikus és autoriter modelljeit elemző tanulmányok is alátámasztják. Emiatt az információs műveletek és az információs tér szabadsága közti viszonyra nézve két kulcskérdést tekintünk kiindulási pontnak: az egyik az információs műveletek és az azokkal szembeni fellépés értékelése az információs tér szabadsága kapcsán, a másik pedig az információs műveletekkel szembeni fellépésnek az információs tér szabadságát leginkább óvó, lehetséges fő irányai. A jelen tanulmány ezekre a fő kérdésekre kíván válaszokat adni azért, hogy az információs teret érintő kiegészítést nyújtson a komplex biztonság szavatolásával összefüggő további kutatásokhoz.

2. Az információs műveletek értelmezési keretei és az információs tér szabadságához való viszonyuk

Az információs műveletek fogalmi értelmezéséhez egyértelműen szilárd alapot tud nyújtani a katonai megközelítés. Ennek tudományos igényű, átfogó szintézisét adja Haig Zsolt, aki a következő definícióval határozza meg az információs műveleteket:

> az információs környezetben érvényesülő információs képességek integrált, összehangolt és koordinált alkalmazására irányuló tevékenységek összessége, [amelyek] kognitív képességekkel közvetlenül, illetve technikai képességekkel közvetetten hatásokat gyakorolnak a műveletekben részt vevő célközönség szándékára, helyzetértelmezésére és képességeire.[6]

Ezt az értelmezést egészíti ki Pozderka Zoltán meghatározása:

> Az információs műveleteknek a 2015-ös NATO INFOOPS-doktrínában található fogalmát az összehasonlítás megkönnyítése érdekében három részre osztva célszerű elemezni: (1) olyan törzsfunkció, (2) amely az információs tevékenységek elemzésével, tervezésével, értékelésével és integrálásával (3) a kívánt hatást fejti ki az ellenség, a lehetséges ellenség, valamint az Észak-atlanti Tanács által

elején. Budapest, Wolters Kluwer, 2015; Koltay András: *A szólásszabadság alapvonalai.* Budapest, Századvég, 2009; Majtényi László: *Az információs szabadságok.* Budapest, CompLex, 2006.

5 Vö. Mary Aiken: *Cybercsapda* (ford. Török Csaba). Budapest, Harmat, 2022; Patricia Wallace: *Az internet pszichológiája* (ford. Krajcsi Attila). Budapest, Osiris, 2006.

6 Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018, 210.

jóváhagyott célközönség akaratára, helyzetismeretére és képességeire, a Szövetség küldetésével kapcsolatban megfogalmazott célkitűzések támogatása érdekében.[7]

Mindehhez érdemes még áttekinteni az Észak-atlanti Szerződés Szervezetének (NATO) az egyes információs műveleti dokumentumaiban – különösen a vonatkozó doktrínájában[8] – tükröződő megközelítését, amely a tagállamok számára iránymutatásként szolgál. Eszerint az információs műveletekben számos tevékenység kapcsolódik össze, például a lélektani és a kibertérműveletek, az elektronikai hadviselés, a civil-katonai együttműködés, a műveleti biztonság, az információs támogatás és a stratégiai kommunikáció.[9] A katonai értelmezés láthatóan elválaszthatatlan a katonai műveletek tervezésére és végrehajtására vonatkozó megközelítéstől, és szorosan kapcsolódik az összhaderőnemi megközelítéshez – az információs műveletek sok esetben támogatják, kiegészítik a hagyományos műveleti tevékenységeket.

Az információs műveletek katonai értelmezése nem elhanyagolható a jelen tanulmány, de általában az információs tér értelmezése szempontjából sem, mert a hibrid hadviselés és konfliktusok vonatkozásában is jelentőséggel bír, ugyanis a hibrid szcenárió mögött jellemzően jelen van a katonai stratégiai megközelítés is. A katonai értelmezés azért is fontos, mert a katonai műveletek tervezésére és szervezett végrehajtására jellemző strukturáltság megjelenik a jelentősebb nem katonai fenyegetésekben, akár a terrorizmus, akár a különféle szélsőséges szervezetek vagy az állami érdeket megvalósító nem állami szereplők részéről. Ez valószínűsíthetővé teszi, hogy az információs térben végzett tevékenységeknél a katonai megközelítés és egyes katonai megoldások átszivárognak a nem katonai megvalósítási formákba. Mindeközben a központi kormányzati és politikai intézmények szerepe is bővül, a döntéshozó-célmeghatározó jellegen túl műveleti jellegű, például stratégiai kommunikációs funkciókkal, amelyeknek összhangban kell lenniük a védelmi-biztonsági tevékenységek rendszerével.

Az információs műveletek katonai megközelítéséből látható, hogy az meglehetősen doktriner felfogással és sematizmussal párosul.[10] Emellett jellegéből adódóan állami kötöttségű is, hiszen egy szisztematikus katonai művelet tervezése és megvalósítása legalább mögöttesen állami jelenlétet feltételez. Azonban az információs tér nyújtotta lehetőségek sokasága lehetővé teszi, hogy más szereplők is befolyásolják az adott egyén, társadalom vagy állam tudatát, biztonságát és stabilitását, katonai szervezettség vagy közvetlen katonai kötődés nélkül is. E téren kézenfekvő az ellenérdekelt hírszerzési tevékenység, amely a katonai műveleteknél nagyobb mozgástérrel, alapvetően rejtettség-fedettség mellett, a tág értelemben vett nemzetbiztonság dimenziójában kívánja érvényesíteni saját érdekeit a célközeg érdekei ellenében. Látni kell azonban azt is, hogy lényegét tekintve a terroristák által az elkövetett támadásokról vagy túszul ejtett személyekről készített videóknak a világhálón való célzott terjesztése is egyfajta információs művelet, hiszen egyszerre szolgálja a szembenálló fél katonai vagy rendészeti állományának de-

7 Pozderka Zoltán: Az információs műveletek helye és szerepe a művelettervezésben. *Hadtudomány,* 2016. különszám, 132.

8 Allied Joint Doctrine for Information Operations. NATO, 2009. november, https://bit.ly/3V5YoHO.

9 Allied Joint Doctrine for Information Operations. NATO, 2023. január, https://bit.ly/3Kay88Z, 17–21.

10 Vö. Allied Joint Doctrine Edition, with UK National Elements. NATO, 2022. december, https://bit.ly/3K8KXk6.

moralizálását és a megcélzott államok, társadalmak biztonságérzetének erodálását. Ebben a megközelítésben a szélsőséges és a legális kereteken túllépő aktivista csoportok különféle nyomásgyakorló információs kampányai is beilleszthetők az információs műveletek közé.

Az információs műveletek tágabb értelmezésével olyan tevékenységek szervezett és célzatos megvalósításáról beszélhetünk, amelyek során információk strukturált és magasan szervezett felhasználásával és terjesztésével elérhető egy adott célközönség tudatának befolyásolása, biztonságérzetének csökkentése vagy cselekvési irányainak megváltoztatása valamely mögöttes és nem kommunikált célból. Ez a megközelítés egyfelől rendkívül tág, másfelől azonban képes reagálni a komplex biztonság kiterjedt vertikumára és horizontjára, valamint a nem állami szereplők jelentőségének növekedésére is a különféle biztonsági fenyegetések kapcsán. Úgy is mondhatjuk, hogy részint megfelel a hibrid fenyegetések értelmezésének, mivel feltételként mögöttesen fenntartja a stratégiai szervezettséget és a nem kommunikált cél elérése érdekében végzett láncolatszerű megvalósítást, részint viszont nem teszi szükségszerű feltétellé a katonai fellépésre jellemző nyílt jelleget és a közvetlen állami kötődést.

Az információs műveletek tágabb értelmezése magába foglalja a fenti példákat – a terrorizmust, a szélsőségességet, a legalitás keretein túlnyúló különféle aktivitásokat és a hibrid fellépést, ami miatt jobban alkalmazható a kortárs biztonsági környezet sajátosságaira. Azt, hogy az információs térben a különféle szervezett befolyásoló tevékenységek rendkívül elterjedtek, ma már a *post truth* és a *fake news* irodalma[11] éppúgy alátámasztja, mint a *terrorfranchise*-ok, a különféle belpolitikai jelenségek nemzetközi szintű – a hibrid szcenáriótól sem távoli – relevanciájának[12] vagy épp az orosz–ukrán szembenállás háború előtti szakaszának tapasztalatai. Látni kell ugyanis, hogy az információs társadalom erősödésével, hasonlóan a kibertér műveletekhez és az ott megvalósítható kártékony cselekményekhez, ma már sok – de nem minden – esetben sokkal célravezetőbb az érdekeket nyílt szembenállás nélkül, az információk torzításával érvényesíteni. Ennek oka az, hogy egy eredményes információs befolyásolás is jelentős hatást tud kiváltani például társadalmi feszültség generálásával, ami még az előkészítés költségei ellenére is sokkal kevéssé forrásigényes és kockázatos, mint a hagyományos beavatkozási formák bármelyike.

Az információs műveletek tágabb értelmezése azonban nemcsak a kortárs biztonsági környezetre való jobb alkalmazhatóság miatt fontos, hanem az információs tér szabadságával kapcsolatos értelmezés szempontjából is.[13] Egyértelmű ugyanis, hogy maguk az információs műveletek lényegében az információs tér szabadságát visszaélésszerűen használják ki a megcélzott

---

11 Erről átfogóan lásd például Cherilyn Ireton – Julie Posetti (szerk.): *Journalism, Fake News and Disinformation.* Paris, UNESCO, 2018; Isabella Garcia-Camargo – Samantha Bradshaw: Disinformation 2.0: Trends for 2021 and Beyond. *Hybrid CoE Working Paper* 11, 2021; Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog – Állam – Politika,* 2021/3., 71–85.

12 Bővebben lásd Georgios Giannopoulos – Hanna Smith – Marianthi Theocharidou (szerk.): *The Landscpae of Hybrid Threats: A Conceptual Model.* Luxembourg, EU – Hybrid CoE, 2021; Kelemen Roland: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban. *SmartLaw Research Group Working Paper,* 2021/2., 1–17.

13 Erről átfogóan lásd Krasznay Csaba: *Kiberbiztonság a XXI. században.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2022; Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018; Kelemen Roland: A kibertér jellemzőinek biztonság központú vizsgálata. *Jog – Állam – Politika,* 2023/1., https://doi.org/10.58528/JAP.2023.15-1.75, 75–90.

közösségétől eltérő, azzal jellemzően ellentétes érdekek érvényesítése érdekében. Egy sikeres ellenérdekelt információs műveleti tevékenység – függetlenül attól, hogy azt állami vagy nem állami szereplő hajtja végre – olyan társadalmi, tudati hatásokat vált ki a megcélzott közegben, amelyek az információs tér szabadságát közvetítő közegként használva gyengítik az adott közösség stabilitását, különféle funkcióit. Az ilyen információs művelet tehát a tág értelemben vett közösségi szabadságot korlátozza, hiszen befolyásolással tereli el a közösséget az eredeti törekvéseitől, céljaitól, lehetőségeitől. Természetesen az információs műveletek szolgálhatnak jó célt is, például amikor az egyébként a tág értelemben vett szabadság korlátozására épülő konstrukciók gyengítését célozzák vagy más, békés társadalmak ellen irányuló cselekmények előkészítésének megakadályozását segítik. Ez persze a másik fél szempontjából vitatható.

A védelmi és a biztonságot szavatoló cselekvések, valamint azok megítélése tehát egyértelműen értékekhez és érdekhez kötött, amiből következően egy információs művelet közvetlen és közvetett hatásai az információs tér szabadságát szolgálhatják. Ha ezt elfogadjuk, akkor az ellenérdekelt információs műveletekkel szembeni fellépés korlátozó jellege is új megvilágításba kerül. Ebben az esetben arról beszélünk, hogy azonosított információs műveleti csatornákra, lehetőségekre és megoldásokra vonatkozóan korlátozó rendszabályok alkalmazását tesszük lehetővé, ami a nagyobb károk elhárítása érdekében csorbítja az információs tér szabadságát. Erre számos uniós szintű példát nyújt a terrorista tartalmak vagy az orosz propaganda korlátozása. Ez a korlátozó jellegű védekezés akár nulla összegű játszmának is tűnhet az információs tér szabadsága kapcsán, hiszen az információs tér szabadságának nagyobb korlátozása eredményezne erőteljesebb védekezést. Ez azonban csak első ránézésre tűnhet így, hiszen a korlátozás alá eső cselekmény vagy információs csatorna a jellegéből adódóan az információs tér szabadsága ellen hat, mivel azt torzító-befolyásoló céllal kívánja eszközként használni, és ezzel a szabadság alapját adó stabilitást erodálni.

A korlátozó jellegű információs műveletek ellen optimálisan alkalmazott védekezés tehát csak látszólag hat az információs tér szabadsága ellenében, lényegében annak megóvását szolgálhatja. Ehhez fontos hozzátenni, hogy lényeges az „optimális" jelző, és azzal is számot kell vetni, hogy az információs műveletek elleni fellépésnek nem csak korlátozó jellegű lehetőségei vannak. Az információs műveletek hatékonyságát jelentős mértékben befolyásolják a megcélzott közeg információs sajátosságai, ha úgy tetszik, információs és kommunikációs rezilienciája is. Ahol az információs közeg nem minősül megbízhatónak, átláthatónak, következetesnek és hitelesnek, ott könnyebb a befolyásoló információs fellépés érvényesítése és a részben-egészben hamis információk terjesztésével való hatáskiváltás. Azonban az ezzel kapcsolatos ellenálló képességet nem a korlátozások erősítik fel, hanem a saját információs közegbe vetett bizalom fokozását szolgáló intézkedések. A kiegyensúlyozott és reziliens információs közeg tehát olyan tényező az információs műveletekkel szembeni védekezésben, amely jelentős mértékben épül az információs tér szabadságára és annak konstruktív kiaknázására. E körben az információs tér szabadságának érvényesítése önmagában is ellenerőként hathat az információs műveletek hatékony megvalósításával szemben.

A fentiek alapján elmondható, hogy az információs műveletek lényegüket tekintve az adott információs közeg befolyásolására, torzítására törekednek, amivel szemben a hatékony védelmet részint a korlátozó intézkedések biztosíthatják, jelentős részben viszont az információs közeg egészséges és reziliens működése. E tekintetben a védekező célú korlátozás optimális alkalmazása csak látszólag hat ellene az információs tér szabadságának, mert azzal valójában megelőzhető vagy elhárítható az információs közeg károsítása. Ugyanakkor az is elképzelhető, hogy az információs művelet olyan közeg ellenében valósul meg, amelynek tartós és zavartalan működése szé-

lesebb szabadságkorlátozáshoz vagy a békés társadalmi berendezkedés elleni ártó cselekményekhez vezetne, vagyis tágabb körben az információs tér szabadságát is korlátozná. Ezek alapján megállapítható, hogy az információs műveletek és az információs tér szabadsága közti viszony nem írható le nulla összegű játszmaként, azonban az információs tér szabadságának sérelmét csak az információs műveletek elleni optimális reagálással lehet minimalizálni vagy elkerülni.

3. Az információs tér szabadságát leginkább megóvni képes lehetséges információs műveleti és védelmi megoldások

Az információs tér szabadságának alapvető értékként kezelése a transzatlanti térségben egyértelmű.[14] Hasonlóan más demokratikus értékekhez, magától értetődőnek látszik az is, hogy e körben is kiemelkedő szerepe van a bizalomnak, különösen a közintézményekbe és az állami fellépésbe vetett bizalomnak. Ez az információs tér szabadsága elleni cselekményekkel szembeni védekezés szempontjából fontos, és a kapcsolódó információs műveleti és védelmi megoldások szempontjából is mérlegelendő.

A védelmi és a biztonsági szféra eszköztára kapcsán hagyományosnak mondható korlátozó vagy tiltó intézkedések értelemszerűen nem lehetnek az ellenérdekelt információs műveleti tevékenységre való reagálás kizárólagos eszközei, hiszen azok nehezen tudnak megfelelni az információs tér szabadsága felől értelmezett szükségesség és arányosság kritériumainak. Itt merül fel a bizalom kérdése, ami a korlátozó vagy tiltó intézkedések és a dezinformáló félre irányuló esetleges ellentevékenységeken túl a hamis tartalmak cáfolata[15] és a társadalom dezinformációval szembeni ellenállóképessége szempontjából is kulcsfontosságú. Ugyanis az ellenérdekelt információs tevékenység hatóképességének csökkentésére, semlegesítésére irányuló állami kommunikáció sikerességének alapvető feltétele, hogy a társadalom – és a különféle állami és nem állami, hazai és külföldi partnerek – bízzanak az állami közlésekben. E bizalomnak a kiépítése egyebek mellett a társadalom számára átlátható, értelmezhető és hiteles védelmi-biztonsági szakmai kommunikációt feltételez, amely bizonyos értelemben – szükségszerű kormányzati kötődései ellenére is – különválik a kormányzás politikai kommunikációjától, mintegy szakmai hátteret ad annak, és önálló kommunikációs tényezőként is megjelenik.

Nem véletlen, hogy a katonai értelmezésben a stratégiai kommunikáció is kiemelt szerepet tölt be. Ez a NATO-ban a kommunikációs képességek és az információs funkciók integrálását jelenti a katonai (törzs- vagy vezetési-irányítási) feladatokba az információs környezet alakítása

---

[14] Részletesen lásd például Török Bernát: Az információszabadság. In Bódi Stefánia – Schweitzer Gábor (szerk.): *Alapjogok – az emberi jogok alkotmányos védelme Magyarországon*. Budapest, Ludovika, 2021; Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása.* Budapest, Gondolat, 2022, https://doi.org/10.24362/cenzura.gosztonyi.2022; Smuk Péter: Közérdek *vs.* közérdek: A vélemény- és információszabadság közérdekre alapozott igazolása és korlátozása. In Lapsánszky András – Smuk Péter – Szigeti Péter (szerk.): *Köz/érdek. Elméleti és szakjogi megoldások egy klasszikus problémára.* Budapest, Gondolat, 2017, 328–348.

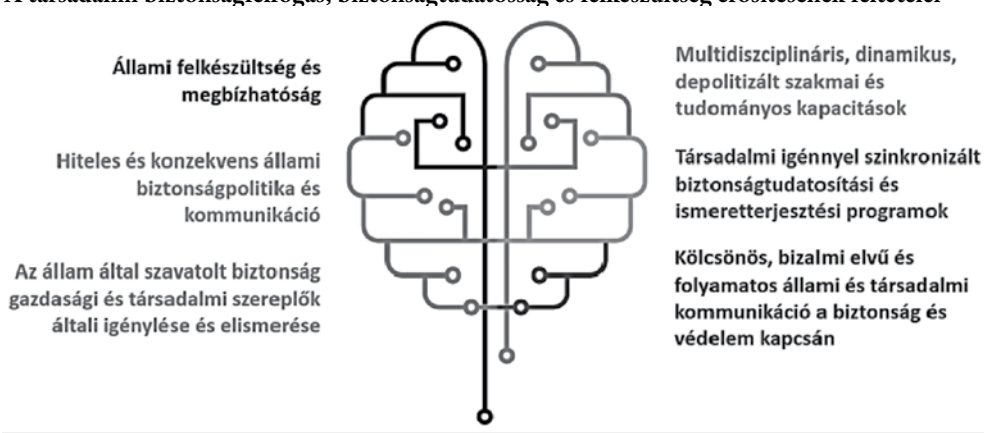
[15] European Digital Media Observatory (EDMO): https://bit.ly/4awlGem; Gyakorlati kézikönyv a félretájékoztatásról (dezinformációról): az új Átláthatósági Központ első alkalommal nyújt betekintést és adatokat az online félretájékoztatásról. Európai Bizottság, 2023. február 9., https://bit.ly/44PaPe9.

és megértése érdekében, a stratégiai célok támogatására.[16] Ennek fontosságát jelzi, hogy a NATO-n belül önálló kiválósági központ, azaz képzési és kutatási intézmény foglalkozik vele, amely szakértői és tudományos megalapozottságot nyújt a kapcsolódó NATO-tevékenységeknek és a döntéshozatalnak. Fontos azonban kiemelni, hogy az objektív szakmai háttértámogatás érdekében a NATO Rigában működő stratégiai kommunikációs kiválósági központja nem része a NATO parancsnoki struktúrájának, szakmai tevékenységének tartalma nem áll az Északatlanti Tanács irányítása alatt.[17] A kommunikációs vonatkozás 21. századi társadalmi és biztonsági jelentőségét mutatja az is, hogy az a NATO szintjén is önálló kiválósági képzési és kutatási irányként jelenik meg, ugyanis e szakmai bázisú kommunikáció sikere jelentős hatást gyakorolhat a védelmi-biztonsági intézmények általános társadalmi megítélésére és konkrét események vonatkozásában a válságkommunikáció és -menedzsment kimenetelére is.[18]

A bizalom kapcsán érdemes felhívni a figyelmet arra, hogy az információs tér szabadságából következően mindenképp lesz valamilyen társadalmi értelmezése és értékelése mind az ellenérdekelt tevékenységnek, mind a megelőző vagy elhárító és reagáló válaszlépéseknek. E szükségszerű reakció miatt a védekezés szempontjából előnyösebb a magasabb bizalmi faktor, aminek viszont feltétele, hogy a bizalom erősítését szolgáló kommunikáció ne csak krízishelyzetekben jelenjen meg, hanem folyamatosan jellemezze a védelmi-biztonsági működést úgy, hogy intenzitását a válságkezelés során csak fokozni kelljen (lásd *1. ábra*). Ez összhangban áll a védelmi-biztonsági célú reziliencia kapcsán azonosított egyéb szempontokkal is.[19]

1. ábra

A társadalmi biztonságfelfogás, biztonságtudatosság és felkészültség erősítésének feltételei



16 Allied Joint Doctrine for Information Operations (9. lj.) 13.

17 NATO Strategic Commmunication Centre of Excellence, https://bit.ly/44UGbQU.

18 Példaként lásd Hadley Newman: *Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework 'DISARM'.* NATO, 2022. november 29., https://bit.ly/3QMHmMn.

19 Vö. Farkas Ádám: *A védelem és biztonságszavatolás szabályozásának alapkérdései Magyarországon*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022, 85–100.

Ugyanezt támasztják alá az ellenállóképes, felkészült és komplex biztonsági környezetben működő védelmi-biztonsági rendszer kritériumai is. Ebben egymásra épülő szintekkel, belülről kifelé haladva az alábbiakat különböztethetjük meg:

1. Döntéshozatali mag
    1.1. Korszerű és gyors kormányzati információs ciklus
    1.2. A kormányzat döntésképessége
    1.3. A kormányzás folytonossága
2. Reagálási mag
    2.1. A védelmi és biztonsági szervek koordinált irányítása
    2.2. Felkészült és reagálóképes védelmi és biztonsági erők, szolgálatok
    2.3. Felkészült állami ellátórendszer és közigazgatás
3. Társadalmi mag
    3.1. Korszerű és dinamikus tudományos és szakértői háttér
    3.2. Felkészült és együttműködő piaci szféra
    3.3. Felkészített és többségileg támogató társadalom

Látható, hogy a társadalmi támogatottság – mint bizalmi jellemző – alapvető fontosságú,[20] de emellett a társadalom és az államszervezet felkészítettsége is kulcskérdés. E körben kiemelkedő szerepe van az információs műveletekkel kapcsolatos biztonságtudatosság és -érzékelés naprakészségének és megalapozottságának, valamint annak is, hogy – egyebek mellett – az információs tér szabadságára építve a nem állami szereplőkkel együttműködve kerüljön megerősítésre a biztonságtudaton belül az információs tényezők fontossága, a lehetséges ellenérdekelt tevékenységek működési sémái és egyes sajátosságai.

A biztonságtudatosság növelésében a tudatosítás, azaz az aktív, például tanfolyami, szervezett graduális és felnőttképzés, szabadegyetemi és szakmai-tudományos ismeretterjesztő képzés, valamint az ennek a mindennapokban szilárd információmegújítási alapot adó, hiteles és szakszerű kommunikáció játszik főszerepet. Emellett fontos egyfajta információs éberségi keretrendszer kialakítása is, amely lényegében az információs tér szabadságával feltehetően visszaélő vagy azt csorbító tevékenységek és platformok azonosítását segítheti elő, a kiberbiztonság terén már általánosan használt *awareness* működéséhez hasonlóan.[21] Természetesen itt számításba kell venni, hogy az információs tér szabadságának potenciális sérelmével, kihasználásával kapcsolatos feltevések mindig tartalmi vizsgálatot igényelnek, ami miatt különös gondosságot igényel ez a fajta *awareness* törekvés, hiszen egyes platformok alap nélküli vagy indokolatlan „bepanaszolása" más megközelítésben éppen a véleményszabadságnak és vele az információs tér szabadságának korlátozása felé hathat. E körben garanciális megoldást jelenthet az állami cselekvés mellett a nem állami szereplők bevonása.

---

20 Uo.; Kelemen Roland: Cyberfare state – egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper,* 2022/1., 1–36.

21 Bővebben lásd Benedikt Lebek et al.: Information Security Awareness and Behavior: A Theory-Based Literature Review. 12 *Management Research Review* (2014), https://doi.org/10.1108/MRR-04-2013-0085, 1049–1092.; Ranjit Bhaskar: Better Cybersecurity Awareness Through Research. (3) *ISACA Journal* (2022) 1–10.; Faisal Alotaibi et al.: A Review of Using Gaming Technology for Cyber-Security Awareness. (2) *International Journal for Information Security Research* (2016660666).

A lehetséges eszköztár komplexitását tekintve – a NATO megközelítését, valamint a reziliencia témaköreit és a hazai védelmi-biztonsági reformot is figyelembe véve – célszerű lehet külön kezelni az információs tér szabadsága és vele a társadalmi stabilitás ellen ható konkrét tevékenységek kapcsán felmerülő eszközöket, valamint általában véve a jelenséggel szembeni megfelelő felkészülés és reagálás eszköztárát. Ezek csoportosítása az *1. táblázatban* látható.

1. táblázat
Az információs tér védelmének eszköztára

Konkrét tevékenységek kapcsán felmerülő eszközök	**A felkészülés és általános reagálás eszközei**
korlátozó/tiltó intézkedések	a biztonságtudat és az ellenállóképesség erősítése állami-társadalmi kommunikációval és tudatosítással
	hiteles, szakszerű, bizalomerősítő védelmi-biztonsági kommunikáció
esetleges válaszlépések (jogi, diplomáciai, védelmi-biztonsági stb.)	a kríziskommunikáció előkészítése
	az ellenérdekelt információs tevékenységek időben történő és megfelelő azonosítását szolgáló megoldások kidolgozása és üzemeltetése *(awareness)*
kríziskommunikáció	korlátozó vagy tiltó intézkedések előkészítése
	esetleges válaszlépések előkészítése

A műveleti és a védelmi megoldások kapcsán megállapítható, hogy azok részint technikai megközelítést és felkészülést igényelnek, például eléréskorlátozásokat, kommunikációs panelek széles körű célba juttatását, ellentevékenységet az illegális tartalmak és más cselekmények vonatkozásában stb., jelentős részben azonban társadalompszichológiai, kommunikációs, szociológiai, védelmi-biztonsági felkészítési és igazgatási szakértelemre épülő megközelítést tesznek szükségessé. Az információs tér szabadságát jelentős mértékben veszélyeztetni vagy korlátozni képes fenyegetések kezeléséhez, különösen az információs műveletek elleni hatékony felkészüléshez és védekezéshez tehát átfogó szemléletre van szükség.

4. Zárszó

Az információs korszak dinamikus fejlődése nem meglepő fordulatként hozta magával az információs tér védelmi-biztonsági, katonai és azon túlmutató értelemben vett műveleti szerepének felértékelődését. Meglepetésként talán az információs technológia és társadalom kibontakozásának dinamikája és ezzel a biztonsági jelentőség gyors és hatványozott növekedése szolgált az elmúlt évtizedben, ami mind a kibertér, mind az információs műveletek értelmezése, mind a hibrid fenyegetések kapcsán komoly figyelmet kapott. Ez a kihíváshalmaz valamennyi államot és társadalmat érinti, mivel a katonai értelmezésen túli keretben is megjelenik, így a hírszerzési verseny, a geopolitika rendeződése, a szélsőségesség különféle formái, de a bűnözés tekintetében

is kapcsolódási pontokat talál. Az információs tér biztonsági kihívásai a hagyományos biztonságra is hatást gyakorolnak, valamint a véleményszabadságra nagyban építő információs tér szabadságát is sajátosan érintik.

Az információs műveletek és az információs térben végzett védelmi-biztonsági tevékenységek nem szükségképpen és egyenes arányban jelentik az információs tér szabadságának korlátozását, hiszen lehet, hogy éppen annak megóvására irányulnak a szándékoltan hamis vagy kártékonyan módosított információs tartalmak elleni fellépéssel. Egyértelműen szoros és komplex az összefüggés az információs műveletek és az információs tér materiális szabadságának megóvása között. Emiatt fontosak a műveleti és a védelmi tevékenységekre hagyományosan jellemző korlátozó vagy tiltó megoldások mellett a további lehetséges fellépési módozatok, amelyek közül kiemelkedő jelentőségű a felkészülés, a biztonságtudatosság és a bizalmon alapuló civil-állami kooperáció.

A lehetséges műveleti és védelmi megoldásokat és a téma egészét érintően is elengedhetetlen az átfogó megközelítés, ami a NATO-ban nem újdonság, és a reziliencia előzményeként is felfogható. Ehhez alapvető követelmény az állami szervek és a társadalmi csoportok megfelelő együttműködése és legalább védelmi téren bizalmi viszonya, a védelmi-biztonsági érdekek, célok, sajátosságok megfelelő artikulálása, a szakszerű és hiteles – szükségképpen depolitizált – védelmi kommunikáció, valamint az állami és a nem állami szakmai-tudományos szereplők konstruktív diskurzusa.

Az uniós tagállamok és a NATO példája alapján külön hangsúlyozandó a témakörrel foglalkozó szakmai-tudományos intézmények és tömörülések megfelelő működése, teljesítményelvű támogatásának megtérülése, és ezek által a konkrét fellépés, a felkészülés és a biztonságtudatosság erősítésének rendszerszintű és széles támogatása. Emellett felvethető olyan kutatási pályázatok indítása is, adott esetben a védelmi-biztonsági vagy a haderőreform égisze alatt, amelyek célzottan a védelem társadalmi dimenzióit erősítő és – megfelelő pályázati kritériumok és intézményi megoldások mellett – az állami feladatellátást és döntés-előkészítést is segítő multidiszciplináris kutatásokat élénkítik.

Mindezek alapján megállapítható, hogy a kérdés kapcsán komoly feladatok várnak még ránk, amelyek között elsőként a tudomány- és a szakterületeken átívelő diskurzus élénkítése és a multidiszciplináris elemzések fontossága emelendő ki. Ezek nélkül a bizalom és a hiteles kommunikáció nehezen képzelhető el, de közben maga a közeg rendkívül dinamikusan, az értékes innováció mellett a biztonsági kihívásoknak és fenyegetéseknek is kedvező módon változik.

Irodalomjegyzék

Aiken, Mary: *Cybercsapda* (ford. Török Csaba). Budapest, Harmat, 2022.

Alotaibi, Faisal et al.: A Review of Using Gaming Technology for Cyber-Security Awareness. (2) *International Journal for Information Security Research* (2016660666).

Bhaskar, Ranjit: Better Cybersecurity Awareness Through Research. (3) *ISACA Journal* (2022) 1–10.

Castells, Manuel: *A hálózati társadalom kialakulása* (ford. Rohonyi András). Budapest, Gondolat, 2005.

Csutak Zsolt: Új idők új hadviselése – kognitív biztonság az információs és a kiberhadviselés korában. *Honvédségi Szemle,* 2018/5., 33–45.
Farkas Ádám: *A védelem és biztonságszavatolás szabályozásának alapkérdései Magyarországon*. Budapest, Magyar Katonai Jogi és Hadijogi Társaság, 2022.
Farkas Ádám – Spitzer Jenő: Az információs korszak és az állami reziliencia egyes kérdései. *Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2021/18., 1–27.
Garcia-Camargo, Isabella – Bradshaw, Samantha: Disinformation 2.0: Trends for 2021 and Beyond. *Hybrid CoE Working Paper* 11, 2021.
Giannopoulos, Georgios – Smith, Hanna – Theocharidou, Marianthi (szerk.): *The Landscpae of Hybrid Threats: A Conceptual Model.* Luxembourg, EU – Hybrid CoE, 2021.
Gosztonyi Gergely: *Cenzúra Arisztotelésztől a Facebookig. A közösségi média tartalomszabályozási gyakorlatának komplexitása*. Budapest, Gondolat, 2022. https://doi.org/10.24362/cenzura.gosztonyi.2022
Haig Zsolt: *Információs műveletek a kibertérben.* Budapest, Dialóg Campus, 2018.
Ireton, Cherilyn – Posetti, Julie (szerk.): *Journalism, Fake News and Disinformation.* Paris, UNESCO, 2018.
Kelemen Roland: A nem állami kibertéri műveletek egyes szereplőinek jelentősége a hibrid konfliktusokban. *SmartLaw Research Group Working Paper,* 2021/2., 1–17.
Kelemen Roland: Radikalizálás, dezinformálás és tömegpszichózis modern köntösben: a hibrid konfliktus kibertérben. *Jog – Állam – Politika,* 2021/3., 71–85.
Kelemen Roland: Cyberfare state – egy hibrid állammodell 21. századi születése. *Military and Intelligence CyberSecurity Research Paper,* 2022/1., 1–36.
Kelemen Roland: A kibertér jellemzőinek biztonság központú vizsgálata. *Jog – Állam – Politika,* 2023/1., 75–90. https://doi.org/10.58528/JAP.2023.15-1.75
Kelemen Roland – Németh Richárd: Társadalmi hálózatok és reziliencia*. Védelmi-biztonsági Szabályozási és Kormányzástani Műhelytanulmányok,* 2022/13., 1–31.
Koltay András: *A szólásszabadság alapvonalai.* Budapest, Századvég, 2009.
Koltay András – Török Bernát (szerk.): *Sajtószabadság és médiajog a 21. század elején.* Budapest, Wolters Kluwer, 2015.
Kovács László: *Kiberbiztonság és -stratégia.* Budapest, Dialóg Campus, 2018.
Krasznay Csaba: *Kiberbiztonság a XXI. században.* Budapest, Katonai Nemzetbiztonsági Szolgálat, 2022.
Krekó Péter: *Tömegparanoia.* Budapest, Athenaeum, 2018.
Krekó Péter: *Tömegparanoia 2.0.* Budapest, Athenaeum, 2021.
Lebek, Benedikt et al.: Information Security Awareness and Behavior: A Theory-Based Literature Review. 12 *Management Research Review* (2014) 1049–1092. https://doi.org/10.1108/MRR-04-2013-0085
Majtényi László: *Az információs szabadságok.* Budapest, CompLex, 2006.
Mattelart, Armand: *Az információs társadalom története* (ford. Gelléri Gábor). Budapest, Gondolat, 2004.
McIntyre, Lee: *Post-Truth.* Cambridge, MIT, 2018. https://doi.org/10.7551/mitpress/11483.001.0001
Negroponte, Nicholas: *Digitális létezés* (ford. Csaba Ferenc). Budapest, Typotex, 2002.

Newman, Hadley: *Foreign Information Manipulation and Interference Defence Standards: Test for Rapid Adoption of the Common Language and Framework 'DISARM'.* NATO, 2022. november 29., https://bit.ly/3QMHmMn.

Peters, Michael A. et al. (szerk.): *Post-Truth, Fake News.* Singapore, Springer Nature, 2018. https://doi.org/10.1007/978-981-10-8013-5

Pozderka Zoltán: Az információs műveletek helye és szerepe a művelettervezésben. *Hadtudomány,* 2016. különszám, 131–141.

Smuk Péter: Közérdek *vs.* közérdek: A vélemény- és információszabadság közérdekre alapozott igazolása és korlátozása. In Lapsánszky András – Smuk Péter – Szigeti Péter (szerk.): *Köz/érdek. Elméleti és szakjogi megoldások egy klasszikus problémára.* Budapest, Gondolat, 2017, 328–348.

Török Bernát: Az információszabadság. In Bódi Stefánia – Schweitzer Gábor (szerk.): *Alapjogok – az emberi jogok alkotmányos védelme Magyarországon.* Budapest, Ludovika, 2021.

Török Bernát – Ződi Zsolt (szerk.): *Az internetes platformok kora.* Budapest, Ludovika, 2022.

Wallace, Patricia: *Az internet pszichológiája* (ford. Krajcsi Attila). Budapest, Osiris, 2006.

White, Christopher – Thrall, A. Trevor – Mazanec, Brian M. (szerk.): *Information Warfare in the Age of Cyber Conflict.* New York, Routledge, 2021. https://doi.org/10.4324/9780429470509