Szenes Zoltán✧

A hibrid fenyegetések elleni szakpolitika Magyarországon

DOI 10.17047/HADTUD.2021.31.4.39

A hibrid hadviselés új típusú biztonsági kihívásként, kockázatként és fenyegetésként jelent meg az elmúlt évtizedben, amely egyre nagyobb szerepet kap a nemzeti és szövetségi biztonságpolitikák alakításában. A cikk a hibrid fenyegetések elleni nemzeti szakpolitika kialakulását és evolúciós fejlődését vizsgálja hazánkban. Stratégiai dokumentumok és jogszabályok értékelése alapján bizonyítja a védekezés kétlépcsős jellegét, amely a nemzetközi – elsősorban az Európai Unióval és a NATO-val való – együttműködésre és a nemzeti feltételrendszer fokozatos kiépítésére épül. Bemutatja a hibrid fenyegetések magyar felfogását, a szövetségi együttműködés hazai fejlődésre gyakorolt hatásait és eredményeit. A szakpolitika gyorsuló ütemben formálódott 2016 és 2021 között, amelyben a nem nevesített felek általi hibrid támadások tapasztalatai, az alkalmazott eszközök típusai, a hibrid tevékenység területei és a védekezési képességek építésének lehetőségei játszottak szerepet. A tanulmány részletesen értékeli a nemzetközi vonatkozásban is erősnek tekinthető kibervédelmi tevékenységet, ismerteti az állam és a társadalom ellenálló tevékenységének erősítését szolgáló terveket. Vizsgálja a nemzeti válságkezelés irányítási és vezetési alkalmasságát a hibrid támadások ellen, támogatja a külső és belső biztonság krízismenedzsmentjének integrációját célzó szakmai javaslatokat, mint olyan formát, amely legalkalmasabb lenne az összetett tömeges hibrid támadások hatékony kezelésére. Rámutat arra, hogy a hibrid támadási spektrumnak megfelelően tovább kell szélesíteni a védekezés lehetőségeit, a kibervédelemhez hasonlóan a többi területen is szisztematikus építkezésre van szükség. Az elemzés azzal a következtetéssel zárul, hogy ehhez szükség van egy nemzeti hibrid stratégia kidolgozására és elfogadására.

KULCSSZAVAK: hibrid fenyegetések, hibrid hadviselés, kibervédelem, ellenálló képesség, válságkezelés, hibrid stratégia

Governmental Policy against hybrid threats in Hungary

Hybrid warfare has emerged as a new type of security challanges, risks, and threats over the past decade that is playing an increasing role in shaping national, international, and allied security policies. The article examines the development and evolution of the national policy

✧ Nemzeti Közszolgálati Egyetem, Hadtudományi és Honvédtisztképző Kar – *University of Public Service, Faculty of Military Sciences and Officer Training;*
e-mail: szenes.zoltan@uni-nke.hu; https://orcid.org/0000-0003-1686-2273

against hybrid threats in Hungary. Based on the evaluation of strategic documents and legislation, it demonstrates the two-step nature of hybrid defence which is built on the international cooperation, primarily with the European Union and NATO, and the gradual development of the successful national protection system. It presents the Hungarian perception of hybrid threats, the effects and results of allied cooperation on national development. The policy evolved at an accelerating pace between 2016 and 2021 as the results of hybrid attacks experience by unnamed parties, types of tools used, domains of hybrid activities, and the opportunities to build defence capabilities. The study evaluates in detail the cyber defence which is considered to be strong in Hungary in the international comparison, and describes the plans to strengthen the resilience of the state and the society. It examines the national management and leadership arrangements against hybrid attacks and supports professional proposals to integrate the external and internal threat management subsystems as the most appropriate form to deal effectively with complex hybrid mass attacks. The article points out that there is a need to widen the protection to another hybrid attack domains similar to what was achieved in the area of cyber defence. The analysis concludes that this requires the development and adoption of a national hybrid strategy.

KEYWORDS: hybrid threats, hybrid warfare, cyber defence, resilience, crisis management, hybrid strategy

Bevezetés

A hibrid fenyegetések problémája jelentős figyelmet kapott a nemzetközi szakirodalomban az elmúlt évtizedben, még ha nincs is egységesen elfogadott definíciója a hibrid hadviselésnek. Abban viszont egyetértés van, hogy háborús küszöb alatti hadviselésről van szó, amikor a támadó hagyományos és nem hagyományos, állami és nem állami, katonai és nem katonai eszközöket használ fel koordinált módon, meghatározott célok elérése érdekében. A hibrid hadviselés során alkalmazott intézkedések köre igen széles lehet, a kritikus infrastruktúrák elleni támadásoktól az állam és a társadalom működéséhez szükséges stratégiai szolgáltatások (energiaellátás, pénzügyi rendszer működése stb.) zavarásán keresztül hírszerzési és dezinformációs kampányokig. Egy ország, társadalom vagy szövetségi rendszer demokratikus működésének sebezhetőségeit támadják, hogy aláássák a bizalmat a kormányzati vagy szövetségi intézmények tevékenysége iránt, akadályozzák a gyors és hatékony döntéshozatalt, gyengítsék az ország vagy szövetség működését. Bár a hibrid hadviselés az ukrajnai válsággal kapcsolatban kapott új értelmet, az amerikai és francia elnökválasztások, egyes balkáni országok választásaiba történő külső beavatkozás vagy a jelenlegi COVID-19-es globális járvány kezelése is rámutat a rendszerszintű sebezhetőségekre, amelyeket rosszindulatú szereplők hatékonyan kihasználhatnak.

A hibrid hadviselés nem tekinthető teljesen újnak, mégis az újfajta biztonsági fenyegetések között tartjuk számon a változékony és kontextus-adaptív jellege, a legújabb technológiák felhasználása, az igénybe vett eszközök és technikák integrált alkalmazása miatt. A hibrid hadviselés széles spektruma megnehezíti a hibrid fenyegetések elleni védekezést, mert a sebezhetőségek különböző formátumokba jelenhetnek meg: társadalmi polarizáció, állami és társadalmi működési zavarok, geostratégiai konfliktusok, kooperációs zavarok, eltérő jogszabályok, technológiai hátrányok vagy történelmi-ideológiai eltérések. A hibrid fenyegetések összetett jellege integrált megközelítést és kormányzati védekezést, összehangolt nemzetközi

együttműködést és multidiszciplináris megközelítést igényel. A 2016. júliusi varsói csúcstalálkozón aláírt EU–NATO együttes nyilatkozat hangsúlyozta, hogy a „hibrid fenyegetések elleni küzdelem közös kötelezettségvállalásokat igényel a reziliencia megerősítése, az elemzés, a megelőzés és a korai felismerés terén, időben történő információ-megosztást feltételez, különösen a hírszerzési információk megosztása vonatkozásában, valamint szoros együttműködést követel a stratégiai kommunikáció és reagálás terén."[1] Ebből a követelményből kiindulva 2021 elején egy V4-es kutatás indult,[2] amely azt a célt tűzte ki, hogy megvizsgálja a hibrid fenyegetések elleni küzdelem helyzetét a visegrádi országokban, feltérképezze a tagállami hibrid szakpolitikák kialakulásának és fejlődésének általános és specifikus jellemzőit, és olyan javaslatokat dolgozzon ki, amely javítja a tagországi és a közös fellépés szervezettségét és hatékonyságát. Jelen tanulmány e kutatás keretében készült,[3] amely az európai hibrid kutatásokkal foglalkozó kiválósági központ elemzési keretét[4] használta. A koncepcionális modell a szereplők, az eszközök, az alkalmazási területek és a tevékenységi fázisok vizsgálatát tartja fontosnak.

A szakpolitika kialakulása és evolúciós fejlődése

Magyarországon a hibrid hadviselés problémája – a többi V4 országhoz hasonlóan – csak lassan tudatosult a kormányzati politikában és a közvéleményben.[5] A tanulási folyamatban nagy szerepet játszott a NATO és az EU, amely 2016-tól már koordináltan veszi fel a harcot az orosz hibrid hadviselés ellen. Az alkalmazkodási politika azonban nemcsak lassan, de szegmentáltan is zajlott, a katonai fenyegetés mellett talán a kiberfenyegetések felismerése volt a leggyorsabb. Ezért az adaptáció *első szakaszában* a Belügyminisztérium (nemzetbiztonság, kibervédelem) és a Honvédelmi Minisztérium (katonai kibererők és a különleges műveleti erők fejlesztése) viselte *az elsődleges felelősséget* a védekezésben. A későbbi tapasztalatok azonban folyamatosan bővítették a hibrid fenyegetések eszköztárát (politikai, diplomáciai, médiapolitika, gazdasági-kereskedelmi, technológiai), a fenyegetések elleni védelembe pedig behoztak olyan területeket is, mint az információvédelem, stratégiai kommunikáció, vegyi támadások elleni fellépés, ellenséges hírszerzés elleni tevékenység, migráció

1 EU–NATO Joint Declaration 2016.

2 A kutatásban a cseh Nemzetvédelmi Egyetem (Brno), a lengyel Védelmi Tanulmányok Egyetem (Varsó), a szlovák Stratégiai Politikai Intézet (Pozsony) és a Nemzeti Közszolgálati Egyetem (Budapest) szakértői vettek részt.

3 A szerző a tanulmány megírásában nyújtott segítségéért köszönetét fejezi ki: Kovács József nemzeti információs államtitkárnak (Miniszterelnöki Kormányiroda), Kádár Pál vezető kormányfőtanácsadónak (Miniszterelnöki Kormányiroda), Németh Gergely védelempolitikáért felelős helyettes államtitkárnak (Honvédelmi Minisztérium), Marosfi Gábor hibrid koordinátornak (Külgazdasági és Külügyminisztérium), Keczer Judit szakértőnek (HM), Kiss Máté szakértőnek (Terrorelhárítási Információs és Bűnügyi Elemző Központ) és Jójárt Krisztián doktorandusznak (NKE Hadtudományi Doktori Iskola).

4 Giannopoulos, Smith, Theocharidou 2021, 12–42.

5 2021. december 19-én a magyar internet oldalon összesen 11 800 hibrid hadviseléssel kapcsolatos hír volt, amely a problémakört nemzetközi és magyar szempontból egyaránt tárgyalja. A téma növekvő aktualitását mutatja, hogy a hírek száma 2021-ben megháromszorozódott. hibrid hadviselés - Search (bing.com) (Letöltés ideje: 2021. 12. 19.)

vagy az ellenálló képesség. A hibrid fenyegetések komolyságát mutatta, hogy 2016 áprilisában az Európai Bizottság és a kül- és biztonságpolitikai főképviselő közös közleményben[6] fogalmazta meg a hibrid fenyegetések elleni fellépés keretrendszerét és feladatait. Ebben a Bizottság négy célt és fogalmazott meg: 1) együttműködési mechanizmusok kialakítása az EU és a tagállamok között a fenyegetések tudatos kezelésére, 2) a stratégiai és kritikus szektorok ellenálló képességének kiépítése, 3) közös fellépés, válaszadás és helyreállítás lehetőségeinek megteremtése, valamint 4) együttműködés a NATO-val[7] és más partner nemzetközi szervezetekkel. A közös állásfoglalást az Európai Parlament és Tanács is jóváhagyta,[8] sőt 2016 júliusában már az EU és a NATO közös együttműködési megállapodást írt alá a varsói NATO-csúcstalálkozón.[9]

Jól lehet jellemezni e korszak kormányzati gondolkodását az akkoriban megjelent politikai nyilatkozatok, kormányzati döntések és jogszabályok alapján. Különösen érdekes ebből a szempontból Simicskó István volt honvédelmi miniszter[10] hibrid hadviseléssel kapcsolatos tanulmánya, amelyet akár az akkori magyar kormány álláspontjának is tekinthetünk. Véleménye szerint Magyarország elsősorban a szövetségi rendszerben betöltött szerepe révén válhat egy komplex hibrid fenyegetés célpontjává, amire elsősorban az ehhez szükséges képességekkel rendelkező autoriter nagyhatalmak képesek. Az ország elleni egyes hibrid támadások (például kibertámadások) elleni védekezés (megelőzés, beazonosítás és kezelése) elsődlegesen nemzeti feladat. Mivel a szövetségi doktrínák szerint is elsőként mindig a hibrid művelet által fenyegetett vagy megtámadott tagállamnak kell reagálnia, a nemzetközi közösségnek készen kell állnia felkérés esetén a segítségnyújtásra. A hibrid fenyegetések komplexitása miatt a politikus (ma a Kereszténydemokrata Néppárt parlamenti frakcióvezetője) összkormányzati együttműködést, a társadalom felkészítését és egy integrált védelmi igazgatási rendszerben történő kezelését szorgalmazta. A hibrid háború a „kemény" és „puha" erők koordinált használatára utal, amelynek hatása, politikai, gazdasági és társadalmi következményei akár katasztrofálisak is lehetnek a megtámadott országban. Ezért minden országnak, így Magyarországnak is erősíteni kell biztonságát, amely már elkezdődött.

A magyar politikai alkalmazkodás *második szakaszát 2019-től számíthatjuk*, amikor is a kormány erősítette az összkormányzati szerepvállalást, és törvénymódosításokkal kívánta javítani a hibrid fenyegetésekkel szembeni ellenálló képességet és védelmet.[11] A törvénycsomag keretében a magyar kormány módosította a nemzetbiztonsági törvényt, a honvédelmi törvényt, a katasztrófavédelem elleni törvényt, illetve

6 Security: EU strengthens response to hybrid threats. Press Release, 2016. Brussels. A dokumentum 22 feladatot fogalmaz meg a hibrid fenyegetésekkel szemben, amelyekhez az EU Hibrid Fúziós Részleg (Brüsszel) és az Hibrid Fenyegetések Elleni Kiválósági Központ (Helsinki) megalakítása, a kritikus infrastruktúra (energia, közlekedési és ellátó rendszerek) védelme, a hibrid hadviselés elleni katonai képességek fejlesztése, az egészségügyi és élelmiszer- ellátás, a pénzügyi biztonság, a szélsőséges szervezetek elleni fellépés és a környező régiók hibrid fenyegetésének elemzése tartozik.

7 Joint EU–NATO Declaration 2018.

8 Joint Communication 2016.

9 Joint EU–NATO Declaration 2018.

10 Simicskó 2017, 13–14.

11 2019. évi CV. törvény.

a létfontosságú rendszerek és létesítmények azonosításáról és védelméről szóló törvényt. Különösen fontosnak értékelhetők a *kritikus infrastruktúra védelmével* kapcsolatos megerősített intézkedések, amelyek a gazdasági és szociális közszolgáltatások biztosítását, az egészségügy működését, a lakosság személyi és vagyonbiztonságát, valamint a honvédelmi feladatok ellátását célozták. Kormányzati hatáskör lett a katonai kibertér-műveleti erők védelmi, támadás-megelőzési és nemzetközi műveletekkel kapcsolatos szabályozása és a kivételes döntéshozatal kereteinek kialakítása is. Bár azóta az EU-ban és a NATO-ban is egyre erőteljesebb *közös tevékenység* folyik az orosz vagy az utóbbi időben már a kínai befolyásszerzés ellen, Magyarország folytatja a nemzeti érdekeken alapuló globális nyitás külpolitikáját, amely nem mindig esik egybe az EU vagy a NATO többségi véleményével. Ráadásul a hibrid hadviselést tekintve a szövetségi politikák[12] is *elsődleges válaszadóknak* a tagállamokat tekintik, komoly felelősséget és mozgásteret adnak az egyes hibrid kockázatok, veszélyek és fenyegetések nemzeti megítéléséhez és kezeléséhez. A nemzetek pedig a hibrid fenyegetés problémáját az Oroszországgal vagy Kínával kapcsolatos kétoldalú kapcsolatok, gazdasági érdekek, külpolitikai stratégiák és más nemzeti szempontok alapján ítélik meg. A magyar kormány például a 2020. évi nemzeti biztonsági stratégiában (NBS) úgy fogalmaz, hogy: „Magyarország – miközben prioritásnak tartja a NATO és az EU kohéziójának megőrzését – érdekelt a magyar–orosz kapcsolatok és gazdasági együttműködés pragmatikus fejlesztésében."[13] Hasonlóképpen a dokumentum a hasznosságon alapuló intenzív kapcsolatokat szorgalmazza Kínával kapcsolatban is, bár hangsúlyozza, hogy a gazdasági együttműködés lehetőségeinek kiaknázása során tekintettel kell lenni biztonsági tényezőkre is.[14] Komoly előrelépés tehát a hibrid fenyegetésekkel szemben szövetségi szinten csak akkor érhető el, ha a tagállamok egységes politika alapján és közösen lépnek fel a beavatkozási fenyegetések ellen.

A hibrid hadviselés elleni fellépés *harmadik szakasza* 2020 végén kezdődött, amikor a magyar Országgyűlés módosította az Alaptörvényt,[15] majd 2021-ben elfogadta a *védelmi és biztonsági tevékenységek összehangolásáról* szóló törvényt (Vbö).[16] Ehhez a szabályozási folyamathoz tartozik a hibrid hadviselés elleni küzdelmet megerősítő új Nemzeti Katonai Stratégia (NKS) megjelenése is 2021 júniusában.[17] A „karácsonyi" alaptörvény-módosítás megreformálja a jelenleg érvényes honvédelmi alkotmányos rendet, és a jelenlegi hat (rendkívüli állapot, szükségállapot, veszélyhelyzet, váratlan támadás, megelőző védelmi helyzet, terrorveszélyhelyzet) különleges jogrendi tényállás helyett hármat *(hadiállapot, szükségállapot, veszélyhelyzet)* vezet be 2023. július 1-jével. A végrehajtást sarkalatos törvények, illetve kormányrendeletek fogják szabályozni,

12 A Europe that protects: Countering hybrid threats 2018, NATO's Response to hybrid threats 2018. A NATO a 2018. júliusi brüsszeli csúcson elfogadta a Kibervédelmi Tervet (Cyber Defence Pledge).

13 Magyarország Nemzeti Biztonsági Stratégiája. Biztonságos Magyarország egy változékony világban, 118. pont.

14 Uo. 119. pont

15 Magyarország Alaptörvényének kilencedik módosítása 2020.

16 2021. évi XCIII. törvény.

17 1393/2021. (VI.24.) Korm. határozat.

de már most látható, hogy az alaptörvény-módosítás megerősíti a kormány hatáskörét, egy korszerűbb, a változó biztonsági környezethez jobban alkalmazkodó válságkezelési rendszer kialakítására ad lehetőséget. A jogszabályi változások igyekeznek a normál jogrendi válságkezelés eszköztárát szélesíteni és erősíteni, bár elképzelhető, hogy bizonyos bevált elemek a jelenlegi különleges jogrendi szabályozásból (mint például Franciaországban) átkerülnek a békeidőszaki védelmi tevékenységbe. *Arra kell ugyanis felkészülni, hogy a hibrid fenyegetéseket alapvetően és döntően a normál jogrendben kell kezelni.*

A reformfolyamat első lépését jelenti az új törvény, amely a védelmi és biztonsági tevékenységek összehangolásával a biztonsági ágazatokon átívelő, integrált, széles értelemben vett honvédelmi igazgatási rendszert céloz meg az állami és nem állami szereplők közötti együttműködés előírásával. A törvény megteremti az összkormányzati működés jogi kereteit, a katonai, rendvédelmi és nemzetbiztonsági szervek kooperációját kombinálja a tág értelemben vett közigazgatással és civil társadalommal való együttműködéssel. Az átfogó megközelítés lehetővé teszi Magyarország jobb alkalmazkodását a változó nemzetközi és hazai biztonsági környezethez, hozzájárul a nemzeti ellenálló képesség fejlesztéséhez. A hibrid tevékenységek kezelésére is alkalmas új törvény további jogalkotási feladatokat irányoz elő, amely segítségével *az elkövetkező két évben teljesen megújulhat* az ország biztonságának és védelmének intézményes rendszere és szabályozása. Ebbe a jogalkotási reformfolyamatba jól illeszkedik az új Nemzeti Katonai Stratégia, amely – többek között – részletesen szabályozza a fegyveres erő hibrid tevékenységek elleni katonai feladatait.

A hibrid hadviselés elleni védekezés *magyarországi evolúciós fejlődése jól felismerhető a témakör szakirodalmi elemzése* kapcsán is. Az első tudományos közlemények és konferenciák még komplex fenyegetésekről, azon belül is elsősorban a katonai dimenzióról, az aszimmetrikus hadviselésről szóltak a külföldi szakirodalom feldolgozása alapján.[18] Az orosz hibrid hadviselés elemzése 2014 után gyorsan megjelent a magyar szakirodalomban, amely a nemzetközi biztonsági környezet háború formáira gyakorolt hatásaitól kezdve[19] az ukrajnai tapasztalatok feldolgozásán át[20] a hibrid hadviselés hadelméleti kérdéseinek vizsgálatáig terjedt.[21] A tisztán katonai elemzéseket fokozatosan kiegészítette a nemzetbiztonsági szolgálatok tevékenységének vizsgálata a dezinformációk elleni harcban.[22] Bár egyre inkább előtérbe kerültek a létfontosságú infrastruktúrák védelmével vagy a társadalom ellenálló képességének növelésével foglalkozó értékelések,[23] átfogó hibrid témakörökkel foglalkozó tanácskozások és publikációk csak 2019-től jelentek meg a magyar tudományos közéletben.[24] Fájdalmasan hiányoznak viszont Magyarország hibrid fenyegetettségével, illetve a hibrid támadások elleni tevékenységével kapcsolatos leírások, a kormányzati tevékenység bemutatása, egyes

18 Resperger, Kiss, Somkúti 2013.
19 Szenes 2018.
20 Rácz 2014; Jójárt 2019.
21 Porkoláb 2015.
22 Resperger 2018; Hódos 2020.
23 Kovács 2018.
24 Kádár 2020; Somodi, Kiss 2019.

hibrid tevékenységi formák országspecifikus elemzése.[25] Viszont az elmúlt időszakban – részben a Covid-19 pandémiának köszönhetően – felerősödtek azok a kutatások, amelyek az államszervezet működésének stabilitását és folyamatosságát vizsgálják,[26] vagy a honvédelmi alkotmányosság megújítását szorgalmazzák.[27] Szükség van egy erős kormányzatra, védelmi igazgatási rendszerre, amely veszélyhelyzetben képes gyorsan rendkívüli döntéseket hozni, intézkedéseket tenni, működtetni azokat az állami szerveket, erőforrásokat, amelyek az ország és a lakosság védelme érdekében szükségesek. Ezek a tapasztalatok már jól hasznosíthatók a hibrid hadviselés elleni összkormányzati tevékenységben is.

A hibrid fenyegetés hazai felfogása és a kétlépcsős védekezési stratégia

Magyarország hibrid fenyegetések elleni szakpolitikája kiolvasható a 2020. évi Nemzeti Biztonsági Stratégiából (NBS), amely *bemutatja a kormány hibrid-felfogását,* azonosítja a hibrid fenyegetéseket, és lerakja a kétlépcsős (nemzeti és szövetségi) védekezés alapjait.[28] Magyar értelmezés szerint hibrid hadviselésről akkor beszélhetünk, ha a háborús küszöb alatti tevékenységek *alkalmasak lehetnek* az ország destabilizálására, a kormányzat cselekvőképességének gyengítésére, a politikai stabilitás és a társadalmi egység megbontására, valamint a nemzetközi érdekérvényesítő képesség korlátozására. A hibrid hadviselés során a támadó/ártó fél arra törekszik, hogy egy meghatározott cél érdekében *nehézségeket és károkat okozzon Magyarországnak, válsághelyzeteket alakítson ki, csökkentse a működő- és érdekérvényesítő képességét.* Az egyes elemek (támadó intézkedések) külön-külön vagy egymást erősítő hatású alkalmazása – a hagyományosnak tekinthető katonai támadási formák nélkül is – alkalmas lehet a befolyásolásra, a zavarkeltésre, a belső rend megbontására, a közvélemény hangulatának formálására. A hibridfenyegetés-felfogást az NBS kiemelt kockázatokkal foglalkozó VII. fejezete rögzíti, amely ide sorolja az összehangolt és széleskörű 1) diplomáciai tevékenységet, 2) az információs és titkosszolgálati műveleteket, 3) a pénzügyi- gazdasági nyomásgyakorlást, 4) a pénzügyi spekulációs támadásokat, valamint 5) az ezekkel párosult katonai fenyegetéseket. A 2021. évi Nemzeti Katonai Stratégia (NKS) *tovább specifikálja* ezt a hibrid-percepciót, amikor már 1) a belföldi és a nemzetközi közvélemény aktív és tudatos befolyásolásáról, 2) az információs csatornák és közösségi médiaplatformok manipulálásáról, 3) a társadalmi, politikai és gazdasági instabilitás gerjesztéséről, 4) a válságok kihasználásáról, valamint 5) a befolyásolási és nyomásgyakorlási eszközként használt katonai és gazdasági-pénzügyi segítségnyújtásról beszél.[29] Mindkét stratégia aláhúzza, hogy ebben az új típusú, „szürke zónás" küzdelemben[30] hangsúlyosabbá vált

25 A Honvéd Tudományos Kutatóhely például 2021. november 17–18-án rendezett hibrid hadviselési konferenciát „Katonák és a hibrid hadviselés: a fegyveres erők szerepe és feladatai a háborús küszöb alatti konfliktusokban" címmel. Azonban a prezentációk többségében itt is a nemzetközi tapasztalatokról szóltak. Honvéd Tudományos Kutatóhely (mil.hu) (Letöltés ideje: 2021. 12. 23.)

26 Kádár 2021, 5; Petruska, Till, Balogh 2021, 87–109.

27 Till 2021.

28 Bak, Németh, Szőke 2020, 14.

29 NKS, 2021. 5071–5072.

30 Hoffmann 2018.

a fedett műveletek végrehajtása, helyettesítő (proxy) erők alkalmazása, rejtett állami támogatással és irányítással működő bűnözői és terrorista csoportok tevékenysége, valamint nem-kormányzati szervezeteknek álcázott kormányzati szereplők felhasználása. Az alkalmazó e tevékenységsorozat közben a modern technológiák által nyújtott kifinomult lehetőségeket is felhasználja, tevékenységét, hibrid műveleteit kiterjeszti a gazdaságra, a médiára, a kibertérre és a közvélemény manipulálására. Az NBS V. fejezete (68. pont) 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."

Mindkét stratégia hangsúlyozza *az ellenséges hírszerzési tevékenységgel szembeni ellenálló képesség erősítését*, a tagállamok egymás közötti, illetve a tagállamok és a nemzetközi szervezetek közötti koordinációt, különösen a NATO-val, illetve az EU-val. Magyarország esetében kiemelt jelentősége van a *nemzetközi együttműködésnek*, mert korlátozott erőforrásokkal rendelkező országként megsokszorozhatja saját lehetőségeit. Ahogy az NBS megfogalmazza: *„Érdekünk a hibrid hadviselés elleni nemzeti, és elsősorban az EU és NATO kereteiben, a többnemzeti válaszadási képesség fejlesztése."* (NBS 100. pont). Az új NKS egy egész fejezetrészt szentelt a nemzetközi együttműködési képesség erősítésének (NKS 4.4.). Ezért is csatlakozott Magyarország 2019-ben a Hibrid Fenyegetések Elleni Európai Kiválósági Központhoz (Hybrid CoE), mert a Helsinkiben működő központ feladata, hogy segítse a stratégiai együttműködést a partner nemzetekkel, elemzéseket készítsen a hibrid fenyegetésekről, illetve kutatásokat végezzen. A Hibrid Kiválósági Központ évente határozza meg a fókuszterületeket és a támogató munkafolyamatokat. Az utóbbi időszakban a Központ a hibrid fenyegetések elleni tudatos küzdelemre (most például a tengeri hibrid fenyegetések témakörét vizsgálják), a vegyi, biológiai, radiológiai és nukleáris fenyegetésekkel való fellépésre, egységes stratégiai kommunikációra, az ellenséges hírszerzés elleni elhárításra, a kiberbiztonság és az ellenálló képesség erősítésére fókuszál. Magyarországot a Honvédelmi Minisztérium (HM) képviseli az intézmény Irányító Testületében, amely évente minimum kétszer ülésezik.[31] A többnemzeti válaszadási képességhez sorolható a NATO déli információs központjához (NSD-S Hub) történő magyar csatlakozás is, amely a nápolyi parancsnokságon állt fel 2017 őszén azzal a feladattal, hogy összekapcsolja a szövetségeseket, a partnereket és a régióval foglalkozó szakértőket a dél felől érkező biztonsági kihívások jobb megismerése és leküzdése érdekében. NATO-megközelítésben a déli régióhoz tartozik a tágabb Közel-Kelet, Észak-Afrika, Száhel-övezet és a szubszaharai Afrika. A központ rendeltetését a 3C (Connect, Consult, Coordination) jelmondat fejezi ki: a Hub célja, hogy hozzájáruljon a NATO

31 1586/2019. (X.16.) Korm. határozat.

tevékenységeinek összehangolásához, szinkronizálásához és a konfliktusmegoldáshoz a déli szárnyon, miközben átfogó megközelítéssel optimalizálja az erőforrásokat és maximalizálja a hatékonyságot. Magyarország védelmi és külügyi szakértők delegálásával vesz részt ebben a tevékenységben. Ezenkívül az ország aktív szereplője az EU és a NATO hibrid tevékenység ellen kialakított együttműködési rendszerének.

A feladatok megvalósítását azonban nehezíti, hogy a *nemzeti biztonsági stratégia nem nevesít egyetlen országot sem,* amely fenyegetheti Magyarországot. Ugyanakkor indirekten felismerhetők ezek az államok, hiszen például amikor a stratégia a tömeges, ellenőrizetlen és illegális migrációt a hibrid hadviselés lehetséges eszközének nevezi (NBS 56. 57. 62.65. 67. pont), következtetni lehet azokra az államokra, amelyek alkalmazhatják ezt az eszközt nyomásgyakorlásra (például Törökország, Oroszország a líbiai és szíriai jelenléten keresztül). Vagy amikor a technológiai szint rohamos fejlődése (digitalizáció, 5G vezeték nélküli hálózat, űrtechnológia stb.) miatt új „lehetőségekről és kihívásokról" beszél a dokumentum, akkor szintén könnyű beazonosítani például Kínát.

Ezeket a felismeréseket bizonyítja egy 2020-es – NATO által szponzorált – biztonsági percepciókutatás is, amelyet a magyar ICDT (*International Center for Development and Democratic Transition*, Budapest) és a szlovák Bakamo Média Kutató cég végzett a V4 országok közösségi médiáiban.[32] A vizsgálat négy biztonsági területen (nagyhatalmi politika, dezinformáció és kiberbiztonság, korrupció, egészségügy) és három szinten (nemzeti, közösségi és egyéni) vizsgálta különböző médiahírszerzési módszerekkel, hogyan gondolkodik a négy ország lakossága. Az elemzés magyar vonatkozásban meglepő módon Oroszország mellett az Egyesült Államokat is kihozta veszélyforrásként, mivel mindkét nagyhatalomnak egyaránt célja a régió feletti ellenőrzés megszerzése. A két ország politikájának és tevékenységének ellentmondásos megítélése (szövetséges, vetélytárs) aggodalmat kelt az emberek körében. Emellett általános a vélekedés arról, hogy nemcsak Oroszország és Kína, hanem az Egyesült Államok is folytat információszerzést az országban, különböző módon (például cégek, kulturális intézmények) leplezve hírszerzési tevékenységét. A külföldi katonai erők (például az amerikai csapatok) állomásoztatása az ország területén szintén aggodalmat kelt a lakosság körében, mivel növelheti a katonai konfliktus kockázatait. A belpolitikai megosztottság miatt a kormány és az ellenzék egymást vádolja az ország külföldi érdekeknek való kiárusításában. Ebben nagy szerepe van a kormány Soros-ellenes állandó propaganda-kampányának, amely támadja az ellenzéki liberális médiát és a civil szervezeteket. A gender-kérdés, a migráció megítélése, a liberális értékek elfogadása/ellenzése szintén megosztja a magyar társadalmat. Mások attól tartanak, hogy Kína a TikTok és a Huawei eszközökön keresztül lopja el személyes adatokat. A helyzet javítására a kutatás a *reziliencia erősítését* javasolja nemzeti, csoport és egyéni szinten is. Fontosnak tartja a nemzeti büszkeség és a bizalom erősítését az állami szervek és a szövetség felé egyaránt, amit a nemzeti hozzájárulások fontosságának hangsúlyozásával, az „erős ország – erős szövetség" összefüggés bemutatásával lehet elérni.

32 Report of the ICDT and Bakamo 2021.

Kibervédelem és az ellenálló képesség növelése

A hibrid fenyegetések elleni fellépés *elsőként a nemzeti kibervédelmi rendszer kiépítésével kezdődött*, amelynek fejlesztése végighúzódott az első két fejlődési szakaszon. A nemzeti biztonsági stratégia a legnagyobb veszélynek a kibertámadásokat tartja, amelyek jelentős károkat okozhatnak a kormányzati informatikai rendszerekben, az e-közigazgatásban, a közműszolgáltatók, a stratégiai vállalatok, a létfontosságú infrastruktúra és a társadalom működésében. A kibervédelem fontossága már a korábbi, a 2012. évi nemzeti biztonsági stratégiában is szerepelt, de csak a második évtized közepére sikerült a nemzetközi követelményeknek megfelelő kibervédelmi rendszert kiépíteni. Ilyen értelemben a kibervédelem fejlesztése a hibrid fenyegetések elleni védekezés *első sikeres programjának* tekinthető, amely mintaként szolgálhat más fontos védelmi tevékenységek, mint például az állami és társadalmi reziliencia erősítésében. Az ország kibervédelmi rendszerének kiépítése egyfajta tesztje volt a mai hibrid tevékenységek elleni szakpolitika megfogalmazásának, amely hangsúlyozza a *védelem össznemzeti jellegét, a koordinált kormányzati munka fontosságát, a védekezés ellenálló képesség növelésére irányuló szándékát, valamint a nemzetközi szervezetekkel és szereplőkkel való együttműködés fontosságát.* A kiberfenyegetések már a 2014. évi paradigmatikus biztonsági változások (Oroszország Ukrajna elleni agressziója, az Iszlám Állam feltámadása, migrációs válság Európában) előtt megjelentek (vízválasztónak a 2007. évi összehangolt kibertámadás tekinthető Észtország ellen), az infokommunikációs eszközök és szolgáltatások fejlődésével párhuzamosan szinte mindennaposokká váltak az állami és civil szektort érő támadások. A kormány kiberterületen megtapasztalta a kétlépcsős stratégia előnyeit, hiszen a szövetséges nemzetközi szervezetek ajánlásokat, megvalósítási stratégiákat dolgoztak ki, normakereteket javasoltak annak érdekében, hogy a nemzetállamok kialakíthassák egyéni kibervédelmi stratégiáikat, biztonsági rendszereiket. Magyarország sokat profitált a NATO Kooperatív Kibervédelmi Kiválósági Központja (CCDCOE), az EU Kiberbiztonsági Ügynöksége (ENISA) és az ENSZ Nemzetközi Távközlési Egyesület (ITU) támogató tevékenységéből.

Az EU és a NATO szakpolitikai fejlődése közvetlen hatást gyakorolt a magyarországi fejleményekre: a 2013. évi EU kiberbiztonsági stratégiája után közvetlenül megszületett a magyar kibervédelmi stratégia.[33] Ugyancsak 2013-ban az Országgyűlés megalkotta az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényt (Ibvt),[34] melynek segítségével 2015-re *központosították a korábbi széttagolt intézményi rendszert,* és a Nemzetbiztonsági Szakszolgálat alárendeltségében létrejött a *Nemzeti Kibervédelmi Intézet* (NKI). Az intézeten belül működik a Nemzeti Elektronikus Információbiztonsági Hatóság, a Kormányzati Eseménykezelő Központ (Gov-CERT), valamint a Biztonságirányítási és Sérülékenységi Igazgatóság. Az intézet hatásköre és feladatai folyamatosan erősödtek: nemzeti kapcsolattartó pont (SPOC) az EU felé, nemrégen átvette a létfontosságú infrastruktúrák infokommunikációs rendszereinek védelmét is. A NKI-n kívül még a honvédelem területen, illetve a kiberbűnözésért felelős rendvédelmi szervezetnél működik külön

33 1139/2013. (III.21.) Korm. határozat.

34 2013. évi L. törvény.

kibervédelmi szervezet, de ide sorolhatók a civil szférát védő intézmények is. A Zrínyi Honvédelmi és Haderőfejlesztési Program részeként komoly fejlesztés zajlik a Magyar Honvédségben (MH), kiépítés alatt van az MH Kiber- és Információs Műveleti Központ. Ezért az Ibvt arra is intézkedett, hogy létre kell hozni egy szakpolitikát formáló és koordináló szervet, amely a *Nemzeti Kiberbiztonsági Koordinációs Tanács* nevet kapta. Az egyévtizedes erőfeszítések eredményeképpen ma Magyarország a 2020. évi globális kiberbiztonsági indexen (GCI) az erős kibervédelemmel rendelkező országcsoportba tartozik, a 35. helyre kapott besorolást, Európában pedig a 22. helyet foglalja el.[35] A kibervédelem jó szervezettsége viszonylag könnyen lehetővé teszi a rendszer változó NATO (a kollektív védelem cikke /5. cikk/ a kibertámadásokra is kiterjeszthető, a kibertér hadszíntérré vált) és EU (például a hálózat- és információbiztonsági irányelv) követelményekhez való alkalmazkodást.

A kibervédelmi rendszer kiépítése után a magyar kormány az *ország ellenálló képességének erősítését* tűzte ki célul, amely a COVID–19 járványhelyzet során tapasztalt kapacitáshiányok, a nemzetközi együttműködés problémái, a saját erőkre és eszközökre történő támaszkodás nehézségei alapján egyaránt nélkülözhetetlenné vált. A reziliencia „izmosítását" a nemzeti biztonsági és katonai stratégia egyaránt szorgalmazza. Az NBS szerint „a tömegpusztító fegyverek, a terrorizmus, a kibertámadások, a hibrid műveletek és a katasztrófák elleni védelem egyaránt megköveteli hazánk nemzeti ellenálló képességének fokozását." (NBS 175. pont.) Ennek érdekében fejleszteni kell a polgári védelmi infrastruktúrát, a védelmi közigazgatás összkormányzati rendszerét (NBS 30. pont). Az NKS önálló fejezetrészt (NKS 4.3.) szán a reziliencia kérdéseinek, rámutat az ellenálló képesség és az elrettentés közötti összefüggésekre, hangsúlyozza a civil felkészültség fontosságát, különösen a védelmi ipari kapacitások kiépítését. Fontosnak tartja a szövetséges erők befogadó nemzeti támogatása feltételeinek javítását, valamint nélkülözhetetlennek nevezi a polgári hatóságok tevékenységének katonai támogatását a legkülönfélébb veszélyhelyzetekben.

A nemzeti ellenálló képességet a 2021. évi XCIII., a védelmi és biztonsági tevékenységek összehangolásáról szóló törvény (Vbö) úgy definiálja (5.§. 7. pont), mint a nemzetet alkotó *lakosság, gazdaság és állam képességét* a veszélyek és fenyegetések előrejelzésére, megelőzésére, a kockázatok csökkentésére, illetve a következmények kezelésére, a helyreállítás feladatainak megoldására. A jogszabály ide sorolja a külső és belső biztonság fenntartásának feladatait, az állam honvédelmi és nemzetbiztonsági érdekeinek fenntartását, az ország stabilitását sértő vagy veszélyeztető törekvéseket, támadásokat, természeti vagy ipari katasztrófákat, járványokat. Kiemelten fontosnak tartja a biztonság-tudatosság erősítését, a hatékony helyreállítást szolgáló polgári és katonai képességek fenntartását, illetve a szükséges védelmi intézkedések meghozatalát. A törvény *egy teljes fejezetben* (V. fejezet) foglalkozik a nemzeti ellenálló képesség témakörével, hangsúlyozza a társadalom felkészültségének fontosságát,

35 Global Cybersecurity Index 2021. 24–30. Az index 20 indikátort vizsgál jogi, technikai, szervezeti, képességfejlesztési és együttműködési területeken. A V4 országok közül legjobb helyezést Lengyelország (a globális lista 30., az európai lajstromon 18. hely) ért el, Szlovákia mindkét ranglistán közvetlenül előttünk van (34., illetve 21.), Csehország pedig csoport utolsó (68., illetve 35. helyezés).

a szabályozás, a vezetés és irányítás egyértelműségét, továbbá az állami közigazgatási rendszer folyamatos működését. Aláhúzza a nemzeti biztonsági stratégiában kifejtett kétlépcsős stratégia fontosságát, miszerint a *szövetségesi kötelezettségekre tekintettel kell a nemzeti ellenálló képességet erősíteni. A* törvény szerint a nemzeti reagáló képességet az alábbi területeken kell biztosítani (42.§. 2. bek.): a) az Alaptörvényben meghatározott állami működés, a kormányzás és az alapvető fontosságú kormányzati szolgáltatások folytonosságának biztosítása, b) rugalmas és a kihívásokhoz alkalmazkodó energetikai rendszer és energiabiztonsági megoldások kialakítása, c) az ellenőrizetlen, tömeges személyi mozgások hatékony kezelésére való képesség, d) a rugalmas és a kihívásokhoz alkalmazkodó, az alapvető élet- és egészségügyi feltételek fenntartását szolgáló rendszerek fenntartása, a társadalom alapvető szükségletei ellátásában nélkülözhetetlen létfontosságú rendszerek működésének biztosítása, e) a tömeges méretű személyi sérüléssel fenyegető események kezelésére való képesség, f) a rugalmas és a kihívásokhoz alkalmazkodó infokommunikációs rendszer és közlekedési rendszer kialakítása és működtetése, valamint g) a védelmi és biztonsági feladatokban részt vevő szervek személyi állományának magas fokú szakmai felkészültsége, elhivatottsága. Nem nehéz ebben a feladatrendszerben a NATO és EU követelményeket felismerni.

A törvény előkészítésével párhuzamosan és azzal összhangban a kormány összeállította *Magyarország Helyreállítási és Ellenálló Képességének Tervét,* amit 2021 májusában benyújtott az Európai Bizottságnak.[36] A terv mintegy 7 milliárd euró uniós hitelt tervez fordítani stratégiai fejlesztési célokra. A tervezett összegből az egészségügy 34%-al, a környezetbarát közlekedés 25%-al, az oktatás és képzés fejlesztése 20%-al részesedik. A többi forrás a fenntartható fejlesztésre, a legelmaradottabb települések felzárkóztatására, valamint környezetvédelmi kezdeményezésekre jut. A kormány egyelőre nem tervezi az EU által biztosított teljes hitelkeretet felvenni, erre 2023-ig van lehetőség. A terv összeállítása során mintegy 500 szervezettel konzultáltak, önkormányzati szövetségekkel, településekkel, gazdasági, szociális és társadalmi érdekképviseletekkel egyeztettek.

Bár a nemzeti reziliencia programjának részletes kidolgozása *az elkövetkező időszak feladata,* néhány területen azonban, mint például az információvédelem, már korábban is történtek kormányzati lépések. E tekintetben különösen fontos volt *az elektronikus információbiztonságról szóló törvény* elfogadása 2013-ban, amely a nemzeti elektronikus adatvagyon, az információs rendszerek, valamint létfontosságú rendszerelemek biztonságát célozta. Ez a követelmény különösen 2014 után értékelődött fel, amikor az orosz információs hadviselés része lett a hibrid hadviselésnek. A tett intézkedések következtében Magyarország információs védelme az orosz befolyásszerzés ellen – ahogyan ezt a 2018. évi *Dezinformációs Reziliencia Index* (DRI) mutatja[37] – javult ugyan, azonban a rejtett dezinformációs források felfedése, illetve ellensúlyozása további

36 Benyújtotta a kormány az uniós helyreállítási alap igénybevételére kidolgozott magyar tervet. (kormany.hu) (Letöltés: 2021. 07. 17.)

37 Yelisejev, Damard 2018, 157–170. Az index három területen méri az orosz befolyást: a) a lakosság kitettsége a Kreml irányítása alatt álló médiának, b) a szisztematikus kormányzati válaszadás képessége, c) digitális hadviselésből fakadó sebezhetőség szintje. Mindegyik mutató 4-6 paraméter alapján,

kihívásokat jelent. Magyarországnak tett javaslatok szakpolitikai fejlesztést, nemzetközi segítség bevonását, államilag szervezett ellentevékenységet és új információbiztonsági programok indítását szorgalmaznak. A DRI a hibrid hadviselés elleni fellépésnek csak egy területét értékeli, de jól jelzi, hogy az ellenálló képesség javítása folyamatos és szisztematikus munkát igényel. A hibrid hadviselés valamennyi területén átfogó és komplex megoldások szükségesek.

Válságkezelés és döntéshozatal

A hibrid kihívások, kockázatok és fenyegetések kezelése hatással van a Magyarországon kialakult válságkezelési rendszerre, „teszteli" a működés, a vezetés-irányítás és a döntéshozatal rendjét, korrekciós igényeket fogalmaz meg. Azt is mondhatjuk, hozzásegíti az országot ahhoz, hogy meghaladja az 1990-es rendszerváltozás után kialakult, a különböző típusú válságokat másféleképpen kezelő, széttagolt rendszert. Sajnos Magyarországon még nem alakult ki integrált válságkezelési rendszer, hiányzik egy nemzeti válságkezelési központ, a krízismenedzsmentet mindig a válság típusának megfelelően alakították ki, ezért a szakértők már régóta javasolják a meglévő ágazatok integrálását.[38] Hibrid szempontból különösen fontos lenne egy országos szintű, integrált korai előrejelző, figyelmeztető és riasztási rendszer kialakítása, amelynek kiépítése a nemzetbiztonsági szolgálatok megerősítésével és tevékenységének koordinációjával éppen csak megkezdődött.

Magyarországon alapvetően *kétféle válságkezelési rendszer* alakult ki a rendszerváltás (1990) után, az egyik a külső katonai támadás elleni védelem feladatainak megoldását, a másik a belső biztonságot veszélyeztető helyzetek kezelésének teendőit hivatott irányítani. Mindkét feladatrendszert az Alaptörvény és sarkalatos törvények határozzák meg.

A külső katonai fenyegetettség kezelésére *jól kiépített honvédelmi igazgatási rendszer funkcionál*, amely felöleli a központi kormányzati szerveket, a megyei és helyi védelmi bizottságokat és a települési önkormányzatok védelmi lehetőségeit. A katonai válságkezelés (idegen hatalom közvetlen támadásának veszélye /rendkívüli állapot/, megelőző védelmi helyzet, váratlan katonai támadás) esetén a kormányzati koordinációt a *Honvédelmi Igazgatási Koordinációs Tárcaközi Munkacsoport* (HIKOM) biztosítja, amelynek folyamatos gyakoroltatását a NATO és EU válságkezelési gyakorlatok is előírják. Ezt a feladatot a Kormány rendeli el és a Honvédelmi Minisztérium koordinálja.

1-4-es skálán értékeli az ország információs védelmi szintjét az orosz befolyás ellen, minél alacsonyabb az érték, annál jobb a védekezés. Magyarországon a lakosság kevésbé kitett az orosz dezinformációs és propaganda kampányoknak, az 1.3-as mutató Lengyelországgal azonos szinten mért. Az információs támadásokra adott kormányzati válaszok mutatója 2.8, amely magasabb a többi visegrádi partnerországéhoz viszonyítva. Sajnos hazánkban nincs olyan dedikált szervezet, amely az információs támadásokra kormányzati szintű válaszokkal foglalkozna. A magyar információs rendszerek sebezhetősége a digitális hadviseléssel szemben 2.4-es értéket kapott, amely a V4 átlagnál (Szlovákia kivételével) rosszabb. A magyarországi értékelést Bartha Dániel, Inotai Edit és Deák András készítette.

38 Keszely 2020, 40–46.

Terrorveszélyhelyzet esetén a feladatokat a *Terrorellenes Koordinációs Bizottság* (TKB) irányítja, amelynek vezetője a Terrorelhárítási Központ főigazgatója. A terrorizmus elleni feladatokat a magyar kormány 2015-ben teljesen újra szabályozta, bővítette a Nemzetbiztonsági Kabinet hatáskörét, meghatározta a TKB feladatait, a közreműködő nemzetbiztonsági szolgálatok, rendvédelmi szervek és kormányzati hivatalok teendőit, nemzetközileg kompatibilis módon (1-4 fokozat, ahol az 1-es fokozat jelenti a legmagasabb kockázatot) állapította meg a terrorfokozatokat. Nehezebb viszont a sokféle egyéb veszélyt (elemi csapások, természeti eredetű veszélyek, ipari szerencsétlenség, civilizációs eredetű veszélyek, valamint egyéb eredetű veszélyek például a tömeges megbetegedést okozó humánjárvány, állatjárvány) előre szabályozni, mert ezek hasonló, de mégis más-más válságkezelést igényelnek. Az ezeket összefoglaló veszélyhelyzet fogalmát és tartalmát az Alaptörvény és a katasztrófavédelmi törvény határozza meg, amelyek kezelésére jogosult szerveket 2000 óta, az integrált katasztrófavédelem létrehozása után a *Katasztrófavédelmi Koordinációs Tárcaközi Bizottság* (KKB) fogja össze. A KKB a Kormány javaslattevő, véleményező, tanácsadói szerve, amelynek elnöke a belügyminiszter, aki egyben a belső biztonságért felelős miniszterelnök-helyettes is. A KKB-hez telepített feladat- és hatáskörök kiemelten az elemi csapások és az ipari szerencsétlenségek elleni hatékony védekezéshez kapcsolódnak, amelyek kiterjednek a megelőzés, a védekezésre való felkészülés, a védekezés és a helyreállítás feladataira. A KKB állandó jelleggel Titkárságot, a Belügyminisztériumban Operatív Törzset, a BM Országos Katasztrófavédelmi Főigazgatóság (BM OKF) bázisán Veszélyhelyzet-kezelési Központot, valamint a védekezés szakmai irányítására védekezési munkabizottságokat működtet. Ez a rendszer a rendkívüli időjárási helyzetek (hóhelyzet, hőségriadó), a H1N1 madárinfluenza, a szarvasmarha szivacsos agyvelőgyulladás járványveszély, valamint az ár- és a belvizek fenyegetései során kiválóan működött. Ezt a BM-en alapuló Operatív Törzset működtette a kormány a 2015. évi tömeges migrációs veszélyhelyzetben is.

A KKB mintájára hozta létre a kormány a pandémia időszakában a *Koronavírus-járvány Elleni Védekezésért Felelős Operatív Törzset* (Operatív Törzs), amelyet a miniszterelnök vezet, helyettese pedig a belügyminiszter.[39] A veszélyhelyzetet kormányrendelettel hirdették ki,[40] melynek értelmében Magyarország egész területére kiterjedő hatállyal bevezették a rendkívüli jogrendet az élet- és vagyonbiztonságot veszélyeztető tömeges megbetegedést okozó humánjárvány következményeinek elhárítása, a magyar állampolgárok egészségének és életének megóvása érdekében. Azonban már ez a megoldás is önmagában jelzi az ad hoc módon felállított rendszerek problémáját, hiszen a BM vezetésű Operatív Törzsben (OT) háttérbe került az egészségügyért felelős tárca, illetve a kormány kénytelen volt az OT-t különböző minisztériumi szintű akciócsoportokkal (oktatás, létfontosságú vállalatok védelme, pénzügyi stb.) megerősíteni. Az ágazati felépítésű irányító és koordinációs szervek ugyanis csak egy bizonyos típusú válságot képesek jól kezelni a rájuk jellemző sajátos gondolkodási mód, cselekvési rend és szervezeti kultúra miatt, az összetett

39 László 2021.

40 40/ 2020. (III.11.) Korm. rendelet.

válságok összkormányzati integrált vezetési-irányítási struktúrát igényelnek. További probléma, hogy a két alrendszer (külső védelem, belső védelem) ugyanazon intézményrendszert, erőforrásokat és képességeket használja, csak más-más feladatokra, helyszínen, más-más alá- és fölérendeltségi rendszerben, eltérő struktúrában, munkarendben és együttműködésben. Mindezt bonyolítja a hibrid hadviselés, amikor a fenyegetéstípusok változnak, összekapcsolódnak, variálódnak, kezelésük nagyfokú rugalmasságot és több ágazat együttes fellépését igényli. Ráadásul a hibrid fenyegetések kezelését általában nem lehet a különleges jogrend szabályai szerint kezelni, mivel ezek általában ún. küszöb alatti válságok formájában jelennek meg. Éppen ezért a hibrid fenyegetések, akárcsak a terrorizmus, a kibertérből érkező fenyegetések vagy a migráció, *lassan, de folyamatosan „nyomot" hagynak az intézményi fejlődésben, a normál békeidőszaki és válságkezelési döntéshozatalban.*

Első lépésként a hibrid hadviseléssel kapcsolatos nemzetközi kapcsolódások, együttműködési fókuszpontok alakultak ki, amelyek a szövetségi rendszereinknek köszönhetők. A kialakított kormányzati rend alapján a NATO felé a HM és a KKM, az EU felé pedig a BM és a KKM megfelelő szervei kaptak kapcsolódási lehetőséget. Fontos lépésként értékelhető a *Terrorelhárítási Információs és Bűnügyi Elemző Központ* (TIBEK) létrehozása 2016-ban, az Információs Államtitkárság létrehozása a Miniszterelnöki Kormányirodán 2018-ban, valamint a hibrid koordinátor státusz rendszeresítése a Külgazdasági- és Külügyminisztériumban. A TIBEK folyamatosan figyelemmel kíséri a titkosszolgálatoktól (Információs Hivatal, Alkotmányvédelmi Hivatal, Katonai Nemzetbiztonsági Szolgálat, Nemzetbiztonsági Szakszolgálat), valamint más kormányzati szervektől kapott információkat, folyamatosan elemzi az ország nemzetbiztonsági, bűnügyi és terrorfenyegetettségi helyzetét. Bár a meglévő válságkezelési rendszer folyamatosan javul, egy összetett krízis kezelése (mint például a COVID-19 járvány) azt mutatja, hogy az elmúlt évtizedekben kialakult rendszer csak kiegészítő szervezési, integrációs és együttműködési megoldásokkal tud funkcionálni.

Egy integrált válságkezelési struktúra létrehozását fogja segíti a 2021. évi Vbö, amely az összkormányzati felelősség érvényesítése érdekében *Nemzeti Védelmi és Biztonsági Fórum* létrehozásáról intézkedett (43§. (1) bek.). A Fórumot a miniszterelnök vezeti majd, amely a védelem és biztonság valamennyi területének fejlesztésével (így a hibrid fenyegetésekkel is) összefüggő állami és nem állami kérdések megvitatására, valamint az ezekkel összefüggő intézkedések kiadására lesz hivatott. E feladatával összefüggésben a Kormány elősegíti saját szervei, valamint a természetes és jogi személyek korszerű adatgazdálkodását, adathasznosítását és adatvédelmét, figyelemmel kíséri a védelmi és biztonsági kihívások, valamint a védelmi technológiák fejlődését. A törvény felhatalmazza a kormányt a védelmi és biztonsági feladatok összehangolt irányítására (Miniszterelnöki Kormányiroda), valamint a nem a kormány irányítása alá tartozó szervekkel való együttműködés megvalósítására. A civil szervezetek, a vallási közösségek és a karitatív szervezetek önkéntes alapon vesznek részt a védelmi és biztonsági feladatok ellátásában, amelyet a védelmi és biztonsági igazgatás szervei koordinálnak. Az operatív irányítás biztosítása érdekében *nemzeti eseménykezelő központot* fognak felállítani (52.§. c.) Mindezen intézkedések – ha nem is pótolják egy *egységes Nemzeti Válságkezelési Központ* létrehozását – javítani fogják

a válságkezelési rendszerét, amely jó hatással lehet a kormány hibrid fenyegetésekkel szembeni koordinált fellépésére. Célszerű lenne azonban a törvényben nevesített intézkedések minél előbbi megvalósításának megkezdése.

Következtetések

A hibrid fenyegetések elleni védelem szakpolitikája Magyarországon folyamatosan alakult ki, amelyben nagy szerepe volt a nemzetközi szervezeteknek, az EU-nak és a NATO-nak. A tudatos építkezés a kibervédelemmel kezdődött, de 2016-tól megkezdődött az átfogó biztonság alapjainak lerakása, 2020-tól pedig előtérbe került a nemzeti ellenállóképesség erősítése. A magyar kormány hamar felismerte, hogy a külföldi befolyás-szerzéssel szemben már nem elegendő csak a Belügyminisztérium eszközrendszerével fellépni, sokrétű civil állami felkészültségre és katonai képességekre van szükség. A nemzeti eszközrendszer spektrumának bővítése mellett a hibrid fenyegetések elleni védekezés koordinációja és irányítása 2019-től a kormány hatáskörébe került, amiben közrejátszottak a COVID-19 ellenes védekezés tapasztalatai. 2020-2021-ben a kormány egy új szabályozási sebességre kapcsolt, megjelentette a nemzeti biztonsági stratégiát, a nemzeti katonai stratégiát, sikeresen új törvény elfogadását kezdeményezte a védelmi és biztonsági tevékenységek összehangolásáról. Bár a válságkezelés vezetésének és irányításának rendje továbbra is „katasztrófavédelmi" szisztémára emlékeztet, egyre több hibrid hadviseléshez is felhasználható elem (pl. a gazdaság újraindítása, a civil hatóságok katonai támogatása) került be az összkormányzati irányító és koordinációs rendszerbe. A fejlődés azonban egyenetlen, egyes területeken (kibervédelem, nemzetbiztonsági szolgálatok együttműködése, kritikus infrastruktúra védelme) komoly előrelépések történtek, más vonatkozásban (információs, pénzügyi-gazdasági, egészségügyi) lemaradások tapasztalhatók. 2023 közepéig Magyarországon egy komplex és integrált védelmi - biztonsági struktúrát hoznak létre, várhatóan a Miniszterelnöki Kormányiroda vezetésével. Az összkormányzati struktúra lényegesen javíthatja a hibrid fenyegetések elleni hatékony fellépés lehetőségét, hiszen közös keretbe foglalja és megtestesíti az átfogó megközelítést, az ágazatokon túlnyúló összkormányzati együttműködést. Ugyanakkor világossá vált az is, hogy nem elég csak védekezési rendszereket létrehozni, szükség van a hibrid fenyegetések elleni szakterületi stratégia minél előbbi kidolgozására az ország biztonságának és függetlenségének biztosítása érdekében.

FELHASZNÁLT IRODALOM

Akadémiai források

Bak, Pál, Németh, Gergely, Szőke, Diána 2020. – Foundations of Hungarian Defence Policy". *Hungarian Defence Policy* 2020. Issue 2. Foundations of Hungarian Defence Policy megtekintése (magyarhonvedseg.hu) (Letöltés ideje: 2021. 07. 22.) https://doi.org/10.35926/HDR.2020.2.1

Giannopoulos, Georgios, Smith, Hanna, Theocharidou, Marianthi 2021. In *The Landscape of Hybrid Threats_ A Conceptual Model.* 12–42. Public Version, Helsinki: Hibrid CoE. conceptual_framework -reference-version-shortened-good_cover_-_publication_office.pdf (hybridcoe.fi) (Letöltés ideje: 2021. 12. 23.)

Global Cybersecurity Index 2021. ITU Publication, Geneva Global Cybersecurity Index 2020 (itu.int) (Letöltés ideje: 2021. 12. 25.)

Hoffmann, G. Frank 2018. – Examining Complex Forces of Conflict: Gray Zone and Hybrid Challanges." PRISM, *Journal of Complex Operations* (National Defence University, Washington D.C.) Vol.7. No. 4. 2018, Examining Complex Forms of Conflict: Gray Zone and Hybrid Challenges > PRISM | National Defense University > News (ndu.edu) (Letöltés ideje: 2021. 12. 10.)

Hódos László 2020. Gondolatok Magyarország Nemzeti Biztonsági Stratégiában azonosított kiemelt biztonsági kockázatok nemzetbiztonsági aspektusairól. *Szakmai Szemle* 18 (3). 2020_3_szam.pdf (gov.hu) (Letöltés ideje: 2021. 04. 24.)

Jójárt, Krisztián 2019. Revising the Theory of Hybrid War: Lessons from Ukraine. 04. 2019. Center for European Policy Analysis, Washington D. C. 2019-04-Revising_the_Theory_of_Hybrid_War.pdf (cepa.org) (Letöltés ideje: 2021. 05. 02.)

Kádár Pál 2020. A hibrid kihívások és a működő államszervezet. Gondolatok egy konferencia margójára. *Honvédségi Szemle* 148 (4): 3–10. A hibrid kihívások és a működő államszervezet – gondolatok egy konferencia margójára megtekintése (magyarhonvedseg.hu) (Letöltés ideje: 2021. 07. 24.) https://doi.org/10.35926/HSZ.2020.4.1

Kádár Pál 2021. A pandémia kezelése mint a nemzeti ellenálló képesség „tesztje". *Honvédségi Szemle* 149 (2): 3–13. A pandémia kezelése mint a nemzeti ellenálló képesség „tesztje" megtekintése (magyarhonvedseg.hu) (Letöltés ideje: 2021. 05. 24.) https://doi.org/10.35926/HSZ.2021.2.1

Keszely László 2020. A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modellje. *Honvédségi Szemle* 148 (4): 24–48. A hibrid konfliktusokkal szembeni átfogó fellépés lehetséges kormányzati modelljei megtekintése (magyarhonvedseg.hu) (Letöltés ideje: 2021. 07. 17.) https://doi.org/10.35926/HSZ.2020.4.3

Kovács László 2018. *Kiberbiztonság és -stratégia.* Budapest: Dialóg Campus Kiadó. web_PDF_Kiberbiztonsag_es_strategia.pdf (Letöltés ideje: 2021. 05. 04.)

László Viktória 2021. A hatályos magyar szabályozás és a koronavírus-járvány első hulláma idején kihirdetett veszélyhelyzet során bevezetett kormányzati intézkedések vizsgálata. *Katonai Jogi és Hadijogi Szemle* 9 (1): 43–76. Katonai-szemle-2021_1_final.pdf (hadijog.hu) (Letöltés ideje: 2021. 07. 15.)

Petruska Ference, Till Szabolcs Péter, Balogh András 2021. A veszélyhelyzet katonai, honvédelmi feladatainak jogi háttere. In Koltay András, Török Bernát (szerk): *Járvány sújtotta társadalom: A koronavírus a társadalomtudományok szemszögéből.* Budapest: Ludovika Egyetemi Kiadó.

Porkoláb Imre 2015. Hibrid hadviselés: új hadviselési forma, vagy régi ismerős? *Hadtudomány* 25 (3–4): 36–48. Hadtudomany_2015_3-4_ONLINE_PDF_A (mhtt.eu) (Letöltés ideje: 2021. 05. 02.)

Rácz András: *Oroszország hibrid háborúja Ukrajnában.* KKI- tanulmányok. T-2014/1. (99+) (PDF) Oroszország hibrid háborúja Ukrajnában (Russia's Hybrid War in Ukraine) | Andras Racz - Academia.edu (Letöltés ideje: 2021. 05. 02.)

Report of the ICDT and Bakamo 2021. Report of the ICDT on the NATO PPD Project on Understanding people's perception on national security risks and increasing resilience through social media in v4 countries in the light of NATO 2030.
Jan. 21. 2021. Resilience jelentes v.pdf Microsoft PowerPoint - resilience bakamo report.pptx (filesusr.com) (Letöltés ideje: 2021. 06. 20.)

Resperger István, Kiss Álmos Péter, Somkúti Bálint 2013. *Aszimmetrikus hadviselés a modern korban. Kis háborúk nagy hatással.* Budapest: Zrínyi Kiadó.

Resperger István 2018. A *válságkezelés és a hibrid hadviselés.* Budapest: Dialóg Kiadó. Resperger István _A válságkezelés és a hibrid hadviselés.pdf (uni-nke.hu) (Letöltés ideje: 2021. 05.12.)

Simicskó István 2017. A hibrid hadviselés előzményei és aktualitásai. *Hadtudomány* 27 (3–4): 3–16. Ht_201734_5-18.pdf (mhtt.eu) (Letöltés ideje: 2021. 05. 10.)

Somodi Zoltán, Kiss Álmos Péter 2019. A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban. *Honvédségi Szemle* 147 (6): 22–28. A hibrid hadviselés fogalmának értelmezése a nemzetközi szakirodalomban megtekintése (magyarhonvedseg.hu) (Letöltés ideje: 2021. 12. 18.) https://doi.org/10.35926/HSZ.2019.6.2

Szenes, Zoltán 2018. Military Security Today. New Threats, New Wars, New Theories. In Géza Finszter, István Sabjanics (Eds): *Security Challenges in the 21th Century.* Budapest: Dialóg Campus. SzenesZ_Security_Challenges_in_the_21st_Century_web-5.pdf (bm-tt.hu)
(Letöltés ideje: 2021. 05. 15.)

Till Szabolcs 2021. A honvédelmi alkotmányosság tematikus trendjei és hangsúlyváltozásai I. *Katonai Jogi és Hadijogi Szemle* 9 (1): 7–42. Katonai-szemle-2021_1_final.pdf (hadijog.hu) (Letöltés ideje: 2021. 07.05.)

Yelisejev, Andrei, Damard, Volha (Eds.) 2018. *Disinformation resilience in Central and Eastern Europe.* Kyiv. DRI - Disinformation Resilience Index (stratpol.sk) (Letöltés ideje: 2021. 07. 16.)

DOKUMENTUMOK

A Europe that protects: Countering hybrid threats. June 2018. hybrid_threats_en_final.pdf (europa.eu); NATO's Response to hybrid threats. NATO - Topic: NATO's response to hybrid threats (Letöltés ideje: 2021. 12. 21.)

Joint EU–NATO Declaration 2018. Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization. NATO – Official text: Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 10-Jul.-2018 (Letöltés ideje: 2021. 12. 20.)

Joint Communication to the European Parliament and the Council. Joint Framework on Countering hybrid threats, a European Union response. EU Commission, Brussels, 6.4.2016. EUR-Lex - 52016JC0018 - EN - EUR-Lex (europa.eu) (Letöltés ideje: 2021. 12. 19.)

Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of North Atlantic Treaty Organization. 08 July 2016. Warsaw. NATO - Official text: Joint Declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization, 08-Jul.-2016 (Letöltés ideje: 2021. 12. 19.)

NATO - Official text: Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization , 08-Jul.-2016 (Letöltés ideje: 2021. 12. 23.)

Security: EU strengthens response to hybrid threats. Press Release, 6. April 2016. Brussels. Security: EU strengthens response to hybrid threats (europa.eu) (Letöltés ideje: 2021. 12. 19.)

MAGYAR JOGSZABÁLYOK

1139/2013. (III.21.) Korm. határozat Magyarország Nemzeti Kiberbiztonsági Stratégiájáról. MK_047.vp (kozlonyok.hu) (Letöltés: 2021. 05. 28.)

2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról 2013. évi L. törvény Az állami és önkormányzati szervek elektronikus információbiztonságáról – Hatályos Jogszabályok Gyűjteménye (jogtar.hu) (Letöltés: 2021. 07.17.)

1586/2019. (X.16.) Korm. határozat A Hibrid Fenyegetések Elleni Európai Kiválósági Központhoz való magyar csatlakozásról. *Magyar Közlöny*, 168. szám. 2019. október 26. Magyar Közlöny Online (kozlonyok.hu) (Letöltés ideje: 2021. 07. 13.)

2019. évi CV. törvény Egyes törvények honvédelmi kérdésekkel összefüggő módosításáról. A törvénymódosítások 2020. január 1-jével léptek hatályba. 2019. évi CV. törvény - Nemzeti Jogszabálytár (njt.hu). (Letöltés ideje: 2021. 04. 30.)

Magyarország Nemzeti Biztonsági Stratégiája. Biztonságos Magyarország egy változékony világban, 1163/2020. (IV.21.) Korm. határozat NBS_MK_2020_81_1163.2020_Korm.hat.pdf (gov.hu) (Letöltés ideje: 2021. 05. 10.)

Magyarország Alaptörvényének kilencedik módosítása. *Magyar Közlöny* 285. szám. 2020. december 22. MK_20_285 (1).pdf (Letöltés ideje: 2021. 06. 10.)

40/ 2020. (III.11.) Korm. rendelet Veszélyhelyzet kihirdetéséről. 40/2020. (III. 11.) Korm. rendelet - Nemzeti Jogszabálytár (njt.hu)

1393/2021. (VI.24.) Korm. határozat Magyarország Nemzeti Katonai Stratégiájáról. *Magyar Közlöny* 2021. évi 119. szám MK_21_119 NKS 2021.pdf (Letöltés ideje: 2021. 07. 01.)

2021. évi XCIII. törvény: A védelmi és biztonsági tevékenységek összehangolása. *Magyar Közlöny* 120. szám. 2021. június 25. MK_21_120.pdf (Letöltés ideje: 2021. 07. 01.)