Babos Tibor

# A Digitális Jólét Program biztonság-, védelem- és katonapolitikai relevanciái

DOI 10.17047/HADTUD.2018.28.E.122

*„Fogd kézen a változásokat,*
*mielőtt azok, torkon ragadnak téged”*
Churchill

**Rezümé:**
A digitális átalakulás feltartóztathatatlan, áthatja a fejlett világ társadalmi rendszerének egészét. Hazánknak nemcsak kapcsolódnia kell ahhoz, hanem célszerű vezető szerepre törnie e folyamatban. A tanulmány röviden összefoglalja a Digitális Jólét Program (DJP) katonai vetületeit, kapcsolódásait; vázolja a Zrínyi 2026 Honvédelmi és Haderő-fejlesztési Program irányait; javaslatokat tesz DJP-hez kapcsolható katonai rendszerekkel szemben támasztott követelmények meghatározására; valamint általános következtetéseket fogalmaz meg a biztonság-, védelem- és katonapolitika DJP-ben történő megjelenítése tárgyában.

**Kulcsszavak:**
Nemzeti Infokommunikációs Stratégia; Digitális Jólét Program; Digitális Munkaerő Program; Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program; biztonság-, védelem- és katonapolitika; digitális, informatikai és hálózatalapú rendszerek; informatika; kibervédelem és -hadviselés.

Babos, Tibor

**Security, Defense and Military aspects of the Digital Welfare Program**

**Abstract:**
The digital transformation is irresistible, penetrates the political, economic and social system of the developed world as a whole. Due to its high standard scientific capacities, Hungary should take a leading position in this global process. The study discusses the relevant security, defense and military aspects of the Digital Welfare Program (DWP), makes recommendations for defining requirements for military systems linked to the DWP, as well as offers general conclusions on the issue of security, defense and military policy in the DWP.

**Key words:**
Hungarian Digital Wellbeing Program; cyber security; cyber defense; cyber operations; digital transformation; digital military; network enabled capabilities; cyber space - global common; global powers in cyber space.

Az informatikai forradalom átfogó és nagyiramú változásokat indukált a társadalom egészében. Gyökeresen alakította át a politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, logisztikai, energetikai, diplomáciai, nemzetbiztonsági és katonai rendszereket. Nagy biztonsággal állapítható meg: e folyamat a történelem globális korszakváltásaként értelmezhető és hosszú távon determinálja az emberiség fejlődésének alternatíváit. Ebből következően alapvető kérdésként vetődik fel: a nemzeti (nemzeti biztonsági, katonai és nemzetbiztonsági) stratégiák milyen módon kezelik az informatikai

forradalmat és az azzal együtt felgyorsuló információs, technológiai haladást, elzárkóznak-e tőle, adaptálódnak-e hozzá, vagy élére állnak és a maguk malmára hajtják az abban rejlő lehetőségeket.[1] Tekintettel arra, hogy a digitális átalakulás feltartóztathatatlan, áthatja a fejlett világ társadalmi rendszerének egészét, hazánknak nemcsak kapcsolódnia kell, hanem célszerű vezető szerepre törnie e folyamatban annál is inkább, mert Magyarország nemzetközi összehasonlításban is magasan pozícionált a tudományos, technológiai, informatikai és matematikai felkészültség, szürkeállomány terén, a magyarok vívmányai, tudományos elismerései vitathatatlanok világszerte.

A Digitális Jólét Program (DJP) egyik legfontosabb feladata éppen annak támogatása, hogy Magyarország állami rendszerei, közigazgatása, vállalkozásai és minden polgára, a digitalizáció és az informatikai forradalom nyertese lehessen. A Program – ezt felismerve – kívánja felkészíteni Magyarország polgárait, gazdasági szereplőit, állami rendszereit e globális átalakulásra. Középtávú célként jelölhető ki, hogy Magyarország, a digitalizáció nyújtotta lehetőségekbe terelve tudományos, technológiai, ipari, oktatási és egyéb rendszereit, egy évtizeden belül a világ élvonalába kerüljön.[2]

A Kormány szándékai szerint az egymásra épülő, egymást kiegészítő kormányzati infokommunikációs programokat a magyar társadalom és a magyar nemzetgazdaság digitális fejlesztését célzó, a Kormány 2012/2015. (XII. 29.) határozatával elfogadott DJP keretében kell összehangolni. A DJP célkitűzéseinek megvalósítása a Nemzeti Infokommunikációs Stratégiával (NIS) összhangban, a Digitális Nemzet Fejlesztési Programban (DNFP) elért, illetve megvalósítás alatt álló eredményekre építve tervezett. A 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról (DJP 2.0), azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről szól.[3]

Tekintettel arra, hogy a politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, energetikai és más polgári rendszerek mellett a digitalizáció és informatika nagyban hat a védelmi, katonai és nemzetbiztonsági felépítményekre is, e tanulmány tézise, hogy a biztonsági, honvédelmi, katonai és nemzetbiztonsági megfontolások részét kell, hogy képezzék a Digitális Jólét Programnak és annak 2.0 verziójának. Pontosabban fogalmazva: a DJP-ben és a DJP 2.0-ban ki kell alakítani a honvédelmi, katonai és nemzetbiztonsági ágazatot azért, mert (1) a biztonsági folyamatok közvetlenül befolyásolják a digitális jólétet; (2) a honvédelmi, a katonai és a nemzetbiztonsági rendszereknek támogatniuk kell azt; (3) a katonai rendszerek maguk is alkalmaznak

---

1 Tibor Babos: The Five Central Pillars of European Security. NATO Public Diplomacy Division, Brussels, Strategic and Defense Research Center, Budapest, NATO School, Oberammergau, 2008, pp. 69−92.

2 2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról. Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2018. január 10.)

3 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről. Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2018. január 18.)

és fejlesztenek informatikai, digitális- és hálózatalapú képességeket; s mert (4) a honvédelmi, nemzetbiztonsági szektor egészének kapcsolatban kell állnia az ország legnagyobb szabású digitális fejlesztési projektjével, elkerülendő az attól való leszakadást, vagy izolációt. A DJP megvalósításának egyébiránt is a biztonsági körülmények, fenyegetések szakszerű, folyamatos vizsgálatán, valamint védelmi, katonai és nemzetbiztonsági oltalmazás alatt kell állnia.

A fentiek tükrében e tanulmány a biztonsági fenyegetések és informatika hatásmechanizmusának bemutatása után röviden összefoglalja a DJP és a DJP 2.0 katonai vetületeit, kapcsolódásait; vázolja a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program nyílt forrásból megismerhető elemeit, irányait; javaslatokat tesz a DJP-hez és a DJP 2.0-hoz kapcsolható katonai rendszerekkel szemben támasztott követelmények meghatározására; valamint általános következtetéseket fogalmaz meg a biztonság-, védelem- és katonapolitika DJP-ben történő megjelenítése tárgyában.

## A biztonság átalakulásának digitális vonatkozásai

„*Messze jövendővel komolyan vess öszve jelenkort*”[4] − írja Kölcsey 1831-ben, a Reform-kor idején, amikor az ország fejlődése új lendületet kapott. A 19. század elejére a fejlődésben Nyugat-Európa mintaadó államaihoz, Angliához, Franciaországhoz és a Habsburg birodalomhoz képest lemaradt magyar társadalomban nemzeti és újítási folyamatok indultak meg. A korszak idején számtalan politikai, gazdasági, szociális és kulturális vívmány született. Azok sorában különösen említésre méltó a magyar nyelv oktatása, a nemzeti összetartozást kifejező művészeti alkotások, a polgári átalakulás útjában álló akadályok elhárítása, valamint nem utolsó sorban az önálló modern ipar és technológia megteremtése.[5] E vívmányok aztán az öntudatra ébredő magyar nemzet újkori történelmének alappilléreivé váltak, s elvezettek a modern, polgári Magyarország létrejöttéhez. A korunkat jellemző informatikai forradalom révén hazánknak a Reformkorhoz fogható körülmények között kell megvalósítania nemzeti törekvéseit és megvédenie évezredes értékeit. Fontos ezért, hogy az aktuális biztonsági folyamatokat, kihívásokat és a nemzetközi folyamatok trendjeit helyesen vegyük számba és megfelelő következtetések levonásával sikeres politikát folytassunk regionális és nemzetközi viszonylatban egyaránt.

Az 1980-as évek végén, a kelet–nyugati szembenállás megszűnésével gyökeresen új globális stratégiai helyzet alakult ki. A közép- és kelet-európai államok sorban szakítottak a szocializmus gyakorlatával, a központosított államrenddel, s deklarálták, hogy a Nyugat és annak társadalmi rendszere felé fordulnak. E történések széles körű dezintegrációs, ugyanakkor integrációs tendenciákat idéztek elő. A Kelet-Európában végbemenő események radikálisan megváltoztatták a világ politikai arculatát, s az annak hatására meginduló változások még ma is meghatározók a kontinensen. A jelenlegi újszerű, a korábbinál sokrétűbb és instabilabb helyzetben a biztonságot befolyásoló tényezők, veszélyforrások,

[4] Kölcsey Ferenc: Huszt. 1831. dec. 29, Kölcsey Ferenc összes művei, Országos Széchenyi Könyvtár, Budapest, online: http://mek.oszk.hu/06300/06367/html/01.htm#120 (2015. október 12.)

[5] Gergely András: A polgári átalakulás programja. A reformkor. Rubicon, Történelmi folyóirat, 1996/10. Kormányfők, 1996/4−5. Államtörténet, 1996/1−2. Ezer év, Budapest

kockázatok is más hangsúlyt kaptak, újakkal bővültek.[6] Előtérbe kerültek a biztonság egyéb alkotóelemei: a gazdasági, a pénzügyi, a társadalmi, a kulturális, a vallási, a környezeti, a közbiztonsági, vagy a migrációs problémák mellett dominánsan jelentkeznek a technológiai és informatikai kockázatok.

Földünk biztonságát még mindig az átfogó történelmi korszakváltás következményeiből adódó átmenetiség, illetve a dinamikus restruktúrálódás, a piaci és politikai konkurenciaharc, a regionalizáció, lokalizáció és a nacionalizmus jellemzi, miközben a digitális forradalom és annak kiteljesedése meghatározó történelmi jelenséggé lép elő. Míg a nyolcvanas évek óta a második világháborúban kialakult hidegháborús rend szétporladása egyre inkább dinamikáját veszti, addig az új globális hatalmi centrumok súlyközéppontjai átalakulnak és újradefiniálódnak Ázsiában, Észak-Amerikában és Európában. E folyamatban az amerikai és a nyugat-európai gazdasági potenciál ugyan továbbra is meghatározó, azonban már egyértelműen nem domináns. A hatalmi központok kialakulása és sikere a digitális, informatikai, információs rendszerek minél aktívabb, céltudatosabb és szélesebb felhasználásán múlik.

Ezzel párhuzamosan mind a globális, mind pedig az európai biztonsági kihívások átfogó és nagyléptékű mutációt is produkálnak. Ma egyre makulátlanabbul és erélyesebben juthatnak kifejezésre a nemzetállamokhoz nem minden esetben köthető, viszont transznacionális karakterisztikát öltő fenyegetettségek. Az olyan, háborús küszöb alatti rizikófaktorok, mint a nacionalizmus; a szeparatizmus; az extrémizmus; a gazdasági, technológiai, társadalmi és kulturális aránytalanságok; a fejlődési perspektívák divergenciái; az etnikai és vallási kontrasztok; a territoriális integritás és a nemzeti, etnikai önrendelkezés közötti ellentmondások; valamint a tömegpusztító fegyverek proliferációja; a terrorizmus, a nemzetközi szervezett bűnözés; a pénzmosás; a kábítószer-, fegyver-, és emberkereskedelem; a migráció; a környezetszennyezés; az ipari és az ember által okozott egyéb mesterséges katasztrófák, vagy a járványok gyűrűzésének a mai országhatárok már egyértelműen nem szabnak gátat. Természetüket tekintve korunk biztonsági kockázati tényezői térben kisebb kiterjedésűek, azonban sokrétűbbek, szerteágazóbbak, s egyben dinamikusabbak is; hatásukat tekintve könnyen akár globális méreteket is ölthetnek; időben pedig szinte behatárolhatatlanok.[7]

A globális stratégiai javakat megcélzó nemzeti gazdasági, politikai és katonai stratégiák esetleges konfrontációja a XXI. században is potenciális biztonsági veszélytényező. Míg a fejlett világban a globális centrumok közötti verseny egyre dinamikusabban fokozódik, addig a bizonytalansággal és átmeneti viszonyokkal küszködő térségekben a biztonsági devianciák folyamatos halmozódása tapasztalható. A túlélésért folytatott harc a gazdasági fejlettség különböző szintjein elhelyezkedő országok között, a jóléttől tulajdonképpen függetlenül zajlik. A fejlett országok éppúgy rivalizálnak egymással, mint a fejletlenek, vagy a fejletlenek a fejlettekkel, és fordítva. Leegyszerűsítve: éppúgy több kell annak, akinek kevés van, mint aki sokkal rendelkezik. A globális stratégiai javak többsége azonban ma még véges. Az informatika adta platformokat azonban minden állami és nem állami entitás használja, fejleszti, ezért a digitális terek nagyban összeolvadnak, ezáltal képezve globális egységet, egyben sokrétűséget.

---

6 Tibor Babos. The Five Central Pillars of European Security, NATO Public Diplomacy Division, Brussels, Strategic and Defense Research Center, Budapest, NATO School, Oberammergau, 2008, pp. 69−92.

7 Uo.

A globalizáció, a digitalizáció, az információ, és a médiák által befolyásolt társadalmi és kulturális értékek súlyos identitászavarokat okoznak makro- és mikroközösségi szinten egyaránt. A tradicionális nemzeti jellemvonások, öntudatok, szabályok és egyéb értékek új értelmezést kapnak, s e sokrétű folyamatban a nemzeti stratégiai célok is merőben átalakulóban vannak. Ennek egyik legfőbb oka, hogy a nyitottabb határok, a szabad információáramlás és az információ globálissá válása következtében a nemzetközi kapcsolatok ”nemzeti”, ”(nemzet)állami” és ”nemzetközi” vizsgálati kategóriái, szintjei merőben átértékelődnek.[8]

A globalizáció hatására univerzálódó biztonsági kihívások nagyban összemossák a ”kül-” és ”belbiztonság-politikák” közötti különbséget. E folyamatban az államközpontú intézmények és szabályok feloldódnak és teret engednek a globális kapcsolati rendszerek és szereplők diktálta törvényeknek. A kockázati tényezők egyetemessé válása folytán egyfelől élénkülnek a közös biztonságpolitikai fellépést szorgalmazó viták, másfelől a nemzetállamok magasabb, a nemzetközi biztonsági intézményrendszerek szintjére emelik érdekeik érvényesítését, amely tendencia a nemzetközi intézményrendszer felelősségének növekedésével jár. E folyamatban az állam, mint a ”nemzetközi kapcsolatok egyik tényezője” szerepe és kompetenciája átformálódik. Ma az államok a poszt-internacionális dinamizmus időszakában működnek, amely a határokat sokkal átjárhatóbbá, az intézményeket kevésbé hatékonnyá és a politikai erőt zavarosabbá teszi. Az állami intézmények ugyan továbbra is fontosak maradnak, azok azonban kisebb hatékonysággal, kevesebb forrással és csökkenő legitimációval funkcionálnak. Tekintettel azonban arra, hogy a nemzetközi szervezetek presztízs- és legitimációvesztése rohamosabban megy végbe, mint az államoké, a nemzeti szereplők ereje relatíve gyarapszik.[9]

A globalizáció és modernizáció útjában még mindig számos, elsősorban kulturális, vallási és nacionalista bástya áll. Kérdés, hogy az olyan erősen zárt, tradicionális jelszavak mentén szerveződő közösségek, mint például az iszlám társadalmak, vagy korunk diktatúrái képesek lesznek-e konfliktusmentesen ellenállni e komplex, és többszintű folyamatnak, vagy konfrontálnak vele. Minthogy maga az iszlám sem homogén, valószínű, hogy a konfliktusok az extrémitások, vagyis egyfelől a túlzottan zárt, fundamentalista diktatúrák, valamint a nyitott, liberalizált társadalmak közötti törésvonalak mentén törnek fel. E két, ellentétes irányú erő minden bizonnyal mindaddig konfrontálódik egymással, amíg a kontrasztok ki nem egyenlítik, vagy megfelelőképpen le nem rontják egymást.[10] A digitális hálózatok e konfrontáció nyílt színterei. Miközben az internet óriási kulturális hatást gyakorol a zárt társadalmakra, addig a fundamentális rendszerek mind gyakrabban használják e rendszert támadásaik érdekében.

A legnagyobb veszély ma talán a radikalizmus és a technológia kontrasztjában rejlik. Az egyenlőtlen társadalmi, gazdasági alapok és az aránytalan erőforrások következtében fokozódó konfrontáció-kockázatot a kulturális, civilizációs, vallási, etnikai retorikák és politikai érdekek tovább élezik. E komplex társadalmi polarizáció aztán kölcsönhatásba kerül(het) a hidegháború örökségeként megmaradt katonai potenciállal, amely folyamatban a szinte összemérhetetlen technológiai kontrasztok és a tömegpusztító fegyverekhez való relatíve könnyű hozzáférés meghatározó szerepet játszanak. Ehhez ok-okozati összefüggésként kapcsolódik a további rohamtempójú és széles spektrumú tudományos-technológiai fejlődés,

[8] Uo.
[9] Uo.
[10] Uo.

amelynek során a gazdagok még inkább gazdagabbá és fejlettebbé válnak, a szegények pedig relatíve még inkább a perifériára sodródnak. Az, hogy ezek a kontrasztok miképpen és mikor egyenlítik ki egymást, ma még beláthatatlan.

Az aszimmetrikus biztonsági kockázati tényezők, úgymint a tömegpusztító fegyverek alkalmazása, azok célba juttathatósága és/vagy a terrorizmus által okozható csapás napjainkban nagyobb valószínűségű fenyegetettséget jelent a fejlett országokra nézve. A hidegháború utáni évek zavaros biztonsági környezetében a tömegpusztító fegyverek és más pusztító technológiák ellenőrizetlenül hagyása és proliferációja következtében ma a világ stratégiai erőegyensúlya átstrukturálódik. A fejlett világgal opponáló országok, nemzetek és nem állami szereplők a nemzetközi érdekérvényesítés ”szabályszerű” eszközei hiányában, vagy azok helyett aszimmetrikus kellékeket ragadnak, amelyek relatíve kis forrásigényűek, ugyanakkor hatásukat tekintve akár egyetemesek is lehetnek. Azok a fejlett hatalmak, ahol kifejlesztették e technológiákat, mára potenciális célponttá váltak. Miután növekszik annak lehetősége, hogy a harmadik világ bizonyos politikai erői az egymás közötti, vagy a fejlett világgal szembeni konfliktusai során a hadviselés ”piszkos” eszközeihez nyúljanak, a nukleáris, vegyi és biológiai technológiákban, a génmanipulációban, a tömegpusztító fegyverek hordozóeszközeiben, a számítógépek tömeges felhasználásában rejlő szerteágazó veszélyforrások, a technológiák illetéktelenekhez kerülése jelenti napjaink talán a legkönnyebben bekövetkezhető fenyegetését.

A globalizáció egyfajta reakciós tényezője, vagy inkább selejtterméke a terrorizmus. A terrorizmus soha többé nem tekinthető belpolitikai problémának, tudniillik a terrorizmus direkt fenyegetést jelent a nemzetközi biztonságra. Az egyenlőtlenség, a szegénység, a diktatúrák expanziós becsvágya és az ehhez kapcsolódó kulturális gyökerek táptalajul szolgálnak a terrorizmus burjánzásának. A terrorizmus, mint az egyetemes fenyegetés, a támadások skálája, a globális veszteségek minőségi és mennyiségi mutatói, valamint a transznacionális, professzionális, mobil és minden gátlást és határt nélkülöző terrorszervezetek által nyilvánul meg, amelyek minden egyes nemzetállam biztonságára potenciális veszélyt jelentenek.

A kultúrák szempontjából a globalizáció, a digitalizáció és az informatikai fejlődés jövőjét illető kérdés úgy fogalmazódik meg, hogy az egyes nemzetek, országok, föderációk, államközösségek, régiók, szövetségek és szervezetek mindegyike képes lesz-e annak érdekében mozgósítani forrásait, hogy konfliktusmentesen kapcsolódjon be e folyamatba, vagy, hogy átalakuljon, esetleg megszűnjön? És ha nem, mely(ek) lesz(nek) az(ok) amely(ek) nem lesz(nek) képes(ek)? Mikor? És milyen áron?

## A ”globális közös terek” „kibertere”

A 2010. november 19−20. között, Lisszabonban megrendezett NATO-csúcsértekezleten Anders Fogh Rasmussen főtitkár bejelentette: az állam és kormányfők elfogadták az új stratégiai koncepciót, amely egy erősebb, hatékonyabb, ugyanakkor a globális szereplők és folyamatok irányába nyitottabb, együttműködőbb Szövetséget vizionál. A NATO-vezetők hitet tettek amellett, hogy a NATO-képességeket úgy alakítják a jövőben, hogy azok megbízhatóbb védelmet nyújtsanak korunk modern kihívásaival szemben. A ballisztikus rakétavédelem, a hibrid fenyegetések elleni küzdelem, az informatikai rendszerek védelme, valamint az

elektronikus hadviselés kiemelt figyelmet kap a Szövetség jövőbeni képességfejlesztésében.[11] A stratégiai koncepció előkészítésében aktívan közreműködő Szövetséges Transzformációs Parancsnokság (Allied Command Transformation – ACT), a modern kihívások alaposabb vizsgálata céljából indította el az ún. ”globális közös terek” (Global Commons) projektet, amely tulajdonképpen azon földrajzi és virtuális dimenziókban rejlő lehetőségeket vizsgálja, amelyek nem köthetők egy adott országhoz, régióhoz, viszont meghatározóak a NATO egésze és tagországai biztonsága szempontjából. Ezek a közös dimenziók alapvetően a tengerek és óceánok; a légtér; a világűr, és a kibertér.

A ”Globális közös terek” címmel indított ACT-tanulmány[12] azon földrajzi és virtuális terekben rejlő biztonsági kihívásokat és hatalmi kontroll-lehetőségeket vizsgálja, amelyek nem köthetők egy adott nemzethez, országhoz, vagy régióhoz, viszont meghatározó fontossággal bírnak a NATO egésze és tagországai szempontjából. A közös tengerek és óceánok, a légtér, a világűr, és a kibertér olyan, egymással összekapcsolt, ugyanakkor egymást át is fedő, illetve egymástól függő terek, amelyek behálózzák a földkerekséget. Mivel lehetővé teszik az információk, áruk, szolgáltatások és az emberiség számára fontos egyéb termékek áramlását, valamint az ember mozgását, mindenki használja azokat.[13] A globalizálódó világban a közös terek stratégiai jelentősége fokozatosan nő nemcsak a jóhiszemű, hanem a rosszhiszemű felhasználók számára.[14] A biztonság kutatásában élenjáró szervezetek, közük a NATO figyelmét az a felismerés vezeti e téren, hogy a dimenziók egyikén, vagy akár többjükön relatíve kis anyagi ráfordítással és innovációval, stratégiai károkat lehet okozni. Annak érdekében, hogy a NATO és annak tagállamai képesek legyenek e kihívások kezelésére, komoly politikai, diplomáciai és katonai lépéseket kell tenniük a külső és belső szabályozás terén egyaránt. E feladat azért is sürgető, mert a probléma kétélű: egyfelől a fokozódó globalizáció és technológiai forradalom miatt gyorsan, nehezen követhetően változnak a biztonsági körülmények, ezért a késlekedés később csak jelentős többletráfordítással behozható, stratégiai hátránnyá nőhet. Másfelől, az Egyesült Államok és nyugati szövetségesei által definiált – és egyébként eddig dominált – globális közös terek adta lehetőségeket mind gyakrabban használják ki azok a rosszhiszemű, rendszerint nem állami szereplők, amelyek károkat, vagy akár direkt csapást mérhetnek a nyugati világra.

A négy dimenzió jelentősége katonai szempontból számottevő, hiszen a legfelsőbb parancsnokságoktól egészen a legkisebb alakulatokig, folyamatosan használják azokat a manőverek, de legfőképpen a vezetés, irányítás, összeköttetés alkalmával.[15] A Szövetség a műveletek során például aktívan használja a csapatok és hadianyagok szállítására a világtengereket és légteret, vezetés-irányításra,

---

[11] NATO Summit paves way for renewed Alliance. NATO HQ, 20 Nov. 2010, online: http://www.nato.int/cps/en/SID-A807E092-E5343B66/natolive/news_68877.htm (2010. december 1.)

[12] The Global Commons Initiative. The Global Commons Homepage. Allied Command Transformation, NATO, online: http://www.act.nato.int/globalcommons (2010. december 1.)

[13] Protecting the Global Commons, Security and Defence Agenda. Atlantic Council, Brussels, 2010 November

[14] Scott Jasper: Securing Freedon int he Global Commons, Stanford University Press, California, USA, 3. o.

[15] Linton Wells II: Maneuver in the Global Commons – The Cyber Dimension. SIGNAL Magazine, December 2010, online: http://www.afcea.org/signal/articles/templates/Signal_Article_Template.asp?articleid=2472&zoneid=306 (2011. január 25.)

felderítésre, navigációra a légteret és világűrt, vagy a vezetés-irányítás fenntartására és kommunikációra a kiberteret. Tekintettel arra, hogy a NATO katonai alakulatainak nemcsak az a feladata, hogy saját magukat védelmezzék, hanem a tagországok érdekeit is (ide értve azok kereskedelmét, kutatásait, vagy távközlését), mindezen felül készen kell állniuk a katonai feladat-végrehajtásra a négy dimenzió bármelyikében. Ez természetesen jelentős felderítő, stratégiai elemző, tervező, vezetési, képesség-fejlesztő, logisztikai és műveleti előkészítő tevékenységet követel a globális terekre vonatkozóan.

A négy dimenzió vonatkozásában egyértelműen megállapítható, hogy sok szempontból közös jegyekkel rendelkeznek, ezért össze is kapcsolódnak, átfedik egymást, más szempontból viszont, számos sajátos tulajdonságuk van. Ebből kifolyólag általános és specifikus szempontból egyaránt vizsgálni kell őket.[16] A biztonság szempontjából a globális dimenziók közül a kibertér kapja a legnagyobb figyelmet, hiszen ezeket az emberiség az utóbbi néhány évtizedben ”kreálta”, s ezért nem áll rendelkezésre elegendő nemzetközi jogi, vagy történelmi tapasztalat annak szabályozására, kezelésére. Eltérően a tengerektől és a légtértől, a kibertér nem írható körül egyértelműen, mert nem rendelkezik tisztán definiálható határokkal. A technológiai fejlődés ezek esetében nem egy behatárolt térben történik, mi több, sokkal inkább az a jellemző rá, hogy a technológia tökéletesedésével a kibertérben rejlő lehetőségek, távlatok is dinamikusan bővülnek.

A globális közös terek jellemvonásai, a bennük rejlő törvényszerűségek megismerése nemcsak azért fontos, mert mindennapi életünkben állandóan használjuk őket, hanem elsősorban azért, mert a szemben álló felek stratégiai előnyöket érhetnek el, vagy veszteségeket szenvedhetnek rajtuk. A kibertér bizonyos szempontból a legegyedibb dimenzió az összes közül, hiszen nem köthető és nem is jellemezhető csak fizikai, vagy földrajzi fogalmakkal. Ugyanakkor a kibertér nagyban függ fizikai eszközöktől, technológiáktól, számítógépektől, szerverektől, termináloktól, kábelektől, antennáktól, műholdaktól, amelyek már nem virtuálisak, hanem birtoklásuk és helyük is meghatározható.[17] Mihelyst egy információ útjára indul a mesterségesen kialakított csatornákon át, adott tartózkodási helyének meghatározása rendkívül bonyolulttá válik. Egy adott számítógépről indított információ szerverek, jeltovábbító tornyok, optikai kábelek, műholdak sokaságán keresztül jut el rendeltetési helyére. Az adathalmaz ez esetben nem a legrövidebb úton halad, hanem útját alapvetően a hálózatok szabad és olcsóbb kapacitásai határozzák meg. Az adott információ eközben egyfelől haladhat a földi optikai, vagy más kábeleken, a légtérben elektronikai jelcsoportként, a tengerekbe lefektetett rugalmas optikai kábeleken, vagy műholdas rendszereken a világűrben. Ez a típusú információ-forgalom már ma is több milliószor megy végbe óránként a világban, miközben mennyisége és minősége, hatványozottan fejlődik. Egyértelműen prognosztizálható: a kibertér rendszerei nagyobbá, gyorsabbá és komplexebbé válnak az idő előrehaladtával.

A kibertér sebezhetősége pontosan komplexitásában van, amelynek (ma ismert) elsődleges támadói a hackerek. Egészen az elmúlt évekig bezárólag a támadások főleg a szoftverekre irányultak, vagyis a hackerek a programokat és a

[16] Tara Murphy: Security Challenges in the 21st Century Global Commons. Yale Journal of International Affairs, Volume 5, Issue 2 - Spring/Summer 2010, Spotlight on Security, July 20, 2010, online: http://yalejournal.org/2010/07/security-challenges-in-the-21st-century-global-commons/ (2010. 12. 09.)

[17] Ron Deibert: Toward a Cyber Security Strategy. Vanguard, Canada, online: http://www.vanguardcanada.com/CyberArmsRaceDeibert (2011. január 28.)

virtuális rendszereket támadták. Ez azonban erőteljesen változik. Eltérően a többi dimenziótól a kibertér információ-bázisa és technológiai infrastruktúrája túlnyomó részt civil és kereskedelmi szereplők tulajdonában van.[18] A kibertér ezért elsősorban nem államoktól, vagy kormányoktól függ, s a különböző rendszerek biztonságát sem azok garantálják elsősorban. Erről maguk a civil cégek gondoskodnak. A helyzetet tovább bonyolítja, hogy a tulajdonosok gazdasági szereplők, így a piac szabályai szerint tevékenykednek és erős gazdasági konkurenciaharcot folytatnak egymással.[19] Ilyen körülmények közt a kibertér szolgáltatóinak sokkal inkább az az érdeke, hogy ellenálljanak a külső korlátozásoknak, kibújjanak az állami és nemzetközi szabályzók alól, s a szabályok által előírt biztonságot háttérbe szorítsák. Ez természetesen nagyobb szabadságot, kreatívabb fejlesztéseket, s nem utolsó sorban olcsóbb fenntartást biztosít számukra. Pontosabban: a külső szabályzókból fakadó kötelezettségek szigorú betartása helyett saját biztonságukra és fejlesztésekre költik az összegeket. Amennyiben ez a paradox helyzet így marad, az államok – nemzetközi jog által biztosított – kontrollszerepe folyamatosan gyengül.

A kiberteret jellemző extrémitások, szabályozatlanságok és veszélyek egyik legjobb példája a 2010 őszén kirobbant wikileaks-botrány. Mint ismert, az internetes szolgáltató és támogatói arra szakosodtak, hogy bizalmas, vagy akár szigorúan titkos információkat tegyenek közre, függetlenül attól, hogy azok egyéni, céges, vagy kormányzati forrásból származnak. Mivel e tevékenység súlyos károkat és érdeksérelmet eredményezett számos civil cégnek és államnak, nagyszabású ellenkampányba kezdtek a sértettek.

Jelenleg nagy intenzitású és szerteágazó hackertámadás, kormányzati felderítő művelet, rendőrségi eljárás, diplomáciai koordináló tevékenység, valamint gazdasági-pénzügyi ellehetetlenítés folyik a wikileaks.com ellen.[20] Valószínűsíthető, hogy az állami érdekeket ért durva wikileaks-támadás apropóul szolgál az állami védekező mechanizmusok megszilárdításához, köztük a titkosszolgálati informatikai képességek fejlesztéséhez.

Katonai szempontból a 2007 májusában, Észtország ellen észlelt kibertámadás és a 2008 nyarán kirobbant orosz−grúz konfliktus szolgáltatja a legutóbbi tanulságot. Az Észtország ellen indított informatikai támadást ma az elemzők a hadtörténelem első nagyszabású, igazi, országok között zajló ”kiber-háborújának” nevezik. A Tallin elleni kiber-haditerv egy ún. DDOS-támadás volt, amely az informatikai rendszerek túlterhelését és ez által működésképtelenségét idézte elő. A célpontok közt az észt parlament, kormányhivatalok, minisztériumok, bankok, telefontársaságok és médiacégek szerverei voltak.

Egybehangzó szakértői vélemények szerint a célpontok kiválasztása, a támadások szervezettsége, egységessége, hadműveleti ütemezése és ereje messze túlmutat azon, amit egyszerű hackercsoportok, vagy akár a szervezett alvilág képes lenne végrehajtani. Az észt informatikai hálózatoknak ugyanis a normális adatforgalom ezerszeresét kellett volna kezelniük, amire természetesen nem voltak

[18] The National Strategy to Secure Cyberspace. The White House Washington, February 2003, online: http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf (2010. december 17.)

[19] Ziad I. Akir: Space Security: Possible Issues & Potential Solutions. Space Journal Issue 6 2004

[20] Láthatatlan seregek vívják a WikiLeaks-háborút. origo.hu, online: http://www.origo.hu/nagyvilag/20101209-wikileaks-julian-assange-internetes-haboru.html (2010. december 16.)

képesek.[21] Mivel Észtország kérte a NATO Tanács összehívását, az incidens kivizsgálására széleskörű nemzetközi összefogás jött létre. Ennek ellenére nem voltak képesek igazolni, hogy a támadások honnan indultak és pontosan mely állam állt a háttérben. A célpontokat ellehetetlenítő adatfolyamok ugyanis vírusokkal voltak fertőzve, és a világon különböző helyein telepített ideiglenes szerverekről érkeztek. Csak gyanítható, hogy mindezek mögött orosz kormányhivatalok álltak valójában.

Az orosz−grúz konfliktus kiberdimenziója ennél világosabb képet mutat. Moszkva rádióelektronikai felderítő szervei − szorosan együttműködve az orosz hadvezetéssel − összehangolt csapást mértek a grúz civil és kormányzati kiber-rendszerek ellen. Ennek következtében a civil nyílt és a minősített kormányzati informatikai hálózatok is összeomlottak.[22] Ez esetben nemcsak a virtuális rendszereket támadták, hanem a fizikai infrastruktúrát is. Mindez tulajdonképpen hosszú időre lebénította a grúz kormányzat teljes egészének védelmi képességét. Túlzás nélkül kimondható, hogy a fent említett hasonló helyzetek még az olyan államok védelmi rendszereit is tönkre tehetik, mint a NATO vezető hatalmaié, nem beszélve arról, ha ezeket konkrét fegyveres cselekmények is követik.

Válaszul a NATO informatikai rendszerei elleni folyamatos támadásokra, a Szövetség 2009-ben kiadta a kiber-védelemre vonatkozó koncepcióját, amely komplexen leírja a virtuális és fizikai infrastruktúrák védelmét, valamint szól azon területekről is, amelyeket a NATO érdekövezetébe sorol.[23] A NATO informatikai rendszereit ért támadások mellett azonban a technológiai fejlődés nyomása is nagyban inspirálta a döntéshozókat.

A NATO vezetése már évekkel ezelőtt felismerte, hogy az ún. digitalizált hadvezetésre és műveleti vezetésre való áttérés ma már alapkövetelmény, amelynek alapvetéseit és védelmét a legmagasabb szintű koncepcionális dokumentumoknak is tartalmazniuk kell.[24] A Szövetség tehát egy ”föntről lefelé” elvet követő szabályzó-mechanizmussal foglalta koncepcióba a stratégiai elveket és sztenderdeket, ugyanakkor a gyakorlati munka során a döntéshozó, felelős szervek és végrehajtók vonatkozásában pedig operatív, ellentétes irányú, ”alulról felfelé” munkamódszerre épít.[25] Mindebben az emberi tényezőt tarja a legfontosabbnak, hiszen minden kiber-támadás és azok kivédése mögött is elsősorban emberi tevékenység áll. A védelem szempontjából tehát mindennél fontosabb a NATO-felhasználók, rendszer-fenntartók és rendszergazdák képzése, felkészítése.

## Nemzetközi kitekintés

[21] Ian Traynor: Russia accused of unleashing cyberwar to disable Estonia. The Guardian, 17 May 2007, online: http://www.guardian.co.uk/world/2007/may/17/topstories3.russia (2010. december 16.)

[22] Gadi Evron: Internet Attacks Against Georgian Websites. CircleID Internet Infrastructure, Aug 11, 2008, online: http://www.circleid.com/posts/88116_internet_attacks_georgia/ (2010. december 16.)

[23] Evgeny Morozov: The Fog of Cyberwar. NATO military strategists are waking up to the threat from online attacks, Newsweek, April 18, 2009, online: http://www.newsweek.com/2009/04/17/the-fog-of-cyberwar.html# (2010. december 16.)

[24] Rex B. Hughes: NATO and Cyber Defence. What steps have been taken by NATO against the threat of cyber attacks? What needs to be done to prevent them in the future? Mission Accomplished? Ap: 2009nr1/4, online: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf (2011. január 28.)

[25] Rex B. Hughes: Mission Accomplished? NATO and Cyber Defence, 2009 1/4 online: http://www.carlisle.army.mil/DIME/documents/NATO%20and%20Cyber%20Defence.pdf (2010. december 16.)

**A NATO és az Egyesült Államok**

A NATO először az 1999-es koszovói bombázás során szembesült a kiber-hadviselés eszközeivel. A katonai beavatkozás 1999. március 24-én indult Slobodan Milosevic csapatai ellen. A támadást követően szerbiai hackerek megtámadták a NATO weboldalait. A folyamatos túlterheléses támadásoknak (Distributed Denial of Service – DDoS) köszönhetően több alkalommal hosszú időre elérhetetlenné vált a NATO honlapja. A támadásokért felelős Fekete Kéz elnevezésű szerb hackercsoport mindezek mellett több kormányzati oldalra helyezte el politikai üzeneteit, és több alkalommal megpróbáltak betörni a NATO parancsnoki szervereibe, nagyrészt sikertelenül. Bár a légierő számítógépes hálózatába sikeresen bejutottak, azonban titkos információkhoz nem fértek hozzá.

A Belgrádban található kínai nagykövetség bombázásának hatására csatlakoztak kínai, majd később orosz hackerek is, akik szintén túlterheléses támadásokkal és deface-technikával szabotálták mind a NATO, mind pedig az amerikai nagykövetségek weblapjait. A „From Russia With Love" elnevezésű orosz hackercsoport volt a zászlóshajója a NATO elleni támadásoknak, statisztikák szerint legalább 14 katonai és állami weboldalt törtek fel szerb hackerekkel együtt az 1999-es balkáni háború alatt.

Nagyrészt a koszovói beavatkozást követő kiber-incidensek segítették hozzá a döntéshozókat ahhoz, hogy felismerjék a kiber-biztonság fontosságát. Ennek eredményeképpen a 2002-es prágai csúcstalálkozó alkalmával elindították a NATO kiber-védelmi programját, melynek részét képezte a Számítógépes Incidenskezelő Képesség kialakítása is. A képesség mögött álló Technikai Központ képes érzékelni a NATO rendszereibe történő behatolásokat. Ezzel kezdetét vette az Észak-atlanti Szerződés Szervezetének felkészülése a kiber-hadviselésre.[26]

Napjainkban a NATO − igazodva az Egyesült Államok koncepció- és stratégia-fejlesztési rendszeréhez, annak mintájára − komplex rendszerként kezeli a digitalizációt és a kiberteret: egyfelől alkalmazza, épít rá és fejleszti saját rendszereiben; másfelől, mint a globális közös terek létének és hadszíntereinek egyikeként tekint rá.[27]

Jóllehet, önálló kiber-erőket a Szövetség még nem hozott létre, rendelkezik egy ún. Kiber-védelmi Kiválósági Központtal (NATO Cooperative Cyber Defence Centre of Excellence – NATO CCD COE). A Tallinnban 2010-ben alapított szervezet egyszerre funkcionál úgy, mint a NATO által akkreditált tudásközpont, kutatóintézet, kiképző és oktatási bázis, valamint gyakorlóközpont. E nemzetközi katonai szervezet interdiszciplináris alkalmazott kutatásokat folytat, valamint oktatási kurrikulumokat, kiképzéseket, gyakorlatokat kezdeményez és fogad be. Állományát tekintve a szervezet nemzetközi szakértőkből, tudósokból, jogászokból, stratégiai tervezőkből és katonákból áll, akik közösen folytatnak kiber-jellegű és technológia-jellegű kutatásokat a NATO és tagországai katonai, kormányzati, közigazgatási és ipari érdekei mentén. A tagság nyitott minden szövetséges állam előtt. A jelenleg aktívan résztvevő országok: az Amerikai Egyesült Államok, Csehország, az Egyesült Királyság, Észtország, Franciaország, Görögország, Hollandia, Lengyelország, Lettország, Litvánia, Magyarország, Németország, Olaszország, Spanyolország,

[26] Szentgáli Gergely: A NATO kíbervédelmi politikájának fejlődése. Nemzet és biztonság, online: http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (2017. december 28.)

[27] Babos Tibor: "Globális közös terek a NATO-ban". Nemzet és Biztonság, 2011. április, On-line: http://www.nemzetesbiztonsag.hu/cikkek/babos_tibor-___globalis_kozos_terek____a_nato_ban.pdf

Szlovákia és Törökország. Ausztria és Finnország, mint nem NATO partnerországok együttműködési partnerséget írt alá.[28]

**Kína**

A kínai gazdasági csoda és az annak nyomán rögzülő komplex hatalmi expanzió mára klisévé vált. Kína minden kétséget kizáróan a világ politikai, gazdasági élvonalába került az elmúlt alig negyed században, s mára egyetlen másik hatalom sem hagyhatja figyelmen kívül Peking érdekeit, s e bővülő expanziót. A kínai csoda és imperializmus azonban nem állt meg, és az ország globális hatalmi terjeszkedésében a kibertér nem egy elhanyagolt portfólió.[29]

Az Internet Live Stats mérései szerint Kínában 721 434 547 internet-felhasználó volt 2016-ban, ami az 1 382 323 332 lélekszámú kínai lakosság 52,2 %-a. Ez a világ 3 424 971 237 összes internet-felhasználójának 21,1%-a.[30] Ez annál is inkább megdöbbentő adat, mert alig egy évtizede az internet egésze a kínai központi Kormányzás által cenzúrázott hálózat volt. Ma Kína rendelkezik a legstrukturáltabb és legnagyobb állami informatikai rendszerrel Ázsiában.[31] Ebbéli pozícióját tartva és fejlesztve, Kína nemzetközi viszonylatban és abszolút értelemben is jelentős fejlesztéseket eszközöl az informatikában, s napjainkban nemcsak, mint felhasználó, hanem mint fejlesztő is jelen van a digitális piacon.

A világ legnépesebb államaként és Földünk egyik legnagyobb digitális rendszerével rendelkező ázsiai hatalomként idejekorán felismerte a kibertér veszélyeit és az abban rejlő lehetőségeket, ideértve annak katonai felhasználását. A kínai biztonsági és katonai rendszerek közvetlen megjelenését, aktivitásuk növekedését a világhálón egyértelműen detektálják a nemzetközi internetes mérések. Ezt azt igazolja, hogy Kína világviszonylatban is számottevő eszközparkot hozott létre és szakembergárdát mozgósított a digitális átalakulás érdekében.

A kínai Kormányzat azonban nem tekinti önálló témának a digitális forradalmat, ezért önálló kiber-szervezeteket, vagy ilyen jellegű hierarchiákat nem hozott létre mindezidáig. A bonyolult kínai államigazgatási struktúrák és ismert koncepcionális dokumentumok inkább arra engednek következtetni, hogy a Kormányzati portfóliók mindegyikét és az állam minden szegmensét alakítják át egyszerre és teszik képessé az informatika befogadására, kezelésére.[32]

Hszi Csin-ping (Xi Jinping), a Kínai Népköztársaság elnöke 2016-ban, személyes felügyelete alatt hozta létre a Központi Internet-biztonsági és az

---

[28] History, Structure, NATO Cooperative Cyber Defence Centre of Excellence, online: http://www.ccdcoe.org./history.html (2018. január 10.)

[29] Mikk Raud: China and Cyber: Attitudes, Strategies, Orgainaztion. NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2017. augusztus 27.)

[30] Internet Live Stats, online: http://www.internetlivestats.com/internet-users/china/ (2018. január 25.)

[31] Desmond Ball: China's Cyber Warfare Capabilities. online: https://indianstrategicknowledgeonline.com/web/china%20cyber.pdf (2017. december 20.)

[32] Mikk Raud: China and Cyber: Attitudes, Strategies, Orgainaztion. NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2018. január 26.)

Információvezetési Csoportot, amelynek fő feladatául szabta Kína kiber-stratégiájának elkészítését. Ez is egyértelműen azt bizonyítja, hogy a digitalizációt és az informatikát Peking a társadalmi fejlődés természetes velejárójának tekinti, ezért azt nem különíti el sem a Kormányzás, sem a Kínai Kommunista Párt ideológiájától. E rendkívül érdekes szemléletből számos következtetés levonható:

- a világ legnagyobb nemzeti internet-közössége központi kormányzás alatt áll;
- a közösség méretére tekintettel e kormányzás direkt módon hat az internethálózat egészére, befolyásolja azt;
- Kína ezzel nemcsak, hogy részévé, hanem domináns szereplőjévé is vált az online világnak, s mivel az internet a nyugati értékek és kultúra mentén kezdett el feltöltődni, közvetlen információs kaput is jelent számára, miközben Kína maga is sok területen adaptálódott a nyugathoz;
- mindez fordítva nem igaz, hiszen Kínából szinte semmi nem jelenik meg nyugaton a világhálón;
- alkalmazkodva az internet adta lehetőségeihez, Kína számtalan területen jutott többlet-információhoz és kapcsolati tőkéhez.[33]

Kihasználva e körülményeket, Kína tudatosan bővítette ilyen jellegű nemzetbiztonsági és katonai képességeit is. Bizonyított tény, hogy a pekingi kormány utasítására a kínai haderő, kínai magánvállalatok és magánszemélyek aktív informatikai és információs tevékenységet folytatnak a nyugati hatalmak és a szomszédállamok irányába. Ezen műveletek célrendszerét a tudományos kutatások, technológiai titkok, az ipari fejlesztések, kormányzati rendszerek, minősített információk képezik. Peking ezzel egyértelműen mutatja, hogy éppúgy, mint az elmúlt 30−40 évben, kész jogellenesen és agresszívan is technológia és know how lopásra, hogy megragadja a stratégiai kezdeményezést és direkt gazdasági, politikai, vagy katonai előnyre tegyen szert. A kínai információs tevékenység sikerét mi sem bizonyítja jobban, mint a komplett amerikai F−35-os vadász- és bombázó repülőgép-fegyverrendszer ellopása, ami az Egyesült Államok legdrágább hadiipari fejlesztése volt.[34]

**Oroszország**

A kiber-hadviselést Oroszország teljesen eltérően értelmezi és kezeli, mint a nyugati szövetségesek. A téma az orosz stratégiai teoretikusok általános és hagyományos koncepcióiba illeszkedik, mint új lehetőség és hadviselési tér.

A Kreml stratégái szerint Oroszországot az Egyesült Államok által dominált és terjeszkedő NATO geostratégiai nyomása alatt tartja és éppúgy, mint minden más területen, az informatikai rendszereken és hálózatokon keresztül is fenyegeti az

[33] Mikk Raud: China and Cyber: Attitudes, Strategies, Orgainaztion. NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2018. január 13.)

[34] Mikk Raud: China and Cyber: Attitudes, Strategies, Orgainaztion. NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2018. január 6.)

ország biztonságát. Az információs teret Oroszország alapvetően állandónak és végtelennek tekinti. Az internet, az információk szabad áramlása, az adatokhoz való nyílt hozzáférés Moszkva számára egyszerre fenyegetés és lehetőség, amit ki kell aknázni. Ezzel együtt a Kreml relatíve sokkal kevésbé ambicionálja az olyan nagyarányú kiber-fejlesztéseket, mint amit az amerikai hadvezetés eszközöl, viszont a téma tudásháttérébe és humántámogatásába komoly tőkét invesztál.

Az orosz katonai szakírók nem használják sem a ”digitális”, sem a ”kiber” szót a katonai rendszerek vonatkozásában. A koncepcionális dokumentumokban sokkal inkább az ún. ”információs rendszerek” és ”információs hadviselés” jelenik meg, ami egy általános keretként szolgál a számítógépes rendszerek, az informatika, az elektronikus hadviselés, az információs műveletek és a pszichológiai hadviselés témákhoz. Ebből kifolyólag a *kiber* és az *informatika* inkább egyfajta eszköz, mint önálló stratégiai dogma Oroszország számára. Eszköz- és térjellegéből adódóan, és illeszkedve az információs rendszer koncepcióba a hadvezetés egyre nagyobb hangsúlyt fektet a témára a hagyományos műveletek során. A mai kiber-műveleteket tanulmányozó számos szakíró felvetette azt is, hogy a komplex információs műveleti képesség kialakítása akár már rövidtávon is felkerülhet Oroszország stratégiai elrettentő képességei közé.

Jóllehet a Vörös Hadsereg meglehetősen elmaradottnak tekinthető az informatikai fejlesztések tekintetében, hiszen mindezidáig a digitalizálás csak a hagyományosan *high tech* űr, rakéta, repülőgép, haditengerészeti és tűzvezetési rendszerekben van jelen, a haderő doktrinálisan és strukturálisan egyaránt nélkülözte az információs kor alapvető vívmányait is. Ennek egyik fő oka, hogy a globális hálózatok adta fenyegetésektől védeni akarták a katonai rendszereket.

A 2008 augusztusában kirobbant orosz−grúz konfliktus műveleti tapasztalatai ugyanakkor egyértelműen arra utalnak, hogy a Vörös Hadsereg kiber-támadó és -elhárító képességei létrejöttek és sikeresen működnek. A Vörös Hadsereg kiber-képességei az orosz−ukrán válságban debütáltak világszínvonalon, amikor egyértelművé vált, hogy magas színvonalú eszközparkkal, kiváló eljárásrenddel és műveleti készséggel voltak képesek uralni a kiber-hadszínteret és elrettenteni az ellenséget támogató külső erőket is.

A nemzetközi kiber-események vizsgálata során született megállapítások mindegyike igazolja, hogy közvetlenül, vagy közvetve Oroszország szinte minden jelentős esetben jelen volt és saját érdekeinek megfelelően zárta a cselekményt. A katonai műveletek információs támogatásán túl az orosz információs képességek szinte naponta felvillannak, legyen az kiber-bűnözés; elektronikus banki rendszerek, tranzakciók; hírközlő csatornák és médiák; vagy informatikai támadások bizonyos állami, közigazgatási rendszerek ellen.

## A Digitális Jólét Program és a Digitális Jólét Program 2.0 katonai kapcsolódásai

A mai értelemben vett digitalizáció, számítástechnika és internet a második világháborús katonai rendszerekben kezdte meg fejlődését, majd a hidegháború katonai tömbjeiben kapott új lendületet, s az ötvenes évekre már a teljesen elszabadult fegyverkezési verseny nukleáris és hagyományos *high tech* fegyverrendszerek műszaki vezérlőberendezéseiben teljesedett ki. Az informatika ma éppúgy jelen van a fejlett világ katonai szervezeteiben, mint a feltörekvő országok haderőiben. Az Egyesült Államok, Franciaország, Nagy-Britannia, vagy Németország

katonai rendszereinek vezetése, irányítása, híradása, logisztikája, utánpótlás-szervezése, vagy hadiipari fejlesztései éppúgy digitális platformokon történnek, mint Kínában, Indiában, Brazíliában, vagy Oroszországban.

A Digitális Jólét Program (DJP) és DJP 2.0 szempontjából ez azt jelenti, hogy a magyar védelmi, nemzetbiztonsági és katonai rendszereket az alábbi követelményeknek kell megfeleltetni:

(1) be kell ágyazódniuk a mindenkori magyar digitális rendszerbe;
(2) NATO-szövetségesi és uniós tagságunkból adódóan biztosítani kell a hazai védelmi, katonai és hadiipari rendszerek NATO- és EU-kapcsolódását, interoperabilitását;
(3) a békeidőben kialakított katonai informatikai rendszereknek arra is képesnek kell lenniük, hogy bármilyen, a békeállapottól eltérő jogrendben, önállóan is képesek legyenek – korlátozásokkal – az ország vezetését, irányítását és a közigazgatás működését biztosítani.

A DJP által rövidtávon kitűzött általános feladatokhoz igazodva az alábbi honvédelmi, katonai és nemzetbiztonsági célrendszer meghatározása indokolt:

- a magyar honvédelmi, nemzetbiztonsági és katonai rendszerek egésze (ide értve az eszközparkot, az azt üzemelő személyi állományt és eljárásrendet) lépjen egyet előre a digitális felkészültség terén;
- minden honvédelmi, katonai és nemzetbiztonsági alrendszer, amely informatikán, technológián alapszik, vagy kapcsolódik ahhoz, a digitalizáció fontosságát időben felismerve növelje verseny-, védelmi és műveleti képességét;
- a honvédelmi, katonai és nemzetbiztonsági informatikai, digitális és hálózatalapú rendszerek kialakítása egy egymásra épülő, egymással kapcsolatban lévő és egymást kiegészítő, szükség esetén redundáns rendszerként is funkcionáló egységet képezzen, hogy a történelmi léptékű digitális átalakulás nyerteseként nagyot lépjen előre a nemzetközi katonai és kiber-hadszíntéren, ezzel is biztosítva Magyarország védelmét és nemzeti érdekeinek megvalósítását;
- mindezzel együtt a katonai informatikai rendszerek fejlesztését úgy kell megvalósítani, hogy azok védve legyenek a polgári és civil platformok támadásaival szemben, bármikor leválaszthatók legyenek azoktól és bármikor, önállóan is képesek legyenek működni, hogy az ország vezetését békétől elérő állapotokban is folyamatosan lehetővé tegyék.

A 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017–2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről szóló kormányzati célok megvalósításához igazodva (a Korm. határozat felépítését követve) az alábbi honvédelmi, katonai és nemzetbiztonsági területek kapcsolódása javasolt:[35]

[35] 1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017−2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről. Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2018. február 1.)

- (Preambulum) a Kormány a Digitális Jólét Program 2.0 végrehajtása során megteremtett széles körű társadalmi párbeszéd fórumaiba, szakmai, társadalmi, érdekképviseleti és tudományos szervezetek közreműködésébe és együttműködésébe be kell vonni a honvédelmi és nemzetbiztonsági szervezeteket (Honvédelmi Minisztérium, Magyar Honvédség, Katonai Nemzetbiztonsági Szolgálat);
- a nemzeti fejlesztési miniszter által bemutatott, „Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentése” című dokumentum (NIS Monitoring jelentés) honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, katonai nemzetbiztonsági és hadiipari vonatkozások);
- a Digitális Jólét Programjával kapcsolatos kormányzati feladatok összehangolásáért és megvalósításáért felelős miniszterelnöki biztos által számára bemutatott, „Digitális Jólét Program 2.0” című stratégiai dokumentum honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, katonai nemzetbiztonsági és hadiipari vonatkozások);
- a Szupergyors Internet Program (SZIP) keretében zajló fejlesztések, a Nemzeti Távközlési Gerinchálózattal (NTG) kapcsolatos fejlesztések, a Nemzeti Információs Infrastruktúra Fejlesztési (NIIF) Program továbbfejlesztése, a magyarországi hírközlési szolgáltatók önerős digitális hálózatfejlesztési beruházásai, valamint a szupergyors internetelérés sebességének megfelelő ütemű emelését célzó program honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadműveleti, vezetési és irányítási, katonai nemzetbiztonsági és hadiipari vonatkozások);
- a mobil távközlés új technológiai megoldása, az 5G hálózati és alkalmazásfejlesztések, és a vezető nélküli gépjárművek elterjesztése, honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (hadműveleti, vezetési és irányítási, haditechnikai és hadiipari vonatkozások);
- szakmai, tudományos és érdekképviseleti szervezetek részvételével megalakuló Magyarországi 5G Koalíció, valamint Magyarország 5G Stratégiája és Akcióterve honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (hadműveleti, vezetési és irányítási, haditechnikai és hadiipari vonatkozások);
- a digitális felkészültség és kompetenciák, a digitálisan felkészült munkavállalók szakirányú honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, hadműveleti, vezetési és irányítási és hadiipari vonatkozások);
- a Digitális Munkaerő Program végrehajtását honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, a HM irányítása alatt álló hadiipari cég-vonatkozások);
- nemzetgazdasági szempontból kiemelten fontos mikro-, kis- és középvállalkozások számára indítandó, a mikrovállalkozások digitális felkészültségének javítását célzó átfogó program honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása

(védelmi igazgatási, katonai igazgatási, hadkiegészítési, hadműveleti és a HM irányítása alatt álló hadiipari cég-vonatkozások);

- a nemzetgazdasági ágazatok digitalizációját támogató egységes módszertani kézikönyv és mérési, minősítési rendszer kidolgozása, valamint a Digitális Szolgáltatás Kereskedelem-fejlesztési Stratégia honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, és a HM irányítása alatt álló hadiipari cég-vonatkozások);
- Magyarország Digitális Agrár Stratégiájának és a stratégia végrehajtását támogató intézkedések honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (katonai és műveleti térképek komplex digitális tartalmai, fóliarendszerei);
- a digitális eszközök és technológiák szerepe az egészségmegőrzésben, a betegségek megelőzése a gyógyászati tevékenységben, illetve az egészségipar digitális innovációs tevékenysége érdekében elrendelt Magyarország Digitális Egészségipar-fejlesztési Stratégiája, valamint az Idősügyi Infokommunikációs Modellprogram honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (katonai egészségügy, Honvédkórház, NATO Egészségügyi Kiválósági Központ);
- a digitális technológiák alkalmazásának felgyorsítása érdekében elrendelt Magyarország Digitális Sport Stratégiája honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (műveleti, kiképzési, képzési, katonai sport- (Honvédelmi Sportszövetség), versenysport vonatkozások);
- a digitális közigazgatási szolgáltatások hatékony támogatása, az állampolgárok és a vállalkozások ügyintézése érdekében elrendelt, a közigazgatás digitalizációjával kapcsolatos feladatok átfogó nyomon követése és koordinációja, illetve a közigazgatásban dolgozók számára egységes referenciakeret, tananyagok és oktatási keretrendszer honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi igazgatási, katonai igazgatási, hadkiegészítési, hadműveleti, vezetési és irányítási és hadiipari vonatkozások);
- a hazai informatikai mikro-, kis- és középvállalkozások, szellemi műhelyek innovációs tevékenységének és termékfejlesztésének támogatását szolgáló intézkedések honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (védelmi és technológiai kutatások, hadiipari vonatkozások);
- a nemzeti kulturális örökség részét képező közgyűjteményi kulturális kincsek egységes szemléletű digitális fejlesztése, a digitalizált kulturális értékek akadálymentes hozzáférhetővé tétele a köznevelés és az oktatás számára, illetve a polgárok digitális kulturális tartalmak iránti érdeklődésének élénkítése célkitűzések honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (hadtörténelem, történeti levéltár [Hadtörténeti Intézet és Múzeum], honvéd hagyományőrzés);
- a polgárok, a vállalkozások és a közintézmények, valamint a magyarországi digitális hálózatok kiber-biztonsága honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);

- a Nemzeti Kiberbiztonsági Stratégia felülvizsgálata, valamint az annak nyomán elkészítendő tételes feladat- és felelős-megjelölést is tartalmazó intézkedési terv honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);
- a DJP 2.0 kapcsán felmerülő információbiztonsági szempontok érvényesítésének honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);
- (19) a digitális ökoszisztéma működését és fejlődését szolgáló hálózati kutatások és azok eredményeinek közvetlen hasznosítása a közigazgatás fejlesztésében, az oktatásban és képzésben honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);
- a helyi, települési és térségi közösségek digitális fejlesztési programjainak, illetve az Okos Város (Smart City) fejlesztések nyomán indított Okos Város munkacsoport, illetve Okos Város és Okos Térség közigazgatási mintaprojekt honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, védelmi igazgatás, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat);
- a digitalizációval együtt járó társadalmi, élettani és környezeti hatások felmérése, a kedvezőtlen hatások enyhítése érdekében elrendelt kutatások, valamint a digitalizáció nyomán megjelenő káros társadalmi hatások kezelése, illetve a jogrendszerben való szankcionálása honvédelmi, katonai, hadiipari és nemzetbiztonsági leágazásainak, kapcsolódásainak kidolgozása (Honvédelmi Minisztérium, Magyar Honvédség, védelmi igazgatás, a HM felügyelete alatt működő hadiipari cégek, Katonai Nemzetbiztonsági Szolgálat).

## Digitális, informatikai és hálózatalapú katonai célrendszerek

Az Alaptörvényben, továbbá a honvédelemről és a Magyar Honvédségről (MH), valamint a különleges jogrendben bevezethető intézkedésekről szóló 2011. évi CXIII. törvényben (Hvt.) meghatározottak szerint az MH-nak, honvédelmi feladatai ellátása érdekében külső fegyveres támadás elhárítására békeidőszakban felkészített erőkkel, eszközökkel és képességekkel kell rendelkeznie. Ebből következik, hogy az MH-nak már békeidőszakban ki kell építenie és működtetnie kell a vezetéshez és irányításhoz szükséges saját üzemeltetésű híradó, informatikai és információvédelmi rendszereket. A Hvt. egyes rendelkezéseinek végrehajtásáról 290/2011. (XII. 22.) Korm. rendelet (Hvt. vhr) értelmében az MH vezetési és irányítási feladatai érdekében MH Kormányzati Célú Elkülönült Hírközlő Hálózatot (MH KCEHH) üzemeltet, melynek fejlesztéséért és működtetésért a honvédelmi miniszter a felelős. A kormányzati célú hálózatokról szóló 346/2010. (XII. 28) Korm. rendelet 2. melléklete elkülönült hírközlő hálózatként nevesíti a honvédelemért felelős miniszter által működtetett Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatot.

Az MH KCEHH az alábbi fő feladatok biztosítására kötelezett:

- a Hvt. vhr értelmében a MH KCEHH a Honvédség vezetési és irányítási feladatai érdekében üzemeltet állandó és tábori telepítésű híradó, informatikai és információvédelmi rendszert;
- a Hvt. vhr 15.§ (1), bekezdése alapján a Honvédség Műveleti Vezetési Rendszere speciális működési feltételeit akkor kell biztosítani, ha a döntéshozatal feltételei, az irányítási és vezetési rendszer működése békeidőszaki rendben nem biztosítható, vagy a békeidőszaki vezetési objektum veszélyeztetettsége olyan mértékű, hogy az irányítás és vezetés feltételei nem biztosíthatók (ilyen esetben a Honvédség stratégiai és műveleti szintű vezetési elemei a béke időszaki objektumtól eltérő helyen működnek, ahol szintúgy biztosítani kell az irányítás és vezetés biztonsági feltételeit);
- a Hvt. vhr 15.§ (2), bekezdése alapján a Honvédség Műveleti Vezetési Rendszere speciális működésének infokommunikációs támogatását a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának rendszerei, továbbá bérelt rendszerek biztosítják;
- a jogszabályban meghatározottakra figyelemmel az MH KCEHH alaprendeltetése, hogy magas rendelkezésre állással biztosítsa az MH alaprendeltetéséből adódó honvédelemi feladatainak végrehajtása érdekében a Honvédség vezetésének és irányításának, ezen belül az MH Műveleti Vezetési Rendszerének infokommunikációs támogatását béke, és különleges jogrend időszakában egyaránt.

Az MH KCEHH stratégiai irányítása három szinten, az alábbiak szerint érvényesül:

- *honvédelmi miniszter*: a Hvt. vhr 2.§ (2) 17. pontja alapján a honvédelmi miniszter felelős az MH KCEHH fejlesztéséért, működtetéséért, megállapítja a Honvédség feladatainak teljesítése szempontjából fontos híradó, informatikai és információvédelmi szolgáltatások működőképességének biztosítása érdekében szükséges együttműködési feladatokat;
- *honvéd vezérkar főnök* (HVKF):
  - a Hvt. vhr 11.§ (1) 2. 3. pontja értelmében a HVKF felelős az ország fegyveres védelmi tervének, a Honvédség különleges jogrend bevezetéséhez kapcsolódó feladatrendszerének, továbbá a készenlét fenntartása és fokozása rendjének előkészítéséért, végrehajtásáért és annak ellenőrzéséért, valamint az ország területének légvédelmi készenléti erőkkel való oltalmazásáért;
  - a Hvt. vhr 11.§ (1) 6. pontja értelmében irányítja a híradó, informatikai és információvédelmi stratégia és szolgáltatási rendszer kialakítását, az MH KCEHH, valamint a MH VIR tervezését, fejlesztését, a szolgáltatások folyamatos biztosítását, üzemeltetését és fenntartását;
  - a Hvt. vhr 11.§ (1) 7. pontja értelmében felelős a Honvédség Műveleti Vezetési Rendszere működtetéséért, működési feltételei biztosításával kapcsolatos feladatok végrehajtásáért, az ehhez szükséges infrastruktúra és infokommunikációs rendszer üzemeltetéséért;
  - a Hvt. vhr 11.§ (1) 8. pontja alapján közreműködik a Honvédség feladatainak teljesítése szempontjából fontos közlekedési hálózat, a híradó, az informatikai és az információvédelmi szolgáltatások, a légi, sugárfigyelő, jelző- és riasztási rendszerek, valamint az energetikai hálózatok elemei közül a létfontosságú rendszerek és létesítmények védelmében.

- *HVK Híradó, Informatikai és Információvédelmi Csoportfőnök*: a HM SZMSZ alapján a honvédelmi minisztertől átruházott jogkörben ellátja az MH KCEHH hálózatgazdai feladatait.

## A Digitális Jólét Programhoz kapcsolható katonai szempontok

A DJP-hez kapcsolódó fejlesztések országos kiterjedésűek és relatíve nagy léptékűek. Nemzetbiztonsági és gazdaságossági szempontból tehát egyaránt indokolt a fejlesztés alatt álló digitális infrastruktúrák megnyitása és elérhetővé tétele a honvédelmi és katonai rendszerek irányába. Ez irányú pozitív vezetői döntés esetén létre kell hozni a DJP védelmi, katonai és nemzetbiztonsági szegmensét, blokkját. Ezzel már a fejlesztések tervezésénél és megvalósításánál is érvényesítésre kerülhetnének az MH távközlő hálózatokkal és infokommunikációs rendszerekkel kapcsolatos követelményei is. A közcélú és kormányzati vezetékes és vezeték nélküli hálózatokat magába foglaló digitális infrastruktúrával kapcsolatos katonai követelményeket az alábbiak mentén javasolt meghatározni:

- biztosítson magas rendelkezésre állást, illetve ennek érdekében robosztus, szövevényes, redundáns kialakítású legyen;
- biztosítsa az adatok bizalmasságát, sértetlenségét és időbeni továbbítását;
- biztosítsa a meghibásodások, a hálózatokban keletkezett incidensek, biztonsági események azonnali észlelését, illetve az azokra történő gyors reagálás lehetőségét az azonnali intézkedések megtétele, a meghibásodások behatárolása, elhárítása, a biztonsági események bekövetkezése esetén a keletkezett károk minimalizálása és a szükséges ellenintézkedések megtétele érdekében;
- biztosítsa a hálózatok, rendszerek, szolgáltatások és alkalmazások MH általi használatát;
- biztosítsa az MH részére a hálózatokhoz történő csatlakozást valamennyi hozzáférési ponton, illetve – külön egyeztetések alapján – hozzáférési pontok kerüljenek kiépítésre az MH által meghatározott helyszíneken;
- a vezetékes, főként optikai átviteli utak kerüljenek végződtetésre valamennyi használatban lévő HM vagyonkezelésű létesítményben (vezetési objektumok, laktanyák, lő- és gyakorlóterek, stb.);
- optikai kábeles átviteli utak kerüljenek kiépítésre valamennyi járási székhelyre;
- a vezeték nélküli hálózatok (közcélú mobil, EDR) országos lefedettséget, illetve a beszédkommunikáció mellett minél nagyobb átviteli sebességű adatforgalmat biztosítsanak;
- kapjon támogatást a katonai célra is alkalmazható, legalább Európát lefedő magyar (esetleg V4) távközlési műhold pályára állításának és üzemeltetésének projektje;
- a digitális infrastruktúráról – annak valós idejű változásait, meghibásodásait tükröző – központi adatbázis kerüljön létrehozásra, melyhez való online hozzáférés – főként különleges jogrend szerinti időszakban – az MH részére biztosított legyen;
- indokolt esetben, illetve különleges jogrend szerinti időszakban, legyen lehetőség a szolgáltatások igénybevételének MH általi priorizálására, a prioritásra jogosult felhasználói kör meghatározására, illetve adott esetben a nyilvános felhasználók forgalomból történő kizárására;

- a kormányzati és közcélú informatikai rendszerekben tárolt – műveleti, logisztikai és hadkiegészítési szempontból releváns – adatokhoz (például elektromos és gáz elosztó központok, víznyerő kutak, vegyi üzemek, logisztikai központok elhelyezkedése, hidak teherbírása, szélessége, a kórházakba beérkezett betegek, sérültek száma, kórházak, orvosi rendelők, polgármesteri hivatalok dolgozóinak lakcíme, a népesség-nyilvántartás hadkiegészítési szempontból fontos adatai, útlezárások, forgalmi akadályok, aktuális rendezvények stb.) előre definiált jogok és felhasználási célok alapján legyen online hozzáférése az MH kijelölt szervezeteinek;
- az MH kijelölt szervezetei legyenek képesek a katasztrófavédelmi, a mentési, a határ- és rendvédelmi szervezetek informatikai szolgáltatásait igénybe venni, azokból aktuális információkat nyerni és oda adatokat küldeni.

Fenti követelményeket Magyarország nemzetközi kötelezettség-vállalásából adódó, illetve az ország védelmével kapcsolatos feladatai indokolják, mely feladatok végrehajtása érdekében elengedhetetlen a Műveleti Vezetési Rendszerhez, a katonai vezetési és irányítási, légi és egyéb fegyverirányítási rendszerek folyamatos és megbízható működéséhez szükséges digitális infrastruktúra fenti követelmények szerinti kialakítása és működtetése.

## Magyar védelemi és hadiipari fejlesztések – „Zrínyi 2026”

*„Zrínyi 2026”* néven az elmúlt huszonhat év legnagyobb honvédelmi és haderő-fejlesztési programját indította el 2017 januárjától a Magyar Honvédség. A 1298/2017. (VI. 2.) Korm. határozat a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról úgy fogalmaz, hogy a Kormány megtárgyalta a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Programot, jóváhagyta annak fő irányait és egyetért azzal, hogy a Programot – Magyarország biztonsági helyzetére és a Magyar Honvédség fejlesztési igényeire tekintettel – a Nemzetbiztonsági Kabinet 2017. február 1-jei ülésén meghatározott prioritási sorrendben kell megvalósítani. A Program részét képező feladatok végrehajtása érdekében felhívta a honvédelmi minisztert az egyes elemeinek megvalósításáról szóló további Kormány-előterjesztések összeállítására és a Kormány részére történő benyújtására.[36]

A Kormány döntése értelmében a honvédelmi kiadások és a hosszú távú tervezés feltételeinek megteremtését szolgáló költségvetési források biztosításáról szóló 1273/2016. (VI. 7.) Korm. határozatban foglaltaknak megfelelően, a támogatási főösszeg GDP arányának 0,1 százalékpontos növelésére vonatkozó előírás szerint, valamint egyéb többletek (közte haditechnikai eszközök felújítására 5000,0 millió forint) miatt 72 048,7 millió forinttal növelésre került a 2017. évi eredeti támogatási főösszeghez képest.[37]

A komplex haderő-fejlesztési terv részleteit magasan minősített dokumentumok képezik, jóllehet sajtóértesülésekből következtetni lehet rá, hogy lényege az erősen elavult, Szovjetúnió-gyártotta eszközök leváltása és korszerű, NATO-kompatibilis és -interoperábilis haditechnika beszerzése, valamint informatikai, digitális- és hálózatalapú fejlesztések véghezvitele tíz éven belül. Ennek megfelelően

[36] 1298/2017. (VI. 2.) Korm. határozat, a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról. Magyar Közlöny, Budapest, online: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK17081.pdf (2017. december 29.)

[37] http://www.parlament.hu/irom40/15381/adatok/fejezetek/13.pdf (2018. február 2.)

átgondolt tervezésre és jól ütemezett, precíz kivitelezésre van szükség, hiszen ez esetben nem egyszeri többletforrásról és annak felhasználásáról van szó, hanem a fokozatosság elvén működő átfogó haditechnikai és hadiipari fejlesztési folyamatról.

Összhangban nemzeti célkitűzéseinkkel és szövetségesi kötelezettségvállalásainkkal a „Zrínyi 2026" jelenleg körvonalazódó fő pillérei az alábbiak: szállító repülőgép-, helikopter-, légvédelmi rendszer beszerzések; fegyverzet-, lőszer-, terepjáró szállító gépjármű-fejlesztések; valamint vezetési, irányítási, híradó, informatikai és kiber-védelmi rendszer-fejlesztések.[38] A DJP katonai relevanciái című fejezetben részletezett jogi, szakmai szabályzóknak és a stratégiai irányítási rendszerrel szemben támasztott további fontos követelmény, hogy szolgálja és biztosítsa a katonai high tech fegyverrendszerek és a hadiipar fejlesztését.

A katonai műszaki, haditechnikai, vezetési, irányítási, híradástechnikai és kommunikációs, felderítési rendszerek fejlesztései elképzelhetetlenek a ma rendelkezésre álló modern informatikai platformok igénybe vétele, alkalmazása nélkül. Ezért a „Zrínyi 2026" haderő-fejlesztési célkitűzései között szerepeltetni szükséges azt, hogy az MH már rövidtávon térjen át és zárkózzon fel a világ informatikai, digitális- és hálózatalapú, ezen keresztül pedig a technológiai élvonalába a katonai rendszerek tekintetében. Mivel a küszöbön álló modernizáció védelempolitikai célrendszere és forrástámogatottsága is jelentősnek mondható fontos, hogy e fejlesztések a súlypontok helyes meghatározásával, a források megtérülés-számításával valósuljanak meg úgy, hogy a honvédelem egészét új pályára, digitális platformra lehessen állítani. Ez csak úgy valósulhat meg, hogy a piacon rendelkezésre álló high tech rendszerekhez és a civil közigazgatás által használt infrastruktúrákhoz kacsolódnak a védelmi, katonai és nemzetbiztonsági rendszerek úgy, hogy azok szükség esetén bármikor leválaszthatók és önállóan is működtethetők legyenek, korlátozott mértékben átvéve a megtámadott, megsérült, vagy rongált kormányzati hálózatok funkcióit a kormány speciális működésének infokommunikációs támogatása érdekében.

## A DJP-hez és a DJP 2.0-hoz illeszthető potenciális katonai fejlesztési irányok

A fentiek tükrében az alábbi konkrét honvédelmi, katonai és haditechnikai fejlesztési irányok kitűzése indokolt a DJP és a DJP 2.0 keretében:

- digitális dominanciájú magyar részvétel a nemzetközi hadiipari munkamegosztásban;
- az 5G technológiára épülő katonai, műveleti, vezetési és irányítási, hírközlési, hadiipari és haditechnikai fejlesztések előnyben részesítése;
- precíziós fegyverek (kézifegyverek, önvezérlő fegyverrendszerek, bombák, rakétarendszerek) fejlesztése;
- intelligens katonai felszerelés-fejlesztés, egyéni és alegység-felszerelésrendszer (intelligens ruha, szenzorrendszer [egyéni és relatív helymeghatározás, valós idejű biofiziologiai állapotmérés, video-kamerarendszer, digitális audio-kommunikáció, hőmérséklet-, páratartalom, vegyi- és sugárzó-anyagmérés], stb.);

[38] Draveczki-Ury Ádám: Zrínyi 2026. Az átfogó fejlesztések időszaka következik. Magyar Honvéd 2017. január, Zrínyi Kiadó, Budapest, online: http://www.honvedelem.hu/cikk/61339 (2017. december 22.)

- önvezérlő katonai járművek (tehergépjárművek, páncélozott járművek, páncélozott szállítójárművek, harcjárművek, repülőgépek [szállító, felderítő, zavaró], helikopterek);
- digitális alapú katonai térkép és fóliarendszer, valamint navigációs rendszer létrehozása;
- a magyar űrprogram nagyarányú digitális és hálózatalapú fejlesztése, magyar műhold fejlesztése és pályára állítása;
- komplex digitális és hálózatalapú vezetési, irányítási, katonai hírközlő és kommunikációs rendszer fejlesztése;
- a honvédelem rendszerében szolgálatot teljesítő katonák és polgári foglalkoztatottak átfogó felkészítése digitális kompetenciákkal (tanfolyamok);
- a katonai képzési, kiképzési rendszer kiegészítése digitális- és hálózatalapú képességekkel;
- a védelmi igazgatási, katonai igazgatási rendszer kiegészítése digitális képességekkel;
- a hadkiegészítési, személyi nyilvántartási rendszerek kiegészítése valós idejű digitális és hálózatalapú platformmal;
- a katonai logisztika és hadtáp (fegyver, lőszer, hadianyag, felszerelés, ruházat, üzemanyag stb.) nyilvántartási rendszere átállítása valós idejű digitális és hálózatalapú platformra;
- a Honvédelmi Minisztérium irányítása alatt működő cégek, hadiipari vállalkozások komplett vállalatirányítási és fejlesztési rendszereinek átállása digitális és hálózatalapú platformra.

## Következtetések

A politikai, közigazgatási, gazdasági, ipari, mezőgazdasági, oktatási, tudományos, egészségügyi, közlekedési, energetikai és más polgári rendszerek mellett a digitalizáció és informatika nagyban hat a védelmi, nemzetbiztonsági és katonai felépítményekre is. A DJP és a DJP 2.0 szempontjából ez azt jelenti, hogy a magyar honvédelmi, katonai és nemzetbiztonsági rendszereket az alábbi követelményeknek kell megfeleltetni:

(1) ágyazódjanak be a teljes magyar digitális és hálózatalapú rendszerbe;
(2) az ország szövetségesi és uniós tagságából adódóan biztosítsák a hazai védelmi, katonai és hadipari rendszerek NATO- és EU-kapcsolódását, -interoperabilitását;
(3) a békeidőben kialakított katonai informatikai, digitális- és hálózatalapú rendszerek legyenek képesek bármilyen, a békeállapottól eltérő jogrendben önállóan is működni, korlátozásokkal biztosítani az ország vezetését, irányítását és a közigazgatás zavartalan működését.

A DJP és a DJP 2.0 tervezése és végrehatása szempontjából ez azt feltételezi, hogy a biztonsági, honvédelmi, katonai és nemzetbiztonsági megfontolások részét kell képezniük a DJP-nek, vagyis a DJP-ben ki kell alakítani a honvédelmi, katonai és nemzetbiztonsági szakágazatot, blokkot. A honvédelmi, katonai és nemzetbiztonsági szakágazat elemezné és értékelné a biztonsági kihívásokat, szaktudásával, képességeivel és eszközeivel támogatná és oltalmazná a Programot, valamint saját maguk informatikai, digitális- és hálózatalapú képességfejlesztéseit is e komplex rendszer keretében végeznék, megnyitva a DJP

más szegmensei előtt is az idekapcsolódás lehetőségét, ezáltal is megteremtve a hazai digitális és informatikai rendszerek, hálózatok egymással való kompatibilitását és interoperabilitását.

IRODALOMJEGYZÉK:

2012/2015. (XII. 29.) Korm. határozat az internetről és a digitális fejlesztésekről szóló nemzeti konzultáció (InternetKon) eredményei alapján a Kormány által végrehajtandó Digitális Jólét Programjáról. Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A15H2012.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2017. szeptember 4.)

1456/2017. (VII. 19.) Korm. határozat a Nemzeti Infokommunikációs Stratégia (NIS) 2016. évi monitoring jelentéséről, a Digitális Jólét Program 2.0-ról, azaz a Digitális Jólét Program kibővítéséről, annak 2017-2018. évi Munkaterve elfogadásáról, a digitális infrastruktúra, kompetenciák, gazdaság és közigazgatás további fejlesztéseiről. Netjogtár, online: https://net.jogtar.hu/jr/gen/hjegy_doc.cgi?docid=A17H1456.KOR&timeshift=fffffff4&txtreferer=00000001.TXT (2017. szeptember 4.)

1298/2017. (VI. 2.) Korm. határozat, a Zrínyi 2026 Honvédelmi és Haderőfejlesztési Program megvalósításáról. Magyar Közlöny, Budapest, online: http://www.kozlonyok.hu/nkonline/MKPDF/hiteles/MK17081.pdf (2017. december 28.), online: http://www.parlament.hu/irom40/15381/adatok/fejezetek/13.pdf (2018. december 22.)

Babos Tibor: Globális közös terek a NATO-ban. Nemzet és Biztonság, 2011. április, On-line: http://www.nemzetesbiztonsag.hu/cikkek/babos_tibor-___globalis_kozos_terek____a_nato_ban.pdf

Tibor Babos: The Five Central Pillars of European Security. NATO Public Diplomacy Division, Brussels, Strategic and Defense Research Center, Budapest, NATO School, Oberammergau, 2008

Desmond Ball: China's Cyber Warfare Capabilities. online: https://indianstrategicknowledgeonline.com/web/china%20cyber.pdf (2017. augusztus 27.)

Draveczki-Ury Ádám: Zrínyi 2026. Az átfogó fejlesztések időszaka következik. Magyar Honvéd 2017. január, Zrínyi Kiadó, Budapest, online: http://www.honvedelem.hu/cikk/61339

Internet Live Stats. online: http://www.internetlivestats.com/internet-users/china/ (2018. január 27.)

History, Structure, NATO Cooperative Cyber Defence Centre of Excellence. online: http://www.ccdcoe.org./history.html (2018. január 19.)

Mikk Raud: China and Cyber: Attitudes, Strategies, Orgainaztion. NATO Cooperative Cyber Defence Centre of Excellence, online: https://ccdcoe.org/sites/default/files/multimedia/pdf/CS_organisation_CHINA_092016.pdf (2018. január 30.)

Szentgáli Gergely: A NATO kíbervédelmi politikájának fejlődése. Nemzet és biztonság, Budapest, online: http://uni-nke.hu/downloads/bsz/bszemle2012/2/05.pdf (2018. január 28.)