Babos Tibor

# „Globális közös terek” a NATO-ban

*A 2010. november 19–20. között Lisszabonban megrendezett NATO-csúcsértekezleten az állam- és kormányfők elfogadták a szövetség új stratégiai koncepcióját. A ballisztikus rakétavédelem, a hibrid fenyegetések elleni küzdelem, az informatikai rendszerek védelme, valamint az elektronikus hadviselés kiemelt figyelmet kap a szövetség jövőbeni képességfejlesztésében. A koncepció előkészítésében aktívan közreműködő Szövetséges Transzformációs Parancsnokság (Allied Command Transformation – ACT) által elindított úgynevezett „globális közös terek” (Global Commons) projekt azokat a 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. E tanulmány bemutatja a „globális közös terek” projektet, áttekinti lényegi elemeit, számba veszi az egyes területek általános és specifikus jellemzőit, rávilágít a NATO fontosabb törekvéseire.*

Ma a világkereskedelem több mint 90%-a a világtengereken zajlik, 2,2 milliárd utas és az exporttermékek mintegy 35%-a a levegőben jut el céljához. A világűrt kommunikációs, megfigyelési vagy navigációs céllal éppúgy használják a különböző kormányok, mint a nemzetközi vállalatok, a hadseregek, vagy akár az egyéni felhasználók. A világon akármelyik internetes komputer képes arra, hogy a másodperc tört része alatt bonyolult üzleti, kormányzati, katonai információt továbbítson a világ bármely részére. Túlzás nélkül állítható, hogy a világ különböző rendszerei rendkívül komplexszé, ugyanakkor nyitottá váltak, illetve egy még nagyobb rendszert alkotva, össze is kapcsolódtak. A rendszerek mindazonáltal bizonyos szempontból átfedik egymást, és függő viszonyba is kerültek egymással. Létrejött az úgynevezett „rendszerek rendszere”, amelynek megismerése, befolyásolása vagy kontrollja döntő jelentőséggel bír a hatalmat gyakorló vagy az azt megragadni akaró entitások, köztük a NATO számára.

Az utóbbi években számos elemzés látott napvilágot, amelyek igazolják, hogy az 1991-ben indított öbölháború óta nagymértékben változtak a biztonsági körülmények. Míg az első öbölháborúban az Egyesült Államok és szövetségesei teljes mértékben uralni tudták a globális közös terek mindegyikét, addig az utóbbi években jelentős befolyásvesztésük tapasztalható. Oroszország, Kína, India, valamint jó néhány multinacionális nagyvállalat is, drasztikusan növelte érdekeltségeit e területeken. Komoly kockázati veszélyt jelent, hogy a mind bonyolultabbá, egyszersmind elérhetőbbé váló rendszerek használata, az azokba tör-

ténő behatolás vagy azok károsítása, relatíve egyre kisebb anyagi ráfordítást igényel, s akár stratégiai szintű veszteséget is eredményezhet. Az államok, kormányok, magáncégek, egyéni felhasználók, jó- és rosszhiszemű szereplők részéről megindult tehát a verseny a globális közös terek feletti kontroll, illetve az azokhoz vezető csatornák szélesítése érdekében.

## A NATO nyitása a globális közös terek felé

Az afganisztáni hadszíntér megnyitása óta mind gyakrabban felmerült, hogy biztosítani kell a szövetség cselekvőképességét azokon a területeken is, amelyek nem tartoznak direkt NATO-illetékesség alá, viszont mindennapi tevékenysége, különösen a műveletek során nagymértékben függ tőle. Az új stratégiai koncepció előkészítése során e téma már a legmagasabb politikai döntéshozók elé került. 2010 májusában Abrial vezérezredes, az ACT parancsnoka utasítást adott stratégiai elemzőrészlegének egy olyan tanulmány elkészítésére, amely feltárja a NATO sebezhetőségét azokban az esetekben, amikor a globális közös terek valamelyikét használja. Az elemzés közvetett célja volt, hogy alapul szolgáljon az azóta már elfogadott új stratégiai koncepcióhoz, valamint egy 2011-ben kiadandó, átfogó koncepcionális dokumentumhoz is. Ez utóbbiról a Szövetséges Transzformációs Parancsnokság parancsnoka *(Supreme Allied Commander Transformation – SACT)* várhatóan 2011 első negyedévében jelent a NATO Katonai Bizottságának *(NATO Military Committee – NATO MC),* majd pedig a Tanácsnak *(North Atlantic Council – NAC).*

A SACT jelentését előkészítendő egy hat alkalommal megrendezett konferenciasorozatot szerveztek. Ennek bázisát az ACT gondozásában 2008-ban kiadott *Multiple Futures Project* következtetéseire és szervezési tapasztalataira építették. A szakmai megbeszélésekre minden olyan szövetséges, partner és együttműködő állam, valamint nem állami szereplő is delegálhatott szakértőket, amely érdekelt a „globális közös terek" témájának megvitatásában, illetve a NATO-val való további együttműködésben. A munkaértekezleteken minden fél aktív, kvázi egyenlő szereplőként vehetett részt, véleményét közreadhatta, valamint konkrét részfeladatot is kapott. A széles nemzetközi bázisra épített, alapos kidolgozótevékenység végül igazolta, hogy a téma kiemelten releváns a NATO-tagok és -partnerek számára, ezért akár a legmagasabb szintű NATO-dokumentumokban is helyet kell kapnia.

## Az ACT-tanulmány fontosabb megállapításai

A tanulmány azokat a földrajzi és virtuális terekben rejlő biztonsági kihívásokat és a hatalmi kontroll olyan lehetőségeit 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, lehetővé téve az információk, áruk, szolgáltatások és az emberiség számára fontos egyéb termékek áramlását.

A NATO-nak a globális közös terekre vonatkozó előzetes állásfoglalása kimondja, hogy a nemzetközi jog által definiált szereplőkhöz, államokhoz tartozó, viszont általuk egyáltalán nem vagy csak alig kor-

mányzott földrajzi területek, mint például bizonyos dél-amerikai, afrikai vagy délkelet-ázsiai – zömmel – határterületek, nem részei a globális közös tereknek. Azok ugyanis szigorúan egy adott állam kompetenciájába tartoznak. Ezzel szemben például az Antarktisz közös területnek értendő, mert státusát a nemzetközi szerződések közösnek definiálják.

A globalizálódó világban a közös terek stratégiai jelentősége fokozatosan nő a rosszhiszemű felhasználók számára is. A NATO figyelmét az a felismerés vezeti e téren, hogy a dimenziókban aránylag kis anyagi ráfordítással és innovációval stratégiai károkat lehet okozni. Annak érdekében, hogy a szövetség és tagállamai képesek legyenek e kihívások kezelésére, komoly politikai, diplomáciai és katonai lépéseket kell tenniük a külső és belső szabályozás terén egyaránt. Ez azért is sürgető, mert egyfelől a globalizáció 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 okozhatnak, akár direkt csapást is mérhetnek a nyugati világra.

Figyelemreméltó, hogy az elmúlt időszakban zajló intenzív kutatások és viták eredményeképpen nagymértékben változott a globális közös terek értelmezése. Míg néhány évvel ezelőtt csak az óceánokat, a sarkvidékeket és az atmoszférát sorolták ide, mára jelentős mértékben bővültek annak elismert vagy hallgatólagosan elfogadott alkotóelemei. Számos ország vagy cég esetenként jóval tágabban vagy szabadabban értelmezi a fogalmat. Úgy gondolják, hogy ha a saját tulajdonukba tartozó termék valamely közös térben van éppen, akkor nemcsak a közös terekre vonatkozó szabályzók érvényesek rá, hanem megilleti őket a teljes védelem joga. Ezt tulajdonképpen azt jelenti, hogy azok az entitások, amelyek használják a közös terek bármelyikét, nemcsak kisajátítják azt az adott helyet, ahol termékük éppen van, hanem számos olyan aktív intézkedést is foganatosítanak, amelyek révén biztosítják annak haladását. Ez a jelenség a gazdaságilag konkurens vagy politikailag ellenérdekelt államok részéről komoly vitákat gerjeszt.

A NATO vezető tisztségviselői azon az állásponton vannak, hogy a béke, a biztonság és a prosperitás garanciáinak szavatolása érdekében a szövetségnek „sajátjaként” kell értelmeznie azokat a termékeket, szolgáltatásokat, létesítményeket vagy információkat, amelyek NATO-érdekeltségben vannak, viszont éppen valamely dimenzióban helyezkednek el. Tény, hogy világos szabályozás híján e tendenciák számos jogi és erkölcsi kérdést vetnek fel, amelyek megválaszolása a jövő feladata lesz. Ma a kellő nemzetközi jogi szabályozás hiányában a dimenziók nagymértékben önszabályzók, s a politikai erő meghatározó súllyal esik latba.

A négy dimenzió jelentősége katonai szempontból szintén számottevő, hiszen a legfelsőbb parancsnokságoktól egészen a legkisebb alakulatokig, folyamatosan használják azokat a manőverek, de legfőképpen a vezetés, irányítás, összeköttetés alkalmával. A szövetség a műveletek során például aktívan használja a csapatok és hadianyagok szállítására a világtengereket és légteret, vezetés-irányításra, felderítésre, navigációra a légteret és világűrt, vagy a vezetés-irányítás fenntartására és kommunikációra a kiberteret. Mivel a NATO katonai alakulatainak nemcsak az a

feladata, hogy saját magukat védelmezzék, hanem a tagországok érdekeit is érvényre kell juttatniuk – ide értve azok kereskedelmét, kutatásait vagy távközlését –, mindezen felül készen kell állniuk katonai feladat végrehajtására a négy dimenzió bármelyikében. Ez természetesen jelentős felderítő, stratégiai elemző, tervező, vezetési, képességfejlesztő, logisztikai és műveleti előkészítő tevékenységet követel a NATO Nemzetközi Katonai Törzsétől.

## A négy globális dimenzió általános jellemzői

A négy dimenzió sok szempontból közös jegyekkel rendelkezik, ezért össze is kapcsolódnak, átfedik egymást, más szempontból viszont számos sajátos tulajdonságuk is van.

A biztonság szempontjából a globális dimenziók közül az űr és a kibertér kapja a legnagyobb figyelmet, hiszen ezekbe az emberiség az utóbbi néhány évtizedben „lépett ki", ezért nem áll rendelkezésre elegendő nemzetközi jogi vagy történelmi tapasztalat a szabályozásukra, kezelésükre. A tengerektől és a légtérről eltérően nem írhatók körül egyértelműen, nincsenek tisztán definiálható határaik. A technológiai fejlődés esetükben nem egy behatárolt térben történik, és a bennük rejlő lehetőségek, távlatok is dinamikusan bővülnek. A globális közös terek jellemvonásai, törvényszerűségeik 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 el bennük.

A NATO-nak jelenleg nincs a globális közös terekre vonatkozóan egységes stratégiája, viszont eseti állásfoglalást több ízben megfogalmazott már az egyes elemek egyikére, másikára vonatkozóan. A felmerülő napi problémák és veszélyek egyre erőteljesebben sürgetik a komplex stratégia kidolgozását. Ennek feltétlenül szólnia kell a globális közös terek általános és minden dimenzióra specifikus értelmezéséről, az átfedésekre vonatkozó szövetségi állásfoglalásról, a veszélyfaktorok számbavételéről, a NATO-t érdeklő lehetőségekről, valamint érdekeiről és viselkedéséről. A szövetség csakis ennek révén tudja leghatékonyabban mobilizálni rendelkezésre álló (erő)forrásait, hogy megelőzze, vagy elrettentse a lehetséges ellenségeket bárminemű támadástól.

## A tengerek és az óceánok

A tengeri a legkorábban megismert dimenzió a négy közül, hiszen a globális kereskedelem nagy része már évszázadok óta itt folyik elsődlegesen. A nyersanyagok és az ember által előállított áruk több mint 90%-a itt mozog, s ezek mintegy 75%-a érinti a legfontosabb nemzetközi tengeri csomópontokat, a csatornákat és a szorosokat. A tengeri szállítás mennyisége 1974 és 2006 között mintegy 284%-kal emelkedett. Míg általában a világ olajszállításának 50%-a szintén a tengereken zajlik, addig például Kína és Japán vonatkozásában ez az arány 80%-os.

A tengeri dimenzió a szállításon kívül még primer élelmiszer- és nyersanyagforrás is egyben, hiszen állat- és növényvilága elemi fontosságú az élelmiszeripar, a gyógyszergyártás számára. Stratégiai jelentősége tehát az „éléskamra-effektus" szempontjából is elvitathatatlan. A fejlődő technológiák következtében a tengerek alatt található nyersanyagok ma már a mélytengeri régiókból is kinyerhetők. A kőolajon és a földgázon kívül egyre nagyobb

ütemben termelhetők ki különböző ércek és más ásványok is. A globális felmelegedés következtében, illetve a modern jégtörő hajóknak köszönhetően rövidültek a tengeri tranzitútvonalak, s olyan helyeken is lehetővé vált a tengerfenéki nyersanyagkitermelés, amelyeket korábban vastag jégtakaró védett. Mivel a szárazföldi nyersanyagforrások is erősen apadnak, a tengerparttal nem rendelkező országok számára is célterületté váltak a mindenki számára nyitott világtengerek és azok nyersanyagkincsei. Kína és India már ma is példa arra, hogy bizonyos államok – az ENSZ vonatkozó rendelkezéseit megsértve – önhatalmúlag kiterjesztik felségvizeik határát. További aggodalomra ad okot, hogy bizonyos nyilvánosságra került nemzeti katonai stratégiák, a fegyverbeszerzések és fejlesztések között prioritásként szerepeltetik azon haditengerészeti rendszereket, amelyek alkalmasak más államok tengeri kijutását megakadályozni, hajóforgalmát blokkolni. Ez egyértelműen bizonyítja, hogy relatív stratégiai előnyük megtartása érdekében adott államok attól sem riadnak vissza, hogy másokat a globális közös tereken ellehetetlenítsenek, netán támadjanak.

A tengerek mai és különösen jövőben használata azonban megköveteli a légi, űrés a kiberdimenzió adta lehetőségek idekapcsolását, valamint a tranzitcsatornák definiálását. A hajózás, a tengerfenéki cső- és kábelvezetékek felügyelete, a nyersanyag-kitermelés, a navigációs követések, az időjárás-figyelés, vagy a kutatások során kapott információk összekapcsolása a többi, felszín feletti globális közös dimenzióval már ma is gyakorlat. Szabályozás hiányában azonban e rendszerhálózatok elleni bármiféle támadás vagy egyáltalán a hozzájuk való kapcsolódás – valamilyen okból történő – akadályozása, pusztítása beláthatatlan következményekkel jár.

Reneszánszát éli a kalózkodás. Ennek oka, hogy Kína, Japán, Dél-Korea és India globális gazdasági szereplőkké válásával meghatványozódott az Európa és a Távol-Kelet, illetve az Egyesült Államok és a Távol-Kelet közötti tengeri kereskedelem, s ezzel együtt az Indiai-óceán és szorosai, valamint az afrikai vizek stratégiai jelentősége. Ezt használják ki a modern kalózszervezetek, a globalizáció, a hiányos nemzetközi szabályozás, a hézagos biztonsági garanciák adta réseket, maximálisan élve a hibrid technológiák lehetőségeivel. A kalózszervezetek ma már több száz sikeres rajtaütést hajtottak végre, és százmillió dollárt meghaladó károkat okoztak a tengeri kereskedelemben. E tények következtében a tengeri nagyhatalmak és a NATO is jelentős haditengerészeti fejlesztésekbe kezdett, valamint fokozódott a nemzetközi összefogás is a tengeri dimenzió szigorúbb szabályozása érdekében.

A tenger a leginkább használt dimenzió az ember-, fegyver-, veszélyesanyag- és egyéb árucsempészek számára. Kifinomult technológiát és fejlett taktikát alkalmazva, a legjobb katonai, vagy titkosszolgálati műveleteket idézve játsszák ki a különböző állami és nemzetközi szabályokat, hivatalos közegeket. A megnövekedett konténeres hajóforgalom bonyolult rendszereinek megtévesztésével terrorszervezetek vagy nemzetközi bűnszervezetek előszeretettel használják a tengeri dimenzió nyújtotta tranzitlehetőségeket. Ezek esetleges kombinálása a különböző tömegpusztító fegyverek csempészetével és alkalmazásával stratégiai fenyegetést jelent a nyugati demokráciák számára. Tekintettel arra, hogy a tömegpusztító fegyverek elterjedését megakadályozni hivatott exportellenőrző rendszerek nem egységesek, a nemzetközi közösségnek e téren is komoly feladatai vannak. A fehér foltok

megszüntetése és az operatív válaszok biztosítása érdekében szükség lenne egy szuperrezsim létrehozására, amely integrálja a jelenlegi szervezetek mindegyikét. Egy ilyen globális alapon szervezett, minden állam által támogatott kontrollszervezet tudna csak hatékonyan fellépni a globális közös terek mindegyikén.

Összességében megállapítható, hogy véges nyersanyagforrásaik, ugyanakkor a világtengerek stratégiai összekötő szerepe miatt alapvetően minden állam, még a tengeri kijárattal nem rendelkezők, valamint a nem állami szereplők is növelni kívánják befolyásukat ebben a dimenzióban. Jóllehet ma még erősen kétséges, hogy az ember képes-e kontrollálni a technológiai fejlődés vagy az annak következtében tapasztalható globális felmelegedés világtengerekre gyakorolt hatásait, e folyamatok együttesen folyamatosan és dinamikusan növelik a tengerek, óceánok jelentőségét a világpolitikában éppúgy, mint az iparban, a kereskedelemben vagy a katonapolitikában.

## A légtér

Az emberiség által nem sokkal több, mint egy évszázada használt légi dimenzió jóval szabályozottabb a tengerinél. Ennek oka, hogy terjedelme véges, jól definiálható, s aktív használatára már napjainkban került sor, így kellő jogi tapasztalat, technológiai háttér állt rendelkezésre a szabályozásra. Hasonlóan a tengereknél alkalmazott nemzetközi jogi szabályzókhoz, az államok saját, szuverén légtérrel rendelkeznek, míg a szerződések által deklarált nemzetközi légtér – a vonatkozó szabályzók betartása mellett – mindenki által használható. A nemzetekhez nem tartozó légteret különböző zónákra osztották, amelyekhez speciális használati jogosultságok tartoznak attól függően, hogy az adott övezet mekkora méretű, milyen közel fekszik a szárazföldhöz, és milyen a repülőeszköz-befogadóképessége. A légi dimenzió fizikai felhasználói leginkább a személy- és teherszállító repülőgépek. A légitársaságok több mint három milliárd utast, míg a teherrepülőgépek a világ nagy értékű termékeinek mintegy nyolcszázalékát szállították 2009-ben.

Az Egyesült Államok ellen 2001. szeptember 11-én elkövetett terrortámadások egyértelműsítették a légi dimenzió biztonságpolitikai jelentőségét. A nemzetközi légtér használatára vonatkozó szabályok drasztikus szigorítása azonban nem teremtett egyértelműen nagyobb rendet. A rendkívül körülményes új biztonsági előírások, illetve a további terrortámadásoktól való félelem következtében erősen visszaesett a légitársaságok forgalma, több légitársaság is tönkrement, ami jelentős nemzetgazdasági károkat okozott. A szigorítások nem vagy csak nagyon kevéssé korlátozták viszont a könnyű repülőeszközök fejlődését, használatát. Míg a vezető nagyhatalmak a globális légi forgalom rendszabályozásán dolgoztak, addig a könnyű légi járművek fejlődése és a rakétatechnológia elérhetősége látványosan liberalizálódott. A légi dimenzióban jelentkező veszélyforrások súlypontja tehát azon könnyű légi járművek és a rakéták irányába mozdult, amelyek mint hordozó- és célba juttató eszköz jöhetnek számításba.

A NATO a megalakulása óta meghatározó szereplője és felhasználója a légi dimenziónak. A hidegháború befejezése óta legfőbb feladata a légtérellenőrzés, amellyel a szövetségesek légterének szuverenitását, valamint a folyó műveletek légi támogatását biztosítja. E feladat azonban napjainkban rendkívül összetetté vált, hiszen az egyes tagállamok eltérőképpen értelmezik a vo-

natkozó szövetségi jogosultságokat. Míg a nagy és régi tagok többsége nem adja át légtérfelügyeletét a szövetségi rendszereknek, addig számos új tag – eszközök és a fenntartás, üzemeltetés forrásainak hiányában – szinte csak a NATO-ra támaszkodik. E különbözőségek kiegyenlítése és a NATO-követelmények homogénné tételének igénye regionális légtér-felügyeleti rendszerek kialakításához vezetett. Ilyen például az 1998 óta sikeresen működő Balti Egyesített Légtérellenőrző Rendszer *(Baltic Joint Airspace Surveillance Network – BaltNet)*. Ezzel ugyan nem jött létre egységes követelményrendszer az egyes tagokkal szemben, viszont azon légterek is NATO-felügyelet alá kerültek, amelyeket bizonyos államok – erőforrás hiányában – nem képesek ellenőrizni.

Elméletileg a 2001. szeptember 11-i terrortámadások is a NATO reagáló képességének paralízisét igazolták, hiszen a szövetség védelmi rendszere nem volt képes megelőzni egy tagállama elleni terrortámadást. Napjaink negatív példája a 2010 tavaszán kitört izlandi vulkán esete, amely több mint két hónapra lebénította a transzatlanti és európai légtérhasználatot. A vulkánkitörés rávilágított arra, hogy a NATO és tagországainak rendszerei – elsősorban kompetenciaviták miatt – nem minden esetben tudtak együttműködni. Pozitív, hogy e problémák kiküszöbölésére a szövetség egy olyan integrált rendszer kialakításába kezdett, amely alapvetően a gyors koordináción és a hatósági jogkörök rugalmasabb átadásán alapszik. Valószínűsíthető, hogy ennek életbeléptetése után nagyban felgyorsul a NATO és tagországai reagáló képessége a meglepetésszerű csapások esetén.

Azoknak a kommunikációs, informatikai, felderítő és egyéb rendszereknek a részletes leírására e helyütt nincs módunk, amelyeknek elektromos jelei állandóan jelen vannak a légi dimenzióban. Ide tartoznak például az olyan katonai rendszerek is, mint például a kommunikációs, az információátviteli, a navigációs, a felderítő, a precíziós célkövető, irányító, rávezető, a korai előrejelző és figyelmeztető vagy a meteorológiai berendezések. Mivel alapvetően egyfelől elavult nemzetközi jogszabályok, másfelől széles technológiai lehetőségek jellemzik, e terület a rosszhiszemű felhasználók számára vonzó lehetőségeket jelent.

Összességében megállapítható, hogy a légi dimenziót illetően mindmáig ellentmondásos folyamatok zajlanak, amelyek feloldásához mielőbbi nemzetközi összefogás szükséges. Bebizonyosodott, hogy a szeptember 11-i terrortámadások nyomán foganatosított biztonsági rendszabályok szabályozták ugyan a légi dimenzió körülményeit, sok részterületen azonban túlzónak bizonyultak. Az egy évtizede hozott szigorú szabályzók nem elsősorban a rosszhiszemű felhasználókat sújtották, így kijelenthető, hogy a terroristák sokkal nagyobb másodlagos – anyagi – károkat okoztak ezekkel a támadásaikkal, mint a direkt veszteségek, ugyanakkor a technológiai fejlődéssel további olyan légi járművek, elsősorban könnyű repülőeszközök, rakéták váltak elérhetővé számukra, amelyek előállítása olcsó, nehezen követhető, ugyanakkor – mint hordozóeszközök – akár hasonló stratégiai veszteségeket képesek okozni.

## A kozmikus tér

Az emberiség űrbe történő kijutása a légtérhasználatból levont minőségi tapasztalatokkal és a technológiai fejlődéssel vált valóra. Az űr megnyílása az emberiség számára gyökeres változásokat eredmé-

nyezett a földi élet minden területén. A légtér és az űr felhasználása ma döntő jelentőségű a béke- és a háborús tevékenységek kimenetele szempontjából.

A korábbi évtizedekben a kozmikus tér csak néhány, a technológiai fejlettség megfelelő fokán álló ország számára volt elérhető. Az elmúlt 20-25 évben azonban nagy változás tapasztalható, ami tulajdonképpen a globalizációval együtt járó növekvő gazdasági, kereskedelmi és információs igényeknek köszönhető. Az űr gazdasági és kereskedelmi kolonializálása olyan gyorsan kezdődött és terjed, hogy azt a nemzetközi jogi szabályzók csak felületesen és késve képesek követni. Az űrtechnológiák hihetetlen iramú fejlődésével, valamint a civil és katonai rendszerek űrbe telepítésével egyidejűleg hatványozottan nőtt ezen eszközök, s különösen az ezeken alapuló globális rendszerek sebezhetősége.

Napjainkban mintegy 18 ezer ember által előállított termék, szerkezet van jelen az űrben, ezek közül 1300 műhold, amelyeket 40 ország üzemeltet. Földünk országai közül tíz képes arra, hogy önállóan műholdat juttasson az űrbe. Ma civil, katonai, privát vagy szövetségi szereplők használják a kozmikus teret. Közülük messze a civil gazdasági, kereskedelmi entitások szerepe a domináns. Ez még akkor is így van, ha – a technológiai háttér hiányában – szinte kivétel nélkül állami vagy katonai eszközöket és létesítményeket kénytelenek igénybe venni az űrbe juttatáshoz vagy eszközeik irányításához. A kozmoszba kijuttatott műholdak túlnyomó többsége információtovábbító, felderítő vagy valamilyen elektronikus jeladó feladatot lát el (például tv- ,meteorológiai, GPS-, kép- és más jeltovábbító szerkezet). Kutatók egybehangzó véleménye szerint a műholdak szerepe annak ellenére növekszik a jövőben, hogy rendkívül költségesek, s a földi információtovábbítást biztosító rugalmas optikai kábelek a kozmikus rendszerek töredékéből kiépíthetők. A műholdak egyértelmű előnye, hogy a vezeték nélküli technológián alapulnak, és elérik a föld minden szegletét.

Mind gyakrabban bizonyosodik be, hogy az 1960-as években köttetett és máig is érvényben lévő szerződések napjainkra elavulttá váltak. Az űr felhasználásának akkori körülményekhez igazított alapvetéseit, így a szabad felhasználás és a nemzeti felelősségek princípiumát írják le. E szabadság azonban azt eredményezte, hogy az állami és polgári felhasználók egyfelől telítették a földközeli kozmoszt, másfelől szinte gátlástalan konkurenciaharcot vívnak. További probléma, hogy az újonnan megjelenő magán és civil szereplők nem minden esetben követik az államok által megkötött szerződéseket. Bizonyos államok megengedték saját cégeik űrtevékenységének fejlődését, így kijátszva a nemzetközi szerződéseket, azt követően pedig, hogy már megjelentek az űrben, politikai és nemzetközi jogi nyomással próbálják szigorítani a feltételeket másokkal szemben, így erősítve saját, már megszerzett előnyeiket.

Az űrben fellelhető eszközök biztonságát illetően a helyzet tragikus. Ma már akár egy nem állami szereplő is képes olyan támadó rakétát készíteni, amely műholdakat tud megsemmisíteni. Még nagyobb probléma, hogy egy ilyen jellegű támadás esetén a mai irányító, követő berendezések nem tudják biztosan igazolni, hogy az adott esemény támadás vagy egyszerű meghibásodásból fakadó megsemmisülés volt-e. Mivel a rádióelektronikai lefogás, félrevezetés eszközei már a nem állami entitások számára is elérhetők, az űreszközök kontrollja és a rosszhiszemű támadások kiszűrése nagy kihívás elé állítja az állami szerveket. Ezért azt is nehéz meg-

mondani, hogy pontosan mikor kezdődött, vagy végződött egy-egy támadás. Az űreszközök sérülékenysége és a megbízható garanciák hiánya következtében az űrben elhelyezkedő rendszerek alapvetően instabilak, ami összességében bizonytalan működést eredményez.

A NATO számára az űrképességek fejlesztése alapvető fontosságú a döntési fölény megtartása érdekében. A kozmikus tér jelenleg ismert szerkezete rendkívül vegyes jellemzőkkel bír, hiszen léteznek nemzetközi szervezetek, államok által, valamint már privát entitások által birtokolt területek is. Megfigyelhető az is, hogy a különböző állami és katonai igények kielégítésére civil cégeket bíznak meg. Ezzel szorosabbá válik az állami és a magánszféra kapcsolata, illetve fokozatosan nő egymásrautaltságuk is. A kozmoszban fellelhető civil és állami érdekeltségek védelme tehát lassan, de biztosan bekerül a katonai feladatok közé.

A hadvezetés illetékes szerveinek tehát világosan érteniük kell e rendszerek teljes működését, és műveleti tervekkel kell rendelkezniük azok védelmére. Mivel az űrdimenzió felhasználása rendkívül komplex, a katonai megoldásoknak is átfogónak kell lenniük, amelyek figyelembe veszik a civil és kereskedelmi szereplők érdekeit is. Tény mindazonáltal, hogy mindennek ellenére csak kevés államnak van ilyen stratégiája, és a NATO-nak sincs olyan koncepcionális dokumentuma, amely világosan meghatározná a hadsereg számára fontos űrbeli eszközöket, számba venné az azok elleni támadások lehetőségeit, és szabályozná a konkrét katonai feladatokat. Az ISAF-misszió mindennapi tapasztalatai, különösen a stratégiai felderítés, kommunikáció és vezetés-irányítás elektronikai támogatása terén folyamatosan jelentkező problémák mindinkább sürgetőbbé teszik az űrdimenzió felhasználásának katonai aspektusait szabályzó stratégiai dokumentum kiadását. Tekintettel arra, hogy ez számottevő anyagi és szervezési feladatokat von maga után, széles katonai szakértői bázis létrehozása szükséges a műveleti felhasználóktól a haderőtervezőkön át az elektronikai vagy logisztikai támogatókig.

## A kibertér

A kibertér bizonyos szempontból a legegyedibb a négy dimenzió közül, hiszen nem jellemezhető csak fizikai vagy földrajzi fogalmakkal. Ugyanakkor nagyban függ fizikai eszközöktől, technológiáktól, számítógépektől, szerverektől, termináloktól, kábelektől, antennáktól, műholdaktól, amelyek már nem virtuálisak, hanem birtoklásuk és helyük is meghatározható. Mihelyt egy információ útjára indul a mesterségesen kialakított csatornákon, 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 információforgalom már ma is több milliószor megy végbe óránként a világban, miközben mennyisége és minősége hatványozottan fejlődik. Egyértelműen prognosztizálható: a kibertér rendszerei egyre nagyobbá, gyorsabbá és komplexebbé válnak.

A kibertér sebezhetősége pontosan komplexitásában rejlik, 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 virtuális rendszereket támadták. Ez azonban erőteljesen változik. A többi dimenziótól eltérően a kibertér információbázisa és technológiai infrastruktúrája túlnyomó részt civil és kereskedelmi szereplők tulajdonában van. A kibertér ezért elsősorban nem államoktól, 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. 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 utolsósorban olcsóbb fenntartást biztosít számukra. Pontosabban: a külső szabályzókból fakadó kötelezettségek szigorú betartása helyett saját biztonságukra és fejlesztésekre költenek. Amennyiben ez a paradox helyzet így marad, az államok – nemzetközi jog által biztosított – kontrollszerepe folyamatosan gyengül, s a kibertér még inkább anarchikussá válik.

Az extrémitások, szabályozatlanságok és veszélyek egyik legjobb példája a 2010 őszén kirobbant Wikileaks-botrány. Az internetes szolgáltató és támogatói arra szakosodtak, hogy bizalmas vagy akár szigorúan titkos információkat tegyenek közzé, függetlenül attól, hogy azok egyéni, cég- vagy kormányzati forrásból származnak. Mivel e tevékenység súlyos károkat és érdeksérelmet okozott számos civil cégnek és államnak egyaránt, a sértettek nagyszabású ellenkampányba kezdtek. Jelenleg nagy intenzitású és szerteágazó hackertámadás, kormányzati felderítő művelet, rendőrségi eljárás, diplomáciai koordináló tevékenység, valamint gazdasági-pénzügyi ellehetetlenítés folyik a wikileaks.com ellen. Valószínűsíthető, hogy az állami érdekeket ért támadás az állami védekező mechanizmusok megszilárdításához, köztük a titkosszolgálati informatikai képességek fejlesztéséhez fog vezetni.

Katonai szempontból a 2007 májusában, Észtország ellen észlelt kibertámadás, illetve a 2008 nyarán kirobbant orosz–grúz konfliktus szolgáltatja a legutóbbi tanulságot. Az Észtország ellen indított informatikai támadást ma az elemzők a hadtörténelem első nagyszabású, országok között zajló „kiberháborújának” nevezik. A Tallinn elleni kiber-haditerv egy úgynevezett DDOS-támadás volt, amely az informatikai rendszerek túlterhelését és ezáltal 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 képesek. Mivel Észtország kérte a NATO Tanács összehívását, az incidens kivizsgálására széles körű 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 világ különböző helyein telepített ideiglenes szerverekről érkeztek. Csak gyanítható, hogy az akció mögött valójában orosz kormányhivatalok álltak.

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 kiberrendszerek ellen, aminek következtében a civil nyílt és a minősített kormányzati informatikai hálózatok is összeomlottak. Ez esetben nemcsak a virtuális rendszereket támadták, hanem a fizikai infrastruktúrát is. Mindez hosszú időre lebénította a grúz kormányzat teljes egészének védelmi képességét. Túlzás nélkül kimondható, hogy hasonló akciók még az olyan államok védelmi rendszereit is tönkretehetik, mint a NATO vezető hatalmaié, nem beszélve arról, ha ezeket konkrét fegyveres cselekmények is követik.

Az informatikai rendszerei elleni folyamatos támadásokra válaszul a NATO 2009-ben kiadta kibervédelmi koncepcióját, amely komplexen leírja a virtuális és fizikai infrastruktúrák védelmét, valamint szól azon területekről is, amelyeket a NATO érdekövezetébe sorol. Az informatikai rendszereit ért támadások mellett azonban a technológiai fejlődés nyomása is nagyban inspirálta a döntéshozókat. A NATO vezetése már évekkel ezelőtt felismerte, hogy a digitalizált had- és műveleti vezetésre való áttérés ma már alapkövetelmény, amelynek alapvetéseit és védelmét a legmagasabb szintű koncepcionális dokumentumoknak is tartalmazniuk kell. 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. Mindebben az emberi tényezőt tarja a legfontosabbnak, hiszen minden kibertámadás és annak kivédése mögött is elsősorban emberi tevékenység áll. A védelem szempontjából tehát mindennél fontosabb a NATO-felhasználók, rendszerfenntartók és rendszergazdák képzése, felkészítése.

## Következtetések

A globalizáció teremtette versenyhelyzet továbbra is ráirányítja a figyelmet az ember ambíciójából és a földi erőforrások korlátozottságából fakadó paradox helyzetre. Ennek direkt következménye a tudomány által ismert és az ember által használt térbeli határok áttörésére, kiszélesítésére irányuló törekvések. A technológiai innovációval, a túlnépesedés fokozódásával, a természeti változások szélsőségessé válásával, az erőforrások apadásával az emberiség új fizikai, és immár virtuális terek meghódítására tesz kísérletet. A globális közös terekben rejlő források és lehetőségek kiaknázását nevezhetjük a kolonializáció egy újabb állomásának.

A NATO elsősorban a globális közös terekben rejlő lehetőségeket és veszélyforrásokat vizsgálja, és nem az ott található erőforrások kiaknázására törekszik. A lehetőségek vonatkozásában a globális közös terek használata, míg a kockázatok kapcsán az onnan érkező fenyegetések, illetve az azokon stratégiai előnyökre szert tevő entitások erőviszonyaira figyel leginkább. Ami a globális közös terekben rejlő lehetőségeket és azok biztonsági körülményeit illeti, NATO-szempontból úgy is tekinthető, hogy

az sok tekintetben azonos a NATO biztonságával, hiszen jelentős átfedések tapasztalhatók az egyes dimenziók és az északatlanti, valamint azon térségek között, ahol a NATO műveleteket folytat. Minden, ami a négy dimenzióban történik, direkt befolyással lehet a szövetség egészére éppúgy, mint tagországaik mindennapi tevékenységére. A globális közös terekre való kijutás, használatuk mindenkori biztosítása és stratégiai kontrolljuk ezért elemi fontossággal bír a szövetség számára.

A tengeri és légi dimenzió tekinthető a NATO két legerősebb területének, hiszen a hatvankét éves, mára hegemónná vált katonai szövetség meg tudta őrizni dominanciáját e területeken. A NATO helyének, szerepének meghatározása az űrt és a kibertért illetően további döntés-előkészítést igényel. A szövetség katonai potenciáljának és fejlett technológiai fegyverrendszereinek köszönhetően a kozmosz vonatkozásában növelni tudja befolyását. Abban az esetben, ha az ENSZ-szel és az EU-val közösen lép fel, domináns szereplője lehet a világűrben való felelősségteljes tevékenység és viselkedés gyakorlatának ellenőrzésében, esetleg a devianciák elrettentésében, büntetésében. A legnyitottabb kérdés, hogy miképpen alakuljon a kapcsolata az informatikai térhez. Tekintettel arra, hogy ma ez a legdinamikusabban fejlődő és bővülő dimenzió, kellő tapasztalat hiányában ez jelenti a legtöbb veszélyforrást is a szövetség számára.

Katonai szempontból a műveletekben részt vevő alakulatok vezetése, utánpótlása és a hátországgal történő mindennemű kommunikáció is e globalizált rendszerhálózaton történik. A ma ismert hibrid hadviselés módszereivel és eszközeivel, vagyis bármilyen hagyományos és nem hagyományos fegyver megfelelő kombinációjával – például a különleges hadviselés adta széles körű taktikai lehetőségekkel, relatíve kis ráfordítással – nem állami szereplők akár stratégiai károkat is képesek okozni a szövetség rendszereiben. Ismertek például olyan fegyvergyártók, akik a jelen kor civil technológiáit továbbfejlesztve akár anyahajó megsemmisítését is garantálni képes kisméretű robotrakétákat *(missiles-in-a-box)* árulnak az interneten. Mivel ezek elérhetők a rosszhiszemű felhasználók számára is, a technológiai fejlődésben rejlő veszélyforrások felderítése, korlátozása és elhárítása komplex, nemzetközi összefogást igényel.

Összességében megállapítható, hogy a globális közös tereknek a NATO jövőbeni sikeres működése szempontjából meghatározó szerepe van. A négy dimenzióban a NATO csak akkor lehet sikeres, ha világos koncepciók mentén megfogalmazza érdekeit, s érvényesítésüket széles és intenzív külkapcsolati gyakorlattal párosítja. Az ENSZ, az EU, az EBESZ, más nemzetközi szervezetek, valamint a világpolitikában súllyal szereplő hatalmakkal történő partnerség és együttműködés nagyban elősegítheti a NATO vezető szerepének kiteljesedését. A NATO ugyanis már régóta nem vezeti és nem is kontrollálja a globális technológiai fejlődést, viszont – mint egyedülálló globális katonai szövetség – szilárd politikai és katonai garanciákat képes nyújtani a nemzetközi jogi és technológiai rendszerek biztonságához. E tényből fakadóan – némi előkészítő és szervezőmunka után – akár vezető szerepet is vállalhatna a globális közös terek rendjének és biztonságának szavatolásában. A jelenlegi történések egyértelműen azt mutatják, hogy nyitott erre, hiszen a téma feldolgozását rendkívül széles nemzetközi közreműködéssel kezdték meg. Ennek későbbi pozitív hatása lehet, hogy a sok entitás, ország, kutatóintézet, vállalat meghívásával, szempontjaik

harmonizálásával olyan egységes (összekovácsolt) nemzetközi álláspont alakul ki, amelyet a nemzetközi jog által elismert entitások legtöbbje nemcsak magáénak érez, hanem ki is áll mellette. Ha pedig ez tartós marad, bizton állítható, hogy a szövetség alkalmazhatja kapacitásait a négy dimenziót illető törvények betartatására, illetve a törvénysértők szankcionálására. ■

## Felhasznált irodalom

Ziad I. Akir: Space Security: Possible Issues & Potential Solutions. *Space Journal,* Issue 6, 2004.
The Netherlands Atlantic Association: NATO and Cyberspace, Mission
Accomplished? *Atlantisch Perspectief,* No. 1, 2009.
The Economist: War in the fifth domain. July 2010.
Security & Defence Agenda: Cyber Security: A Transatlantic Perspective. April 2010.
United States Joint Ciefs of Staff – J5: Global Maritime Security
Cooperation in an Age of Terrorism and Transnational Threats at Sea Multilateral Planners Conference (MPC) VI. May 2008.
Council of the European Union: Coucil Conclusions on Maritime Security Strategy. April 2010.
Royal United Services Institute for Defence and Security Studies (RUSI): Building Global Maritime Security through Global Cooperation.