HADMÉRNÖK

XI. Évfolyam 3. szám - 2016. szeptember

Tóth András
toth.hir.andras@uni-nke.hu

A PRÁGAI NATO CSÚCSTALÁLKOZÓT KÖVETŐ HATÁROZATOK, MEGÁLLAPODÁSOK A PARANCSNOKI RENDSZER- ÉS A VEZETÉSI RENDSZER KORSZERŰSÍTÉSÉRE, VALAMINT AZ EGYÜTTES TEVÉKENYSÉG KÉPESSÉG FEJLESZTÉSÉRE

Absztrakt

A NATO prágai csúcstalálkozóját követően a szövetség nagy hangsúlyt fektetett a hálózat nyújtotta képességének fejlesztésére, amely idővel képessé vált a szövetséges műveletek teljes spektrumában az információk megbízható módon, biztonságosan és késedelem nélkül történő megosztására. Ezzel egy időben különböző védelmi rendszereket alakítottak ki úgy, mint például a NATO rakétavédelmi rendszer. A találkozók alkalmával egyre nagyobb hangsúlyt kapott a kibervédelem, az arra való képességek gyors kialakítása a kritikus információs rendszerek védelme érdekében.

After the NATO Prague Summit the alliance focused on the development of the network enabled capability, with witch the members are able to to share the information safely and in near real time in the full spectrum of operations. At the same time different defence systems were installed, such as the NATO missile defence system. NATO started to focus on the cyber defence during these summits, to carry out the capabilities of the protection of the critical information networks.

Kulcsszavak: *NATO, csúcstalálkozó, hálózat nyújtotta képesség, védelmi rendszer, kibervédelem ~ NATO, summit, network enabled capability, defence system, cyber defence*

BEVEZETÉS

Vizsgálataim során átnéztem a 2002-es prágai csúcstalálkozót követő NATO állam és kormányfői találkozókat. Számos esetben találtam olyan döntéseket, határozatokat, melyek a fenti fejlesztések, korszerűsítések egyikére vagy akár egészére vonatkozik, illetve azok védelmére irányul. Különösen nagy hangsúly került az elmúlt pár évben a kibervédelemre,

amely napjainkra operatív területté vált, és szintén vonatkoznak rá a NATO 5. cikkelyben megfogalmazottak.

NATO ÁLLAM ÉS KORMÁNYFŐI TALÁLKOZÓK

Isztambul (2004. június 28-29.)

A csúcstalálkozón a XXI. századi műveletekhez való alkalmazhatóságot és a felhasználhatóságot helyezték előtérbe, amely értelmében komplexebb hozzájárulást (szárazföldi, haditengerészeti, légi) követeltek meg a tagországoktól. Az afganisztáni nemzetközi erők fokozottabb támogatását sürgették, amely a közelgő választásokat volt hivatott biztosítani. Ennek megfelelően kellett a helyi erőket felkészíteni mind képességben, mind technikai eszközökkel a megfelelő biztosítás érdekében. Az együttműködési képességek további megerősítése nélkülözhetetlen volt a sikeres műveleti feladatok ellátásában, amelyre nagy hangsúlyt kellett fektetni a misszió többnemzeti jellegéből adódóan. Korszerű technikai eszközökkel felszerelt, új vezetés-irányítási elvekkel rendelkező, „használhatóbb", telepíthető alegységek megszervezésére volt szükség, amelyek felállítása a nemzetek feladata, és lehetséges alkalmazásuk segíti elő a Szövetség elkötelezettségét a nemzetközi béke és stabilitás iránt. [1]; [2; p.19.]

Riga (2006. november 28-29.)

Fontos kérdéskör volt a találkozón a terrorista akciókra történő fellépés új dimenziói. Előtérbe kell helyezni a legmodernebb technológiai eszközök alkalmazását, amelyek képesek megerősíteni az ellenséges erők új típusú támadásaira történő hatásos reagálást, illetve a megelőzést. Mindezek érdekében minden nemzetnek folyamatos fejlesztéseket kell végrehajtania, amelyek tovább erősítik a Szövetség katonai képességeit. A rigai-csúcson ismételten kihangsúlyozták a mobilitás kérdéskörét, amely elengedhetetlenül fontos eleme a hatékony, időbeli reagálásnak. Ezen a csúcsértekezleten ismét megfogalmazásra került a hálózat nyújtotta képesség egyre növekvő igénye, amely alapvetően a műveletekben résztvevő Szövetséges erők között az információk megosztását, és azok megbízható, gyors és biztonságos továbbítását jelenti, illetve azok védelmét a számítógépes hálózatok elleni támadások során. A gyorsreagáló képesség további fejlesztése, valamint az NRF erők felállítása, biztosítása a későbbiekben is jelentősnek bizonyult a követelményeknek való megfelelésben. [3]; [2; p.19.]

Bukarest (2008. április 2-4.)

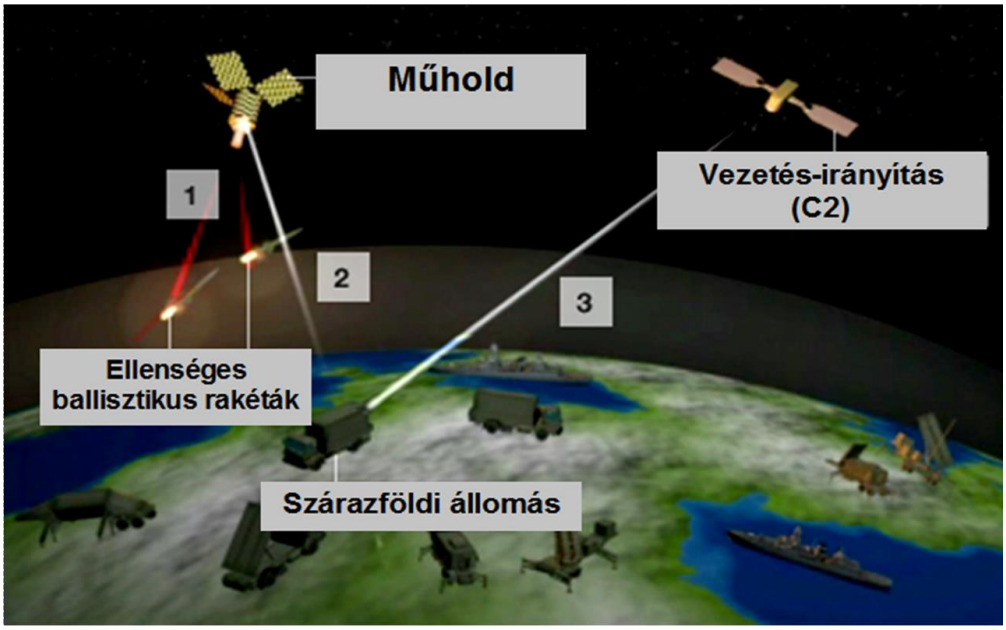
Kiemelték a terrorizmus elleni fellépés fontos elemének, a hírszerzésnek és az információcserének a megerősítését, amely hatékony alkalmazása tovább erősíti a NATO műveletekben résztvevő erők jelenlétét, védelmét. Egyetértés született a hálózat nyújtotta képességek megerősítésére az információs fölény kivívása érdekében, amely integrált vezetés-irányítási rendszert követel meg a nagyobb hatásfokú művelet-végrehajtás érdekében. A NATO továbbra is elkötelezett a szabványosítás és magas fokú együttműködő képesség fejlesztése, és az informatikai hálózatok megóvása, biztonságának növelése területén. [4]; [2; p.20.]

Strasbourg–Kehl (2009. április 3-4.)

Az egyeztetések értelmében megállapodás született, hogy továbbra is kiemelten kell kezelni és folytatni az addigi technológiai fejlesztéseket, és nagy hangsúlyt kell fektetni a NATO missziók támogatása érdekében az információszerzésre, és a megszerzett adatok megosztására. A telepíthető, fenntartható, rugalmas erők alkalmazását tovább kell erősíteni, és törekedni kell az esetleges hiányosságok megszüntetésére. A Szövetség és a tagországok informatikai hálózatainak nagyobb védelme érdekében az informatikai- és kommunikációs eszközök fejlesztésére különös figyelmet kell fordítani. [5]; [2; p.21.]

Lisszabon (2010. november 19-20.)

A találkozó során megállapításra került, hogy a kibertámadások, melyek a Szövetség egészét vagy csak egyes tagállamait érhetik egyre gyakoribbak, szervezettebbek és jelentős anyagi kárral járnak. A támadások többsége a kormányok adminisztrációs, gazdasági, szállítási, valamint utánpótlási hálózatait éri, és számos esetben egyéb kritikus infrastruktúrák rendszereibe is megpróbáltak sikeresen vagy sikertelenül behatolni. Ezt felismerve a vezetők megállapodtak, hogy szükséges egy a képességek teljes spektrumában alkalmazható védelmi rendszer kialakítása, amely képes felismerni az ilyen típusú támadásokat és megvédeni a hálózatokat. Ehhez megkezdték a nemzeti kibervédelmi képességek kialakítását, mellyel a NATO tagállamok egy központosított, integrált kibervédelmi rendszerbe tömörülnek. Az elfogadott dokumentumban kiemelt helyen szerepel egy a vezetés-irányítási rendszer részeként működő rakétavédelmi rendszer alkalmazása. Ez lehetővé tenné a NATO európai tagországai, valamint az Amerikai Egyesült Államok és Kanada elleni külső ballisztikus rakétákkal végrehajtott támadás elleni védelmet.



1. ábra: A NATO rakétavédelmi terve [6]

A rendszer működése a fenti ábrán látható, ahol a számozás mutatja be az információ áramlását:

1. Az infravörös műholdrendszer érzékeli az ellenséges ballisztikus rakéták hősugárzását.
2. A műholdas információt eljuttatják a szárazföldi állomásra.
3. A feldolgozott információt továbbítják a NATO vezetési és irányítási (C2) hálózatához.

2012. Chicago (2012. 05. 20-21.)

A találkozón továbbra is a dinamikusan változó biztonsági környezet által támasztott követelményeken volt a hangsúlyt, de súlyos problémaként merült fel a pénzügyi források szűkössége. Erre reagálva megalkották az okos védelem[1] koncepciót az elégséges források biztosításához, melynek alapjait a NATO Erők 2020[2] dokumentumban fektettek le. A cél továbbra is a modern, rugalmasan akár stratégiai távolságban is bevethető, interoperábilis erők fenntartása és fejlesztése, melyre a többnemzeti képességfejlesztési programok és együttműködés jelentenek megoldást. Fő feladatként a NATO stratégiai koncepciója által a képességek erősítése került meghatározásra, melyek szükségesek a lakosság védelméhez, a válságkezelési műveletekhez és a kollektív biztonsághoz. Ehhez néhány a téma szempontjából kulcsfontosságúnak mondható elem kialakítása már megkezdődött.

- Ilyen például a ballisztikus rakétavédelmi képesség, ami az első lépésként létrehozott NATO rakétavédelmi rendszer, amely megvédi a NATO-európai területeit, a lakosságot és az erőket a ballisztikus rakéták elterjedése által okozott növekvő fenyegetések ellen.
- Egy kifinomult szövetséges földi megfigyelő[3] rendszer kerül kiépítésre, abból a célból, hogy a feladatot végrehajtó erők jobban és nagyobb biztonsággal végezhessék küldetéseiket. Ennek érdekében számos szövetséges állam által elkezdődött egy kezdeményezés az összhaderőnemi hírszerzési, megfigyelési és felderítési[4] rendszerek korszerűsítésére, fejlesztésére.
- Az összekapcsolt haderők kezdeményezés[5], melynek célja hogy erősítse a legmagasabb szintű összekapcsolódási és az interoperabilitási lehetőségeket a szövetséges erők részére a műveletek során, és ennek segítségével képesek legyen a feladatban résztvevő partnerek az együttműködésre. Ehhez olyan jól felszerelt és kiképzett erőkre van szükség, melyek bármilyen környezetben bevethetőek, és képesek együtt tevékenykedni, valamint feladatot végrehajtani más csapatokkal egy interoperábilis környezetben. [7]

[1] Smart Defense
[2] NATO Forces 2020
[3] Alliance Ground Surveillance
[4] Joint Intelligence, Surveillance and Reconnaissance - JISR
[5] Connected Forces Initiative – CFI

2014. Wales (2014. 09. 4-5.)

A csúcstalálkozón központi szerepet kapó kollektív védelemi képességek megerősítésének központi eleme a rendelkezésre álló katonai képességek megerősítése, a NATO cselekvési potenciáljának, készenlétének fokozása. Ennek eszközei a 2010-es stratégiai koncepció és a 2011-ben elfogadott stabilizációs és válságkezelő műveleti képesség, az okos védelem program és a chicagói csúcstalálkozóra kialakított összekapcsolt haderők kezdeményezés program, valamint a 2013 őszén német kezdeményezésre induló keretnemzet koncepció[6]. A csúcstalálkozó idején már számos a vezetés-irányítást támogató képességfejlesztési projekt zajlott, mint például a szövetséges rakétavédelmi rendszer, a földfelszín-megfigyelési rendszer, az integrált légtérellenőrzés és az összhaderőnemi hírszerzési, megfigyelési, felderítési rendszer. Ismét napirendre került a kiberbiztonság. Felismerték, hogy egy kibertámadás hatalmas károkat képes okozni és képes veszélyeztetni az euroatlanti térség biztonságát és stabilitását. Meghatározásra került, hogy egy ilyen jellegű támadás a Szövetség irányába akár kollektív válaszhoz is vezethet, illetve a nemzetközi jog alkalmazható a kibertérben is. A probléma összetettségét mutatja, hogy erről a területről érkező fenyegetések túlnőnek a Szövetség határain, ezért a NATO szorosabb együttműködésbe kezdett az EU-val, az ENSZ-szel és más nemzetközi szervezetekkel is. A magánszektor is kulcsfontosságú szereppel bír a kibertérben, hiszen az innen áramló szakértelem és technológiai újítások elengedhetetlenek egy hatékony kibervédelmi rendszer létrehozásához. [8] Az összekapcsolt haderők kezdeményezés program keretében olyan interoperábilis technológiák kerültek kialakításra és alkalmazásra, mint a szövetségi küldetés hálózati keretrendszer[7], ami támogatja az információ-megosztást a Szövetségen belül, valamint a partnerek között, ezzel támogatva a kiképzést, a gyakorlatokat és a feladat-végrehajtást. [9]

2016. Varsó (2016. 07. 8-9.)

A találkozó folyamán az állam és kormányfők egyöntetűen kinyilvánították a kibertér operatív területté válása melletti elkötelezettségüket, ennek megfelelően azt elfogadták ötödik műveleti dimenziónak (szárazföldi, légi, tengeri, űr mellett). A kibervédelem megerősítése érdekében az új típusú fenyegetések ellen a szövetség kibervédelmi hozzájárulásokkal próbálja felvenni a harcot, valamint próbálják javítani az egyes tagállamok ellenálló képességeit. A találkozón megszületett egy új NATO-terminológiába illesztett fogalom, a resilience, ami ellenálló képességet, életképességet jelent. A kifejezés nem feltétlenül a kibertérrel kapcsolatban jelenik meg, sokkal inkább a kollektív védelem fontos eleme, amelynek erősítése minden fenyegetés (hibrid, kiber, CBRN, terrorista, hagyományos) szempontjából fontos. Kommunikációs és információs szempontból ez a folyamatos rendelkezésre állást, és a redundáns kialakítást jelenti, mely elengedhetetlen egy rendszer zavartalan működéséhez, annak egyes vagy akár több elemének sérülése, támadása esetén is. [10]

[6] Framework Nation Concept – FNC
[7] Federated Mission Networking framework

ÖSSZEGZÉS

2002. után a NATO csúcstalálkozók mindegyikén szóba került valamilyen módon a kommunikációs és információs rendszerek védelme. Számos olyan rendszer, jogszabály és intézkedés került megfogalmazásra, ami nagymértékben hozzájárul a tagállamok védelméhez. Ennek megfelelően született meg például a Rakétavédelmi megvalósíthatósági tanulmány[8]. A tanulmány tartalmazza:

- a Szövetség területe, erői és a lakosság elleni rakéta fenyegetések teljes körű védelmének vizsgálatát, valamint a lehetséges megoldásokat;
- az alkalmazásra kerülő NATO konzultációs, vezetés-irányítási rendszereket és architektúrákat;
- a legjobb NATO rakétavédelmi architektúrát, amely ötvözi a rendszereket és képességeket, melyekkel képes megfelelni a katonai műveleti követelményeknek, figyelembe véve a teljesítmény, a költségek és kockázat;
- javaslatokat a rendszerelemekre és azok konfigurációira úgy, mint szenzorok és vezetés-irányítási eszközök. [11]

A rakétavédelem mellett kialakításra került egy szövetséges földi megfigyelő rendszer a csapatok tevékenységének támogatásához. A NATO hálózat nyújtotta képességének fejlesztéséről is szó esett, melynek a fejlesztése a résztvevők szerint nagyon jó úton halad, és alkalmas a szövetséges műveletek teljes spektrumában az információk megbízható módon, biztonságosan és késedelem nélkül történő megosztására. A találkozók során folyamatosan szóba került a kibervédelem fontossága. Kimondták, hogy nem elegendő csak a NATO-nak fejlesztenie a kibervédelmi tervét, fontos, hogy a tagállamok mindegyike szintén nagy hangsúlyt fordítson rá, mivel az a teljes Szövetségre hatással van. Amennyiben egy állam rendszere nincs megfelelő szinten kiépítve az a teljes Szövetség sebezhetőségét okozza. Elfogadásra került a NATO kibervédelmi irányelv. Ez átdolgozott irányelveket fogalmaz meg, amelynek középpontjában a számítógépes fenyegetések megelőzése és az infrastruktúrák ellenálló-képessége áll. Minden NATO-struktúra központosított védelem alá kerül, és új számítógépes védelmi követelményeket fogalmaz meg. A dokumentum tisztázza a NATO politikai és katonai válaszait a számítógépes támadásokra. Meghatározza azokat a NATO kibervédelmi alapelveket, melyek szükségesek a partnerországokkal, a nemzetközi szervezetekkel, a magánszektorral való együttműködéshez.

Felhasznált irodalom

[1] Istanbul Summit expands operations, strengthens partnerships, improves capabilities: http://www.nato.int/docu/comm/2004/06-istanbul/home.htm (2016. 08. 19.)

[2] Farkas Tibor: A válságreagáló műveletek vezetését és irányítását támogató híradó- és informatikai rendszer megszervezése a Magyar Honvédség többnemzeti műveleteinek tükrében, PhD doktori értekezés, ZMNE, 144 p., 2010.

[8] Missile Defence Feasibility Study

[3] Summit meetings of Heads of State and Government, Riga, Latvia: http://www.nato.int/docu/comm/2006/0611-riga/index.htm (2016. 08. 19.)

[4] Summit meetings of Heads of State and Government, Bucharest, Romania: http://www.nato.int/docu/comm/2008/0804-bucharest/index.html (2016. 08. 19.)

[5] Summit meetings of Heads of State and Government, Lisbon Portugal: http://www.nato.int/docu/comm/2009/0904-summit/index.html (2016. 08. 19.)

[6] Csiki Tamás, Pocsarovszky Ráchel: A NATO lisszaboni csúcstalálkozójának eredményei: http://old.biztonsagpolitika.hu/?id=16&aid=958&title=a-nato-lisszaboni-csucstalalkozojanak-eredmenyei (2016. 08. 19.)

[7] Chicago Summit Declaration: http://nato.int/cps/en/natohq/official_texts_87593.htm ?mode=pressrelease (2016. 08. 20.)

[8] Goldfinger Klaudia – Torő Ágnes: A NATO walesi csúcstalálkozójának értékelése, Hadtudományi Szemle, 2014. VII. évfolyam 4. szám, ISSN 2060-0437, pp.: 267-290

[9] Wales Summit Declaration, Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Wales: http://nato.int/cps/en/natohq/official_texts_112964.htm?mode=pressrelease (2016. 08. 20.)

[10] Szenes Zoltán: Meglepetések nélkül, A varsói NATO csúcs értékelése, http://biztonsagpolitika.hu/kiemelt/meglepetesek-nelkul-a-varsoi-nato-csucs-ertekelese, (2016. 08 25.)

[11] NATO Missile Defence Advances,New Missile Defence Feasibility Study Reaches Major Milestone: http://www.nato.int/docu/pr/2003/p03-069e.htm (2016. 08. 25.)