Gerőfi Szilárd

A Magyar Honvédség vezetéstámogató rendszere alkalmazásának lehetőségei a XXI. századi kihívások tükrében

DOI 10.17047/HADTUD.2017.27.3–4.96

A Magyar Honvédség vezetéstámogató rendszere folyamatosan változik, fejlődik összhangban a rohamos technológiai fejlődéssel és az elmúlt évtizedekben kialakított korszerű hadviselési elvekkel. Az eszközök és eljárások fejlődése napról napra, évről évre nyomon követhető. A Magyar Honvédség híradó, informatikai és információvédelmi szolgáltatási tevékenységének módszerei, eszközei, valamint szakembereinek tudása, tapasztalata minőségileg új generációt képvisel a XXI. század fordulójához képest.

Az elmúlt 10 évben a hírközlés és informatika dinamikus fejlődésen ment keresztül, mellyel a Magyar Honvédség híradó, informatikai és információvédelmi szakszolgálata igyekezett lépést tartani, illetve, ha volt rá lehetősége, elébe menni.

Számos területen jelentős előrelépés történt: bevezettük a kormányzati rádiótelefon rendszert a tárcánál, erősödött a missziók híradó-informatikai támogatottsága, előrehaladt a harcjárművek híradó-informatikai eszközeinek cseréje, folyamatban van az MH nagytávolságú adatátviteli hálózat kapacitásának növelése és a tábori C2 szoftver fejlesztése, bővültek a központi informatikai szolgáltatások, fejlődtek az ágazati informatikai rendszerek. A hagyományos, papíralapon nyugvó dokumentumkezelés jelentős változás alatt áll, az elektronikus iratkezelés térhódítása eddig nem tapasztalt kihívás elé állítja a szakterületet és a felhasználókat.

Ugyancsak jelentős előrelépést hozott a HM-I híradó-informatikai központ teljes megújítása 2010–2012-ben a 2008. évi csőtörés okozta vízbetörés következményeinek felszámolása kapcsán. Az elmúlt évek kiemelkedő sikere a NATO szervezeti struktúrájába tagolt nemzeti, telepíthető híradó-informatikai század (Deployable CIS Modul – DCM) megalakítása Székesfehérvárott az MH Összhaderőnemi Parancsnokság bázisán, amely a szövetséges műveletek kommunikációját hivatott biztosítani a műveleti területen.

Az elmúlt évek szintén fontos kihívása a kibertérből érkező támadások elleni védekezés szervezet- és eszközrendszerének, eljárásrendjének és ezek alapjaként törvényi hátterének megszervezése. Ez a feladatrendszer a közeljövőben további

jelentős erőfeszítéseket igényel majd a szakemberek és a szakmán kívüliek részéről is. A folyamat a korábbiaktól gyökeresen eltérő szemléletmódot, szaktudást és módszert igényel, amelynek végig vitele az elkövetkezendő évek híradó-informatikai fejlesztései sikerének egyik záloga.

Az elmúlt időszak sokszor szűkös pénzügyi, logisztikai és humán feltételei mellett ugyancsak jelentős eredményként értékelhető, hogy a csökkentett tartalmú külső üzemeltetés-támogatás, a folyamatosan fogyatkozó – sok esetben hiányzó – cserekészülék és alkatrész, valamint a magas szintű tudást felhalmozó, tapasztalt mérnökállomány nagyfokú elvándorlása, fluktuációja ellenére sikerült biztosítani a híradó-informatikai rendszerek folyamatos működését, a szolgáltatások követelmény szerinti biztosítását, rendelkezésre állását.

Nem segítette munkánkat az elmúlt 10 éves időszak első felére különösen jellemző gyakori szervezet-átalakítás, amelynek során számos alkalommal kellett új szervezeti keretek között, nagyrészt megújult, és csökkenő létszámú állománnyal helytállni úgy, hogy a feladatok száma és komplexitása nőtt, a szakterületi felelősség és hatáskör több szervezet között oszlott meg, ugyanakkor a közös technikai alapok miatt szoros együttműködésre ítélt, összetartozó szakterületek eltérő szervezeti alárendeltségben tevékenykedtek. Ezzel együtt – a bonyolult körülmények ellenére – a vezetés híradó-informatikai támogatása javult, az infokommunikációs szolgáltatások színvonala emelkedett.

Mindezek alapján bizton állítható, hogy az elmúlt tíz évben az infokommunikációs szolgáltatások fejlődése a honvédelmi tárca eredményes tevékenységének egyik meghatározó tényezője volt.

A honvédség híradó szolgálatnak folyamatos fejlődése és hathatós tevékenysége nélkül a katonai informatikai rendszerek látványos bővülésére nem kerülhetett volna sor, hisz az adatok nagytömegű, nagysebességű továbbítása alapvető feltétele az informatikai szolgáltatások kiterjesztésének, színvonaluk emelésének. Napjainkra a két szolgálat eszköz- és feladatrendszere jelentősen közelített egymáshoz, a két szakterület szoros együttműködése nélkül nem megvalósítható a tárca tevékenységének hatékony támogatása. Mindez az utóbbi másfél évtizedben kiegészült az elektronikus információvédelemmel, amely a vonali rejtjelzésből a számítógép-hálózatok védelmének komplex, átfogó szakterületévé nőtte ki magát.

* * *

Az infokommunikációs rendszerek széleskörű alkalmazása nélkül nem létezik hatékony kormányzás, modern társadalom, korszerű haderő. A fejlett országok és haderők az utóbbi tizenöt-húsz évben fokozott mértékben függnek az informatikai rendszerek alkalmazásától, amely egyúttal a sérülékenységüket is jelentheti. A közigazgatási, banki, társadalombiztosítási, ingatlan-nyilvántartási, közlekedési, energetikai, rendészeti és nem utolsó sorban katonai informatikai rendszerek működésének zavarása, bénítása valamely ország működésének szétzilálása, hatalmi viszonyainak megváltoztatása szempontjából hasonló eredménnyel járhat, mint a hagyományos fegyverek által kiváltott csapások. Az országvédelemnek ezért a kibertérben is meg kell valósulnia. Ez jelenleg – sok más országhoz hasonló módon – Magyarországon sem katonai feladat, de vannak országok, ahol a haderő alá tartozó speciális szervezetek

feladata a kibertérből érkező támadások kezelése. A honvédelmi tárca infokommunikációs rendszerei védelmének megszervezése és végrehajtása a Magyar Honvédség alapvető kötelessége.

A globalizáció térhódítása, az országok és régiók kölcsönös függésének erősödése egyre inkább ellenérdekeltté teszi a rivalizáló feleket abban, hogy egymás ellen hagyományos pusztító eszközök és eljárások alkalmazásával közvetlenül érvényesítsék politikai és gazdasági törekvéseiket. Jelentős mértékben előtérbe kerültek a párhuzamos, egyeztetett politikai, gazdasági, pénzügyi, információs és diverzáns műveletek, amely a XXI. században kiegészült a terrorizmussal, mint a tömeges megfélemlítés (és azon keresztül a politikai befolyásolás) eszközével, valamint a kiberhadviselléssel, amelyet annak sajátos eljárásaiból fakadóan a politika a mai napig nem képes adekvát módon, kiforrott nemzetközi szabályok alapján kezelni. A NATO álláspontja, hogy a kibertérben is érvényesek a nemzetközi jog előírásai, azonban nem tisztázott, hogyan lehet azokat érvényesíteni. A NATO a kibertérben a védelemre összpontosít, azonban nem korlátozza tagállamokat, hogy adott esetben a kiberhadviselés más területeit is fejlessze. Hazánknak szintén át kell gondolnia az álláspontját ezzel kapcsolatban, mivel a védelem (és részben a felderítés) magától értetődő a kibertérben, azonban a kibertámadás képességének megteremtése és esetleges alkalmazása politikai döntést igényel.

* * *

A híradó-informatikai szolgálat tevékenységét nagyban befolyásolja napjainkban az illegális migráció és a terrorizmus veszélye, aminek nyomán a korábbiaktól eltérő híradás-szervezési gyakorlatot kell követnünk: nagy kiterjedésű területen igen sok járőr kapcsolatát kell párhuzamosan biztosítani a rendvédelmi szervekkel és egymással, ami nem szolgálható ki hagyományos katonai, harcászati rádiókkal. A változásokkal lépést kell tartanunk, különben nem tudunk megfelelni a kor kihívásainak.

Az aszimmetrikus hadviselés, a hibrid hadviselés, valamint a proxy háborúk (idegen erőkkel a saját céljaink érdekében megvívott háborúk) a történelem folyamán mindig voltak, azonban az egyre bonyolultabbá váló válsághelyzetek komplex kezelésének igénye miatt – az átfogó megközelítés jegyében – napjainkban mindinkább előtérbe kerülnek.

A kiberhadviselés mind a hibrid, mind az aszimmetrikus hadviselés fontos eleme, amely a hagyományos eszközökkel kiváltott csapásokra, illetve az egyéb nem fegyveres, de szintén hagyományos műveletekre egészen más eszközök és módszerek alkalmazásával képes hatékony választ adni úgy, hogy az arra fordított költségek legtöbbször a töredékét képezik az előbbieknek.

A NATO varsói csúcstalálkozója a kiberteret – a szárazföld, a légtér és a tengerek mellett – önálló hadszíntérként (domain of operations) definiálta, amelynek fontos folyománya, hogy az ott végrehajtott műveletek eszközei, eljárásai, módszerei, szabályai és hatásmechanizmusa jelentősen eltérnek a többi hadszíntéren alkalmazott haderőnemek és fegyvernemek sajátosságaitól, és szükség esetén az utóbbiaktól függetlenül, önállóan is alkalmazhatók. A varsói döntést be kell illeszteni a magyar jogrendbe, amely felveti a kibervédelemnek, illetve a kiberműveleteknek a Nemzeti Biztonsági Stratégiába és a Nemzeti Katonai Stratégiába történő beemelését.

A kibervédelemért a honvédelmi tárcánál politikai szinten a HM Védelempolitikai Főosztály a felelős, míg a honvédelmi ágazat elektronikus információvédelmi felügyeletéért és hatósági feladatainak ellátásáért a Katonai Nemzetbiztonsági Szolgálat, az MH Kormányzati Célú Elkülönült Hírközlő Hálózat (MH KCEHH) kibervédelmi tevékenysége szakirányításáért pedig a Honvéd Vezérkar Híradó, Informatikai és Információvédelmi Csoportfőnökség felel.

Az MH három lépcsőben tervezi a kibervédelmi képesség megteremtését, amely összhangban van a NATO kibervédelem kapcsán megfogalmazott követelményeivel. Ezek a kezdeti, az alap és a teljes kibervédelmi képesség. A Magyar Honvédség kibervédelmi fejlesztései integráns részét képezik a honvédelmi szakpolitikai programnak, amelynek keretében az MH Budapest Helyőrség Dandár (MH BHD) állományában létrehozták az Elektronikus Eseménykezelő Főközpontot. Az eszközök beszerzése és az állomány feltöltése folyamatban van, azonban a szervezet már most rendelkezik egyes kezdeti és alapképességekkel. Ezzel együtt további szervezeti-hatásköri változtatásokra lehet szükség az MH-ban az egységes kibervédelmi rendszer megteremtéséhez, amelynek érdekében a HVK Híradó, Informatikai és Információvédelmi Csoportfőnökség munkacsoport felállítására tett javaslatot annak tisztázására, hogy milyen vezetési szinten milyen kibervédelmi szervezetre van szükség. A kibervédelem legnagyobb kihívása a reagálási képesség időtényezőjének csökkentése, a felderítés hatékonyságának növelése, ennek érdekében komoly hangsúlyt kell helyezni az automatizációra.

* * *

Az egyes országok a kibervédelmi struktúra felállítását különbözőképpen értelmezik, van, ahol nemzeti (illetve haderő) szinten kiberparancsnokságot hoztak létre az alapvető elektronikus védelmi funkciók összefogására. A NATO képességfejlesztési projektje keretében 2018-ig meg kell mondanunk, hogy melyik az a magyarországi szervezet, amelyik a Szövetség előtt a műveletek vonatkozásában felel a magyar kibervédelemért.

De nemcsak a technika fejlődött az elmúlt évtizedekben, hanem a módszerek is. A kezdetekkor a felülről lefelé történő építkezés volt a jellemző, tehát először kidolgozták az információs rendszer tervét, megalkották a programok leírását és kapcsolatait, leprogramozták a szoftvert, és csak ezután foglalkoztak a számítógépek beszerzésével és azok hálózatba szervezésével. Mára az informatika alapszolgáltatássá vált, ami azt jelenti, hogy egy mindenki számára elérhető informatikai infrastruktúrára építkezve valósulnak meg a fejlesztések, a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának (MH KCEHH) egységesedő elvei szerint.

A felső szintű szakterületi szabályozó rendszer ugyancsak fejlődött: a 39/2014. (V. 30.) sz. HM utasítás mellékleteként kiadták a Magyar Honvédség Informatikai Szabályzatát, amely az 1993-ban kiadott szabályzatot váltotta fel. Szintén HM utasítás mellékleteként, 58/2014. (IX. 10.) számon kiadták a Magyar Honvédség Informatikai Stratégiáját, amely a 2014–2024 évekre vonatkozóan határozza meg az informatikai fejlesztés és üzemeltetés fő feladatait a tárcánál. Kiadták *a Magyar Honvédség Kormányzati Célú Elkülönült Hírközlő Hálózatának békeidejű üzemeltetési és felügyeleti rendjéről, valamint a központilag biztosított szolgáltatások igénybevételének szabályairól* szóló,

55/2013. (IX. 13.) HM utasítást, illetve az előbbiekkel párhuzamosan számos kibervédelmi jogszabály, szabályozó dokumentum is megjelent, megteremtve az új szakterület tevékenységi kereteit.

A tárca informatikai fejlesztési irányait – az MH Informatikai Stratégián túl – egyre inkább meghatározzák a kormányzati követelmények. A Nemzeti Infokommunikációs Stratégiából következően, a digitális állam koncepciója keretében az elektronikus ügyintézés bevezetése jelentős feladatokat ró a honvédelmi ágazatra. 2017. május 1-től a köztisztviselők számára kötelező a személyügyi okmányok digitális aláírása, 2018. január 1-től pedig a tárcának is be kell vezetnie az elektronikus ügyintézést először a minisztériumban, majd a teljes honvédségben.

Ugyanakkor az informatikai alkalmazás már a kezdetektől fogva sem pusztán egy matematikai alapokon nyugvó technikai jellegű tevékenység. Viszonylag korán felismerték, hogy az informatikai rendszerek bevezetése alapjaiban kell, hogy megváltoztassa a szervezetek információs folyamatait, nem egyszerűen felgyorsítva, hanem új minőségű alapra helyezve azt. Ennek eredményeként változik a szervezetek vezetési-döntési struktúrája, eljárásrendje, hatékonyabbá válik az együttműködés, ami jelentős mértékben javítja a döntések időbeniségét és minőségét, ezért az informatika fejlesztése közös ügyünk, amelyhez minden szervezet hozzáteszi a maga részét.

Ugyanez a helyzet az informatika alkalmazásának megszervezésével, a szolgáltatások igénybe vételével, ami azzal az ismert mondással fejezhető ki legjobban, hogy minden informatikai rendszer annyit ér, amennyit a benne tárolt és feldolgozott adatok, illetve amit abból hasznosítanak. Az informatikai szolgáltatások kialakítása, fenntartása és igénybe vétele sosem volt egyetlen szolgálat belügye, abban tevékeny részt vállaltak és vállalnak a felhasználó szervezetek is.

* * *

A híradó és informatikai támogatás a katonai vezetés működőképességének, a csapatvezetés végrehajtásának nélkülözhetetlen feltétele. Napjaink katonai műveleteiben az eredményes tevékenység alapvető feltétele a vezetési fölény, és az azt megalapozó információs fölény, valamint az egyeztetett közös helyzetismeret kialakítása és fenntartása. Mindez megvalósíthatatlan korszerű távközlési- és információtechnológia, a híradás és az informatika eszközrendszerének átfogó, tervszerű alkalmazása nélkül.

A korszerű katonai műveletekben az információk áramlása, feldolgozása, tárolása és rendelkezésre bocsátása nem feltétlenül tükrözi a katonai szervezeti hierarchiát, az alá és fölérendeltségi viszonyokat, hanem attól sok esetben eltér. Az információ a szükséges időben, helyen, formában, bontásban és tartalomban ott jelenik meg, ahol azt felhasználják, függetlenül attól, hogy az információ hol, mikor, ki által, milyen módon került a rendszerbe. A különböző vezetési szintekhez és szervezetekhez tartozó katonai kommunikációs és információs rendszerek összekapcsolása – köszönhetően a korszerű információs technológiának – lehetővé teszi, hogy a felhasználók a híradó és informatikai rendszerből a számukra szükséges információkat jogosultságuknak megfelelően munkaállomásaikon, mobil kommunikációs eszközeiken valós időben kinyerjék, és eközben az információk fizikai elhelyezkedésével, tárolásuk és kódolásuk módjával nem kell törődniük.

Ez a technológiai és szemléleti fejlődés tette lehetővé a *Hálózatalapú* (hálózatközpontú) *hadviselés* (Network Centric Warfare – NCW) koncepciójának kidolgozását és megvalósítását a korszerű hadseregekkel rendelkező államokban, amely a NATO-ban *NATO Hálózat-nyújtotta Képesség* (NATO Network Enabled Capability – NNEC) megnevezéssel indult, majd a *Federated Mission Networking* (FMN) programmal folytatódott, hazánkban a *Hálózatalapú Műveleti Képesség* (HAMK) nevet kapta.

Az MH Összhaderőnemi Híradó és Informatikai Doktrína részletesen tárgyalja a HAMK elveit, tulajdonságait. Eszerint a Hálózatalapú Műveleti Képesség egy rendszerbe fogja össze a saját csapatokról szóló információkat, a műveleti környezetről szóló térkép-, terep- és időjárás-adatokat, a valósidejű felderítési információkat (beleértve a szenzorok, műholdak, drónok, rádiólokátorok, hőkamerák, barát-ellenség felismerő rendszerek által biztosított álló és mozgóképeket), a műveletek civil környezete által biztosított információkat, a navigációs adatokat és GPS-jeleket, a saját csapatok automatikus nyomkövető rendszerének adatait (Blue Force Tracking System), a fegyverirányítási rendszerek elektronikus információit és még számos automatizált adatgyűjtő rendszerből származó információt, amelyek – a hozzáférési jogosultságnak megfelelően rétegekbe szervezve – a Közös Műveleti Képen (Common Operational Picture – COP) jelennek meg. A különböző szintű kötelékek a minden szervezet számára egységes Közös Műveleti Kép alapján tevékenykednek, ezért vezetésük és együttműködésük alapfeltétele biztosított.

Az MH tábori híradó-informatikai rendszer fejlesztése, digitális alapokra helyezése, az alakulatok infokommunikációs képességeinek hálózatba szervezése folyamatban van, a század szintű korszerű híradó-informatikai rendszer kialakítása a csapatok többségénél megvalósult. Jelenleg a zászlóalj-harccsoport vezetéstámogató rendszer hadműveleti követelményeinek kidolgozása zajlik, amely a kiépítést követően eleget fog tenni a hálózatalapú hadviselés követelményeinek.

A Hálózatalapú Műveleti Képesség nemcsak a híradó és informatikai rendszerek felépítésében és alkalmazásában hoz változást, hanem az információs képesség fejlődésének megfelelően változik a döntési-parancskiadási rend, a döntési szintek a szervezeti hierarchiában szükség szerint feljebb vagy lejjebb tolódhatnak. Az infokommunikációs rendszer kiterjesztett képességeinek köszönhetően előfordulhat, hogy stratégiai szinten vezetnek zászlóalj vagy századszintű köteléket, ugyanakkor – az idő szorító kényszerének hatására, felső szintű utasítás alapján – akár század vagy szakasz szinten is vezethetnek és végrehajthatnak stratégiai jelentőségű feladatokat, köszönhetően a döntéshozatalhoz és vezetéshez szükséges információk és valósidejű felderítési adatok akár harcászati szinten történő megjeleníthetőségének.

A Hálózatalapú Műveleti Képesség biztosítása egyik alappillérét jelenti az ún. átfogó megközelítés (Comprehensive Approach) koncepció megvalósításának, amikor a műveletek végrehajtásában résztvevő együttműködő partnerek a kormányzati-államigazgatási szférából vagy a civil szférából (Non Governmental Organizations – NGO) kerülnek ki, és a műveletek végrehajtásának módját, eredményét nem elsősorban katonai szempontból, hanem össztársadalmi szempontból határozzák meg, illetve ítélik meg. A katonai műveletekhez szükséges információk biztosítása ebben az esetben jelentős részt a kormányzati vagy a civil szférából kell, hogy történjék, ezért a Hálózatalapú Műveleti Képességnek lehetővé kell tennie – a hazai vagy a

műveleti területen lévő – kormányzati és civil infokommunikációs rendszerekhez történő kapcsolódást minden vezetési szinten, és onnan a műveletekhez szükséges információk kinyerését, illetve az együttműködést érdekében biztosítani szükséges a katonai információk meghatározott körének a polgári szervezetekkel történő megosztását.

* * *

Az elkövetkező tíz év fejlődési iránya a sokfunkciós, mobil, könnyen kezelhető, komplex infokommunikációs szolgáltatások irányába mutat, amely magában foglalja a mozgókép, a hang, az írásos és egyéb adatok integrált kezelését, a sokszereplős kommunikáció egyidejű megvalósítását, az automatikus információkeresést és adattársítást. Mindez a mobilitást és integritást támogató, egymástól akár jelentős távolságra települt, együttműködő hírrendszerek, adatközpontok és szolgáltatások alkalmazásának irányába hat, amelyek virtuális környezettel teremtik meg az elérhetőséget, átjárhatóságot, összekapcsolhatóságot és védelmet a különböző funkciójú eszközök és szolgáltatások között. Ezzel együtt továbbra is fontosak maradnak a helyi hálózatokba szervezett asztali munkaállomások, az irodai környezetben nyújtott szolgáltatások, amelyek kiegészülnek a szervezeti információk interneten keresztül történő, távoli elérhetőségével, az otthoni munkavégzés és távmunka feltételeinek megteremtésével.

A katonai információs rendszerek fejlődési irányait a híradó-informatikai szolgáltatásoknak az egyes katona szintjéig történő eljuttatása, a műveletek számítógépes modellezése, a műholdas helymeghatározási módszerek széleskörű alkalmazása, az integrált szolgáltatások, adatbázisok és műveleti kép minden együttműködő számára történő biztosítása, a valósidejű videofelvételek szükség szerinti rendelkezésre bocsátása, a vezetési, navigációs, azonosítási és fegyverirányítási információk egységes rendszerben történő kezelése, a kormányzati és civil szervezetekkel való átfogó kommunikációs képesség kialakítása határozta és határozza meg, kiemelt figyelmet fordítva az információbiztonság kritériumainak teljesítésére, a szolgáltatások folyamatos rendelkezésre állásának biztosítására.

Napjainkban a sűrűjében vagyunk egy olyan nagyszabású, több milliárd forint értékű fejlesztésnek, amely a Magyar Honvédség központi híradó-informatikai rendszere stabilizálását, biztonságának növelését, szolgáltatásainak bővítését tűzi ki célul. Ilyen mértékű fejlesztésre hosszú évek óta nem került sor a tárcánál. Sőt, megkockáztatom, ez az első ilyen jellegű komplex projekt a központi rendszerek vonatkozásában. A fejlesztés magában foglalja többek között több ezer elavult felhasználói számítógép cseréjét, a szerverpark megújítását, a nagytávolságú adatátvitel sebességének jelentős növelését, a korszerűtlenné és megbízhatatlanná vált adatátviteli kapcsoló berendezések, routerek kiváltását, a video-telekonferencia rendszer megújítását, a honvédség védett, minősített informatikai hálózatának kiépítését, a kibervédelemet támogató számítógépes eseménykezelő központ kialakítását, az elektronikus iratkezelés bevezetését és a hagyományos papíralapú iratnyilvántartás kiváltását, az elektronikus aláírás és digitális időbélyeg szolgáltatás bevezetését, az idejétmúlt szoftverlicenszek megújítását, egyes portálalapú alkalmazói programfejlesztéseket, az üzemeltetés-támogatás újraszervezését.

A fejlesztések eredményeként nő a rendszer biztonsága, a szolgáltatások rendelkezésre állása és színvonala, hatékonyabbá válik az üzemeltetés, lehetővé válik olyan programrendszerek és alkalmazások igénybe vétele, amelyekre a jelentős részt elavult technika és technológia miatt eddig nem volt lehetőség. Ugyanakkor a viharos fejlődésből adódóan a híradó-informatikai eszközök gyorsan elavulnak, amely különösen nagy kihívást jelent mind a felhasználói, mind a híradó-informatikai, mind a logisztikai szervezetek részére.

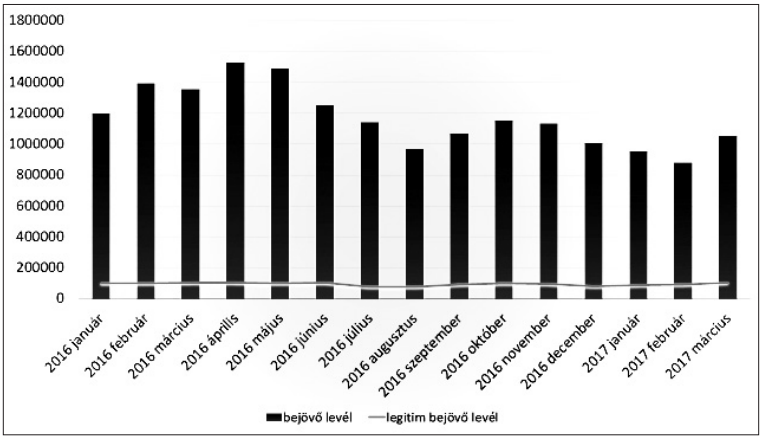
A berendezések és szoftverek erkölcsi amortizációja jelentős biztonsági kockázatot jelentenek, mivel a támadások többsége azok gyengeségeit, hiányosságait használja ki. A jelenleg zajló komplex fejlesztéseknek is ez az egyik alapvető oka. A támadások 90%-a a nemzetközi trendek szerint egy (vagy több) emaillel indul. Hatványozottan igaz ez az MH külvilágtól részlegesen elzárt rendszereire, ahol a külső kapcsolatok elsősorban a levelezési rendszeren keresztül valósulnak meg. A külső hálózatokból érkező e-mailek száma havonta 800 ezer és 1,5 millió között van, amelyből a legitim, valós megkeresés nem éri el a 10%-ot, tehát hatalmas mennyiséget kell kiszűrni (*l.* ábra). Időnként egy-egy nem kívánatos levél mégis „átcsúszik" az elektronikus határvédelmen, ami aláhúzza a biztonságtudatos felhasználói gondolkodás megerősítésének szükségszerűségét. Szintén fontos feladatot jelent a „false pozitív" találatként megállított fontos és legitim levelek számának csökkentése, amihez a nem mintaalapú szűrő rendszerek jelenthetnek megoldást a közeli jövőben.

A technikai fejlesztés azonban egyedül nem elég: céljaink eléréséhez szükség van megfelelő szervezeti keretekre és elkötelezett, magas tudású szakemberekre is. Az elmúlt évtizedekben sokszor változtak az informatikai szakterület szervezeti keretei: hol az informatikai központok és informatikai irányítás decentralizálása, hol azok központosítása volt napirenden, hol szétvált a közigazgatási informatika a katonai informatikától, hol egyesült vele, de az elektronikus információvédelem is sokáig kereste a helyét a struktúrában, amíg a híradással és informatikával egy szervezetbe került. A sok változásnak csak kis részben volt a technológiai fejlődés az okozója, így sajnos elmondható, hogy azok összességében csökkentették a szakterület hatékonyságát és érdekérvényesítő képességét, ami egyrészt forráshiányhoz, másrészt az erőforrások szétforgácsolásához vezetett.

Az utóbbi hat-hét évben a híradó–informatikai–információvédelmi szakterület ismét egységes irányítás alatt, és egységes szervezeti rendben működik, amely fontos záloga a további eredményes munkának. Ezzel együtt nagy kihívás a magasan kvalifikált szakállomány biztosítása és megtartása, mivel a polgári életben a szakemberek számára felkínált 6–8-szoros fizetések a honvédséghez képest óriási elszívó erőt jelentenek.

* * *

Összefoglalásul elmondható, hogy a Magyar Honvédség vezetéstámogató rendszere az utóbbi évek, évtizedek rohamos technológiai fejlődésnek, és az annak nyomán kialakított korszerű hadviselési elveknek megfelelően folyamatos változás, fejlődés alatt állt és áll, az eszközök és eljárások fejlődése napról napra, évről évre nyomon követhető. Ugyanakkor az elavult berendezések és rendszerek egységes rendben, közel azonos időben történő lecserélése, valamint az eljárások, módszerek egyik



Az MH bejövő és legitim leveleinek aránya
(Forrás: MH BHD Informatikai Főközpont)

napról a másikra történő megváltoztatása – alapvetően a pénzügyi források rendelkezésre bocsátásának ütemezése miatt – nem volt megvalósítható, és előreláthatólag a jövőben sem lesz az.

Ezzel együtt, ha visszatekintünk a szakterület tíz-tizenöt évvel korábbi helyzetére, kellő távolságból egyértelműen megállapítható, hogy a Magyar Honvédség híradó, informatikai és információvédelmi tevékenységének módszerei, eszközei, valamint szakembereinek tudása, tapasztalata minőségileg új generációt képvisel a XXI. század fordulójához képest. Ez fokozottan igaz az informatikai szolgáltatások igénybe vételére a honvédelmi szervezetekben, ahol a napi kidolgozó munka nélkülözhetetlen részévé vált, amelynek hatóköre, minősége dinamikusan növekszik.

IRODALOMJEGYZÉK

Az MH Informatikai Stratégiája. 58/2014. (IX. 10.) HM út. 1. sz. melléklet.

Az MH Összhaderőnemi Híradó és Informatikai Doktrína. (1. kiadás) MH DOFT KÓD: HÍD 6 (1)

Dr. Munk Sándor: Katonai informatika a XXI. század elején. Zrínyi kiadó, 2007.

Gerőfi Szilárd: Az új MH Informatikai Stratégia megvalósításának kulcsfontosságú feltételei. Honvédségi Szemle, 2015/4.

60/2013. (IX. 30.) HM utasítás a Magyar Honvédség Kibervédelmi Szakmai Koncepciójának kiadásáról.

Warsaw Summit Communiqué (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw 8–9 July 2016) http://www.nato.int/cps/en/natohq/official_texts_133169.htm

Cyber Defence Pledge. http://www.nato.int/cps/en/natohq/official_texts_133177.htm

Commitment to enhance resilience (Issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Warsaw, 8–9 July 2016) http://www.nato.int/cps/en/natohq/official_texts_133180.htm?selectedLocale=en

NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit (NATO CCD COE) https://www.linkedin.com/pulse/nato-recognises-cyberspace-domain-operations-warsaw-summit-min%C3%A1rik?articleId=6163600545262116864

Is NATO Ready to Cross the Rubicon on Cyber Defence? (NATO CCD COE) Tallinn, June 2016 https://ccdcoe.org/sites/default/files/multimedia/pdf/NATO%20CCD%20COE%20policy%20paper.pdf

The role of offensive cyber operations in NATO's Collective Defence. (NATO CCD COE) https://ccdcoe.org/multimedia/role-offensive-cyber-operations-natos-collective-defence.html

Wales Summit Declaration (NATO) http://www.europarl.europa.eu/meetdocs/2014_2019/documents/sede/dv/sede240914walessummit_/sede240914walessummit_en.pdf

Piret Pernik: NATO's Cyber Deterrence (International Centre for Defence and Security – Estonia)

Dorothy E. Denning: Rethinking the Cyber Domain and Deterrence (National Defense University Press)

Cyber, Extended Deterrence, and NATO (Atlantic Council, BRENT SCOWCROFT CENTER ON INTERNATIONAL SECURITY) http://www.atlanticcouncil.org/blogs/natosource/cyber-extended-deterrence-and-nato