BIZTONSÁG AZ ELEKTRONIKUS VILÁGRENDBEN

Deák Péter
a hadtudomány doktora – dyly@freemail.hu

A *biztonság* terminológiája a múlt század második felében jelent meg a politikai szóhasználatban, mint a hadügy tapasztalatai alapján kialakult axióma kifejezõdése. A két világháború olyan következményeket produkált, hogy a védelmi doktrínák, szervezetek és infrastruktúrák anakronizmussá váltak. A védelem, a védekezés ugyanis *post factum* jelenség, az adott korban a fegyveres támadás bekövetkezését követõ cselekvéssorozat, amely már kezdeti idõszakban is súlyos következményekkel jár mind a támadó, mind a védõ számára. Ezért elõször elvekben, majd a nemzetközi intézményrendszerben, napjainkban pedig különbözõ stratégiákban a társadalom igénye a biztonság primátusa, a konfliktusok, a veszélyjelenségek megelõzése, és ez számos új jelenség észlelése nyomán fokozódik

Biztonságpolitikai dilemmák

A harmadik évezred kezdetén a világ biztonsági képét egymással összefonódó jelenségek determinálják: 1.) A hidegháború lezáródásával a világ olyan értelemben lett egypólusú, hogy szuperhatalmi megtestesítõje a katonai képességben, gazdasági erõben, technológiai fölényben, politikai befolyásban, demokratikus intézményrendszerében és világméretû érdekeiben egyedülálló Amerikai Egyesült Államok lett; 2.) további tény, hogy a globalizációt indukáló tényezõk között egy új technikai forradalom termékei és következményei is ebben az idõben bontakoztak ki. Ez a technikai váltás az elektronika világában, a biogenetikában szinte egyszerre hatotta át a világot, hozadékaival és negatív következményeivel együtt. A biztonság szempontjából is, elsõ pillanattól kezdve, áldás- vagy átokként jelent meg, mert hihetetlen lehetõségeket eredményezett a gyarapodó fajtájú kihívások elleni elõrejelzésben, védekezésben, kárfelszámolásban. A bipolaritás felbomlásához vezetõ intenzív idõszakban a leszerelés ellenõrzése és a bizalomépítõ intézkedések technikai verifikációja is hozzájárult a hidegháború végéhez vezetõ lépésekhez. Ugyanakkor jelentõsen megemelte a vétlen vagy akaratlagos kártevési kockázatokat, a közbiztonság felé irányuló intervenciók lehetõségét.

A fenti jelenségek századunk elejére a világrend jelentõs átalakulásához vezettek. Az egy szuperhatalomra épülõ politikai-gazdasági-katonai alakzat a világnak ma kulcskérdése, és átalakítása vagy fenntartása alapvetõ jellemzõje a nemzetközi mozgástérnek.

Henry Kissinger joggal teszi fel a kérdést, hogy vajon alkalmazható-e a wilsoni elv, mely szerint az amerikai nemzetközi doktrína a „demokrácia kiterjesztése", és – ezt már én tenném hozzá – milyen (netán erõszakos) eszközökkel. Vajon a globális rend megteremtése a nagyhatalmi intervenció, avagy a nemzetközi konszolidáció útján megy-e végbe?

A jelenleg konstatálható, és feszültségek sorozatát teremtõ aszimmetrikus helyzet a biztonság kezelési metodikáiban is egyensúlytalanságot eredményez, a válságkezelõ

intervenciós katonai akciók is aszimmetrikusak. Egyrészt azért, mert a kettõs szembenállásokat egy „háromszög" váltotta fel, a harmadik, beavatkozó erõ anullálja a felek közötti erõviszonyokat, a „konszolidáló" erõ mindig felülmúlja a két fél összerejét.

Ez a helyzet a hadügyben is struktúra- és doktrínaváltást eredményezett, a területfoglalás helyett az operativitás a katonai cél, e tekintetben az erõk már nem mérhetõk össze. A „háborúkép" a front helyett a válsághelyszínt állította középpontba, csökkent a terített rombolás, a nehézfegyver-koncentráció jelentõsége.

Az amúgy is politikai vonakodás tárgyát képezõ védelmi költségeken belül a fejlesztési kiadásokban az elektronikai terület aránya eléri a 65-80 %-ot. Ennek következtében a globalizált piacon a hadfelszerelés terén igen magas és kíméletlen verseny fejlõdik ki. A Pentagon még 2001. szeptember 11-e elõtt meghirdette a *Run Faster Strategy*-t, annak érdekében, hogy az USA mindig egy lépéssel elõbbre járjon. Ennek eleme, hogy a generációváltás, a K+F ciklus és a felszerelésváltás üteme felgyorsul, az adott készletektõl a hatalmak alacsony áron igyekeznek megszabadulni. Ez a piaci offenzíva viszont olyan országokat, csoportokat juttat fegyverzethez, amelyek politikai céljai között szerepel e fegyverek alkalmazása is.

A védelem új technikai arculata

Katonai értelemben az elektronizáció igen széles spektrumot fog át. Frank Barnaby szerint az elektronika katonai alkalmazásakor öt alapvetõ szektort lehet számba venni, nevezetesen: a célpontosságban, a tengeralattjáró-elhárításban, a repülõgéprendszerek vezérlésében, a felderítésben és az automatizált harcmezõn való használatot. Barnaby ezt több mint húsz éve írta, és természetesen ma a skála nem csak bõvült, hanem el is tolódott.

A fegyverrendszerek alaptechnológiájában is változás következett be. A szelektivitást eredményezõ precízió, a hagyományos radar, mûholdas figyelés kiegészül a hõpellengációval, az infratechnikával, a zajérzékeléssel, a szenzorok hálózatával, a hangazonosítási eszközökkel, a rádiófelderítés zavarvédettségével, az egyre nagyobb szerepet vállaló lézertechnikával. Hihetetlenül megnõtt az információ rapiditása, a távolság nem jelent tényezõt. A vezetés és végrehajtás között kialakultak az együttlátó és együtthallgató rendszerek. Az észlelt kép és hang megjeleníthetõ a fegyvert elindító katona elõtt.

Az elektronika összefügg a miniatürizálással. Ez teszi lehetõvé, hogy a rendõr, a katona, a határrendész és a felderítõ a komplex bázisok valamennyi eszközét maga a személy saját felszereléseként, mi több, öltözeti elemeként „hordja" és alkalmazza. Éjjel látás, képi megjelenítés, együtthallgató-látó rendszerek, infrafelismerés, helymeghatározás, zajértékelés – akár csak a mobiltelefon legújabb generációiban – szinte egyedi elemként, zsebben van jelen, és az alkalmazásra való kiképzés fekete doboz jellegû.

A biztonság tartalmának jelentõs bõvülése, a nem katonai veszélytényezõk elõtérbe kerülése szempontjából a magas technológiájú eszközök rendeltetése is változik. Az elektronikára épülõ észlelõrendszerek éppen preventív szempontból játszanak fontos szerepet a katasztrófakövetkezmények megelõzésében és csökkentésében, a környezetvédelemben, az ipari, nukleáris balesetek idõben való észlelésében, a természeti csapások körzetének, epicentrumának, pusztítási gócpontjainak meghatározásában.

A számítógépes technológia, a szoftverfejlõdés a biztonsági kockázatok megelõzésében egy sajátos új hozadékot is eredményez. Ez pedig a forgatókönyv-változatok nagy száma és kombinációs lehetõsége. Az emberi fantáziára bízott védelmi vagy éppen offenzív scenáriók számos véletlennek voltak kitéve, míg ezek 90 %-a ma megfelelõ szoftverrel kizárhatók, illetve a folyamatok

szinte azonnal korrigálhatók. Ennek kezdeti elemei több tíz évvel ezelõtt a modern gondolkodásban a hálótervezés, illetve a PERT rendszer alkalmazásával már megjelentek, sõt, a hatás-, illetve következményvizsgálatoknál néha alkalmazásra kerültek.

Napjaink gondjai

Az információsebesség és a döntési idõszükséglet ellentmondásai gyakran okozhatnak problémákat bizonyos (nem csak katonai) akcióknál a civil kontroll érvényesítésében. A politika és az adott fegyveres vagy kárelhárító erõ folyamatos kapcsolata a konfliktus idõszakában fellazul, az operatív cselekvés lehetséges gyorsulása és önmozgása mindinkább „kibújhat" a politika megfontolt beavatkozása alól.

Maga a világháló és különbözõ kommunikációs rendszerek ezzel való integrációja azon képességek és lehetõségek mellett, amelyek a biztonság, a prevenció, az elhárítás rendszereit szolgálják, egyszerre jelentkeznek veszélyjelenségként is, ami ismét a szemben álló elektronikus eszközhalmaz rivalizációját, az erõviszony-fordulat elérését szolgálják, amely egy permanens folyamat. Ennek központi eleme a tûzfal, illetve a kódrendszer folyamatos cseréje és bõvülése.

Részletekbe merülés nélkül, csak összefoglalásként és evidenciaként az informatikai integrált rendszerek elleni veszélyek, mi több, fenyegetések a következõk:

• Vírusterjesztéssel, illetve tömeges terheléssel a vezérlõ, vezetõ rendszerek blokkolása, kapcsolatok megszakítása, katasztrófák elõidézése, katonai és határrendészeti eszközpark kiiktatása.

• Gazdasági, politikai, katonai, mûszaki és tudományos dezinformációk bejuttatása kompetens rendszerekbe.

• Demagóg, populista, extrém nézetek terjesztése mint a lélektani hadviselés szinte korlátlan eszköze, elektronikus „röplap".

• Információlopás, -szerzés, ill. -törlés.

Természetesen az elektronikus társadalom, a világháló megléte és fejlõdése nem lehet biztonsági megközelítés tárgya a nemzetközi, tömegeket pusztító, gyilkos-öngyilkos terrorizmus szempontjai nélkül. A hipertechnika és a primitív eszközök és metodikák együttalkalmazásával járó cselekmények világában az elektronika a terrorizmus és az ellene való küzdelem közös eszközparkja.

Az már evidencia, hogy az új évezred, a globalizációs korszak, a fundamentalizmusok feléledésének korában jelentkezõ elsõ számú biztonsági kihívás józan és hosszú távú politikai kezelése mellett – amely egyelõre még várat magára – a védelem fõ területe a megelõzés. A prevenció fõ tartalma az információ folyamatos beszerzése és naprakész állapotban tartása. És ez alatt nem csupán a hírszerzést, a titkosszolgálati tevékenységet kell értenünk. Az egyes események, tendenciák tudományos és szakszerû elemzése, a mozaikok következtetéssé való összerakása az elõrejelzés egyetlen lehetõsége. Szeptember 11-e váratlanságának *egyik* oka az intézmény közötti és nemzetközi információcsere szinte teljes hiánya volt. E tekintetben az egyes integrációkon belül a nagyhatalmak és a kis országok részérõl jelentkezõ szubjektív „visszatartás" a kutató szemével nézve tûrhetetlen. Az információszerzés *másik*, többszörös kudarcot kiváltó hiányossága a felderítõ technikák szerepének misztikus felnagyítása és a humán elemek, magyarul ügynökök és legális pozícióból megvalósuló hírszerzés leépülése volt. A „kémek" szerepe a kemény katonai szembenállás lebomlásával megváltozott. A titkosszolgálati tevékenység a bizalom és a biztonság eszközévé vált, a demokratikus társadalmakban komoly civil kontroll alatt áll, és ennek az új stratégiában még erõsödnie kell.

Zárásként és összefoglaló gyanánt egy idézet: „Az a fõkérdés, hogy a kormányok… képesek lesznek-e a mikroelektronika új le-

hetõségeinek elõre megfontolt és tudatos kihasználására a társadalom átformálása céljából, vagy csak passzívan próbálnak igazodni a következményekhez" (King, 1982).

Kulcsszavak: *biztonságpolitika, hadügy, új kihívások*

IRODALOM

Barnaby, Frank (1982): *Microelectronics in the War. Microelectronics and Society. For Better or for Worse. Report for Club of Rome*. Pergamon Press. New York

Deák Péter (2000): *Új típusú fegyveres konfliktusok, nemzetközi terrorizmus. Info-társadalom*. Országgyûlési Könyvtár

Deák Péter (2001): *Új biztonsági kihívások a XXI. század közepén*. Szakmai Tudományos Közlemények. KBH

Global Trends 2015 (2000): *A Dialogue About the Future With Nongovernment Experts*. National Foreign Intelligence Board. Washington

Gwyn, Prins (1998): The Four-stroke Cycle in Security Studies. International Affairs. 4.

King, Alexander (1982): in Schaff Adam – Friedrichs Günter (eds.): *Microelectronics and Society. For Better or Worse. Report for the Club of Rome*. Pergamon Press, N. Y., 34.

Kissinger, Henry (2003): *Diplomácia*. Panem-Grafo Kft., Budapest

Müller, Harald (2003): *Terrorism, Proliferation: A European Threat Assessment.* Chaillot Papers. N'58 Institute for Security Studies. Paris

Ráth Tamás (2002): *A terroristák elleni harc és a modern haditechnika. Válaszok a terrorizmusra*. SVKH, Budapest

Ráth, Tamás (2002): *Modern Military Technology and the Combat against Terrorists. Is there a Route from the „Huntdown" in Afghanistan to Sustainable Globalization?* SVKH, Budapest

Sassen, Saskia (2000: *Elveszített kontroll? Szuverenitás a globalizáció korában*. Helikon Kiadó, Budapest

Szászné Tolnai Klára – Tamás Ferenc (1986): *Mesterséges holdak*. Zrínyi Katonai Kiadó, Budapest

Várhegyi István: *A haderõ korszerûsítésének elektronikai aspektusai*. Hadtudományi Tájékoztató. 1966, 3.