2013-04-20 07:33, Kovács Dániel

Kibertér – csatatér

Címkék: biztonságpolitika, haditechnika, informatika, jog, NATO, terrorizmus

Kiberháborús fenyegetés, informatikai hadviselés, informatikai biztonság – ezek a fogalmak tíz évvel ezelőtt még jóformán ismeretlenek voltak számunkra. Ma pedig már a védelmi ipar egyik legnagyobb kihívását jelentik. De nem kisebb fejtörést okoz a NATO jogi szakértőinek a haditechnika fejlődésével előálló új helyzet, a kiberhadviselés nemzetközi jogi elvek szerint történő szabályozása.

Hogyan jelenhet meg a hagyományos katonai erő a kibertérben? Mi számít kiberterrorizmusnak? Ki és hogyan szabályozza az informatikai hadviselést? Ezekre a kérdésekre kísérel meg választ adni a NATO új kibervédelmi kézikönyve, a *Tallin Manual*. Az új szabályokról, a világszerte eluralkodó, így hazánkat is érintő fenyegetésről, illetve az új típusú hadviselés eszközeiről tartotta áprilisi vitaestjét a Pallas Páholy kül- és biztonságpolitikai klubja, ahol dr. Krasznay Csaba, a HP informatikai biztonsági szakértője és Varga-Perke Bálint hacker tartottak előadást.

Nem véletlen, hogy Tallinban készült el a jegyzőkönyv – derült ki az előadásból –, hiszen az Észtországra 2007-ben lesújtó, talán az eddig ismert legnagyobb hatású kibertámadás-sorozat hatására került az észt fővárosba a NATO kibervédelemmel foglalkozó kiválósági központja. A dokumentum 300 oldalon keresztül, 95 pontban próbálja meg pótolni a nemzetközi kiberháborús jog alapvető hiányosságait.

A szakemberek legfontosabb feladata volt, hogy átültessék a tényleges hadviselés során alkalmazandó normákat on-line környezetbe. Ennek megfelelően találhatunk benne a genfi és a hágai egyezményekben leírtakhoz hasonló szabályokat, kifejezéseket. Itt is megjelenik, hogy elsődleges a civilek védelme, illetve tisztázza – abban az esetben beszélhetünk on-line háborús cselekményről, ha a kibertámadás következtében emberek halnak meg, vagy kiemelt anyagi kár keletkezik.

A kórházakhoz hasonlóan kiemelt védelmet élveznek itt is a vízi és nukleáris erőművek, ezek ellen nem lehet támadást indítani. A jegyzőkönyv azt is meghatározza, hogy milyen ellencsapás megengedett on-line háborús cselekmények esetén: akár hagyományos fegyveres támadás is megengedett válaszként, s mivel katonának minősülnek, így maguk a támadást indító hackerek is áldozatául eshetnek.

Nem meglepő tehát, hogy a Tallin Manual megjelenése hatalmas visszhangot keltett. Irán azonnal reagált, bejelentve, hogy ezek alapján amerikai valamint izraeli támadás érte az országot, utalva ezzel arra a Stuxnet-féregre, mely 2009 végén és 2010 elején mintegy ezer urándúsító centrifugát tett működésképtelenné a natanzi nukleáris központban működő kilencezer közül. Az incidens nem kavart nagy port, mivel Irán nem tudta az érintett országok támadásban való részvételét hitelt érdemlően bebizonyítani, ami egyben a legnagyobb problémára is rávilágít: rendkívül nehéz és bonyolult folyamat a kibertámadók felkutatása.

A hackerek láthatatlanul tevékenykednek, így többnyire olyan információk alapján lehet csak nyomozni, mint hogy ki volt a célpont, kinek állt érdekében megtámadni, illetve milyen információk segítségével tudták a támadást végrehajtani. Egyszerűbb a helyzet akkor, ha egy már hagyományos eszközökkel zajló fegyveres konfliktus során, mintegy ötödik hadoszlopként lépnek akcióba a hackerek. Ilyenkor nem kétséges, hogy ki a „megrendelő”.

Valószínűleg évek kellenek még hozzá, hogy ez a fajta jogi szabályozás igazi, jelentős eredményeket tudjon felmutatni. Mivel nyilvánvaló, hogy a kibertérben ellenőrizhetetlenül, és eddig szabályozatlanul zajlottak és zajlani is fognak olyan folyamatok, amelyek képesek egy egész ország működését befolyásolni, így hazánk védelme szempontjából rendkívül fontos olyan stratégiák, folyamatok megteremtése, melyek egy esetleges kibertámadáskor alkalmazhatók.

Fotó: Galovtsik Gábor