Hozzászólások

Elsőként *Cserhát András*, a Paksi Atomerőmű Zrt. főosztályvezetője, nukleáris mérnök, fizikus, a ZMNE doktorandusza kért szót. Az iráni nukleáris létesítmények elleni hackertámadás kapcsán a sajtóban, főként a bulvármédiában megjelent híradások nyomán, sokan összetévesztik a dúsítóművet az atomerőművel – kezdte mondandóját. A Stuxnet nevű vírus három rétegben támad. Jellemző módon USB-tárolókról fertőz valamilyen különálló számítógépet vagy hálózatot, ami nem szükségképpen kapcsolódik az internetre. A következő réteg egy Siemens-típusú konfiguráló számítógép, amelyet kábellel szokták összekötni a programozható logikai kontrollerekkel (PLC). A vírus ezt követően lép közvetlen kapcsolatba a technológiával. A támadás eszköze adott esetben a Siemens közepes és nagy PLC-je, a technológiát pedig az urándúsító gázcentrifugák jelentik. Utóbbiak arra szolgálnak, hogy a természetes állapotú uránt olyan mértékben dúsítsák, ami után az alkalmassá válik atomerőműben történő felhasználásra. A dúsítóban mintegy 2 méteres házban igen gyorsan, 1200 Hz fordulatszámmal forgó rotorok működnek, amelyek kerületi sebessége a hangsebesség tartományába esik. Így a rotorba bekerülő gázból a nehezebb izotópok kicsapódnak a centrifuga szélére, a könnyű (ti. a 235-ös) izotópok pedig középen gyűlnek össze és ezt ki lehet szívni. Ezeket a centrifugákat szokták láncba kötni. A lánc egymás utáni fokozatokból áll és a fokozatokon belül párhuzamosan kötött centrifugák is vannak. A centrifuga-kaszkád optimális elrendezése a 15 fokozatból álló, 164 darab egység. 2009-ben mintegy 1000 darab centrifugáról kellett leüríteni az urán-hexafluorid gázt. Röviddel ezután le is kellett szerelni további 1000 darabot. Nagy valószínűséggel ekkor következett be az a támadás, ami miatt csökkent a centrifugák száma, és ami kb. két évvel vetette vissza az iráni nukleáris programot. Ennek ellenére 2010-ben növekedett a dúsítói kapacitás, csak sokkal kisebb mértékben, mintha a támadás elmaradt volna. A közepes PLC-re visszafejtették a támadókódot. A támadás lényege: a kód kivárásokkal és rövid támadószakaszokkal úgy operál, hogy felpörgeti a centrifugákat 1400 Hz-re, ezzel majdnem a törésig viszi el a rotort, utána pedig lefékezi azokat 2 Hz-re. Így a tengely oda is meg vissza is kétszer megy át a kritikus fordulatszámon, ami egyfelől rongálja a centrifugákat, másfelől ilyenkor összekeveredik a korábban már szeparált urán-hexafluorid a még szét nem választott gázzal. Összességében nem igaz, hogy az iráni nukleáris infrastruktúra minden elemét érintő támadásra került volna sor. A támadásokkal kapcsolatban számos feltételezés látott napvilágot anélkül, hogy kiderült volna, ki áll a

támadás hátterében. Az viszont tény, hogy ez a legkifinomultabb számítógépes vírus, amelyet az elmúlt időszakban készítettek. Alkalmazásával korszakhatárt értünk el a kritikus infrastruktúrát, így a nukleáris energetikát veszélyeztető vírusok fejlesztésében, amelyen valószínűleg sok helyen dolgoznak ma is. A Stuxnet-vírus tehát valóban veszedelmes.

Prof. dr. Haig Zsolt mk. ezredes hozzászólásának indításaként annak a reményének adott hangot, hogy sikerült előadásában érzékeltetni, miszerint az információs műveletek igen szerteágazó tevékenységet jelentenek. A fizikai térben, a tudati térben és a fizikai valóságban egyaránt alkalmazhatók olyan információs megoldások, amelyek alkalmasak befolyásolásra. *Rózsa* ezredes úr foglalkozott előadásában a Magyar Honvédség vonatkozó doktrínájának jelenlegi állapotával – emlékeztetett az ezredes. A Magyar Honvédség képességei tekintetében érdemes lenne elgondolkodni azon, hogy az említett befolyásoló-képességeken (tömegtájékoztatás, CIMIC-, PSYOPS-tevékenység stb.) túl az információs rendszerek támadhatósága és védelme terén is lenne még mit tenni. A számítógépes műveleti képesség számos fontos, egymással összefüggő területet jelent: jelenti a számítógépes rendszerekbe történő behatolást felderítési céllal; a hálózatok ellen irányuló támadást, amely valamely képesség rombolására irányul; jelenti a védelem kérdését, tehát saját rendszereink működésének biztosítását. Ha más nem is, de a védelem doktrínákban történő megjelenítése mindenképpen indokolt és fontos akár békeműködés, akár a műveleti vezetés szempontjából. Ami a támadóképességeket illeti, ez az a terület, ahol nem szükségeltetik hatalmas költség, technikai eszközállomány, csupán jól képzett emberek, vagyis megfelelő szürkeállomány. Az etikus hackerek, akik jó cél érdekében hajtanak végre támadásokat, alkalmasak lennének erre. Ilyenek vannak nem kevesen a civil szférában, de a Magyar Honvédség kötelékében is. Nem feltétlenül költségigényes eszközök beszerzésén múlik megfelelő képességeink kialakítása. Indokolt tehát, hogy a problémával ne csak teoretikus, hanem gyakorlati szempontból is foglalkozzanak az erre illetékesek.

Nagy szükség van a Hadtudományi Lexikon újabb kötetére, amelyben le lehet végre írni, hogy valójában mit is jelent a kíberhadviselés – vélekedett hozzászólásában *prof. dr. Kovács László* mk. alezredes. Annál is inkább, mivel *Várhegyi* ezredes úr előadásában már felmerültek az újabb problémák, a kíberhadviselés második hullámának sajátosságai. Az elhangzott előadásokban nem esett szó a szakemberek felkészítéséről, az oktatásról. De vajon kikből lehet akár a védelem, akár a támadóműveletek számára szakembereket képezni? Nos, legalább 10–15 éves szakmai tapasztalat kell ahhoz, hogy valaki például etikus hackerré váljon, hogy speciális információvédelmi szakember lehessen. Ilyen felkészültségű embereket keresnek ma az üzleti szférában, Magyarországon is, hiszen ők tudják: ha nem védekeznek, akkor könnyen áldozatul esnek. Ugyanakkor ezek a szakemberek nem rendelkeznek biztonsági fogalmakkal. Itt, az egyetemen juthatnának azokhoz a biztonsági és védelempolitikai elvekhez, amelyek munkájukhoz szükségesek. Mindez integrálható akár a nemzetbiztonsági képzésekbe, akár az egyetem hagyományos képzéseibe. Az ehhez szükséges tudás ma az egyetemen rendelkezésre áll. Magyarországot is bármikor érheti olyan támadás, amelynek elhárítása szükségessé tenné ilyen erők alkalmazását. Kérdés, hogy a védelem mellett kell-e nekünk támadó képesség is.

Tudjuk, hogy kell, hiszen annak monitorozása, hogy kik a potenciális ellenfeleink, feltételezi azt, hogy a támadásra azonnal tudjunk reagálni. És a védelem nagyon sokszor a támadásban realizálódik.

Úgy érzi, hogy a mai konferencia elsősorban az információs műveletek technikai oldaláról szól és az ő mondandója a „kakukktojás" – jegyezte meg hozzászólásában *Rózsa Tibor* ezredes. A Magyar Honvédség afganisztáni műveletei és az MH ÖHP-nél előkészületben levő doktrína kétségkívül ezen alapszik, de nemcsak ezen! A doktrínának természetesen ösztönzést kell adnia a technikai oldal számára is és reméli, hogy ehhez is rendelkezésre állnak majd a szükséges erőforrások. Olyan doktrínát szeretnének készíteni, ami gyakorlati útmutatást ad a felhasználóknak. Olyat, ami bizonyos időtávon helytálló, hiszen a körülmények, a szövetség Afganisztánban alkalmazott stratégiája, taktikája folyamatosan változnak. E változásokhoz természetesen ellenfeleink is alkalmazkodnak. Miért közelíti a szövetség főként befolyásolási oldalról az afganisztáni műveleteket? Afganisztánban az amerikaiak kiterjedt eszközrendszerrel rendelkeznek. Mindent és mindenhol látnak és tele vannak információval. De az okokat, azt, hogy miért történik az, ami történik, még mindig nem tudjuk. Nem tudjuk például, hogy a tálibok, akikkel küzdünk Afganisztánban, miért csinálják azt, amit csinálnak, azt, hogy tulajdonképpen kik azok a tálibok. Annak ellenére tehát, hogy rendkívül sok információval rendelkezünk róluk, sokszor nem tudjuk az információt értelmezni, feldolgozni. Az információ önmagában tehát kevés ahhoz, hogy úgy tudjuk befolyásolni a magatartásukat – különösen a gondolkodásukat hosszú távon –, hogy számunkra is elfogadható körülmények alakuljanak ki a térségben. Arra irányulnak az erőfeszítések, hogy a rendelkezésünkre álló információkat tudássá tudjuk alakítani.

2001. szeptember 11. történései kapcsán felmerült benne az a gondolat, hogy amit korábban rendőri, bűnügyi problémaként kezelt terrorizmus valójában katonaivá vált. Bush elnök a romokon állva úgy fogalmazott, hogy Amerika hadban áll – idézte fel a sokak számára emlékezetes eseményt *Szövényi György*, a Magyar Rendészettudományi Társaság Biztonságpolitikai Tagozatának vezetője, a műszaki doktori iskola hallgatója. Ez – megítélése szerint – korszakhatárt jelentett, hiszen a korábban rendőriként, titkosszolgálatiként kezelt kihívás katonaivá is vált. A cyberterrorizmusról hallottak déjà vu-érzést keltettek benne. A kérdés: vajon felmerült-e már végre annak az igénye, hogy együttműködés alakuljon ki a katonai és rendőri szakemberek, esetleg a védekezésre sokat áldozó civil szféra képviselői között a képességek összehangolt fejlesztése érdekében. Csupán a saját eszközökkel egyik szférában sem kezelhető hatékonyan a probléma, hiszen, ahogy Einstein megállapította: *a problémákat nem lehet ugyanazzal a gondolkodással megoldani, mint amivel előidézték azokat.*

A cyberhadviseléshez erősen kötődnek, politikailag korrekten talán úgy lehetne mondani, extrém és radikális csoportok, amelyeknek az interneten is felbukkan lenyomata – hívta fel a figyelmet egy igen veszélyes jelenségre *Molnár Bálint*, a Corvinus Egyetem egyetemi docense. És ezek a lenyomatok nemcsak a Facebookon és más közösségi portálokon találhatók meg, hanem a különböző honlapokon, amelyek felhasználása jellemző az említett csoportokra. Különösen az al-Kaidára, amely kiterjedten alkalmazza üzeneteinek közvetítésére a különböző képformátumokat, a

sztenográfiát. Az internetvilág mögött jelentős kapcsolati hálók alakulnak ki. Ezen a ponton különböző tudományterületek: társadalomtudományok, azokon belül különböző viselkedési modelleket, nyelvtani, nyelvészeti szinten megjelenő kifejezéseket, azoknak konkrét cselekvéssé és konkrét társadalmi hatássá történő átalakulását tanulmányozó kutatási területek képviselői kellene, hogy találkoznak. A cybertérben tehát hálózati kapcsolatok alakulnak ki. Ezek ellenében folytak és folynak kutatások, amelyek közül még az egyszerűbbek is hatalmas erőforrásokat igényelnek. Hiszen például egzotikus (arab, fárszi stb.) nyelven készült honlapokat, adatbázisokat kell átvizsgálni, elemezni, feltárni a kapcsolati hálókat. Mindez egyfajta felderítés, védelemre való felkészülés. Nagyon nagy jelentősége volna annak, ha kitalálnánk, felismernénk azokat a mérőszámokat, társadalmi jelentőségű indikátorokat, amelyek segítenék a társadalmak, a globalizálódó világ figyelmét felhívni az esetleg itt rejlő veszélyekre.

Kocsis Márton ny. mk. ezredes, a Magyar Védelmiipari Szövetség főtitkára rövid hozzászólásában elmondta, hogy az általa képviselt szövetség támogatja a különféle érintettek közötti együttműködést és felajánlja abban tagszervezeteik közreműködését.

A Rendészettudományi Társaság képviselőjének felvetése ismételt hozzászólásra ösztönözte *dr. Kovács László* mk. alezredest. A cyberbűnözés, a terrorizmus elleni fellépés nemcsak katonai, de nem is csak rendőri feladat – vélekedett a professzor. A tevékenységüket beszüntető szervezetek eddig főként rendőrségi, illetve nemzetbiztonsági ellentevékenység miatt szüntették be műveleteiket. Másfelől viszont Németországban vagy az USA-ban a hadsereg tart fenn cybervédelmi és támadó szervezeteket. A kettő közötti átjárás nálunk is szükséges, ezért is örül a kezdeményezésnek. Az egyetem szakemberei a civil szervezetek, a nemzetbiztonsági szolgálatok felé már nyitottak és jó az együttműködésük a nemzeti hálózatbiztonsági központtal. A Nemzeti Nyomozóirodával a felső vezetés szintjén azonban nem igazán sikeres az együttműködés, legfeljebb a kutatók közötti kapcsolattartás működik. A kapcsolatkeresés valószínűleg nem az egyetem feladata, de tanácsaikkal, kezdeményezéseikkel talán befolyásolni tudják az illetékeseket.

Prof. dr. Szabó József ny. vezérőrnagy, az MHTT korábbi elnöke elmondta, hogy immáron 20 éve tanítja az űrdinamikát a műegyetemen, és foglalkozik a világűr megismertetésével. A hallottak alapján úgy érzi, az általa kutatott terület – egyebek mellett a távközlés, a meteorológiai előrejelzések révén – szorosan kapcsolódik az elhangzott előadások mindegyikéhez. Örömére szolgál, hogy az űrdinamika rejtelmeinek oktatása végre a ZMNE-n is megkezdődik.

A Nemzeti Nyomozó Iroda csúcstechnológiai bűnözéssel foglalkozó osztályának jelenlévő képviselője rövid hozzászólásában arra hívta fel a figyelmet, miszerint az információtechnológiai háttérrel rendelkező cégek hatalomhoz jutnak pusztán annál fogva, hogy információkkal rendelkeznek, illetve kisebb cégek az általuk biztosított szolgáltatások keretében tárolják információikat. Munkatársai nevében elmondta, hogy üdvözlik és elfogadják az egyetem szakembereinek az együttműködésre vonatkozó kezdeményezését.

Kun István, a Budapesti Kommunikációs Főiskola tanára örömének adott hangot, hogy részt vehetett ezen az érdekes tanácskozáson. Három kérdése van. Ezek a

következők: vajon ki állhat az iráni létesítmények elleni informatikai támadás hátterében, vajon mekkora számítástechnikai apparátusra van szükség egy ilyen támadáshoz és képesek-e terrorista szervezetek ilyen eszközök előállítására. Szívesen hallott volna többet a Várhegyi professzor úr előadásában említett intuitív tudásról. A szovjet vezérkari akadémián egykor fontos, oktatandó ismeretanyag volt a sakkjáték, amely éppen az intuitív, stratégiai képességek fejlesztéséhez járul hozzá. A sakkhoz hasonló távol-keleti go nevű játék legalább ilyen hatékony a maga nemében. Sőt, annak variációs lehetőségei meghaladják a sakkét. Amíg a sakktudás számítógéppel ma már igen eredményesen modellezhető, addig ez a go játékra nem érvényes. *Kun* professzor úr kérdésére *prof. dr. Kovács* alezredes vállalkozott gyors válaszra. Elmondta, bár feltételezések vannak arra vonatkozóan, hogy kik hozták létre a Stuxnet-vírust, ezt alátámasztó egyértelmű bizonyítékok nem állnak rendelkezésre. Egy ilyen vírus kidolgozása óriási összegeket, szakapparátusokat igényel, amiből következik, hogy feltehetően államok állnak a háttérben. A mai terrorszervezetek önerőből valószínűleg nem képesek annak kifejlesztésére, illetve szakszerű alkalmazására, de a vírusoknak virágzó piaca van, és még inkább az lesz.

Az utolsó hozzászólóként szót kérő *dr. Kis-Benedek József* ny. ezredes arra hívta fel a figyelmet, miszerint a mai tanácskozáson vizsgált probléma nem csak katonai, vagy rendőri kérdés, annak nagyon sok polgári vonatkozása is van. Különböző területek találkozásával kell számolni, tehát komplex megközelítésre van szükség. Nyilván vannak kormányzati feladatok is ezzel összefüggésben, és bár ma nincs informatikai minisztérium, megvan itthon is a szakterület felelős kormányzati szerve. A katonák, rendőrök, nemzetbiztonsági szakemberek szintjén nem árt kezdeményezni ebben a kérdésben, mert az idő túlléphet rajtuk.