HANKISS ÁGNES

Kiberbiztonság: az Európai Parlament feladatai

Engedjék meg, hogy megköszönjem a megtisztelő meghívást és - ha röviden és vázlatosan is - bemutassam Önöknek, hogy a kiberbiztonság vonatkozásában milyen kérdéskörökkel foglalkozik az Európai Parlament.

Mindenekelőtt két olyan állítás fogalmazható meg, amelyben mindenki egyetért, aki így vagy úgy kiberbiztonsággal foglalkozik. Az egyik, hogy a kiberbiztonság, illetve a kiber-fenyegetettség a következő évtizedek egyik legfőbb biztonsági kihívását jelenti. A másik, hogy a kiberbiztonság megvalósítására irányuló erőfeszítések jelenleg elég fragmentáltak, azaz a különböző szereplők hatékony együttműködése még hagy maga után kívánnivalót. Ahogyan az Európai Parlament nézőpontjából látom, a kiberbiztonság területén még komoly problémákat okoz az a fajta párhuzamosság, amely az energiák herdálásával és hasznos információk elsikkadásával járhat. Nem véletlenül ismételgetjük már-már mantraként, hogy milyen fontos a kooperáció, megvalósulását azonban a gyakorlatban számos körülmény nehezíti. Engedjék meg, hogy megemlítsek egy apró példát. Múltkoriban, egyik parlamenti szakbizottságomban vendégül láttuk az Európai Unió Hírszerzési Központjának (Intelligence Center, IntCen) a vezetőjét. Ez a hivatal, bár műveleti felhatalmazással nem rendelkezik, a terrorelhárítási koordinátor hivatala mellett, az Európai Unió egyik legfontosabb értékelő és elemző központja. A találkozón feltettem azt a kérdést, hogyan áll az együttműködés az Intcen és az Unió védelmi - katonai szervei között. Az Intcen vezetője némi tűnődés után azt felelte: „szoktak kérni tőlünk információkat, amit mi megadunk, mi is szoktunk kérni, de még soha nem kaptunk egyet sem”.

Az Európai Parlament gyakorlata is a párhuzamosságot tükrözi. A kiberbiztonság kérdésével több szakbizottság is foglalkozik. Ez egyik a Biztonság- és Védelempolitikai albizottság, amelyben magam is dolgozom. A másik az Állampolgári, Jogi, Bel- és Igazságügyi bizottság, amely igen széles területet fog át, emberi és kisebbségi jogoktól a rendvédelemig. Magam ezen belül a szervezett bűnözés és a terrorelhárítás területével foglalkozom. Visszatérő tapasztalatom, hogy miközben a kiberbiztonság témája mind a két szakbizottság agendáján előkelő helyen szerepel valójában alig van átjárás a két bizottság munkája között. Míg a Biztonság - és Védelempolitikai albizottság elsősorban a kiberhadviselés és a nagyobb horderejű kibertámadások

veszélyével és elháríthatóságával foglalkozik, a Bel- és Igazságügyi bizottság elsősorban a kiberbűnözés kihívásait tartja napirendjén. Csupán a kritikus infrastruktúrák védelme és a kiberterrorizmus fenyegetése jelent közös nevezőt a két bizottság tevékenysége között.

Ami a kiberhadviselést illeti, ahogyan mások is hangsúlyozták, a kiberhadviselés ma még inkább a jövő rémképe, mint közvetlenül fenyegető valóság. A legsúlyosabb incidens, az észtországi informatikai rendszer megtámadása volt 2007-ben. Az Oroszország és Grúzia közötti konfliktus során komoly támadások érték a grúz kormányzati IT-rendszereket, súlyosan gyengítve Grúzia védelmi képességeit. Ugyancsak az IT-rendszerek, és rajtuk keresztül a társadalmak, államok sebezhetőséget állította a figyelem fókuszába egy sor olyan kíber-támadás, amely más NATO-országokat ért az elmúlt évtizedben. Az Egyesült Államokat ért egyik támadás alkalmával például 22 kormányhivatal és tucatnyi olyan szerződéses honvédelmi partner is kárt szenvedett, akik védett katonai titkokat őriztek. Ezek az incidensek nyilvánvalóvá tették, hogy a nemzetállamok nem csupán célpontjai lehetnek súlyos kiber-támadásoknak, hanem ugyanakkor maguk is képesek az IT-rendszereken keresztül intézni támadásokat más országok vagy nemzetközi szereplők ellen. A kíbervédelmi képességek fő letéteményese ma a NATO 2008. elejére körvonalazódott a NATO új kíbervédelmi stratégiája, amely lefektette a szövetség kíber-politikájának három alappillérét. Ezek: a biztonság, a szubszidiaritás és a párhuzamosságok kiiktatása. A 2010-es lisszaboni döntés értelmében a kíbervédelem kiépítése folyamatosan és önállóan napirenden lesz a NATO stratégiai célkitűzései között. Az új stratégiai célok kidolgozása mellett a NATO végrehajtja olyan már meglévő struktúrák szükséges megújítását, mint amilyen például a NATO Számítógépes Biztonsági Események Kezelése (CIRC). Fő cél egy továbbfejlesztett „Kíbervédelem 2.0” kialakítása a teljes körű védelem érdekében. Érdemes megemlíteni azt is, hogy a válságövezetekben a NATO olyan „ernyőt” hozott létre, amely a kommunikáció biztonságát hivatott szavatolni.

Több konferencián, amelyen részt vettem, felmerült az a kérdés, hogy a NATO 5. cikkelye, azaz a szolidaritási cikkely, érvényes-e súlyos kibertámadás esetében. Ahogy látom, a NATO vezetőinek egyértelmű álláspontja az, hogy a kibertámadás nem eshet az 5. cikkely érvénye alá, magyarán, ha egy NATO tagországot komoly kibertámadás érne, a NATO katonai erővel nem kelne a védelmére. Ugyanakkor abban mindenki egyetért, hogy a 4. cikkely, amely előírja a közös fellépést és egymást megsegítését, garantálhatja a tagországok védelmét. Kérdés, hogy ennek mennyi a realitása, de az biztosan nem árt, ha van kidolgozott, saját védelmi rendszerünk is.

Ami a kiberkémkedést illeti, három különböző változatát érdemes megemlíteni.

Az egyik, amikor a kiberkémkedés személyes titkok megszerzésére irányul. Az illegális úton megszerzett szenzitív adatok használhatók zsarolásra vagy a kényszerítés és befolyásolás bármilyen más formájára. A másik, azok a többségükben ipari-üzleti kémkedés körébe vágó esetek, amikor cégek akarják megtudni egymás titkait és a piaci versenyben hasznosítani. A harmadik, amely a legközelebb áll a kémkedés hagyományos formáihoz, országok között zajlik. Az igazság az, hogy a dolog természeténél fogva, erről, mi képviselők keveset tudhatunk, de annyit talán érdemes megemlíteni, hogy szakértők szerint az Európai Unió és maga a Parlament is erősen kitett a kémkedés, és ezen belül a kiberkémkedés minden lehető formájának.

A kiberterrorizmust mindenképpen meg kell különböztetni a puszta vandalizmustól. Azt, hogy egy jól képzett hacker belép egy rendszerbe és szándékosan rombol, nem volna értelme terrortámadásnak tekinteni. A kiberterrorizmus meghatározásában, ahogyan a hagyományos terrorizmus definíciójában is, alapkritériumnak kell tekintenünk az ideológiai, politikai vagy vallási célképzetet. Ha az ideológikus töltet hiányzik, kiberterrorizmusról aligha beszélhetünk. Kiberterrorista akciónak az tekinthető, ha a hagyományos terrorizmus információs infrastruktúrákba behatolva és azokat céljaira felhasználva a kritikus infrastruktúrák ellen indít támadást. Az ismert esetek igen különbözőek. Primer változata védett információk megszerzésére irányul. 2003-ban Afganisztánban például találtak egy olyan terrorista kézikönyvet, amiben rengeteg adat az amerikai védelmi minisztérium honlapjáról származott. Donald Rumsfeld védelmi miniszter elrendelte, hogy szűkítsék a honlapot, és szorítkozzanak minimális adatközlésre. Később kiderült, hogy a terrorisztikus szándékú hackelések a legkülönbözőbb honlapokról szedik össze azokat a részinformációkat, amelyekből azután összerakják a képet. Kétségkívül lehetséges a legkülönbözőbb internetes helyekről leemelni olyan információkat, amelyek önmagukban véve ártalmatlanok, de kiadhatnak egy olyan egészet, amely igen veszélyes tudást adhat illetéktelen kezekbe.

Az Internet számos lehetőséget kínál propagandára és toborzásra is. Újszerű elem, hogy míg korábban propagandisztikus célra olyan filmeket gyártottak, amelyben mondjuk Oszama Bin Laden ül egy széken és egy kamerába monoton szónokol, mára a terroristák is rájöttek arra, hogy a fiatalokat jobban el lehet érni flashmobokkal, tehát műfajt váltottak, és a propagandisztikus üzeneteket szívesen csomagolják modernebb köntösbe, tarka animációkba. Használható az Internet felkészülésre is. Közismert, hogyan lehet

szert tenni bombagyártásra alkalmas ismeretekre. Terrorista csoportok az internet segítségével tarthatják egymással a kapcsolatot, egyeztethetik stratégiai terveiket és egy-egy terrorista akció konkrét lépéseit. Az internetről letölthető és viszonylag könnyen kezelhető titkosító programok segítségével biztosíthatják, hogy kommunikációikhoz illetéktelenek ne férjenek hozzá. A titkosítás ismert megoldása az is, hogy a titkos információkat beépítik látszólag közömbös és ártalmatlan tartalmakba, például kódolt szövegrészekbe, képekbe vagy hangfájlok háttérzajába. Újszerű trend, hogy azokat a részleteket, amelyekből az üzenet összerakható, egymástól távol eső, közömbös és ártalmatlan tartalmakba rejtik.

A kibertér a terrorfinanszírozás szempontjából is kiaknázható. Csalás, bankkártya-feltörés és adománygyűjtés sajátos formáit dolgozták már ki. Például a Hezbollah, mint ismert, külön oldalt tart fenn, ahol különböző bújtatott csatornákon keresztül adományokat gyűjtenek. Az Európai Bizottság most dolgozik a terrorfinanszírozással kapcsolatos jelentésen, amely várhatóan jövőre kerül az Európai Parlament szakbizottsága elé. A kiberterrorizmus elméletileg lehetőséget nyújthat erőszakos támadás végrehatására is. A legnagyobb fenyegetést a kritikus infrastruktúrák, illetve a kritikus informatikai infrastruktúrák megtámadása jelenti.

Az Európai Parlamentben nemrégen készült erről jelentés, amelynek véleménykészítője voltam a szakbizottságom részéről. Engedjék meg, hogy idő híján csupán egy-két szempontot említsek meg, amelyet a véleménytervezetembe bevettem. Az egyik az interdiszciplináris megközelítés szükségessége. A védelem fontos területe a jogharmonizáció, az oktatás, különböző képzési tréningek, a gyengébben teljesítő tagországok felzárkóztatása, ami szoros együttműködést feltételez az egyes területek között. A jelentés a kritikus infrastruktúrák meghatározásának befejezését sürgeti, ez ugyanis uniós szinten még nem történt meg. Kiemelném, hogy Magyarország már felállított egy tételes listát, amellyel élen jár a tagországok között. A magyar kormány megjelölte azokat a kritikus infrastruktúrákat, amelyekre az ország védelme érdekében különös figyelmet kell fordítani. Éspedig: energiaellátás, közművesítés, közlekedés, szállítás, távközlés, elektronikus adatforgalom, informatikai hálózat, bankrendszer, szolgáltatások, média, ivóvíz, élelmiszer alapellátás, egészségügyi biztosítás. A véleménytervezetben sürgettük a tagállamokat, hogy hozzák létre a maguk CERT-jét, amely még nincsen készen minden tagállamban. Sokáig nyitott kérdésként feküdt az Európai Parlament, az Európai Bizottság és a Tanács asztalán, hogy létrehozzunk-e egy önálló EU CERT-et, a nemzeti CERT-ek fölött.

Úgy tudom, hogy ezt végül elvetették, mivel a legtöbb tagország amellett van, hogy a nemzeti CERT-ek laza szövetségként működjenek együtt, de külön uniós ügynökséget helyezni föléjük nem indokolt. Javaslatot tettem a véleménytervezetben arra is, hogy a kritikus informatikai infrastruktúrák meghatározásába belefoglalhatnánk minden olyan rendszert, amely szenzitív személyes adatokat tartalmaz, például egészségügyi adatbázisok, stb. Kiemeltük a páneurópai gyakorlatok szükségességét is, illetve az egységes fenyegetés-értékelő rendszer mielőbbi létrehozását. Hangsúlyoztuk továbbá az állami és a magánszektor közötti együttműködés jelentőségét, legyen szó akár internetbiztonsági cégekről, szoftver vagy hardver készítőkről, online rendszerek üzemeltetőiről, hiszen a magánszektorra nagyon komoly szerep hárul a közös védelemben, mivel tudásban általában az állami szektor előtt jár. A magánszektort valahogyan rá kell bírni arra, hogy prioritásainak listáján a haszonszerzést sorolja kicsit hátrébb és a védelmet egy kicsit előbbre. Ehhez azonban hozzá kell tennünk valamit. A magánszektor képviselői részéről felmerül rendre az az igény, hogy a jogszabályok ne legyenek olyan szigorúak, hogy ha belépnek egy rendszerbe és ott veszélyt észlelnek, nyugodt lélekkel jelenthessék, ne kelljen attól félniük, hogy megvádolják őket azzal, hogy illetéktelenül léptek be valahova. Ez a szempont megfontolandó, ha ez az együttműködés ára.

A kiberbűnözés és szervezett bűnözés szerteágazó össszefüggéseit éppen csak érinthetjük itt. Tipikus formája a pénzmosás, a felül-alul számlázások, online aukciók, ahol túlfizetik, amit megvesznek. Vagy az online szerencsejáték, amelyen belül külön is megemlíthetők a karibi off-shore-okba áramló pénzek. Ma szervezett bűnözői csoportok felelősek az adatlopások 80-90 százalékáért. Riasztó mértékű az orosz és oroszajkú szervezett bűnözés térhódítása a kíberbűnözés terén. Az orosz és oroszajkú szervezett bűnözés, amelynek érdeklődési köre az ingatlan értékesítéstől, az illegális fegyverkereskedelmen át a műkincs-csempészetig sok mindenre kiterjed, mára élen járnak a kibertér illegális használatában. Vírusok gyártásával és hálózatok akadályozásával zavarnak meg európai és amerikai weboldalakat. Ráadásul sokszor saját embereiket sikeresen beépítik kiszemelt cégekbe. Érdekes, ahogyan a kiberbűnözés szétrobbantotta, vagy legalábbis átalakította a bűnszervezetek organigramját, ismert maffia-felépítését. Amikor egy szervezett bűnözői kör már elsősorban hackerek láncolatát jelenti, már sem szükség, sem lehetőség nincs a személyes kapcsolatoknak arra a hagyományos, „kézcsókos” változatára, amelyet a Keresztapa című filmben megcsodálhattunk. Jeffrey Robinson, az orosz maffia szakértője szerint az orosz szervezett bűnözés legalább 50 országban megtelepedett, beleértve majdnem minden európai országot, azzal a

nyilvánvaló szándékkal, hogy a világ egyik legnagyobb hatalmú érdekcsoportjává váljék. Ismert olyan eset is, amikor egy moszkvai internetes kávézóból törték fel nyugat-európai országok polgárainak bankkártyáit. Az orosz belügyminisztérium felmérése szerint 5006 bűnözői csoport mintegy százezer tagja vesz részt naponta az internetes bűnözésben. Ez megdöbbentő. Azok a szakértők, akiket Oroszországban és az orosz utódállamokban a szervezett bűnözői csoportok beszívnak magukhoz, többnyire igen magasan képzett hackerek, akik lehet, hogy puszta csínytevésként, vagy szórakozásként kezdik a hackelést, ami később főbb megélhetési forrásukká válik. Elemzők szerint szép számban akadnak közöttük olyanok is, akik a volt KGB vagy az FSZB leszerelt, vagy netán még mindig állományban lévő tagjai, az orosz titkosszolgálatok ilyen-olyan szereplői. Részvételük a kíberbűnözésben felveti a „kettős felhasználás" lehetőségét: az üzleti haszonszerzés összekapcsolását a hivatalos szervek részére végzett információszerzéssel.

Végezetül néhány megjegyzés a kiberbiztonság úniós szereplőiről. Az Európai Unió két legjelentősebb intézménye ebből a szempontból az ENISA és az EUROPOL. Az ENISA-ról Suba Ferenc beszámolója után nehéz volna mit hozzátenni, hisz ő avatott ismerője és tevőleges résztvevője is az Európai Információs és Hálózatbiztonsági Ügynökség munkájának. Az ENISA ügye nemrég került a parlament elé, és igen jelentős támogatást kapott szervezeti megújulásához. 2013-ra kell felállnia a Kiberbiztonsági Központnak, amelynek az EUROPOL lesz a gazdája. Erről korábban vita folyt, magam teljesen indokoltnak látom ezt a felállást, hiszen az EUROPOL rendkívül magas színvonalú kibervédelmi egységgel rendelkezik. Hadd utaljak például arra, milyen bravúros módon tártak fel egy 22 országra kiterjedő pedofil-hálózatot úgy, hogy többségében már kihűlt szálakon kellett elindulniuk a rekonstrukciós munkában. Megemlíteném még az Európai Védelmi Ügynökséget, ezen belül a Katonai Parancsnokságot (Military Staff), amely fontos szerepet tölt be a kibervédelem terén. A tavalyi évben megalakult az Európai Néppárt Kiberbiztonsági Tanácsadó Testülete, amelyben hárman vagyunk néppárti képviselők, egyébként európai és tengerentúli rendvédelmi vezetők és szakértők vesznek részt a munkában. Egy olyan konferenciával indítottunk, amely azt a kérdést járta körül, hogy „Kiberbiztonság. Felkészültek vagyunk-e a kiberbűnözés, a terrorizmus és hadviselés megelőzésére?" Az Európai Néppárt szándéka az, hogy a testület aktívan részt vegyen a kiberbiztonságot szolgáló együttműködés előmozdításában.

Zárásként engedjenek meg egy személyes megjegyzést. Azért is örültem annak, hogy az Európai Néppárt szakmai síkon kívánja kezelni a kiberbiztonságot, mert sajnos az Európai Parlamentben elég rossz

tapasztalatokat szereztem a szakszerűség és a politikai marketing arányát illetően. Csüggesztő és kiábrándító, ahogyan a rendvédelmi témák vitái rendre emberi jogi show-műsorrá válnak. Ne értsenek félre, az adatvédelem és a személyiségi jogok védelme alapvető jelentőségű feladat. Az azonban elég kártékony, amikor egyoldalúvá, és a rendvédelmi erőfeszítéseket paranoid túlzásokkal megkérdőjelező propagandává silányítják, elsősorban a Parlament baloldalán. Célszerű volna, ha az Európai Parlament egészének a szemléletmódjában helyreállna a kívánatos egyensúly a biztonság (security) és az adatvédelem (privacy) szempontja között.