Beszámoló

DOSz-HTO Fiatal tudós est

2015. október 30.-án került megrendezésre a DOSz - Hadtudományi osztály Fiatal Tudós Estjére. Az est címe „A kibertér, mint hadszíntér”volt. Az eladók: Prof. Dr. Kovács László egyetemi tanár, Dr. Muha Lajos főiskolai tanár, Török Szilárd kiberbisztonsági szakértő és Bányász Péter valamint Orbók Ákos a témával foglalkozó doktoranduszok voltak. Az est moderátora Berki Gábor szintén kiberbiztonsággal foglakozó doktorandusz volt.

A beszélgetés bevezetőjében a kibertér fogalomrendszerét próbálták tisztázni a szereplők. Abban mindenki egyetértett, hogy a jelenleg több féle meghatározást is használnak, mint a kibertér fogalom meghatározásánál, mint a vele kapcsolatos fogalmak definiálásánál. Az egyik közös pontkén kiemelték, hogy a hadviselésben kibertér először az információs műveletek részeként jelent meg. Ez nagyon fontos terület a hadviselésben, hiszen már a csata előtt eldöntheti melyik fél fog felülkerekedni.

A kibertér szerepe napjainkra átértékelődött, hiszen ma már a hagyományos eszközök bevetése nélkül is lehet csak a kibertér használatával komoly károkat okozni az ellenség infrastruktúrájában. Ezekre a támadásokra nagyon jó példa a 2007-ben Észtországot és a 2008-ban Grúziát ért támadások. A támadások jellemzően olyan országokat fenyegetnek amelyek internet penetrációja magas és az állam működésének egy része is ezekre a csatornákra van bízva így a támadások elérhetik céljukat.

A kibertérben használható rosszindulatú softwerek egy része már kifejezetten egy bizonyos cél megtámadására fejlesztenek ki. Ezek a precíziós „kiberfegyverek” csak akkor lépnek működésbe, ha a célpontjuk rendszerét érzékelik, így az elhárításuk is sokkal nehezebb. A leghírhedtebb példa erre a típusra a Stuxnet, amely 2008-ban megbénította az Iráni urándúsító üzem centrifugáit ezzel több évre hátráltatva az iráni atomprogramot.

A kibertér jelentette kihívások jelentős részben a civil felhasználóknál jelentkeznek. Az információ biztonság nagy szerepet kap a komplex biztonság elérésében. Az előadók kiemelték, hogy az információs rendszerek biztonsági szempontból leggyengébb láncszeme mindig az ember. Ezért nagyon fontos hogy több lábon álljon minden biztonsági struktúra. Azt a Snowden-ügy is bebizonyította, hogy a legjobb softweres és fizikai biztonság mellett is komoly kockázatot jelenthet az a személy, aki minősített adatokhoz férhet hozzá.

A beszélgetésben szóba kerültek a terrorizmus és a kibertér kapcsolata is. A legnagyobb változás ebben a témakörben hogy egy teljesen új paradigmát fedezhetünk fel az ISIS-hez kapcsolódó internetes tartalmak vizsgálatánál. a kibertér eddig is fontos terepe volt a terrorista szervezeteknek. Jellemzően a kibertérben oldották még a finanszírozásuk, a kapcsolattartás és a információk- instrukciók továbbadásának egy részét. Azonban az ISIS a kiberteret a profi marketing és a média elérésének fő eszközeként használva elérte, hogy a

célországok lakosságát komolyabb terrortámadás nélkül is a terror légkörében tartsa. (Az előadás Párizs-i terrortámadás előtt rendezték).

Az előadók kitértek Magyarország kibervédelmi képességeire is. A legfontosabb jogi szabályozások mellett fontos intézményi változások is történtek október 1.ével. a 2013.évi L. törvény módosításával megalakult a Nemzeti Kibervédelmi Intézet, amely az eddigi heterogén struktúrát váltotta fel és egy hierarchiába rendezte a kibervédelemi hatóságot(NEIH) és eseménykezelő központot(GovCERT).

Az beszélgetés két befejező témája volt a közösségi média és az okos városok szerepe a kibertérből érkező kihívások szempontjából. A közösségi médiát akár egy új biztonsági kihívásként is kezelhetjük, hiszen a nyílt forrású hírszerzés és a social engineering egyik legjobb forrása lehet az önmagról adatokat megosztó személy.

Az okos város koncepciója az információs társadalom és a dolgok internetére épül. A koncepció szerinte az élhetőbb város kialakítása szükségessé teszi, hogy az eszközeink többsége kapcsolódjon az internethez és távolról is irányítható legyen, vagy akár önműködően szolgálja a jólétünket. Ez azt jelentheti, hogy a kényelmünk érdekében lemondunk a függetlenségünk egy részéről, ami több szempontból is aggasztó lehet, ha a biztonságunkról beszélünk.

Az est végén több kérdés is felmerült a közönségben. A kérdések elsősorban arra irányultak, hogy milyen terednek várhatók a kiberbiztonság területén a jövőben. Válaszként az előadók úgy fogalmaztak, hogy sajnos a védekezők mindig hátrányban lesznek a támadókkal szemben, így nem lehet pontosan megmondani merre fejlődik ez a szakma.