„Változó környezet, változó biztonság – Kiberfenyegetések kihívásai napjainkban” című nemzetközi szakmai-tudományos konferencia záró dokumentuma

A Belügyminisztérium illetve annak Tudományos Tanácsa a Nemzetközi Kibertér Konferencia (Budapest, 2012) rendezvényéhez kapcsolódva 2012. szeptember 17-18-án megszervezte és lebonyolította a *„Változó környezet, változó biztonság – Kiberfenyegetések kihívásai napjainkban”* című rendezvényt. Komoly előrelépésként könyvelhetjük el, hogy a rendészeti szervek, a nemzetbiztonsági szolgálatok, a hazai és nemzetközi civil szervezetek és a tudományos élet képviselői tudományos igényű, közös gondolkodásának lehettünk részesei.

A résztvevők a kibertér és az Internet használatának összefüggéseit tekintették át különféle témakörökben. Rámutattak arra, hogy mennyire sokrétű, a társadalom és az állam különböző szegmenseiben jelenlévő jelenségről van szó, amelynek feltérképezése, megértése és a káros elemeinek felfedése és hatékony üldözése, a nemzeti érdekek közös konszenzusos érvényre juttatása mellett kell, hogy történjen. A *„Kritikus infrastruktúra védelmi kutatások”* szekcióban világossá vált, hogy a kiberfenyegetések és az erre adott válaszok még nem alkotnak homogén rendszert. Valamennyi érintettnek – terroristáknak, a szervezett alvilágnak, a védelmi, civil és üzleti élet résztvevőinek – más-más a motivációja, mindegyiknek sajátos nézőpontja, eszközrendszere van. Az információs társadalom informatikai függősége és az ebből fakadó új típusú kihívások nem kezelhetők pusztán technológia kérdésként. E téren különös jelentőséggel bír a civil és üzleti szféra szerepvállalása, amelyek eredményei katalizátorként jelenhetnek meg az állami szereplők tevékenységéhez kapcsolódva. Közös munkánk egyik legfontosabb sarokpontja volt, hogy az új típusú kihívások közé tartozó kiberfenyegetések eredményesebb felfedése, hatásmechanizmusuk megértése és kezelése, az együttműködés továbbfejlesztése az érdekeltek között elindulhasson.

„A civil és üzleti szféra szerepvállalása az informatikai bűnözés ellen folytatott küzdelemben” szekcióban értékes előadások hangzottak el. E szekcióban résztvevő hallgatóság tájékoztatókat hallhatott a jogalkotótól egészen a magán szektort képviselő biztonsági vezetőkig.

A létfontosságú rendszerekkel és létesítményekkel kapcsolatos elkötelezettséget mutatja az idén elfogadott új Nemzeti Biztonsági Stratégia, amely rögzíti azt, hogy hazánk kiemelten kezeli az ország mindennapi életkörülményeinek fenntartásához, a gazdaság és az államszervezet működéséhez szükséges kritikus infrastruktúrák hatékony védelmét. Ismerjük a kapcsolódási pontokat az egyes szakosított infrastruktúrák között, és kockázatelemzési módszereinkkel képesek vagyunk válaszokat adni a kritikus infrastruktúra üzemeltetése során megjelenő kihívásokra. Ugyanakkor a konferencia tapasztalatai világossá tették azt is számunkra, hogy növelve a kormányzati szerepvállalást, közre kell működnünk egy nemzeti kiber biztonsági stratégia kidolgozásában, amelyhez alapul szolgálhatnak a NATO és az Európai Unió vonatkozó stratégiai dokumentumai. A stratégiát egy információbiztonságról szóló jogszabály és annak végrehajtási dokumentumai hasznosan egészíthetnék ki. Továbbá közös elhivatottság szükséges az előzőleg említett szabályozókban előírt kötelezettségek összehangolt végrehajtásához is. A konferencia egyik tapasztalata az is, hogy a jogalkotás során támaszkodni kell a tudomány által elért eredményekre. Saját szakterületünk vonatkozásában további szerepünk lesz az egyén és a szervezet tudatosításában és az oktatási, kutatás-fejlesztési lehetőségek támogatásában.
A *„Kiberterrorizmus”* szekcióban kiváló előadásokat hallhattak a német Szövetségi Bűnügyi Hivatal és az Alkotmányvédelmi Hivatal képviselőitől, melyek gyakorlati példákkal szolgáltak arra nézve, hogy miként lehet sikeresen felvenni a harcot a kiber térben tevékenykedő ellenérdekelt

felekkel. A hazai előadók, amellett, hogy bemutatták a technológiai újdonságokat, rámutattak arra a sarkalatos problémára, hogy a technika mesteri szintű ismerete mellett szükséges a megfelelő, tevékenységüket támogató jogszabályi háttér megalkotása. Külön öröm volt, hogy az előadások széles spektrumában, a technikai megoldások taglalása mellett, helyet kapott a leginkább mellőzött „social engineering" elleni védekezési lehetőségeket bemutató prezentáció is.

A szekciókat levezető elnökök, a rendezvényt a tudományos szféra, a szabályozást képviselő állam, a szakmaiság és a biztonságkultúráért való tenni akarás találkozásának nevezték.

A belügyi tárcához kötődő feladatok – a kihívás jellegéből adódóan – akkor lehetnek sikeresen végrehajthatóak, ha a jövőben szakértő partnereink tapasztalataira támaszkodva végezzük munkánkat. Ennek során kiemelten fontos az informatikai, hálózatbiztonsági és komplex információvédelmi tevékenység, a sérülékenység-vizsgálatok tapasztalatainak megosztása, továbbá a hatósági felügyeleti tevékenység során szerzett ismeretek felhasználása.

Mivel manapság multidimenzionális térben dolgozunk, ahol globális kockázatok keletkeznek, olyan közös és konvertálható tudástartalomra van szükség, amely hasznos ismereteket nyújt a kiberfenyegetések kezelésének különböző formáihoz. A pontos ismeretszerzés érdekében a kiberbiztonság okozta problémákat helyi struktúrákra szükséges lebontanunk. Közös fellépésünknek azonban tekintettel kell lenni a rendelkezésre álló eszközök korlátozott mivoltára és az eltérő technológiai színvonalra.

Fontos számunkra, hogy felelősséget vállaljunk a Belügyminisztérium felügyelete alatt működő szervezetek cselekvési irányainak korszerűsítése érdekében, kiküszöbölve az együttműködés esetleges diszfunkcióit.

Mindemellett fontosnak tartottuk azonosítani, tartalommal megtölteni – a társadalom hosszabb távú biztonsági érdekeire tekintettel – a digitális biztonság alappilléreinek összetevőit, azokat a rendészetpolitikai, nemzetbiztonsági kérdéseket, amelyek segítséget nyújthatnak a kiberfenyegetések gyakorlatban történő kezelésére, a veszélytényezők minimalizálására.

A jövőben lehetőséget kell teremtenünk a háttérben meghúzódó bűnös viselkedésformák és kiváltó okaik társadalmi, technológiai, kulturális közegének feltárására, a közös megoldási módozatok kimunkálására. Tovább segítheti törekvéseinket, amennyiben sikerül világosan megfogalmazni a kiber- és hagyományos biztonság közötti kapcsolatokat. Különös felelősségünk a társadalom kiberbűnözéstől mentes közegének megteremtésében rejlik, amelynek eléréséhez a kezeléshez jelenleg szükséges hosszabb időintervallum csökkentése közös érdekünk.

Kötelességünk, hogy saját képességeinkkel járuljunk hozzá a nemzetközi küzdelemben a jövőben meghatározó pozíciót betöltő európai uniós kiber bűnözés elleni központ tevékenységének kialakításához, továbbfejlesztéséhez, valamint a NATO incidenskezelő speciális képességének fejlesztéséhez. Minderre tekintettel a különböző nemzetközi tapasztalatok, technológiai fejlesztések, bűnügyi és nemzetbiztonsági gyakorlatok, megoldási metódusok megvitatása szükséges a sikeres fellépéshez. Ez feltételez egy folyamatos kormányzati koordinációs tevékenységet nemzeti és nemzetközi viszonylatban is, ami elvezet bennünket az együttműködési fórumok rendszeressé tételéhez, a szakosított intézményekkel való közös munkavégzéshez. A problémakör széleskörű kormányzati érintettsége okán célszerű ágazati munkacsoportokra bontva, koordináltan végezni az egyes speciális részfeladatokat. Így fókuszba helyezhetünk olyan területeket is, mint a kiber kémkedés, a kiber terrorizmus, a kiber bűnözés és a szervezett bűnözés kapcsolata, vagy a kiber hadviselés.

Tudományos rendezvényünkön végzett munkánkkal igyekeztünk hozzájárulni a Budapesten, 2012.

október 4-5-én megrendezésre kerülő Nemzetközi Kibertér Konferencia szakmai megalapozásához. Fontos eredménynek tartjuk, hogy tanácskozásunk a problémák azonosításán túl eljutott a lehetséges megoldások feltárásáig. Szűkebb szakterületünk vonatkozásában lehetővé vált az előttünk álló kibervédelmi feladataink azonosítása, a fontosabb kommunikációs, jogalkotási és együttműködési kérdések tisztázása.