FPI/8-2/2015

SZAKMAI BESZÁMOLÓ

PADS SZAKKOLLÉGIUMI PROGRAM
2014/2015

Szakmai beszámoló

a Pallas Athéné Domus Scientiae alapítvány 2014/2015 akadémiai év őszi félévére meghirdetett szakkollégiumi programja keretében megvalósított „A kiberbiztonság aktuális kérdései" című konferenciáról

A Szent György Szakkollégium szervezésében megrendezésre került 2014. november 12-én „A KIBERBIZTONSÁG AKTUÁLIS KÉRDÉSEI" című szakmai konferencia a Nemzeti Közszolgálati Egyetem Rendészettudományi Karán. A megvalósításban közreműködő partnerek voltak az NKE Rendészetelméleti Kutatóműhely, a Rendészeti Doktoranduszok Országos Egyesülete, valamint az ORFK Bűnügyi Főigazgatósága.

A konferencia célja

A konferencia egyik kiemelt célja volt a bűnüldöző szervek és a gazdaság különféle szegmenseinek összehívása és a kapcsolataik fejlesztése, melyet sikerrel teljesített. Témánk között szerepeltek többek között a készpénz helyettesítő fizetési eszközökkel történő visszaélések elleni fellépés aktuális kérdései, és a létfontosságú rendszerelemek elleni támadások is (pénzügyi eszközök kereskedelmi, fizetési, valamint klíring- és elszámolási infrastruktúrái és rendszerei bank- és hitelintézeti biztonság). A hatékony fellépés csak közös célmegjelölésekkel és szoros együttműködésben lehetséges és ehhez kiemelten fontosak az ilyen, országos szintű rendezvények. A konferencia célkitűzése volt továbbá, hogy a XXI. századi társadalmak működésére - mind állami, mind pénzügyi-gazdasági alapintézményeire - veszélyt jelentő kiberbiztonság témakörében értékes szakmai munkára biztosítson lehetőséget. E cél elérését nagyban támogatta, hogy azon képviseltették magukat a Kar tudományos műhelyei, valamint hogy a Szakkollégium kezdeményezte valamennyi olyan szakmai

szervezet részételét, melyek a kiberbiztonság megteremtésében alapvető feladatokat látnak el. A rendezvénnyel egyúttal a Szakkollégium módot kívánt, és biztosított is arra, hogy széles szakmai közönség ismerhesse meg a programjainkon zajló élénk szakmai életet.

A támogató reprezentálása

A támogatási szerződésben foglaltaknak megfelelően a konferencia szóróanyagaként készített plakátok, hirdetmények valamint a meghívók mindegyikén feltüntettük a Pallas Athéné Domis Scientiae Alapítvány logóját, továbbá az elektronikus úton folytatott propaganda során is szerepeltettük a támogatót. A rendezvényre látogató minden személy számára biztosítottunk egy mappát, rajta a szervezők és a támogató PADS logójával. A támogató roll up hirdetőplakátját a rendezvény plenáris szekciójának és „A" szekciójának helyet adó teremben állítottuk fel. Itt helyeztük el a támogató által 30- 30 példányban biztosított könyveket (Wiedermann Helga: Sakk és póker – Krónika a magyar gazdasági szabadságharc győztes csatáiról; Lamfalussy Lectures Conferense – The Euro Dilemma: Inside or outside – Conference logbook; 2002-2013 – Válogatás Matolcsy György Heti Válaszban megjelent írásaiból). Az ingyenes kiadványok iránt nagy volt az érdeklődés a rendezvényen, valamennyi példány gazdára talált az országos szintű érdeklődést kiváltó konferencia résztvevői között.

SZAKMAI BESZÁMOLÓ

PADS SZAKKOLLÉGIUMI PROGRAM
2014/2015

A rendezvény rövid leírása

A konferencia 2014. november 12-én a Nemzeti Közszolgálati Egyetem Rendészettudományi Karán került megrendezésre. A Plenáris ülés a Kar főépületében lévő „A" teremben zajlott 13:00-16:00 óra között, majd a továbbiakban két szekció került kialakításra, melyeket 16:00 órától 18:00-ig az „A" valamint a 126-os teremben hallgathatott meg a rendezvényre látogató 121 fő érdeklődő. A továbbiakban 18:00-19:00 óra között Workshop zajlott, mely a konferencia méltó zárása volt. A konferenciát megelőzően, az ülések és szekciók szüneteiben, valamint a rendezvény zárásakor részben a támogató, részben a Nemzeti Közszolgálati Egyetem által biztosított költségkeretből biztosítottunk frissítőket vendégeink részére. A konferencia előadói a kiberbiztonság különböző területeivel foglalkozó, jelentős szakmai illetőleg tudományos eredményeket elért szakemberek voltak. Számukra a támogató által biztosított költségkeretből összeállított előadói csomagokat adtunk át. Előadásaik rövid összefoglalása az alábbiakban olvasható.

Plenáris ülés

Dr. Parti Katalin, az Országos Kriminológiai intézet kutatója: "Kiberbiztonság az állampolgárok szemével''

Az előadáson kifejtésre került, hogy mi is az online harassment, online profillopás milyen mértékű és milyen veszélyei vannak. Hangsúlyt kapott, hogy Magyarországon jelenleg több facebook felhasználó van, mint amennyi internettel rendelkező ember. Megtudtuk, hogy a ritka internethasználatból az következik, hogy kevésbé jól informáltak az emberek a világban történő változásokról. A magyar internet hozzáférés alacsonyabb (59%) az EU 27 átlaghoz képest, de nálunk a legnagyobb a növekedés a tavalyi évben (11%) Első helyen Hollandia áll 89%. Nagy veszélyt jelent, hogy a PC védelemmel ellentétben a magyar köztudatban egyelőre mobilvédelem még nem elterjedt.

Dr. Szabó Endre Győző, elnökhelyettes, Nemzeti Adatvédelmi és Információszabadság Hatóság: Magánszféravédelem a biztonság kontextusában

Az offline és online élesen nem választható el egymástól" mondattal kezdte előadását. Az előadó szerint nem hangos konfliktusra is oda kell figyelni, mely legtöbbször online zaklatás, olyan észrevehetetlen hackelések, amelyek látensek, emiatt sem a hatóság, sem a sértett nem szerez tudomást, de ennek ellenére megtörténik a jogsértés, emberi méltóság tiszteletben tartása. Az adatvédelem elveit részletesen kifejtette, ilyenekről, mint a tisztességesség, törvényesség, naprakészség, teljesség, privacy by design, ami azt jelenti, hogy már a tervezésnél be kell építeni az adatvédelmi elemeket, tehát csírájában már védekezni kell és elkerülni a későbbi érdekellentéteket. Elmondta, hogy a kamerás megfigyelésnél mik azok a követelmények, amiket mindenképpen be kell tartani, hogy az jogszerű legyen. Pl.: belépésnél tájékoztatni kell, hogy nem lehet jogellenes, valamint a törlés ésszerű határidőn belül követi. Kitért külön a magánterületes kamerás figyelésre is, erről is elmondta, hogy miket kell figyelembe venni. Beszélt a felvétel megőrzésének módjáról és idejéről (3 nap, kivételes esetben 30-60 nap). Csak megemlítésképpen szó volt a munkahelyi kamerákról és ennek a jogi szabályozásának megváltozásáról. Zárásként, viszonylag vázlatosan a biometrikus beléptető rendszerek, gps által tárolt tartózkodási helyek, személyes adattal összefüggő kapcsolatairól beszélt.

Otti Csaba, az Óbudai Egyetem, Alkalmazott Biometria Intézet munkatársa: Biztonság és big data

A 'big data' kifejezés magyarázatával kezdte meg előadását, elmesélte, hogy naponta 2500 petabájt adat is keletkezhet valamint, hogy ez egy strukturálatlan adathalmaz. Szerinte a digitális korszak a 2002-es évektől lendült be igazán világszerte, ezzel lassan-lassan leváltva az analóg technológiát. Egyes számítások szerint ez az adathalmaz 2020-ra 35 zetabájt lesz évente, ami annyi nulla, hogy elfáradunk, míg leírjuk. Példaként említette, hogy a facebookon 1 hónap alatt akár 30 milliárd mozgás is lehet, de ami ennél is lélegzetelállítóbb szám, az a youtube-n történő 1 nap alatti 4 milliárd video megtekintés. Ez az adathalmaz a

térinformációs adatkeletkezésből, számítógépek egymással kommunikálása közben is keletkezik. Megtudhattuk mik is a big data forrásai. Egyes társaságok a weboldalaikon bizonyos módszerekkel meg tudják figyelni, hogy hova kattintanak legtöbben az oda látogatók és ezáltal tudni lehet, hogy mit kell fejleszteni jobban, miken kell javítani. Nagy problémát jelent a térfigyelés, mivel a nagy felbontású, éles képet felvevő készülékek, irdatlan nagy mennyiségű adatforgalmat generálnak és ezek tárolása, illetve visszanézése nehéz feladat. Pl. 3 nap alatt 30 terrabájt forgalmat generál 50 kamera, amely 2-8 megapixeles képkockákat rögzít. Ezek után feltette a kérdést, hogy akkor számítsuk ki, hogy Londonban az 1,5 millió kamera mi mennyiséget képes összehozni. Elmagyarázta, hogy mi az adatvizualizáció, prediktív analitika és milyen biztonsági lehetőségek vannak jelenleg, és a jövőben mire lehet még számítani. Zárásként még röviden beszélt a futó projektekről, úgymint az Epoolice, Athena, Odyssey.

Dr. Nagy Zoltán András, a Pécsi Tudományegyetem Állam- és Jogtudományi Kar egyetemi docense: A 2013/40-es Uniós direktíva az informatikai rendszereket érő támadásokról

Az előadása első részében egyéb rávezető témák kerültek bemutatásra, ami különösen érdekessé tette az előadást. Az előadó olyan trükköket mutatott, amiket a bűnözők gyakran használnak, pl. piszkozatban hagynak egymásnak üzenetet mivel ennek nincsenek hálózati nyomai. Az előadásra szánt prezentációt úgy nyitotta meg, hogy egy JPEG-et kicsomagolt winrarral és abból bukkant elő a PPT file. Elmondta, hogy milyenféle támadások léteznek, úgy, mint a spyware, hacking, sniffing, stuxnet, duqu, defacing, flame kémprogram, és hogy mit is tartalmazott a 2013-as Symantec jelentés. Elmondása szerint Budapesten kb. 34.000 botnet van. Mutatott pár módszert, amivel sok pénzt csaltak el ártatlan internetezőktől, mint pl. a Raiffeisen weboldalát lemásolták és így sikerült adatokat ellopni. Kitért arra is, hogy mire figyeljünk oda, hogy mi ne eshessünk áldozatul az ilyenfajta csalásoknak, pl. mindig nézzük meg, hogy a böngészőbe https-el kezdődik-e a webcím. Elmagyarázta mi is az a fordított védelmi pénz, ami úgy szólt, hogy nem támadják meg pl. botnettel a szervert, ha fizetnek. Továbbá kifejtésre került a Stuxnet, Tyupkin malware, amelyek sok kárt okoztak

már a társadalomnak. Az előadás végén kitért arra, hogy az 2013\40 EU irányelv tulajdonképpen arra is törekszik, hogy az országok Büntetőtörvénykönyveit összehangolja a kiberbűnözés terén.

Prof. Dr. Kovács László, a Nemzeti Közszolgálati Egyetem Hadtudományi és Honvédtisztképző Kar Tudományos és nemzetközi dékán helyettes egyetemi tanár: Digitális dzsihád (kiberterrorizmus a hagyományos terrorizmus árnyékában)

Mit is jelent a dzsihád? Ez nem más, mint Allah útján való küzdelem. Az előadó bemutatott egy csokoládét ábrázoló képet, melyen az ISIS márkanév van, ami azonos terrorszervezet megnevezésével, mely egyre nagyobb és nagyobb lesz, folyamatosan növekszik, olyan mértékben, hogy több száz tagos bővülés van naponta. Ezt a bővülést még jobban segíti az az 1500 weboldal, ahol a különféle, ide kapcsolódó témákat feszegetik, és ami az embereket az iszlámhoz húzza és képes radikalizálni minket. Több újsággal is rendelkeznek az ilyen terrorszervezetek, legnagyobb és legismertebb az Inspire, amit 5 éve ad ki az Al-Kaida. Ezeken az oldalakon leírásokat lehet kapni, hogy hogyan lehet robbanóeszközt összeállítani, és egyéb illegális tevékenységekre buzdítanak. A terrorizmus fő motivátora a politikai döntés befolyásolása. Megtudhattuk, hogy egyes adatok szerint kb. 3 milliárd ember használja a netet, ezen a tömegkommunikációs eszközön pedig nagyon gyorsan és hatékonyan lehet szervezkedni.

Szongoth Richárd, a Készenléti Rendőrség, Nemzeti Nyomozó Iroda, Csúcstechnológiai Bűnözés Elleni Osztály vezetője: A kiberbűnözés rendvédelmi tapasztalatai

Előadása a köré épült, hogy a Nemzeti Nyomozó Iroda Csúcstechnológiai Bűnözés Elleni Osztály hány emberből épül fel, mik a feladatai, kivel működnek együtt, valamint hogy főleg forensic tevékenységet folytatnak, hdd-t, mobiltelefonokat olvasnak ki, híváslistákat ellenőriznek, adathordozókat elemeznek. A nemzetközi együttműködés tekintetében nagyrészt az Interpol (ICSE), Europol (FP CYBORG,FP TWINS), Empact (CYBER ATTACKS, CSE),FBI(NCEMEC, USCIE, SS, BKA, NCA) szervezeteivel

dolgoznak együtt. Megtudhattuk, hogy mit is jelent a wailing: nagy pénzes embereket céloznak meg és az ő pénzüket húzzák le. Statisztika alátámasztja, hogy annak ellenére, hogy az adatok ellopását célzó levelek nagymértékben kiszúrhatóak, látható hogy nem igaziak, 100 emberből kb. 5 ember ennek ellenére mégis pórul jár. Röviden beszélt az Anonymous cybercsoport 2012-es felemelkedéséről, és az E-banking csalásokról. Mivel feladata az Osztálynak a gyermek pornográfia elleni védekezés, így erről is említést tett, elmesélte hogyan is működhet a gyermekek online kizsákmányolása, ilyenek a TCSO, grooming (befolyásolás), sextortion (zsarolás), livestream, selfmade.

Zala Mihály, a Nemzeti Biztonsági Felügyelet elnöke: Kiberbiztonság és rendvédelem

Előadását nemrég megjelent újságcikkek bemutatásával kezdte, ami gondolatindító volt arról, hogy mi is folyik jelenleg a világban. A cikkek a következőek voltak: „Rejtélyes drónok a francia atomerőmű felett"; „V. kerület felett is rengeteg drón van"; „USA legfélelmetesebb fegyvere a Google"; „Lehet TOR-t használni a facebookon". Szerinte az adatgyűjtés megelőzésére nincs egyelőre válasz egy országban sem. Az adatokat tároló infrastruktúra 70%-a magánkézben van. Érdekes megállapítást tett, miszerint minden politikai esemény után hackertámadás van, ami következtet arra, hogy a hackerkedésnek igenis van politikai megbízatási szintje. Rövid fogalommagyarázat következett arról, hogy mi is az at insource, outsource? Felhívta figyelmünket, hogy jelenleg Magyarországon, de nem csak itt, nagy az alulképzettség a rendszergazdák, egyéb informatikához értő emberek körében. Elmondta, hogy alátámasztható az a tény hogy a kiberfelkészültség és a GDP veszteség fordítottan arányos. Statisztikai adatokat mutatott a kiberfegyverkezést végző, továbbá országokra lebontott malwarekészítők számáról, eszerint pl. Észak-Koreának 9000 fő szakembere van, és ez szám bővül, de tőlük nem sokkal marad le sem Szíria, sem Irán, mely országoknak szintén 4500 fő felett áll az e tevékenységet végző szakembereik száma. Kb. 8 másodpercenként keletkezik egy új vírus, ezzel szemben a vírusölők nem képesek ilyen szintű fejlődésre. Manapság már nem weblapon fertőznek, hanem e-mailekben. Szerinte a

legnagyobb veszélyt az okozná, hogyha nem az egyes felhasználókat, hanem az állami hálózatot tennék zombivá.

A plenáris ülés után rövid alkalom nyílt arra, hogy az előadóknak kérdéseket tehessünk fel.

SZAKMAI BESZÁMOLÓ

PADS SZAKKOLLÉGIUMI PROGRAM
2014/2015

A szekció

Máté István Zsolt doktorandusz, Rendészeti Doktoranduszok Országos Egyesülete, igazságügyi informatikai szakértő: Felhőszolgáltatások – a kiberbiztonságtól a szakértői bizonyításig

Mi is a felhőszolgáltatás? Részletesen elmagyarázta, hogy napjainkban mi tartozik ezen kategória alá és hogyan is képzelhetjük el mindennek működését. Előadásában bemutatásra került elméleti szinten a Staas (szolgáltató alkalmazásainak használata), a Saas, a Paas (ügyfél alkalmazásainak futtatása, Iaas (tárolási kapacitás bérlése). Ezt követően történelmi előzményekről tanulhattunk a cloud forensic történelméből. A felhőszolgáltatásokkal nyomozási szempontból a legnagyobb probléma az, hogy ez egy dinamikus digitális bizonyíték, ami nem egy gépen található, hanem folyamatosan mozog az adat az egyik szerverről a másikra. Sajnos a magyar jogban ez még nincs szabályozva sem.

Bemutatásra került a módszertana, hogy mik azok a legfontosabb követelmények, amelyeknek teljesülnie kellene, hogy legálisan működhessen a felhőszolgáltatás. Ilyenek voltak az ellenőrizhetőség, megismételhetőség, reprodukálhatóság, igazolhatóság, azonosítás, összegyűjtés, kinyerés, megőrzés. Ezt követően a módszertani és gyakorlati feladatokról esett szó, hogy mivel lehetne gördülékenyebbé tenni az igazságügyi informatikus szakértő és a nyomozóhatóság együttműködését. A legnagyobb problémát az okozza, hogy a felhő más országokat is érint, emiatt nehéz a beszerezni, mert az ottani jogrendszer nem biztos hasonló, sőt legtöbbször nagyban eltér a miénktől, ezáltal fennáll a veszélye, hogy az adatot nem adják ki más országoknak.

SZAKMAI BESZÁMOLÓ

PADS SZAKKOLLÉGIUMI PROGRAM
2014/2015

dr. Márton András tanár, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Magánbiztonsági és Önkormányzati Rendészeti Tanszék: A magánszféra bevonásának modellje a vállalati- információvédelmi feladatok ellátásába Németországban

Hangzatos statisztikai adatokkal nyitotta előadását, olyanokkal, mint pl. 2013-ban a Német gazdaságnak 1,6%-os GDP veszteséget okozott a kiberbűnözés, ez kevésnek tűnik százalékban kifejezve, de ha 4.000 milliárd dollárra gondolunk, akkor ez hatalmas veszteség. Ehhez képest Magyarországnak 0,41%-os GDP veszteséget okoz ugyanez a jelenség, ami alacsonyabb az EU átlaghoz képest, ami 0,63%. Körülbelül 64.000 IT támadás éri Németországot évente, de fontos kihangsúlyozni, hogy ez az adat csak a felfedett eseteket tartalmazza, tehát ennek többszörösével számolhatunk a valóságban. A Németországot érő támadások főleg Kínából, Oroszországból és USA-ból érkeznek. Az előadó a látens támadást két kategóriába sorolta, az egyik az, amikor a sértett nem veszi észre, hogy áldozatul esett, a másik, amikor a támadás bejelentése rontana a cég vagy személy hírnevének. A támadott célpontok nagyrészt a minősített adatok, hatósági nyilvántartások, ipari üzemek adatai, pénzintézetek, vegyipar, járműgyártás, megújuló energia, növényi nemesítés és a hadi ipar.

Zárásként és röviden, mivel a 15 perces limit kötötte beszélt az Alkotmányvédelmi Hivatal Awareness programjáról, amely elmondása szerint még a rendészeti dolgozók körében sem annyira ismert, pedig nagyon jó lenne beépíteni minden védekezésre jogosult szerv tudatába.

dr. Gyaraki Réka doktorandusz, Rendészeti Doktoranduszok Országos Egyesülete, nyomozó, Budapesti Rendőr-főkapitányság: Gyermekek biztonsága a kibertérben

Gyaraki Réka r. főhadnagy a „Gyermekek biztonsága a kibertérben" címmel tartott előadást, a gyermek-és fiatalkorúakra irányuló folyamatos fenyegetésről a kibertérben. Az internetes közösségi oldalakon mára már mindenki rajta van, saját illetve kitalált névvel. Az előadás rávilágított arra, hogy önmagában nem az a probléma, ha valaki nem a saját adataival regisztrál, hanem ha ezt mások megtévesztésére céljából teszi.

A weben található tartalmak lehetnek illegálisak, amik büntetendőek, de sok adat „csak káros", ami még önmagában nem büntetendő, de a fiatalkorúak erkölcsi fejlődését veszélyeztetheti. Az online zaklatás, vagyis a cyberbullying egy új típusa az elsősorban kamaszok közötti infokommunikációs eszközök segítségével elkövetett iskolai zaklatásnak vagy kiközösítésnek, ami durvább csúfolódásokból, kárörvendésből és fenyegetésből álló, az áldozathoz eljutó üzenetek sorozatát jelenti, melyet egyetlen, vagy több felhasználó végez. Emellett szó volt még a szülők megítéléséről és felelősségéről a témában. Az előadás rávilágított arra, hogy gyermekeiket nem védik fokozottan és következetesen az világháló veszélyeitől. Ennek oka lehet a hanyagság, a felelőtlenség, a tudatlanság és a kamaszok felé nyújtott túlzott bizalom mind előzményei az elektronikus zaklatásnak. Ezért fontos az informatikai biztonság, a megfelelő jelszavak, az adatkezelés szabályainak betartása. Megoldás lehetne a szülők és a gyermekek folyamatos oktatása és felvilágosítása már az általános iskolától kezdve. A fiatalkorúak ellen irányuló internetes bűncselekmények közé tartozik a gyermekpornográfia, a személyes és közérdekű adatokkal való visszaélés, a zaklatás, a magán- és levéltitok megsértése, a becsület csorbítására alkalmas hang és képfelvétel készítése, becsületsértés, stb. Az érintettek nagyrészt fiatalkorúak az elkövető pedig lehet bárki. A szülők az iskola és a Rendőrség feladata a prevenció és a segítségnyújtás. Az internethasználat helyes használatának minél fiatalabb korban való tudatosítása. A káros vagy illegális tartalmakat jelenteni kell, amit a safarinternet.hu-n illetve az internethotline.hu-n tehetünk meg.

***Dr.* jur. *Székely Zoltán r. őrnagy* egyetemi tanársegéd: A robotok rendészeti célú felhasználása során alkalmazott automatikus adattovábbítások biztonsági kockázatai- Robotok és a Prümi Szerződés**

Az előadó hivatásosok által kitöltött kérdőíves kutatásai során arra a következtetésre jutott, hogy a rendőrök nagy része pozitív véleménnyel van a robotok rendészeti felhasználásáról és támogatnák a biometrikus azonosító eszközök alkalmazását munkájuk során. Szabálysértési nyomtatványok kitöltését elvégezné egy gép, mely átlagosan tizenkét munkaórájukból legalább hármat elvesz. A sisak és autó kamera rendszerek pedig biztonságosabbá tennék munkájukat és bizonyítékként szolgálhatnának az esetleges

szabálysértések és bűncselekmények elbírálásakor. Az információszabadság alapjog, ami viszont ütközik a szabadság és biztonság jogával. Kérdés viszont, hogy az alapjog túlvédése nem ad-e segítséget feltűnés nélküli terrorcselekmények és bűncselekmények elkövetésére, illetve biztonsági érdekből szabad-e alapjogot korlátozni. A korlátozás forrásai lehetnek nemzeti vagy szövetségi alkotmányok és nemzetközi szerződések, uniós tagállamok esetében uniós jog vagy nemzeti jogszabályok. Szó volt továbbá a Prümi szerződésről, ami DNS-adatok tagállamok közötti cseréjét teszi lehetővé. Ez a DNS-adatokokról és ujjlenyomatokról, gépjármű nyilvántartási adatokról, személyes-és nem személyes adatokról szóló információk cseréjét könnyíti meg a tagállamok között, a határokon átnyúló bűnözés és a nemzetközi terrorizmus elleni harc érdekében, valamint az illegális migrációval összefüggésben. Az EP támogatta a szerződés kiterjesztését az összes tagállamra. A határozat célja az Európai Unió tagállamai közötti, határokon átnyúló rendőrségi és igazságügyi bűnüldözési együttműködés megerősítése. Különösen törekszik a bűncselekmények megelőzéséért és kivizsgálásáért felelős hatóságok közötti információcsere javítására.

A 2014-2020 ciklus középtávú kutatási terve a robotok rendészeti alkalmazására uniós és hazai pályázati források nemzetközi konzorciuma magyar vezetéssel. Cél olyan rendőrségi robotok kifejlesztése, amik egyben piacképes biztonsági robotokként is szolgálnának.

SZAKMAI BESZÁMOLÓ

PADS SZAKKOLLÉGIUMI PROGRAM
2014/2015

B szekció

Arany Bíró Martin hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Szent György Szakkollégium: Kiberbiztonság Nyugatról Keletre

Az előadás fő témája a kiberbűnözést nyugat és kelet viszonylatában volt. Az előadó kitért magára a téma aktualitására és az adaptációs lehetőségekre, kifejtette, hogy mi is valójában a kiberbűnözés, és a digitális térben történő bűnözés. Európában egyre nagyobb hangsúlyt kap a kiberbűnözés elleni küzdelem. Martin rávilágított arra, hogy mindehhez hogyan kapcsolódik az internet és a számítógép, valamint prezentált nemzetközi támadásokat és azok felderítési módszereit nemzetközi kitekintésben.

Girhiny Kornél tanár, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Kriminalisztikai Tanszék: A nyomozások új irányvonalai, a technikai jellegű bizonyítási módszerek dominanciája

A napjainkban folyó nyomozások során kollégáink naponta találkoznak olyan új típusú kihívásokkal, melyek megoldása egyre sürgetőbb. Taxatív felsorolás helyett az előadó komplexitásában értékelte a változó folyamatokat az előadás során. Ezen gondolatok mentén bizonyos tendenciákat külön kiemelt, és ezekre a jelenségekre ki is tért előadásában.
Az egyik ilyen jelenség az a taktikai jellegű bizonyítással kapcsolatos tendencia, mely szerint ezen módszerek gyakran másodlagos szerepet kapnak a bizonyításban. A másik, ezzel szorosan összefüggő jelenség a technikai jellegű bizonyítási módszerek felértékelődése, mind a nyomozásban, mind pedig a bizonyításban.
Annak a vizsgálata, hogy mely sarokpontok mentén változtak meg a nyomozások, az előadásnak nem voltak tartalmi elemei, azonban napjaink nyomozásainak új irányvonalai az előadás szerves részét képezték.

SZAKMAI BESZÁMOLÓ

PADS SZAKKOLLÉGIUMI PROGRAM
2014/2015

Zsákai Lénárd hallgató, Nemzeti Közszolgálati Egyetem Rendészettudományi Kar Szent György Szakkollégium: Biometrikus azonosításon alapuló biztonságtechnikai rendszerek, rendészeti alkalmazásuk jelene és jövője

„Ki kell használnunk az új technológia nyújtotta lehetőségeket, melyek biztosítják határainkon a magas szintű biztonságot, s közben könnyítik a törvényes utasok utazását"- egy Alan Sharer, Írország igazságügyi és esélyegyenlőségi miniszterének szájából 2014. februári Európai Bizottsági konferencián elhangzott idézettel indította előadását. A határok ellenőrzésére vonatkozó jövőképet nagymértékben az újabb és újabb technológiák alkotják, melyek hatékonyságuk, komfortjuk valamint gyorsaságuk által nagymértékben megnövelnék a határellenőrzésben és biztonságtechnikában betöltött szerepüket. A technológia kulcsa napjainkban nem más, mint a biometria, az ember egyedi, biometrikus azonosítóinak felhasználása az ellenőrzések során. Az előadás központi kérdésköre volt, hogy miként lehet jelen a biometrikus azonosítás a magánbiztonságban és a rendészetben, s a jövőre tekintettel a korszerű, egyelőre jórészt magánbiztonsági szférában (pl. Groupama Aréna) alkalmazott beléptető, személyazonosító rendszerek hogyan válhatnak a rendészeti munka, különösen a határrendészetben alkalmazott személyazonosítás, beléptetés, jogosultság ellenőrzés stb. egyik „alappillérévé".

Poór Péter Készenléti Rendőrség Nemzeti Nyomozó Iroda Csúcstechnológiai Bűnözés Elleni Osztály: A jelen vagy a jövő kihívása? A Darknet

Az internet sötét oldala az a felület, amit a hagyományos értelemben vett internetezés során nem láthatunk. Speciális módon lehet bejutni a darknetbe, és lehetőségeket biztosít a bűncselekményekhez kötődő tárgyakkal, szerekkel, filmekkel kereskednek ezen a felületeken. A legalapvetőbb példák erre: gyermekpornográfia, kábítószer, fegyverek. Akadnak extrém esetek is, találtak már olyan oldat is, ahol meghatározott összegért bérgyilkost lehet felfogadni. A darknet kereső motorja az úgynevezett Thor program, amely nagyjából egy böngészőnek felel meg a hagyományos felszínű internetnél. Az ezeket használó személyeket igen nehéz felkutatni, ilyennel foglalkozik az FBI, nálunk az NNI csúcstechnológiai osztály. Az előadó előadásában láthattunk különböző képeket, és példákat a darknet világáról. A

darnethez hozzá tartozik egy speciális fizető eszköz, bitcoin, ezzel fizetnek, amit legtöbbször dollárral, de egyéb valutákkal is ki lehet váltani, pl. euró. A darknet, valamint az ezzel való küzdelem napjaink egyik legfontosabb kihívása, a technológia folyamatos fejlődése miatt.

SZAKMAI BESZÁMOLÓ

PADS SZAKKOLLÉGIUMI PROGRAM
2014/2015

A konferenciáról interneten megjelent oldalak:

https://www.facebook.com/events/667170093380262/?ref_newsfeed_story_type=regular

http://rtk.uni-nke.hu/uploads/media_items/meghivo-a-kiberbiztonsag-cimu-konferenciara.original.pdf