Hadtudomány, kiberbiztonság
2020. október 16. 13.00-14.45
Szekciófelelős:
Tóth Beatrix, +36 70 529 6073

Hadtudomány

	Szekcióelnök:	**Hadtudomány, kiberbiztonság Dr. Németh András, alezredes (NKE)**
II. panel	**13.00-13.15**	Kiss Adrienn
	13.15-13.30	Sándor Barnabás
	13.30-13.45	Katona Gergő
	13.45-14.00	Deák Veronika
	14.00-14.15	Hankó Viktória
	14.15-14.30	Balogh Péter
	14.30-14.45	Dub Máté

Hadtudomány, kiberbiztonság
2020. október 16. 13.00-14.45
Szekciófelelős:
Tóth Beatrix, +36 70 529 6073

Mongúz vs. cyberbullying

KISS Adrienn
Nemzeti Közszolgálati Egyetem
Kiberbiztonság
adriennk73@gmail.com

Napjainkban, a világ számtalan csodálatos dolgot nyújt a számunkra. Ilyen fantasztikus dolgoknak számítanak a különféle elektronikus eszközök és az Internet. Viszont az idő alatt, míg ez az új világ, kezdve a kibertérrel és a vele járó előnyökkel kitárult előttünk, a ránk leselkedő veszélyek is megnövekedtek és fejlődtek. Sajnálatos módon felütötte fejét többek között az adathalászat, adatlopás, a pénzlopás, identitáslopás, de ami a kutatásom szempontjából most lényeges, az az online zaklatás, más néven cyberbullying is. Több kutatás is kimutatja, hogy sajnos az általános és középiskolások körében egyre gyorsabb ütemben növekedik az internetes zaklatás előfordulása. Viszont nem lehet még fellelni egyetlen, széles körben ismert, jól működő megoldást sem, amely megállítaná és visszaszorítaná ezt a jelenséget, így a fiatalabb generáció egészséges önértékelés hiányában tűzzel harcol a tűz ellen.

Régebben a fiatalok körében kézzel foghatóan tapasztalható volt a hagyományos bántalmazás, zaklatás és a vele járó következmények, ám manapság a virtuális harcok során, csak idővel lehet észrevenni a súlyos vele járóit a másikkal való erőszaknak, gorombaságnak, durvaságnak.

De mégis hogyan, miért alakult ki napjainkban az internetes zaklatás? Mit tudunk vele kezdeni? Hogyan tudjuk felvenni ezzel a harcot?

Előadásomban ezekre a kérdésekre szeretnék választ adni és bemutatni, hogy hiába sokasodnak a problémák a fiatalok körében a bántalmazások „népszerűsödésével", a jövőben egy jól működő megoldást is ugyanúgy tudunk erre találni. Már létező programcsomagokkal és egy konkrét, feltörekvő alkalmazás bemutatásával szeretném felhívni a figyelmet az Internet és a vele járó applikációk tudatos használatának fontosságára. A Mongu for Teen nevezetű alkalmazással, vajon meg lehet állítani az egyre növekedő számú online zaklatásokat? A kutatásommal erre keresem a választ, előadásomban pedig, ezt a választ meg is osztom.

Hadtudomány, kiberbiztonság
2020. október 16. 13.00-14.45
Szekciófelelős:
Tóth Beatrix, +36 70 529 6073

Okosvárosok kiberbiztonságának helyzetfelmérése IoT eszközök aspektusában

SÁNDOR Barnabás
Óbudai Egyetem, Biztonságtudományi Doktori Iskola
Had- és rendészettudomány
sandor.barnabas@gmail.com

DR. SZÁDECZKY Tamás
Óbudai Egyetem, Kandó Kálmán Villamosmérnöki Kar
Had- és rendészettudomány
szadeczky.tamas@kvk.uni-obuda.hu

Kutatásunkban a 21. század új városi modelljének az okos város vagy „future city” névre keresztelt megvalósítási koncepció keretében vizsgálom a „Dolgok Internete” (Internet of Things - IoT) rendszerek kiberbiztonsági aspektusait. Ezen városokban alkalmazott technológiák folyamatosan fejlődnek és épülnek, melyek védelméről folyamatosan gondoskodnia kell a szakembereknek. Ezen rendszerek az alap fizikai, beágyazott rendszertől, a szoftvereken át, az üzemeltető személyekig rejthetnek magukban sérülékenységeket. Az új technológiai irány megoldást kínálhat a városaink újratervezésére és az üzemeltetésének környezetkímélő módon való alkalmazására, továbbá élhetőbb környezet megteremtésére. Kutatásom során összegyűjtöttük ezen alkalmazási területeket, hatásvizsgálatot végeztünk, ezt követően pedig legalkalmasabb területre fókuszálva ajánlást készítettünk a hatályos jogszabályok alapján a rendszer implementálására.

A kutatással a célunk az volt, hogy feltérképezzük az IoT eszközök és az alkalmazott rendszerek technológia alkalmazásának lehetőségét a világ fejlett országaiban, kiberbiztonsági szempontból. Hatásvizsgálat keretében megvizsgáltuk azokat a területeket, ahol felhasználható a technológia, majd biztonsági, jogi és gazdasági szempontok alapján elemeztük az integrálhatóságát. Empirikus elemzést végeztünk a felhasználási lehetőségekről és a technológia sérülékenységéről, feldolgozva hazai és nemzetközi szakirodalmat. Mérnöki szempontból megvizsgáltuk az alkalmazható eszközök szabványi és keretrendszeri hátterét, melyek beletartozhatnak például az alábbiakba: GDPR, IEEE 802.11, MQTT, NIST IES-City Framework.

Összegezve, kutatásunkban bemutattuk az okosváros és IoT technológiában rejlő lehetőségeket és veszélyeket, a gazdaságra vonatkozó hatásainak feltárását, ami indokolttá teszi a korábban tárgyalt biztonságos keretrendszer megalkotását és legitimitását.

Kulcsszavak: okosváros, kiberbiztonság, IoT, NIST IES-City, MQTT

Hadtudomány, kiberbiztonság
2020. október 16. 13.00-14.45
Szekciófelelős:
Tóth Beatrix, +36 70 529 6073

A távoli munkavégzés tömeges megjelenése a SARS-CoV-2 vírus alatt , és annak információ- és kiberbiztonságra gyakorolt hatása

KATONA Gergő
Nemzeti Közszolgálati Egyetem, Államtudományi és Nemzetközi Tanulmányok Kar
Kiberbiztonság
katonagergo520@gmail.com

2019 decemberében a kínai Vuhan tartományban egy ismeretlen tüdőgyulladásos betegség ütötte fel a fejét, ami igen gyorsan terjedt először az említett tartományban, majd Kínából kiszabadulva a világ nagy részén is megjelent ez a vírusos megbetegedés, Magyarországon 2020. március elején regisztrálták az első fertőzötteket. Világszerte kijárási korlátozásokat vagy éppen tilalmat rendeltek el, amivel - a köznyelven koronavírusként ismert SARS-CoV-2- vírus terjedését próbálták, illetve és mai napig próbálják lassítani. A védelmi intézkedések az élet számos területére nagy hatást gyakoroltak, a gazdasági tevékenységek számos országban szinte teljesen leálltak, emberek milliói veszítették el az állásukat. Egyik napról a másikra egyes közigazgatási szerveknek és a gazdasági vállalatok nagy részének kellett átállni távoli munkavégzésre. A szerző a kutatásában feltárja azon kockázatokat, amelyek a távoli munkavégzés során a közigazgatási szerveket és vállalatokat fenyegetik. Megvizsgálja azon lehetősségeket, amelyekkel az általa által feltárt és rendszerezett fenyegetéseket csökkenteni, illetve megszüntetni lehet.

Kulcsszavak: távolimunkavégzés, koronavírus, covid-19, kiberbiztonság, home office

Hadtudomány, kiberbiztonság
2020. október 16. 13.00-14.45
Szekciófelelős:
Tóth Beatrix, +36 70 529 6073

A közszolgálati kibervédelmi képesség gyakorlati képzésének technikai és technológiai alapjai

DEÁK Veronika
Nemzeti Közszolgálati Egyetem – Katonai Műszaki Doktori Iskola
Védelmi elektronika, informatika és kommunikáció
deak.veronika@uni-nke.hu

A közszolgálat kiemelt célpontja a kibertámadásoknak, így ezek megelőzése és eredményes elhárítása érdekében különösen nagy hangsúlyt kell fektetni a különféle szervezetek védelmi képességeinek kialakítására és folyamatos fejlesztésére. Ennek részeként értelmezhető a lehetséges támadási alternatívák megismerését és alkalmazhatóságát célzó közszolgálati kiberbiztonsági képzés megalkotása.

A képzési program kialakítása során az elméleti oktatás mellett a hallgatók gyakorlati készségeinek fejlesztésére is kiemelt figyelmet kell fordítani. Ehhez szükséges a képzés gyakorlati részének, valamint a technikai és technológiai alapjainak meghatározása, amely során a hallgatók különféle kibertámadásokkal szembesülhetnek. A konkrét támadások szimulálásával a már meglévő tudásra alapozva összekapcsolható az elméleti és a gyakorlati tudás. Ennek következtében a hallgatók képesek lesznek felismerni a kibertérből érkező fenyegetéseket, támadásokat és az esetleges kockázatokat. A képzés gyakorlati része során a mindennapos üzemeltetési feladatokkal és az információs rendszer, valamint az ehhez kapcsolódó folyamatok, eljárások megfelelőségének ellenőrzésével is meg kell birkózniuk a hallgatóknak.

Jelen előadás egy kétlépcsős gyakorlati képzés felépítését mutatja be, ahol a hallgatók először a saját infokommunikációs eszközük védelmi mechanizmusaival ismerkednek meg, majd szimulált környezetben a támadások elhárítását hajtják végre. A második szinten egy fiktív szervezeti infrastruktúra általános architektúráját, komponenseit, illetve azok védelmi mechanizmusait azonosítják, majd szimulált kibertámadások során védelmi stratégiákat alkalmaznak. A bemutatott kétlépcsős képzés megvalósításához definiálásra kerül egy általános keretrendszer, amely megfelelő platformot biztosít kibertámadások szimulációjához és az azok során alkalmazandó védelmi eszközök, eljárások kipróbálásához.

Kulcsszavak: kiberbiztonság, közszolgálati kiberbiztonsági képzés, kibertámadás, képzési program, gyakorlati képzés

Hadtudomány, kiberbiztonság
2020. október 16. 13.00-14.45
Szekciófelelős:
Tóth Beatrix, +36 70 529 6073

A drónok adatvédelmi kérdései

HANKÓ Viktória
Nemzeti Közszolgálati Egyetem, Államtudományi és Nemzetközi Tanulmányok Kar
Kiberbiztonság
hanko.viktoria@hallg.uni-nke.hu

Napjainkban egyre többször és többször találkozhatunk a drónok megjelenésével legyen szó akár a köz-, akár a magánszféráról. A pilóta nélküli légijárművek feltűnése, elterjedése különböző kérdéseket vet fel, amelynek megítélésem szerint egyik legfontosabb eleme az adatvédelemmel kapcsolatos témakör. Többször hallhattunk már olyan esetről, mikor egy csendes szombati napon egy drón berepült egy magánszemély kertjébe, ezzel megfigyelve az ő tevékenységét. Az esetre vonatkozó jogi szabályozások a világ különböző részein nem egységesek, bizonyos helyeken megengedőbbek a szabályok, bizonyos helyeken szigorúbbak, és olyan esetre is találhatunk példát, ahol a teljes szabályozás hiányzik. Magyarországra, mint az Európai Unió (EU) tagjára kiterjednek az egyesülés drónokkal kapcsolatosan alkotott rendeletei, melynek megalkotásában és betartásában segédkezik Európai Repülésbiztonsági Ügynökség (EASA) is. Azonban ez csak a tagállamokra terjed ki, a világ különböző részein más-más szabályozások érvényesek. A jogi szabályozásból, vagy annak hiányából eredhet az adatvédelmi kockázat, mely további problémákat jelenthet a magánszférával kapcsolatban.

Az előadás célja a releváns hazai és nemzetközi szakirodalmak összehasonlításával bemutatni a drónok különböző típusait, felhasználási területeit és az ezekben rejlő innovációs lehetőségeket. Emellett a különböző jogi szabályozásokat is ismertetem, (amennyiben van) hazai és nemzetközi szinten egyaránt. Ezek közül kiemelve az Európai Unión belüli szabályozásokat, ajánlásokat, valamint a készülő magyarországi jogszabály is szemléltetésre kerül. Végül, de nem utolsó sorban a különböző kockázatok is felsorolásra és kifejtésre kerülnek, valamint ezekre reflektálva különböző megoldási javaslatokkal is készülök az előadáshoz.

Kulcsszavak: drón, adatvédelem, magánszféra, kockázat, kiberbiztonság

Hadtudomány, kiberbiztonság
2020. október 16. 13.00-14.45
Szekciófelelős:
Tóth Beatrix, +36 70 529 6073

Kiberhadviselés és globális kiberfenyegetettség – Az államok által támogatott kiberműveletek nemzetközi hálózatának elemzése

BALOGH Péter
Szegedi Tudományegyetem
Szociológia
baloghp@socio.u-szeged.hu

A tervezett prezentáció keretében a kiberműveletek globális hálózatának elemzését célzó kutatómunkánk főbb eredményeiből kívánunk áttekintést nyújtani.
Az info-kommunikációs technológiák egyre szélesebb körű elterjedése és a társadalmi élet megannyi folyamatában egyre meghatározóbbá válása a fejlett jóléti társadalmak nagyfokú átalakulásához vezetett. A folyamat a XXI. század második évtizedének közepére-végére olyan szintre jutott el, hogy a gazdasági-üzleti, a kommunikációs, a technológiai és a jóléti társadalmi szféra mellett a politika és a nemzetközi konfliktusok kérdéskörének szakterülete is szembesül a jelenség meghatározó, szinte mindent átható következményeivel (lásd pl. Beck 2008, Castells 2005). Utóbbi tekintetben mindez – viszonylag rövid idő alatt – egy új területté önállósodott, s stratégiai, szakpolitikai és egyéb szinteken egyaránt megjelent a kibertér és a kiberhadviselés mint az átalakuló biztonsági környezet egy kiemelt dimenziója (lásd pl. Kiss 2019). Hiszen pl. a globális gazdaságban a különféle üzleti csoportok, gazdasági érdekek versenyszituációban tevékenykedő szereplői mellett nemzetközi porondon az egyes államok is egyértelműen a stratégiai előny kivívásának, ill. fenntartásának hatékony terepeként tekintenek a kibertér adta lehetőségekre (Kovács 2018: 169-174).

Prezentációnkban arra vállalkozunk, hogy feltárjuk és átfogóan bemutassuk korunk kibertérben zajló műveleteit, támadásait – mind azok általánosabb jellemezőinek, mind pedig a szereplők viszonyrendszerének felderítésével. Kutatómunkánk keretében internetes források alapján, a nyilvánosságra került, államok által támogatott kiberműveletekre vonatkozó információk, adatok alapján, illetve azok további mutatókkal történő kiegészítésével komplex adatbázist építettünk, melyek elsődleges bemeneti forrásként szolgálnak az adatelemzések lefolytatásához. Elemzőmunkánk keretében egyrészt alapszintű statisztikai eljárásokat használunk, másrészt a társadalmi kapcsolatháló elemzés bizonyos – ugyancsak jellemzően alapvető – eljárásait alkalmazzuk, kiegészítve a megfelelő grafikus vizualizációs technikákkal.
Az elemzőmunka eredményeinek áttekintése során egyrészt felvázoljuk az államok által támogatott kiberműveletek jellemző vonásait illetve típusok szerinti eloszlásait, másrészt feltárjuk a kibertámadások mint az egyes országok közötti viszonyrendszer alapján felépülő globális hálózat főbb sajátosságait – különös tekintettel az egyes országok helyzetére egyedileg, illetve a teljes hálózat viszonylatában.
Eredményeink alapján – egyebek mellett – megfogalmazható, hogy az államok által támogatott kiberműveletek globális hálózata a komplex hálózatok sajátos jegyeit mutatja – számos többszörös, ill. több kölcsönös kapcsolattal illetve változatos strukturális pozíciókkal –, s a teljes hálózatbeli pozíció összefüggést mutat az egyes országok jellemzőivel (azaz pl. jellemzően a kevéssé demokratikus államok esetében mérhető magasabb támadási gyakoriság).
A tervezett prezentáció végén az eredmények összegzésén túl a további lehetséges kutatási irányok felvázolására is kitérünk.

Hadtudomány, kiberbiztonság
2020. október 16. 13.00-14.45
Szekciófelelős:
Tóth Beatrix, +36 70 529 6073

Phishing támadások - Empirikus kísérletek eredményei magyar viszonylatban

DUB Máté
Nemzeti Közszolgálati Egyetem
Kiberbiztonság
Dub.Mate@hallg.uni-nke.hu

A XXI. században az információs társadalom kialakulásának, és a technológia rohamos fejlődésének köszönhetően napjainkban a kiberteret, az úgynevezett ötödik műveleti teret tekinthetjük az egyik legjelentősebb biztonsági kockázatnak. Ezt leginkább a globális szinten is szignifikánsan növekvő kibertámadások száma támasztja alá. A célpontok skálája pedig az állami szinttől egészen a privát szféránkig terjedhet. A támadások hátterében a legkülönbözőbb indítékok is állhatnak, mint például a zsarolás, anyagi haszonszerzés, adatok jogosulatlan megszerzése, kritikus infrastruktúrák támadása, vagy akár államok belpolitikai döntéshozatalának befolyásolása. A támadási típusok, kampányok, trendek egyre kifinomultabban, egyre hatásosabban, az aktualitást szem előtt tartva szofisztikálódnak napról napra. A védelmi és a támadási képességek növelésének, stratégiák fejlesztésének lehetőségei jelentősen eltérnek, ugyanis a védelmi kiadások -a megfelelő hardware-es, software-es, és humán-tényezőket érintő fejlesztések- jelentősen magasabbak, mint az offenzív területen.
Az egyik legjelentősebb terület, ami egyben az egyik legveszélyesebb pont is a kiberbiztonságban, az maga az ember, más szóval a humán tényező.

Az egyik legjelentősebb humán-alapú támadási típus az úgynevezett phishing, vagyis adathalász támadás. Ezen kockázat csökkentésének egyik legkifizetődőbb módja az emberek felkészítése az új kihívásokra, hisz a támadók legkedveltebb célpontjai is ebben a csoportban találhatók, mely csoport tagjait pedig az alacsony szintű adat- és információbiztonság tudatossággal rendelkező polgárok alkotják.

A támadók egyik jelentős, és gyakran használt módszere a social engineering támadás. Ennek lényege, hogy a célpontokat a befolyásolás és rábeszélés eszközével tévesztik meg, manipulálják és meggyőzik őket, majd -akár technológia használatával, akár anélkül-, az embereket információszerzés céljából kihasználják.
Az előadás a humán támadásokat, a védekezési lehetőségeket, és a témával kapcsolatos -civilek és szakemberek körében elvégzett- empirikus kutatások eredményeit tartalmazza. A kísérletben a fent említett adathalász támadásnak és social engineering tevékenységnek voltak kitéve a résztvevők az offline térben. A 2 különböző empirikus kutatás tehát 2 teljesen különböző csoporton lett végrehajtva. Az első résztvevői egyetemi polgárok, munkatársak, civilek voltak, akik közül többen a jövőben az államigazgatásban, rendvédelmi és honvédelmi területen vezető pozícióban helyezkedhetnek el. A kontrollcsoport tagjait kifejezetten az IT- és kiberbiztonsággal, a social engineeringgel foglalkozó emberek csoportja adta. A kutatások eredményeként lehetőség nyílt a védelmi képességeket, legfőképp annak humán-aspektusát új perspektívában megvizsgálni. A végeredmény tekintetében pedig következtetések vonhatók le az oktatás, a potenciális fenyegetettség súlyának megértetése, valamint a megfelelő biztonságtudatosság kiépítésének tekintetében.